DSM Configuration Guide

Release 7.7.2.5

Published July 2015
9034854

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, 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 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

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, 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/support/

Contact

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

Toll-free: +1 888-257-3000

Table of Contents

About This Guide

The *DSM Configuration Guide* for SIEM provides you with information for configuring Device Support Modules (DSMs).

DSMs allow SIEM to integrate events from security appliances, software, and devices in your network that forward events to SIEM.

Audience

This guide is intended for the system administrator responsible for setting up OpenStack 2.0 in your network. This guide assumes that you have OpenStack 2.0 administrative access and a knowledge of your corporate network and networking technologies.

Formatting Conventions

The following notes are used to draw your attention to additional information:

NOTE

Notes identify useful information, such as reminders, tips, or other ways to perform a task.

CAUTION

Cautionary notes identify essential information, which if ignored can adversely affect the operation of your equipment or software.

WARNING

Warning notes identify essential information, which if ignored can lead to personal injury or harm.

Related Documentation

For more information, go to the Extreme Networks Support Portal to obtain the latest SIEM documentation: www.extremenetworks.com/documentation

Getting Help

For additional support related to the K10 chassis or this document, contact Extreme Networks using one of the following methods:

Website	http://support.extremenetworks.com/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 To find the Extreme Networks Support toll-free number in your country: www.extremenetworks.com/support/contact/
Email	support@extremenetworks.com

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.

1 Overview

The DSM Configuration guide is intended to assist with device configurations for systems, software, or appliances that provide events to SIEM.

Device Support Modules (DSMs) parse event information for SIEM products to log and correlate events received from external sources such as security equipment (for example, firewalls), and network equipment (for example, switches and routers).

Events forwarded from your log sources are displayed in the **Log Activity** tab. All events are correlated and security and policy offenses are created based on correlation rules. These offenses are displayed on the **Offenses** tab. For more information, see the *SIEM Users Guide*.

NOTE

Information found in this documentation about configuring Device Support Modules (DSMs) is based on the latest RPM files located on the Extreme Networks Support Portal at http://support.extremenetworks.com.

To configure SIEM to receive events from devices, you must:

1 Configure the device to send events to SIEM.

2 Configure log sources for SIEM to receive events from specific devices. For more information, see the *SIEM Log Sources User Guide*.

2 Installing DSMs

You can download and install weekly automatic software updates for DSMs, protocols, and scanner modules.

After Device Support Modules (DSMs) are installed the SIEM Console provides any rpm file updates to managed hosts after the configuration changes are deployed. If you are using high availability (HA), DSMs, protocols, and scanners are installed during replication between the primary and secondary host. During this installation process, the secondary displays the status Upgrading. For more information, see Managing High Availability in the *SIEM Administration Guide*.

CAUTION

Uninstalling a Device Support Module (DSM) is not supported in SIEM. If you need technical assistance, contact Customer Support. For more information, see Getting Help on page xxvi.

Scheduling Automatic Updates

You can schedule when automatic updates are downloaded and installed on your SIEM Console.

SIEM performs automatic updates on a recurring schedule according to the settings on the Update Configuration page; however, if you want to schedule an update or a set of updates to run at a specific time, you can schedule an update using the Schedule the Updates window. Scheduling your own automatic updates is useful when you want to schedule a large update to run during off-peak hours, thus reducing any performance impacts on your system.

If no updates are displayed in the Updates window, either your system has not been in operation long enough to retrieve the weekly updates or no updates have been issued. If this occurs, you can manually check for new updates

Procedure

1 Click the **Admin** tab.

2 On the navigation menu, click **System Configuration**.

3 Click the **Auto Update** icon.

4 Optional. If you want to schedule specific updates, select the updates you want to schedule.

5 From the **Schedule** list, select the type of update you want to schedule. Options include:

- All Updates
- Selected Updates
- DSM, Scanner, Protocol Updates
- Minor Updates

NOTE

Protocol updates installed automatically require you to restart Tomcat. For more information on manually restarting Tomcat, see the *SIEM Log Sources User Guide*.

6 Using the calendar, select the start date and time of when you want to start your scheduled updates.

7 Click **OK**.

The selected updates are now scheduled.

Viewing Updates

You can view or install any pending software updates for SIEM through the **Admin** tab.

Procedure

1 Click the **Admin** tab.

2 On the navigation menu, click **System Configuration**.

3 Click the **Auto Update** icon.

The Updates window is displayed. The window automatically displays the Check for Updates page, providing the following information:

Table 1: Check for Updates Window Parameters

Parameter	Description
Updates were installed	Specifies the date and time the last update was installed.
Next Update install is scheduled	Specifies the date and time the next update is scheduled to be installed. If there is no date and time indicated, the update is not scheduled to run.
Name	Specifies the name of the update.
Type	Specifies the type of update. Types include: • DSM, Scanner, Protocol Updates • Minor Updates
Status	Specifies the status of the update. Status types include: • **New** - The update is not yet scheduled to be installed. • **Scheduled** - The update is scheduled to be installed. • **Installing** - The update is currently installing. • **Failed** - The updated failed to install.
Date to Install	Specifies the date on which this update is scheduled to be installed.

The Check for Updates page toolbar provides the following functions:

Table 2: Auto updates toolbar

Function	Description
Hide	Select one or more updates, and then click **Hide** to remove the selected updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page. For more information, see the *SIEM Administrator Guide*.
Install	From this list, you can manually install updates. When you manually install updates, the installation process starts within a minute.
Schedule	From this list, you can configure a specific date and time to manually install selected updates on your Console. This is useful when you want to schedule the update installation during off-peak hours.
Unschedule	From this list, you can remove preconfigured schedules for manually installing updates on your Console.
Search By Name	In this text box, you can type a keyword and then press Enter to locate a specific update by name.
Next Refresh	This counter displays the amount of time until the next automatic refresh. The list of updates on the Check for Updates page automatically refreshes every 60 seconds. The timer is automatically paused when you select one or more updates.
Pause	Click this icon to pause the automatic refresh process. To resume automatic refresh, click the **Play** icon.
Refresh	Click this icon to manually refresh the list of updates.

4 To view details on an update, select the update.

The description and any error messages are displayed in the right pane of the window.

Manually Installing a DSM

You can use the Extreme Networks Support Portal to download and manually install the latest RPM files for SIEM: http://support.extremenetworks.com

Most users do not need to download updated DSMs as auto updates installs the latest rpm files on a weekly basis. If your system is restricted from the Internet, you might need to install rpm updates manually. The DSMs provided on the IBM website, or through auto updates contain improved event parsing for network security products and enhancements for event categorization in the SIEM Identifier Map (QID map).

CAUTION

Uninstalling a Device Support Module (DSM) is not supported in SIEM. If you need technical assistance, contact Customer Support. For more information, see Getting Help on page xxvi.

Installing a Single DSM

The Extreme Networks Support Portal contains individual DSMs that you can download and install using the command-line.

Procedure

1 Download the DSM file to your system hosting SIEM.

2 Using SSH, log in to SIEM as the root user.
Username: `root`
Password: `<password>`

3 Navigate to the directory that includes the downloaded file.

4 Type the following command:
`rpm -Uvh <filename>`
Where `<filename>` is the name of the downloaded file. For example:
`rpm -Uvh DSM-CheckPointFirewall-7.0-209433.noarch.rpm`

5 Log in to SIEM.
https://`<IP Address>`
Where `<IP Address>` is the IP address of the SIEM Console or Event Collector.

6 On the Admin tab, click Deploy Changes.
The installation is complete.

Installing a DSM Bundle

The Extreme Networks Support Portal contains a DSM bundle which is updated daily with the latest DSM versions that you can install.

Procedure

1 Download the DSM bundle to your system hosting SIEM.

2 Using SSH, log in to SIEM as the root user.
Username: `root`
Password: `<password>`

3 Navigate to the directory that includes the downloaded file.

4 Type the following command to extract the DSM bundle:
`tar -zxvf SIEM_bundled-DSM-<version>.tar.gz`
Where `<version>` is your version of SIEM.

5 Type the following command:
`for FILE in *Common*.rpm DSM-*.rpm; do rpm -Uvh "$FILE"; done`
The installation of the DSM bundle can take several minutes to complete.

6 Log in to SIEM.
https://`<IP Address>`
Where `<IP Address>` is the IP address of SIEM.

7 On the Admin tab, click Deploy Changes.
The installation is complete.

3 3Com 8800 Series Switch

The 3COM 8800 Series Switch DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant status and network condition events forwarded from your 3Com 8800 Series Switch using syslog.

Configure Your 3COM 8800 Series Switch

You can configure your 3COM 8800 Series Switch to forward syslog events to SIEM.

Procedure

1 Log in to the 3Com 8800 Series Switch user interface.

2 Enable the information center.

```
info-center enable
```

3 Configure the host with the IP address of your SIEM system as the loghost, the severity level threshold value as informational, and the output language to English.

```
info-center loghost <ip_address> facility <severity> language english
```

Where:

`<ip_address>` is the IP address of your SIEM.

`<severity>` is the facility severity.

4 Configure the ARP and IP information modules to log.

```
info-center source arp channel loghost log level informational
info-center source ip channel loghost log level informational
```

The configuration is complete. The log source is added to SIEM as 3COM 8800 Series Switch events are automatically discovered. Events forwarded to SIEM by 3COM 880 Series Switches are displayed on the **Log Activity** tab.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from 3COM 8800 Series Switches. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select 3Com 8800 Series Switch.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 3: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your 3COM 8800 Series Switch.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

4 Ambiron TrustWave ipAngel

The Ambiron TrustWave ipAngel DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all Snort-based events from the ipAngel console.

Before You Begin

Before you configure SIEM to integrate with ipAngel, you must forward your cache and access logs to your SIEM. The events in your cache and access logs that are forwarded from Ambiron TrustWave ipAngel are not automatically discovered. For information on forwarding device logs to SIEM, see your vendor documentation.

Configure a Log Source

To integrate Ambiron TrustWave ipAngel events with SIEM, you must manually configure a log source.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 4: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Ambiron TrustWave ipAngel appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Ambiron TrustWave ipAngel are displayed on the **Log Activity** tab.

5 Ahnlab Policy Center

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

6 Apache HTTP Server

The Apache HTTP Server DSM for SIEM accepts Apache events using syslog or syslog-ng.

SIEM records all relevant HTTP status events. The procedure in this section applies to Apache DSMs operating on UNIX/Linux platforms only.

Do not run both syslog and syslog-ng at the same time.

Select one of the following configuration methods:

- Configuring Apache HTTP Server with syslog on page 3
- Configuring Apache HTTP Server with syslog-ng on page 4

Configuring Apache HTTP Server with Syslog

You can configure your Apache HTTP Server to forward events with the syslog protocol.

Procedure

1 Log in to the server hosting Apache, as the root user.

2 Edit the Apache configuration file httpd.conf.

3 Add the following information in the Apache configuration file to specify the custom log format:

```
LogFormat "%h %A %l %u %t \"%r\" %>s %p %b" <log format name>
```

Where `<log format name>` is a variable name you provide to define the log format.

4 Add the following information in the Apache configuration file to specify a custom path for the syslog events:

```
CustomLog "|/usr/bin/logger -t httpd -p <facility>.<priority>"
<log format name>
```

Where:

`<facility>` is a syslog facility, for example, local0.

`<priority>` is a syslog priority, for example, info or notice.

`<log format name>` is a variable name you provide to define the custom log format. The log format name must match the log format defined in Step 4.

For example,

```
CustomLog "|/usr/bin/logger -t httpd -p local1.info" MyApacheLogs
```

5 Type the following command to disabled hostname lookup:

```
HostnameLookups off
```

6 Save the Apache configuration file.

7 Edit the syslog configuration file.

```
/etc/syslog.conf
```

8 Add the following information to your syslog configuration file:

```
<facility>.<priority> <TAB><TAB>@<host>
```

Where:

<facility> is the syslog facility, for example, local0. This value must match the value you typed in Step 4.

<priority> is the syslog priority, for example, info or notice. This value must match the value you typed in Step 4.

<TAB> indicates you must press the **Tab** key.

<host> is the IP address of the SIEM Console or Event Collector.

9 Save the syslog configuration file.

10 Type the following command to restart the syslog service:

```
/etc/init.d/syslog restart
```

11 Restart Apache to complete the syslog configuration.

The configuration is complete. The log source is added to SIEM as syslog events from Apache HTTP Servers are automatically discovered. Events forwarded to SIEM by Apache HTTP Servers are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source in SIEM

You can configure a log source manually for Apache HTTP Server events in SIEM.

SIEM automatically discovers and creates a log source for syslog events from Apache HTTP Server. However, you can manually create a log source for SIEM to receive syslog events. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Apache HTTP Server**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 5: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apache installations.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information on Apache, see www.apache.org/.

Configuring Apache HTTP Server with Syslog-ng

You can configure your Apache HTTP Server to forward events with the syslog-ng protocol.

Procedure

1 Log in to the server hosting Apache, as the root user.

2 Edit the Apache configuration file.
`/etc/httpd/conf/httpd.conf`

3 Add the following information to the Apache configuration file to specify the LogLevel:
`LogLevel info`
The LogLevel might already be configured to the info level depending on your Apache installation.

4 Add the following to the Apache configuration file to specify the custom log format:
`LogFormat "%h %A %l %u %t \"%r\" %>s %p %b" <log format name>`
Where `<log format name>` is a variable name you provide to define the custom log format.

5 Add the following information to the Apache configuration file to specify a custom path for the syslog events:
`CustomLog "|/usr/bin/logger -t 'httpd' -u /var/log/httpd/apache_log.socket" <log format name>`
The log format name must match the log format defined in Step 4.

6 Save the Apache configuration file.

7 Edit the syslog-ng configuration file.
`/etc/syslog-ng/syslog-ng.conf`

8 Add the following information to specify the destination in the syslog-ng configuration file:

```
source s_apache {
    unix-stream("/var/log/httpd/apache_log.socket"
    max-connections(512)
    keep-alive(yes));
};
destination auth_destination { <udp|tcp>("<IP address>"
port(514)); };
log{
    source(s_apache);
    destination(auth_destination);
};
```

Where:

`<IP address>` is the IP address of the SIEM Console or Event Collector.

`<udp|tcp>` is the protocol you select to forward the syslog event.

9 Save the syslog-ng configuration file.

10 Type the following command to restart syslog-ng:

```
service syslog-ng restart
```

11 You are now ready to configure the log source in SIEM.

The configuration is complete. The log source is added to SIEM as syslog events from Apache HTTP Servers are automatically discovered. Events forwarded to SIEM by Apache HTTP Servers are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

You can configure a log source manually for Apache HTTP Server events in SIEM.

SIEM automatically discovers and creates a log source for syslog-ng events from Apache HTTP Server. However, you can manually create a log source for SIEM to receive syslog events. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Apache HTTP Server**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 6: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apache installations.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information on Apache, see www.apache.org/.

7 APC UPS

The APC UPS DSM for SIEM accepts syslog events from the APC Smart-UPS family of products.

NOTE

Events from the RC-Series Smart-UPS are not supported.

Supported Event Types

SIEM supports the following APC Smart-UPS syslog events:

- UPS events
- Battery events
- Bypass events
- Communication events
- Input power events
- Low battery condition events
- SmartBoost events
- SmartTrim events

Before You Begin

To integrate Smart-UPS events with SIEM, you must manually create a log source to receive syslog events.

Before you can receive events in SIEM, you must configure a log source, then configure your APC UPS to forward syslog events. Syslog events forwarded from APC Smart-UPS series devices are not automatically discovered. SIEM can receive syslog events on port 514 for both TCP and UDP.

Configuring a Log Source in SIEM

SIEM does not automatically discover or create log sources for syslog events from APC Smart-UPS series appliances.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select APC UPS.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 7: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your APC Smart-UPS series appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to configure your APC Smart-UPS to forward syslog events to SIEM.

Configuring Your APC UPD to Forward Syslog Events

You can configure syslog event forwarding on your APC UPS.

Procedure

1 Log in to the APC Smart-UPS web interface.

2 In the navigation menu, select **Network > Syslog**.

3 From the **Syslog** list, select **Enable**.

4 From the **Facility** list, select a facility level for your syslog messages.

5 In the **Syslog Server** field, type the IP address of your SIEM Console or Event Collector.

6 From the **Severity** list, select **Informational**.

7 Click **Apply**.

The syslog configuration is complete. Events forwarded to SIEM by your APC UPS are displayed on the **Log Activity** tab.

8 Amazon AWS CloudTrail

The SIEM DSM for Amazon AWS CloudTrail can collect audit events from your Amazon AWS CloudTrail S3 bucket.

The following table identifies the specifications for the Amazon AWS CloudTrail DSM:

Table 8: Amazon AWS CloudTrail DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	Amazon AWS CloudTrail
Supported versions	1.0
Protocol	Log File
SIEM recorded events	All relevant events
Automatically discovered	No
Includes identity	No
More information	http://docs.aws.amazon.com/awscloudtrail/latest/userguide/whatisawscloudtrail.html

AWS CloudTrail DSM Integration Process

To integrate Amazon AWS CloudTrail with SIEM, use the following procedure:

1 Obtain and install a certificate to enable communication between your Amazon AWS CloudTrail S3 bucket and SIEM.

2 Install the most recent version of the Log File Protocol RPM on your SIEM Console. You can install a protocol by using the procedure to manually install a DSM.

3 Install the Amazon AWS CloudTrail DSM on your SIEM Console.

4 Configure the Amazon AWS CloudTrail log source in SIEM.

Related tasks

Manually Installing a DSM on page 4

Enabling Communication between SIEM and AWS CloudTrail on page 19

Configuring an Amazon AWS CloudTrail Log Source in SIEM on page 19

Enabling Communication between SIEM and AWS CloudTrail

A certificate is required for the HTTP connection between SIEM and Amazon AWS CloudTrail.

Procedure

1 Access your Amazon AWS CloudTrail S3 bucket.

2 Export the certificate as a DER-encoded binary certificate to your desktop system. The file extension must be `.DER`.

3 Copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory on the SIEM host on which you plan to configure the log source.

Configuring an Amazon AWS CloudTrail Log Source in SIEM

To collect Amazon AWS CloudTrail events, you must configure a log source in SIEM. When you configure the log source, use the location and keys that are required to access your Amazon AWS CloudTrail S3 bucket.

Before You Begin

Ensure that the following components are installed and deployed on your SIEM host:

- PROTOCOL-LogFileProtocol-*build_number*.noarch.rpm
- DSM-AmazonAWSCloudTrail-*build_number*.noarch.rpm

Also ensure that audit logging is enabled on your Amazon AWS CloudTrail S3 bucket. For more information, see your vendor documentation.

About this task

The following table provides more information about some of the extended parameters:

Table 9: Amazon AWS CloudTrail log source parameters

Parameter	Description
Bucket Name	The name of the AWS CloudTrail S3 bucket where the log files are stored.
AWS Access Key	The public access key required to access the AWS CloudTrail S3 bucket.
AWS Secret Key	The private access key required to access the AWS CloudTrail S3 bucket.
Remote Directory	The root directory location on the AWS CloudTrail S3 bucket from which the files are retrieved, for example, *user_account_name*
FTP File Pattern	`.*?\.json\.gz`
Processor	GZIP

Table 9: Amazon AWS CloudTrail log source parameters

Parameter	Description
Event Generator	Amazon AWS JSON Applies additional processing to the retrieved event files.
Recurrence	Defines how often the Log File Protocol connects to the Amazon cloud API, checks for new files, and retrieves them if they exist. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **Amazon AWS CloudTrail**.

7 From the **Protocol Configuration** list, select **Log File**.

8 From the **Service Type** field, select **AWS**.

9 Configure the remaining parameters.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

9 Apple Mac OS X

The Apple Mac OS X DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant firewall, web server access, web server error, privilege escalation, and informational events.

Before You Begin

To integrate Mac OS X events with SIEM, you must manually create a log source to receive syslog events.

To complete this integration, you must configure a log source, then configure your Mac OS X to forward syslog events. Syslog events forwarded from Mac OS X devices are not automatically discovered. It is recommended that you create a log source, then forward events to SIEM. Syslog events from Mac OS X can be forwarded to SIEM on TCP port 514 or UDP port 514.

Configuring a Log Source

SIEM does not automatically discover or create log sources for syslog events from Apple Mac OS X.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Mac OS X.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 10: Mac OS X syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apple Mac OS X device.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to configure your Apple Mac OS X device to forward syslog events to SIEM.

Configuring Syslog on Your Apple Mac OS X

You can configure syslog on systems running Mac OS X operating systems.

Procedure

1 Using SSH, log in to your Mac OS X device as a root user.

2 Open the `/etc/syslog.conf` file.

3 Add the following line to the top of the file. Make sure all other lines remain intact:

```
*.*            @<IP address>
```

Where `<IP address>` is the IP address of the SIEM.

4 Save and exit the file.

5 Send a hang-up signal to the syslog daemon to make sure all changes are enforced:

```
sudo killall - HUP syslogd
```

The syslog configuration is complete. Events forwarded to SIEM by your Apple Mac OS X are displayed on the **Log Activity** tab. For more information on configuring Mac OS X, see your Mac OS X vendor documentation.

10 AccessData InSight

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

11 Application Security DbProtect

You can integrate Application Security DbProtect with SIEM.

Supported Event Types

The Application Security DbProtect DSM for SIEM accepts syslog events from DbProtect devices installed with the Log Enhanced Event Format (LEEF) Service.

Before You Begin

To forward syslog events from Application Security DbProtect to SIEM requires the LEEF Relay module.

The LEEF Relay module for DbProtect translates the default events messages to Log Enhanced Event Format (LEEF) messages for SIEM, enabling SIEM to record all relevant DbProtect events. Before you can receive events in SIEM, you must install and configure the LEEF Service for your DbProtect device to forward syslog events. The DbProtect LEEF Relay requires that you install the .NET 4.0 Framework, which is bundled with the LEEF Relay installation.

Installing the DbProtect LEEF Relay Module

The DbProtect LEEF Relay module for DbProtect must be installed on the same server as the DbProtect console. This allows the DbProtect LEEF Relay to work alongside an existing installation using the standard hardware and software prerequisites for a DbProtect console.

NOTE

Windows 2003 hosts require the Windows Imaging Components (wic_x86.exe). The Windows Imaging Components are located on the Windows Server Installation CD and must be installed before you continue. For more information, see your Windows 2003 Operating System documentation.

Procedure

1. Download the DbProtect LEEF Relay module for DbProtect from the Application Security, Inc. customer portal: www.appsecinc.com
2. Save the setup file to the same host as your DbProtect console.
3. Double click **setup.exe** to start the DbProtect LEEF Relay installation.
   The Microsoft .NET Framework 4 Client Profile is displayed.
4. Click **Accept**, if you agree with the Microsoft .NET Framework 4 End User License Agreement.

The Microsoft .NET Framework 4 is installed on your DbProtect console. After the installation is complete, the DbProtect LEEF Relay module installation Wizard is displayed.

5 Click **Next**.

The Installation Folder window is displayed.

6 To select the default installation path, click **Next**.

If you change the default installation directory, make note of the file location as it is required later. The Confirm Installation window is displayed.

7 Click **Next**.

The DbProtect LEEF Relay module is installed.

8 Click **Close**.

You are now ready to configure the DbProtect LEEF Relay module.

Configuring the DbProtect LEEF Relay

After the installation of the DbProtect LEEF Relay is complete, you can configure the service to forward events to SIEM.

NOTE

The DbProtect LEEF Relay must be stopped before you edit any configuration values.

Procedure

1 Navigate to the DbProtect LEEF Relay installation directory.
`C:\Program Files (x86)\AppSecInc\AppSecLEEFConverter`

2 Edit the DbProtect LEEF Relay configuration file:
`AppSecLEEFConverter.exe.config`

3 Configure the following values:

Table 11: DbProtect LEEF Relay Configuration Parameters

Parameter	Description
SyslogListenerPort	Optional. Type the listen port number the DbProtect LEEF Relay uses to listen for syslog messages from the DbProtect console. By default, the DbProtect LEEF Relay listens on port 514.
SyslogDestinationHost	Type the IP address of your SIEM Console or Event Collector.
SyslogDestinationPort	Type **514** as the destination port for LEEF formatted syslog messages forwarded to SIEM.
LogFileName	Optional. Type a file name for the DbProtect LEEF Relay to write debug and log messages. The LocalSystem user account that runs the DbProtect LEEF Relay service must have write privileges to the file path you specify.

4 Save the configuration changes to the file.

5 On your desktop of the DbProtect console, select **Start > Run**.
The Run window is displayed.

6 Type the following:
`services.msc`

7 Click OK.
The Services window is displayed.

8 In the details pane, verify the DbProtect LEEF Relay is started and set to automatic startup.

9 To change a service property, right-click on the service name, and then click Properties.

10 Using the **Startup type** list, select Automatic.

11 If the DbProtect LEEF Relay is not started, click Start.
You are now ready to configure alerts for your DbProtect console.

Configure DbProtect Alerts

You can configure sensors on your DbProtect console to generate alerts.

Procedure

1 Log in to your DbProtect console.

2 Click the **Activity Monitoring** tab.

3 Click the **Sensors** tab.

4 Select a sensor and click **Reconfigure**.
Any database instances that are configured for your database are displayed.

5 Select any database instances and click **Reconfigure**.

6 Click **Next** until the Sensor Manager Policy window is displayed.

7 Select the **Syslog** check box and click **Next**.

8 The Syslog Configuration window is displayed.

9 In the **Send Alerts to the following Syslog console** field, type the IP address of your DbProtect console.

10 In the **Port** field, type the port number you configured in the SyslogListenerPort field of the DbProtect LEEF Relay.
By default, 514 is the default Syslog listen port for the DbProtect LEEF Relay. For more information, see Configuring the DbProtect LEEF Relay on page 26,step 3.

11 Click **Add**.

12 Click **Next** until you reach the Deploy to Sensor window.

13 Click **Deploy to Sensor**.

The configuration is complete. Events forwarded to SIEM by your DbProtect console are added as a log source and automatically displayed on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Application Security DbProtect. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Application Security DbProtect.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 12: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Application Security DbProtect device.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The log source is added to SIEM.

12 Arbor Networks Peakflow

SIEM can collect and categorize syslog events from Arbor Networks Peakflow SP appliances that are in your network.

Configuration Overview

Arbor Networks Peakflow SP appliances store the syslog events locally.

To collect local syslog events, you must configure your Peakflow SP appliance to forward the syslog events to a remote host. SIEM automatically discovers and creates log sources for syslog events that are forwarded from Arbor Networks Peakflow SP appliances. SIEM supports syslog events that are forwarded from Peakflow V5.8.

To configure Arbor Networks Peakflow SP, complete the following tasks:

1 On your Peakflow SP appliance, create a notification group for SIEM.

2 On your Peakflow SP appliance, configure the global notification settings.

3 On your Peakflow SP appliance, configure your alert notification rules.

4 On your SIEM system, verify that the forwarded events are automatically discovered.

Supported Event Types for Arbor Networks Peakflow SP

The Arbor Networks Peakflow DSM for SIEM collects events from several categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, authentication events can have low-level categories of login successful or login failure.

The following list defines the event categories that are collected by SIEM from Peakflow SP appliances:

- Denial of Service (DoS) events
- Authentication events
- Exploit events
- Suspicious activity events
- System events

Configuring Remote Syslog in Peakflow SP

To collect events, you must configure a new notification group or edit existing groups to add SIEM as a remote syslog destination.

Procedure

1. Log in to the configuration interface for your Peakflow SP appliance as an administrator.
2. In the navigation menu, select **Administration > Notification > Groups**.
3. Click **Add Notification Group**.
4. In the **Destinations** field, type the IP address of your SIEM system.
5. In the **Port** field, type 514 as the port for your syslog destination.
6. From the **Facility** list, select a syslog facility.
7. From the **Severity** list, select **info**.
   The informational severity collects all event messages at the informational event level and higher severity.
8. Click **Save**.
9. Click **Configuration Commit**.

Configuring Global Notifications Settings for Alerts in Peakflow SP

Global notifications in Peakflow SP provide system notifications that are not associated with rules. This procedure defines how to add SIEM as the default notification group and enable system notifications.

Procedure

1. Log in to the configuration interface for your Peakflow SP appliance as an administrator.
2. In the navigation menu, select **Administration > Notification > Global Settings**.
3. In the **Default Notification Group** field, select the notification group that you created for SIEM syslog events.
4. Click **Save**.
5. Click **Configuration Commit** to apply the configuration changes.
6. Log in to the Peakflow SP command-line interface as an administrator.
7. Type the following command to list the current alert configuration:
   `services sp alerts system_errors show`
8. Optional. Type the following command to list the fields names that can be configured:
   `services sp alerts system_errors ?`
9. Type the following command to enable a notification for a system alert:
   `services sp alerts system_errors <name> notifications enable`

Where <name> is the field name of the notification.

10 Type the following command to commit the configuration changes:

```
config write
```

Configuring Alert Notification Rules in Peakflow SP

To generate events, you must edit or add rules to use the notification group that SIEM as a remote syslog destination.

Procedure

1 Log in to the configuration interface for your Peakflow SP appliance as an administrator.

2 In the navigation menu, select **Administration > Notification > Rules**.

3 Select one of the following options:

- Click a current rule to edit the rule.
- Click **Add Rule** to create a new notification rule.

4 Configure the following values:

Table 13: Notification rule parameters

Parameter	Description
Name	Type the IP address or host name as an identifier for events from your Peakflow SP installation. The log source identifier must be unique value.
Resource	Type a CIDR address or select a managed object from the list of Peakflow resources.
Importance	Select the importance of the rule.
Notification Group	Select the notification group that you assigned to forward syslog events to SIEM.

5 Repeat these steps to configure any other rules you want to forward to SIEM.

6 Click **Save**.

7 Click **Configuration Commit** to apply the configuration changes.

SIEM automatically discovers and creates a log source for Peakflow SP appliances. Events that are forwarded to SIEM are displayed on the **Log Activity** tab.

Configuring a Peakflow SP Log Source

SIEM automatically discovers and creates a log source for syslog events forwarded from Arbor Peakflow. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 Optional. In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Arbor Networks Peakflow**.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 14: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name as an identifier for events from your Peakflow SP installation. The log source identifier must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

13 Arbor Networks Pravail

The SIEM DSM for Arbor Networks Pravail can collect event logs from your Arbor Networks Pravail servers.

The following table identifies the specifications for the Arbor Networks Pravail DSM:

Table 15: Arbor Networks Pravail DSM specifications

Specification	Value
Manufacturer	Arbor Networks
DSM	Arbor Networks Pravail
RPM file name	DSM-ArborNetworksPravail-*build_number*.noarch.rpm
Supported versions	
Protocol	Syslog
SIEM recorded events	All relevant events
Automatically discovered	Yes
Includes identity	No
More information	www.stealthbits.com/resources

Arbor Networks Pravail DSM Integration Process

To integrate Arbor Networks Pravail DSM with SIEM, use the following procedure:

1 If automatic updates are not enabled, download and install the most recent Arbor Networks Pravail RPM on your SIEM Console.

2 For each instance of Arbor Networks Pravail, configure your Arbor Networks Pravail system to enable communication with SIEM.

3 If SIEM automatically discovers the DSM, for each Arbor Networks Pravail server you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually Installing a DSM on page 4

Configuring Your Arbor Networks Pravail System for Communication with SIEM on page 34

Configuring an Arbor Networks Pravail Log Source in SIEM on page 34

Configuring Your Arbor Networks Pravail System for Communication with SIEM

To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies SIEM as the syslog server.

Procedure

1 Log in to your Arbor Networks Pravail server.

2 Click **Settings & Reports**.

3 Click **Administration > Notifications**.

4 On the **Configure Notifications** page, click **Add Destinations.**

5 Select **Syslog**.

6 Configure the following parameters:

Parameter	Description
Host	The IP address for the SIEM Console
Port	514
Severity	Info
Alert Types	The alert types that you want to send to the SIEM Console

7 Click **Save**.

Configuring an Arbor Networks Pravail Log Source in SIEM

To collect Arbor Networks Pravail events, configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **Arbor Networks Pravail**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

14 Arpeggio SIFT-IT

The SIEM SIFT-IT DSM accepts syslog events from Arpeggio SIFT-IT running on IBM iSeries® that are formatted using the Log Enhanced Event Protocol (LEEF).

Supported Versions

SIEM supports events from Arpeggio SIFT-IT 3.1 and later installed on IBM iSeries version 5 revision 3 (V5R3) and later.

Supported Events

Arpeggio SIFT-IT supports syslog events from the journal QAUDJRN in LEEF format.

For example,

Jan 29 01:33:34 RUFUS LEEF:1.0|Arpeggio|SIFT-IT|3.1|PW_U|sev=3 usrName=ADMIN src=100.100.100.114 srcPort=543 jJobNam=QBASE jJobUsr=ADMIN jJobNum=1664 jrmtIP=100.100.100.114 jrmtPort=543 jSeqNo=4755 jPgm=QWTMCMNL jPgmLib=QSYS jMsgId=PWU0000 jType=U jUser=ROOT jDev=QPADEV000F jMsgTxt=Invalid user id ROOT. Device QPADEV000F.

Events SIFT-IT forwards to SIEM are determined with a configuration rule set file. SIFT-IT includes a default configuration rule set file that you can edit to meet your security or auditing requirements. For more information on configuring rule set files, see your *SIFT-IT User Guide*.

Configuring a SIFT-IT Agent

Arpeggio SIFT-IT is capable of forwarding syslog events in LEEF format with SIFT-IT agents.

A SIFT-IT agent configuration defines the location of your SIEM installation, the protocol and formatting of the event message, and the configuration rule set.

Procedure

1 Log in to your IBM iSeries.

2 Type the following command and press Enter to add SIFT-IT to your library list:
`ADDLIBLE SIFTITLIB0`

3 Type the following command and press Enter to access the SIFT-IT main menu:
`GO SIFTIT`

4 From the main menu, select **1. Work with SIFT-IT Agent Definitions**.

5 Type **1** to add an agent definition for SIEM and press Enter.

6 Configure the following agent parameters:
a In the **SIFT-IT Agent Name** field, type a name.

For example, **SIEM**.

b In the **Description** field, type a description for the agent.

For example, `Arpeggio agent for` **SIEM**.

c In the **Server host name or IP address** field, type the location of your SIEM Console or Event Collector.

d In the **Connection type** field, type either ***TCP**, ***UDP**, or ***SECURE**.

The *SECURE option requires the TLS protocol. For more information, see the *SIEM Log Sources User Guide*.

e In the **Remote port number** field, type **514**.

By default, SIEM supports both TCP and UDP syslog messages on port 514.

f In the **Message format options** field, type ***SIEM**.

g Optional. Configure any additional parameters for attributes that are not SIEM specific.

The additional operational parameters are described in the *SIFT-IT User Guide*.

h Press **F3** to exit to the Work with SIFT-IT Agents Description menu.

7 Type **9** and press Enter to load a configuration rule set for SIEM.

8 In the **Configuration file** field, type the path to your SIEM configuration rule set file.

For example,

`/sifitit/SIEMconfig.txt`

9 Press **F3** to exit to the Work with SIFT-IT Agents Description menu.

10 Type **11** to start the SIEM agent.

The configuration is complete.

Next Steps

Syslog events forwarded by Arpeggio SIFT-IT in LEEF format are automatically discovered by SIEM. In most cases, the log source is automatically created in SIEM after a small number of events are detected. If the event rate is extremely low, then you might be required to manually create a log source for Arpeggio SIFT-IT in SIEM. Until the log source is automatically discovered and identified, the event type displays as Unknown on the **Log Activity** tab of SIEM. Automatically discovered log sources can be viewed on the **Admin** tab of SIEM by clicking the Log Sources icon.

Configuring a Log Source

SIEM automatically discovers and creates a log source for system authentication events forwarded from Arpeggio SIFT-IT. This procedure is optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Arpeggio SIFT-IT.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 16: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Arpeggio SIFT-IT installation.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Additional Information

After you create your SIEM agent definition, you can use your Arpeggio SIFT-IT software and SIEM integration to customize your security and auditing requirements.

This can include:

- Creating custom configurations in Apreggio SIFT-IT with granular filtering on event attributes.

  For example, filtering on job name, user, file or object name, system objects, or ports. All events forwarded from SIFT-IT and the contents of the event payload in SIEM are easily searchable.
- Configuring rules in SIEM to generate alerts or offenses for your security team to identify potential security threats, data loss, or breaches in real-time.
- Configuring processes in Apreggio SIFT-IT to trigger real-time remediation of issues on your IBM iSeries.
- Creating offenses for your security team from Arpeggio SIFT-IT events in SIEM with the **Offenses** tab or configuring email job logs in SIFT-IT for your IBM iSeries administrators.
- Creating multiple configuration rule sets for multiple agents that run simultaneously to handle specific security or audit events.

  For example, you can configure one SIEM agent with a specific rule sets for forwarding all IBM iSeries events, then develop multiple configuration rule sets for specific compliance purposes. This allows you to easily manage configuration rule sets for compliance regulations, such as FISMA, PCI. HIPPA, SOX, or ISO 27001. All of the events forwarded by SIFT-IT SIEM agents is contained in a single log source and categorized to be easily searchable.

15 Array Networks SSL VPN

The Array Networks SSL VPN DSM for SIEM collects events from an ArrayVPN appliance using syslog.

Supported Event Types

SIEM records all relevant SSL VPN events forwarded using syslog on TCP port 514 or UDP port 514.

Configuring a Log Source

To integrate Array Networks SSL VPN events with SIEM, you must manually create a log source.

SIEM does not automatically discover or create log sources for syslog events from Array Networks SSL VPN.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Array Networks SSL VPN Access Gateways.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 17: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Array Networks SSL VPN appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Array Networks SSL VPN are displayed on the **Log Activity** tab.

Next Steps

You are now ready to configure your Array Networks SSL VPN appliance to forward remote syslog events to SIEM. For more information on configuring Array Networks SSL VPN appliances for remote syslog, please consult your Array Networks documentation.

16 Aruba Mobility Controllers

The Aruba Mobility Controllers DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant events forwarded using syslog on TCP port 514 or UDP port 514.

Configure Your Aruba Mobility Controller

You can configure the Aruba Wireless Networks (Mobility Controller) device to forward syslog events to SIEM.

Procedure

1 Log in to the Aruba Mobility Controller user interface.

2 From the top menu, select Configuration.

3 From the Switch menu, select Management.

4 Click the Logging tab.

5 From the Logging Servers menu, select Add.

6 Type the IP address of the SIEM server that you want to collect logs.

7 Click Add.

8 Optional. Change the logging level for a module:
   a Select the check box next to the name of the logging module.
   b Choose the logging level you want to change from the list that is displayed at the bottom of the window.

9 Click Done.

10 Click Apply.

   The configuration is complete. The log source is added to SIEM as Aruba Mobility Controller events are automatically discovered. Events forwarded to SIEM by Aruba Mobility Controller are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Aruba Mobility Controllers. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Aruba Mobility Controller .

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 18: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Aruba Mobility Controller.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Aruba Mobility Controller appliances are displayed on the **Log Activity** tab.

17 Avaya VPN Gateway

The SIEM DSM for Avaya VPN Gateway can collect event logs from your Avaya VPN Gateway servers.

The following table identifies the specifications for the Avaya VPN Gateway DSM:

Table 19: Avaya VPN Gateway DSM specifications

Specification	Value
Manufacturer	Avaya Inc.
DSM	Avaya VPN Gateway
RPM file name	DSM-AvayaVPNGateway-7.1-799033.noarch.rpm DSM-AvayaVPNGateway-7.2-799036.noarch.rpm
Supported versions	9.0.7.2
Protocol	syslog
SIEM recorded events	OS, System Control Process, Traffic Processing, Startup, Configuration Reload, AAA Subsystem, IPsec Subsystem
Automatically discovered	Yes
Includes identity	Yes
More information	www.avaya.com

Avaya VPN Gateway DSM Integration Process

To integrate Avaya VPN Gateway DSM with SIEM, use the following procedure:

1 If automatic updates are not enabled, download and install the most recent version of the following RPMs on your SIEM Console:

- Syslog protocol RPM
- DSMCommon RPM
- Avaya VPN Gateway RPM

2 For each instance of Avaya VPN Gateway, configure your Avaya VPN Gateway system to enable communication with SIEM.

3 If SIEM automatically discovers the log source, for each Avaya VPN Gateway server you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually Installing a DSM on page 4

Configuring your Avaya VPN Gateway System for Communication with SIEM on page 43

Configuring an Avaya VPN Gateway Log Source in SIEM on page 43

Configuring your Avaya VPN Gateway System for Communication with SIEM

To collect all audit logs and system events from Avaya VPN Gateway, you must specify SIEM as the syslog server and configure the message format.

Procedure

1 Log in to your Avaya VPN Gateway command-line interface (CLI).

2 Type the following command:
`/cfg/sys/syslog/add`

3 At the prompt, type the IP address of your SIEM system.

4 To apply the configuration, type the following command:
`apply`

5 To verify that the IP address of your SIEM system is listed, type the following command:
`/cfg/sys/syslog/list`

Configuring an Avaya VPN Gateway Log Source in SIEM

To collect Avaya VPN Gateway events, configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **Avaya VPN Gateway**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

18 BalaBit IT Security

The BalaBit Syslog-ng Agent application can collect and forward syslog events for the Microsoft Security Event Log DSM and the Microsoft ISA DSM in SIEM.

To configure a BalaBIt IT Security agent, select a configuration:

- Configuring BalaBIt IT Security for Microsoft Windows Events on page 44
- Configuring BalaBit IT Security for Microsoft ISA or TMG Events on page 48

Configuring BalaBIt IT Security for Microsoft Windows Events

The Microsoft Windows Security Event Log DSM in SIEM can accept Log Extended Event Format (LEEF) events from BalaBit's Syslog-ng Agent.

Supported Event Types

The BalaBit Syslog-ng Agent forwards Windows events to SIEM using syslog.

- Windows security
- Application
- System
- DNS
- DHCP
- Custom container event logs

Before You Begin

Before you can receive events from BalaBit IT Security Syslog-ng Agents, you must install and configure the agent to forward events.

Review the following configuration steps before you attempt to configure the BalaBit Syslog-ng Agent:

1. Install the BalaBit Syslog-ng Agent in your Windows host. For more information, see your BalaBit Syslog-ng Agent documentation.
2. Configure Syslog-ng Agent Events.
3. Configure SIEM as a destination for the Syslog-ng Agent.
4. Restart the Syslog-ng Agent service.
5. Optional. Configure the log source in SIEM.

Configuring the Syslog-ng Agent Event Source

Before you can forward events to SIEM, you must specify what Windows-based events the Syslog-ng Agent collects.

Procedure

1 From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.

The Syslog-ng Agent window is displayed.

2 Expand the syslog-ng Agent Settings pane, and select **Eventlog Sources**.

3 Double-click on **Event Containers**.

The Event Containers Properties window is displayed.

4 From the Event Containers pane, select the **Enable** radio button.

5 Select a check box for each event type you want to collect:

- **Application** - Select this check box if you want the device to monitor the Windows application event log.
- **Security** - Select this check box if you want the device to monitor the Windows security event log.
- **System** - Select this check box if you want the device to monitor the Windows system event log.

NOTE

BalaBit's Syslog-ng Agent supports additional event types, such as DNS or DHCP events using custom containers. For more information, see your BalaBit Syslog-ng Agent documentation.

6 Click **Apply**, and then click **OK**.

The event configuration for your BalaBit Syslog-ng Agent is complete. You are now ready to configure SIEM as a destination for Syslog-ng Agent events.

Configuring a Syslog Destination

The Syslog-ng Agent allows you to configure multiple destinations for your Windows-based events.

To configure SIEM as a destination, you must specify the IP address for SIEM, and then configure a message template for the LEEF format.

Procedure

1 From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.

The Syslog-ng Agent window is displayed.

2 Expand the syslog-ng Agent Settings pane, and click **Destinations**.

3 Double-click on **Add new sever**.

The Server Property window is displayed.

4 On the **Server** tab, click **Set Primary Server**.

5 Configure the following parameters:
   a **Server Name** - Type the IP address of your SIEM Console or Event Collector.
   b **Server Port** - Type **514** as the TCP port number for events forwarded to SIEM.

6 Click the **Messages** tab.

7 From the **Protocol** list, select **Legacy BSD Syslog Protocol**.

8 In the **Template** field, define a custom template message for the protocol by typing:
```
<${PRI}>${BSDDATE} ${HOST} LEEF:${MSG}
```
The information typed in this field is space delimited.

9 From the Event Message Format pane, in the **Message Template** field, type the following to define the format for the LEEF events:
```
1.0|Microsoft|Windows|2k8r2|${EVENT_ID}|devTime=${R_YEAR}-
${R_MONTH}-${R_DAY}T
${R_HOUR}:${R_MIN}:${R_SEC}GMT${TZOFFSET} devTimeFormat=yyyy-MM-
dd'T'HH:mm:ssz cat=${EVENT_TYPE}sev=${EVENT_LEVEL}
resource=${HOST} usrName=${EVENT_USERNAME} application=$
{EVENT_SOURCE} message=${EVENT_MSG}
```

NOTE

The LEEF format uses tab as a delimiter to separate event attributes from each other. However, the delimiter does not start until after the last pipe character for {Event_ID}. The following fields must include a tab before the event name: devTime, devTimeFormat, cat, sev, resource, usrName, application, and message.

You might need to use a text editor to copy and paste the LEEF message format into the **Message Template** field.

10 Click **OK**.
The destination configuration is complete. You are now ready to restart the Syslog-ng Agent service.

Restart the Syslog-ng Agent Service

Before the Syslog-ng Agent can forward LEEF formatted events, you must restart the Syslog-ng Agent service on the Windows host.

Procedure

1 From the **Start** menu, select **Start > Run**.
The Run window is displayed.

2 Type the following:
`services.msc`

3 Click OK.
The Services window is displayed.

4 In the Name column, right-click on **Syslog-ng Agent for Windows**, and select **Restart**.
After the Syslog-ng Agent for Windows service restarts, the configuration is complete. Syslog events from the BalaBit Syslog-ng Agent are automatically discovered by SIEM. The Windows events that are automatically discovered are displayed as Microsoft Windows Security Event Logs on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from LEEF formatted messages. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your BalaBit Syslog-ng Agent log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Microsoft Windows Security Event Log.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 20: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from the BalaBit Syslog-ng Agent.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Configuring BalaBit IT Security for Microsoft ISA or TMG Events

You can integrate the BalaBit Syslog-ng Agent application to forward syslog events to SIEM.

Supported Event Types

The BalaBit Syslog-ng Agent reads Microsoft ISA or Microsoft TMG event logs and forwards syslog events using the Log Extended Event Format (LEEF).

The events forwarded by BalaBit IT Security are parsed and categorized by the Microsoft Internet and Acceleration (ISA) DSM for SIEM. The DSM accepts both Microsoft ISA and Microsoft Threat Management Gateway (TMG) events.

Before You Begin

Before you can receive events from BalaBit IT Security Syslog-ng Agents, you must install and configure the agent to forward events.

NOTE

This integration uses BalaBit's Syslog-ng Agent for Windows and BalaBit's Syslog-ng PE to parse and forward events to SIEM for the DSM to interpret.

Review the following configuration steps before you attempt to configure the BalaBit Syslog-ng Agent:

To configure the BalaBit Syslog-ng Agent, you must:

1 Install the BalaBit Syslog-ng Agent in your Windows host. For more information, see your BalaBit Syslog-ng Agent vendor documentation.

2 Configure the BalaBit Syslog-ng Agent.

3 Install a BalaBit Syslog-ng PE for Linux or Unix in relay mode to parse and forward events to SIEM. For more information, see your BalaBit Syslog-ng PE vendor documentation.

4 Configure syslog for BalaBit Syslog-ng PE.

5 Optional. Configure the log source in SIEM.

Configure the BalaBit Syslog-ng Agent

Before you can forward events to SIEM, you must specify the file source for Microsoft ISA or Microsoft TMG events in the Syslog-ng Agent collects.

If your Microsoft ISA or Microsoft TMG appliance is generating event files for the Web Proxy Server and the Firewall Service, both files can be added.

Configure the File Source

File sources allow you to define the base log directory and files monitored by the Syslog-ng Agent.

Procedure

1 From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.

The Syslog-ng Agent window is displayed.

2 Expand the syslog-ng Agent Settings pane, and select **File Sources**.

3 Select the **Enable** radio button.

4 Click **Add** to add your Microsoft ISA and TMG event files.

5 From the **Base Directory** field, click **Browse** and select the folder for your Microsoft ISA or Microsoft TMG log files.

6 From the **File Name Filter** field, click **Browse** and select a log file containing your Microsoft ISA or Microsoft TMG events.

NOTE

The **File Name Filter** field supports the wildcard (*) and question mark (?) characters to follow log files that are replaced after reaching a specific file size or date.

7 In the **Application Name** field, type a name to identify the application.

8 From the **Log Facility** list, select **Use Global Settings**.

9 Click **OK**.

10 To add additional file sources, click **Add** and repeat this process from Step 4.

Microsoft ISA and TMG store Web Proxy Service events and Firewall Service events in individual files.

11 Click **Apply**, and then click **OK**.

The event configuration is complete. You are now ready to configure a syslog destinations and formatting for your Microsoft TMG and ISA events.

Configuring a Syslog Destination

The event logs captured by Microsoft ISA or TMG cannot be parsed by the BalaBit Syslog-ng Agent for Windows, so you must forward your logs to a BalaBit Syslog-ng Premium Edition (PE) for Linux or Unix.

To forward your TMG and ISA event logs, you must specify the IP address for your PE relay and configure a message template for the LEEF format. The BalaBit Syslog-ng PE acts as an intermediate syslog server to parse the events and forward the information to SIEM.

Procedure

1. From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.
   The Syslog-ng Agent window is displayed.
2. Expand the syslog-ng Agent Settings pane, and click **Destinations**.
3. Double-click on **Add new sever**.
4. On the **Server** tab, click **Set Primary Server.**
5. Configure the following parameters:
   a. **Server Name** - Type the IP address of your BalaBit Syslog-ng PE relay.
   b. **Server Port** - Type **514** as the TCP port number for events forwarded to your BalaBit Syslog-ng PE relay.
6. Click the **Messages** tab.
7. From the **Protocol** list, select **Legacy BSD Syslog Protocol**.
8. From the File Message Format pane, in the **Message Template** field, type the following format command:
   `${FILE_MESSAGE}${TZOFFSET}`
9. Click **Apply**, and then click **OK**.
   The destination configuration is complete. You are now ready to filter comment lines from the event log.

Filtering the Log File for Comment Lines

The event log file for Microsoft ISA or Microsoft TMG can contain comment markers, these comments must be filtered from the event message.

Procedure

1. From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.
   The Syslog-ng Agent window is displayed.
2. Expand the syslog-ng Agent Settings pane, and select **Destinations**.
3. Right-click on your SIEM syslog destination and select **Event Filters > Properties**.
   The Global event filters Properties window is displayed.
4. Configure the following values:

- From the Global file filters pane, select **Enable**.
- From the Filter Type pane, select **Black List Filtering**.

5 Click **OK**.

6 From the filter list menu, double-click **Message Contents**.
The Message Contents Properties window is displayed.

7 From the Message Contents pane, select the **Enable** radio button.

8 In the Regular Expression field, type the following regular expression:
^#

9 Click **Add**.

10 Click **Apply**, and then click **OK**.
The event messages containing comments are no longer forwarded.

NOTE

You might be required to restart Syslog-ng Agent for Windows service to begin syslog forwarding. For more information, see your BalaBit Syslog-ng Agent documentation.

Configuring a BalaBit Syslog-ng PE Relay

The BalaBit Syslog-ng Agent for Windows sends Microsoft TMG and ISA event logs to a Balabit Syslog-ng PE installation, which is configured in relay mode.

The relay mode installation is responsible for receiving the event log from the BalaBit Syslog-ng Agent for Windows, parsing the event logs in to the LEEF format, then forwarding the events to SIEM using syslog.

To configure your BalaBit Syslog-ng PE Relay, you must:

1 Install BalaBit Syslog-ng PE for Linux or Unix in relay mode. For more information, see your BalaBit Syslog-ne PE vendor documentation.

2 Configure syslog on your Syslog-ng PE relay.

NOTE

For a sample syslog.conf file you can use to configure Microsoft TMG and ISA logs using your BalaBit Syslog-ng PE relay, see http://support.extremenetworks.com.

The BalaBit Syslog-ng PE formats the TMG and ISA events in the LEEF format based on the configuration of your syslog.conf file. The syslog.conf file is responsible for parsing the event logs and forwarding the events to SIEM.

Procedure

1 Using SSH, log in to your BalaBit Syslog-ng PE relay command-line interface (CLI).

2 Edit the following file:

```
/etc/syslog-ng/etc/syslog.conf
```

3 From the destinations section, add an IP address and port number for each relay destination.

For example,

```
######
# destinations
destination d_messages { file("/var/log/messages"); };
destination d_remote_tmgfw { tcp("SIEM_IP" port(SIEM_PORT)
log_disk_fifo_size(10000000) template(t_tmgfw)); };
destination d_remote_tmgweb { tcp("SIEM_IP" port(SIEM_PORT)
log_disk_fifo_size(10000000) template(t_tmgweb)); };
```

Where:

`SIEM_IP` is the IP address of your SIEM Console or Event Collector.

`SIEM_PORT` is the port number required for SIEM to receive syslog events. By default, SIEM receives syslog events on port 514.

4 Save the syslog configuration changes.

5 Restart Syslog-ng PE to force the configuration file to be read.

The BalaBit Syslog-ng PE configuration is complete. Syslog events forwarded from the BalaBit Syslog-ng relay are automatically discovered by SIEM as Microsoft Windows Security Event Log on the **Log Activity** tab. For more information, see the *SIEM Users Guide*.

NOTE

When using multiple syslog destinations, messages are considered delivered after they successfully arrived at the primary syslog destination.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from LEEF formatted messages provided by your BalaBit Syslog-ng relay. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Microsoft ISA.

9 From the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 21: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for Microsoft ISA or Microsoft Threat Management Gateway events from the BalaBit Syslog-ng Agent.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The BalaBit IT Security configuration for Microsoft ISA and Microsoft TMG events is complete.

19 Barracuda

SIEM supports the following Barracuda devices:

Barracuda Spam & Virus Firewall

You can integrate Barracuda Spam & Virus Firewall with SIEM.

Supported Event Types

The Barracuda Spam & Virus Firewall DSM for SIEM accepts both Mail syslog events and Web syslog events from Barracuda Spam & Virus Firewall appliances.

Mail syslog events contain the event and action taken when the firewall processes email. Web syslog events record information on user activity and configuration changes on your Barracuda Spam & Virus Firewall appliance.

Before You Begin

Syslog messages are sent to SIEM from Barracuda Spam & Virus Firewall using UDP port 514. You must verify any firewalls between SIEM and your Barracuda Spam & Virus Firewall appliance allow UDP traffic on port 514.

Configuring Syslog Event Forwarding

You can configure syslog forwarding for Barracuda Spam & Virus Firewall.

Procedure

1. Log in to the Barracuda Spam & Virus Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Advanced Networking**.
4. In the **Mail Syslog** field, type the IP address of your SIEM Console or event collector.
5. Click **Add**.
6. In the **Web Interface Syslog** field, type the IP address of your SIEM Console or event collector.
7. Click **Add**.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Barracuda Spam & Virus Firewall appliances. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select Barracuda Spam & Virus Firewall.

8 From the Protocol Configuration list, select **Syslog**.

9 In the **Log Source Identifier** field, type the IP address or host name for the log source.

10 Click Save.

11 On the Admin tab, click Deploy Changes.

Barracuda Web Application Firewall

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

Barracuda Web Filter

You can integrate Barracuda Web Filter appliance events with SIEM.

Supported Event Types

The Barracuda Web Filter DSM for SIEM accepts web traffic and web interface events in syslog format forwarded by Barracuda Web Filter appliances.

Web traffic events contain the event and action taken when the appliance processes web traffic. Web interface events contain user login activity and configuration changes to the Web Filter appliance.

Before You Begin

Syslog messages are forward to SIEM using UDP port 514. You must verify any firewalls between SIEM and your Barracuda Web Filter appliance allow UDP traffic on port 514.

Configuring Syslog Event Forwarding

Configure syslog forwarding for Barracuda Web Filter.

Procedure

1 Log in to the Barracuda Web Filter web interface.

2 Click the **Advanced** tab.

3 From the Advanced menu, select **Syslog**.

4 From the **Web Traffic Syslog** field, type IP address of your SIEM Console or Event Collector.

5 Click **Add**.

6 From the **Web Interface Syslog** field, type IP address of your SIEM Console or Event Collector.

7 Click **Add**.

The syslog configuration is complete.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Barracuda Web Filter appliances. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Barracuda Web Filter.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 22: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Barracuda Web Filter appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded by Barracuda Web Filter are displayed on the **Log Activity** tab of SIEM.

20 Bit9 Security

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

21 BlueCat Networks Adonis

The BlueCat Networks Adonis DSM for SIEM accepts events forwarded in Log Enhanced Event Protocol (LEEF) using syslog from BlueCat Adonis appliances managed with BlueCat Proteus.

Supported Versions

SIEM supports BlueCat Networks Adonis appliances using version 6.7.1-P2 and later.

You might be required to include a patch on your BlueCat Networks Adonis to integrate DNS and DHCP events with SIEM. For more information, see KB-4670 and your BlueCat Networks documentation.

Supported Event Types

SIEM is capable of collecting all relevant events related to DNS and DHCP queries.

This includes the following events:

- DNS IPv4 and IPv6 query events
- DNS name server query events
- DNS mail exchange query events
- DNS text record query events
- DNS record update events
- DHCP discover events
- DHCP request events
- DHCP release events

Event Type Format

The LEEF format consists of a pipe (|) delimited syslog header and a space delimited event payload.

For example:

```
Aug 10 14:55:30 adonis671-184
LEEF:1.0|BCN|Adonis|6.7.1|DNS_Query|cat=A_record src=10.10.10.10
url=test.example.com
```

If the syslog events forwarded from your BlueCat Adonis appliance are not formatted similarly to the sample above, you must examine your device configuration. Properly formatted LEEF event messages are automatically discovered by the BlueCat Networks Adonis DSM and added as a log source to SIEM.

Before You Begin

BlueCat Adonis must be configured to generate events in Log Enhanced Event Protocol (LEEF) and redirect the event output by way of syslog to SIEM.

BlueCat Networks provides a script on their appliance to assist you with configuring syslog. To complete the syslog redirection, you must have administrative or root access to the command-line interface of the BlueCat Adonis or your BlueCat Proteus appliance. If the syslog configuration script is not present on your appliance, you can contact your BlueCat Networks representative.

Configuring BlueCat Adonis

You can configure your BlueCat Adonis appliance to forward DNS and DHCP events to SIEM.

Procedure

1. Using SSH, log in to your BlueCat Adonis appliance command-line interface.
2. Type the following command to start the syslog configuration script:
   `/usr/local/bluecat/qradar/setup-qradar.sh`
3. Type the IP address of your SIEM Console or Event Collector.
4. Type **yes** or **no** to confirm the IP address.
   The configuration is complete when a success message is displayed.
   The log source is added to SIEM as BlueCat Networks Adonis syslog events are automatically discovered. Events forwarded to SIEM are displayed on the **Log Activity** tab. If the events are not automatically discovered, you can manually configure a log source.

Configuring a Log Source in SIEM

SIEM automatically discovers and creates a log source for syslog events from BlueCat Networks Adonis. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

Procedure

1. Log in to SIEM.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the Log Sources icon.
5. Click Add.
6. In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select BlueCat Networks Adonis.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 23: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your BlueCat Networks Adonis appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

22 Blue Coat SG

The Blue Coat SG DSM for SIEM allows you to integrate events from a Blue Coat SG appliance with SIEM.

SIEM records all relevant and available information from name-value events that are separated by pipe (|) characters.

SIEM can receive events from your Blue Coat SG appliance using syslog or can retrieve events from the Blue Coat SG appliance using the Log File protocol. The instructions provided describe how to configure Blue Coat SG using a custom name-value pair format. However, SIEM supports the following formats:

- Custom Format
- SQUID
- NCSA
- main
- IM
- Streaming
- smartreporter
- bcereportermain_v1
- bcreporterssl_v1
- p2p
- SSL
- bcreportercifs_v1
- CIFS
- MAPI
  For more information about your Blue Coat SG Appliance, see your vendor documentation.

Creating a Custom Event Format

The Blue Coat SG DSM for SIEM accepts custom formatted events from a Blue Coat SG appliance.

Procedure

1 Using a web browser, log in to the Blue Coat Management Console.

2 Select **Configuration > Access Logging > Formats**.

3 Select New.

4 Type a format name for the custom format.

5 Select Custom format string.

6 Type the following custom format for SIEM:

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-
address)|dstport=$(cs-uri-port)|username=$(cs-
username)|devicetime=$(gmttime)|s-action=$(s-action)|sc-
status=$(sc-status)|cs-method=$(cs-method)|time-taken=$(time-
taken)|sc-bytes=$(sc-bytes)|cs-bytes=$(cs-bytes)|cs-uri-
scheme=$(cs-uri-scheme)|cs-host=$(cs-host)|cs-uri-path=$(cs-uri-
path)|cs-uri-query=$(cs-uri-query)|cs-uri-extension=$(cs-uri-
extension)|cs-auth-group=$(cs-auth-group)|rs(Content-
Type)=$(rs(Content-Type))|cs(User-Agent)=$(cs(User-
Agent))|cs(Referer)=$(cs(Referer))|sc-filter-result=$(sc-filter-
result)|filter-category=$(sc-filter-category)|cs-uri=$(cs-uri)
```

7 Select Log Last Header from the list.

8 Click OK.

9 Click Apply.

NOTE

The custom format for SIEM supports additional key-value pairs using the Blue Coat ELFF format. For more information, see Creating Additional Custom Format Key-Value Pairs on page 68.

You are ready to enable access logging on your Blue Coat device.

Creating a Log Facility

To use the custom log format created for SIEM, you must associate the custom log format for SIEM to a facility.

Procedure

1 Select **Configuration > Access Logging > Logs**.

2 Click New.

3 Configure the following parameters:

- Log Name - Type a name for the log facility.
- Log Format - Select the custom format you created in Creating a Custom Event Format on page 61, step 4.
- Description - Type a description for the log facility.

4 Click OK.

5 Click Apply.

You are ready to enable logging on the Blue Coat device. For more information, see Enabling Access Logging on page 63.

Enabling Access Logging

You must enable access logging on your Blue Coat SG device.

Procedure

1 Select **Configuration > Access Logging > General**.

2 Select the Enable Access Logging check box.

If the Enable Access Logging check box is not selected, logging is disabled globally for all of the formats listed.

3 Click Apply.

You are ready to configure the Blue Coat upload client. For more information, see Retrieving Blue Coat Events on page 63.

Retrieving Blue Coat Events

Events from your Blue Coat SG appliance are forwarded using the Blue Coat upload client.

SIEM can receive forwarded events using FTP or syslog.

- If you are using FTP, see Log File Protocol Configuration on page 63.
- If you are using syslog, see Syslog Configuration on page 67.

Log File Protocol Configuration

To use FTP, you must configure the Blue Coat upload client.

Procedure

1 Select **Configuration > Access Logging > Logs > Upload Client**.

2 From the Log list, select the log containing your custom format.

3 From the Client type list, select FTP Client.

4 Select the **text file** option.

If you select the **gzip file** option on your Blue Coat appliance, you must configure a **Processor** for your log source with the **GZIP** option.

5 Click Settings.

6 From the Settings For list, select Primary FTP Server.

7 Configure the following values:

a Host - Type the IP address of the FTP server receiving the Blue Coat events.

b Port - Type the FTP port number.

c Path - Type a directory path for the log files.

d Username - Type the username required to access the FTP server.

8 Click OK.

9 Select the Upload Schedule tab.

10 From the Upload the access log option, select periodically.

11 Configure the Wait time between connect attempts.

12 Select if you want to upload the log file to the FTP daily or on an interval.

13 Click Apply.

Configuring a Log Source in SIEM

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 From the Log Source Type list, select the Bluecoat SG Appliance option.

8 From the Protocol Configuration list, select the Log File option.

9 Configure the following values:

Table 24: Blue Coat SG log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.

Table 24: Blue Coat SG log file protocol parameters (Continued)

Parameter	Description
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **Note:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files ending with .log, type the following: `.*\.log` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when using ASCII as the FTP Transfer Mode.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.

Table 24: Blue Coat SG log file protocol parameters (Continued)

Parameter	Description
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM system for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The log file protocol configuration for Blue Coat SG is complete.

Syslog Configuration

To allow syslog event collection, you must configure your Blue Coat appliance to forward syslog events.

If your Blue Coat SG appliance is reporting events using syslog (rather than a file transfer protocol) and the destination syslog server becomes unavailable, it is possible that other syslog destinations can stop receiving data until all syslog destinations are again available. This creates the potential for some syslog data to not be sent at all. If you are sending to multiple syslog destinations, a disruption in availability in one syslog destination might interrupt the stream of events to other syslog destinations from your Blue Coat SG appliance.

Procedure

1 Select **Configuration > Access Logging > Logs > Upload Client**.

2 From the Log list, select the log containing your custom format.

3 From the Client type drop-down list bow, select Custom Client.

4 Click Settings.

5 From the Settings For list, select Primary Custom Server.

6 Configure the following values:
   a Host - Type the IP address for your SIEM.
   b Port - Type 514 as the syslog port for SIEM.

7 Click OK.

8 Select the Upload Schedule tab.

9 From the Upload the access log, select continuously.

10 Click Apply.
   You are now ready to configure a log source for Blue Coat SG events.

Configure a Log Source

To integrate Barracuda Web Application Firewall with SIEM, you must manually create a log source to receive Blue Coat SG events.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Blue Coat SG Appliance.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 25: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Blue Coat SG appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Blue Coat SG are displayed on the **Log Activity** tab.

Creating Additional Custom Format Key-Value Pairs

The custom format allows you to forward specific Blue Coat data or events to SIEM using the Extended Log File Format (ELFF).

The custom format is a series of pipe delimited fields starting with `Bluecoat|` and containing `$(Blue Coat ELFF Parameter)`. Custom format fields for SIEM must be separated by the pipe character.

For example:

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-
address)|dstport=$(cs-uri-port)|username=$(cs-
username)|devicetime=$(gmttime)|s-action=$(s-action)|sc-
status=$(sc-status)|cs-method=$(cs-method)
```

Table 26: SIEM Custom Format Examples

Blue Coat ELFF Parameter	SIEM Custom Format Example
sc-bytes	$(sc-bytes)
rs(Content-type)	$(rs(Content-Type))

For more information on the available Blue Coat ELFF parameters, see your Blue Coat appliance documentation.

23 Bridgewater

The Bridgewater Systems DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant events forwarded from Bridgewater AAA Service Controller devices using syslog.

Configuring Syslog for your Bridgewater Systems Device

You must configure your Bridgewater Systems appliance to send syslog events to SIEM.

Procedure

1 Log in to your Bridgewater Systems device command-line interface (CLI).

2 To log operational messages to the RADIUS and Diameter servers, open the following file:
`/etc/syslog.conf`

3 To log all operational messages, uncomment the following line:
`local1.info /WideSpan/logs/oplog`

4 To log error messages only, change the `local1.info /WideSpan/logs/oplog` line to the following:
`local1.err /WideSpan/logs/oplog`

NOTE

RADIUS and Diameter system messages are stored in the /var/adm/messages file.

5 Add the following line:
`local1.*@<IP address>`
Where `<IP address>` is the IP address your SIEM Console.

6 The RADIUS and Diameter server system messages are stored in the /var/adm/messages file. Add the following line for the system messages:
`<facility>.*@<IP address>`
Where:
`<facility>` is the facility used for logging to the /var/adm/messages file.
`<IP address>` is the IP address of your SIEM Console.

7 Save and exit the file.

8 Send a hang-up signal to the syslog daemon to make sure all changes are enforced:
`kill -HUP `cat /var/run/syslog.pid``

The configuration is complete. The log source is added to SIEM as Bridgewater Systems appliance events are automatically discovered. Events forwarded to SIEM by your Bridgewater Systems appliance are displayed on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from a Bridgewater Systems appliance. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Bridgewater Systems AAA Service Controller.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 27: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Bridgewater Systems appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

24 Brocade Fabric OS

SIEM can collect and categorize syslog system and audit events from Brocade switches and appliances that use Fabric OS V7.x.

To collect syslog events, you must configure your switch to forward syslog events. Each switch or appliance must be configured to forward events.

Events that you forward from Brocade switches are automatically discovered. A log source is configured for each switch or appliance that forwards events to SIEM. Brocade switches or appliance that run Fabric OS V7.x.

Configuring Syslog for Brocade Fabric OS appliances

To collect events, you must configure syslog on your Brocade appliance to forward events to SIEM.

Procedure

1 Log in to your appliance as an admin user.

2 To configure an address to forward syslog events, type the following command:
`syslogdipadd <IP address>`
Where `<IP address>` is the IP address of the SIEM Console, Event Processor, Event Collector, or all-in-one system.

3 To verify the address, type the following command:
`syslogdipshow`

Result

As events are generated by the Brocade switch, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the Brocade appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the SIEM Console and verify that the log source is created on the Console and that the **Log Activity** tab displays events from the Brocade appliance.

25 CA Technologies

This section provides information on the following DSMs:

CA ACF2

SIEM includes two options for integrating CA Access Control Facility (ACF2) events:

Integrate CA ACF2 with SIEM using IBM Security zSecure

The CA ACF2 DSM allows you to integrate LEEF events from an ACF2 image on an IBM z/OS mainframe using IBM Security zSecure.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows SIEM to retrieve the events on the schedule you have defined.

To integrate CA ACF2 events:

1 Confirm your installation meets any prerequisite installation requirements.

2 Configure your CA ACF2 z/OS image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

3 Create a log source in SIEM for CA ACF2 to retrieve your LEEF formatted event logs.

4 Optional. Create a custom event property for CA ACF2 in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following installation prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.

- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.
  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Create a Log Source for ACF2 in SIEM

You can use the Log File protocol to retrieve archived log files containing events from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

To configure a log source in SIEM for CA ACF2:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **CA ACF2**.

9 From the **Protocol Configuration** list, select **Log File**.

10 Configure the following values:

Table 28: CA ACF2 Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify the IP address or host name of the device that uniquely identifies the log source. This allows events to be identified at the device level in your network, instead of identifying the event for the file repository.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.

Table 28: CA ACF2 Log File Parameters (Continued)

Parameter	Description
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern ACF2.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with ACF2 and ending with .gz, type the following: `ACF2.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.

Table 28: CA ACF2 Log File Parameters (Continued)

Parameter	Description
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The CA ACF2 configuration is complete. If your configuration requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Integrate CA ACF2 with SIEM using Audit Scripts

The CA Access Control Facility (ACF2) DSM allows you to use an IBM mainframe to collect events and audit transactions with the log file protocol.

Configuration Overview

QexACF2.load.trs is a TERSED file containing a PDS loadlib with the QEXACF2 program. A tersed file is similar to a zip file and requires you to use the TRSMAIN program to uncompress the contents. The TRSMAIN program is available from http://support.extremenetworks.com.

To upload a TRS file from a workstation, you must pre-allocate a file with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL= 1024, BLKSIZE=6144. The file transfer type must be BINARY APPEND. If the transfer type is TEXT or TEXT APPEND, then the file cannot properly uncompress.

After you upload the file to the mainframe into the preallocated dataset the tersed file can be UNPACKED using the TRSMAIN utility using the sample JCL also included in the tar package. A return code of 0008 from the TRSMAIN utility indicates the dataset is not recognized as a valid TERSED file. This error might be the result of the file not being uploaded to a file with the correct DCB attributes or due to the fact that the transfer was not performed using the BINARY APPEND transfer mechanism.

After you have successfully UNPACKED the loadlib file, you can run the QEXACF2 program with the sample JCL file. The sample JCL file is contained in the tar collection. To run the QEXACF2 program, you must modify the JCL to your local naming conventions and JOB card requirements. You might also need to use the STEPLIB DD if the program is not placed in a LINKLISTED library.

To integrate CA ACF2 events into SIEM:

1 The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.

2 The CA ACF2 data is extracted from the live repository using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.

3 The `QexACF2.load.trs` program pulls data from the SMF formatted file. The `QexACF2.load.trs` program only pulls the relevant events and fields for SIEM and writes that information in a condensed format for compatibility. The information is saved in a location accessible by SIEM.

4 SIEM uses the log file protocol source to retrieve the output file information on a scheduled basis. SIEM then imports and processes this file.

Configure CA ACF2 to Integrate with SIEM

SIEM uses scripts to write audit events to from CA ACF2 installations, which are retrieved by SIEM using the Log File protocol.

Procedure

1 From the Extreme Networks Support Portal (http://support.extremenetworks.com), download the following compressed file:
`qexacf2_bundled.tar.gz`

2 On a Linux-based operating system, extract the file:
`tar -zxvf qexacf2_bundled.tar.gz`
The following files are contained in the archive:
QexACF2.JCL.txt - Job Control Language file
QexACF2.load.trs - Compressed program library (requires IBM TRSMAIN)
trsmain sample JCL.txt - Job Control Language for TRSMAIN to decompress the .trs file

3 Load the files onto the IBM mainframe using the following methods:
   a Upload the sample `QexACF2_trsmain_JCL.txt` and `QexACF2.JCL.txt` files using the TEXT protocol.
   b Upload the `QexACF2.load.trs` file using a BINARY mode transfer and append to a pre-allocated data set. The `QexACF2.load.trs` file is a tersed file containing the executable (the mainframe program QexACF2). When you upload the .trs file from a

workstation, pre-allocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

NOTE

QexACF2 is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. QexACF2 adds a header to each record containing event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for SIEM and the blank suppression reduces network traffic to SIEM. This program does not consume CPU or I/O disk resources.

4 Customize the `trsmain sample_JCL.txt` file according to your installation-specific parameters.

For example, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The `trsmain sample_JCL.txt` file uses the IBM utility TRSMAIN to extract the program stored in the `QexACF2.load.trs` file.

An example of the `QexACF2_trsmain_JCL.txt` file includes:

```
//TRSMAIN    JOB (yourvalidjobcard),Q1labs,
//   MSGCLASS=V
//DEL      EXEC PGM=IEFBR14
//D1      DD    DISP=(MOD,DELETE),DSN=<yourhlq>.QEXACF2.LOAD.TRS
//          UNIT=SYSDA,
//          SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT   DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE     DD DISP=SHR,DSN=<yourhlq>.QEXACF2.LOAD.TRS
//OUTFILE    DD DISP=(NEW,CATLG,DELETE),
//             DSN=<yourhlq>.LOAD,
//          SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

The .trs input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the **`QexACF2`** program as a member.

5 You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.

6 After uploading, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct dataset name of the library that will contain the program.

7 The **`QexACF2_jcl.txt`** file is a text file containing a sample JCL. You must configure the job card to meet your configuration.

The **`QexACF2_jcl.txt`** sample file includes:

```
//QEXACF2  JOB  (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
//  MSGCLASS=P,
//  REGION=0M
```

```
//*
//*QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1 SET SMFIN='MVS1.SMF.RECORDS(0)',
// QEXOUT='Q1JACK.QEXACF2.OUTPUT',
// SMFOUT='Q1JACK.ACF2.DATA'
//*************************************************************
//* Delete old datasets                                       *
//*************************************************************
//DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&SMFOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&QEXOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset                                      *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QEXOUT,
// SPACE=(CYL,(100,100)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute ACFRPTPP (Report Preprocessor GRO) to extract ACF2*
//* SMF records                                               *
//*************************************************************
//PRESCAN EXEC PGM=ACFRPTPP
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DISP=SHR,DSN=&SMFIN
//SMFFLT DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//*************************************************************
//* execute QEXACF2                                           *
//*************************************************************
//EXTRACT EXEC PGM=QEXACF2,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//ACFIN DD DISP=SHR,DSN=&SMFOUT
//ACFOUT DD DISP=SHR,DSN=&QEXOUT
//*************************************************************
```

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//*
```

8 After the output file is created, you must choose one of the following options:

a Schedule a job to a transfer the output file to an interim FTP server.

Each time the job completes, the output file is forwarded to an interim FTP server. You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

For example:

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

Where:

<IPADDR> is the IP address or host name of the interim FTP server to receive the output file.

<USER> is the user name required to access the interim FTP server.

<PASSWORD> is the password required to access the interim FTP server.

<THEIPOFTHEMAINFRAMEDEVICE> is the destination of the mainframe or interim FTP server receiving the output.

For example:

```
PUT 'Q1JACK.QEXACF2.OUTPUT.C320' /192.168.1.101/ACF2/
QEXACF2.OUTPUT.C320
```

<QEXOUTDSN> is the name of the output file saved to the interim FTP server.

You are now ready to create a log source in SIEM. For more information, see Create a Log Source on page 81.

b Schedule SIEM to retrieve the output file from CA ACF2.

If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is required and SIEM can pull the output file directly from the mainframe. The following text must be commented out using //* or deleted from the **QexACF2_jcl.txt** file:

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
```

```
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

You are now ready to configure the a log source in SIEM.

Create a Log Source

A log file protocol source allows SIEM to retrieve archived log files from a remote host.

The CA ACF2 DSM supports the bulk loading of log files using the log file protocol source. When configuring your CA ACF2 DSM to use the log file protocol, make sure the hostname or IP address configured in the CA ACF2 is the same as configured in the Remote Host parameter in the Log File protocol configuration.

To configure a log source in SIEM for CA ACF2:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **CA ACF2**.

9 From the **Protocol Configuration** list, select **Log File**.

10 Configure the following values:

Table 29: CA ACF2 Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify the IP address or host name of the device that uniquely identifies the log source. This allows events to be identified at the device level in your network, instead of identifying the event for the file repository.

Table 29: CA ACF2 Log File Parameters (Continued)

Parameter	Description
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.

Table 29: CA ACF2 Log File Parameters (Continued)

Parameter	Description
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern zOS.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: `ACF2.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.

Table 29: CA ACF2 Log File Parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The CA ACF2 configuration is complete. If your configuration requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

CA SiteMinder

The CA SiteMinder DSM collects and categorizes authorization events from CA SiteMinder appliances using syslog-ng.

Supported Event Types

The CA SiteMinder DSM accepts access and authorization events logged in smaccess.log and forwards the events to SIEM using syslog-ng.

Configure a Log Source

CA SiteMinder with SIEMSIEM does not automatically discover authorization events forwarded using syslog-ng from CA SiteMinder appliances.

To manually create a CA SiteMinder log source:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

3 Click the Log Sources icon.

The Log Sources window is displayed.

4 In the **Log Source Name** field, type a name for your CA SiteMinder log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select CA SiteMinder.

7 From the Protocol Configuration list, select Syslog.
The syslog protocol parameters are displayed.

NOTE

The Log File protocol is displayed in the **Protocol Configuration** list, however, polling for log files is not a recommended configuration method.

8 Configure the following values:

Table 30: Adding a Syslog Log Source

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your CA SiteMinder appliance.
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source device. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** list in the System Settings window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on Settings, see the *SIEM Administration Guide*.
Store Event Payload	Select this check box to enable or disable SIEM from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list in the System Settings window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on Settings, see the *SIEM Administration Guide*.

9 Click **Save**.

The **Admin** tab toolbar detects log source changes and displays a messages to indicate when you need to deploy a change.

10 On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure syslog-ng on your CA SiteMinder appliance to forward events to SIEM.

Configure Syslog-ng for CA SiteMinder

You must configure your CA SiteMinder appliance to forward syslog-ng events to your SIEM Console or Event Collector.

SIEM can collect syslog-ng events from TCP or UDP syslog sources on port 514.

To configure syslog-ng for CA SiteMinder:

1 Using SSH, log in to your CA SiteMinder appliance as a root user.

2 Edit the syslog-ng configuration file.
`/etc/syslog-ng.conf`

3 Add the following information to specify the access log as the event file for syslog-ng:
```
source s_siteminder_access {
file("/opt/apps/siteminder/sm66/siteminder/log/smaccess.log");
};
```

4 Add the following information to specify the destination and message template:
```
destination d_remote_q1_siteminder {
     udp("<SIEM IP>" port(514) template ("$PROGRAM $MSG\n"));
};
```
Where `<SIEM IP>` is the IP address of the SIEM Console or Event Collector.

5 Add the following log entry information:
```
log {
     source(s_siteminder_access);
     destination(d_remote_q1_siteminder);
};
```

6 Save the syslog-ng.conf file.

7 Type the following command to restart syslog-ng:
```
service syslog-ng restart
```
After the syslog-ng service restarts, the CA SiteMinder configuration is complete. Events forwarded to SIEM by CA SiteMinder are display on the **Log Activity** tab.

CA Top Secret

SIEM includes two options for integrating CA Top Secret events:

- Integrate CA Top Secret with SIEM using IBM Security zSecure on page 87
- Integrate CA Top Secret with SIEM using Audit Scripts on page 91

Integrate CA Top Secret with SIEM using IBM Security zSecure

The CA Top Secret DSM allows you to integrate LEEF events from a Top Secret image on an IBM z/OS mainframe using IBM Security zSecure.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows SIEM to retrieve the events on the schedule you have defined.

To integrate CA Top Secret events:

1. Confirm your installation meets any prerequisite installation requirements.
2. Configure your CA Top Secret z/OS image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.
3. Create a log source in SIEM for CA Top Secret to retrieve your LEEF formatted event logs.
4. Optional. Create a custom event property for CA Top Secret in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.

  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Create a Log Source

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

To configure a log source in SIEM for CA Top Secret:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **CA Top Secret**.

9 From the **Protocol Configuration** list, select **Log File**.

10 Configure the following values:

Table 31: CA Top Secret Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify the IP address or host name of the device that uniquely identifies the log source. This allows events to be identified at the device level in your network, instead of identifying the event for the file repository.

Table 31: CA Top Secret Log File Parameters (Continued)

Parameter	Description
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.

Table 31: CA Top Secret Log File Parameters (Continued)

Parameter	Description
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern TSS.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with TSS and ending with .gz, type the following: `TSS.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.

Table 31: CA Top Secret Log File Parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The CA Top Secret configuration is complete. If your configuration requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Integrate CA Top Secret with SIEM using Audit Scripts

The CA Top Secret DSM allows you to integrate with an IBM zOS mainframe to collect events and audit transactions.

SIEM records all relevant and available information from the event.

To integrate CA Top Secret events into SIEM:

1 The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.

2 At midnight, the CA Top Secret data is extracted from the live repository using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.

3 The `qextopsloadlib` program pulls data from the SMF formatted file. The `qextopsloadlib` program only pulls the relevant events and fields for SIEM and writes that information in a condensed format for compatibility. The information is saved in a location accessible by SIEM.

4 SIEM uses the log file protocol source to retrieve the output file information on a scheduled basis. SIEM then imports and processes this file.

Configure CA Top Secret to Integrate with SIEM

To integrate CA Top Secret with SIEM:

1 From the Extreme Networks Support Portal (http://support.extremenetworks.com). download the following compressed file:
`qextops_bundled.tar.gz`

2 On a Linux-based operating system, extract the file:
`tar -zxvf qextops_bundled.tar.gz`
The following files are contained in the archive:
qextops_jcl.txt
qextopsloadlib.trs
qextops_trsmain_JCL.txt

3 Load the files onto the IBM mainframe using any terminal emulator file transfer method.
   a Upload the sample `qextops_trsmain_JCL.txt` and `qextops_jcl.txt` files using the TEXT protocol.
   b Upload the `qextopsloadlib.trs` file using a BINARY mode transfer. The `qextopsloadlib.trs` file is a tersed file containing the executable (the mainframe program qextops). When you upload the .trs file from a workstation, pre-allocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

NOTE

Qextops is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. Qextops adds a header to each record containing event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for SIEM and the blank suppression reduces network traffic to SIEM. This program does not consume CPU or I/O disk resources.

4 Customize the `qextops_trsmain_JCL.txt` file according to your installation-specific requirements.
The `qextops_trsmain_JCL.txt` file uses the IBM utility TRSMAIN to extract the program stored in the `qextopsloadlib.trs` file.
An example of the `qextops_trsmain_JCL.txt` file includes:

```
//TRSMAIN    JOB (yourvalidjobcard),Q1labs,
//   MSGCLASS=V
//DEL      EXEC PGM=IEFBR14
//D1      DD    DISP=(MOD,DELETE),DSN=<yourhlq>.QEXTOPS.TRS
//          UNIT=SYSDA,
//          SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT   DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE      DD DISP=SHR,DSN=<yourhlq>.QEXTOPS.TRS
//OUTFILE    DD DISP=(NEW,CATLG,DELETE),
//             DSN=<yourhlq>.LOAD,
```

```
//         SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

You must update the file with your installation specific information for parameters, for example, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The .trs input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the **qextops** program as a member.

5 You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in the LINKLST. The program does not require authorization.

6 After uploading, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct dataset name of the library that will contain the program.

7 The **qextops_jcl.txt** file is a text file containing a sample JCL. You must configure the job card to meet your configuration.

The **qextops_jcl.txt** sample file includes:

```
//QEXTOPS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXTOPS   JCL version 1.0   September, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1   SET   TSSOUT='Q1JACK.EARLOUT.ALL',
//             EARLOUT='Q1JACK.QEXTOPS.PROGRAM.OUTPUT'
//*************************************************************
//*     Delete old datasets                                    *
//*************************************************************
//DEL     EXEC PGM=IEFBR14
//DD1     DD    DISP=(MOD,DELETE),DSN=&TSSOUT,
//         UNIT=SYSDA,
//         SPACE=(CYL,(10,10)),
//         DCB=(RECFM=FB,LRECL=80)
//DD2     DD    DISP=(MOD,DELETE),DSN=&EARLOUT,
//         UNIT=SYSDA,
//         SPACE=(CYL,(10,10)),
//         DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//*     Allocate new dataset                                   *
//*************************************************************
//ALLOC   EXEC PGM=IEFBR14
//DD1     DD    DISP=(NEW,CATLG),DSN=&EARLOUT,
//         SPACE=(CYL,(100,100)),
//         DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute Top Secret TSSUTIL utility to extract smf records*
//*************************************************************
//REPORT EXEC PGM=TSSUTIL
```

```
//SMFIN  DD   DISP=SHR,DSN=&SMFIN1
//SMFIN1  DD  DISP=SHR,DSN=&SMFIN2
//UTILOUT  DD  DSN=&UTILOUT,
//              DISP=(,CATLG),UNIT=SYSDA,SPACE=(CYL,(50,10),RLSE),
//              DCB=(RECFM=FB,LRECL=133,BLKSIZE=0)
//EARLOUT  DD  DSN=&TSSOUT,
//              DISP=(NEW,CATLG),UNIT=SYSDA,
//              SPACE=(CYL,(200,100),RLSE),
//              DCB=(RECFM=VB,LRECL=456,BLKSIZE=27816)
//UTILIN  DD  *
  NOLEGEND
  REPORT  EVENT(ALL)   END
/*
//*************************************************************
//EXTRACT   EXEC  PGM=QEXTOPS,DYNAMNBR=10,
//            TIME=1440
//STEPLIB    DD   DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN    DD   DUMMY
//SYSTSPRT   DD   SYSOUT=*
//SYSPRINT   DD   SYSOUT=*
//CFG          DD   DUMMY
//EARLIN      DD   DISP=SHR,DSN=&TSSOUT
//EARLOUT    DD   DISP=SHR,DSN=&EARLOUT
//*************************************************************
//FTP  EXEC  PGM=FTP,REGION=3800K
//INPUT  DD  *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
QUIT
//OUTPUT  DD  SYSOUT=*
//SYSPRINT  DD  SYSOUT=*
```

8 After the output file is created, you must choose one of the following options:

a Schedule a job to a transfer the output file to an interim FTP server.

Each time the job completes, the output file is forwarded to an intermin FTP server. You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

For example:

```
//FTP  EXEC  PGM=FTP,REGION=3800K
//INPUT  DD  *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
QUIT
//OUTPUT  DD  SYSOUT=*
//SYSPRINT  DD  SYSOUT=*
```

Where:

<IPADDR> is the IP address or host name of the interim FTP server to receive the output file.

<USER> is the user name required to access the interim FTP server.

<PASSWORD> is the password required to access the interim FTP server.

<THEIPOFTHEMAINFRAMEDEVICE> is the destination of the mainframe or interim FTP server receiving the output.

For example:

```
PUT 'Q1JACK.QEXTOPS.OUTPUT.C320' /192.168.1.101/CA/
QEXTOPS.OUTPUT.C320
```

<QEXOUTDSN> is the name of the output file saved to the interim FTP server.

You are now ready to configure the Log File protocol. See Create a Log Source on page 81.

b Schedule SIEM to retrieve the output file from CA Top Secret.

If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is required and SIEM can pull the output file directly from the mainframe. The following text must be commented out using //* or deleted from the **qextops_jcl.txt** file:

```
//FTP  EXEC  PGM=FTP,REGION=3800K
//INPUT  DD  *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
QUIT
//OUTPUT  DD  SYSOUT=*
//SYSPRINT  DD  SYSOUT=*
```

You are now ready to configure the Log File protocol. See Create a Log Source on page 81.

Create a Log Source

A log file protocol source allows SIEM to retrieve archived log files from a remote host. The CA Top Secret DSM supports the bulk loading of log files using the log file protocol source.

When configuring your CA Top Secret DSM to use the log file protocol, make sure the hostname or IP address configured in the CA Top Secret is the same as configured in the Remote Host parameter in the Log File Protocol configuration.

To configure a log source in SIEM for CA Top Secret:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **CA Top Secret**.

9 From the **Protocol Configuration** list, select **Log File**.

10 Configure the following values:

Table 32: CA Top Secret Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify the IP address or host name of the device that uniquely identifies the log source. This allows events to be identified at the device level in your network, instead of identifying the event for the file repository.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.

Table 32: CA Top Secret Log File Parameters (Continued)

Parameter	Description
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your event files. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.

Table 32: CA Top Secret Log File Parameters (Continued)

Parameter	Description
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The CA Top Secret configuration is complete. If your configuration requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

26 Check Point

This section provides information on the following DSMs for SIEM:

Check Point FireWall-1

You can configure SIEM to integrate with a Check Point FireWall-1 device using one of the following methods:

NOTE

Depending on your Operating System, the procedures for the Check Point FireWall-1 device might vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integrating Check Point FireWall-1 Using OPSEC

This section describes how to ensure that SIEM accepts Check Point FireWall-1 events using Open Platform for Security (OPSEC/LEA).

To integrate Check Point OPSEC/LEA with SIEM, you must create two Secure Internal Communication (SIC) files and enter the information in to SIEM as a Check Point Firewall-1 log source.

Check Point Firewall-1 Configuration Overview

To integrate Check Point Firewall-1 with SIEM, you must complete the following procedures in sequence:

1. Add SIEM as a host for Check Point Firewall-1.
2. Add an OPSEC application to Check Point Firewall-1.
3. Locate the Log Source Secure Internal Communications DN.
4. In SIEM, configure the OPSEC LEA protocol.
5. Verify the OPSEC/LEA communications configuration.

Adding a Check Point Firewall-1 Host

To add SIEM as a host in Check Point Firewall-1 SmartCenter:

1 Log in to the Check Point SmartDashboard user interface.

2 Select **Manage > Network Objects > New > Node > Host**.

3 Type parameters for your Check Point Firewall-1 host:

Name: `SIEM`

IP Address: `<IP address of SIEM>`

Comment: `<Optional>`

4 Click OK.

5 Select Close.

You are now ready to create an OPSEC Application Object for Check Point Firewall-1.

Creating an OPSEC Application Object

To create the OPSEC Application Object:

1 Open the Check Point SmartDashboard user interface.

2 Select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.

3 Assign a name to the OPSEC Application Object.

For example:

`SIEM-OPSEC`

The OPSEC Application Object name must be different than the host name you typed when creating the node.

a From the **Host** list, select **SIEM**.

b From the **Vendor** list, select **User Defined**.

c In Client Entities, select the **LEA** check box.

d To generate a Secure Internal Communication (SIC) DN, click **Communication**.

e Enter an activation key.

NOTE

The activation key is a password used to generate the SIC DN. When you configure your Check Point log source in SIEM, the activation key is typed into the Pull Certificate Password parameter.

f Click **Initialize.**

The window updates the Trust state from `Uninitialized` to `Initilialized but trust not established`.

g **Click** Close.

The OPSEC Application Properties window is displayed.

h Write down or copy the displayed SIC DN to a text file.

NOTE

The displayed SIC value is required for the OPSEC Application Object SIC Attribute parameter when you configure the Check Point log source in SIEM. The OPSEC Application Object SIC resembles the following example: CN=SIEM-OPSEC,O=cpmodule..tdfaaz.

You are now ready to locate the log source SIC for Check Point Firewall-1.

Locating the Log Source SIC

To locate the Log Source SIC from the Check Point SmartDashboard:

1 Select **Manage > Network Objects**.

2 Select your Check Point Log Host object.

NOTE

You must know if the Check Point Log Host is a separate object in your configuration from the Check Point Management Server. In most cases, the Check Point Log Host is the same object as the Check Point Management Server.

3 Click Edit.

The Check Point Host General Properties window is displayed.

4 Copy the Secure Internal Communication (SIC).

NOTE

Depending on your Check Point version, the Communication button might not be available to display the SIC attribute. You can locate the SIC attribute from the Check Point Management Server command-line interface. You must use the `cpca_client lscert` command from the command-line interface of the Management Server to display all certificates. The Log Source SIC Attribute resembles the following example: cn=cp_mgmt,o=cpmodule...tdfaaz. For more information, see your *Check Point Command Line Interface Guide*.

You must now install the Security Policy from the Check Point SmartDashboard user interface.

5 Select **Policy > Install > OK**.

You are now ready to configure the OPSEC LEA protocol.

Configuring an OPSEC/LEA Log Source in SIEM

To configure the log source in SIEM:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the **Log Sources** icon.

4 Click **Add**.

5 In the **Log Source Name** field, type a name for your log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the **Log Source Type** list, select **Check Point FireWall-1**.

8 Using the Protocol Configuration list, select OPSEC/LEA.

9 Configure the following values:

Table 33: OPSEC/LEA protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address for the log source. This value must match the value configured in the Server IP parameter. The log source identifier must be unique for the log source type.
Server IP	Type the IP address of the Check Point host or Check Point Management Server IP.
Server Port	Type the port used for OPSEC communication. Administrators must ensure the existing firewall policy permits the LEA/ OPSEC connection from your SIEM.
Use Server IP for Log Source	Select this check box if you want to use the LEA server's IP address instead of the managed device's IP address for a log source. By default, the check box is selected.
Statistics Report Interval	Type the interval, in seconds, during which the number of syslog events are recorded in the qradar.log file. The valid range is 4 to 2,147,483,648 and the default is 600.
Authentication Type	From the list, select the authentication type you want to use for this LEA configuration. The options include: • sslca (default) • sslca_clear • clear This value must match the authentication method configured on the Check Point Firewall or Check Point custom log management server.
OPSEC Application Object SIC Attribute (SIC Name)	Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: `CN=LEA, o=fwconsole..7psasx.`

Table 33: OPSEC/LEA protocol parameters (Continued)

Parameter	Description
Log Source SIC Attribute (Entity SIC Name)	Type the SIC name for the server generating log sources. For example: `cn=cp_mgmt,o=fwconsole..7psasx.`
Specify Certificate	Select this check box to define a certificate for this LEA configuration.
Certificate Filename	Type the directory path of the certificate you want to use for this configuration.
Certificate Authority IP	Type the IP address of the SmartCenter server from which you want to pull your certificate.
Pull Certificate Password	Type the password you want to use when requesting a certificate.
OPSEC Application	Type the name of the application you want to use when requesting a certificate. This value can be up to 255 characters in length.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

You are now ready to verify your OPSEC/LEA communications for Check Point Firewall-1.

Editing Your OPSEC Communications Configuration

This section describes how to modify your Check Point FireWall-1 configuration to allow OPSEC communications on non-standard ports, configure communications in a clear text, un-authenticated stream, and verify the configuration in SIEM.

Changing Your Check Point Custom Log Manager (CLM) IP Address

If your Check Point configuration includes a Check Point Custom Log Manager (CLM), you might eventually need to change the IP address for the CLM, which impacts any of the automatically discovered Check Point log sources from that CLM in SIEM. This is because when you manually add the log source for the CLM using the OPSEC/LEA protocol, then all Check Point firewalls that forward logs to the CLM are automatically discovered by SIEM. These automatically discovered log sources cannot be edited. If the CLM IP address changes, you must edit the original Check Point CLM log source that contains the OPSEC/LEA protocol configuration and update the server IP address and log source identifier.

After you update the log source for the new Check Point CLM IP address, then any new events reported from the automatically discovered Check Point log sources are updated.

NOTE

Do not delete and recreate your Check Point CLM or automatically discovered log sources in SIEM. Deleting a log source does not delete event data, but can make finding previously recorded events more difficult to find.

To update your Check Point OPSEC log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the **Log Sources** icon.

5 Select the original Check Point CLM log source containing the OPSEC/LEA protocol configuration and click **Edit**.

6 In the **Log Source Identifier** field, type a new identifying name of your Check Point CLM.

7 In the **Server IP** field, type the new IP address of your Check Point CLM.

8 Click **Save**.

The IP address update for your Check Point CLM in SIEM is complete.

Changing the Default Port for OPSEC LEA Communication

To change the default port on which OPSEC LEA communicates (that is, port 18184):

1 At the command-line prompt of your Check Point SmartCenter Server, type the following command to stop the firewall services:

```
cpstop
```

2 Depending on your Check Point SmartCenter Server operating system, open the following file:

- **Linux** - `$FWDIR\conf\fwopsec.conf`
- **Windows** - `%FWDIR%\conf\fwopsec.conf`

The default contents of this file are as follows:

```
# The VPN-1/FireWall-1 default settings are:
#
#   sam_server   auth_port   0
#   sam_server         port    18183
#
#   lea_server   auth_port    18184
#   lea_server         port    0
#
#   ela_server   auth_port    18187
#   ela_server         port         0
#
#   cpmi_server auth_port    18190
#
#   uaa_server   auth_port    19191
#   uaa_server         port         0
#
```

3 Change the default lea_server auth_port from `18184` to another port number.

4 Remove the hash (`#`) mark from that line.

For example:

```
lea_server   auth_port    18888
#   lea_server         port    0
```

5 Save and close the file.

6 Type the following command to start the firewall services:
`cpstart`

Configuring OPSEC LEA for Un-encrypted Communications

To configure the OPSEC LEA protocol for un-encrypted communications:

1 At the command-line prompt of your Check Point SmartCenter Server, stop the firewall services by typing the following command:
`cpstop`

2 Depending on your Check Point SmartCenter Server operating system, open the following file:

- **Linux** - `$FWDIR\conf\fwopsec.conf`
- **Windows** - `%FWDIR%\conf\fwopsec.conf`

3 Change the default lea_server auth_port from `18184` to `0`.

4 Change the default lea_server port from `0` to `18184`.

5 Remove the hash (`#`) marks from both lines.
For example:
```
lea_server   auth_port    0
lea_server         port    18184
```

6 Save and close the file.

7 Type the following command to start the firewall services:
`cpstart`

8 You are now ready to configure the log source in SIEM.
To configure SIEM to receive events from a Check Point Firewall-1 device:

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the **Log Sources** icon.

5 Click **Add**.

6 From the **Log Source Type** list, select **Check Point FireWall-1**.

7 Using the Protocol Configuration list, select OPSEC/LEA.

8 Configure the following parameters:

Table 34: OPSEC/LEA protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address for the log source. This value must match the value configured in the Server IP parameter. The log source identifier must be unique for the log source type.
Server IP	Type the IP address of the server.
Server Port	Type the port used for OPSEC communication. The valid range is 0 to 65,536 and the default is 18184.
Use Server IP for Log Source	Select this check box if you want to use the LEA server's IP address instead of the managed device's IP address for a log source. By default, the check box is selected.
Statistics Report Interval	Type the interval, in seconds, during which the number of syslog events are recorded in the qradar.log file. The valid range is 4 to 2,147,483,648 and the default is 600.
Authentication Type	From the list, select the authentication type you want to use for this LEA configuration. The options are sslca (default), sslca_clear, or clear. This value must match the authentication method used by the server. The following parameters appear if sslca or sslca_clear is selected as the authentication type. • OPSEC Application Object SIC Attribute (SIC Name) - Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: `CN=LEA, o=fwconsole..7psasx.` The name can be up to 255 characters in length and is case sensitive. • Log Source SIC Attribute (Entity SIC Name) - Type the SIC name of the server, for example: `cn=cp_mgmt,o=fwconsole..7psasx.` The name can be up to 255 characters in length and is case sensitive. • Specify Certificate - Select this check box if you want to define a certificate for this LEA configuration. SIEM attempts to retrieve the certificate using these parameters when the certificate is required. If you select the **Specify Certificate** check box, the Certificate Filename parameter is displayed: • Certificate Filename - This option only appears if Specify Certificate is selected. Type the directory path of the certificate you want to use for this configuration. If you clear the **Specify Certificate** check box, the following parameters appear: • Certificate Authority IP - Type the IP address of the SmartCenter server from which you want to pull your certificate. • Pull Certificate Password - Type the password you want to use when requesting a certificate. The password can be up to 255 characters in length. • OPSEC Application - Type the name of the application you want to use when requesting a certificate. This value can be up to 255 characters in length.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

Integrating Check Point FireWall-1 Using Syslog

This section describes how to ensure that the SIEM Check Point FireWall-1 DSMs accepts FireWall-1 events using syslog.

Configuring Syslog for Check Point FireWall-1

Before you configure SIEM to integrate with a Check Point FireWall-1 device:

NOTE

If Check Point SmartCenter is installed on Microsoft Windows, you must integrate Check Point with SIEM using OPSEC. For more information, see Integrating Check Point FireWall-1 Using OPSEC on page 99.

1 Type the following command to access the Check Point console as an expert user:
`expert`
A password prompt is displayed.

2 Type your expert console password. Press the Enter key.

3 Open the following file:
`/etc/rc.d/rc3.d/S99local`

4 Add the following lines:
`$FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority> > /dev/null 2>&1 &`
Where:
`<facility>` is a Syslog facility, for example, `local3`.
`<priority>` is a Syslog priority, for example, `info`.
For example:
`$FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info > /dev/null 2>&1 &`

5 Save and close the file.

6 Open the syslog.conf file.

7 Add the following line:
`<facility>.<priority> <TAB><TAB>@<host>`
Where:
`<facility>` is the syslog facility, for example, `local3`. This value must match the value you typed in step 4.
`<priority>` is the syslog priority, for example, `info` or `notice`. This value must match the value you typed in step 4.

<TAB> indicates you must press the Tab key.

<host> indicates the SIEM Console or managed host.

8 Save and close the file.

9 Depending on your operating system, type the following command to restart syslog:

In Linux: `service syslog restart`

In Solaris: `/etc/init.d/syslog start`

10 Type the following command:

```
nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
<facility>.<priority> > /dev/null 2>&1 &
```

Where:

<facility> is a Syslog facility, for example, local3. This value must match the value you typed in step 4.

<priority> is a Syslog priority, for example, info. This value must match the value you typed in step 4.

The configuration is complete. The log source is added to SIEM as Check Point Firewall-1 syslog events are automatically discovered. Events forwarded to SIEM are displayed on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Check Point FireWall-1. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Check Point FireWall-1**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 35: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Check Point FireWall-1 appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Integrating Check Point Firewall Events from External Syslog Forwarders

Check Point Firewall events can be forwarded from external sources, such as Splunk Forwarders or other third party syslog forwarders that send events to SIEM.

When Check Point Firewall events are provided from external sources in syslog format, the events identify with IP address in the syslog header. This causes events to identify incorrectly when they are processed with the standard syslog protocol. The syslog redirect protocol provides administrators a method to substitute an IP address from the event payload into the syslog header to correctly identify the event source.

To substitute an IP address, administrators must identify a common field from their Check Point Firewall event payload that contains the proper IP address. For example, events from Splunk Forwarders use `orig=` in the event payload to identify the original IP address for the Check Point firewall. The protocol substitutes in the proper IP address to ensure that the device is properly identified in the log source. As Check Point Firewall events are forwarded, SIEM automatically discovers and create new log sources for each unique IP address.

Substitutions are done with regular expressions and can support either TCP or UDP syslog events. The protocol automatically configures iptables for the initial log source and port configuration. If an administrator decides to change the port assignment a Deploy Full Configuration is required to update the iptables configuration and use the new port assignment.

Configuring a LogSource for Check Point Forwarded Events

To collect raw events forwarded from an external source, you must configure a log source before events are forwarded to SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Check Point FireWall-1**.

9 From the **Protocol Configuration** list, select **Syslog Redirect**.

10 Configure the following values:

Table 36: Syslog redirect protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for the Check Point Firewall events. The log source identifier must be unique value.
Log Source Identifier RegEx	Type the regular expression (regex) required to identify the Check Point Firewall IP address from the event payload. For example, administrators can use the following regular expression to parse Check Point Firewall events provided by Splunk Forwarders. `orig=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`
Listen Port	Type the port number used by SIEM to accept incoming syslog redirect events. The default listen port is 517. The port number you configure must match the port that you configured on the appliance that forwards the syslog events. Administrators cannot specify port 514 in this field.
Protocol	From the list, select either **UDP** or **TCP.** The syslog redirect protocol supports any number of UDP syslog connection, but restricts TCP connections to 2500. If an administrator has more than 2500 log sources in the syslog stream, a second Check Point log source and listen port number is required.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.

Table 36: Syslog redirect protocol parameters (Continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

Check Point Provider-1

You can configure SIEM to integrate with a Check Point Provider-1 device.

All events from Check Point Provider-1 are parsed using the Check Point FireWall-1 DSM. You can integrate Check Point Provider-1 using one of the following methods:

- Integrating Syslog for Check Point Provider-1 on page 111
- Configuring OPSEC for Check Point Provider-1 on page 113

NOTE

Depending on your Operating System, the procedures for the Check Point Provider-1 device can vary. The following procedures are based on the Check Point SecurePlatform operating system.

Integrating Syslog for Check Point Provider-1

This method ensures the Check Point FireWall-1 DSM for SIEM accepts Check Point Provider-1 events using syslog.

SIEM records all relevant Check Point Provider-1 events.

Configure syslog on Check Point Provider-1

To configure syslog on your Check Point Provider-1 device:

1 Type the following command to access the console as an expert user:
`expert`
A password prompt is displayed.

2 Type your expert console password. Press the Enter key.

3 Type the following command:
`csh`

4 Select the desired customer logs:

```
mdsenv <customer name>
```

5 Type the following command:

```
# nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
<facility>.<priority> 2>&1 &
```

Where:

`<facility>` is a Syslog facility, for example, local3.

`<priority>` is a Syslog priority, for example, info.

You are now ready to configure the log source in SIEM.

The configuration is complete. The log source is added to SIEM as Check Point Firewall-1 syslog events are automatically discovered. Events forwarded to SIEM are displayed on the **Log Activity** tab.

Configure a Log source

SIEM automatically discovers and creates a log source for syslog events from Check Point Provider-1 as Check Point FireWall-1 events. The following configuration steps are optional.

To manually configure a log source for Check Point Provider-1 syslog events:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Check Point Firewall-1**.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 37: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Check Point Provider-1 appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Configuring OPSEC for Check Point Provider-1

This method ensures the SIEM Check Point FireWall-1 DSM accepts Check Point Provider-1 events using OPSEC.

Reconfigure Check Point Provider-1 SmartCenter

This section describes how to reconfigure the Check Point Provider-1 SmartCenter.

In the Check Point Provider-1 Management Domain GUI (MDG), create a host object representing the SIEM. The leapipe is the connection between the Check Point Provider-1 and SIEM.

To reconfigure the Check Point Provider-1 SmartCenter (MDG):

1 To create a host object, open the Check Point SmartDashboard user interface and select **Manage > Network Objects > New > Node > Host**.

2 Type the Name, IP Address, and optional Comment for your host.

3 Click **OK**.

4 Select **Close**.

5 To create the OPSEC connection, select **Manage > Servers and OPSEC Applications New > OPSEC Application Properties**.

6 Type a name and optional comment.
The name you type must be different than the name used in step 2.

7 From the Host drop-down menu, select the SIEM host object that you just created.

8 From **Application Properties**, select User Defined as the Vendor type.

9 From **Client Entries**, select **LEA**.

10 Configure the Secure Internal Communication (SIC) certificate, click Communication and enter an activation key.

11 Select **OK** and then **Close**.

12 To install the Policy on your firewall, select **Policy > Install > OK**.

Configure an OPSEC Log Source

To configure the log source in SIEM:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the **Log Sources** icon.
The Log Sources window is displayed.

5 Click **Add**.
The Add a log source window is displayed.

6 From the **Log Source Type** list, select **Check Point FireWall-1**.

7 Using the Protocol Configuration list, select OPSEC/LEA.

The OPSEC/LEA protocol parameters appear.

8 Configure the following values:

a **Log Source Name** - Type a name for the log source.

b L**og Source Identifier** - Type the IP address for the log source. This value must match the value you typed in the Server IP parameter.

c **Server IP** - Type the IP address of the Check Point Provider-1.

d **Server Port** - Type the port used for OPSEC/LEA. The default is 18184.

You must ensure the existing firewall policy permits the LEA/OPSEC connection from your SIEM.

e **OPSEC Application Object SIC Attribute** - Type the SIC DN of the OPSEC Application Object.

f **Log Source SIC Attribute** - Type the SIC name for the server generating the log source.

SIC attribute names can be up to 255 characters in length and are case sensitive.

g **Specify Certificate** - Ensure the Specify Certificate check box is clear.

h **Pull Certificate Password** - Type the activation key password.

i **Certificate Authority IP** - Type the Check Point Manager Server IP address.

j **OPSEC Application** - Type the name of the application requesting a certificate.

For example:

If the value is `CN=SIEM-OPSEC,O=cpmodule...tdfaaz,` the OPSEC Application value is `SIEM-OPSEC`.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. For detailed information on the OPSEC/LEA protocol, see the *SIEM Log Sources User Guide*.

27 Cilasoft QJRN/400

SIEM collects detailed audit events from Cilasoft QJRN/400 software for IBM i (AS/400, iSeries, System i).

Configuration Overview

To collect events, administrators can configure Cilasoft QJRN/400 to forward events with syslog or optionally configure the integrated file system (IFS) to write events to a file. Syslog provides real-time events to SIEM and provides automatic log source discovery for administrators, which is the easiest configuration method for event collection. The IFS option provides an optional configuration to write events to a log file, which can be read remotely by using the Log File protocol. SIEM supports syslog events from Cilasoft QJRN/400 V5.14.K and later.

To configure Cilasoft QJRN/400, complete the following tasks:

1 On your Cilasoft QJRN/400 installation, configure the Cilasoft Security Suite to forward syslog events to SIEM or write events to a file.

2 For syslog configurations, administrators can verify that the events forwarded by Cilasoft QJRN/400 are automatically discovered on the Log Activity tab.

Cilasoft QJRN/400 configurations that use IFS to write event files to disk are considered an alternative configuration for administrators that cannot use syslog. IFS configurations require the administrator to locate the IFS file and configure the host system to allow FTP, SFTP, or SCP communications. A log source can then be configured to use the log file protocol with the location of the event log file.

Configuring Cilasoft QJRN/400

To collect events, you must configure queries on your Cilasoft QJRN/400 to forward syslog events to SIEM.

Procedure

1 To start the Cilasoft Security Suite, type the following command:
`IJRN/QJRN`

The account that is used to make configuration changes must have ADM privileges or USR privileges with access to specific queries through an Extended Access parameter.

2 To configure the output type, select one of the following options:
   a To edit several selected queries, type **2EV** to access the Execution Environment and change the **Output Type** field and type **SEM**.
   b To edit large numbers of queries, type the command CHGQJQRYA and change the **Output Type** field and type **SEM**.

3 On the Additional Parameters screen, configure the following parameters:

Table 38: Cilasoft QJRN/400 output parameters

Parameter	Description
Format	Type ***LEEF** to configure the syslog output to write events in Log Extended Event Format (LEEF). LEEF is a special event format that is designed to for SIEM.
Output	To configure an output type, one of the following parameters to select an output type: ***SYSLOG** - Type this parameter to forward events with the syslog protocol. This option provides real-time events. ***IFS** - Type this parameter to write events to a file with the Integrated File System. This option requires the administrator to configure a log source with the Log File protocol. This option writes events to a file, which can only be read in 15 minute intervals.
IP Address	Type the IP address of your SIEM system. If an IP address for SIEM is defined as a special value in the WRKQJVAL command, you can type ***CFG**. Events can be forwarded to either the Console, an Event Collector, an Event Processor, or your SIEM all-in-one appliance.
Port	Type **514** or ***CFG** as the port for syslog events. By default, *CFG automatically selects port 514.
Tag	This field is not used by SIEM.
Facility	This field is not used by SIEM.
Severity	Select a value for the event severity. For more information on severity that is assigned to *QRY destinations, see command WRKQJFVAL in your Cilasoft documentation.

For more information on Cilasoft configuration parameters, see the *Cilasoft QJRN/400 User's Guide*.

Syslog events that are forwarded to SIEM are viewable on the **Log Activity** tab.

Configuring a Cilasoft QJRN/400 Log Source

SIEM automatically discovers and creates a log source for syslog events that are forwarded from Cilasoft QJRN/400. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 From the Log Source Type list, select **Cilasoft QJRN/400**.

7 From the **Protocol Configuration** list, select **Syslog**.

NOTE

If Cilasoft QJRN/400 is configured to write events to the integrated file system with the *IFS option, the administrator must select Log File. Configuration instructions for the log file protocol are available in the *Log Sources User Guide*.

8 Configure the following values:

Table 39: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address as an identifier for events from your Cilasoft QJRN/400 installation. The log source identifier must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

28 Cisco

This section provides information on the following DSMs:

Cisco ACE Firewall

You can integrate a Cisco ACE firewall with SIEM.

SIEM can accept events forwarded from Cisco ACE Firewalls using syslog. SIEM records all relevant events. Before you configure SIEM to integrate with an ACE firewall, you must configure your Cisco ACE Firewall to forward all device logs to SIEM.

Configure Cisco ACE Firewall

To forward Cisco ACE device logs to SIEM:

1 Log in to your Cisco ACE device.

2 From the shell interface, select **Main Menu > Advanced Options > Syslog Configuration**.

3 The Syslog Configuration menu varies depending on whether there are any syslog destination hosts configured yet. If no syslog destinations have been added, create one by selecting the **Add First Server** option. Click **OK**.

4 Type the hostname or IP address of the destination host and port in the **First Syslog Server** field. Click **OK**.

The system restarts with new settings. When finished, the Syslog server window displays the host you have configured.

5 Click OK.

The Syslog Configuration menu is displayed. Notice that options for editing the server configuration, removing the server, or adding a second server are now available.

6 If you want to add another server, click **Add Second Server**.

At any time, click the View Syslog options to view existing server configurations.

7 To return to the Advanced Menu, click **Return**.

The configuration is complete. The log source is added to SIEM as Cisco ACE Firewall events are automatically discovered. Events forwarded to SIEM by Cisco ACE Firewall appliances are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco ACE Firewalls.

However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

To manually configure a log source for Cisco ACE Firewall:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco ACE Firewall.

9 Using the Protocol Configuration list, select **Syslog**.

The syslog protocol configuration is displayed.

10 Configure the following values:

Table 40: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco ACE Firewalls.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Cisco Aironet

You can integrate a Cisco Aironet devices with SIEM.

A Cisco Aironet DSM accepts Cisco Emblem Format events using syslog. Before you configure SIEM to integrate with a Cisco Aironet device, you must configure your Cisco Aironet appliance to forward syslog events.

Configure Cisco Aironet

To configure Cisco Aironet to forward events:

1 Establish a connection to the Cisco Aironet device using one of the following methods"

- Telnet to the wireless access point
- Access the console

2 Type the following command to access privileged EXEC mode:
`enable`

3 Type the following command to access global configuration mode:
`config terminal`

4 Type the following command to enable message logging:
`logging on`

5 Configure the syslog facility. The default is local7.
`logging facility <facility, for example, local7>`

6 Type the following command to log messages to your SIEM:
`logging <IP address of your SIEM>`

7 Enable timestamp on log messages:
`service timestamp log datatime`

8 Return to privileged EXEC mode:
`end`

9 View your entries:
`show running-config`

10 Save your entries in the configuration file:
`copy running-config startup-config`

The configuration is complete. The log source is added to SIEM as Cisco Aironet events are automatically discovered. Events forwarded to SIEM by Cisco Aironet appliances are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco Aironet. The following configuration steps are optional.

To manually configure a log source for Cisco Aironet:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Aironet.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 41: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco Aironet appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco ACS

The Cisco ACS DSM for SIEM accepts syslog ACS events using syslog.

SIEM records all relevant and available information from the event. You can integrate Cisco ACS with SIEM using one of the following methods:

- Configure your Cisco ACS device to directly send syslog to SIEM for Cisco ACS v5.x. See Configure Syslog for Cisco ACS v5.x on page 122.
- Configure your Cisco ACS device to directly send syslog to SIEM for Cisco ACS v4.x. See Configure Syslog for Cisco ACS v4.x on page 124.
- A server using the SIEM WinCollect or Adaptive Log Exporter (Cisco ACS software version 3.x or later). See Configure Cisco ACS for the Adaptive Log Exporter on page 125.

NOTE

SIEM only supports Cisco ACS versions prior to v3.x using a Universal DSM.

Configure Syslog for Cisco ACS v5.x

The configure syslog forwarding from a Cisco ACS appliance with software version 5.x, you must:

Create a Remote Log Target

To create a remote log target for your Cisco ACS appliance:

1 Log in to your Cisco ACS appliance.

2 On the navigation menu, click System Administration > Configuration > Log Configuration > Remote Log Targets.

The Remote Log Targets page is displayed.

3 Click **Create**.

4 Configure the following parameters:

Table 42: Remote Target Parameters

Parameter	Description
Name	Type a name for the remote syslog target.
Description	Type a description for the remote syslog target.
Type	Select **Syslog**.
IP Address	Type the IP address of SIEM or your Event Collector.

5 Click **Submit**.

You are now ready to configure global policies for event logging on your Cisco ACS appliance.

Configure Global Logging Categories

To configure Cisco ACS to forward log failed attempts to SIEM:

1 On the navigation menu, click System Administration > Configuration > Log Configuration > Global.
The Logging Categories window is displayed.

2 Select the **Failed Attempts** logging category and click Edit.

3 Click **Remote Syslog Target**.

4 From the **Available targets** window, use the arrow key to move the syslog target for SIEM to the **Selected targets** window.

5 Click **Submit**.
You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco ACS v5.x.

However, you can manually create a log source for SIEM to receive Cisco ACS events.

To manually configure a log source for Cisco ACS:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 From the Log Source Type list, select Cisco ACS.

7 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

8 Configure the following values:

Table 43: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for Cisco ACS events.

9 Click Save.

10 On the Admin tab, click Deploy Changes.
The configuration is complete.

Configure Syslog for Cisco ACS v4.x

To configure syslog forwarding from a Cisco ACS appliance with software version 4.x, you must:

Configure Syslog Forwarding for Cisco ACS v4.x

To configure an ACS device to forward syslog events to SIEM:

1 Log in to your Cisco ACS device.

2 On the navigation menu, click System Configuration.
The System Configuration page opens.

3 Click Logging.
The logging configuration is displayed.

4 In the Syslog column for **Failed Attempts**, click Configure.
The Enable Logging window is displayed.

5 Select the Log to Syslog Failed Attempts report check box.

6 Add the following Logged Attributes:
- Message-Type
- User-Name
- Nas-IP-Address
- Authen-Failure-Code
- Caller-ID
- NAS-Port
- Author-Data
- Group-Name
- Filter Information
- Logged Remotely

7 Configure the following syslog parameters:
- IP - Type the IP address of SIEM.
- Port - Type the syslog port number of SIEM. The default is port 514.
- Max message length (Bytes) - Type 1024 as the maximum syslog message length.

NOTE

Cisco ACS provides syslog report information for a maximum of two syslog servers.

8 Click Submit.
You are now ready to configure the log source in SIEM.

Configure a Log Source for Cisco ACS v4.x

SIEM automatically discovers and creates a log source for syslog events from Cisco ACS v4.x. The following configuration steps are optional.

To manually create a log source for Cisco ACS v4.x:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 From the Log Source Type list, select Cisco ACS.

7 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

8 Configure the following values:

Table 44: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for Cisco ACS events.

9 Click Save.

10 On the Admin tab, click Deploy Changes.
The configuration is complete.

Configure Cisco ACS for the Adaptive Log Exporter

If you are using an older version of Cisco ACS, such as v3.x, you can log events from your Cisco ACS appliance to a comma-seperated file.

The Cisco ACS device plug-in for the Adaptive Log Exporter can be used to read and forward events from your comma-separated file to SIEM.

Configure Cisco ACS to Log Events

Your Cisco ACS appliance must be configured to write comma-seperated event files to integrate with the Adaptive Log Exporter.

To configure Cisco ACS:

1 Log in to your Cisco ACS appliance.

2 On the navigation manu, click System Configuration.

The System Configuration page opens.

3 Click Logging.
The logging configuration is displayed.

4 In the **CSV column for Failed Attempts**, click Configure.
The Enable Logging window is displayed.

5 Select the Log to CSV Failed Attempts report check box.

6 Add the following Logged Attributes:
- Message-Type
- User-Name
- Nas-IP-Address
- Authen-Failure-Code
- Caller-ID
- NAS-Port
- Author-Data
- Group-Name
- Filter Information
- Logged Remotely

7 Configure a time frame for Cisco ACS to generate a new comma-seperated value (CSV) file.

8 Click Submit.
You are now ready to configure the Adaptive Log Exporter.
For more information on installing and using the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

Cisco ASA

You can integrate a Cisco Adaptive Security Appliance (ASA) with SIEM.

A Cisco ASA DSM accepts events using syslog or NetFlow using NetFlow Security Event Logging (NSEL). SIEM records all relevant events. Before you configure SIEM, you must configure your Cisco ASA device to forward syslog or NetFlow NSEL events.

Choose one of the following options:

- Forward events to SIEM using syslog. See Integrate Cisco ASA Using Syslog on page 126
- Forward events to SIEM using NetFlow NSEL. See Integrate Cisco ASA for NetFlow Using NSEL on page 128

Integrate Cisco ASA Using Syslog

This section includes the following topics:

- Configure Syslog Forwarding on page 131
- Configure a Log Source on page 132

Configure Syslog Forwarding

This section describes how to configure Cisco ASA to forward syslog events.

1 Log in to the Cisco ASA device.

2 Type the following command to access privileged EXEC mode:
```
enable
```

3 Type the following command to access global configuration mode:
```
conf t
```

4 Enable logging:
```
logging enable
```

5 Configure the logging details:
```
logging console warning
logging trap warning
logging asdm warning
```

6 Type the following command to configure logging to SIEM:
```
logging host <interface> <IP address>
```
Where:

`<interface>` is the name of the Cisco Adaptive Security Appliance interface.

`<IP address>` is the IP address of SIEM.

NOTE

Using the command `show interfaces` displays all available interfaces for your Cisco device.

7 Disable the output object name option:
```
no names
```
You must disable the output object name option to ensure that the logs use IP addresses and not object names.

8 Exit the configuration:
```
exit
```

9 Save the changes:
```
write mem
```
The configuration is complete. The log source is added to SIEM as Cisco ASA syslog events are automatically discovered. Events forwarded to SIEM by Cisco ASA are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco ASA. The following configuration steps are optional.

To manually configure a log source for Cisco ASA syslog events:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Adaptive Security Appliance (ASA).

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 45: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your OSSEC installations.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Integrate Cisco ASA for NetFlow Using NSEL

This section includes the following topics:

- Configure NetFlow Using NSEL on page 128
- Configure a Log Source on page 121

Configure NetFlow Using NSEL

To configure Cisco ASA to forward NetFlow events using NSEL.

1 Log in to the Cisco ASA device command-line interface (CLI).

2 Type the following command to access privileged EXEC mode:
`enable`

3 Type the following command to access global configuration mode:
`conf t`

4 Disable the output object name option:
`no names`

5 Type the following command to enable NetFlow export:

`flow-export destination <interface-name> <ipv4-address or hostname> <udp-port>`

Where:

`<interface-name>` is the name of the Cisco Adaptive Security Appliance interface for the NetFlow collector.

`<ipv4-address or hostname>` is the IP address or host name of the Cisco ASA device with the NetFlow collector application.

`<udp-port>` is the UDP port number to which NetFlow packets are sent.

NOTE

SIEM typically uses port 2055 for NetFlow event data on Behavioral Flow Collectors. You must configure a different UDP port on your Cisco Adaptive Security Appliance for NetFlow using NSEL.

6 Type the following command to configure the NSEL class-map:
`class-map flow_export_class`

7 Choose one of the following traffic options:
a To configure a NetFlow access list to match specific traffic, type the command:
`match access-list flow_export_acl`
b To configure NetFlow to match any traffic, type the command:
`match any`

NOTE

The Access Control List (ACL) must exist on the Cisco ASA device before defining the traffic match option in step 7.

8 Type the following command to configure the NSEL policy-map:
`policy-map flow_export_policy`

9 Type the following command to define a class for the flow-export action:
`class flow_export_class`

10 Type the following command to configure the flow-export action:
`flow-export event-type all destination <IP address>`
Where `<IP address>` is the IP address of SIEM.

NOTE

If you are using a Cisco ASA version before v8.3 you can skipstep 10 as the device defaults to the flow-export destination. For more information, see your Cisco ASA documentation.

11 Type the following command to add the service policy globally:
`service-policy flow_export_policy global`

12 Exit the configuration:

```
exit
```

13 Save the changes:

```
write mem
```

You must verify that your collector applications use the Event Time field to correlate events.

Configure a Log Source

To integrate Cisco ASA using NetFlow with SIEM, you must manually create a log source to receive NetFlow events. SIEM does not automatically discover or create log sources for syslog events from Cisco ASA using NetFlow and NSEL.

NOTE

Your system must be running the latest version of the NSEL protocol to integrate with a Cisco ASA device using NetFlow NSEL. The NSEL protocol is available on the Extreme Networks Support Portal, http://support.extremenetworks.com, or through auto updates in SIEM.

To configure a log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Cisco Adaptive Security Appliance (ASA)**.

9 Using the Protocol Configuration list, select **Cisco NSEL**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 46: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source.

Table 46: Syslog Parameters (Continued)

Parameter	Description
Collector Port	Type the UDP port number used by Cisco ASA to forward NSEL events. The valid range of the Collector Port parameter is 1-65535. **NOTE:** SIEM typically uses port 2055 for NetFlow event data on Behavioral Flow Collectors. You must define a different UDP port on your Cisco Adaptive Security Appliance for NetFlow using NSEL.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Cisco ASA are displayed on the **Log Activity** tab. For more information on configuring NetFlow with your Cisco ASA device, see your vendor documentation.

Cisco CallManager

The Cisco CallManager DSM for SIEM collects application events forwarded from Cisco CallManager devices using syslog.

Before receiving events in SIEM, you must configure your Cisco Call Manager device to forward events. After you forward syslog events from Cisco CallManager, SIEM automatically detects and adds Cisco CallManager as a log source.

Configure Syslog Forwarding

To configure syslog on your Cisco CallManager:

1 Log in to your Cisco CallManager interface.

2 Select **System > Enterprise Parameters**.

The Enterprise Parameters Configuration is displayed.

3 In the **Remote Syslog Server Name** field, type the IP address of the SIEM Console.

4 From the **Syslog Severity For Remote Syslog messages** list, select **Informational**

The informational severity allows you to collect all events at the information level and later.

5 Click **Save**.

6 Click **Apply Config**.

The syslog configuration is complete. You are now ready to configure a syslog log source for Cisco CallManager.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco CallManager devices. The following configuration steps are optional.

To manually configure a syslog log source for Cisco CallManager:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Call Manager.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 47: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco CallManager.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco CatOS for Catalyst Switches

The Cisco CatOS for Catalyst Switches DSM for SIEM accepts events using syslog.

SIEM records all relevant device events. Before configuring a Cisco CatOS device in SIEM, you must configure your device to forward syslog events.

Configure Syslog

To configure your Cisco CatOS device to forward syslog events:

1 Log in to your Cisco CatOS user interface.

2 Type the following command to access privileged EXEC mode:
```
enable
```

3 Configure the system to timestamp messages:
```
set logging timestamp enable
```

4 Type the IP address of SIEM:
```
set logging server <IP address>
```

5 Limit messages that are logged by selecting a severity level:
```
set logging server severity <server severity level>
```

6 Configure the facility level that should be used in the message. The default is local7.
```
set logging server facility <server facility parameter>
```

7 Enable the switch to send syslog messages to the SIEM.
```
set logging server enable
```
You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco CatOS appliances. The following configuration steps are optional.

To manually configure a syslog log source for Cisco CatOS:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco CatOS for Catalyst Switches

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 48: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco CatOS for Catalyst Switch appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco CSA

You can integrate a Cisco Security Agent (CSA) server with SIEM.

Supported Event Types

The Cisco CSA DSM accepts events using syslog, SNMPv1, and SNMPv2. SIEM records all configured Cisco CSA alerts.

Configure Syslog for Cisco CSA

To configure your Cisco CSA server to forward events:

1 Open the Cisco CSA user interface.

2 Select **Events > Alerts**.

3 Click **New**.
The Configuration View window is displayed.

4 Type in values for the following parameters:
a **Name** - Type a name you wish to assign to your configuration.
b **Description** - Type a description for the configuration. This parameter is optional.

5 From the **Send Alerts**, select the event set from the list to generate alerts.

6 Select the SNMP check box.

7 Type a Community name.
The Community name entered in the CSA user interface must match the Community field configured on SIEM. This option is only available using the SNMPv2 protocol.

8 In the Manager IP address parameter, type the IP address of SIEM.

9 Click **Save**.
You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco CSA appliances. The following configuration steps are optional.

To manually configure a syslog log source for Cisco CSA:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco CSA.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 49: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco CSA appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco FWSM

You can integrate Cisco Firewall Service Module (FWSM) with SIEM.

Supported Event Types

The Cisco FWSM DSM for SIEM accepts FWSM events using syslog. SIEM records all relevant Cisco FWSM events.

Configure Cisco FWSM to Forward Syslog Events

To integrate Cisco FWSM with SIEM, you must configure your Cisco FWSM appliances to forward syslog events to SIEM.

To configure Cisco FWSM:

1 Using a console connection, telnet, or SSH, log in to the Cisco FWSM.

2 Enable logging:
```
logging on
```

3 Change the logging level:
```
logging trap level (1-7)
```
By default, the logging level is set to 3 (error).

4 Designate SIEM as a host to receive the messages:
```
logging host [interface] ip_address [tcp[/port] | udp[/port]]
[format emblem]
```
For example:
```
logging host dmz1 192.168.1.5
```
Where 192.168.1.5 is the IP address of your SIEM system.

You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco FWSM appliances. The following configuration steps are optional.

To manually configure a syslog log source for Cisco FWSM:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Firewall Services Module (FWSM).

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 50: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco FWSM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco IDS/IPS

The Cisco IDS/IPS DSM for SIEM polls Cisco IDS/IPS for events using the Security Device Event Exchange (SDEE) protocol.

The SDEE specification defines the message format and the protocol used to communicate the events generated by your Cisco IDS/IPS security device. SIEM supports SDEE connections by polling directly to the IDS/IPS device and not the management software, which controls the device.

NOTE

You must have security access or web authentication on the device before connecting to SIEM.

After you configure your Cisco IDS/IPS device, you must configure the SDEE protocol in SIEM. When configuring the SDEE protocol, you must define the URL required to access the device.

For example, `https://www.mysdeeserver.com/cgi-bin/sdee-server`.

You must use an http or https URL, which is specific to your Cisco IDS version:

- If you are using RDEP (for Cisco IDS v4.0), the URL should have /cgi-bin/event-server at the end. For example: `https://www.my-rdep-server.com/cgi-bin/event-server`
- If you are using SDEE/CIDEE (for Cisco IDS v5.x and later), the URL should have /cgi-bin/sdee-server at the end. For example: `https://www.my-sdee-server/cgi-bin/sdee-server`

SIEM does not automatically discover or create log sources for syslog events from Cisco IDS/IPS devices. To integrate Cisco IDS/IPS device events with SIEM, you must manually create a log source for each Cisco IDS/IPS in your network.

To configure a Cisco IDS/IPS log source using SDEE polling:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Intrusion Prevention System (IPS).

9 Using the Protocol Configuration list, select **SDEE**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 51: SDEE Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the SDEE event source. IP addresses or hostnames are recommended as they allow SIEM to identify a log file to a unique event source. The log source identifier must be unique for the log source type.
URL	Type the URL required to access the log source, for example, https://www.mysdeeserver.com/cgi-bin/sdee-server. You must use an http or https URL. The options include: • If you are using SDEE/CIDEE (for Cisco IDS v5.x and later), the URL should have /cgi-bin/sdee-server at the end. For example, `https://www.my-sdee-server/cgi-bin/sdee-server` • If you are using RDEP (for Cisco IDS v4.0), the URL should have /cgi-bin/event-server at the end. For example, `https://www.my-rdep-server.com/cgi-bin/event-server`
Username	Type the username. This username must match the SDEE URL username used to access the SDEE URL. The username can be up to 255 characters in length.
Password	Type the user password. This password must match the SDEE URL password used to access the SDEE URL. The password can be up to 255 characters in length.

Table 51: SDEE Parameters (Continued)

Parameter	Description
Events / Query	Type the maximum number of events to retrieve per query. The valid range is 0 to 501 and the default is 100.
Force Subscription	Select this check box if you want to force a new SDEE subscription. By default, the check box is selected. The check box forces the server to drop the least active connection and accept a new SDEE subscription connection for this log source. Clearing the check box continues with any existing SDEE subscription.
Severity Filter Low	Select this check box if you want to configure the severity level as low. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.
Severity Filter Medium	Select this check box if you want to configure the severity level as medium. Log sources that supports SDEE returns only the events that match this severity level. By default, the check box is selected.
Severity Filter High	Select this check box if you want to configure the severity level as high. Log sources that supports SDEE returns only the events that match this severity level. By default, the check box is selected.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events polled from your Cisco IDS/IPS appliances are displayed on the **Log Activity** tab of SIEM.

Cisco IronPort

The Cisco IronPort DSM for SIEM provides event information for email spam, web content filtering, and corporate email policy enforcement.

Before you configure SIEM to integrate with your Cisco IronPort device, you must select the log type to configure:

- To configure IronPort mail logs, see IronPort Mail Log Configuration on page 139.
- To configure IronPort content filtering logs, see IronPort Web Content Filter on page 141.

IronPort Mail Log Configuration

The SIEM Cisco IronPort DSM accepts events using syslog. To configure your IronPort device to send syslog events to SIEM, you must:

1 Log in to your Cisco IronPort user interface.

2 Select System Administration\Log Subscriptions.

3 Click Add Log Subscription.

4 Configure the following values:

- Log Type - Define a log subscription for both Ironport Text Mail Logs and System Logs.
- Log Name - Type a log name.
- File Name - Use the default configuration value.
- Maximum File Size - Use the default configuration value.
- Log Level - Select Information (Default).
- Retrieval Method - Select Syslog Push.
- Hostname - Type the IP address or server name of your SIEM system.
- Protocol - Select UDP.
- Facility - Use the default configuration value. This value depends on the configured Log Type.

5 Save the subscription.

You are now ready to configure the log source in SIEM.

Configure a Log Source

To integrate Cisco IronPort with SIEM, you must manually create a log source to receive Cisco IronPort events. SIEM does not automatically discover or create log sources for syslog events from Cisco IronPort appliances.

To create a log source for Cisco IronPort events:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Cisco IronPort**.

9 Using the Protocol Configuration list, select **Syslog**.

The syslog protocol configuration is displayed.

10 Configure the following values:

Table 52: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco IronPort appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Cisco IronPort are displayed on the **Log Activity** tab.

IronPort Web Content Filter

The Cisco IronPort DSM for SIEM retrieves web content filtering events in W3C format from a remote source using the log file protocol.

Your system must be running the latest version of log file protocol to integrate with a Cisco IronPort device. To configure your Cisco IronPort device to push web content filter events, you must configure a log subscription for the web content filter using the W3C format. For more information on configuring a log subscription, see your Cisco IronPort documentation.

You are now ready to configure the log source and protocol SIEM.

1 From the **Log Source Type** drop-down list box, select **Cisco IronPort**.

2 From the **Protocol Configuration** list, select **Log File** protocol option.

3 Select **W3C** as the **Event Generator** used to process the web content filter log files.

4 The **FTP File Pattern** parameter must use a regular expression that matches the log files generated by the web content filter logs.

For more information on configuring the Log File protocol, see the *Log Sources User Guide*.

Cisco NAC

The Cisco NAC DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant audit, error, and failure events as well as quarantine and infected system events. Before configuring a Cisco NAC device in SIEM, you must configure your device to forward syslog events.

Configuring Cisco NAC to Forward Events

To configure the device to forward syslog events:

Procedure

1 Log in to the Cisco NAC user interface.

2 In the Monitoring section, select Event Logs.

3 Click the Syslog Settings tab.

4 In the Syslog Server Address field, type the IP address of your SIEM.

5 In the Syslog Server Port field, type the syslog port. The default is 514.

6 In the System Health Log Interval field, type the frequency, in minutes, for system statistic log events.

7 Click Update.

You are now ready to configure the log source in SIEM.

Configuring a Log Source

To integrate Cisco NAC events with SIEM, you must manually create a log source to receive Cisco NAC events. SIEM does not automatically discover or create log sources for syslog events from Cisco NAC appliances.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Cisco NAC Appliance**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 53: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco NAC appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Cisco NAC are displayed on the **Log Activity** tab.

Cisco Nexus

The Cisco Nexus DSM for SIEM supports alerts from Cisco NX-OS devices.

The events are forwarded from Cisco Nexus to SIEM using syslog. Before you can integrate events with SIEM, you must configure your Cisco Nexus device to forward syslog events.

Configure Cisco Nexus to Forward Events

To configure syslog on your Cisco Nexus server:

1 Type the following command to switch to configuration mode:

```
config t
```

2 Type the following commands:

```
logging server <IP address> <severity>
```

Where:

`<IP address>` is the IP address of your SIEM Console.

`<severity>` is the severity level of the event messages, which range from 0-7.

For example, `logging server 100.100.10.1 6` forwards information level (6) syslog messages to 100.100.10.1.

3 Type the following to configure the interface for sending syslog events:

```
logging source-interface loopback
```

4 Type the following command to save your current configuration as the start up configuration:

```
copy running-config startup-config
```

The configuration is complete. The log source is added to SIEM as Cisco Nexus events are automatically discovered. Events forwarded to SIEM by Cisco Nexus are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco Nexus. The following configuration steps are optional.

To manually configure a log source for Cisco Nexus:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Nexus.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 54: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco Nexus appliances.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information on configuring a Virtual Device Context (VDC) on your Cisco Nexus device, see your vendor documentation.

Cisco IOS

You can integrate Cisco IOS series devices with SIEM.

Supported Event Types

The Cisco IOS DSM for SIEM accepts Cisco IOS events using syslog. SIEM records all relevant events. The following Cisco Switches and Routers are automatically discovered as Cisco IOS and have their events parsed by the Cisco IOS DSM:

- Cisco 12000 Series Routers
- Cisco 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Routing System
- Cisco Integrated Services Router.

NOTE

Make sure all Access Control Lists (ACLs) are set to LOG.

Configure Cisco IOS to Forward Events

To configure a Cisco IOS-based device to forward events:

1 Log in to your Cisco IOS Server, switch, or router.

2 Type the following command to log in to the router in privileged-exec.
```
enable
```

3 Type the following command to switch to configuration mode:
```
conf t
```

4 Type the following commands:
```
logging <IP address>
logging source-interface <interface>
```
Where:

`<IP address>` is the IP address hosting SIEM and the SIM components.

`<interface>` is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.

5 Type the following to configure the priority level:
```
logging trap warning
logging console warning
```
Where `warning` is the priority setting for the logs.

6 Configure the syslog facility:
```
logging facility syslog
```

7 Save and exit the file.

8 Copy running-config to startup-config:

```
copy running-config startup-config
```

You are now ready to configure the log source in SIEM.

The configuration is complete. The log source is added to SIEM as Cisco IOS events are automatically discovered. Events forwarded to SIEM by Cisco IOS-based devices are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco IOS. The following configuration steps are optional.

To manually configure a log source for Cisco IOS-based devices:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select one of the following:

- Cisco IOS
- Cisco 12000 Series Routers
- Cisco 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Routing System
- Cisco Integrated Services Router

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 55: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco IOS-based device.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Cisco Pix

You can integrate Cisco Pix security appliances with SIEM.

The Cisco Pix DSM for SIEM accepts Cisco Pix events using syslog. SIEM records all relevant Cisco Pix events.

Configure Cisco Pix to Forward Events

To Configure Cisco Pix:

1 Log in to your Cisco PIX appliance using a console connection, telnet, or SSH.

2 Type the following command to access Privileged mode:
```
enable
```

3 Type the following command to access Configuration mode:
```
conf t
```

4 Enable logging and timestamp the logs:
```
logging on
logging timestamp
```

5 Set the log level:
```
logging trap warning
```

6 Configure logging to SIEM:
```
logging host <interface> <ip address>
```

Where:

`<interface>` is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.

`<ip address>` is the IP address hosting SIEM.

The configuration is complete. The log source is added to SIEM as Cisco Pix Firewall events are automatically discovered. Events forwarded to SIEM by Cisco Pix Firewalls are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco Pix Firewalls. The following configuration steps are optional.

To manually configure a log source for Cisco Pix:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco PIX Firewall.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 56: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco Pix Firewall.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Concentrator DSM for SIEM accepts

Cisco VPN Concentrator events using syslog. SIEM records all relevant events. Before you can integrate with a Cisco VPN concentrator, you must configure your device to forward syslog events to SIEM.

Configure a Cisco VPN 3000 Concentrator

To configure your Cisco VPN 3000 Concentrator:

1 Log in to the Cisco VPN 3000 Concentrator command-line interface (CLI).

2 Type the following command to add a syslog server to your configuration:
`set logging server <IP address>`
Where `<IP address>` is the IP address of SIEM or your Event Collector.

3 Type the following command to enable system message logging to the configured syslog servers:
`set logging server enable`

4 Set the facility and severity level for syslog server messages:
`set logging server facility server_facility_parameter`
`set logging server severity server_severity_level`
The configuration is complete. The log source is added to SIEM as Cisco VPN Concentrator events are automatically discovered. Events forwarded to SIEM are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco VPN 3000 Series Concentrators. These configuration steps are optional.

To manually configure a log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco VPN 3000 Series Concentrator.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 57: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco VPN 3000 Series Concentrators.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Cisco Wireless Services Module

You can integrate a Cisco Wireless Services Module (WiSM) device with SIEM.

A Cisco WiSM DSM for SIEM accepts events using syslog. Before you can integrate SIEM with a Cisco WiSM device, you must configure Cisco WiSM to forward syslog events.

Configure Cisco WiSM to Forward Events

To configure Cisco WiSM to forward syslog events to SIEM:

1 Log in to the Cisco Wireless LAN Controller user interface.

2 Click **Management > Logs > Config**.
The Syslog Configuration window is displayed.

3 In the **Syslog Server IP Address** field type the IP address of the SIEM host to which you want to send the syslog messages. Click **Add**.

4 Using the **Syslog Level** list, set the severity level for filtering syslog messages to the syslog servers using one of the following options:
- **Emergencies** - Severity level 0
- **Alerts** - Severity level 1 (Default)
- **Critical** - Severity level 2
- **Errors** - Severity level 3
- **Warnings** - Severity level 4
- **Notifications** - Severity level 5
- **Informational** - Severity level 6
- **Debugging** - Severity level 7

If you set a syslog level, only those messages whose severity level is equal or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

5 From the **Syslog Facility** list, set the facility for outgoing syslog messages to the syslog server using one of the following options:
- **Kernel** - Facility level 0
- **User Process** - Facility level 1
- **Mail** - Facility level 2
- **System Daemons** - Facility level 3
- **Authorization** - Facility level 4
- **Syslog** - Facility level 5 (default value)
- **Line Printer** - Facility level 6
- **USENET** - Facility level 7
- **Unix-to-Unix Copy** - Facility level 8
- **Cron** - Facility level 9
- **FTP Daemon** - Facility level 11
- **System Use 1** - Facility level 12
- **System Use 2** - Facility level 13

- **System Use 3** - Facility level 14
- **System Use 4** - Facility level 15
- **Local Use 0** - Facility level 16
- **Local Use 1** - Facility level 17
- **Local Use 2** - Facility level 18
- **Local Use 3** - Facility level 19
- **Local Use 4** - Facility level 20
- **Local Use 5** - Facility level 21
- **Local Use 6** - Facility level 22
- **Local Use 7** - Facility level 23

6 Click **Apply**.

7 From the **Buffered Log Level** and the **Console Log Level** listes, select the severity level for log messages to the controller buffer and console using one of the following options:

- **Emergencies** - Severity level 0
- **Alerts** - Severity level 1
- **Critical** - Severity level 2
- **Errors** - Severity level 3 (default value)
- **Warnings** - Severity level 4
- **Notifications** - Severity level 5
- **Informational** - Severity level 6
- **Debugging** - Severity level 7

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

8 Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.

9 Select the **Proc Info** check box if you want the message logs to include process information. The default value is disabled.

10 Select the **Trace Info** check box if you want the message logs to include traceback information. The default value is disabled.

11 Click **Apply** to commit your changes.

12 Click **Save Configuration** to save your changes.

The configuration is complete. The log source is added to SIEM as Cisco WiSM events are automatically discovered. Events forwarded by Cisco WiSM are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cisco WiSM. The following configuration steps are optional.

To manually configure a log source for Cisco WiSM:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Cisco Wireless Services Module (WiSM)**.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 58: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco WiSM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Cisco Wireless LAN Controllers

The Cisco Wireless LAN Controllers DSM for SIEM collects events forwarded from Cisco Wireless LAN Controller devices using syslog or SNMPv2.

This section includes the following topics:

Before You Begin

If you collect events from Cisco Wireless LAN Controllers, you should select the best collection method for your configuration. The Cisco Wireless LAN Controller DSM for SIEM supports both syslog and SNMPv2 events. However, syslog provides all available Cisco Wireless LAN Controller events, where SNMPv2 only sends a limited set of security events to SIEM.

Configuring Syslog for Cisco Wireless LAN Controller

You can configure Cisco Wireless LAN Controller for forward syslog events to SIEM.

Procedure

1 Log in to your Cisco Wireless LAN Controller interface.

2 Click the **Management** tab.

3 From the menu, select **Logs > Config**.

4 In the **Syslog Server IP Address** field, type the IP address of your SIEM Console.

5 Click **Add**.

6 From the **Syslog Level** list, select a logging level.

The Information level allows you to collect all Cisco Wireless LAN Controller events above the debug level.

7 From the **Syslog Facility** list, select a facility level.

8 Click **Apply**

9 Click **Save Configuration**.

What to do next

You are now ready to configure a syslog log source for Cisco Wireless LAN Controller.

Configuring a Syslog Log Source in SIEM

SIEM does not automatically discover incoming syslog events from Cisco Wireless LAN Controllers. You must create a log source for each Cisco Wireless LAN Controller providing syslog events to SIEM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Wireless LAN Controllers.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 59: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco Wireless LAN Controller.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** drop-down in the SIEM Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *SIEM Administration Guide*.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.

Table 59: Syslog protocol parameters (Continued)

Parameter	Description
Store Event Payload	Select this check box to enable or disable SIEM from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** drop-down in the SIEM Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Configuring SNMPv2 for Cisco Wireless LAN Controller

SNMP event collection for Cisco Wireless LAN Controllers allows you to capture the following events for SIEM:

- SNMP Config Event
- bsn Authentication Errors
- LWAPP Key Decryption Errors

Procedure

1 Log in to your Cisco Wireless LAN Controller interface.

2 Click the **Management** tab.

3 From the menu, select **SNMP > Communities**.

You can use the one of the default communities created or create a new community.

4 Click **New**.

5 In the **Community Name** field, type the name of the community for your device.

6 In the **IP Address** field, type the IP address of SIEM.

The IP address and IP mask you specify is the address from which your Cisco Wireless LAN Controller accepts SNMP requests. You can treat these values as an access list for SNMP requests.

7 In the **IP Mask** field, type a subnet mask.

8 From the **Access Mode** list, select **Read Only** or **Read/Write**.

9 From the **Status** list, select **Enable**.

10 Click **Save Configuration** to save your changes.

What to do next

You are now ready to create a SNMPv2 trap receiver.

Configure a Trap Receiver for Cisco Wireless LAN Controller

Trap receivers configured for Cisco Wireless LAN Controllers define where the device can send SNMP trap messages.

Procedure

1 Click the **Management** tab.

2 From the menu, select **SNMP > Trap Receivers**.

3 In the **Trap Receiver Name** field, type a name for your trap receiver.

4 In the **IP Address** field, type the IP address of SIEM.

The IP address you specify is the address to which your Cisco Wireless LAN Controller sends SNMP messages. If you plan to configure this log source on an Event Collector, you want to specify the Event Collector appliance IP address.

5 From the **Status** list, select **Enable**.

6 Click **Apply** to commit your changes.

7 Click **Save Configuration** to save your settings.

What to do next

You are now ready to create a SNMPv2 log source in SIEM.

Configure a Log Source for SNMPv2 for Cisco Wireless LAN Controller

SIEM does not automatically discover and create log sources for SNMP event data from Cisco Wireless LAN Controllers. You must create a log source for each Cisco Wireless LAN Controller providing SNMPv2 events.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cisco Wireless LAN Controllers.

9 Using the Protocol Configuration list, select **SNMPv2**.

10 Configure the following values:

Table 60: SNMPv2 protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cisco Wireless LAN Controller.

Table 60: SNMPv2 protocol parameters (Continued)

Parameter	Description
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Select the **Include OIDs in Event Payload** check box. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** drop-down in the SIEM Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *SIEM Administration Guide*.
Store Event Payload	Select this check box to enable or disable SIEM from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** drop-down in the SIEM Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. Events forwarded to by Cisco Wireless LAN Controller are displayed on the **Log Activity** tab of SIEM.

Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) DSM for SIEM accepts syslog events from Cisco ISE appliances with log sources configured to use the UDP Multiline protocol.

Configuration Overview

SIEM supports syslog events forwarded by Cisco ISE versions 1.1. Before you configure your Cisco ISE appliance, you should consider which logging categories you want to configure on your Cisco ISE to forward to SIEM. Each logging category must be configured with a syslog severity and included as a remote target to allow Cisco ISE to forward the event to SIEM. The log source you configure in SIEM receives the event forwarded from Cisco ISE and uses a regular expression to assemble the multiline syslog event in to an event readable by SIEM.

To integrate Cisco ISE events with SIEM, you must perform the following tasks:

1 Configure a log source in SIEM for your Cisco ISE appliance forwarding events to SIEM.

2 Create a remote logging target for SIEM on your Cisco ISE appliance.

3 Configure the logging categories on your Cisco ISE appliance.

Supported Event Logging Categories

The Cisco ISE DSM for SIEM is capable of receiving syslog events from the following event logging categories.

Table 61: Supported Cisco ISE event logging categories

Event logging category
AAA audit
Failed attempts
Passed authentication
AAA diagnostics
Administrator authentication and authorization
Authentication flow diagnostics
Identity store diagnostics
Policy diagnostics
Radius diagnostics
Guest
Accounting
Radius accounting
Administrative and operational audit
Posture and client provisioning audit
Posture and client provisioning diagnostics
Profiler
System diagnostics

Table 61: Supported Cisco ISE event logging categories (Continued)

Event logging category
Distributed management
Internal operations diagnostics
System statistics

Configuring a Cisco ISE Log Source in SIEM

To collect syslog events, you must configure a log source for Cisco ISE in SIEM to use the UDP Multiline Syslog protocol.

You must configure a log source for each individual Cisco ISE appliance that forwards events to SIEM. However, all Cisco ISE appliances can forward their events to the same listen port on SIEM that you configure.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Cisco Identity Services Engine**.

9 From the **Protocol Configuration** list, select **UDP Multiline Syslog**.

10 Configure the following values:

Table 62: Cisco ISE log source parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name to identify the log source or appliance providing UDP Multiline Syslog events to SIEM.
Listen Port	Type **517** as the port number used by SIEM to accept incoming UDP Multiline Syslog events. The valid port range is 1 to 65535. To edit a saved configuration to use a new port number: **1** In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. **2** Click **Save**. **3** On the **Admin** tab, select **Advanced > Deploy Full Configuration**. After the full deploy completes, SIEM is capable of receiving events on the updated listen port. **NOTE:** When you click Deploy Full Configuration, SIEM restarts all services, resulting in a gap in data collection for events and flows until the deployment completes.

Table 62: Cisco ISE log source parameters (Continued)

Parameter	Description
Message ID Pattern	Type the following regular expression (regex) required to filter the event payload messages. `CISE_\S+ (\d{10})`

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

What to do next

You are now ready to configure your Cisco ISE appliance with a remote logging target.

Creating a Remote Logging Target in Cisco ISE

To forward syslog events to SIEM, you must configure your Cisco ISE appliance with a remote logging target.

Procedure

1 Log in to your Cisco ISE Administration Interface.

2 From the navigation menu, select **Administration > System > Logging > Remote Logging Targets**.

3 Click **Add**.

4 In the **Name** field, type a name for the remote target system.

5 In the **Description** field, type a description.

6 In the **IP Address** field, type a the IP address of the SIEM Console or Event Collector.

7 In the **Port** field, type **517** or use the port value you specific in your Cisco ISE log source for SIEM.

8 From the **Facility Code** list, select the syslog facility to use for logging events.

9 In the **Maximum Length** field, type **1024** as the maximum packet length allowed for the UDP syslog message.

10 Click **Submit**.

The remote logging target is created for SIEM.

What to do next

You are now ready to configure the logging categories forwarded by Cisco ISE to SIEM.

Configuring Cisco ISE Logging Categories

To define which events are forwarded by your Cisco ISE appliance, you must configure each logging category with a syslog severity and the remote logging target your configured for SIEM.

For a list of pre-defined event logging categories for Cisco ISE, see Supported Event Logging Categories on page 158.

Procedure

1. From the navigation menu, select **Administration > System > Logging > Logging Categories**.
2. Select a logging category, and click **Edit**.
3. From the **Log Severity** list, select a severity for the logging category.
4. In the **Target** field, add your remote logging target for SIEM to the **Select** box.
5. Click **Save**.
6. Repeat this process for each logging category you want to forward to SIEM.

   The configuration is complete. Events forwarded by Cisco ISE are displayed on the **Log Activity** tab in SIEM.

29 Citrix

This section provides information on the following DSMs:

Citrix NetScaler

The Citrix NetScaler DSM for SIEM accepts all relevant audit log events using syslog.

Configuring Syslog on Citrix NetScaler

To integrate Citrix NetScaler events with SIEM, you must configure Citrix NetScaler to forward syslog events.

Procedure

1 Using SSH, log in to your Citrix NetScaler device as a root user.

2 Type the following command to add a remote syslog server:

```
add audit syslogAction <ActionName> <IP Address> -serverPort 514
-logLevel Info -dateFormat DDMMYYYY
```

Where:

`<ActionName>` is a descriptive name for the syslog server action.

`<IP Address>` is the IP address or hostname of your SIEM Console.

For example:

```
add audit syslogAction action-SIEM 10.10.10.10 -serverPort 514 -
logLevel Info -dateFormat DDMMYYYY
```

3 Type the following command to add an audit policy:

```
add audit syslogPolicy <PolicyName> <Rule> <ActionName>
```

Where:

`<PolicyName>` is a descriptive name for the syslog policy.

`<Rule>` is the rule or expression the policy uses. The only supported value is `ns_true`.

`<ActionName>` is a descriptive name for the syslog server action.

For example:

```
add audit syslogPolicy policy-SIEM ns_true action-SIEM
```

4 Type the following command to bind the policy globally:

```
bind system global <PolicyName> -priority <Integer>
```

Where:

`<PolicyName>` is a descriptive name for the syslog policy.

`<Integer>` is a numeric value used to rank message priority for multiple policies that are communicating using syslog.

For example:

```
bind system global policy-SIEM -priority 30
```

When multiple policies have priority assigned to them as a numeric value the lower priority value is evaluated before the higher value.

5 Type the following command to save the Citrix NetScaler configuration.

```
save config
```

6 Type the following command to verify the policy is saved in your configuration:

```
sh system global
```

NOTE

For information on configuring syslog using the Citrix NetScaler user interface, see http://support.citrix.com/article/CTX121728 or your vendor documentation.

The configuration is complete. The log source is added to SIEM as Citrix NetScaler events are automatically discovered. Events forwarded by Citrix NetScaler are displayed on the **Log Activity** tab of SIEM.

Configuring a Citrix NetScaler Log Source

SIEM automatically discovers and creates a log source for syslog events from Citrix NetScaler. This procedure is optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Citrix NetScaler.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 63: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Citrix NetScaler devices.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Citrix Access Gateway

The Citrix Access Gateway DSM accepts access, audit, and diagnostic events forwarded from your Citrix Access Gateway appliance using syslog.

Configuring Syslog for Citrix Access Gateway

This procedure outlines the configure steps required to configure syslog on your Citrix Access Gateway to forward events to the SIEM Console or an Event Collectors.

Procedure

1. Log in to your Citrix Access Gateway web interface.
2. Click the **Access Gateway Cluster** tab.
3. Select **Logging/Settings**.
4. In the **Server** field, type the IP address of your SIEM Console or Event Collector.
5. From the **Facility** list, select a syslog facility level.
6. In the **Broadcast interval (mins)**, type **0** to continuously forward syslog events to SIEM.
7. Click **Submit** to save your changes.

   The configuration is complete. The log source is added to SIEM as Citrix Access Gateway events are automatically discovered. Events forwarded to SIEM by Citrix Access Gateway are displayed on the **Log Activity** tab in SIEM.

Configuring a Citrix Access Gateway Log Source

SIEM automatically discovers and creates a log source for syslog events from Citrix Access Gateway appliances. This procedure is optional.

Procedure

1. Log in to SIEM.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the Log Sources icon.
5. Click Add.
6. In the **Log Source Name** field, type a name for your log source.
7. In the **Log Source Description** field, type a description for the log source.
8. From the Log Source Type list, select Citrix Access Gateway.
9. Using the Protocol Configuration list, select **Syslog**.
10. Configure the following values:

Table 64: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Citrix Access Gateway appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

30 CloudPassage Halo

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

31 Correlog Agent for IBM zOS

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

32 CRYPTOCard CRYPTO-Shield

The SIEM CRYPTOCard CRYPTO-Shield DSM for SIEM accepts events using syslog.

Before You Begin

To integrate CRYPTOCard CRYPTO-Shield events with SIEM, you must manually create a log source to receive syslog events.

Before you can receive events in SIEM, you must configure a log source, then configure your CRYPTOCard CRYPTO-Shield to forward syslog events. Syslog events forwarded from CRYPTOCard CRYPTO-Shield devices are not automatically discovered. SIEM can receive syslog events on port 514 for both TCP and UDP.

Configuring a Log Source

SIEM does not automatically discover or create log sources for syslog events from CRYPTOCard CRYPTO-Shield devices.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select CRYPTOCard CRYPTOShield.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 65: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CRYPTOCard CRYPTO-Shield device.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM.

Configure Syslog for CRYPTOCard CRYPTO-Shield

To configure your CRYPTOCard CRYPTO-Shield device to forward syslog events:

1 Log in to your CRYPTOCard CRYPTO-Shield device.

2 Configure the following System Configuration parameters:

NOTE

You must have CRYPTOCard Operator access with the assigned default Super-Operator system role to access the System Configuration parameters.

- `log4j.appender.<protocol>` - Directs the logs to a syslog host where the `<protocol>` is the type of log appender, which determines where you want to send logs for storage. The options are: ACC, DBG, or LOG. For this parameter, type the following: `org.apache.log4j.net.SyslogAppender`
- `log4j.appender.<protocol>.SyslogHost <IP address>` - Type the IP address or hostname of the syslog server where:
  - `<protocol>` is the type of log appender, which determines where you want to send logs for storage. The options are: ACC, DBG, or LOG.
  - `<IP address>` is the IP address of the SIEM host to which you want to send logs. This value can only be specified when the first parameter is configured.

    This parameter can only be specified when the log4j.apender.<protocol> parameter is configured.

  The configuration is complete. Events forwarded to SIEM by CRYPTOCard CRYPTO-Shield are displayed on the **Log Activity** tab.

33 Cyber-Ark Vault

The Cyber-Ark Vault DSM for SIEM accepts events using syslog formatted for Log Enhanced Event Format (LEEF).

Supported Event Types

SIEM records both user activities and safe activities from the Cyber-Ark Vault in the audit log events. Cyber-Ark Vault integrates with SIEM to forward audit logs using syslog to create a complete audit picture of privileged account activities.

Event Type Format

Cyber-Ark Vault must be configured to generate events in Log Enhanced Event Protocol (LEEF) and forward these events using syslog. The LEEF format consists of a pipe (|) delimited syslog header and tab separated fields in the event payload.

If the syslog events forwarded from your Cyber-Ark Vault is not formatted as described above, you must examine your device configuration or software version to ensure your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to SIEM.

Configure Syslog for Cyber-Ark Vault

To configure Cyber-Ark Vault to forward syslog events to SIEM:

Procedure

1 Log in to your Cyber-Ark device.

2 Edit the DBParm.ini file.

3 Configure the following parameters:

- SyslogServerIP - Type the IP address of SIEM.
- SyslogServerPort - Type the UDP port used to connect to SIEM. The default value is 514.
- SyslogMessageCodeFilter - Configure which message codes are sent from the Cyber-Ark Vault to SIEM. You can define specific message numbers or a range of numbers. By default, all message codes are sent for user activities and safe activities.

  For example, to define a message code of 1,2,3,30 and 5-10, you must type: `1,2,3,5-10,30.`
- SyslogTranslatorFile - Type the file path to the LEEF.xsl translator file. The translator file is used to parse Cyber-Ark audit records data in the syslog protocol.

4 Copy LEEF.xsl to the location specified by the SyslogTranslatorFile parameter in the DBParm.ini file.

The configuration is complete. The log source is added to SIEM as Cyber-Ark Vault events are automatically discovered. Events forwarded by Cyber-Ark Vault are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Cyber-Ark Vault. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Cyber-Ark Vault.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 66: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Cyber-Ark Vault appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

34 CyberGuard Firewall/VPN Appliance

The CyberGuard Firewall VPN Appliance DSM for SIEM accepts CyberGuard events using syslog.

Supported Event Types

SIEM records all relevant CyberGuard events for CyberGuard KS series appliances forwarded using syslog.

Configure Syslog Events

To configure a CyberGuard device to forward syslog events:

Procedure

1 Log in to the CyberGuard user interface.

2 Select the Advanced page.

3 Under System Log, select Enable Remote Logging.

4 Type the IP address of SIEM.

5 Click Apply.

The configuration is complete. The log source is added to SIEM as CyberGuard events are automatically discovered. Events forwarded by CyberGuard appliances are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from CyberGuard appliances. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **CyberGuard TSP Firewall/VPN**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 67: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CyberGuard appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

35 Damballa Failsafe

The Failsafe DSM for SIEM accepts syslog events using the Log Enhanced Event Protocol (LEEF), enabling SIEM to record all relevant Damballa Failsafe events.

Event Type Format

Damballa Failsafe must be configured to generate events in Log Enhanced Event Protocol (LEEF) and forward these events using syslog. The LEEF format consists of a pipe (|) delimited syslog header and tab separated fields in the event payload.

If the syslog events forwarded from your Damballa Failsafe is not formatted as described above, you must examine your device configuration or software version to ensure your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to SIEM.

Configuring Syslog for Damballa Failsafe

To collect events, you must configure your Damballa Failsafe device to forward syslog events to SIEM.

Procedure

1 Log in to your Damballa Failsafe Management Console

2 From the navigation menu, select **Setup > Integration Settings**.

3 Click the **Q1 SIEM** tab.

4 Select **Enable Publishing to Q1 SIEM**.

5 Configure the following options:
   a **Q1 Hostname** - Type the IP address or Fully Qualified Name (FQN) of your SIEM Console.
   b **Destination Port** - Type **514**. By default, SIEM uses port 514 as the port for receiving syslog events.
   c **Source Port** - Optional. Type the source port your Damballa Failsafe device uses for sending syslog events.

6 Click **Save**.

   The configuration is complete. The log source is added to SIEM as Damballa Failsafe events are automatically discovered. Events forwarded by Damballa Failsafe are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Damballa Failsafe devices. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Damballa Failsafe**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 68: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Damballa Failsafe devices.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

36 DG Technology MEAS

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

37 Digital China Networks (DCN)

The Digital China Networks (DCN) DCS/DCRS Series DSM for SIEM can accept events from Digital China Networks (DCN) switches using syslog.

Supported Event Types

SIEM records all relevant IPv4 events forwarded from DCN switches. To integrate your device with SIEM, you must configure a log source, then configure your DCS or DCRS switch to forward syslog events.

Supported Appliances

The DSM supports the following DCN DCS/DCRS Series switches:

- DCS - 3650
- DCS - 3950
- DCS - 4500
- DCRS - 5750
- DCRS - 5960
- DCRS - 5980
- DCRS - 7500
- DCRS - 9800

Configuring a Log Source

SIEM does not automatically discover incoming syslog events from DCN DCS/DCRS Series switches.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **DCN DCS/DCRS Series**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following value:

Table 69: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address, hostname, or name for the log source as an identifier for your DCN DCS/DCRS Series switch. Each log source you create for your DCN DCS/DCRS Series switch should include a unique identifier, such as an IP address or hostname.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to configure your Digital China Networks DCS or DCRS Series switch to forward events to SIEM.

Configure a DCN DCS/DCRS Series Switch

To collect events, you must configure your DCN DCS/DCRS Series switch in SIEM.

Procedure

1 Log in to your DCN DCS/DCRS Series switch command-line Interface (CLI).

2 Type the following command to access the administrative mode:
`enable`

3 Type the following command to access the global configuration mode:
`config`
The command-line interface displays the configuration mode prompt:
`Switch(Config)#`

4 Type the following command to configure a log host for your switch:
`logging <IP address> facility <local> severity <level>`
Where:
`<IP address>` is the IP address of the SIEM Console.
`<local>` is the syslog facility, for example, local0.
`<level>` is the severity of the syslog events, for example, informational. If you specify a value of informational, you forward all information level events and later, such as, notifications, warnings, errors, critical, alerts, and emergencies.
For example,
`logging 10.10.10.1 facility local0 severity informational`

5 Type the following command to save your configuration changes:
`write`
The configuration is complete. You can verify events forwarded to SIEM by viewing events in the **Log Activity** tab.

38 Extreme Networks

This section provides information on the following DSMs:

Extreme Dragon

The Extreme Dragon DSM for SIEM accepts Extreme events using either syslog or SNMPv3 to record all relevant Extreme Dragon events.

To configure your SIEM Extreme Dragon DSM, you must:

1 Choose one of the following:
   a Create an Alarm Tool policy using an SNMPv3 notification rule. See Create an Alarm Tool Policy for SNMPv3 on page 179.
   b Create an Alarm Tool policy using a Syslog notification rule. See Create a Policy for Syslog on page 181.

2 Configure the log source within SIEM. See Configure a Log Source on page 183.

3 Configure Dragon Enterprise Management Server (EMS) to forward syslog messages. See Configure the EMS to Forward Syslog Messages on page 184

Create an Alarm Tool Policy for SNMPv3

This procedure describes how to configure an Alarm Tool policy using an SNMPv3 notification rule. Use SNMPv3 notification rules if you need to transfer PDATA binary data elements.

To configure Extreme Dragon with an Alarm Tool policy using an SNMPv3 notification rule:

1 Log in to the Extreme Dragon EMS.

2 Click the Alarm Tool icon.

3 Configure the Alarm Tool Policy:
   a In the **Alarm Tool Policy View > Custom Policies** menu tree, right-click and select Add Alarm Tool Policy.

   The Add Alarm Tool Policy window is displayed.

b In the Add Alarm Tool Policy field, type a policy name.

For example:

SIEM

c Click OK.

d In the menu tree, select the policy name you entered from Step b.

4 To configure the event group:

a Click the Events Group tab.

b Click New.

The Event Group Editor is displayed.

c Select the event group or individual events to monitor.

d Click **Add**.

A prompt is displayed.

e Click Yes.

f In the right column of the Event Group Editor, type `Dragon-Events`.

g Click OK.

5 Configure the SNMPv3 notification rules:

a Click the Notification Rules tab.

b Click New.

c In the name field, type `SIEM-Rule`.

d Click OK.

e In the Notification Rules panel, select **SIEM**-Rule.

f Click the **SNMP V3** tab.

g Click **New**.

h Update SNMP V3 values, as required:

- Server IP Address - Type the SIEM IP address.

NOTE

Do not change the OID.

- Inform - Select the Inform check box.
- Security Name - Type the SNMPv3 username.
- Auth Password - Type the appropriate password.
- Priv Password - Type the appropriate password.
- Message - Type the following on one line:

```
Dragon Event: %DATE%,,%TIME%,,%NAME%,,%SENSOR%,,%PROTO%,,%SIP%,,
%DIP%,,%SPORT%,,%DPORT%,, %DIR%,,%DATA%,,<<<%PDATA%>>>
```

NOTE

Verify that the security passwords and protocols match data configured in the SNMP configuration.

i Click **OK**.

6 Verify that the notification events are logged as separate events:
   a Click the **Global Options** tab.
   b Click the **Main** tab.
   c Make sure that **Concatenate Events** is not selected.

7 Configure the SNMP options:
   a Click the Global Options tab.
   b Click the SNMP tab
   c Type the IP address of the EMS server sending SNMP traps.

8 Configure the alarm information:
   a Click the Alarms tab.
   b Click New.
   c Type values for the following parameters:
      - Name - Type `SIEM-Alarm`.
      - Type - Select Real Time.
      - Event Group - Select Dragon-Events.
      - Notification Rule - Select the SIEM-Rule check box.
   d Click OK.
   e Click Commit.

9 Navigate to the Enterprise View.

10 Right-click on the Alarm Tool and select Associate Alarm Tool Policy.

11 Select the SIEM policy. Click OK.

12 From the Enterprise menu, right-click and select Deploy.
   You are now ready to configure the log source SNMP protocol in SIEM.

Create a Policy for Syslog

This procedure describes how to configure an Alarm Tool policy using a syslog notification rule in the Log Event Extended Format (LEEF) message format.

LEEF is the preferred message format for sending notifications to Dragon Network Defense when the notification rate is very high or when IPv6 addresses are displayed. If you prefer not to use syslog notifications in LEEF format, refer to your *Extreme Dragon documentation* for more information.

NOTE

Use SNMPv3 notification rules if you need to transfer PDATA, which is a binary data element. Do not use a syslog notification rule.

To configure Extreme Dragon with an Alarm Tool policy using a syslog notification rule:

1 Log in to the Extreme Dragon EMS.

2 Click the Alarm Tool icon.

3 Configure the Alarm Tool Policy:

a In the **Alarm Tool Policy View > Custom Policies** menu tree, right-click and select Add Alarm Tool Policy.

The Add Alarm Tool Policy window is displayed.

b In the Add Alarm Tool Policy field, type a policy name.

For example:

`SIEM`

c Click OK.

d In the menu tree, select **SIEM**.

4 To configure the event group:

a Click the Events Group tab.

b Click New.

The Event Group Editor is displayed.

c Select the event group or individual events to monitor.

d Click **Add**.

A prompt is displayed.

e Click Yes.

f In the right column of the Event Group Editor, type `Dragon-Events`.

g Click OK.

5 Configure the Syslog notification rule:

a Click the Notification Rules tab.

b Click New.

c In the name field, type `SIEM-RuleSys`.

d Click OK.

e In the Notification Rules panel, select the newly created **SIEM**-RuleSys item.

f Click the **Syslog** tab.

g Click **New**.

The Syslog Editor is displayed.

h Update the following values:

- **Facility** - Using the Facility list, select a facility.
- **Level** - Using the Level list, select notice.
- **Message** - Using the Type list, select LEEF.

```
LEEF:Version=1.0|Vendor|Product|ProductVersion|eventID|devTime|
proto|src|sensor|dst|srcPort|dstPort|direction|eventData|
```

NOTE

The LEEF message format delineates between fields using a pipe delimiter between each keyword.

i Click **OK**.

6 Verify that the notification events are logged as separate events:

a Click the **Global Options** tab.

b Click the **Main** tab.

c Make sure that **Concatenate Events** is not selected.

7 Configure the alarm information:
   a Click the Alarms tab.
   b Click New.
      - Type values for the parameters:
      - Name - Type `SIEM-Alarm`.
      - Type - Select Real Time.
      - Event Group - Select Dragon-Events.
      - Notification Rule - Select the SIEM-RuleSys check box.
   c Click OK.
   d Click Commit.
8 Navigate to the Enterprise View.
9 Right-click on the **Alarm Tool** and select Associate Alarm Tool Policy.
10 Select the newly created SIEM policy. Click OK.
11 In the Enterprise menu, right-click the policy and select Deploy.
   You are now ready to configure a syslog log source in SIEM.

Configure a Log Source

You are now ready to configure the log source in SIEM:

1 Log in to SIEM.
2 Click the **Admin** tab.
3 On the navigation menu, click **Data Sources**.
4 Click the Log Sources icon.
5 Click Add.
6 In the **Log Source Name** field, type a name for your log source.
7 In the **Log Source Description** field, type a description for the log source.
8 From the Log Source Type list, select Extreme Dragon Network IPS.
9 From the **Protocol Configuration** list, select either the SNMPv3 or Syslog option. For more information on configuring a specific protocol, see the *SIEM Log Sources User Guide*.

For more information about Extreme Dragon device, see your Extreme Dragon documentation.

NOTE

Using the event mapping tool in the **Log Activity** tab, you can map a normalized or raw event to a high-level and low-level category (or QID). However, you cannot map combination Dragon messages using the event mapping tool. For more information, see the *SIEM Users Guide*.

Configure the EMS to Forward Syslog Messages

Starting with Dragon Enterprise Management Server (EMS) v7.4.0 appliances, you must use syslog-ng for forwarding events to a Security and Information Manager such as SIEM.

Syslogd has been replaced by syslog-ng in Dragon EMS v7.4.0 and later.

To configure EMS to forward syslog messages, you must choose one of the following:

- If you are using syslog-ng and Extreme Dragon EMS v7.4.0 and later, see Configuring Syslog-ng Using Extreme Dragon EMS v7.4.0 and Later on page 184.
- If you are using syslogd and Extreme Dragon EMS v7.4.0 and below, see Configuring Syslogd Using Extreme Dragon EMS v7.4.0 and Below on page 185.

Configuring Syslog-ng Using Extreme Dragon EMS v7.4.0 and Later

This section describes the steps to configure syslog-ng in non-encrypted mode and syslogd to forward syslog messages to SIEM.

If you are using encrypted syslog-ng, refer to your Extreme documentation.

Do not run both syslog-ng and syslogd at the same time.

To configure syslog-ng in non-encrypted mode:

1 On your EMS system, open the following file:
```
/opt/syslog-ng/etc/syslog-ng.conf
```

2 Configure a Facility filter for the Syslog notification rule.

For example, if you selected facility local1:
```
filter filt_facility_local1 {facility(local1); };
```

3 Configure a Level filter for the Syslog notification rule.

For example, if you selected level notice:
```
filter filt_level_notice {level(notice); };
```

4 Configure a destination statement for the SIEM.

For example, if the IP address of the SIEM is 10.10.1.1 and you want to use syslog port of 514, type:
```
destination siem { tcp("10.10.1.1" port(514)); };
```

5 Add a log statement for the notification rule:
```
log {
source(s_local);
filter (filt_facility_local1); filter (filt_level_notice);
destination(siem);
};
```

6 Save the file and restart syslog-ng.
```
cd /etc/rc.d
./rc.syslog-ng stop
./rc.syslog-ng start
```

7 The Extreme Dragon EMS configuration is complete.

Configuring Syslogd Using Extreme Dragon EMS v7.4.0 and Below

If your Dragon Enterprise Management Server (EMS) is using a version earlier than v7.4.0 on the appliance, you must use syslogd for forwarding events to a Security and Information Manager such as SIEM.

To configure syslogd, you must:

1 On the Dragon EMS system, open the following file:
`/etc/syslog.conf`

2 Add a line to forward the facility and level you configured in the syslog notification rule to SIEM.

For example, to define the local1 facility and notice level:
`local1.notice @<IP address>`

Where:

`<IP address>` is the IP address of the SIEM system.

3 Save the file and restart syslogd.

```
cd /etc/rc.d
./rc.syslog stop
./rc.syslog start
```

The Extreme Dragon EMS configuration is complete.

Extreme HiGuard Wireless IPS

The Extreme HiGuard Wireless IPS DSM for SIEM records all relevant events using syslog

Before configuring the Extreme HiGuard Wireless IPS device in SIEM, you must configure your device to forward syslog events.

Configure Extreme HiGuard

To configure the device to forward syslog events:

1 Log in to the HiGuard Wireless IPS user interface.

2 In the left navigation pane, click Syslog, which allows the management server to send events to designated syslog receivers.

The Syslog Configuration panel is displayed.

3 In the System Integration Status section, enable syslog integration.

This allows the management server to send messages to the configured syslog servers. By default, the management server enables syslog.

The Current Status field displays the status of the syslog server. The options are: Running or Stopped. An error status is displayed if one of the following occurs:

- One of the configured and enabled syslog servers includes a hostname that cannot be resolved.
- The management server is stopped.
- An internal error has occurred. If this occurs, please contact Extreme Technical Support.

4 From **Manage Syslog Servers**, click Add.

The Syslog Configuration window is displayed.

5 Type values for the following parameters:

- **Syslog Server (IP Address/Hostname)** - Type the IP address or hostname of the syslog server to which events should be sent.

NOTE

Configured syslog servers use the DNS names and DNS suffixes configured in the Server initialization and Setup Wizard on the HWMH Config Shell.

- **Port Number** - Type the port number of the syslog server to which HWMH sends events. The default is 514.
- **Message Format** - Select **Plain Text** as the format for sending events.
- **Enabled?** - Select if the events are to be sent to this syslog server.

6 Save your configuration.

The configuration is complete. The log source is added to SIEM as HiGuard events are automatically discovered. Events forwarded to SIEM by Extreme HiGuard are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Extreme HiGuard. The following configuration steps are optional.

To manually configure a log source for Extreme HiGuard:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Extreme HiGuard.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 70: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme HiGuard.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Extreme HiPath Wireless Controller

The Extreme HiPath Wireless Controller DSM for SIEM records all relevant events using syslog.

Supported Event Types

SIEM supports the following Extreme HiPath Wireless Controller events:

- Wireless access point events
- Application log events
- Service log events
- Audit log events

Configure Your HiPath Wireless Controller

To integrate your Extreme HiPath Wireless Controller events with SIEM, you must configure your device to forward syslog events.

To forward syslog events to SIEM:

1 Log in to the HiPath Wireless Assistant.

2 Click Wireless Controller Configuration.
The HiPath Wireless Controller Configuration window is displayed.

3 From the menu, click System Maintenance.

4 From the Syslog section, select the Syslog Server IP check box and type the IP address of the device receiving the syslog messages.

5 Using the Wireless Controller Log Level list, select Information.

6 Using the Wireless AP Log Level list, select Major.

7 Using the Application Logs list, select local.0.

8 Using the Service Logs list, select local.3.

9 Using the Audit Logs list, select local.6.

10 Click Apply.
You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Extreme HiPath. The following configuration steps are optional.

To manually configure a log source for Extreme HiPath:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Extreme HiPath.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 71: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme HiPath.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information about your Extreme HiPath Wireless Controller device, see your vendor documentation.

Extreme Stackable and Standalone Switches

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

Extreme XSR Security Router

The Extreme XSR Security Router DSM for SIEM accepts events using syslog.

SIEM records all relevant events. Before configuring an Extreme XSR Security Router in SIEM, you must configure your device to forward syslog events.

To configure the device to send syslog events to SIEM:

1 Using Telnet or SSH, log in to the XSR Security Router command-line interface.

2 Type the following command to access config mode:

```
enable
config
```

3 Type the following command:

```
logging <IP address> low
```

Where `<IP address>` is the IP address of your SIEM.

4 Exit from config mode.

5 Save the configuration:

```
exit
copy running-config startup-config
```

6 You are now ready to configure the log sources in SIEM.

To configure SIEM to receive events from an Extreme XSR Security Router:

u From the **Log Source Type** list, select **Extreme XSR Security Routers.**

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

For more information about your Extreme XSR Security Router, see your vendor documentation.

Extreme Matrix Router

The Extreme Matrix Router DSM for SIEM accepts Extreme Matrix events using SNMPv1, SNMPv2, SNMPv3, and syslog.

You can integrate Extreme Matrix Router version 3.5 with SIEM. SIEM records all SNMP events and syslog login, logout, and login failed events. Before you configure SIEM to integrate with Extreme Matrix, you must:

1 Log in to the switch/router as a privileged user.

2 Type the following command:

```
set logging server <server number> description <description>
facility <facility> ip_addr <ip address> port <port> severity
<severity>
```

Where:

`<server number>` is the server number 1 to 8.

`<description>` is a description of the server.

`<facility>` is a syslog facility, for example, local0.

`<ip address>` is the IP address of the server you wish to send syslog messages.

`<port>` is the default UDP port that the client uses to send messages to the server. Use port 514 unless otherwise stated.

`<severity>` is the server severity level 1 to 9 where 1 indicates an emergency and 8 is debug level.

For example:

```
set logging server 5 description ourlogserver facility local0
ip_addr 1.2.3.4 port 514 severity 8
```

3 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from an Extreme Matrix device:

u From the **Log Source Type** list, select **Extreme Matrix E1 Switch.**

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Extreme NetSight Automatic Security Manager

The Extreme NetSight Automatic Security Manager DSM for SIEM accepts events using syslog.

SIEM records all relevant events. Before configuring an Extreme NetSight Automatic Security Manager device in SIEM, you must configure your device to forward syslog events.

To configure the device to send syslog events to SIEM:

1 Log in to the Automatic Security Manager user interface.

2 Click the Automated Security Manager icon to access the Automated Security Manager Configuration window.

NOTE

You can also access the Automated Security Manager Configuration window from the Tool menu.

3 From the left navigation menu, select Rule Definitions.

4 Choose one of the following options:
   a If a rule is currently configured, highlight the rule. Click Edit.
   b To create a new rule, click Create.

5 Select the Notifications check box.

6 Click Edit.

   The Edit Notifications window is displayed.

7 Click Create.
The Create Notification window is displayed.

8 Using the Type list, select Syslog.

9 In the **Syslog Server IP/Name** field, type the IP address of the device that will receive syslog traffic.

10 Click Apply.

11 Click Close.

12 In the Notification list, select the notification configured above.

13 Click OK.

14 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from an Extreme NetSight Automatic Security Manager device:

u From the **Log Source Type** list, select **Extreme NetsightASM**.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

For more information about your Extreme NetSight Automatic Security Manager device, see your vendor documentation.

Extreme Matrix K/N/S Series Switch

The Extreme Matrix Series DSM for SIEM accepts events using syslog. SIEM records all relevant Matrix K-Series, N-Series, or S-Series standalone device events.

Before you configure SIEM to integrate with a Matrix K-Series, N-Series, or S-Series, you must:

1 Log in to your Extreme Matrix device command-line interface (CLI).

2 Type the following commands:

```
set logging server 1 ip-addr <IP Address of Event Processor>
state enable
set logging application RtrAcl level 8
set logging application CLI level 8
set logging application SNMP level 8
set logging application Webview level 8
set logging application System level 8
set logging application RtrFe level 8
set logging application Trace level 8
set logging application RtrLSNat level 8
set logging application FlowLimt level 8
set logging application UPN level 8
set logging application AAA level 8
set logging application Router level 8
set logging application AddrNtfy level 8
set logging application OSPF level 8
```

```
set logging application VRRP level 8
set logging application RtrArpProc level 8
set logging application LACP level 8
set logging application RtrNat level 8
set logging application RtrTwcb level 8
set logging application HostDoS level 8
set policy syslog extended-format enable
```

For more information on configuring the Matrix Series routers or switches, consult your vendor documentation.

3 You are now ready to configure the log sources in SIEM.

To configure SIEM to receive events from an Extreme Matrix Series device:

From the **Log Source Type** list, select **Extreme Matrix K/N/S Series Switch**.

For information on configuring log sources, see the *SIEM Log Sources User Guide*.

Extreme NAC

The Extreme NAC DSM for SIEM accepts events using syslog. SIEM records all relevant events.

For details on configuring your Extreme NAC appliances for syslog, consult your vendor documentation. After the Extreme NAC appliance is forwarding syslog events to SIEM, the configuration is complete. The log source is added to SIEM as Extreme NAC events are automatically discovered. Events forwarded by Extreme NAC appliances are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Extreme NAC. The following configuration steps are optional.

To manually configure a log source for Extreme NAC:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Extreme NAC.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 72: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme NAC appliances.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Extreme 800-Series Switch

The Extreme 800-Series Switch DSM for SIEM accepts events using syslog.

SIEM records all relevant audit, authentication, system, and switch events. Before configuring your Extreme 800-Series Switch in SIEM, you must configure your switch to forward syslog events.

Configure Your Extreme 800-Series Switch

To configure the device to forward syslog events:

1 Log in to your Extreme 800-Series Switch command-line interface.

You must be a system administrator or operator-level user to complete these configuration steps.

2 Type the following command to enable syslog:

```
enable syslog
```

3 Type the following command to create a syslog address for forwarding events to SIEM:

```
create syslog host 1 <IP address> severity informational
facility local7 udp_port 514 state enable
```

Where `<IP address>` is the IP address of your SIEM Console or Event Collector.

4 Optional. Type the following command to forward syslog events using an IP interface address:

```
create syslog source_ipif <name> <IP address>
```

Where:

`<name>` is the name of your IP interface.

`<IP address>` is the IP address of your SIEM Console or Event Collector.

The configuration is complete. The log source is added to SIEM as Extreme 800-Series Switch events are automatically discovered. Events forwarded to SIEM by Extreme 800-Series Switches are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Extreme 800-Series Switches. The following configuration steps are optional.

To manually configure a log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Extreme 800-Series Switch.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 73: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme 800-Series Switch.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

39 Extreme Networks ExtremeWare

The Extreme Networks ExtremeWare DSM for SIEM records all relevant Extreme Networks ExtremeWare and Extremeware XOS devices events using syslog.

To integrate SIEM with an ExtremeWare device, you must configure a log source in SIEM, then configure your Extreme Networks ExtremeWare and Extremeware XOS devices to forward syslog events. SIEM does not automatically discover or create log sources for syslog events from ExtremeWare appliances.

Configuring a Log Source

To integrate with SIEM, you must manually create a log source to receive the incoming ExtremeWare events forwarded to SIEM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Extreme Networks ExtremeWare Operating System (OS).

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 74: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ExtremeWare appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Extreme Networks ExtremeWare appliances are displayed on the **Log Activity** tab.

For information on configuring syslog forwarding for your Extremeware appliances, see your vendor documentation.

40 F5 Networks

This section provides information on the following DSMs:

F5 Networks BIG-IP AFM

The F5 Networks BIG-IP Advanced Firewall Manager (AFM) DSM for SIEM accepts syslog events forwarded from F5 Networks BIG-IP AFM systems in name-value pair format.

Supported Event Types

SIEM is capable of collecting the following events from F5 BIG-IP appliances with Advanced Firewall Managers:

- Network events
- Network Denial of Service (DoS) events
- Protocol security events
- DNS events
- DNS Denial of Service (DoS) events

Before You Begin

Before you can configure the Advanced Firewall Manager, you must verify that your BIG-IP appliance is licensed and provisions to include Advanced Firewall Manager.

Procedure

1 Log in to your BIG-IP appliance Management Interface.

2 From the navigation menu, select **System > License**.

3 In the License Status column, verify the Advanced Firewall Manager is licensed and enabled.

4 To enable the Advanced Firewall Manager, select **System > Resource Provisioning**.

5 From the Provisioning column, select the check box and select **Nominal** from the list.

6 Click **Submit** to save your changes.

Configure a Logging Pool

A logging pool allows you to define a pool of servers that receive syslog events. The pool contains the IP address, port, and a node name that you provide.

Procedure

1 From the navigation menu, select **Local Traffic > Pools**.

2 Click **Create**.

3 In the **Name** field, type a name for the logging pool.
For example, Logging_Pool.

4 From the **Health Monitor** field, in the Available list, select **TCP** and click **<<**.
This moves the TCP option from the Available list to the Selected list.

5 In the Resource pane, from the **Node Name** list, select **Logging_Node** or the name you defined in Step 3.

6 In the **Address** field, type the IP address for the SIEM Console or Event Collector.

7 In the **Service Port** field, type **514**.

8 Click **Add**.

9 Click **Finish**.

Creating a High-speed Log Destination

The process to configure logging for BIG-IP AFM requires that you create a high-speed logging destination.

Procedure

1 From the navigation menu, select **System > Logs > Configuration > Log Destinations**.

2 Click **Create**.

3 In the **Name** field, type a name for the destination.
For example, Logging_HSL_dest.

4 In the **Description** field, type a description.

5 From the **Type** list, select **Remote High-Speed Log**.

6 From the **Pool Name** list, select a logging pool from the list of remote log servers.
For example, Logging_Pool.

7 From the **Protocol** list, select **TCP**.

8 Click **Finish**.

Creating a Formatted Log Destination

The formatted log destination allows you to specify any special formatting required on the events forwarded to the high-speed logging destination.

Procedure

1 From the navigation menu, select **System > Logs > Configuration > Log Destinations**.

2 Click **Create**.

3 In the **Name** field, type a name for the logging format destination.
For example, Logging_Format_dest.

4 In the **Description** field, type a description.

5 From the **Type** list, select **Remote Syslog**.

6 From the **Syslog Format** list, select **Syslog**.

7 From the **High-Speed Log Destination** list, select your high-speed logging destination.
For example, Logging_HSL_dest.

8 Click **Finished**.

Creating a Log Publisher

Creating a publisher allows the BIG-IP appliance to publish the formatted log message to the local syslog database.

Procedure

1 From the navigation menu, select **System > Logs > Configuration > Log Publishers**.

2 Click **Create**.

3 In the **Name** field, type a name for the publisher.
For example, Logging_Pub.

4 In the **Description** field, type a description.

5 From the **Destinations** field, in the Available list, select the log destination name you created in Step 3 and click **<<** to add items to the Selected list.
This moves your logging format destination from the Available list to the Selected list. To include local logging in your publisher configuration, you can add **local-db** and **local-syslog** to the Selected list.

Creating a Logging Profile

Logging profiles allow you to configure the types of events that your Advanced Firewall Manager is producing and associates your events with the logging destination.

Procedure

1 From the navigation menu, select **Security > Event Logs > Logging Profile**.

2 Click **Create**.

3 In the **Name** field, type a name for the log profile.
For example, Logging_Profile.

4 In the **Network Firewall** field, select the **Enabled** check box.

5 From the **Publisher** list, select the log publisher you configured.
For example, Logging_Pub.

6 In the **Log Rule Matches** field, select the **Accept**, **Drop**, and **Reject** check boxes.

7 In the **Log IP Errors** field, select the **Enabled** check box.

8 In the **Log TCP Errors** field, select the **Enabled** check box.

9 In the **Log TCP Events** field, select the **Enabled** check box.

10 In the **Storage Format** field, from the list, select **Field-List**.

11 In the **Delimiter** field, type **,** (comma) as the delimiter for events.

12 In the **Storage Format** field, select all of the options in the Available Items list and click **<<**.
This moves the all Field-List options from the Available list to the Selected list.

13 In the IP Intelligence pane, from the **Publisher** list, select the log publisher you configured.
For example, Logging_Pub.

14 Click **Finished**.

Associate the Profile to a Virtual Server

The log profile you created must be associated with a virtual server in the **Security Policy** tab. This allows the virtual server to process your network firewall events, along with local traffic.

Procedure

1 From the navigation menu, select **Local Traffic > Virtual Servers**.

2 Click the name of a virtual server to modify.

3 From the **Security** tab, select **Policies**.

4 From the **Log Profile** list, select **Enabled**.

5 From the **Profile** field, in the Available list, select **Logging_Profile** or the name you specified in Step 3 and click **<<**.
This moves the Logging_Profile option from the Available list to the Selected list.

6 Click **Update** to save your changes.

The configuration is complete. The log source is added to SIEM as F5 Networks BIG-IP AFM syslog events are automatically discovered. Events forwarded to SIEM by F5 Networks BIG-IP AFM are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP AFM. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select F5 Networks BIG-IP AFM.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 75: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 BIG-IP AFM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

F5 Networks BIG-IP APM

The F5 Networks BIG-IP Access Policy Manager (APM) DSM for SIEM collects access and authentication security events from a BIG-IP APM device using syslog.

Configure Remote Syslog

To configure your BIG-IP LTM device to forward syslog events to a remote syslog source, choose your BIG-IP APM software version:

- Configure Remote Syslog for F5 BIG-IP APM 11.x on page 201
- Configure Remote Syslog for F5 BIG-IP APM 10.x on page 201

Configure Remote Syslog for F5 BIG-IP APM 11.x

To configure syslog for F5 BIG-IP APM 11.x:

1 Log in to the command-line of your F5 BIG-IP device.

2 Type the following command to add a single remote syslog server:

```
tmsh syslog remote server {<Name> {host <IP Address>}}
```

Where:

`<Name>` is the name of the F5 BIG-IP APM syslog source.

`<IP Address>` is the IP address of the SIEM Console.

For example,

```
bigpipe syslog remote server {BIGIP_APM {host 10.100.100.101}}
```

3 Type the following to save the configuration changes:

```
tmsh save sys config partitions all
```

The configuration is complete. The log source is added to SIEM as F5 Networks BIG-IP APM events are automatically discovered. Events forwarded to SIEM by F5 Networks BIG-IP APM are displayed on the **Log Activity** tab in SIEM.

Configure Remote Syslog for F5 BIG-IP APM 10.x

To configure syslog for F5 BIG-IP APM 10.x:

1 Log in to the command-line of your F5 BIG-IP device.

2 Type the following command to add a single remote syslog server:

```
bigpipe syslog remote server {<Name> {host <IP Address>}}
```

Where:

`<Name>` is the name of the F5 BIG-IP APM syslog source.

`<IP Address>` is the IP address of SIEM Console.

For example,

```
bigpipe syslog remote server {BIGIP_APM {host 10.100.100.101}}
```

3 Type the following to save the configuration changes:

```
bigpipe save
```

The configuration is complete. The log source is added to SIEM as F5 Networks BIG-IP APM events are automatically discovered. Events forwarded to SIEM by F5 Networks BIG-IP APM are displayed on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP APM appliances. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select F5 Networks BIG-IP APM.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 76: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP APM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

F5 Networks BIG-IP ASM

The F5 Networks BIG-IP Application Security Manager (ASM) DSM for SIEM collects web application security events from BIG-IP ASM appliances using syslog.

Configure F5 Networks BIG-IP ASM

To forward syslog events from an F5 Networks BIG-IP ASM appliance to SIEM, you must configure a logging profile.

A logging profile allows you to configure remote storage for syslog events, which can be forwarded directly to SIEM.

Procedure

1 Log in to the F5 Networks BIG-IP ASM appliance user interface.

2 On the navigation pane, select **Application Security > Options**.

3 Click Logging Profiles.

4 Click Create.

5 From the Configuration list, select Advanced.

6 Configure the following parameters:

a Type a Profile Name.

For example, type **`SIEM`**.

b Optional. Type a Profile Description.

NOTE

If you do not want data logged locally as well as remotely, you must clear the **Local Storage** check box.

c Select the Remote Storage check box.

d From the Type list, select Reporting Server.

e From the Protocol list, select TCP.

f Configure the **Server Addresses** fields:

- IP address - Type the IP address of the SIEM Console.
- Port - Type a port value of 514.

g Select the Guarantee Logging check box.

NOTE

Enabling the Guarantee Logging option ensures the system log requests continue for the web application when the logging utility is competing for system resources. Enabling the Guarantee Logging option can slow access to the associated web application.

h Select the Report Detected Anomalies check box, to allow the system to log details.

i Click Create.

The display refreshes with the new logging profile. The log source is added to SIEM as F5 Networks BIG-IP ASM events are automatically discovered. Events forwarded by F5 Networks BIG-IP ASM are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP ASM appliances. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select F5 Networks BIG-IP ASM.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 77: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP ASM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

F5 Networks BIG-IP LTM

The F5 Networks BIG-IP Local Traffic Manager (LTM) DSM for SIEM collects networks security events from a BIG-IP device using syslog.

Before receiving events in SIEM, you must configure a log source for SIEM, then configure your BIG-IP LTM device to forward syslog events. We recommend you create your log source before forward events as SIEM does not automatically discover or create log sources for syslog events from F5 BIG-IP LTM appliances.

Configuring a Log Source

To integrate F5 BIG-IP LTM with SIEM, you must manually create a log source to receive syslog events.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **F5 Networks BIG-IP LTM**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 78: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your BIG-IP LTM appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

You are now ready to configure your BIG-IP LTM appliance to forward syslog events to SIEM.

Configuring Syslog Forwarding in BIG-IP LTM

To configure your BIG-IP LTM device to forward syslog events, select your BIG-IP LTM software version:

- Configuring Remote Syslog for F5 BIG-IP LTM 11.x (page 11)
- Configuring Remote Syslog for F5 BIG-IP LTM 10.x (page 12)
- Configuring Remote Syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8 (page 13)

Configuring Remote Syslog for F5 BIG-IP LTM 11.x

To configure syslog for F5 BIG-IP LTM 11.x:

1 Log in to the command-line of your F5 BIG-IP device.

2 To log in to the Traffic Management Shell (tmsh), type the following command:
```
tmsh
```

3 To add a syslog server, type the following command:
```
modify /sys syslog remote-servers add {<Name> {host <IP Address> remote-port 514}}
```
Where:

`<Name>` is a name that you assign to identify the syslog server on your BIG-IP LTM appliance.

`<IP Address>` is the IP address of SIEM.

For example,
```
modify /sys syslog remote-servers add {BIGIPsyslog {host 10.100.100.100 remote-port 514}}
```

4 Save the configuration changes:
```
save /sys config
```
Events forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in SIEM.

Configuring Remote Syslog for F5 BIG-IP LTM 10.x

To configure syslog for F5 BIG-IP LTM 10.x:

1 Log in to the command-line of your F5 BIG-IP device.

2 Type the following command to add a single remote syslog server:
```
bigpipe syslog remote server {<Name> {host <IP Address>}}
```
Where:

`<Name>` is the name of the F5 BIG-IP LTM syslog source.

`<IP Address>` is the IP address of SIEM.

For example:
```
bigpipe syslog remote server {BIGIPsyslog {host 10.100.100.100}}
```

3 Save the configuration changes:
```
bigpipe save
```

NOTE

F5 Networks modified the syslog output format in BIG-IP v10.x to include the use of `local/` before the hostname in the syslog header. The syslog header format containing `local/` is not supported in SIEM, but a workaround is available to correct the syslog header. For more information, see http://support.extremenetworks.com.

Events forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in SIEM.

Configuring Remote Syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8

To configure syslog for F5 BIG-IP LTM 9.4.2 to 9.4.8:

1 Log in to the command-line of your F5 BIG-IP device.

2 Type the following command to add a single remote syslog server:

```
bigpipe syslog remote server <IP Address>
```

Where `<IP Address>` is the IP address of SIEM.

For example:

```
bigpipe syslog remote server 10.100.100.100
```

3 Type the following to save the configuration changes:

```
bigpipe save
```

The configuration is complete. Events forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in SIEM.

F5 Networks FirePass

The F5 Networks FirePass DSM for SIEM collects system events from an F5 FirePass SSL VPN device using syslog.

By default, remote logging is disabled and must be enabled in the F5 Networks FirePass device. Before receiving events in SIEM, you must configure your F5 Networks FirePass device to forward system events to SIEM as a remote syslog server.

Configuring Syslog Forwarding for F5 FirePass

To forward syslog events from an F5 Networks BIG-IP FirePass SSL VPM appliance to SIEM, you must enable and configure a remote log server.

The remote log server can forward events directly to your SIEM Console or any Event Collectors in your deployment.

Procedure

1 Log in to the F5 Networks FirePass Admin Console.

2 On the navigation pane, select **Device Management > Maintenance > Logs**.

3 From the System Logs menu, select the Enable Remote Log Server check box.

4 From the System Logs menu, clear the Enable Extended System Logs check box.

5 In the Remote host parameter, type the IP address or hostname of your SIEM.

6 From the Log Level list, select Information.

The Log Level parameter monitors application level system messages.

7 From the Kernel Log Level list, select Information.

The Kernel Log Level parameter monitors Linux kernel system messages.

8 Click Apply System Log Changes.

The changes are applied and the configuration is complete. The log source is added to SIEM as F5 Networks FirePass events are automatically discovered. Events forwarded to SIEM by F5 Networks BIG-IP ASM are displayed on the **Log Activity** tab in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from F5 Networks FirePass appliances. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select F5 Networks FirePass.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 79: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks FirePass appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

41 Fair Warning

The Fair Warning DSM for SIEM retrieves event files from a remote source using the log file protocol.

SIEM records event categories from the Fair Warning log files about user activity related to patient privacy and security threats to medical records. Before you can retrieve log files from Fair Warning, you must verify your device is configured to generate an event log. Instructions for generating the event log can be found in your Fair Warning documentation.

When configuring the log file protocol, make sure the hostname or IP address configured in the Fair Warning system is the same as configured in the Remote Host parameter in the Log File Protocol configuration.

Configuring a Log Source

You can configure SIEM to download an event log from a Fair Warning device.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list box, select **Fair Warning**.

9 Select the Log File option from the Protocol Configuration list.

10 In the **FTP File Pattern** field, type a regular expression that matches the log files generated by the Fair Warning system.

11 In the **Remote Directory** field, type the path to the directory containing logs from your Fair Warning device.

12 From the Event Generator list, select **Fair Warning**.

13 Click **Save**.

14 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information on full parameters for the Log File protocol, see the *SIEM Log Sources User Guide*.

For more information on configuring Fair Warning, consult your vendor documentation.

42 Fidelis XPS

The Fidelis XPS DSM for SIEM accepts events forwarded in Log Enhanced Event Protocol (LEEF) from Fidelis XPS appliances using syslog.

Supported Event Types

SIEM is capable of collecting all relevant alerts triggered by policy and rule violations configured on your Fidelis XPS appliance.

Event Type Format

Fidelis XPS must be configured to generate events in Log Enhanced Event Protocol (LEEF) and forward these events using syslog. The LEEF format consists of a pipe (|) delimited syslog header and tab separated fields in the event payload.

If the syslog events forwarded from your Fidelis XPS is not formatted as described above, you must examine your device configuration or software version to ensure your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to SIEM.

Configuring Fidelis XPS

You can configure syslog forwarding of alerts from your Fidelis XPS appliance.

Procedure

1 Log in to CommandPost to manage your Fidelis XPS appliance.

2 From the navigation menu, select **System > Export**.

A list of available exports is displayed. If this is the first time you have used the export function, the list is empty.

3 Select one of the following options:

- Click **New** to create a new export for your Fidelis XPS appliance.
- Click **Edit** next to an export name to edit an existing export on your Fidelis XPS appliance.

The Export Editor is displayed.

4 From the **Export Method** list, select **Syslog LEEF**.

5 In the **Destination** field, type the IP address or host name for SIEM.

For example, `10.10.10.100:::514`

This field does not support non-ASCII characters.

6 From **Export Alerts**, select one of the following options:

- **All alerts** - Select this option to export all alerts to SIEM. This option is resource intensive and it can take time to export all alerts.

- **Alerts by Criteria** - Select this option to export specific alerts to SIEM. This option displays a new field that allows you to define your alert criteria.

7 From **Export Malware Events**, select **None**.

8 From **Export Frequency**, select **Every Alert / Malware**.

9 In the **Save As** field**,** type a name for your export.

10 Click **Save**.

11 Optional. To verify events are forwarded to SIEM, you can click **Run Now**.

Run Now is intended as a test tool to verify that alerts selected by criteria are exported from your Fidelis appliance. This option is not available if you selected to export all events in step 6.

The configuration is complete. The log source is added to SIEM as Fidelis XPS syslog events are automatically discovered. Events forwarded to SIEM by Fidelis XPS are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Fidelis XPS. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Fidelis XPS.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 80: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Fidelis XPS appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

43 FireEye

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

44 ForeScout CounterACT

The ForeScout CounterACT DSM for SIEM accepts Log Extended Event Format (LEEF) events from CounterACT using syslog.

Supported Event Types

SIEM records the following ForeScout CounterACT events:

- Denial of Service (DoS)
- Authentication
- Exploit
- Suspicious
- System

Configuring a Log Source

To integrate ForeScout CounterACT with SIEM, you must manually create a log source to receive policy-based syslog events.

SIEM does not automatically discover or create log sources for syslog events from ForeScout CounterACT appliances.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select ForeScout CounterACT.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 81: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ForeScout CounterACT appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM.

Configure ForeScout CounterACT

Before configuring SIEM, you must install a plug-in for your ForeScout CounterACT appliance and configure ForeScout CounterACT to forward syslog events to SIEM.

Configure the ForeScout CounterACT Plug-in

To integrate SIEM with ForeScout CounterACT, you must download, install and configure a plug-in for CounterACT. The plug-in extends ForeScout CounterACT and provides the framework for forwarding LEEF events to SIEM.

Procedure

1 From the ForeScout website, download the plug-in for ForeScout CounterACT.

2 Log in to your ForeScout CounterACT appliance.

3 From the CounterACT Console toolbar, select **Options > Plugins > Install** and select the location of the plug-in file.

The plug-in is installed and displayed in the Plugins pane.

4 From the Plugins pane, select the **SIEM** plug-in and click **Configure**.

The Add SIEM wizard is displayed.

5 In the **Server Address** field, type IP address of SIEM.

6 From the **Port** list, select **514**.

7 Click **Next**.

8 From the Assigned CounterACT devices pane, choose one of the following options:

- **Default Server** - Select this option to make all devices on this ForeScout CounterACT forward events to SIEM.
- **Assign CounterACT devices** - Select this option to assign which individual devices running on ForeScout CounterACT forward events to SIEM. The Assign CounterACT devices option is only available if you have one or more ForeScout CounterACT server.

9 Click **Finish**.

The plug-in configuration is complete. You are now ready to define the events forwarded to SIEM by ForeScout CounterACT policies.

Configuring ForeScout CounterACT Policies

ForeScout CounterACT policies test conditions to trigger management and remediation actions on the appliance.

The plug-in provides an additional action for policies to forward the event to the SIEM using syslog. To forward events to SIEM, you must define a CounterACT policy that includes the SIEM update action. The policy condition must be met at least once to initiate an event to SIEM. You must configure each policy to send updates to SIEM for events you want to record.

Procedure

1 Select a policy for ForeScout CounterACT.

2 From the Actions tree, select **Audit > Send Updates to SIEM Server**.

3 From the **Contents** tab, configure the following values:
   a Select the **Send host property results** check box.
   b Choose one of the type of events to forward for the policy:
      - **Send All** - Select this option to include all properties discovered for the policy to SIEM.
      - **Send Specific** - Select this option to select and send only specific properties for the policy to SIEM.
   c Select the **Send policy status** check box.

4 From the **Trigger** tab, select the interval ForeScout CounterACT uses for forwarding the event to SIEM:

- **Send when the action starts** - Select this check box to send a single event to SIEM when the conditions of your policy are met.
- **Send when information is updated** - Select this check box to send a report when there is a change in the host properties specified in the **Contents** tab.
- **Send periodically every** - Select this check box to send a reoccurring event to SIEM on an interval if the policy conditions are met.

5 Click **OK** to save the policy changes.

6 Repeat this process to configure any additional policies with an action to send updates to SIEM, if required.

The configuration is complete. Events forwarded by ForeScout CounterACT are displayed on the **Log Activity** tab of SIEM.

45 Fortinet FortiGate

The Fortinet FortiGate DSM for SIEM records all relevant FortiGate IPS/Firewall events using syslog.

The following table identifies the specifications for the Fortinet FortiGate DSM:

Table 82: Fortinet FortiGate DSM specifications

Specification	Value
Manufacturer	Fortinet
DSM	Fortinet FortiGate
RPM file name	DSM-FortinetFortiGate-7.x-xxxxxx.noarch.rpm
Supported version	FortiOS v2.5 and later
Protocol	Syslog
SIEM recorded events	All relevant events
Auto discovered	Yes
Includes identity	Yes
For more information	www.fortinet.com

Fortinet FortiGate DSM Integration Process

To integrate Fortinet FortiGate DSM with SIEM, use the following procedures:

1 Download and install the most recent Fortinet FortiGate RPM to your SIEM Console. If automatic updates are enabled, this procedure is not required. RPMs need to be installed only one time.

2 Optional. Install the Syslog Redirect protocol RPM to collect events through Fortigate FortiAnalyzer. When you use the Syslog Redirect protocol, SIEM can identify the specific Fortigate firewall that sent the event. You can use the procedure to manually install a DSM to install a protocol.

3 Configure your Fortinet FortiGate system to enable communication with SIEM. This procedure must be performed for each instance of Fortinet FortiGate. For more information on configuring a Fortinet FortiGate device, see your vendor documentation.

4 For each Fortinet FortiGate server you want to integrate, create a log source on the SIEM Console. If SIEM automatically discovers the DSM, this step is not required.

Related tasks

Manually Installing a DSM on page 4

Configuring a Fortinet FortiGate Log Source on page 218

Configuring a Fortinet FortiGate Log Source

SIEM automatically discovers and creates a log source for syslog events from Fortinet FortiGate. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Fortinet FortiGate Security Gateway.

9 Using the Protocol Configuration list, select one of the following options:

- Select **Syslog**.
- To configure SIEM to receive FortiAnalyzer events, select **Syslog Redirect**.

10 Configure the following values:

Table 83: Syslog Parameters

Parameter	Description
Log Source Identifier RegEx	devname=([\w-]+)
Listen Port	517
Protocol	UDP

11 Configure the remaining parameters.

12 Click Save.

13 On the Admin tab, click Deploy Changes.

46 Foundry FastIron

You can integrate a Foundry FastIron device with SIEM to collect all relevant events using syslog.

Configure Syslog for Foundry FastIron

To integrate SIEM with a Foundry FastIron RX device, you must configure the appliance to forward syslog events.

Procedure

1 Log in to the Foundry FastIron device command-line interface (CLI).

2 Type the following command to enable logging:
`logging on`
Local syslog is now enabled with the following defaults:

- Messages of all syslog levels (Emergencies - Debugging) are logged.
- Up to 50 messages are retained in the local syslog buffer.
- No syslog server is specified.

3 Type the following command to define an IP address for the syslog server:
`logging host <IP Address>`
Where `<IP Address>` is the IP address of your SIEM.
You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Foundry FastIron. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Foundry FastIron.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 84: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Foundry FastIron appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

47 Generic Firewall

The generic firewall server DSM for SIEM accepts events using syslog. SIEM records all relevant events.

Configuring Event Properties

To configure SIEM to interpret the incoming generic firewall events:

1 Forward all firewall logs to your SIEM.

For information on forwarding firewall logs from your generic firewall to SIEM, see your firewall vendor documentation.

2 Open the following file:

`/opt/qradar/conf/genericFirewall.conf`

Make sure you copy this file to systems hosting the Event Collector and the SIEM Console.

3 Restart the Tomcat server:

`service tomcat restart`

A message is displayed indicating that the Tomcat server has restarted.

4 Enable or disable regular expressions in your patterns by setting the regex_enabled property accordingly. By default, regular expressions are disabled. For example:

`regex_enabled=false`

When you set the regex_enabled property to false, the system generates regular expressions based on the tags you entered while attempting to retrieve the corresponding data values from the logs.

When you set the regex_enabled property to true, you can define custom regex to control patterns. These regex are directly applied to the logs and the first captured group is returned. When defining custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

To integrate a generic firewall with SIEM, make sure you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Also, instead of using numeric qualifiers, re-write the expression to use the primitive qualifiers `(/?/,/*/ and /+/)`.

5 Review the file to determine a pattern for accepted packets.

For example, if your device generates the following log messages for accepted packets:

```
Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1
Source Port: 80 Destination IP: 192.168.1.2 Destination Port: 80
Protocol: tcp
```

The pattern for accepted packets is `Packet accepted`.

6 Add the following to the file:

`accept_pattern=<accept pattern>`

Where <accept pattern> is the pattern determined instep 5. For example:

`accept pattern=Packet accepted`

Patterns are case insensitive.

7 Review the file to determine a pattern for denied packets.

For example, if your device generates the following log messages for denied packets:

```
Aug. 5, 2005 08:30:00 Packet denied. Source IP: 192.168.1.1
Source Port: 21 Destination IP: 192.168.1.2 Destination Port: 21
Protocol: tcp
```

The pattern for denied packets is `Packet denied.`

8 Add the following to the file:

```
deny_pattern=<deny pattern>
```

Where <deny pattern> is the pattern determined in step 7.

Patterns are case insensitive.

9 Review the file to determine a pattern, if present, for the following:

source ip

source port

destination ip

destination port

protocol

For example, if your device generates the following log message:

```
Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1
Source Port: 80 Destination IP: 192.168.1.2 Destination Port: 80
Protocol: tcp
```

The pattern for source IP is `Source IP`.

10 Add the following to the file:

```
source_ip_pattern=<source ip pattern>
source_port_pattern=<source port pattern>
destination_ip_pattern=<destination ip pattern>
destination_port_pattern=<destination port pattern>
protocol_pattern=<protocol pattern>
```

Where `<source ip pattern>`, `<source port pattern>`, `<destination ip pattern>`, `<destination port pattern>`, and `<protocol pattern>` are the corresponding patterns identified in step 9.

NOTE

Patterns are case insensitive and you can add multiple patterns. For multiple patterns, separate using a # symbol.

11 Save and exit the file.

You are now ready to configure the log source in SIEM.

Configuring a Log Source

To integrate generic firewalls with SIEM, you must manually create a log source to receive the events as SIEM does not automatically discover or create log sources for events from generic firewall appliances.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Configurable Firewall Filter.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 85: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your generic firewall appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The log source is added to SIEM. Events forwarded to SIEM by generic firewalls are displayed on the **Log Activity** tab.

48 Generic Authorization Server

The generic authorization server DSM for SIEM records all relevant generic authorization events using syslog.

Configuring Event Properties

To configure SIEM to interpret the incoming generic authorization events:

1 Forward all authentication server logs to your SIEM system.

For information on forwarding authentication server logs to SIEM, see your generic authorization server vendor documentation.

2 Open the following file:

`/opt/qradar/conf/genericAuthServer.conf`

Make sure you copy this file to systems hosting the Event Collector and the Console.

3 Restart the Tomcat server:

`service tomcat restart`

A message is displayed indicating that the Tomcat server has restarted.

4 Enable or disable regular expressions in your patterns by setting the regex_enabled property accordingly. By default, regular expressions are disabled. For example:

`regex_enabled=false`

When you set the regex_enabled property to false, the system generates regular expressions (regex) based on the tags you entered while attempting to retrieve the corresponding data values from the logs.

When you set the regex_enabled property to true, you can define custom regex to control patterns. These regex are directly applied to the logs and the first captured group is returned. When defining custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

To integrate the generic authorization server with SIEM, make sure you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Also, instead of using numeric qualifiers, re-write the expression to use the primitive qualifiers `(/?/,/*/ and /+/)`.

5 Review the file to determine a pattern for successful login:

For example, if your authentication server generates the following log message for accepted packets:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for successful login is `Accepted password`.

6 Add the following entry to the file:

`login_success_pattern=<login success pattern>`

Where `<login success pattern>` is the pattern determined in step 5.

For example:

`login_success_pattern=Accepted password`

All entries are case insensitive.

7 Review the file to determine a pattern for login failures.

For example, if your authentication server generates the following log message for login failures:

```
Jun 27 12:58:33 expo sshd[20627]: Failed password for root from
10.100.100.109 port 1849 ssh2
```

The pattern for login failures is `Failed password`.

8 Add the following to the file:

```
login_failed_pattern=<login failure pattern>
```

Where `<login failure pattern>` is the pattern determined for login failure.

For example:

```
login_failed_pattern=Failed password
```

All entries are case insensitive.

9 Review the file to determine a pattern for logout:

For example, if your authentication server generates the following log message for logout:

```
Jun 27 13:00:01 expo su(pam_unix)[22723]: session closed for
user genuser
```

The pattern for lookout is `session closed.`

10 Add the following to the genericAuthServer.conf file:

```
logout_pattern=<logout pattern>
```

Where `<logout pattern>` is the pattern determined for logout in step 9.

For example:

```
logout_pattern=session closed
```

All entries are case insensitive.

11 Review the file to determine a pattern, if present, for source IP address and source port.

For example, if your authentication server generates the following log message:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for source IP address is `from` and the pattern for source port is `port`.

12 Add an entry to the file for source IP address and source port:

```
source_ip_pattern=<source IP pattern>
source_port_pattern=<source port pattern>
```

Where `<source IP pattern>` and `<source port pattern>` are the patterns identified in step 11 for source IP address and source port.

For example:

```
source_ip_pattern=from
source_port_pattern=port
```

13 Review the file to determine if a pattern exists for username.

For example:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root
from 10.100.100.109 port 1727 ssh2
```

The pattern for username is `for`.

14 Add an entry to the file for the username pattern:

For example:

```
user_name_pattern=for
```

You are now ready to configure the log source in SIEM.

Configure a Log Source

To integrate generic authorization appliance event with SIEM, you must manually create a log source to receive the events as SIEM does not automatically discover or create log sources for events from generic authorization appliances.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Configurable Authentication message filter.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 86: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your generic authorization appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by generic authorization appliances are displayed on the **Log Activity** tab.

49 Great Bay Beacon

The Great Bay Beacon DSM for SIEM supports syslog alerts from the Great Bay Beacon Endpoint Profiler.

SIEM records all relevant endpoint security events. Before you can integrate with SIEM, you must configure your Great Bay Beacon Endpoint Profiler to forward syslog event messages to SIEM.

Configuring Syslog for Great Bay Beacon

You can configure your Great Bay Beacon Endpoint Profiler to forward syslog events.

Procedure

1 Log in to your Great Bay Beacon Endpoint Profiler.

2 To create an event, select **Configuration > Events > Create Events**.
A list of currently configured events is displayed.

3 From the Event Delivery Method pane, select the **Syslog** check box.

4 To apply your changes, select **Configuration Apply Changes > Update Modules**.

5 Repeat step 2 to step 4 to configure all of the events you want to monitor in SIEM.

6 Configure SIEM as an external log source for your Great Bay Beacon Endpoint Profiler.
For information on configuring SIEM as an external log source, see the *Great Bay Beacon Endpoint Profiler Configuration Guide*.

You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Great Bay Beacon. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Great Bay Beacon.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 87: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Great Bay Beacon appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

50 HBGary Active Defense

The HBGary Active Defense DSM for SIEM accepts several event types forwarded from HBGary Active Defense devices, such as access, system, system configuration, and policy events.

Events from Active Defense are forwarded in the Log Event Extended Format (LEEF) to SIEM using syslog. Before you can configure SIEM, you must configure a route for your HBGary Active Defense device to forward events to a syslog destination.

Configuring HBGary Active Defense

You can configure a route for syslog events in Active Defense for SIEM.

Procedure

1 Log in to the Active Defense Management Console.

2 From the navigation menu, select **Settings > Alerts**.

3 Click **Add Route**.

4 In the **Route Name** field, type a name for the syslog route you are adding to Active Defense.

5 From the **Route Type** list, select **LEEF (Q1 Labs)**.

6 In the Settings pane, configure the following values:

- **Host** - Type the IP address or hostname for your SIEM Console or Event Collector.
- **Port** - Type **514** as the port number.

7 In the Events pane, select any events you want to forward to SIEM.

8 Click **OK** to save your configuration changes.

The Active Defense device configuration is complete. You are now ready to configure a log source in SIEM. For more information on configuring a route in Active Defense, see your HBGary Active Defense User Guide.

Configuring a Log Source

SIEM automatically discovers and creates a log source for LEEF formatted syslog events forwarded from Active Defense. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **HBGary Active Defense**.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 88: HBGary Active Defense syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your HBGary Active Defense device. The IP address or hostname identifies your HBGary Active Defense device as a unique event source in SIEM.

For more information on configuring log sources, see the *SIEM Log Sources Users Guide*.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The HBGary Active Defense configuration is complete.

51 Honeycomb Lexicon File Integrity Monitor (FIM)

You can use the Honeycomb Lexicon File Integrity Monitor (FIM) DSM with SIEM to collect detailed file integrity events from your network.

Configuration Overview

SIEM supports syslog events that are forwarded from Lexicon File Integrity Monitor installations that use Lexicon mesh v3.1 and later. The syslog events that are forwarded by Lexicon FIM are formatted as Log Extended Event Format (LEEF) events by the Lexicon mesh service.

To integrate Lexicon FIM events with SIEM, you must complete the following tasks:

1. On your Honeycomb installation, configure the Lexicon mesh service to generate syslog events in LEEF.
2. On your Honeycomb installation, configure any Lexicon FIM policies for your Honeycomb data collectors to forward FIM events to your SIEM Console or Event Collector.
3. On your SIEM Console, verify that a Lexicon FIM log source is created and that events are displayed on the **Log Activity** tab.
4. Optional. Ensure that no firewall rules block communication between your Honeycomb data collectors and the SIEM Console or Event Collector that is responsible for receiving events.

Supported Honeycomb FIM Event Types Logged by SIEM

The Honeycomb FIM DSM for SIEM can collect events from several categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, file rename events might have a low-level categories of either file rename successful or file rename failed.

The following list defines the event categories that are collected by SIEM for Honeycomb file integrity events:

- Baseline events
- Open file events
- Create file events
- Rename file events
- Modify file events
- Delete file events
- Move file events
- File attribute change events

- File ownership change events

SIEM can also collect Windows and other log files that are forwarded from Honeycomb Lexicon. However, any event that is not a file integrity event might require special processing by a Universal DSM or a log source extension in SIEM.

Configuring the Lexicon Mesh Service

To collect events in a format that is compatible with SIEM, you must configure your Lexicon mesh service to generate syslog events in LEEF.

Procedure

1. Log in to the Honeycomb LexCollect system that is configured as the dbContact system in your network deployment.
2. Locate the Honeycomb installation directory for the installImage directory.
   For example, `c:\Program Files\Honeycomb\installImage\data`.
3. Open the `mesh.properties` file.
   If your deployment does not contain Honeycomb LexCollect, you can edit `mesh.properties` manually.
   For example, `c:\Program Files\mesh`
4. To export syslog events in LEEF, edit the **formatter** field.
   For example, `formatter=leef`.
5. Save your changes.
   The mesh service is configured to output LEEF events. For information about the Lexicon mesh service, see your Honeycomb documentation.

Configuring a Honeycomb Lexicon FIM Log Source in SIEM

SIEM automatically discovers and creates a log source for file integrity events that are forwarded from the Honeycomb Lexicon File Integrity Monitor. This procedure is optional.

Procedure

1. Log in to SIEM.
2. Click the Admin tab.
3. In the navigation menu, click Data Sources.
4. Click the Log Sources icon.
5. Click Add.
6. In the **Log Source Name** field, type a name for your log source.
7. Optional. In the **Log Source Description** field, type a description for your log source.
8. From the Log Source Type list, select **Honeycomb Lexicon File Integrity Monitor**.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 89: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Honeycomb Lexicon FIM installation. The log source identifier must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

Honeycomb Lexicon File Integrity Monitor events that are forwarded to SIEM are displayed on the **Log Activity** tab.

52 HP

This section provides information on the following DSMs:

HP ProCurve

You can integrate an HP ProCurve device with SIEM to record all relevant HP Procurve events using syslog.

Configuring Syslog for HP ProCurve

You can configure your HP ProCurve device to forward syslog events to SIEM

Procedure

1. Log into the HP ProCurve device.
2. Type the following command to make global configuration level changes.
   `config`
   If successful, the CLI will change to `ProCurve(config)#` as the prompt.
3. Type the following command to `logging <syslog-ip-addr>`
   Where `<syslog-ip-addr>` is the IP address of the SIEM.
4. To exit config mode, press **CTRL+Z**.
5. Type `write mem` to save the current configuration to the startup configuration for your HP ProCurve device.
   You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for LEEF formatted syslog events forwarded from Active Defense. These configuration steps are optional.

Procedure

1. Log in to SIEM.
2. Click the Admin tab.
3. In the navigation menu, click Data Sources.
4. Click the Log Sources icon.
5. Click Add.
6. In the **Log Source Name** field, type a name for the log source.
7. In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **HP ProCurve**.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 90: HP ProCurve syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your HP ProCurve device.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.
The configuration is complete.

HP Tandem

You can integrate an HP Tandem device with SIEM. An HP Tandem device accepts SafeGuard Audit file events using a log file protocol source.

A log file protocol source allows SIEM to retrieve archived log files from a remote host. The HP Tandem DSM supports the bulk loading of log files using the log file protocol source.

When configuring your HP Tandem device to use the log file protocol, make sure the hostname or IP address configured in the HP Tandem device is the same as configured in the Remote Host parameter in the Log File Protocol configuration.

The SafeGuard Audit file names have the following format:

`Annnnnnn`

The single alphabetic character `A` is followed by a seven-digit decimal integer `nnnnnnn`, which increments by one each time a name is generated in the same audit pool.

You are now ready to configure the log source and protocol in SIEM:

Procedure

1 From the Log Source Type list, select HP Tandem.

2 To configure the log file protocol, from the Protocol Configuration list, select Log File.

NOTE

Your system must be running the latest version of the log file protocol to integrate with an HP Tandem device.

For the full list of Log File protocol parameters, see the *SIEM Log Sources User Guide*. For more information about HP Tandem see your vendor documentation.

Hewlett Packard UNIX (HP-UX)

You can integrate an HP-UX device with SIEM. An HP-UX DSM accepts events using syslog.

Configuring Syslog for HP-UX

You can configure syslog on your HP-UX device to forward events to SIEM.

Procedure

1 Log in to the HP-UX device command-line interface.

2 Open the following file:
`/etc/syslog.conf`

3 Add the following line:
`<facility>.<level>  <destination>`
Where:
`<facility>` is auth.
`<level>` is info.
`<destination>` is the IP address of the SIEM.

4 Save and exit the file.

5 Type the following command to ensure that syslogd enforces the changes to the syslog.conf file.
`kill -HUP 'cat /var/run/syslog.pid'`

NOTE

The above command is surrounded with back quotation marks.

You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events forwarded from HP-UX. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Hewlett Packard UniX.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 91: HP-UX syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your Hewlett Packard UniX device.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

53 Huawei

This section includes configurations for the following DSMs:

Huawei AR Series Router

The Huawei AR Series Router DSM for SIEM can accept events from Huawei AR Series Routers using syslog.

SIEM records all relevant IPv4 events forwarded from Huawei AR Series Router. To integrate your device with SIEM, you must create a log source, then configure your AR Series Router to forward syslog events.

Supported Routers

The DSM supports events from the following Huawei AR Series Routers:

- AR150
- AR200
- AR1200
- AR2200
- AR3200

Configuring a Log Source

SIEM does not automatically discover incoming syslog events from Huawei AR Series Routers.

If your events are not automatically discovered, you must manually create a log source from the **Admin** tab in SIEM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Huawei AR Series Router**.

9 From the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 92: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your Huawei AR Series Router. Each log source you create for your Huawei AR Series Router should include a unique identifier, such as an IP address or host name.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to configure your Huawei AR Series Router to forward events to SIEM.

Configuring Your Huawei AR Series Router

To forward syslog events to SIEM, you must configure your Huawei AR Series Router as an information center, then configure a log host.

The log host you create for your Huawei AR Series Router should forward events to your SIEM Console or an Event Collector.

Procedure

1 Log in to your Huawei AR Series Router command-line Interface (CLI).

2 Type the following command to access the system view:
```
system-view
```

3 Type the following command to enable the information center:
```
info-center enable
```

4 Type the following command to send informational level log messages to the default channel:
```
info-center source default channel loghost log level
informational debug state off trap state off
```

5 Optional. To verify your Huawei AR Series Router source configuration, type the command:
```
display channel loghost
```

6 Type the following command to configure the IP address for SIEM as the loghost for your switch:
```
info-center loghost <IP address> facility <local>
```
Where:

`<IP address>` is the IP address of the SIEM Console or Event Collector.

`<local>` is the syslog facility, for example, local0.

For example,
```
info-center loghost 10.10.10.1 facility local0
```

7 Type the following command to exit the configuration:
```
quit
```
The configuration is complete. You can verify events forwarded to SIEM by viewing events on the **Log Activity** tab.

Huawei S Series Switch

The Huawei S Series Switch DSM for SIEM can accept events from Huawei S Series Switch appliances using syslog.

SIEM records all relevant IPv4 events forwarded from Huawei S Series Switches. To integrate your device with SIEM, you must configure a log source, then configure your S Series Switch to forward syslog events.

Supported Switches

The DSM supports events from the following Huawei S Series Switches:

- S5700
- S7700
- S9700

Configuring a Log Source

SIEM does not automatically discover incoming syslog events from Huawei S Series Switches.

If your events are not automatically discovered, you must manually create a log source from the **Admin** tab in SIEM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Huawei S Series Switch**.

9 From the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 93: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your Huawei S Series switch. Each log source you create for your Huawei S Series switch should include a unique identifier, such as an IP address or host name.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to configure your Huawei S Series Switch to forward events to SIEM.

Configuring Your Huawei S Series Switch

To forward syslog events to SIEM, you must configure your Huawei S Series Switch as an information center, then configure a log host.

The log host you create for your Huawei S Series Switch should forward events to your SIEM Console or an Event Collector.

Procedure

1 Log in to your Huawei S Series Switch command-line Interface (CLI).

2 Type the following command to access the system view:
```
system-view
```

3 Type the following command to enable the information center:
```
info-center enable
```

4 Type the following command to send informational level log messages to the default channel:
```
info-center source default channel loghost log level
informational debug state off trap state off
```

5 Optional. To verify your Huawei S Series Switch source configuration, type the command:
```
display channel loghost
```

6 Type the following command to configure the IP address for SIEM as the loghost for your switch:
```
info-center loghost <IP address> facility <local>
```
Where:

`<IP address>` is the IP address of the SIEM Console or Event Collector.

`<local>` is the syslog facility, for example, local0.

For example,
```
info-center loghost 10.10.10.1 facility local0
```

7 Type the following command to exit the configuration:
```
quit
```
The configuration is complete. You can verify events forwarded to SIEM by viewing events on the **Log Activity** tab.

54 IBM

This section provides information about IBM DSMs:

IBM AIX

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

IBM AS/400 iSeries

SIEM has three options for integrating events from an IBM AS/400® (or IBM OS/400) iSeries using one of the following software products:

- Integrating an IBM AS/400 iSeries DSM on page 242 - The IBM AS/400 iSeries DSM uses the DSPJRN command to write audit journal records to a database file that is pushed to an FTP server for retrieval by SIEM using the Log File protocol source.

  For more information, see Integrating an IBM AS/400 iSeries DSM on page 242.

  For more information on configuring log sources and protocols, see Pulling Data Using Log File Protocol on page 244.
- LogAgent for System i - Accepts all Common Event Format (CEF) formatted syslog messages. You can integrate an IBM OS/400 device and later using the LogAgent for System i software. After you configure your LogAgent for System i software, use the Log File protocol source to pull the syslog CEF messages.

  For more information, see your Patrick Townsend Security Solutions LogAgent for System i documentation.

  For more information on configuring log sources and protocols, see Pulling Data Using Log File Protocol on page 244.
- PowerTech Interact - Accepts all Common Event Format (CEF) formatted syslog messages. You can integrate an IBM OS/400 device using the PowerTech Interact software. After you configure your PowerTech Interact software, use the Log File protocol source to pull the syslog CEF messages.
- RazLee iSecurity - This DSM configuration is provided in a separate chapter. See Chapter 85, "Raz-Lee iSecurity".

Integrating an IBM AS/400 iSeries DSM

The SIEM IBM AS/400 iSeries DSM allows you to integrate with an IBM AS/400 iSeries to collect audit records and event information.

The IBM AS/400 iSeries DSM uses an agent running on the iSeries that manages, gathers and transfers the event information. The program leverages the DSPJRN command to write audit journal records to a database file. These records are reformatted and forwarded to an FTP server where SIEM can retrieve the records using FTP.

To integrate IBM iSeries events into SIEM:

1 The IBM iSeries system records and writes security events in the Audit Journal and the QHST logs. QHST logs are stored in the Audit Journal as TYPE5 messages. For more information on configuring your AS/400 iSeries DSM, see Configure an IBM iSeries to Integrate with SIEM on page 243.

2 During your scheduled audit collection, the `AJLIB/AUDITJRN` command is run by an iSeries Job Scheduler using DSPJRN to collect, format and write the Audit Journal records to a database file. The database file containing the audit record information is transferred from the iSeries to an FTP server.

3 Use the log file protocol source to pull the formatted audit file from the FTP server on a scheduled basis. For more information on configuring log sources and protocols, see Pulling Data Using Log File Protocol on page 244.

Configure an IBM iSeries to Integrate with SIEM

To integrate an IBM iSeries with SIEM:

1 From the Extreme Networks Support Portal (http://support.extremenetworks.com), download the following files:

`AJLIB.SAVF`

2 Copy the `AJLIB.SAVF` file onto a computer or terminal that has FTP access to the IBM AS/400 iSeries.

3 Create a generic online SAVF file on the iSeries using the command:

```
CRTSAVF QGPL/SAVF
```

4 Using FTP on the computer or terminal, replace the iSeries generic `SAVF` with the `AJLIB.SAVF` file downloaded from http://support.extremenetworks.com:

```
bin
cd qgpl
lcd c:\
put ajlib.savf savf
quit
```

If you are transferring your SAVF file from another iSeries, the file must be sent with the required FTP subcommand mode BINARY before the GET or PUT statement.

5 Restore the AJLIB library on the IBM iSeries:

```
RSTLIB
```

6 Setup the data collection start date and time for the Audit Journal Library (AJLIB):

```
AJLIB/SETUP
```

You are prompted for a username and password. If you start the Audit Journal Collector a failure message is sent to QSYSOPR.

The setup function sets a default start date and time for data collection from the Audit Journal to 08:00:00 of the current day.

NOTE

To preserve your previous start date and time information for a previous installation you must run `AJLIB/DATETIME.` Record the previous start date and time and type those values when you run `AJLIB/SETUP`. The start date and time must contain a valid date and time in the six character system date and system time format. The end date and time must be a valid date and time or left blank.

7 Run `AJLIB/DATETIME.`

This updates the IBM AS/400 iSeries with the data collection start date and time if you made changes.

8 Run `AJLIB/AUDITJRN.`

This launches the Audit Journal Collection program to gather and send the records to your remote FTP server: If the transfer to the FTP server fails, a message is sent to QSYSOPR. The process for launching `AJLIB/AUDITJRN` is typically automated by an iSeries Job Scheduler to collect records periodically.

NOTE

If the FTP transfer is successful, the current data and time information is written into the start time for `AJLIB/DATETIME` to update the gather time and the end time is set to blank. If the FTP transfer fails, the export file is erased and no updates are made to the gather date or time.

Pulling Data Using Log File Protocol

You are now ready to configure the log source and protocol in SIEM:

1 To configure SIEM to receive events from an IBM AS/400 iSeries, you must select the IBM AS/400 iSeries option from the Log Source Type list.

2 To configure the log file protocol for the IBM AS/400 iSeries DSM, you must select the Log File option from the Protocol Configuration list and define the location of your FTP server connection settings.

NOTE

If you are using the PowerTech Interact or LogAgent for System i software to collect CEF formatted syslog messages, you must select the Syslog option from the Protocol Configuration list.

3 We recommend when you use the Log File protocol option that you select a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).

For more information on configuring log sources and protocols, see the *SIEM Log Sources User Guide*.

IBM CICS

The IBM CICS® DSM allows you to integrate events from IBM Custom Information Control System (CICS®) events from an IBM z/OS® mainframe using IBM Security zSecure.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows SIEM to retrieve the events on the schedule you have defined.

To integrate IBM CICS events:

1 Confirm your installation meets any prerequisite installation requirements. For more information, see Before You Begin on page 245.

2 Configure your IBM z/OS image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

3 Create a log source in SIEM for IBM CICS to retrieve your LEEF formatted event logs. For more information, see Create a Log Source on page 246.

4 Optional. Create a custom event property for IBM CICS in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.

  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Create a Log Source

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **IBM CICS**.

7 From the **Protocol Configuration** list, select **Log File**.

8 Configure the following values:

Table 94: IBM CICS log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM CICS log source. This allows events to be identified at the image or location level in your network that your users can identify.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.

Table 94: IBM CICS log file protocol parameters (Continued)

Parameter	Description
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern CICS.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: `CICS.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

Table 94: IBM CICS log file protocol parameters (Continued)

Parameter	Description
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.

Table 94: IBM CICS log file protocol parameters (Continued)

Parameter	Description
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The IBM CICS configuration is complete. If your IBM CICS requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

IBM Lotus Domino

You can integrate an IBM Lotus Domino® device with SIEM. An IBM Lotus Domino device accepts events using SNMP.

Setting Up SNMP Services

To set up the SNMP services on the IBM Lotus Domino server:

Procedure

1 Install the Lotus Domino SNMP Agent as a service. From the command prompt, go to the Lotus\Domino directory and type the following command:

```
Insnmp -SC
```

2 Confirm that the Microsoft SNMP service is installed.

3 Start the SNMP and LNSNMP services. From a command prompt, type the following commands:

```
net start snmp
net start lnsnmp
```

4 Select **Start > Program > Administrative Tools > Services** to open the Services MMC

5 Double-click on the SNMP service and select the Traps tab.

6 In the **Community name** field, type **public** and click add to list:

7 In the Traps destinations section, select Add and type the IP address of your SIEM. Click Add.

8 Click OK.

9 Confirm that both SNMP agents are set to Automatic so they run upon server boot.

Starting the Domino Server Add-in Tasks

After you configure the SNMP services, you must start the Domino server add-in tasks. Repeat the below procedure for each Domino partition.

Procedure

1 Log in to the Domino Server console.

2 To support SNMP traps for Domino events, type the following command to start the Event Interceptor add-in task:

```
load intrcpt
```

3 To support Domino statistic threshold traps, type the following command to start the Statistic Collector add-in task:

```
load collect
```

4 Arrange for the add-in tasks to be restarted automatically the next time that Domino is restarted. Add intrcpt and collect to the ServerTasks variable in Domino's NOTES.INI file.

Configuring SNMP Services

To configure SNMP services:

NOTE

Configurations might vary depending on your environment. See your vendor documentation for more information.

Procedure

1 Open the Domino Administrator utility and authenticate with administrative credentials.

2 Click on the Files tab, and the Monitoring Configuration (events4.nsf) document.

3 Expand the DDM Configuration Tree and select DDM Probes By Type.

4 Select Enable Probes, and then select Enable All Probes In View.

NOTE

You might receive a warning after performing this action. This is a normal result, as some of the probes require additional configuration.

5 Select DDM Filter.

You can either create a new DDM Filter or edit the existing DDM Default Filter.

6 Apply the DDM Filter to enhanced and simple events. Choose to log all event types.

7 Depending on the environment, you can choose to apply the filter to all servers in a domain or only to specific servers.

8 Click Save. Close when finished.

9 Expand the Event Handlers tree and select Event Handlers By Server.

10 Select New Event Handler.

11 Configure the following parameters:

- Basic - Servers to monitor: Choose to monitor either all servers in the domain or only specific servers.
- Basic - Notification trigger: Any event that matches the criteria.
- Event - Criteria to match: Events can be any type.
- Event - Criteria to match: Events must be one of these priorities (Check all the boxes).
- Event - Criteria to match: Events can have any message.
- Action - Notification method: SNMP Trap.
- Action - Enablement: Enable this notification.

12 Click Save. Close when finished.

You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM does not automatically discover incoming syslog events from Huawei AR Series Routers.

If your events are not automatically discovered, you must manually create a log source from the **Admin** tab in SIEM.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select **IBM Lotus Domino**.

6 From the Protocol Configuration list, select **SNMPv2**.

7 Configure the following values:

Table 95: SNMPv2 protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the SNMPv2 event source. IP addresses or hostnames are recommended as they allow SIEM to identify a log file to a unique event source.
Community	Type the SNMP community name required to access the system containing SNMP events.
Include OIDs in Event Payload	Clear the value from this check box. When selected, this option constructs SNMP events with name-value pairs instead of the standard event payload format.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

IBM Fiberlink Maas360

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

IBM Proventia Management SiteProtector

The IBM Proventia® Management SiteProtector™ DSM for SIEM accepts SiteProtector events by polling the SiteProtector database.

The DSM allows SIEM to record Intrusion Prevention System (IPS) events and audit events directly from the IBM SiteProtector database.

NOTE

The IBM Proventia Management SiteProtector DSM requires the latest JDBC Protocol to collect audit events.

The IBM Proventia Management SiteProtector DSM for SIEM can accept detailed SiteProtector events by reading information from the primary SensorData1 table. The SensorData1 table is generated with information from several other tables in the IBM SiteProtector database. SensorData1 remains the primary table for collecting events.

IDP events include information from SensorData1, along with information from the following tables:

- SensorDataAVP1
- SensorDataReponse1

Audit events include information from the following tables:

- AuditInfo
- AuditTrail

Audit events are not collected by default and make a separate query to the AuditInfo and AuditTrail tables when you select the **Include Audit Events** check box. For more information about your SiteProtector database tables, see your vendor documentation.

Before you configure SIEM to integrate with SiteProtector, we recommend you create a database user account and password in SiteProtector for SIEM. Your SIEM user must have read permissions for the SensorData1 table, which stores SiteProtector events. The JDBC - SiteProtector protocol allows SIEM to log in and poll for events from the database. Creating a SIEM account is not required, but it is recommended for tracking and securing your event data.

NOTE

Ensure that no firewall rules are blocking the communication between the SiteProtector console and SIEM.

Configure a Log Source

To configure SIEM to poll for IBM SiteProtector events:

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the **Log Source Type** list, select IBM Proventia Management SiteProtector.

6 Using the Protocol Configuration list, select JDBC - SiteProtector.

7 Configure the following values:

Table 96: JDBC - SiteProtector protocol parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. The log source identifier must be defined in the following format: `<database>@<hostname>` Where: `<database>` is the database name, as defined in the Database Name parameter. The database name is a required parameter. `<hostname>` is the hostname or IP address for the log source as defined in the IP or Hostname parameter. The hostname is a required parameter. The log source identifier must be unique for the log source type.
Database Type	From the list, select **MSDE** as the type of database to use for the event source.
Database Name	Type the name of the database to which you want to connect. The default database name is **RealSecureDB**.
IP or Hostname	Type the IP address or hostname of the database server.

Table 96: JDBC - SiteProtector protocol parameters (Continued)

Parameter	Description
Port	Type the port number used by the database server. The default that is displayed depends on the selected Database Type. The valid range is 0 to 65536. The default for MSDE is port 1433. The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections enabled to communicate with SIEM. The default port number for all options include: • **MSDE** - 1433 • **Postgres** - 5432 • **MySQL** - 3306 • **Oracle** - 1521 • **Sybase** - 1521 **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the database username. The username can be up to 255 alphanumeric characters in length. The username can also include underscores (_).
Password	Type the database password. The password can be up to 255 characters in length.
Confirm Password	Confirm the password to access the database.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Windows Authentication Domain. Otherwise, leave this field blank. The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.).
Database Instance	If you select MSDE as the Database Type and you have multiple SQL server instances on one server, define the instance to which you want to connect. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type the name of the view that includes the event records. The default table name is `SensorData1.`
AVP View Name	Type the name of the view that includes the event attributes. The default table name is `SensorDataAVP`.
Response View Name	Type the name of the view that includes the response events. The default table name is `SensorDataResponse`.

Table 96: JDBC - SiteProtector protocol parameters (Continued)

Parameter	Description
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `SensorDataRowID` to identify new events added between queries to the table.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
Use Named Pipe Communication	If you select MSDE as the Database Type, select this check box to use an alternative method to a TCP/IP port connection. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.
Include Audit Events	Select this check box to collect audit events from IBM SiteProtector. By default, this check box is clear.
Use NTLMv2	Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Use SSL	Select this check box if your connection supports SSL communication.
Log Source Language	Select the language of the log source events.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

The configuration is complete.

IBM ISS Proventia

The IBM Integrated Systems Solutions® (ISS) Proventia DSM for SIEM records all relevant IBM Proventia® events using SNMP.

Procedure

1 In the Proventia Manager user interface navigation pane, expand the System node.

2 Select System.

3 Select Services.
The Service Configuration page is displayed.

4 Click the SNMP tab.

5 Select SNMP Traps Enabled.

6 In the **Trap Receiver** field, type the IP address of your SIEM you wish to monitor incoming SNMP traps.

7 In the **Trap Community** field, type the appropriate community name.

8 From the **Trap Version** list, select the trap version.

9 Click Save Changes.

You are now ready to configure SIEM to receive SNMP traps.

To configure SIEM to receive events from an ISS Proventia device:

u From the **Log Source Type** list, select **IBM Proventia Network Intrusion Prevention System (IPS)**.

For information on configuring SNMP in the SIEM, see the *SIEM Log Sources User Guide*. For more information about your ISS Proventia device, see your vendor documentation.

IBM RACF

SIEM includes two options for integrating event from IBM RACF®:

- Integrating IBM RACF with SIEM Using IBM Security zSecure on page 256
- Integrate IBM RACF with SIEM Using Audit Scripts on page 261

Integrating IBM RACF with SIEM Using IBM Security zSecure

The IBM RACF DSM allows you to integrate events from an IBM z/OS® mainframe using IBM Security zSecure™.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows SIEM to retrieve the events on the schedule you have defined.

To integrate IBM RACF LEEF events:

1 Confirm your installation meets any prerequisite installation requirements. For more information, see Before You Begin on page 257.

2 Configure your IBM z/OS image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

3 Create a log source in SIEM for IBM RACF to retrieve your LEEF formatted event logs. For more information, see Creating an IBM RACF Log Source in SIEM on page 257.

4 Optional. Create a custom event property for IBM RACF in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.
  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Creating an IBM RACF Log Source in SIEM

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **IBM Resource Access Control Facility (RACF)**.

7 From the **Protocol Configuration** list, select **Log File**.

8 Configure the following values:

Table 97: IBM RACF log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM RACF log source. This allows events to be identified at the image or location level in your network that your users can identify.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.

Table 97: IBM RACF log file protocol parameters (Continued)

Parameter	Description
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern RACF.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: `RACF.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.

Table 97: IBM RACF log file protocol parameters (Continued)

Parameter	Description
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The IBM RACF configuration is complete. If your IBM RACF requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Integrate IBM RACF with SIEM Using Audit Scripts

The IBM Resource Access Control Facility (RACF®) DSM for SIEM allows you to integrate with an IBM z/OS mainframe using IBM RACF for auditing transactions.

SIEM records all relevant and available information from the event.

NOTE

zSecure integration is the only integration that provides custom events to the log source. Custom events may be displayed even when you collect events by using the Native QEXRACF integration.

To integrate the IBM RACF events into SIEM:

1 The IBM mainframe system records all security events as Service Management Framework (SMF) records in a live repository.

2 At midnight, the IBM RACF data is extracted from the live repository using the SMF dump utility. The RACFICE utility IRRADU00 (an IBM utility) creates a log file containing all of the events and fields from the previous day in a SMF record format.

3 The QEXRACF program pulls data from the SMF formatted file, as described above. The program only pulls the relevant events and fields for SIEM and writes that information in a condensed format for compatibility. The information is also saved in a location accessible by SIEM.

4 SIEM uses the log file protocol source to pull the QEXRACF output file and retrieves the information on a scheduled basis. SIEM then imports and process this file.

Configure IBM RACF to Integrate with SIEM

To integrate an IBM mainframe RACF with SIEM:

1 From the Extreme Networks Support Portal (http://support.extremenetworks.com), download the following compressed file:
`qexracf_bundled.tar.gz`

2 On a Linux-based operating system, extract the file:
`tar -zxvf qexracf_bundled.tar.gz`
The following files are contained in the archive:
`qexracf_jcl.txt`
`qexracfloadlib.trs`
`qexracf_trsmain_JCL.txt`

3 Load the files onto the IBM mainframe using any terminal emulator file transfer method.
Upload the `qexracf_trsmain_JCL.txt` and `qexracf_jcl.txt` files using the TEXT protocol.
Upload the `QexRACF loadlib.trs` file using binary mode and append to a pre-allocated data set. The `QexRACF loadlib.trs` file is a tersed file containing the executable (the mainframe program QEXRACF). When you upload the .trs file from a workstation, pre-allocate a file on the mainframe with the following DCB attributes:

DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

4 Customize the `qexracf_trsmain_JCL.txt` file according to your installation-specific requirements.

The `qexracf_trsmain_JCL.txt` file uses the IBM utility Trsmain to uncompress the program stored in the `QexRACF loadlib.trs` file.

An example of the `qexracf_trsmain_JCL.txt` file includes:

```
//TRSMAIN    JOB (yourvalidjobcard),Q1labs,
//   MSGCLASS=V
//DEL      EXEC PGM=IEFBR14
//D1      DD    DISP=(MOD,DELETE),DSN=<yourhlq>.QEXRACF.TRS
//          UNIT=SYSDA,
//          SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT   DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE      DD DISP=SHR,DSN=<yourhlq>.QEXRACF.TRS
//OUTFILE    DD DISP=(NEW,CATLG,DELETE),
//             DSN=<yourhlq>.LOAD,
//          SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

You must update the file with your installation specific information for parameters, such as, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The .trs input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the QEXRACF program as a member.

5 You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in the LINKLST. The program does not require authorization.

6 After uploading, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct dataset name of the library that will contain the program.

7 The `qexracf_jcl.txt` file is a text file containing a sample JCL deck to provide you with the necessary JCL to run the IBM IRRADU00 utility. This allows SIEM to obtain the necessary IBM RACF events. Configure the job card to meet your local standards.

An example of the `qexracf_jcl.txt` file includes:

```
//QEXRACF   JOB (<your valid jobcard>),Q1LABS,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXRACF JCL version 1.0   April 2009
//*
//*************************************************************
//*     Change below dataset names to sites specific datasets
names    *
//*************************************************************
//SET1   SET   SMFOUT='<your hlq>.CUSTNAME.IRRADU00.OUTPUT',
//               SMFIN='<your SMF dump ouput dataset>',
//            QRACFOUT='<your hlq>.QEXRACF.OUTPUT'
```

```
//*************************************************************
//*     Delete old datasets *
//*************************************************************
//DEL     EXEC  PGM=IEFBR14
//DD2     DD    DISP=(MOD,DELETE),DSN=&QRACFOUT,
//         UNIT=SYSDA,
//         SPACE=(TRK,(1,1)),
//         DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//*     Allocate new dataset *
//*************************************************************
//ALLOC   EXEC  PGM=IEFBR14
//DD1     DD    DISP=(NEW,CATLG),DSN=&QRACFOUT,
//         SPACE=(CYL,(1,10)),UNIT=SYSDA,
//         DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute IBM IRRADU00 utility to extract RACF smf records *
//*************************************************************
//IRRADU00 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=*
//OUTDD     DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
//               DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
//               UNIT=SYSALLDA
//SMFDATA   DD DISP=SHR,DSN=&SMFIN
//SMFOUT    DD DUMMY
//SYSIN     DD *
     INDD(SMFDATA,OPTIONS(DUMP))
     OUTDD(SMFOUT,TYPE(30:83))
     ABEND(NORETRY)
     USER2(IRRADU00)
     USER3(IRRADU86)
/*
//EXTRACT   EXEC PGM=QEXRACF,DYNAMNBR=10,
//           TIME=1440
//*STEPLIB    DD   DISP=SHR,DSN=<the loadlib containing the
QEXRACF program if not in LINKLST>
//SYSTSIN    DD   DUMMY
//SYSTSPRT   DD   SYSOUT=*
//SYSPRINT   DD   SYSOUT=*
//RACIN       DD   DISP=SHR,DSN=&SMFOUT
//RACOUT     DD   DISP=SHR,DSN=&QRACFOUT
//
//*************************************************************
//* FTP Output file from C program (Qexracf) to an FTP server *
//* QRadar will go to that FTP Server to get file             *
//* Note you need to replace <user>, <password>,<serveripaddr>*
//* <THEIPOFTHEMAINFRAMEDEVICE> and <QEXRACFOUTDSN>           *
//*************************************************************
//*FTP   EXEC   PGM=FTP,REGION=3800K
//*INPUT   DD *
//*<FTPSERVERIPADDR>
```

```
//*<USER>
//*<PASSWORD>
//*ASCII
//*PUT '<QEXRACFOUTDSN>' /<THEIPOFTHEMAINFRAMEDEVICE>/
<QEXRACFOUTDSN>
//*QUIT
//*OUTPUT    DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
//*
//*
```

8 After the output file is created, you must send this file to an FTP server. This ensures that every time you run the utility, the output file is sent to a specific FTP server for processing at the end of the above script. If the z/OS platform is configured to serve files through FTP or SFTP, or allow SCP, then no interim server is required and SIEM can pull those files directly from the mainframe. If an interim FTP server is needed, SIEM requires a unique IP address for each IBM RACF log source or they will be joined as one system.

Create an IBM RACF Log Source

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM RACF with z/OS writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your event files and a polling interval.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **IBM Resource Access Control Faclilty (RACF)**.

7 From the **Protocol Configuration** list, select **Log File**.

8 Configure the following values:

Table 98: IBM RACF log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM RACF log source. This allows events to be identified at the image or location level in your network that your users can identify.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 98: IBM RACF log file protocol parameters (Continued)

Parameter	Description
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select the transfer mode you want to apply to this log source: • **Binary** - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • **ASCII** - Select ASCII for log sources that require an ASCII FTP file transfer.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.

Table 98: IBM RACF log file protocol parameters (Continued)

Parameter	Description
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM system for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The IBM RACF configuration is complete. If your IBM RACF requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

IBM DB2

SIEM has two options for integrating events from IBM DB2®:

- Integrating IBM DB2 with LEEF Events on page 268
- Integrating IBM DB2 Audit Events on page 272

Integrating IBM DB2 with LEEF Events

The IBM DB2 DSM allows you to integrate DB2 events in LEEF format from an IBM z/OS® mainframe using IBM Security zSecure®.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows you to retrieve the events on the schedule you have defined.

To integrate IBM DB2 events:

1 Confirm your installation meets any prerequisite installation requirements. For more information, see Before You Begin on page 268.

2 Configure your IBM DB2 image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

3 Create a log source in SIEM for IBM DB2 to retrieve your LEEF formatted event logs. For more information, see Creating a Log Source on page 269.

4 Optional. Create a custom event property for IBM DB2 in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your IBM DB2 z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.

  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring

zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Creating a Log Source

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **IBM DB2**.

7 From the **Protocol Configuration** list, select **Log File**.

8 Configure the following values:

Table 99: IBM DB2 log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM DB2 log source. This allows events to be identified at the image or location level in your network that your users can identify.

Table 99: IBM DB2 log file protocol parameters (Continued)

Parameter	Description
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.

Table 99: IBM DB2 log file protocol parameters (Continued)

Parameter	Description
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern DB2.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: `DB2.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.

Table 99: IBM DB2 log file protocol parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

The IBM DB2 LEEF configuration is complete. If your configuration requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Integrating IBM DB2 Audit Events

The IBM DB2 DSM allows you to integrate your DB2 audit logs into SIEM for analysis.

The db2audit command creates a set of comma-delimited text files with a .del extension that defines the scope of audit data for SIEM when auditing is configured and enabled. Comma-delimited files created by the db2audit command include:

- audit.del
- checking.del
- context.del
- execute.del
- objmaint.del
- secmaint.del
- sysadmin.del
- validate.del

To integrate the IBM DB2 DSM with SIEM, you must:

1 Use the db2audit command to ensure the IBM DB2 records security events. See your IBM DB2 vendor documentation for more information.

2 Extract the DB2 audit data of events contained in the instance to a log file, depending on your version of IBM DB2:

- If you are using DB2 v9.5 and later, see Extract Audit Data: DB2 v9.5 and Later on page 273.
- If you are using DB2 v8.x to v9.4, see Extract Audit Data: DB2 v8.x to v9.4 on page 274

3 Use the log file protocol source to pull the output instance log file and send that information back to SIEM on a scheduled basis. SIEM then imports and processes this file. See Creating a Log Source for IBM DB2 on page 275.

NOTE

The IBM DB2 DSM does not support the IBM z/OS mainframe operating system.

Extract Audit Data: DB2 v9.5 and Later

To extract audit data when you are using IBM DB2 v9.5 and later:

1 Log into a DB2 account with SYSADMIN privilege.

2 Move the audit records from the database instance to the audit log:

```
db2audit flush
```

For example, the flush command response might resemble the following:

```
AUD00001 Operation succeeded.
```

3 Archive and move the active instance to a new location for future extraction:

```
db2audit archive
```

For example, an archive command response might resemble the following:

```
Node AUD Archived or Interim Log File
Message
---- --- ----------------------------
0 AUD00001 dbsaudit.instance.log.0.20091217125028
AUD00001 Operation succeeded.
```

NOTE

In DB2 v9.5 and later, the archive command replaces the prune command. The archive command moves the active audit log to a new location, effectively pruning all non-active records from the log. An archive command must be complete before an extract can be performed.

4 Extract the data from the archived audit log and write the data to .del files:

```
db2audit extract delasc from files
db2audit.instance.log.0.200912171528
```

For example, an archive command response might resemble the following:

AUD00001 Operation succeeded.

NOTE

Double-quotation marks (“) are used as the default text delimiter in the ASCII files, do not change the delimiter.

5 Move the .del files to a storage location where SIEM can pull the file. The movement of the comma-delimited (.del) files should be synchronized with the file pull interval in SIEM.

You are now ready to configure SIEM to receive DB2 log files. See Creating a Log Source for IBM DB2 on page 275.

Extract Audit Data: DB2 v8.x to v9.4

To extract audit data when you are using IBM DB2 v8.x to v9.4.

1 Log into a DB2 account with SYSADMIN privilege.

2 Type the following start command to audit a database instance:
`db2audit start`
For example, the start command response might resemble the following:
AUD00001 Operation succeeded.

3 Move the audit records from the instance to the audit log:
`db2audit flush`
For example, the flush command response might resemble the following:
AUD00001 Operation succeeded.

4 Extract the data from the archived audit log and write the data to .del files:
`db2audit extract delasc`
For example, an archive command response might resemble the following:
AUD00001 Operation succeeded.

NOTE

Double-quotation marks (“) are used as the default text delimiter in the ASCII files, do not change the delimiter.

5 Remove non-active records:
`db2audit prune all`

6 Move the .del files to a storage location where SIEM can pull the file. The movement of the comma-delimited (.del) files should be synchronized with the file pull interval in SIEM.
You are now ready to create a log source in SIEM to receive DB2 log files.

Creating a Log Source for IBM DB2

A log file protocol source allows SIEM to retrieve archived log files from a remote host.

The IBM DB2 DSM supports the bulk loading of log files using the log file protocol source. When configuring your IBM DB2 to use the log file protocol, make sure the hostname or IP address configured in the IBM DB2 system is the same as configured in the Remote Host parameter in the Log File protocol configuration. For more information, see the *SIEM Log Sources User Guide*.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **IBM DB2**.

8 From the **Protocol Configuration** list, select **Log File**.

9 Configure the following values:

Table 100: IBM DB2 log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM DB2 log source. This allows events to be identified at the image or location level in your network that your users can identify.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.

Table 100: IBM DB2 log file protocol parameters (Continued)

Parameter	Description
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect comma-delimited files ending with .del, type the following: .*.del Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	From the list, select **ASCII** for comma-delimited, text, or ASCII log sources that require an ASCII FTP file transfer mode. This option only displays if you select FTP as the Service Type.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.

Table 100: IBM DB2 log file protocol parameters (Continued)

Parameter	Description
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **None**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The configuration for IBM DB2 is complete.

IBM Privileged Session Recorder

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

IBM Security Network IPS

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

IBM SmartCloud Orchestrator

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

IBM WebSphere Application Server

The IBM WebSphere® Application Server DSM for SIEM accepts events using the log file protocol source.

SIEM records all relevant application and security events from the WebSphere Application Server log files.

Configuring IBM WebSphere

You can configure IBM WebSphere Application Server events for SIEM.

Procedure

1 Using a web browser, log in to the IBM WebSphere administrative console.

2 Click **Environment > WebSphere Variables**.

3 Define Cell as the Scope level for the variable.

4 Click New.

5 Configure the following values:

- Name - Type a name for the cell variable.
- Description - Type a description for the variable (optional).
- Value - Type a directory path for the log files.
  For example:
  `{QRADAR_LOG_ROOT} = /opt/IBM/WebSphere/AppServer/profiles/Custom01/logs/QRadar`

You must create the target directory specified in step 5 before proceeding.

6 Click OK.

7 Click Save.

8 You must restart the WebSphere Application Server to save the configuration changes.

NOTE

If the variable you created affects a cell, you must restart all WebSphere Application Servers in the cell before you continue.

If the variable you created affects a cell, you must restart all WebSphere Application Servers in the cell before you continue.

You are now ready to customize the logging option for the IBM WebSphere Application Server DSM.

Customizing the Logging Option

You must customize the logging option for each application server WebSphere uses and change the settings for the JVM Logs (Java Virtual Machine logs).

Procedure

1 Select **Servers > Application Servers**.

2 Select your WebSphere Application Server to load the server properties.

3 Select **Logging and Tracing > JVM Logs**.

4 Configure a name for the JVM log files.

For example:

System.Out log file name:

```
${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemOut.log
```

System.Err log file name:

```
${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemErr.log
```

5 Select a time of day to save the log files to the target directory.

6 Click OK.

7 You must restart the WebSphere Application Server to save the configuration changes.

NOTE

If the JVM Logs changes affect the cell, you must restart all of the WebSphere Application Servers in the cell before you continue.

You are now ready to import the file into SIEM using the Log File Protocol.

Create a Log Source

The log file protocol allows SIEM to retrieve archived log files from a remote host. The IBM WebSphere Application Server DSM supports the bulk loading of log files using the log file protocol source.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select IBM WebSphere Application Server.

8 Using the Protocol Configuration list, select **Log File**.

9 Configure the following values:

Table 101: Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify your IBM WebSphere Application Server as an event source in SIEM. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple IBM WebSphere Application Serves that provides logs to a file repository, you should specify the IP address or hostname of the device that created the event log. This allows events to be identified at the device level in your network, instead of identifying the file repository.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of your IBM WebSphere Application Server storing your event log files.

Table 101: Log File Parameters (Continued)

Parameter	Description
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. The **Remote Password** field is ignored when you provide an SSH Key File.
Remote Directory	Type the directory location on the remote host to the cell and file path you specified in Step 5. This is the directory you created containing your IBM WebSphere Application Server event files. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your JVM logs in Step 4. For example, to collect system logs, type the following: `System.*\.log` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

Table 101: Log File Parameters (Continued)

Parameter	Description
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when using ASCII as the FTP Transfer Mode.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, 2H if you want the directory to be scanned every 2 hours. The default is 1H. **NOTE:** We recommend when scheduling a Log File protocol, you select a recurrence time for the log file protocol shorter than the scheduled write interval of the WebSphere Application Server log files. This ensures that WebSphere events are collected by the Log File Protocol before a the new log file overwrites the old event log.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed. Files that have been previously processed are not processed a second time. This check box only applies to FTP and SFTP Service Types.

Table 101: Log File Parameters (Continued)

Parameter	Description
Change Local Directory?	Select this check box to define the local directory on your SIEM that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select WebSphere Application Server. The Event Generator applies additional processing, which is specific to retrieved event files for IBM WebSphere Application Server events.

10 Click Save.

11 On the Admin tab, click Deploy Changes.

The configuration is complete. For more information about IBM WebServer Application Server, see your vendor documentation.

IBM Informix Audit

The IBM Informix® Audit DSM allows SIEM to integrate IBM Informix audit logs into SIEM for analysis.

SIEM retrieves the IBM Informix archived audit log files from a remote host using the Log File protocol configuration. SIEM records all configured IBM Informix Audit events.

For more information about IBM Informix auditing configuration, see your IBM Informix documentation at the following website: http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.tfg.doc/tfg26.htm

When configuring your IBM Informix to use the log file protocol, make sure the hostname or IP address configured in the IBM Informix is the same as configured in the Remote Host parameter in the Log File protocol configuration.

You are now ready to configure the log source and protocol in SIEM:

1 To configure SIEM to receive events from an IBM Informix device, you must select the IBM Informix Audit option from the Log Source Type list.

2 To configure the log file protocol, you must select the Log File option from the Protocol Configuration list.

3 We recommend that you use a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).

For more information on configuring log sources and protocols, see the *SIEM Log Sources User Guide*.

IBM IMS

The IBM Information Management System (IMS™) DSM for SIEM allows you to use an IBM mainframe to collect events and audit IMS database transactions.

Configuration Overview

To integrate IBM IMS events with SIEM, you must download scripts that allow IBM IMS events to be written to a log file.

Overview of the event collection process:

1 The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.

2 The IBM IMS data is extracted from the live repository using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.

3 The `qeximsloadlib.trs` program pulls data from the SMF formatted file. The `qeximsloadlib.trs` program only pulls the relevant events and fields for SIEM and writes that information in a condensed format for compatibility. The information is saved in a location accessible by SIEM.

4 SIEM uses the log file protocol source to retrieve the output file information for SIEM on a scheduled basis. SIEM then imports and processes this file.

Configure IBM IMS

To integrate IBM IMS with SIEM:

Procedure

1 From the Extreme Networks Support Portal (http://support.extremenetworks.com), download the following compressed file:
`QexIMS_bundled.tar.gz`

2 On a Linux-based operating system, extract the file:
`tar -zxvf qexims_bundled.tar.gz`
The following files are contained in the archive:
qexims_jcl.txt - Job Control Language file
qeximsloadlib.trs - Compressed program library (requires IBM TRSMAIN)
qexims_trsmain_JCL.txt - Job Control Language for TRSMAIN to decompress the .trs file

3 Load the files onto the IBM mainframe using the following methods:
   a Upload the sample `qexims_trsmain_JCL.txt` and `qexims_jcl.txt` files using the TEXT protocol.
   b Upload the `qeximsloadlib.trs` file using BINARY mode transfer and append to a pre-allocated data set. The `qeximsloadlib.trs` file is a tersed file containing the executable (the mainframe program QexIMS). When you upload the .trs file from a workstation, pre-allocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL= 1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

NOTE

QexIMS is a small C mainframe program that reads the output of the IMS log file (EARLOUT data) line by line. QexIMS adds a header to each record containing event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for SIEM and the blank suppression reduces network traffic to SIEM. This program does not consume CPU or I/O disk resources.

4 Customize the `qexims_trsmain_JCL.txt` file according to your installation specific information for parameters.

For example, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The `qexims_trsmain_JCL.txt` file uses the IBM utility TRSMAIN to extract the program stored in the `qeximsloadlib.trs` file.

An example of the `qexims_trsmain_JCL.txt` file includes:

```
//TRSMAIN    JOB (yourvalidjobcard),Q1labs,
//   MSGCLASS=V
//DEL      EXEC PGM=IEFBR14
//D1      DD    DISP=(MOD,DELETE),DSN=<yourhlq>.QEXIMS.TRS
//          UNIT=SYSDA,
//          SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT   DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE     DD DISP=SHR,DSN=<yourhlq>.QEXIMS.TRS
//OUTFILE    DD DISP=(NEW,CATLG,DELETE),
//             DSN=<yourhlq>.LOAD,
//          SPACE=(CYL,(1,1,5),RLSE),UNIT=SYSDA
//
```

The .trs input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the **`qexims`** program as a member.

5 You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.

6 The **`qexims_jcl.txt`** file is a text file containing a sample JCL. You must configure the job card to meet your configuration.

The **`qexims_jcl.txt`** sample file includes:

```
//QEXIMS  JOB  (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXIMS  JCL  VERSION  1.0   FEBRUARY  2011
//*
//*************************************************************
//* Change  dataset  names  to  site  specific  dataset  names  *
```

```
//*************************************************************
//SET1   SET   IMSOUT='Q1JACK.QEXIMS.OUTPUT',
//               IMSIN='Q1JACK.QEXIMS.INPUT.DATA'
//*************************************************************
//*     Delete old datasets *
//*************************************************************
//DEL      EXEC  PGM=IEFBR14
//DD1      DD    DISP=(MOD,DELETE),DSN=&IMSOUT,
//          UNIT=SYSDA,
//          SPACE=(CYL,(10,10)),
//          DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//*     Allocate new dataset
//*************************************************************
//ALLOC   EXEC  PGM=IEFBR14
//DD1      DD    DISP=(NEW,CATLG),DSN=&IMSOUT,
//          SPACE=(CYL,(21,2)),
//          DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//EXTRACT   EXEC  PGM=QEXIMS,DYNAMNBR=10,
//            TIME=1440
//STEPLIB    DD   DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN    DD   DUMMY
//SYSTSPRT   DD   SYSOUT=*
//SYSPRINT   DD   SYSOUT=*
//IMSIN      DD   DISP=SHR,DSN=&IMSIN
//IMSOUT     DD   DISP=SHR,DSN=&IMSOUT
//*FTP   EXEC   PGM=FTP,REGION=3800K
//*INPUT   DD *
//*<target server>
//*<USER>
//*<PASSWORD>
//*ASCII
//*PUT '<IMSOUT>' /TARGET DIRECTORY>/<IMSOUT>
//*QUIT
//*OUTPUT    DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
//*
```

7 After the output file is created, you must choose one of the following options:

a Schedule a job to transfer the output file to an interim FTP server.

Each time the job completes, the output file is forwarded to an intermin FTP server. You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

For example:

```
//*FTP EXEC PGM=FTP,REGION=3800K
//*INPUT   DD *
//*<target server>
//*<USER>
//*<PASSWORD>
//*ASCII
```

```
//*PUT '<IMSOUT>' /TARGET DIRECTORY>/<IMSOUT>
//*QUIT
//*OUTPUT    DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
```

Where:

<target server> is the IP address or host name of the interim FTP server to receive the output file.

<USER> is the user name required to access the interim FTP server.

<PASSWORD> is the password required to access the interim FTP server.

<IMSOUT> is the name of the output file saved to the interim FTP server.

For example:

```
PUT 'Q1JACK.QEXIMS.OUTPUT.C320' /192.168.1.101/IMS/
QEXIMS.OUTPUT.C320
```

NOTE

You must remove commented lines beginning with //* for the script to properly forward the output file to the interim FTP server.

You are now ready to configure the Log File protocol.

b Schedule SIEM to retrieve the output file from IBM IMS.

If the mainframe is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is required and SIEM can pull the output file directly from the mainframe. The following text must be commented out using //* or deleted from the **qexims_jcl.txt** file:

```
//*FTP   EXEC   PGM=FTP,REGION=3800K
//*INPUT   DD *
//*<target server>
//*<USER>
//*<PASSWORD>
//*ASCII
//*PUT '<IMSOUT>' /TARGET DIRECTORY>/<IMSOUT>
//*QUIT
//*OUTPUT    DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
```

You are now ready to configure the Log File protocol.

Configure a Log Source

A log file protocol source allows SIEM to retrieve archived log files from a remote host.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 From the Log Source Type list, select IBM IMS.

5 Using the Protocol Configuration list, select Log File.

6 Configure the following parameters:

Table 102: Log File protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service types requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or hostname of the IBM IMS system.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 to 65535.
Remote User	Type the username necessary to log in to your IBM IMS system. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to your IBM IMS system.
Confirm Password	Confirm the Remote Password to log in to your IBM IMS system.
SSH Key File	If you select SCP or SFTP from the **Service Type** field you can define a directory path to an SSH private key file. The SSH Private Key File allows you to ignore the **Remote Password** field.
Remote Directory	Type the directory location on the remote host from which the files are retrieved. By default, the newauditlog.sh script writes the human-readable logs files to the **/var/log/** directory.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. For example, if you want to retrieve all files in the <starttime>.<endtime>.<hostname>.log format, use the following entry: `\d+\.\d+\.\w+\.log`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

Table 102: Log File protocol parameters (Continued)

Parameter	Description
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the **Processor** field and **LINEBYLINE** the **Event Generator** field when using ASCII as the transfer mode.
SCP Remote File	If you select SCP as the Service Type, you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File(s) parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a .zip, .gzip, .tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your SIEM system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LINEBYLINE.

7 Click **Save**.

The configuration is complete. Events that are retrieved using the log file protocol are displayed on the **Log Activity** tab of SIEM.

IBM Guardium

IBM Guardium® is a database activity and audit tracking tool for system administrators to retrieve detailed auditing events across database platforms.

NOTE

These instructions require that you install the 8.2p45 fix for InfoSphere Guardium. For more information on this fix, see the Fix Central website at www.ibm.com/support/fixcentral/.

Supported Event Types

SIEM collects informational, error, alert, and warnings from IBM Guardium using syslog. SIEM receives IBM Guardium Policy Builder events in the Log Event Extended Format (LEEF).

SIEM can only automatically discover and map events the default policies that ship with IBM Guardium. Any user configured events require are displayed as unknowns in SIEM and you must manually map the unknown events.

Configuration Overview

The following list outlines the process required to integrate IBM Guardium with SIEM.

1 Create a syslog destination for policy violation events. For more information, see Creating a Syslog Destination for Events on page 291.

2 Configure your existing policies to generate syslog events. For more information, see Configuring Policies to Generate Syslog Events on page 292.

3 Install the policy on IBM Guardium. For more information, see Installing an IBM Guardium Policy on page 293.

4 Configure the log source in SIEM. For more information, see Configure a Log Source on page 293.

5 Identify and map unknown policy events in SIEM. For more information, see Creating an Event Map for IBM Guardium Events on page 294.

Creating a Syslog Destination for Events

To create a syslog destination for these events on IBM Guardium, you must log in to the command-line interface (CLI) and define the IP address for SIEM.

Procedure

1 Using SSH, log in to IBM Guardium as the root user.

Username: `<username>`

Password: `<password>`

2 Type the following command to configure the syslog destination for informational events:

`store remote add daemon.info <IP address>:<port> <tcp|udp>`

For example, store remote add daemon.info 10.10.1.1:514 tcp

Where:

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<port>` is the syslog port number used to communicate to the SIEM Console or Event Collector.

`<tcp|udp>` is the protocol used to communicate to the SIEM Console or Event Collector.

3 Type the following command to configure the syslog destination for warning events:

`store remote add daemon.warning <IP address>:<port> <tcp|udp>`

Where:

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<port>` is the syslog port number used to communicate to the SIEM Console or Event Collector.

`<tcp|udp>` is the protocol used to communicate to the SIEM Console or Event Collector.

4 Type the following command to configure the syslog destination for error events:

`store remote add daemon.err <IP address>:<port> <tcp|udp>`

Where:

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<port>` is the syslog port number used to communicate to the SIEM Console or Event Collector.

`<tcp|udp>` is the protocol used to communicate to the SIEM Console or Event Collector.

5 Type the following command to configure the syslog destination for alert events:

`store remote add daemon.alert <IP address>:<port> <tcp|udp>`

Where:

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<port>` is the syslog port number used to communicate to the SIEM Console or Event Collector.

`<tcp|udp>` is the protocol used to communicate to the SIEM Console or Event Collector.

You are now ready to configure a policy for IBM InfoSphere Guardium.

Configuring Policies to Generate Syslog Events

Policies in IBM Guardium are responsible for reacting to events and forwarding the event information to SIEM.

Procedure

1 Click the **Tools** tab.

2 From the left-hand navigation, select **Policy Builder**.

3 From the Policy Finder pane, select an existing policy and click **Edit Rules**.

4 Click **Edit this Rule individually**.
The Access Rule Definition is displayed.

5 Click **Add Action**.

6 From the **Action** list, select one of the following alert types:

- **Alert Per Match** - A notification is provided for every policy violation.
- **Alert Daily** - A notification is provided the first time a policy violation occurs that day.
- **Alert Once Per Session** - A notification is provided per policy violation for unique session.
- **Alert Per Time Granularity** - A notification is provided per your selected time frame.

7 From the **Message Template** list, select **SIEM**.

8 From **Notification Type**, select **SYSLOG**.

9 Click **Add**, then click **Apply**.

10 Click **Save**.

11 Repeat Step 2 to Step 10 for all rules within the policy you want to forward to SIEM.
For more information on configuring a policy, see your IBM InfoSphere Guardium vendor documentation. After you have configured all of your policies, you are now ready to install the policy on your IBM Guardium system.

NOTE

Due to the configurable policies, SIEM can only automatically discover the default policy events. If you have customized policies that forward events to SIEM, you must manually create a log source to capture those events.

Installing an IBM Guardium Policy

Any new or edited policy in IBM Guardium must be installed before the updated alert actions or rule changes can occur.

Procedure

1 Click the **Administration Console** tab.

2 From the left-hand navigation, select **Configuration > Policy Installation**.

3 From the Policy Installer pane, select a policy you modified in Step 3, Configuring Policies to Generate Syslog Events on page 292.

4 From the drop-down list, select **Install and Override**.

A confirmation is displayed to install the policy to all Inspection Engines.

5 Click **OK**.

For more information on installing a policy, see your IBM InfoSphere Guardium vendor documentation. After you have installed all of your policies, you are ready to configure the log source in SIEM.

Configure a Log Source

SIEM only automatically discovers default policy events from IBM Guardium.

Due to the configurable nature of policies, we recommend that you configure a log source manually for IBM Guardium.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **IBM Guardium**.

8 From the **Protocol Configuration** list, select **Syslog**.

9 Configure the following values:

Table 103: IBM Guardium Syslog Configuration

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the IBM InfoSphere Guardium appliance.

For more information on configuring log sources, see the *SIEM Log Sources Users Guide*.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The IBM Infosphere Guardium configuration is complete.

Creating an Event Map for IBM Guardium Events

Event mapping is required for a number of IBM Guardium events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined SIEM Identifier (QID) map to categorize security events.

You can individually map each event for your device to an event category in SIEM. Mapping events allows SIEM to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for IBM Guardium are categorized as unknown. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

Discovering Unknown Events

As your device forwards events to SIEM, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we recommend you repeat this search until you are comfortable that you have identified the majority of your events.

Procedure

1 Log in to SIEM.

1 Click the **Log Activity** tab.

2 Click **Add Filter**.

3 From the first list, select **Log Source**.

4 From the **Log Source Group** list, select the log source group or **Other**.

Log sources that are not assigned to a group are categorized as Other.

5 From the **Log Source** list, select your IBM Guardium log source.

6 Click **Add Filter**.

The **Log Activity** tab is displayed with a filter for your log source.

7 From the **View** list, select **Last Hour**.

Any events generated by the IBM Guardium DSM in the last hour are displayed. Events displayed as unknown in the Event Name column or Low Level Category column require event mapping in SIEM.

NOTE

You can save your existing search filter by clicking **Save Criteria**.

You are now ready to modify the event map.

Modifying the Event Map

Modifying an event map allows you to manually categorize events to a SIEM Identifier (QID) map. Any event categorized to a log source can be remapped to a new SIEM Identifier (QID).

NOTE

Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1 On the Event Name column, double-click an unknown event for IBM Guardium.

The detailed event information is displayed.

2 Click **Map Event**.

3 From the Browse for QID pane, select any of the following search options to narrow the event categories for a SIEM Identifier (QID):

a From the **High-Level Category** list, select a high-level event categorization.

For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *SIEM Administration Guide*.

b From the **Low-Level Category** list, select a low-level event categorization.

c From the **Log Source Type** list, select a log source type.

The **Log Source Type** list allows you to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, IBM Guardium provides policy events, you might select another product that likely captures similar events.

d To search for a QID by name, type a name in the **QID/Name** field.

The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, policy.

4 Click **Search**.

A list of QIDs are displayed.

5 Select the QID you want to associate to your unknown event.

6 Click **OK**.

SIEM maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by SIEM.

If you update an event with a new SIEM Identifier (QID) map, past events stored in SIEM are not updated. Only new events are categorized with the new QID.

IBM Security Directory Server

The SIEM DSM for IBM Security Directory Server can collect event logs from your IBM Security Directory Server.

The following table identifies the specifications for the IBM Security Directory Server DSM:

Table 104: IBM Security Directory Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM	IBM Security Directory Server
RPM file name	DSM-IBMSecurityDirectoryServer-*build_number*.noarch.rpm
Supported version	6.3.1 and later
Protocol	Syslog (LEEF)
SIEM recorded events	All relevant events
Automatically discovered	Yes
Includes identity	Yes
For more information	http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc_6.3.1%2Fadmin_gd381.htm&path=9_3_4_13_18_3

IBM Security Directory Server Integration Process

To integrate IBM Security Directory Server with SIEM, use the following procedure:

1 If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your SIEM Console:

- DSMCommon RPM
- IBM Security Directory Server RPM

2 Configure each IBM Security Directory Server system in your network to enable communication with SIEM.

For more information, see *Enabling communication between SIEM and IBM Security Directory Server* (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc_6.3.1%2Fadmin_gd381.htm&path=9_3_4_13_18_3)

3 If SIEM does not automatically discover the log source, for each IBM Security Directory Server on your network, create a log source on the SIEM Console.

Related tasks

Manually Installing a DSM on page 4

Configuring an IBM Security Directory Server Log Source in SIEM on page 297

Configuring an IBM Security Directory Server Log Source in SIEM

To collect IBM Security Directory Server events, configure a log source in SIEM.

Before You Begin

Ensure that the `DSM-IBMSecurityDirectoryServer-build_number.noarch.rpm` file is installed and deployed on your SIEM host:

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **IBM Security Directory Server**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

IBM Tivoli Access Manager for e-business

The IBM Tivoli® Access Manager for e-business DSM for SIEM accepts access, audit, and HTTP events forwarded from IBM Tivoli Access Manager.

SIEM collects audit, access, and HTTP events from IBM Tivoli Access Manager for e-business using syslog. Before you can configure SIEM, you must configure Tivoli Access Manager for e-business to forward events to a syslog destination.

Configure Tivoli Access Manager for e-business

You can configure syslog on your Tivoli Access Manager for e-business to forward events.

Procedure

1 Log in to Tivoli Access Manager's IBM Security Web Gateway.

2 From the navigation menu, select **Secure Reverse Proxy Settings > Manage > Reverse Proxy**.

The Reverse Proxy pane is displayed.

3 From the Instance column, select an instance.

4 Click the **Manage** list and select **Configuration > Advanced**.

The text of the WebSEAL configuration file is displayed.

5 Locate the Authorization API Logging configuration.

The remote syslog configuration begins with logcfg. For example,

As an example, to send authorization events to a remote syslog server:
logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>

6 Copy the remote syslog configuration (logcfg) to a new line without the comment (#) marker.

7 Edit the remote syslog configuration.

For example,

```
logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>
logcfg = audit.authn:rsyslog server=<IP address>,port=514,log_id=<log name>
logcfg = http:rsyslog server=<IP address>,port=514,log_id=<log name>
```

Where:

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<Log name>` is the name assigned to the log that is forwarded to SIEM. For example, `log_id=WebSEAL-log`.

8 Click **Submit**.

The Deploy button is displayed in the navigation menu.

9 From the navigation menu, click **Deploy**.

10 Click **Deploy**.

You must restart the reverse proxy instance to continue.

11 From the Instance column, select your instance configuration.

12 Click the **Manage** list and select **Control > Restart**.

A status message is displayed after the restart completes. For more information on configuring a syslog destination, see your IBM Tivoli Access Manager for e-business vendor documentation. You are now ready to configure a log source in SIEM.

Configure a Log Source

SIEM automatically discovers syslog audit and access events, but does not automatically discover HTTP events forwarded from IBM Tivoli Access Manager for e-business.

Since SIEM automatically discovers audit and access events, you are not required to create a log source. However, you can manually create a log source for SIEM to receive IBM Tivoli Access Manager for e-business syslog events. The following configuration steps for creating a log source are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **IBM Tivoli Access Manager for e-business**.

8 From the **Protocol Configuration** list, select **Syslog**.

9 Configure the following values:

Table 105: IBM Tivloi Access Manager for e-business Syslog Configuration

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your IBM Tivoli Access Manager for e-business appliance. The IP address or hostname identifies your IBM Tivoli Access Manager for e-business as a unique event source in SIEM.

For more information on configuring log sources, see the *SIEM Log Sources Users Guide*.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The IBM Tivoli Access Manager for e-business configuration is complete.

IBM z/Secure® Audit

The IBM z/OS® DSM for SIEM allows you to integrate with an IBM z/OS mainframe using IBM Security zSecure® Audit to collect security, authorization, and audit events.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). SIEM retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule SIEM to retrieve events on a polling interval, which allows SIEM to retrieve the events on the schedule you have defined.

To integrate IBM z/OS events from IBM Security zSecure Audit into SIEM:

1 Confirm your installation meets any prerequisite installation requirements. For more information, see Before You Begin on page 300.

2 Configure your IBM z/OS image. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide.

3 Create a log source in SIEM for IBM z/OS to retrieve your LEEF formatted event logs. For more information, see Create an IBM z/OS Log Source on page 300.

4 Optional. Create a custom event property for IBM z/OS in SIEM. For more information, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for SIEM to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between SIEM and your z/OS image.
  After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide.

Create an IBM z/OS Log Source

The Log File protocol allows SIEM to retrieve archived log files from a remote host.

Log files are transferred, one at a time, to SIEM for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM z/OS with zSecure writes log files to a specified directory as gzip archives. SIEM extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. SIEM requires credentials to log in to the system hosting your LEEF formatted event files and a polling interval.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **IBM z/OS**.

8 From the **Protocol Configuration** list, select **Log File**.

9 Configure the following values:

Table 106: z/OS Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM z/OS log source. This allows events to be identified at the image or location level in your network that your users can identify.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 106: z/OS Log File Parameters (Continued)

Parameter	Description
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. IBM z/OS mainframe using IBM Security zSecure Audit writes event files using the pattern zOS.<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: `zOS.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select Binary. The binary transfer mode is required for event files stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.

Table 106: z/OS Log File Parameters (Continued)

Parameter	Description
Processor	From the list, select **gzip**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded to SIEM. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. SIEM examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your SIEM for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The IBM z/OS with IBM zSecure configuration is complete. If your IBM z/OS for zSecure requires custom event properties, see the *SIEM Custom Event Properties for IBM z/OS* technical note.

IBM Tivoli Endpoint Manager

The IBM Tivoli® Endpoint Manager DSM for SIEM accepts system events in Log Extended Event Format (LEEF) retrieved from IBM Tivoli Endpoint Manager.

SIEM uses the Tivoli Endpoint Manager SOAP protocol to retrieve events on a 30 second interval. As events are retrieved the IBM Tivoli Endpoint Manager DSM parses and categorizes the events for SIEM. The SOAP API for IBM Tivoli Endpoint Manager is only available after you have installed with the Web Reports application. The Web Reports application for Tivoli Endpoint Manager is required to retrieve and integrate IBM Tivoli Endpoint Manager system event data with SIEM.

NOTE

SIEM is compatible with IBM Tivoli Endpoint Manager versions 8.2.x. However, we recommend that you update and use the latest version of IBM Tivoli Endpoint Manager that is available.

To integrate IBM Tivoli Endpoint Manager with SIEM, you must manually configure a log source as events from IBM Tivoli Endpoint Manager are not automatically discovered.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **IBM Tivoli Endpoint Manager**.

8 From the **Protocol Configuration** list, select **IBM Tivoli Endpoint Manager SOAP**.

9 Configure the following values:

Table 107: IBM Tivoli Endpoint Manager SOAP Protocol Configuration

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your IBM Tivoli Endpoint Manager appliance. The IP address or hostname identifies your IBM Tivoli Endpoint Manager as a unique event source in SIEM.
Port	Type the port number used to connect to the IBM Tivoli Endpoint Manager using the SOAP API. By default, port 80 is the port number for communicating with IBM Tivoli Endpoint Manager. If you are use HTTPS, you must update this field to the HTTPS port number for your network. Most configurations use port 443 for HTTPS communications.

Table 107: IBM Tivoli Endpoint Manager SOAP Protocol Configuration (Continued)

Parameter	Description
Use HTTPS	Select this check box to connect using HTTPS. If you select this check box, the hostname or IP address you specify uses HTTPS to connect to your IBM Tivoli Endpoint Manager. If a certificate is required to connect using HTTPS, you must copy any certificates required by the SIEM Console or managed host to the following directory: `/opt/qradar/conf/trusted_certificates` **NOTE:** SIEM support certificates with the following file extensions: .crt, .cert, or .der. Any required certificates should be copied to the trusted certificates directory before you save and deploy your changes.
Username	Type the username required to access your IBM Tivoli Endpoint Manager.
Password	Type the password required to access your IBM Tivoli Endpoint Manager.
Confirm Password	Confirm the password necessary to access your IBM Tivoli Endpoint Manager.

For more information on configuring SIEMto import IBM Tivoli Endpoint Manager vulnerabilities assessment information, see the *SIEM Managing Vulnerability Assessment Guide*.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

The IBM Tivoli Endpoint Manager configuration is complete.

IBM zSecure Alert

The IBM zSecure Alert DSM for SIEM accepts alert events using syslog, allowing SIEM to receive alert events in real-time.

The alert configuration on your IBM zSecure Alert appliance determines which alert conditions you want to monitor and forward to SIEM. To collect events in SIEM, you must configure your IBM zSecure Alert appliance to forward events in a UNIX syslog event format using the SIEM IP address as the destination. For information on configuring UNIX syslog alerts and destinations, see the *IBM Security zSecure Alert User Reference Manual*.

SIEM automatically discovers and creates a log source for syslog events from IBM zSecure Alert. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select IBM zSecure Alert.

8 Using the Protocol Configuration list, select **Syslog**.

9 Configure the following values:

Table 108: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM zSecure Alert.

10 Click Save.

11 On the Admin tab, click Deploy Changes.
The configuration is complete.

IBM Security Identity Manager

The IBM Security Identity Manager DSM for SIEM accepts audit, recertification, and system events from IBM Security Identity Manager appliances.

To collect events with SIEM, you must have the IBM Security Identity Manager JDBC protocol installed, which allows SIEM to poll for event information in the ITIMDB database. IBM Security Identity Manager events are generated from the audit table along with several other tables from the database.

Before you configure SIEM to integrate with IBM Security Identity Manager, we recommend you create a database user account and password in IBM Security Identity Manager for SIEM. Your SIEM user must have read permissions to the ITIMDB database, which stores IBM Security Identity Manager events. The IBM Security Identity Manager protocol allows SIEM to log in and poll for events from the database. Creating a SIEM account is not required, but it is recommended for tracking and securing your event data.

NOTE

Ensure no firewall rules are blocking the communication between your IBM Security Identity Manager appliance and SIEM.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **IBM Security Identity Manager**.

7 Using the Protocol Configuration list, select **IBM Security Identity Manager** JDBC.

8 Configure the following values:

Table 109: IBM Security Identity Manager JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. The log source identifier must be defined in the following format: `ITIMDB@<hostname>` Where `<hostname>` is the IP address or host name for your IBM Security Identity Manager appliance. The log source identifier must be unique for the log source type.
Database Type	From the list, select a database to use for the event source. The options include: • **DB2** - Select this option if DB2 is the database type on your IBM Security Identity Manager appliance. DB2 is the default database type. • **MSDE** - Select this option if MSDE is the database type on your IBM Security Identity Manager appliance • **Oracle** - Select this option if MSDE is the database type on your IBM Security Identity Manager appliance
Database Name	Type the name of the database to which you want to connect. The default database name is **ITIMDB**. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
IP or Hostname	Type the IP address or hostname of the IBM Security Identity Manager appliance.
Port	Type the port number used by the database server. The default that is displayed depends on the selected Database Type. The valid range is 0 to 65536. The default for DB2 is port 50000. The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections enabled to communicate with SIEM. The default port number for all options include: • **DB2** - 50000 • **MSDE** - 1433 • **Oracle** - 1521 **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.

Table 109: IBM Security Identity Manager JDBC Parameters (Continued)

Parameter	Description
Username	Type the database username. The username can be up to 255 alphanumeric characters in length. The username can also include underscores (_).
Password	Type the database password. The password can be up to 255 characters in length.
Confirm Password	Confirm the password to access the database.
Table Name	Type `ITIMUSER.AUDIT_EVENT` as the name of the table or view that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the IBM Security Identity Manager JDBC protocol. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `TIMESTAMP` to identify new events added between queries to the table by their timestamp. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Start Date and Time	Optional. Configure the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval in seconds, which is the amount of time between queries to the database table. The default polling interval is 30 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.

Table 109: IBM Security Identity Manager JDBC Parameters (Continued)

Parameter	Description
Authentication Domain	If you select MSDE as the Database Type, the **Authentication Domain** field is displayed. If your network is configured to validate users with domain credentials, you must define a Windows Authentication Domain. Otherwise, leave this field blank. The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.).
Database Instance	If you select MSDE as the Database Type, the **Database Instance** field is displayed. Type the type the instance to which you want to connect, if you have multiple SQL server instances on one server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Use Named Pipe Communication	If you select MSDE as the Database Type, the **Use Named Pipe Communications** check box is displayed. By default, this check box is clear. Select this check box to use an alternative method to a TCP/IP port connection. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Use NTLMv2	If you select MSDE as the Database Type, the **Use NTLMv2** check box is displayed. Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Database Cluster Name	If you select the **Use Named Pipe Communication** check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

IBM Security Network Protection (XGS)

The IBM Security Network Protection (XGS) DSM accepts events by using the Log Enhanced Event Protocol (LEEF), which enables SIEM to record all relevant events.

The following table identifies the specifications for the IBM Security Network Protection (XGS) DSM:

Table 110: IBM Security Network Protection (XGS) specifications

Specification	Value
Manufacturer	IBM
DSM	Security Network Protection (XGS)
RPM file name	
Supported versions	v5.0 with fixpack 7
Protocol	syslog (LEEF)
SIEM recorded events	All relevant system, access, and security events
Automatically discovered	Yes
Includes identity	No
More information	*IBM Network Security Protection (XGS) website* (http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.alps.doc/tasks/alps_configuring_system_alerts.htm)

Before you configure an Network Security Protection (XGS) appliance in SIEM, you must configure remote syslog alerts for your IBM Security Network Protection (XGS) rules or policies to forward events to SIEM.

Configure IBM Security Network Protection (XGS) Alerts

All event types are sent to SIEM using a remote syslog alert object that is LEEF enabled.

Remote syslog alert objects can be created, edited and deleted from each context in which an events is generated. To configure a remote syslog alert object log in to the Network Security Protection (XGS) local management interface as admin and navigate to one of the following:

- **Manage > System Settings > System Alerts** (System events)
- **Secure > Network Access Policy** (Access events)
- **Secure > IPS Event Filter Policy** (Security events)
- **Secure > Intrusion Prevention Policy** (Security events)
- **Secure > Network Access Policy > Inspection > Intrusion Prevention Policy**

In the IPS Objects, the Network Objects pane, or the System Alerts page, complete the following steps.

Procedure

1 Click **New > Alert > Remote Syslog**.

2 Select an existing remote syslog alert object, and then click **Edit**.

3 Configure the following options:

Table 111: Syslog Configuration Parameters

Option	Description
Name	Type a name for the syslog alert configuration.
Remote Syslog Collector	Type the IP address of your SIEM Console or Event Collector.
Remote Syslog Collector Port	Type **514** for the Remote Syslog Collector Port.
Remote LEEF Enabled	Select this check box to enable LEEF formatted events. This field is required. **NOTE:** If you do not see this option, verify you have software version 5.0 and fixpack 7 installed on your IBM Security Network Protection appliance.
Comment	Optional. Type a comment for the syslog configuration.

4 Click **Save Configuration**.

The alert is added to the Available Objects list.

5 To update your IBM Security Network Protection (XGS) appliance, click **Deploy**.

6 Add the LEEF alert object for SIEM to the following locations:

- One or more rules in a policy
- **Added Objects** pane on the System Alerts page

7 Click **Deploy**

For more information about the Network Security Protection (XGS) device, click Help in the Network Security Protection (XGS) local management interface browser client window or access the online Network Security Protection (XGS) documentation.

Configuring a Log Source in SIEM

SIEM automatically discovers and creates a log source for LEEF-enabled syslog events from IBM Security Network Protection (XGS). The following configuration steps are optional.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select **IBM Security Network Protection (XGS)**.

6 Using the Protocol Configuration list, select **Syslog**.

7 Configure the following values:

Table 112: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM Security Network Protection (XGS).

8 Click Save.

9 On the Admin tab, click Deploy Changes.

IBM Security Access Manager for Enterprise Single Sign-On

You can use the IBM® Security Access Manager for Enterprise Single Sign-On DSM for SIEM to receive events forwarded using syslog.

Supported Versions

SIEM can collect events from IBM Security Access Manager for Enterprise Single Sign-On version 8.1 or 8.2.

Supported Event Types

Events forwarded by the IBM Security Access Manager for Enterprise Single Sign-On include audit, system, and authentication events.

Events are read from the following database tables and forwarded using syslog:

- IMSLOGUserService
- IMSLOGUserAdminActivity
- IMSLOGUserActivity

All events forwarded to SIEM from IBM Security Access Manager for Enterprise Single Sign-On use ### as a syslog field-separator. IBM Security Access Manager for Enterprise Single Sign-On forwards events to SIEM using UDP on port 514.

Before You Begin

To configure syslog forwarding for events, you must be an administrator or your user account must include credentials to access the IMS Configuration Utility.

Any firewalls configured between your IBM Security Access Manager for Enterprise Single Sign-On and SIEM should be configured to allow UDP communication on port 514. This configuration requires you to restart your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Configuring a Log Server Type

IBM Security Access Manager for Enterprise Single Sign-On appliance requires you to configure a log server type to forward syslog formatted events:

Procedure

1 Log in to the IMS Configuration Utility for IBM Security Access Manager for Enterprise Single Sign-On.

For example, https://localhost:9043/webconf

2 From the navigation menu, select **Advanced Settings > IMS Server > Logging > Log Server Information**.

3 From the **Log server types** list, select **syslog**.

4 Click **Add**.

5 Click **Update** to save the configuration.

Configuring Syslog Forwarding

To forward events to SIEM, you must configure a syslog destination on your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Procedure

1 From the navigation menu, select **Advanced Settings > IMS Server > Logging > Syslog**.

2 Configure the following options:

Table 113: Syslog Parameters

Field	Description
Enable syslog	From the **Available Tables** list, select the following tables and click **Add**. You must add the following tables: • logUserService • logUserActivity • logUserAdminActivity
Syslog server port	Type **514** as the port number used for forwarding events to SIEM.
Syslog server hostname	Type the IP address or hostname of your SIEM Console or Event Collector.
Syslog logging facility	Type an integer value to specify the facility of the events forwarded to SIEM. The default value is 20.
Syslog field-separator	Type **###** as the characters used to separate name-value pair entries in the syslog payload.

3 Click **Update** to save the configuration.

4 Restart your IBM Security Access Manager for Enterprise Single Sign-on appliance.

The syslog configuration is complete. The log source is added to SIEM as IBM Security Access Manager for Enterprise Single Sign-On syslog events are automatically discovered. Events forwarded to SIEM are displayed on the **Log Activity** tab.

Configuring a Log Source in SIEM

SIEM automatically discovers and creates a log source for syslog events from IBM Security Access Manager for Enterprise Single Sign-On. The following procedure is optional.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select **IBM Security Access Manager for Enterprise Single Sign-On**.

6 Using the Protocol Configuration list, select **Syslog**.

7 Configure the following values:

Table 114: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM Security Access Manager for Enterprise Single Sign-On appliance.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.

Table 114: Syslog Parameters (Continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

55 ISC Bind

You can integrate an Internet System Consortium (ISC) BIND device with SIEM. An ISC BIND device accepts events using syslog.

Configuring Syslog for ISC BIND

You can configure syslog on your ISC BIND device to forward events to SIEM.

Procedure

1 Log in to the ISC BIND device.

2 Open the following file to add a logging clause:

```
named.conf
logging {
channel <channel_name> {
syslog <syslog_facility>;
            severity <critical | error | warning | notice | info
| debug [level ] | dynamic >;
print-category yes;
print-severity yes;
print-time yes;
};
category queries {
<channel_name>;
};
category notify {
<channel_name>;
};
category network {
<channel_name>;
};
category client {
<channel_name>;
};
};
```

For Example:

```
logging {
channel SIEM {
syslog local3;
severity info;
};
category queries {
SIEM;
};
category notify {
SIEM;
};
category network {
```

```
SIEM;
};
category client {
SIEM;
};
};
```

3 Save and exit the file.

4 Edit the syslog configuration to log to your SIEM using the facility you selected in Step 2:

`<syslog_facility>.* @<IP Address>`

Where `<IP Address>` is the IP address of your SIEM.

For example:

```
local3.* @192.16.10.10
```

NOTE

SIEM only parses logs with a severity level of info or higher.

5 Restart the following services.

```
service syslog restart
service named restart
```

You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from ISC BIND. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select ISC BIND.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 115: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ISC BIND appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

56 Infoblox NIOS

The Infoblox NIOS DSM for SIEM accepts events using syslog, which enables SIEM to record all relevant events from an Infoblox NIOS device.

Before you configure SIEM, configure your Infoblox NIOS device to send syslog events to SIEM. For more information on configuring logs on your Infoblox NIOS device, see your Infoblox NIOS vendor documentation.

The following table identifies the specifications for the Infoblox NIOS DSM:

Table 116: Infoblox NIOS DSM specifications

Specification	Value
Manufacturer	Infoblox
DSM	NIOS
Version	v6.x
Events accepted	Syslog
SIEM recorded events	• ISC Bind events • Linux DHCP events • Linux Server events • Apache events
Option in SIEM	Infoblox NIOS
Auto discovered	No
Includes identity	Yes
For more information	www.infoblox.com

Configuring a Log Source

SIEM does not automatically discover or create log sources for syslog events from Infoblox NIOS appliances.To integrate Infoblox NIOS appliances with SIEM, you must manually create a log source to receive Infoblox NIOS events.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Infoblox NIOS.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the remaining parameters.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

57 iT-CUBE agileSI

The iT-CUBE agileSI DSM for SIEM can accept security-based and audit SAP events from agileSI installations that are integrated with your SAP system.

SIEM uses the event data defined as security risks in your SAP environment to generate offenses and correlate event data for your security team. SAP security events are written in Log Event Extended Format (LEEF) to a log file produced by agileSI. SIEM retrieves the new events using the SMB Tail protocol. To retrieve events from agileSI, you must create a log source using the SMB Tail protocol and provide SIEM credentials to log in and poll the LEEF formatted agileSI event file. SIEM is updated with new events each time the SMB Tail protocol polls the event file for new SAP events.

Configuring agileSI to Forward Events

To configure agileSI, you must create a logical filename for your events and configure the connector settings with the path to your agileSI event log.

The location of the LEEF formatted event file must be in a location viewable by Samba and accessible with the credentials you configure for the log source in SIEM.

Procedure

1 In agileSI core system installation, define a logical file name for the output file containing your SAP security events.

SAP provides a concept which enables you to use platform-independent logical file names in your application programs. Create a logical file name and path using transaction “FILE” (Logical File Path Definition) according to your organization’s requirements.

2 Log in to agileSI.

For example, `http://<sap-system-url:port>/sap/bc/webdynpro/itcube/ccf?sap-client=<client>&sap-language=EN`

Where:

`<sap-system-url>` is the IP address and port number of your SAP system, such as 10.100.100.125:50041.

`<client>` is the agent in your agileSI deployment.

3 From the menu, click **Display/Change** to enable change mode for agileSI.

4 From the toolbar, select **Tools > Core Consumer Connector Settings**.

The Core Consumer Connector Settings are displayed.

5 Configure the following values:

a From the **Consumer Connector** list, select **Q1 Labs**.

b Select the **Active** check box.

c From the **Connector Type** list, select **File**.

d From the **Logical File Name** field, type the path to your logical file name you configured in step 1.

For example, `/ITCUBE/LOG_FILES`.

The file created for the agileSI events is labeled LEEFYYYYDDMM.TXT where YYYYDDMM is the year, day, and month. The event file for the current day is appended with new events every time the extractor runs. iT-CUBE agileSI creates a new LEEF file for SAP events daily.

6 Click **Save**.

The configuration for your connector is saved. Before you can complete the agileSI configuration, you must deploy the changes for agileSI using extractors.

7 From the toolbar, select **Tools > Extractor Management**.

The Extractor Management settings are displayed.

8 Click **Deploy all**.

The configuration for agileSI events is complete. You are now ready to configure a log source in SIEM.

Configure an agileSI Log Source

SIEM must be configured to log in and poll the event file using the SMB Tail protocol.

The SMB Tail protocol logs in and retrieves events logged by agileSI in the LEEFYYYYDDMM.txt file.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select iT-CUBE agileSI.

9 Using the Protocol Configuration list, select **SMB Tail**.

10 Configure the following values:

Table 117: SMB Tail protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address, hostname, or name for the log source as an identifier for your iT-CUBE agileSI events.
Server Address	Type the IP address of your iT-CUBE agileSI server.
Domain	Type the domain for your iT-CUBE agileSI server. This parameter is optional if your server is not located in a domain.

Table 117: SMB Tail protocol parameters (Continued)

Parameter	Description
Username	Type the username required to access your iT-CUBE agileSI server. **NOTE:** The username and password you specify must be able to read to the LEEFYYYYDDMM.txt file for your agileSI events.
Password	Type the password required to access your iT-CUBE agileSI server.
Confirm Password	Confirm the password required to access your iT-CUBE agileSI server.
Log Folder Path	Type the directory path to access the LEEFYYYYDDMM.txt file. Parameters that support file paths allow you to define a drive letter with the path information. For example, you can use `c$/LogFiles/` for an administrative share, or `LogFiles/` for a public share folder path, but not `c:/LogFiles`. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the proper access required to read the log files. Local or domain administrators have sufficient privileges to access log files that reside on administrative shares.
File Pattern	Type the regular expression (regex) required to filter the filenames. All matching files are included for processing when SIEM polls for events. For example, if you want to list all files ending with `txt`, use the following entry: `.*\.txt`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
Force File Read	Select this check box to force the protocol to read the log file. By default, the check box is selected. If the check box is clear the event file is read when SIEM detects a change in the modified time or file size.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the event file to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.
Throttle Events/Sec	Type the maximum number of events the SMB Tail protocol forwards per second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default is 100 EPS.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. As your iT-CUBE agileSI log source retrieves new events, the **Log Activity** tab in SIEM is updated.

58 Itron Smart Meter

The Itron Smart Meter DSM for SIEM collects events from an Itron Openway Smart Meter using syslog.

The Itron Openway Smart Meter sends syslog events to SIEM using Port 514. For details of configuring your meter for syslog, see your Itron Openway Smart Meter documentation.

SIEM automatically discovers and creates a log source for syslog events from Itron Openway Smart Meters. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Itron Smart Meter.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 118: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Itron Openway Smart Meter installation.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

59 Juniper Networks

SIEM supports the following Juniper Networks DSMs:

Juniper Networks AVT

The Juniper Networks Application Volume Tracking (AVT) DSM for SIEM accepts events using Java Database Connectivity (JDBC) protocol.

SIEM records all relevant events. To integrate with Juniper Networks NSM AVT data, you must create a view in the database on the Juniper Networks NSM server. You must also configure the Postgres database configuration on the Juniper Networks NSM server to allow connections to the database since, by default, only local connections are allowed.

NOTE

This procedure is provided as a guideline. For specific instructions, see your vendor documentation.

Procedure

1 Log in to your Juniper Networks AVT device command-line interface (CLI).

2 Open the following file:
`/var/netscreen/DevSvr/pgsql/data/pg_hba.conf file`

3 Add the following line to the end of the file:
`host all all <IP address>/32 trust`
Where `<IP address>` is the IP address of your SIEM Console or Event Collector you want to connect to the database.

4 Reload the Postgres service:

```
su - nsm -c "pg_ctl reload -D /var/netscreen/DevSvr/pgsql/data"
```

5 As the Juniper Networks NSM user, create the view:

```
create view strm_avt_view as SELECT a.name, a.category,
v.srcip,v.dstip,v.dstport, v."last", u.name as userinfo, v.id,
v.device, v.vlan,v.sessionid, v.bytecnt,v.pktcnt, v."first" FROM
avt_part v JOIN app a ON v.app =a.id JOIN userinfo u ON
v.userinfo = u.id;
```

The view is created.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Juniper Networks AVT device:

1 From the Log Source Type list, select Juniper Networks AVT.

2 You must also configure the JDBC protocol for the log source. Use the following parameters to configure the JDBC protocol:

a **Database Type** - From the **Database Type** list, select **Postgres**.

b **Database Name** - Type `profilerDb`.

c **IP or Hostname** - Type the IP address of the Juniper Networks NSM system.

d **Port** - Type `5432`.

e **Username** - Type the username for the profilerDb database.

f **Password** - Type the password for profilerDB database.

g **Table Name** - Type `strm_avt_view`.

h **Select List** - Type `*` for the select list.

i **Compare Field** - Type `id` for the Compare Field.

j **Use Prepared Statements** -The **Use Prepared Statements** check box must be clear. The Juniper Networks AVT DSM does not support prepared statements.

k **Polling Interval** - Type `10` for the Polling interval.

NOTE

The Database Name and Table Name parameters are case sensitive.

For more information on configuring log sources and protocols, see the *SIEM Log Sources User Guide*.

Juniper DDoS Secure

The Juniper DDoS Secure DSM for SIEM receives events from Juniper DDoS Secure devices by using syslog in Log Event Extended Format (LEEF) format. SIEM records all relevant status and network condition events.

Procedure

1 Log in to Juniper DDoS Secure.

2 Go to the Structured Syslog Server window.

3 In the **Server IP Address(es)** field, type the IP address of the SIEM Console.

4 From the **Format** list, select **LEEF**.

5 Optional. If you do not want to use the default of `local0` in the **Facility** field, type a facility.

6 From the **Priority** list, select the syslog priority level that you want to include. Events that meet or exceed the syslog priority level you select are forwarded to SIEM.

7 Log in to SIEM.

8 Click the **Admin** tab.

9 From the navigation menu, click **Data Sources**.

10 Click the Log Sources icon.

11 Click Add.

12 From the Log Source Type list, select the Juniper DDoS Secure option.

13 Configure the parameters.

14 Click **Save**.

For more information about log source management, see the *SIEM Log Sources User Guide*.

Juniper DX Application Acceleration Platform

The Juniper DX Application Acceleration Platform DSM for SIEM uses syslog to receive events. SIEM records all relevant status and network condition events. Before configuring SIEM, you must configure your Juniper device to forward syslog events.

Procedure

1 Log in to the Juniper DX user interface.

2 Browse to the desired cluster configuration (Services - Cluster Name), Logging section.

3 Select the Enable Logging check box.

4 Select the desired Log Format.
SIEM supports Juniper DX logs using the common and perf2 formats only.

5 Select the desired Log Delimiter format.

SIEM supports comma delimited logs only.

6 In the Log Host section, type the IP address of your SIEM system.

7 In the Log Port section, type the UDP port on which you wish to export logs.

8 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Juniper DX Application Acceleration Platform:

From the Log Source Type list, select the Juniper DX Application Acceleration Platform option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Juniper EX Series Ethernet Switch

The Juniper EX Series Ethernet Switch DSM for SIEM accepts events using syslog.

The Juniper EX Series Ethernet Switch DSM supports Juniper EX Series Ethernet Switches running Junos OS. Before you can integrate SIEM with a Juniper EX Series Ethernet Switch, you must configure your Juniper EX Series Switch to forward syslog events.

Procedure

1 Log in to the Juniper EX Series Ethernet Switch command-line interface (CLI).

2 Type the following command:
`configure`

3 Type the following command:
`set system syslog host <IP address> <option> <level>`
Where:
`<IP address>` is the IP address of your SIEM.
`<level>` is info, error, warning, or any.
`<option>` is one of the following options from Table 119.

Table 119: Juniper Networks EX Series Switch Options

Option	Description
any	All facilities
authorization	Authorization system
change-log	Configuration change log
conflict-log	Configuration conflict log
daemon	Various system processes
dfc	Dynamic flow capture
explicit-priority	Include priority and facility in messages
external	Local external applications
facility-override	Alternate facility for logging to remote host
firewall	Firewall filtering system

Table 119: Juniper Networks EX Series Switch Options (Continued)

Option	Description
ftp	FTP process
interactive-commands	Commands run by the UI
kernel	Kernel
log-prefix	Prefix for all logging to this host
match	Regular expression for lines to be logged
pfe	Packet Forwarding Engine
user	User processes

For example:

```
set system syslog host 10.77.12.12 firewall info
```

Configures the Juniper EX Series Ethernet Switch to send info messages from firewall filtering systems to your SIEM.

4 Repeat Step 3 to configure any additional syslog destinations and options. Each additional option must be identified using a separate syslog destination configuration.

5 You are now ready to configure the Juniper EX Series Ethernet Switch in SIEM.

To configure SIEM to receive events from a Juniper EX Series Ethernet Switch:

u From the **Log Source Type** list. select **Juniper EX-Series Ethernet Switch** option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Juniper switch, see your vendor documentation.

Juniper IDP

The Juniper IDP DSM for SIEM accepts events using syslog. SIEM records all relevant Juniper IDP events.

Configuring Syslog for Juniper IDP

You can configure a sensor on your Juniper IDP to send logs to a syslog server:

Procedure

1 Log in to the Juniper NSM user interface.

2 In NSM, double-click on the **Sensor in Device Manager**.

3 Select Global Settings.

4 Select Enable Syslog.

5 Type the Syslog Server IP address to forward events to SIEM.

6 Click OK.

7 Use Update Device to load the new settings onto the IDP Sensor.

The format of the syslog message sent by the IDP Sensor is as follows:

```
<day id>, <record id>, <timeReceived>, <timeGenerated>, <domain>,
<domainVersion>, <deviceName>, <deviceIpAddress>, <category>,
<subcategory>,<src zone>, <src intface>, <src addr>, <src port>,
<nat src addr>, <nat src port>, <dstzone>,
<dst intface>, <dst addr>, <dst port>, <nat dst addr>,
<nat dst port>,<protocol>, <rule domain>, <rule domainVersion>,
<policyname>, <rulebase>, <rulenumber>, <action>, <severity>, <is
alert>, <elapsed>, <bytes in>, <bytes out>, <bytestotal>,
<packet in>, <packet out>, <packet total>, <repeatCount>,
<hasPacketData>,<varData Enum>, <misc-str>, <user str>,
<application str>, <uri str>
```

For example:

```
[syslog@juniper.net dayId="20061012" recordId="0" timeRecv="2006/
10/12 21:52:21" timeGen="2006/10/12 21:52:21" domain=""
devDomVer2="0" device_ip="10.209.83.4" cat="Predefined"
attack="TROJAN:SUBSEVEN:SCAN" srcZn="NULL" srcIntf="NULL"
srcAddr="192.168.170.20" srcPort="63396" natSrcAddr="NULL"
natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL"
natDstPort="0" protocol="TCP" ruleDomain="" ruleVer="5"
policy="Policy2" rulebase="IDS" ruleNo="4" action="NONE"
severity="LOW" alert="no" elaspedTime="0" inbytes="0"
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0"
repCount="0" packetData="no" varEnum="31"
misc="<017>'interface=eth2" user="NULL" app="NULL" uri="NULL"]
```

Configure a Log Source

Juniper NSM is a central management server for Juniper IDP. You can configure SIEM to collect and represent the Juniper IDP alerts as coming from a central NSM, or SIEM can collect syslog from the individual Juniper IDP device.

To configure SIEM to receive events from Juniper Networks Secure Access device:

From the **Log Source Type** list, select Juniper Networks Intrusion Detection and Prevention (IDP).

For more information on configuring devices, see the *SIEM Log Sources User Guide*. For more information about Juniper IDP, see your Network and Security Manager documentation.

Juniper Networks Secure Access

The Juniper Networks Secure Access DSM for SIEM accepts login and session information using syslog in WebTrends Enhanced Log File (WELF) format. You can integrate Juniper SA and Juniper IC with SIEM.

NOTE

If your Juniper device is running release 5.5R3-HF2 - 6.1 or above, we recommend that you use the WELF:WELF format for logging. See your vendor documentation to determine if your device and license support logging in WELF:WELF format.

This document provides information for integrating a Juniper Secure Access device using one of the following formats:

- WELF:WELF (Recommended). See Use the WELF:WELF Format on page 332.
- Syslog. See Use the Syslog Format on page 334.

Use the WELF:WELF Format

To integrate a Juniper Networks Secure Access device with SIEM using the WELF:WELF format.

Procedure

1 Log in to your Juniper device administration user interface:
`https://10.xx.xx.xx/admin`

2 Configure syslog server information for events:
   a If a WELF:WELF file is configured, go to Step f. Otherwise, go to Step b.
   b From the left panel, select **System > Log/Monitoring > Events > Filter**.
   c Click New Filter.
   d Select WELF.
   e Click Save Changes.
   f From the left panel, select **System > Log/Monitoring > Events > Settings**.
   g From the Select Events to Log pane, select the events that you wish to log.
   h In the **Server name/IP** field, type the name or IP address of the syslog server.
   i From the Facility list, select the facility.
   j From the Filter list, select WELF:WELF.
   k Click Add, then click Save Changes.

3 Configure syslog server information for user access:
   a If a WELF:WELF file is configured, go to Step e. Otherwise, go to Step b.
   b From the left panel, select **System > Log/Monitoring > User Access > Filter**.
   c Click New Filter.
   d Select **WELF**. Click Save Changes.
   e From the left panel, select **System > Log/Monitoring > User Access > Settings**.
   f From the Select Events to Log pane, select the events that you wish to log.

g In the **Server name/IP** field, type the name or IP address of the syslog server.
h From the Facility list, select the facility.
i From the Filter list, select WELF:WELF.
j Click Add and click Save Changes.

4 Configure syslog server information for administrator access:
a If a WELF:WELF file is configured, go to Step f. Otherwise, go to Step b.
b From the left panel, select **System > Log/Monitoring > Admin Access > Filter**.
c Click New Filter.
d Select WELF.
e Click Save Changes.
f From the left panel, select **System > Log/Monitoring > Admin Access > Settings**.
g From the Select Events to Log pane, select the events that you wish to log.
h In the **Server name/IP** field, type the name or IP address of the syslog server.
i From the Facility list, select the facility.
j From the Filter list, select WELF:WELF.
k Click Add, then click Save Changes.

5 Configure syslog server information for client logs:
a If a WELF:WELF file is configured, go to Step e. Otherwise, go to Step b.
b From the left panel, select **System > Log/Monitoring > Client Logs > Filter**.

The Filter menu is displayed.
c Click New Filter.
d Select WELF. Click Save Changes.
e From the left pane, select **System > Log/Monitoring > Client Logs > Settings**.
f From the Select Events to Log pane, select the events that you wish to log.
g In the **Server name/IP** field, type the name or IP address of the syslog server.
h From the Facility list, select the facility.
i From the Filter list, select WELF:WELF.
j Click Add, then click Save Changes.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from Juniper Networks Secure Access device:

From the Log Source Type list, select Juniper Networks Secure Access (SA) SSL VPN.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Juniper device, see your vendor documentation.

Use the Syslog Format

You can use the syslog format to integrate a Juniper Networks Secure Access device with SIEM.

Procedure

1 Log in to your Juniper device administration user interface:
`https://10.xx.xx.xx/admin`

2 Configure syslog server information for events:
   a From the left pane, select **System > Log/Monitoring > Events > Settings**.
   b From the Select Events to Log section, select the events that you wish to log.
   c In the Server name/IP field, type the name or IP address of the syslog server.

3 Configure syslog server information for user access:
   a From the left pane, select **System > Log/Monitoring > User Access > Settings**.
   b From the Select Events to Log section, select the events that you wish to log.
   c In the Server name/IP field, type the name or IP address of the syslog server.

4 Configure syslog server information for administrator access:
   a From the left pane, select **System > Log/Monitoring > Admin Access > Settings**.
   b From the Select Events to Log section, select the events that you wish to log.
   c In the Server name/IP field, type the name or IP address of the syslog server.

5 Configure syslog server information for client logs:
   a From the left pane, select **System > Log/Monitoring > Client Logs > Settings**.
   b From the Select Events to Log section, select the events that you wish to log.
   c In the Server name/IP field, type the name or IP address of the syslog server.

   You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from Juniper Networks Secure Access device:

From the Log Source Type list, select Juniper Networks Secure Access (SA) SSL VPN.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Juniper device, see your vendor documentation.

Juniper Infranet Controller

The Juniper Networks Infranet Controller DSM for SIEM accepts DHCP events using syslog. SIEM records all relevant events from a Juniper Networks Infranet Controller. Before you configure SIEM to integrate with a Juniper Networks Infranet Controller, you must configure syslog within the server. For more information on configuring your Juniper Networks Infranet Controller, consult your vendor documentation.

After you configure syslog for your Juniper Infranet Controller, you are now ready to configure the log source in SIEM.

To configure SIEM to receive events from your Juniper Networks Infranet Controller:

From the Log Source Type list, select Juniper Networks Infranet Controller option.

For more information on configuring devices, see the *SIEM Log Sources User Guide*.

Juniper Networks Firewall and VPN

The Juniper Networks Firewall and VPN DSM for SIEM accepts Juniper Firewall and VPN events using UDP syslog. SIEM records all relevant firewall and VPN events.

NOTE

TCP syslog is not supported. You must use UDP syslog.

You can Juniper Networks Firewall and VPN device to export events to SIEM.

Procedure

1 Log in to your Juniper Networks Firewall and VPN user interface.

2 Select **Configuration > Report Settings > Syslog**.

3 Select the enable syslog messages check box.

4 Type the IP address of your SIEM Console or Event Collector.

5 Click Apply.
You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Juniper Networks Firewall and VPN device:

From the Log Source Type list, select Juniper Networks Firewall and VPN option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Juniper Networks Firewall and VPN device, see your Juniper documentation.

Juniper Networks Network and Security Manager

The Juniper Networks Network and Security Manager (NSM) DSM for SIEM accepts Juniper Networks NSM and Juniper Networks Secure Service Gateway (SSG) logs. All Juniper SSG logs must be forwarded through Juniper NSM to SIEM. All other Juniper devices should be forwarded directory to SIEM.

For more information on advanced filtering of Juniper Networks NSM logs, see your Juniper Networks vendor documentation.

To integrate a Juniper Networks NSM device with SIEM, you must:

- Configuring Juniper Networks NSM to Export Logs to Syslog on page 336
- Configuring a Log Source for Juniper Networks NSM on page 336

Configuring Juniper Networks NSM to Export Logs to Syslog

Juniper Networks NSM uses the syslog server when exporting qualified log entries to syslog. Configuring the syslog settings for the management system only defines the syslog settings for the management system.

It does not actually export logs from the individual devices. You can enable the management system to export logs to syslog.

Procedure

1 Log in to the Juniper Networks NSM user interface.

2 From the **Action Manager** menu, select Action Parameters.

3 Type the IP address for the syslog server to which you want to send qualified logs.

4 Type the syslog server facility for the syslog server to which you want to send qualified logs.

5 From the Device Log Action Criteria node, select the Actions tab.

6 Select Syslog Enable for **Category**, **Severity**, and **Action**.

You are now ready to configure the log source in SIEM.

Configuring a Log Source for Juniper Networks NSM

You can configure a log source in SIEM for Juniper Networks NSM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

1 From the **Log Source Type** list, select **Juniper Networks Network and Security Manager**.

2 From the **Protocol Configuration** list, select **Juniper NSM**.

3 Configure the following values for the Juniper NSM protocol:

Table 120: Juniper NSM Protocol Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. The log source identifier must be unique for the log source type.
IP	Type the IP address or hostname of the Juniper Networks NSM server.
Inbound Port	Type the inbound port to which the Juniper Networks NSM sends communications.The valid range is 0 to 65536. The default is 514.
Redirection Listen Port	Type the port to which traffic is forwarded. The valid range is 0 to 65,536. The default is 516.

Table 120: Juniper NSM Protocol Parameters (Continued)

Parameter	Description
Use NSM Address for Log Source	Select this check box to use the Juniper NSM management server IP address instead of the log source IP address. By default, the check box is selected.

NOTE

In the SIEM interface, the Juniper NSM protocol configuration enables you to use the Juniper Networks NSM IP address by selecting the Use NSM Address for Event Source check box. If you wish to change the configuration to use the originating IP address (clear the check box), you must log in to your SIEM Console, as a root user, and reboot the Console (for an all-in-one system) or the Event Collector hosting the log sources (in a distributed environment) using the following command: `shutdown -r now`.

Juniper Junos OS

The Juniper Junos OS Platform DSM for SIEM accepts events using syslog, structured-data syslog, or PCAP (SRX Series only). SIEM records all valid syslog or structured-data syslog events.

The Juniper Junos OS Platform DSM supports the following Juniper devices running Junos OS:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper T Series Core Platform
- Juniper SRX Series Services Gateway

For information on configuring PCAP data using a Juniper Networks SRX Series appliance, see Configure the PCAP Protocol on page 339.

NOTE

For more information about structured-data syslog, see RFC 5424 at the Internet Engineering Task Force: www.ietf.org/

Before you configure SIEM to integrate with a Juniper device, you must forward data to SIEM using syslog or structured-data syslog.

Procedure

1 Log in to your Juniper platform command-line interface (CLI).

2 Include the following syslog statements at the `set system` hierarchy level:

```
[set system]
syslog {
   host (hostname) {
     facility <severity>;
     explicit-priority;
     any any;
     authorization any;
     firewall any;
    }
  source-address source-address;
  structured-data {
  brief;
  }
}
```

Table 121 lists and describes the configuration setting variables to be entered in the syslog statement.

Table 121: List of Syslog Configuration Setting Variables

Parameter	Description
host (hostname)	Type the IP address or the fully-qualified hostname of your SIEM.
Facility <severity>	Define the severity of the messages that belong to the named facility with which it is paired. Valid severity levels are: • any • none • emergency • alert • critical • error • warning • notice • info Messages with the specified severity level and higher are logged. The levels from emergency through info are in order from highest severity to lowest.
Source-address	Type a valid IP address configured on one of the router interfaces for system logging purposes. The source-address is recorded as the source of the syslog message send to SIEM. This IP address is specified in host hostname statement set system syslog hierarchy level; not, however, for messages directed to the other routing engine, or to the TX Matrix platform in a routing matrix.
structured-data	Inserts structured-data syslog into the data.

You are now ready to configure the log source in SIEM.

The following devices are auto discovered by SIEM as a Juniper Junos OS Platform devices:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper SRX Series
- Juniper EX Series Ethernet Switch
- Juniper T Series Core Platform

To manually configure SIEM to receive events from a Juniper Junos OS Platform device:

From the Log Source Type list, select one of the following options: Juniper JunOS Platform, Juniper M-Series Multiservice Edge Routing, Juniper MX-Series Ethernet Services Router, Juniper SRX-series, or Juniper T-Series Core Platform.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Juniper device, see your vendor documentation.

Configure the PCAP Protocol

The Juniper SRX Series appliance supports forwarding of packet capture (PCAP) and syslog data to SIEM.

Syslog data is forwarded to SIEM on port 514. The IP address and outgoing PCAP port number is configured on the Juniper Networks SRX Series appliance interface. The Juniper Networks SRX Series appliance must be configured using the to forward PCAP data in the format
`<IP Address>:<Port>`.

Where:

`<IP Address>` is the IP address of SIEM.

`<Port>` is the outgoing port address for the PCAP data.

For more information on Configuring Packet Capture, see your Juniper Networks Junos OS documentation.

You are now ready to configure the log source and protocol in SIEM. For more information see Configuring a New Juniper Networks SRX Log Source with PCAP on page 339.

Configuring a New Juniper Networks SRX Log Source with PCAP

The Juniper Networks SRX Series appliance is auto discovered by SIEM as a Juniper Junos OS Platform.

SIEM detects the syslog data and adds the log source automatically. The PCAP data can be added to SIEM as Juniper SRX Series Services Gateway log source using the PCAP Syslog Combination protocol. Adding the PCAP Syslog Combination protocol after SIEM auto discovers the Junos OS syslog data adds an additional log source to your existing log source limit. Deleting the existing syslog entry, then adding the PCAP Syslog Combination protocol adds both syslog and PCAP data as single log source.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select Juniper SRX-series Services Gateway.

7 From the Protocol Configuration list, select PCAP Syslog Combination.

8 Type the Log Source Identifier.

9 Type the Incoming PCAP Port.

To configure the Incoming PCAP Port parameter in the log source, enter the outgoing port address for the PCAP data as configured on the Juniper Networks SRX Series appliance interface. For more information on configuring log sources, see the Log Sources User Guide.

10 Click Save.

11 Select the auto discovered syslog-only Junos OS log source for your Juniper Networks SRX Series appliance.

12 Click Delete.

A delete log source confirmation window is displayed.

13 Click Yes.

The Junos OS syslog log source is deleted from the log source list. You should now have the PCAP Syslog Combination protocol in your log source list.

14 On the **Admin** tab, click Deploy Changes.

Juniper Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for SIEM accepts syslog events from a client running the WinCollect or the Adaptive Log Exporter utility using the Windows operating system, or on Linux using syslog.

SIEM records all successful and unsuccessful login attempts. You can integrate Juniper Networks Steel-Belted Radius with SIEM using one of the following methods:

- Configure Juniper Steel Belted-Radius to use WinCollect or Adaptive Log Exporter on Microsoft Windows operating systems. For more information, see Configuring Juniper Steel-Belted Radius for the Adaptive Log Exporter on page 341 or the *WinCollect Use Guide*.
- Configure Juniper Steel-Belted Radius using syslog on Linux-based operating systems. For more information, see Configuring Juniper Steel-Belted Radius for Syslog on page 342.

Configuring Juniper Steel-Belted Radius for the Adaptive Log Exporter

You can integrate a Juniper Steel-Belted Radius DSM with SIEM using the Adaptive Log Exporter.

Procedure

1 From the Start menu, select **Start > Programs > Adaptive Log Exporter > Configure Adapter Log Exporter**.

The Adaptive Log Exporter must be installed on the same system as your Juniper SBR system. The Adaptive Log Exporter must be updated to include the Juniper SBR device plug-in. For more information, see your Adaptive Log Exporter Users Guide.

2 Click the Devices tab.

3 Select **Juniper SBR**, right-click and select **Add Device**.

The New Juniper SBR Properties window is displayed.

4 Configure the following parameters:

a Name - Type a name for the device. The name can include alphanumeric characters and underscore (_) characters.

b Description - Type a description for this device.

c Device Address - Type the IP address or hostname that the device. The IP address or hostname is used to identify the device in syslog messages forwarded to SIEM. This is the IP address or hostname that will appear in SIEM.

d Root Log Directory - Type the location where Juniper SBR stores log files. Report log files should be located in the Steel-Belted Radius directory `<radiusdir>\authReports`. The Adaptive Log Exporter monitors the Root Log Directory for any .CSV files having a date stamp in the file name matching the current day.

5 From the Adaptive Log Exporter toolbar, click **Save**.

6 From the Adaptive Log Exporter toolbar, click **Deploy**.

NOTE

You must use the default values for the log file heading in the Juniper Steel-Belted Radius appliance. If the log file headings have been changed from the default values and SIEM is not parsing SBR events properly, please contact Customer Support.

7 You are now ready to configure the log source in SIEM.

Juniper SBR events provided from the Adaptive Log Exporter are automatically discovered by SIEM. If you want to manually configure SIEM to receive events from Juniper Steel-Belted Radius:

From the **Log Source Type** drop-down box, select the Juniper Steel-Belted Radius option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Configuring Juniper Steel-Belted Radius for Syslog

You can integrate a Juniper Steel-Belted Radius DSM with SIEM using syslog on a Linux-based operating system.

Procedure

1 Using SSH log in to your Juniper Steel-Belted Radius device, as a root user.

2 Edit the following file:

`/etc/syslog.conf`

3 Add the following information:

`<facility>.<priority>  @<IP address>`

Where:

`<facility>` is the syslog facility, for example, `local3`.

<priority> is the syslog priority, for example, `info`.

`<IP address>` is the IP address of SIEM.

4 Save the file.

5 From the command-line, type the following command to restart syslog:

`service syslog restart`

6 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from Juniper Steel-Belted Radius:

From the **Log Source Type** list, select the **Juniper Steel-Belted Radius** option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information on configuring your Steel-Belted Radius server consult your vendor documentation.

Juniper Networks vGW Virtual Gateway

The Juniper Networks vGW Virtual Gateway DSM for SIEM accepts events using syslog and NetFlow from your vGW management server or firewall. SIEM records all relevant events, such as admin, policy, IDS logs, and firewall events. Before configuring an Juniper Networks vGW Virtual Gateway in SIEM, you must configure vGW to forward syslog events.

Procedure

1 Log in to your Juniper Networks vGW user interface.

2 Select **Settings**.

3 From **Security Settings**, select **Global**.

4 From External Logging, select one of the following:

- Send Syslog from vGW management server - Central logging with syslog event provided from a management server.

If you select the option **Send Syslog from vGW management server**, all events forwarded to SIEM contain the IP address of the vGW management server.

- Send Syslog from Firewalls - Distribute logging with each Firewall Security VM providing syslog events.

5 Type values for the following parameters:
   a **Syslog Server** - Type the IP address of your vGW management server if you selected to **Send Syslog from vGW management server**. Or, type the IP address of SIEM if you selected Send Syslog from Firewalls.
   b **Syslog Server Port** - Type the port address for syslog. This is typically port 514.

6 From the External Logging panel, click **Save**.

   Only changes made to the External Logging section are stored when you click **Save**. Any changes made to NetFlow require that you save using the button within **NetFlow Configuration** section.

7 From the **NetFlow Configuration** panel, select the **enable** check box.

   NetFlow does not support central logging from a vGW management server. From the External Logging section, you must select the option **Send Syslog from Firewalls**.

8 Type values for the following parameters:
   a **NetFlow collector address** - Type the IP address of SIEM.
   b **NetFlow collector port** - Type a port address for NetFlow events.

NOTE

SIEM typically uses port 2055 for NetFlow event data on QFlow Collectors. You must configure a different NetFlow collector port on your Juniper Networks vGW Series Virtual Gateway for NetFlow.

9 From the **NetFlow Configuration**, click **Save**.

10 You are now ready to configure the log source in SIEM.

SIEM automatically detects syslog forwarded from Juniper Networks vGW. If you want to manually configure SIEM to receive syslog events:

From the **Log Source Type** list, select **Juniper vGW**.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information, see your Juniper Networks vGW documentation.

Juniper Security Binary Log Collector

The Juniper Security Binary Log Collector DSM for SIEM can accept audit, system, firewall and intrusion prevention system (IPS) events in binary format from Juniper SRX or Juniper Networks J Series appliances. The Juniper Networks binary log file format is intended to increase performance when writing large amounts of data to an event log. To integrate your device with SIEM, you must configure your Juniper appliance to stream binary formatted events, then configure a log source in SIEM.

This section includes the following topics:

Configuring the Juniper Networks Binary Log Format

The binary log format from Juniper SRX or J Series appliances are streamed to SIEM using the UDP protocol. You must specify a unique port for streaming binary formatted events, the standard syslog port for SIEM cannot understand binary formatted events. The default port assigned to SIEM for receiving streaming binary events from Juniper appliances is port 40798.

NOTE

The Juniper Binary Log Collector DSM only supports events forwarded in Streaming mode. The Event mode is not supported.

Procedure

1 Log in to your Juniper SRX or J Series using the command-line Interface (CLI).

2 Type the following command to edit your device configuration:
`configure`

3 Type the following command to configure the IP address and port number for streaming binary formatted events:

`set security log stream <Name> host <IP address> port <Port>`

Where:

`<Name>` is the name assigned to the stream.

`<IP address>` is the IP address of your SIEM Console or Event Collector.

`<Port>` is a unique port number assigned for streaming binary formatted events to SIEM. By default, SIEM listens for binary streaming data on port 40798. For a list of ports used by SIEM, see the *SIEM Common Ports List* technical note.

4 Type the following command to set the security log format to binary:
`set security log stream <Name> format binary`

Where `<Name>` is the name you specified for your binary format stream in Step 3.

5 Type the following command to enable security log streaming:
`set security log mode stream`

6 Type the following command to set the source IP address for the event stream:
`set security log source-address <IP address>`
Where `<IP address>` is the IP address of your Juniper SRX Series or Juniper J Series appliance.

7 Type the following command to save the configuration changes:
`commit`

8 Type the following command to exit the configuration mode:
`exit`
The configuration of your Juniper SRX or J Series appliance is complete. You are now ready to configure a log source in SIEM.

Configure a Log Source

SIEM does not automatically discover incoming Juniper Security Binary Log Collector events from Juniper SRX or Juniper J Series appliances.

If your events are not automatically discovered, you must manually create a log source using the **Admin** tab in SIEM.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Juniper Security Binary Log Collector**.

9 Using the Protocol Configuration list, select **Juniper Security Binary Log Collector**.

10 Configure the following values:

Table 122: Juniper Security Binary Log Collector protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address or hostname to identify the log source. The identifier address should be the Juniper SRX or J Series appliance generating the binary event stream.

Table 122: Juniper Security Binary Log Collector protocol parameters (Continued)

Parameter	Description
Binary Collector Port	Specify the port number used by the Juniper Networks SRX or J Series appliance to forward incoming binary data to SIEM. The UDP port number for binary data is the same port configured in Configuring the Juniper Networks Binary Log Format on page 344, Step 3. If you edit the outgoing port number for the binary event stream from your Juniper Networks SRX or J Series appliance, you must also edit your Juniper log source and update the **Binary Collector Port** parameter in SIEM. To edit the port: **1** In the **Binary Collector Port** field, type the new port number for receiving binary event data. **2** Click **Save**. Event collection is stopped for the log source until you fully deploy SIEM. **3** On the **Admin** tab, select **Advanced > Deploy Full Configuration**. The port update is complete and event collection starts on the new port number. **NOTE:** When you click Deploy Full Configuration, SIEM restarts all services, resulting in a gap in data collection for events and flows until the deployment completes.
XML Template File Location	Type the path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance. By default, SIEM includes an XML template file for decoding the binary stream in the following directory: `/opt/qradar/conf/security_log.xml`

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. You can verify events forwarded to SIEM by viewing events in the **Log Activity** tab.

Juniper Junos WebApp Secure

The Juniper WebApp Secure DSM for SIEM accepts events forwarded from Juniper Junos WebApp Secure appliances using syslog.

Juniper Junos WebApp Secure provides incident logging and access logging events to SIEM. Before you can receive events in SIEM, you must configure event forwarding on your Juniper Junos WebApp Secure, then define the events you want to forward.

Configuring Syslog Forwarding

To configure a remote syslog server for Juniper Junos WebApp Secure, you must SSH in to a configuration interface. The configuration interface allows you to setup or configure core settings on your Juniper Junos WebApp Secure appliance.

Procedure

1 Using SSH, log in to your Juniper Junos WebApp device using port 2022.
`https://<IP address>:<port>`
Where:
`<IP address>` is the IP address of your Juniper Junos WebApp Secure appliance.
`<Port>` is the port number of your Juniper Junos WebApp Secure appliance configuration interface. The default SSH configuration port is 2022.

2 From the Choose a Tool menu, select **Logging**.

3 Click **Run Tool**.

4 From the Log Destination menu, select **Remote Syslog Server**.

5 In the **Syslog Server** field, type the IP address of your SIEM Console or Event Collector.

6 Click **Save**.

7 From the Choose a Tool menu, select **Quit**.

8 Type **Exit** to close your SSH session.
You are now ready to configure event logging on your Juniper Junos WebApp Secure appliance.

Configuring Event Logging

The Juniper Junos WebApp Secure appliance must be configured to determine which logs are forwarded to SIEM.

Procedure

1 Using a web browser, log in to the Configuration Site for your Juniper Junos WebApp Secure appliance.
`https://<IP address>:<port>`
Where:
`<IP address>` is the IP address of your Juniper Junos WebApp Secure appliance.

<Port> is the port number of your Juniper Junos WebApp Secure appliance. The default configuration uses a port number of 5000.

2 From the navigation menu, select **Configuration Manager**.

3 From the Configuration menu, select **Basic Mode**.

4 Click the **Global Configuration** tab and select **Logging**.

5 Click the link **Show Advanced Options**.

6 Configure the following parameters:

Table 123: Juniper Junos WebApp Secure logging parameters

Parameter	Description
Access logging: Log Level	Click this option to configure the level of information logged when access logging is enabled. The options include: • **0** - Access logging is disabled. • **1** - Basic logging. • **2** - Basic logging with headers. • **3** - Basic logging with headers and body. **NOTE:** Access logging is disabled by default. It is recommended that you only enable access logging for debugging purposes. For more information, see your Juniper Junos WebApp Secure documentation.
Access logging: Log requests before processing	Click this option and select **True** to log the request before it is processed, then forward the event to SIEM.
Access logging: Log requests to access log after processing	Click this option and select **True** to log the request after it is processed. After Juniper Junos WebApp Secure processes the event, then it is forwarded to SIEM.
Access logging: Log responses to access log after processing	Click this option and select **True** to log the response after it is processed. After Juniper Junos WebApp Secure processes the event, then the event is forwarded to SIEM.
Access logging: Log responses to access log before processing	Click this option and select **True** to log the response before it is processed, then forward the event to SIEM.

Table 123: Juniper Junos WebApp Secure logging parameters (Continued)

Parameter	Description
Incident severity log level	Click this option to define the severity of the incident events to log. All incidents at or above the level defined are forwarded to SIEM. The options include: The options include: • **0** - Informational level and later incident events are logged and forwarded. • **1** - Suspicious level and later incident events are logged and forwarded. • **2** - Low level and later incident events are logged and forwarded. • **3** - Medium level and later incident events are logged and forwarded. • **4** - High level and later incident events are logged and forwarded.
Log incidents to the syslog	Click this option and select **Yes** to enable syslog forwarding to SIEM.

The configuration is complete. The log source is added to SIEM as Juniper Junos WebApp Secure events are automatically discovered. Events forwarded to SIEM by Juniper Junos WebApp Secure are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Juniper Junos WebApp Secure. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Juniper Junos WebApp Secure**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 124: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Juniper Junos WebApp Secure appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

Juniper Networks WLC Series Wireless LAN Controller

SIEM can collect and categorize syslog events from Juniper Networks WLC Series Wireless LAN Controllers.

Configuration Overview

To collect syslog events, you must configure your Juniper Networks Wireless LAN Controller to forward syslog events to SIEM. Administrators can use either the RingMaster interface or the command-line interface to configure syslog forwarding for their Juniper Networks Wireless LAN Controller appliance. SIEM automatically discovers and creates log sources for syslog events that are forwarded from Juniper Networks WLC Series Wireless LAN Controllers. SIEM supports syslog events from Juniper WLAN devices that run on Mobility System Software (MSS) V7.6.

To integrate Juniper WLC events with SIEM, administrators can complete the following tasks:

1 On your Juniper WLAN appliance, configure syslog server.

- To use the RingMaster user interface to configure a syslog server, see Configuring a Syslog Server from the Juniper WLC User Interface on page 350.
- To use the command-line interface to configure a syslog server, see Configuring a Syslog Server with the Command-Line Interface for Juniper WLC on page 351.

2 On your SIEM system, verify that the forwarded events are automatically discovered.

Configuring a Syslog Server from the Juniper WLC User Interface

To collect events, you must configure a syslog server on your Juniper WLC system to forward syslog events to SIEM.

Procedure

1 Log in to the RingMaster software.

2 From the Organizer panel, select a Wireless LAN Controller.

3 From the System panel, select **Log**.

4 From the Task panel, select **Create Syslog Server**.

5 In the **Syslog Server** field, type the IP address of your SIEM system.

6 In the **Port** field, type **514**.

7 From the **Severity Filter** list, select a severity.

Logging debug severity events can negatively affect system performance on the Juniper WLC appliance. As a best practice, administrators can log events at the error or warning severity level and slowly increase the level to get the data you need. The default severity level is error.

8 From the **Facility Mapping** list, select a facility between Local 0 - Local 7.

9 Click **Finish**.

Result

As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to SIEM. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the SIEM Console and verify that the log source is created on the Console. The **Log Activity** tab displays events from the Juniper WLC appliance.

Configuring a Syslog Server with the Command-Line Interface for Juniper WLC

To collect events, you must configure a syslog server on your Juniper WLC system to forward syslog events to SIEM.

Procedure

1 Log in to the command-line interface of the Juniper WLC appliance.

2 To configure a syslog server, type the following command:

```
set log server <ip-addr> [port 514 severity <severity-level>
local-facility <facility-level>]
```

For example, `set log server 1.1.1.1 port 514 severity error local-facility local0`.

3 To save the configuration, type the following command:

```
save configuration
```

Result

As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to SIEM. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the Console and verify that the log source is created. The **Log Activity** tab displays events from the Juniper WLC appliance.

60 Kaspersky Security Center

The Kaspersky Security Center DSM retrieves events directly from a database on your Kaspersky Security Center appliance.

Supported Event Types

SIEM uses the JDBC protocol to poll a view created specifically for SIEM to collect antivirus, server, and audit events.

Before You Begin

Before you can receive events in SIEM, you must create a database view for SIEM to poll using the JDBC protocol.

We also recommend that you create a user for SIEM, as SIEM requires a user account to poll the database for events. After you have configured a database view and a user account for SIEM, you are ready to configure a log source in SIEM for Kaspersky Security Center.

Creating a Database View for Kaspersky Security Center

To collect audit event data, you must create a database view on your Kaspersky server that is accessible to SIEM.

To create a database view, you can download the klsql2.zip tool, which is available from Kaspersky or use another program that allows you to create database views. The instructions provided below define the steps required to create the dbo.events view using the Kaspersky Labs tool.

Procedure

1 From the Kaspersky Labs website, download the klsql2.zip file: http://support.kaspersky.com/9284

2 Copy klsql2.zip to your Kaspersky Security Center Administration Server.

3 Extract klsql2.zip to a directory.

4 The following files are included:

- klsql2.exe
- libmysql.dll
- src.sql
- start.cmd

5 In any text editor, edit the src.sql file.

6 Clear the contents of the src.sql file.

7 Type the following Transact-SQL statement to create the dbo.events database view:

```
create view dbo.events as select e.nId, e.strEventType as
'EventId', e.wstrDescription as 'EventDesc', e.tmRiseTime as
'DeviceTime', h.nIp as 'SourceInt', e.wstrPar1, e.wstrPar2,
e.wstrPar3, e.wstrPar4, e.wstrPar5, e.wstrPar6, e.wstrPar7,
e.wstrPar8, e.wstrPar9 from dbo.v_akpub_ev_event e,
dbo.v_akpub_host h where e.strHostname = h.strName;
```

8 Save the src.sql file.

9 From the command line, navigate to the location of the klsql2 files.

10 Type the following command to create the view on your Kaspersky Security Center appliance:

```
klsql2 -i src.sql -o result.xml
```

The dbo.events view is created. You are now ready to configure the log source in SIEM to poll the view for Kaspersky Security Center events.

NOTE

Kaspersky Security Center database administrators should ensure that SIEM is allowed to poll the database for events using TCP port 1433 or the port configured for your log source. Protocol connections are often disabled on databases by default and additional configuration steps might be required to allow connections for event polling. Any firewalls located between Kaspersky Security Center and SIEM should also be configured to allow traffic for event polling.

Configuring the Log Source in SIEM

SIEM requires a user account with the proper credentials to access the view you created in the Kaspersky Security Center database.

To successfully poll for audit data from the Kaspersky Security Center database, you must create a new user or provide the log source with existing user credentials to read from the dbo.events view. For more information on creating a user account, see your Kaspersky Security Center documentation.

Procedure

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select **Kaspersky Security Center**.

7 From the Protocol Configuration list, select JDBC.

8 Configure the following values:

Table 125: JDBC protocol parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Kaspersky Database>@<Kaspersky Database Server IP or Host Name>` Where: `<Kaspersky Database>` is the database name, as entered in the Database Name parameter. `<Kaspersky Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type KAV as the name of the Kaspersky Security Center database.
IP or Hostname	Type the IP address or hostname of the SQL server that hosts the Kaspersky Security Center database.
Port	Type the port number used by the database server. The default port for MSDE is 1433. You must enable and verify you can communicate using the port you specify in the **Port** field. The JDBC configuration port must match the listener port of the Kaspersky database. The Kaspersky database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username the log source can use to access the Kaspersky database.
Password	Type the password the log source can use to access the Kaspersky database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the **Password** field.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type dbo.events as the name of the table or view that includes the event records.

Table 125: JDBC protocol parameters (Continued)

Parameter	Description
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type nld as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Kaspersky Security Center log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The Kaspersky Security Center configuration is complete. Events collected using the JDBC protocol are displayed on the **Log Activity** tab of SIEM.

61 Lieberman Random Password Manager

The Lieberman Random Password Manager DSM for allows you to integrate SIEM with Lieberman Enterprise Random Password Manager and Lieberman Random Password Manager software using syslog events in the Log Extended Event Format (LEEF).

The Lieberman Random Password Manager forwards syslog events to SIEM using Port 514. SIEM records all relevant password management events. For information on configuring syslog forwarding, see your vendor documentation.SIEM

SIEM automatically detects syslog events forwarded from Lieberman Random Password Manager and Lieberman Enterprise Random Password Manager devices. However, if you want to manually configure SIEM to receive events from these devices:

From the Log Source Type list, select Lieberman Random Password Manager.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

62 Linux

This section provides information on the Linux DHCP, IPtables, and OS DSMs:

Linux DHCP

The Linux DHCP Server DSM for SIEM accepts DHCP events using syslog.

Configuring Syslog for Linux DHCP

SIEM records all relevant events from a Linux DHCP Server. Before you configure SIEM to integrate with a Linux DHCP Server, you must configure syslog within your Linux DHCP Server to forward syslog events to SIEM.

For more information on configuring your Linux DHCP Server, consult the man pages or associated documentation for your DHCP daemon.

Configuring a Log Source

SIEM automatically discovers and creates log sources for syslog events forwarded from Linux DHCP Servers. The following procedure is optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your Linux DHCP Server.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **Linux DHCP Server**.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 126: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Linux DHCP Server.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

Linux IPtables

The Linux IPtables DSM for SIEM accepts firewall IPtables events using syslog.

SIEM records all relevant from Linux IPtables where the syslog event contains any of the following words: Accept, Drop, Deny, or Reject. Creating a customized log prefix in the event payload allows SIEM to easily identify IPtables behavior.

Configure IPtables

IPtables is a powerful tool, which allows you to create rules on the Linux kernel firewall for routing traffic.

To configure IPtables, you must examine the existing rules, modify the rule to log the event, and assign a log identifier to your IPtables rule that can be identified by SIEM. This process allows you to determine which rules are logged by SIEM. SIEM includes any events that are logged that include the words: accept, drop, reject, or deny in the event payload.

Procedure

1 Using SSH, log in to your Linux Server as a root user.

2 Edit the IPtables file in the following directory:
`/etc/iptables.conf`

NOTE

The file containing IPtables rules can vary according to the specific Linux operating system you are configuring. For a system operating Red Hat Enterprise, the file is in the /etc/sysconfig/iptables directory. Consult your Linux operating system documentation for more information on configuring IPtables.

3 Review the file to determine the IPtables rule you want to log.
For example, if you want to log the rule defined by the entry:
```
-A INPUT -i eth0 --dport 31337 -j DROP
```

4 Insert a matching rule immediately before each rule you want to log:
```
-A INPUT -i eth0 --dport 31337 -j DROP
-A INPUT -i eth0 --dport 31337 -j DROP
```

5 Update the target of the new rule to LOG for each rule you want to log. For example:
```
-A INPUT -i eth0 --dport 31337 -j LOG
-A INPUT -i eth0 --dport 31337 -j DROP
```

6 Set the log level of the LOG target to a SYSLOG priority level, such as info or notice:
```
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info
-A INPUT -i eth0 --dport 31337 -j DROP
```

7 Configure a log prefix to identify the rule behavior. Set the log prefix parameter to `Q1Target=<rule>`.
Where `<rule>` is one of fw_accept, fw_drop, fw_reject, or fw_deny.

For example, if the rule being logged by the firewall targets dropped events, the log prefix setting should be `Q1Target=fw_drop`.

```
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-
prefix "Q1Target=fw_drop "
-A INPUT -i eth0 --dport 31337 -j DROP
```

NOTE

The trailing space is required before the closing quotation mark.

8 Save and exit the file.

9 Restart IPtables:

```
/etc/init.d/iptables restart
```

10 Open the `syslog.conf` file.

11 Add the following line:

```
kern.<log level>          @<IP address>
```

Where:

`<log level>` is the previously set log level.

`<IP address>` is the IP address of SIEM.

12 Save and exit the file.

13 Restart the syslog daemon:

```
/etc/init.d/syslog restart
```

After the syslog daemon restarts, events are forwarded to SIEM. IPtable events forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates log sources for IPtables syslog events forwarded from Linux Servers. The following steps for configuring a log source are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your Linux DHCP Server.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Linux iptables Firewall.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 127: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for IPtables events forwarded from your Linux Server.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. IPtables events forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of SIEM.

For more information on configuring IPtables on Linux Servers, consult the man pages or your associated Linux documentation.

Linux OS

The Linux OS DSM for SIEM records Linux operating system events and forwards the events using syslog or syslog-ng.

If you are using syslog on a UNIX host, upgrade the standard syslog to a more recent version, such as, syslog-ng.

Do not run both syslog and syslog-ng at the same time.

To integrate Linux OS with SIEM, select one of the following syslog configurations for event collection:

- Configuring Linux OS using syslog (page 7)
- Configure Linux OS using syslog-ng (page 7)

You can also configure your Linux operating system to send audit logs to SIEM. For more information, see Configuring Linux OS to Send Audit Logs on page 365.

Supported Event Types

The Linux OS DSM supports the following event types:

- cron
- HTTPS
- FTP
- NTP
- Simple Authentication Security Layer (SASL)
- SMTP
- SNMP
- SSH
- Switch User (SU)
- Pluggable Authentication Module (PAM) events.

Configuring Linux OS using syslog

Configure Linux OS using the syslog protocol.

Procedure

1 Log in to your Linux OS device, as a root user.

2 Open the `/etc/syslog.conf` file.

3 Add the following facility information:

```
authpriv.*              @<IP address>
```

Where `<IP address>` is the IP address of the SIEM.

4 Save the file.

5 Restart syslog:

```
service syslog restart
```

6 Log in to the SIEM user interface.

7 Add a Linux OS log source. For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

8 On the **Admin** tab, click **Deploy Changes**.

For more information on syslog, see your Linux operating system documentation.

Configure Linux OS Using Syslog-ng

Configure Linux OS using the syslog-ng protocol.

Procedure

1 Log in to your Linux OS device, as a root user.

2 Open the `/etc/syslog-ng/syslog-ng.conf` file.

3 Add the following facility information:

```
filter auth_filter{ facility(authpriv); };
destination auth_destination { tcp("<IP address>" port(514)); };
log{
        source(<Sourcename>);
           filter(auth_filter);
        destination(auth_destination);
};
```

Where:

`<IP address>` is the IP address of the SIEM.

`<Source name>` is the name of the source defined in the configuration file.

4 Save the file.

5 Restart syslog-ng:

```
service syslog-ng restart
```

6 Log in to the SIEM user interface.

7 Add a Linux OS log source. For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

8 On the **Admin** tab, click **Deploy Changes**.

For more information on syslog-ng, see your Linux operating system documentation.

Configuring Linux OS to Send Audit Logs

Configure Linux OS to send audit logs to SIEM.

About this task

This task applies to Red Hat Enterprise Linux v6 operating systems. If you use SUSE, Debian, or Ubuntu operating system, see your vendor documentation for specific steps for your operating system.

Procedure

1 Log in to your Linux OS device, as a root user.

2 Type the following commands:

```
yum install audit
service auditd start
chkconfig auditd on
```

3 Open the following file:

```
/etc/audisp/plugins.d/syslog.conf
```

4 Ensure the parameters match the following values:

```
active = yes
direction = out
path = builtin_syslog
type = builtin
args = LOG_LOCAL6
format = string
```

5 Open the following file:

```
/etc/rsyslog.conf
```

6 Add the following line to the end of the file:

```
local6.* @@SIEM_Collector_IP_address
```

7 Log in to the SIEM user interface.

8 Add a Linux OS log source. For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

9 On the **Admin** tab, click **Deploy Changes**.

10 Log in to SIEM as the root user.

11 Type the following commands:

```
service auditd restart
service syslog restart
```

63 McAfee

This section provides information on the following DSMs:

McAfee ePolicy Orchestrator

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

McAfee Intrushield

A SIEM McAfee Intrushield DSM accepts events that use syslog. SIEM records all relevant events.

Before you configure SIEM to integrate with a McAfee Intrushield device, you must select your McAfee Intrushield version.

- To collect alert events from McAfee Intrushield V2.x - V5.x, see Configuring Alert Events for McAfee Intrushield V2.x - V5.x on page 366.
- To collect alert events from McAfee Intrushield V6.x - V7.x, see Configuring Alert Events for McAfee Intrushield V6.x and V7.x on page 368.
- To collect fault notification events from McAfee Intrushield V6.x - V7.x, see Configuring Fault Notification Events for McAfee Intrushield V6.x and V7.x on page 370.

Configuring Alert Events for McAfee Intrushield V2.x - V5.x

To collect alert notification events from McAfee Intrushield, administrators must configure a syslog forwarder to send events to SIEM

Procedure

1 Log in to the McAfee Intrushield Manager user interface.

2 In the dashboard click Configure.

3 From the Resource Tree, click the root node (Admin-Domain-Name).

4 Select **Alert Notification > Syslog Forwarder**.

5 Type the Syslog Server details.
   a The Enable Syslog Forwarder must be configured as Yes.
   b The Port must be configured to 514.

6 Click Edit.

7 Choose one of the following:

Table 128: McAfee Intrushield V2.x - V5.x custom message formats

Parameter	Description
Unpatched McAfee Intrushield V2.x systems	|$ALERT_ID$|$ALERT_TYPE$|$ATTACK_TIME$|"$ATTACK_NAME$"|$ATTACK_ID$|$ATTACK_SEVERITY$|$ATTACK_SIGNATURE$|$ATTACK_CONFIDENCE$|$ADMIN_DOMAIN$|$SENSOR_NAME$|$INTERFACE$|$SOURCE_IP$|$SOURCE_PORT$|$DESTINATION_IP$|$DESTINATION_PORT$|
McAfee Intrushield that have patches applied to update to V3.x - V5.x	|IV_ALERT_ID|IV_ALERT_TYPE|IV_ATTACK_TIME|"IV_ATTACK_NAME"|IV_ATTACK_ID|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|IV_ADMIN_DOMAIN|IV_SENSOR_NAME|$IV_INTERFACE$|IV_SOURCE_IP|IV_SOURCE_PORT|$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|

NOTE

The custom message string must be entered as a single line without carriage returns or spaces. McAfee Intrushield appliances that do not have software patches applied use different message strings than patched systems. McAfee Intrushield expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly.

If you are unsure what event message format to use, contact McAfee Customer Support.

8 Click **Save**.

Result

As events are generated by McAfee Intrushield, they are forwarded to the syslog destination that you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Intrushield appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the SIEM Console and and verify that the log source is created on the Console and that the **Log Activity** tab displays events from the McAfee Intrushield appliance.

Configuring Alert Events for McAfee Intrushield V6.x and V7.x

To collect alert notification events from McAfee Intrushield, administrators must configure a syslog forwarder to send events to SIEM

Procedure

1 Log in to the McAfee Intrushield Manager user interface.

2 On the Network Security Manager dashboard, click Configure.

3 Expand the Resource Tree, click **IPS Settings** node.

4 Click the **Alert Notification** tab.

5 In the Alert Notification menu, click the **Syslog** tab.

6 Configure the following parameters to forward alert notification events:

Table 129: McAfee Intrushield v6.x & 7.x alert notification parameters

Parameter	Description
Enable Syslog Notification	Select **Yes** to enable syslog notifications for McAfee Intrushield. You must enable this option to forward events to SIEM.
Admin Domain	Select any of the following options: • **Current** - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Select this check box to send syslog notifications for alerts in any child domains within the current domain.
Server Name or IP Address	Type the IP address of your SIEM Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
UDP Port	Type **514** as the UDP port for syslog events.
Facility	Select a syslog facility value.
Severity Mappings	Select a value to map the informational, low, medium, and high alert notification level to a syslog severity. The options include: • **Emergency** - The system is down or unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system has a warning message indicating an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages.

Table 129: McAfee Intrushield v6.x & 7.x alert notification parameters (Continued)

Parameter	Description
Send Notification If	Select the following check boxes: • **The attack definition has this notification option explicitly enabled** • **The following notification filter is matched** - From the list, select **Severity Informational and later**.
Notify on IPS Quarantine Alert	Select **No** as the notify on IPS quarantine option.
Message Preference	Select the **Customized** option.

7 From the **Message Preference** field, click **Edit** to add a custom message filter.

8 To ensure that alert notifications are formatted correctly, type the following message string:

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"
|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATT
ACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_INTERFACE$|
$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|$IV_DESTINATIO
N_PORT$|$IV_DIRECTION$|$IV_SUB_CATEGORY$
```

NOTE

The custom message string must be entered as a single line without carriage returns or spaces. McAfee Intrushield expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly.

You might require a text editor to properly format the custom message string as a single line.

9 Click Save.

Result

As alert events are generated by McAfee Intrushield, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Intrushield appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the SIEM Console and and verify that the log source is created on the Console and that the **Log Activity** tab displays events from the McAfee Intrushield appliance.

Configuring Fault Notification Events for McAfee Intrushield V6.x and V7.x

To integrate fault notifications with McAfee Intrushield, you must configure your McAfee Intrushield to forward fault notification events.

Procedure

1 Log in to the McAfee Intrushield Manager user interface.

2 On the Network Security Manager dashboard, click Configure.

3 Expand the Resource Tree, click **IPS Settings** node.

4 Click the **Fault Notification** tab.

5 In the Alert Notification menu, click the **Syslog** tab.

6 Configure the following parameters to forward fault notification events:

Table 130: McAfee Intrushield V6.x - V7.x fault notification parameters

Parameter	Description
Enable Syslog Notification	Select **Yes** to enable syslog notifications for McAfee Intrushield. You must enable this option to forward events to SIEM.
Admin Domain	Select any of the following options: • **Current** - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Select this check box to send syslog notifications for alerts in any child domains within the current domain.
Server Name or IP Address	Type the IP address of your SIEM Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
Port	Type **514** as the port for syslog events.
Facilities	Select a syslog facility value.

Table 130: McAfee Intrushield V6.x - V7.x fault notification parameters (Continued)

Parameter	Description
Severity Mappings	Select a value to map the informational, low, medium, and high alert notification level to a syslog severity. The options include: • **Emergency** - The system is down or unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system has a warning message indicating an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages.
Forward Faults with severity level	Select **Informational and later**.
Message Preference	Select the **Customized** option.

7 From the **Message Preference** field, click **Edit** to add a custom message filter.

8 To ensure that fault notifications are formatted correctly, type the following message string:

```
|%INTRUSHIELD-FAULT|$IV_FAULT_NAME$|$IV_FAULT_TIME$|
```

NOTE

The custom message string must be entered as a single line with no carriage returns. McAfee Intrushield expects the format of the custom message syslog information to contain a dollar sign ($) delimiter before and after each element. If you are missing a dollar sign for an element, the event might not parse properly.

9 Click Save.

Result

As fault events are generated by McAfee Intrushield, they are forwarded to the syslog destination that you specified.

What to do next

You can log in to the SIEM Console and verify that the **Log Activity** tab contains fault events from the McAfee Intrushield appliance.

McAfee Application / Change Control

The McAfee Application / Change Control DSM for SIEM accepts change control events using Java Database Connectivity (JDBC). SIEM records all relevant McAfee Application / Change Control events. This document includes information on configuring SIEM to access the database containing events using the JDBC protocol.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the Log Sources icon.

4 Click Add.

5 Using the Log Source Type list, select McAfee Application / Change Control.

6 Using the Protocol Configuration list, select JDBC.

You must refer to the Configure Database Settings on your Application / Change Control Management Console to configure the McAfee Application / Change Control DSM in SIEM.

7 Configure the following values:

Table 131: McAfee Application / Change Control JDBC protocol parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<McAfee Change Control Database>@<Change Control Database Server IP or Host Name>` Where: `<McAfee Change Control Database>` is the database name, as entered in the Database Name parameter. `<Change Control Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. When defining a name for your log source identifier, you must use the values of the McAfee Change Control Database and Database Server IP address or hostname from the ePO Management Console.
Database Type	From the list, select MSDE.
Database Name	Type the exact name of the McAfee Application / Change Control database.
IP or Hostname	Type the IP address or host name of the McAfee Application / Change Control SQL Server.

Table 131: McAfee Application / Change Control JDBC protocol parameters (Continued)

Parameter	Description
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the McAfee Application / Change Control database. The McAfee Application / Change Control database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type SCOR_EVENTS as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type AutoID as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.

Table 131: McAfee Application / Change Control JDBC protocol parameters (Continued)

Parameter	Description
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. **NOTE:** Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your McAfee Application / Change Control log source with a higher importance compared to other log sources in SIEM.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

McAfee Web Gateway

You can configure McAfee Web Gateway to integrate with SIEM using one of the following methods:

- Configuring McAfee Web Gateway to Communicate with SIEM (Syslog) on page 376
- Configuring McAfee Web Gateway to Communicate with SIEM (Log File Protocol) on page 377

NOTE

McAfee Web Gateway is formerly known as McAfee WebWasher.

The following table identifies the specifications for the McAfee Web Gateway DSM:

Table 132: McAfee Web Gateway DSM specifications

Specification	Value
Manufacturer	McAfee
DSM	McAfee Web Gateway
RPM file name	DSM-McAfeeWebGateway-*siemversion-buildnumber*.noarch
Supported versions	v6.0.0 and later
Protocol	Syslog, Log File Protocol
SIEM recorded events	All relevant events
Automatically discovered	Yes
Includes identity	No
More information	*McAfee web site* (www.mcafee.com)

McAfee Web Gateway DSM Integration Process

To integrate McAfee Web Gateway DSM with SIEM, use the following procedure:

1 Download and install the most recent version of the McAfee Web Gateway DSM RPM on your SIEM Console.

2 For each instance of McAfee Web Gateway, configure your McAfee Web Gateway VPN system to enable communication with SIEM.

3 If SIEM does not automatically discover the log source, for each McAfee Web Gateway server you want to integrate, create a log source on the SIEM Console.

4 If you use McAfee Web Gateway v7.0.0 or later, create an event map.

Related tasks

Manually Installing a DSM on page 4

Configuring McAfee Web Gateway to Communicate with SIEM (Syslog) on page 376

Configuring McAfee Web Gateway to Communicate with SIEM (Log File Protocol) on page 377

Creating an Event Map for McAfee Web Gateway Events on page 379

Configuring McAfee Web Gateway to Communicate with SIEM (Syslog)

To collect all events from McAfee Web Gateway, you must specify SIEM as the syslog server and configure the message format.

Procedure

1 Log in to your McAfee Web Gateway console.

2 Using the toolbar, click Configuration.

3 Click the File Editor tab.

4 Expand the appliance files and select the file **/etc/rsyslog.conf.**

The file editor displays the rsyslog.conf file for editing.

5 Modify the rsyslog.conf file to include the following information:

```
# send access log to qradar
*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/
messages
*.info;mail.none;authpriv.none;cron.none @<IP Address>:<Port>
```

Where:

`<IP Address>` is the IP address of SIEM.

`<Port>` is the syslog port number, for example 514.

6 Click Save Changes.

You are now ready to import a policy for the syslog handler on your McAfee Web Gateway appliance. For more information, see Importing the Syslog Log Handler on page 376.

Importing the Syslog Log Handler

To Import a policy rule set for the syslog handler:

1 From the support website, download the following compressed file:

`log_handlers-1.1.tar.gz`

2 Extract the file.

The extract file provides XML files that are version dependent to your McAfee Web Gateway appliance.

Table 133: McAfee Web Gateway required log handler file

Version	Required XML file
McAfee Web Gateway V7.0	syslog_loghandler_70.xml
McAfee Web Gateway V7.3	syslog_loghandler_73.xml

3 Log in to your McAfee Web Gateway console.

4 Using the menu toolbar, click Policy.

5 Click Log Handler.

6 Using the menu tree, select Default.

7 From the Add list, select Rule Set from Library.

8 Click Import from File button.

9 Navigate to the directory containing the syslog_handler file you downloaded in and select syslog_loghandler.xml as the file to import.

NOTE

If the McAfee Web Gateway appliance detects any conflicts with the rule set, you must resolve the conflict. For more information, see your McAfee Web Gateway documentation.

10 Click OK.

11 Click Save Changes.

12 You are now ready to configure the log source in SIEM.

SIEM automatically discovers syslog events from a McAfee Web Gateway appliance.

If you want to manually configure SIEM to receive syslog events, select McAfee Web Gateway from the Log Source Type list.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Configuring McAfee Web Gateway to Communicate with SIEM (Log File Protocol)

The McAfee Web Gateway appliance allows you to forward event log files to an interim file server for retrieval by SIEM.

Procedure

1 From the support website, download the following file:
`log_handlers-1.1.tar.gz`

2 Extract the file.

This will give you the access handler file required to configure your McAfee Web Gateway appliance.
`access_log_file_loghandler.xml`

3 Log in to your McAfee Web Gateway console.

4 Using the menu toolbar, click Policy.

NOTE

If there is an existing access log configuration in your McAfee Web Gateway appliance, you must delete the existing access log from the Rule Set Library before adding access_log_file_loghandler.xml.

5 Click Log Handler.

6 Using the menu tree, select Default.

7 From the Add list, select Rule Set from Library.

8 Click Import from File button.

9 Navigate to the directory containing the access_log_file_loghandler.xml file you downloaded and select syslog_loghandler.xml as the file to import.

When importing the rule set for access_log_file_loghandler.xml, a conflict occurs stating the Access Log Configuration already exists in the current configuration and a conflict solution is presented.

10 If the McAfee Web Gateway appliance detects that the Access Log Configuration already exists, select the Conflict Solution: Change name option presented to resolve the rule set conflict.

For more information on resolving conflicts, see your McAfee Web Gateway vendor documentation.

You must configure your access.log file to be pushed to an interim server on an auto rotation. It does not matter if you push your files to the interim server based on time or size for your access.log file. For more information on auto rotation, see your McAfee Web Gateway vendor documentation.

NOTE

Due to the size of access.log files generated, we recommend you select the option GZIP files after rotation in your McAfee Web Gate appliance.

11 Click OK.

12 Click Save Changes.

NOTE

By default McAfee Web Gateway is configured to write access logs to the /opt/mwg/log/user-defined-logs/access.log/ directory.

You are now ready to configure SIEM to receive access.log files from McAfee Web Gateway. For more information, see Pulling Data Using the Log File Protocol on page 379.

Pulling Data Using the Log File Protocol

A log file protocol source allows SIEM to retrieve archived log files from a remote host. The McAfee Web Gateway DSM supports the bulk loading of access.log files using the log file protocol source. The default directory for the McAfee Web Gateway access logs are

You are now ready to configure the log source and protocol in SIEM:

1 To configure SIEM to receive events from a McAfee Web Gateway appliance, select McAfee Web Gateway from the Log Source Type list.

2 To configure the protocol, you must select the Log File option from the Protocol Configuration list.

3 To configure the **File Pattern** parameter, you must type a regex string for the access.log file, such as access[0-9]+\.log.

NOTE

If you selected to GZIP your access.log files, you must type access[0-9]+\.log\.gz for the **FIle Pattern** field and from the Processor list, select GZIP.

Creating an Event Map for McAfee Web Gateway Events

Event mapping is required for all events that are collected from McAfee Web Gateway v7.0.0 and later.

You can individually map each event for your device to an event category in SIEM. Mapping events allows SIEM to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, some events that are displayed in the **Log Activity** tab for McAfee Web Gateway are categorized as `unknown`. and some events might be already assigned to an existing QID map. Unknown events are easily identified as the **Event Name** column and **Low Level Category** columns display Unknown.

Discovering Unknown Events

This ensures that you map all event types and that you do not miss events that are not generated frequently, repeat this procedure several times over a period of time.

Procedure

1 Log in to SIEM.

1 Click the **Log Activity** tab.

2 Click **Add Filter**.

3 From the first list, select **Log Source**.

4 From the **Log Source Group** list, select the log source group or **Other**.
Log sources that are not assigned to a group are categorized as Other.

5 From the **Log Source** list, select your McAfee Web Gateway log source.

6 Click **Add Filter**.

The **Log Activity** tab is displayed with a filter for your log source.

7 From the **View** list, select **Last Hour**.

Any events generated by the McAfee Web Gateway DSM in the last hour are displayed. Events displayed as unknown in the Event Name column or Low Level Category column require event mapping in SIEM.

NOTE

You can save your existing search filter by clicking **Save Criteria**.

You are now ready to modify the event map.

Modifying the Event Map

Modifying an event map allows you to manually categorize events to a SIEM Identifier (QID) map. Any event categorized to a log source can be remapped to a new SIEM Identifier (QID).

NOTE

Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1 On the Event Name column, double-click an unknown event for McAfee Web Gateway.

The detailed event information is displayed.

2 Click **Map Event**.

3 From the Browse for QID pane, select any of the following search options to narrow the event categories for a SIEM Identifier (QID):

a From the **High-Level Category** list, select a high-level event categorization.

b From the **Low-Level Category** list, select a low-level event categorization.

c From the **Log Source Type** list, select a log source type.

The **Log Source Type** list allows you to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, McAfee Web Gateway provides policy events, you might select another product that likely captures similar events.

d To search for a QID by name, type a name in the **QID/Name** field.

The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, policy.

4 Click **Search**.

A list of QIDs are displayed.

5 Select the QID you want to associate to your unknown event.

6 Click **OK**.

SIEM maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by SIEM.

If you update an event with a new SIEM Identifier (QID) map, past events stored in SIEM are not updated. Only new events are categorized with the new QID.

64 MetaInfo MetaIP

The MetaInfo MetaIP DSM for SIEM accepts MetaIP events using syslog.

SIEM records all relevant and available information from the event. Before configuring a MetaIP device in SIEM, you must configure your device to forward syslog events. For information on configuring your MetaInfo MetaIP appliance, see your vendor documentation.

After you configure your MetaInfo MetaIP appliance the configuration for SIEM is complete. SIEM automatically discovers and creates a log source for syslog events forwarded from MetaInfo MetaIP appliances. However, you can manually create a log source for SIEM to receive syslog events. The following configuration steps are optional.

To manually configure a log source for MetaInfo MetaIP:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Metainfo MetaIP.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 134: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your MetaInfo MetaIP appliances.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

65 Microsoft

This section provides information on DSMs for Microsoft products.

Microsoft Exchange Server

The Microsoft Exchange Server DSM for SIEM accepts Exchange events by polling for event log files.

Supported Versions

SIEM supports collecting events from Microsoft Exchange Servers with the following products:

Table 135: Microsoft Exchange Supported Versions

Version	Product
Microsoft Exchange 2003	WinCollect **NOTE:** For more information, see the WinCollect User Guide.
Microsoft Exchange 2007	Microsoft Exchange Protocol
Microsoft Exchange 2010	Microsoft Exchange Protocol

Supported Event Types

The Microsoft Exchange Protocol for SIEM supports several event types for mail and security events. Each event type contains events in a separate log file on your Microsoft Exchange Server. To retrieve events, you must create a log source in SIEM to poll the Exchange Server for the event log, which is downloaded by the Microsoft Exchange Protocol.

SIEM supports the following event types for Microsoft Exchange:

- Outlook Web Access events (OWA)
- Simple Mail Transfer Protocol events (SMTP)
- Message Tracking Protocol events (MSGTRK)

The log files for each event type are located in the following default directories:

Table 136: Microsoft Exchange Server Default File Path

Version	Event Type	Default File Path
Microsoft Exchange 2003	OWA	c$/WINDOWS/system32/LogFiles/W3SVC1/
	SMTP	c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/
	MSGTRK	Not supported with SIEM.

Table 136: Microsoft Exchange Server Default File Path

Version	Event Type	Default File Path
Microsoft Exchange 2007	OWA	c$/WINDOWS/system32/LogFiles/W3SVC1/
	SMTP	c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/
	MSGTRK	c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/
Microsoft Exchange 2010	OWA	c$/inetpub/logs/LogFiles/W3SVC1/
	SMTP	c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/
	MSGTRK	c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/

The Exchange Protocol configuration supports file paths that allow you to define a drive letter with the path information. The default file paths are typical for standard Exchange Server installations, but if you have changed the ExchangeInstallPath environment variable, you need to adjust the Microsoft Exchange Protocol accordingly. The Microsoft Exchange Protocol is capable of reading subdirectories of the OWA, SMTP, and MSGTRK folders for event logs.

Directory paths can be specified in the following formats:

- Correct - c$/LogFiles/
- Correct - LogFiles/
- Incorrect - c:/LogFiles
- Incorrect - c$\LogFiles

Required Ports and Privileges

The Microsoft Exchange Protocol polls your Exchange Server for OWA, SMTP, and MSGTRK event logs using NetBIOS.

You must ensure any firewalls located between the Exchange Server and the remote host being remotely polled allow traffic on the following ports:

- **TCP port 135** is used by the Microsoft Endpoint Mapper.
- **UDP port 137** is used for NetBIOS name service.
- **UDP port 138** is used for NetBIOS datagram service.
- **TCP port 139** is used for NetBIOS session service.
- **TCP port 445** is required for Microsoft Directory Services to transfer files across a Windows share.

If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the proper access required to read the log files. Local or domain administrators have sufficient privileges to access log files that reside on administrative shares. Clearing the file path information from any log folder path field disables monitoring for that log type.

Configure OWA Logs

Outlook Web Access event logs for Microsoft Exchange are generated by the Microsoft Internet Information System (IIS) installed with your Windows operating system.

IIS is capable of writing OWA event logs in several different formats. We recommend using the W3C log file format because the W3C format contains the highest level of configurable logging detail.

The following log formats are supported by the Microsoft Exchange Protocol:

- W3C
- NCSA
- IIS

The configuration steps to enable OWA event logs for your Microsoft Exchange Server is dependant on the version of IIS installed.

Table 137: Microsoft IIS Versions

Operating system	IIS version
Microsoft Server 2003	IIS 6.0
Microsoft Server 2008	IIS 7.0
Microsoft Server 2008R2	IIS 7.0

Configure OWA Event Logs with IIS 6.0

To configure OWA event logs for Microsoft IIS 6.0:

1 On the desktop, select **Start > Run**.

2 Type the following command:
`inetmgr`

3 Click OK.

4 In the IIS 6.0 Manager menu tree, expand Local Computer.

5 Expand Web Sites.

6 Right-click **Default Web Site** and select Properties.

7 From the Active Log Format list, choose one of the following options:

- Select W3C (Go to Step 8)
- Select NCSA (Go to Step 11)
- Select IIS (Go to Step 11)

8 Click Properties.

9 Click the Advanced tab.

10 From the list of properties, select all properties that you want to apply to the Microsoft Exchange Server DSM. You must select the following check boxes:

- **Method (cs-method)**
- **Protocol Version (cs-version)**

11 Click OK.

SIEM supports OWA, SMTP, and MSGTRK event logs. After you configure the event log types required, then you are ready to create a log source in SIEM.

Configure OWA Event Logs with IIS 7.0

To configure OWA event logs for Microsoft IIS 7.0:

1 On the desktop, select **Start > Run**.

2 Type the following command:
`inetmgr`

3 Click OK.

4 In the IIS 7.0 Manager menu tree, expand Local Computer.

5 Click Logging.

6 From the Format list, choose one of the following options:

- Select W3C (Go to Step 7)
- Select NCSA (Go to Step 9)
- Select IIS (Go to Step 9)

7 Click Select Fields.

8 From the list of properties, select all properties that you want to apply to the Microsoft Exchange Server DSM. You must select the following check boxes:
   - **Method (cs-method)**
   - **Protocol Version (cs-version)**

9 Click OK.Mic

SIEM supports OWA, SMTP, and MSGTRK event logs. After you configure all of the event log types you want to collect, then you are ready to create a log source in SIEM.

Configure SMTP Logs

SMTP logs created by the Exchange Server write SMTP send and receive email events that are part of the message delivery process.

SMTP protocol logging is not enabled by default on Exchange 2007 or Exchange 2010 installations. You must enable SMTP logging on both send and receive connectors. The instructions for enabling SMTP event logs apply to both Exchange Server 2007 and Exchange Server 2010.

To enable SMTP event logs:

1 Start the Exchange Management Console.

2 Configure your receive connector based on the server type:

- For edge transport servers - In the console tree, select **Edge Transport** and click the **Receive Connectors** tab.
- For hub transport servers - In the console tree, select **Server Configuration > Hub Transport**, then select the server and click the **Receive Connectors** tab.

3 Select your Receive Connector and click **Properties**.

4 Click the **General** tab.

5 From the **Protocol logging level** list, select **Verbose**.

6 Click **Apply**.

7 Click **OK**.

You are now ready to configure your send connectors.

8 Configure your send connector based on the server type:

- For edge transport servers - In the console tree, select **Edge Transport** and click the **Send Connectors** tab.
- For hub transport servers - In the console tree, select **Organization Configuration > Hub Transport**, then select the server and click the **Send Connectors** tab.

9 Select your Send Connector and click **Properties**.

10 Click the **General** tab.

11 From the **Protocol logging level** list, select **Verbose**.

12 Click **Apply**.

13 Click **OK**.

Logging for SMTP is now enabled.

Configure MSGTRK Logs

Message Tracking logs created by the Exchange Server detail the message activity that takes on your Exchange Server, including the message path information.

MSGTRK logs are enabled by default on Exchange 2007 or Exchange 2010 installations. The following configuration steps are optional.

To enable MSGTRK event logs:

1 Start the Exchange Management Console.

2 Configure your receive connector based on the server type:

- For edge transport servers - In the console tree, select **Edge Transport** and click **Properties**.
- For hub transport servers - In the console tree, select **Server Configuration > Hub Transport**, then select the server and click **Properties**.

3 Click the **Log Settings** tab.

4 Select the **Enable message tracking** check box.

5 Click **Apply**.

6 Click **OK**.

MSGTRK events are now enabled on your Exchange Server.

Configure a Log Source

The Microsoft Windows Exchange protocol supports SMTP, OWA, and message tracking logs for Microsoft Exchange.

To configure a log source:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select Microsoft Exchange Server.

7 From the Protocol Configuration list, select **Microsoft Exchange**.

8 Configure the following parameters:

Table 138: Microsoft Exchange Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the Windows Exchange event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source.
Server Address	Type the IP address of the Microsoft Exchange server.
Domain	Type the domain required to access the Microsoft Exchange server. This parameter is optional.
Username	Type the username required to access the Microsoft Exchange server.
Password	Type the password required to access the Microsoft Exchange server.
Confirm Password	Confirm the password required to access the Microsoft Exchange server.
SMTP Log Folder Path	Type the directory path to access the SMTP log files. Clearing the file path information from the SMTP Log Folder Path field disables SMTP monitoring.
OWA Log Folder Path	Type the directory path to access the OWA log files. Clearing the file path information from the OWA Log Folder Path field disables OWA monitoring.
MSGTRK Log Folder Path	Type the directory path to access message tracking log files. Message tracking is only available on Microsoft Exchange 2007 servers assigned the Hub Transport, Mailbox, or Edge Transport server role.
File Pattern	Type the regular expression (regex) required to filter the filenames. All files matching the regex are processed. The default is `.*\.(?:log|LOG)`

Table 138: Microsoft Exchange Parameters (Continued)

Parameter	Description
Force File Read	Select this check box to force the protocol to read the log file. By default, the check box is selected. If the check box is cleared, the log file is read when the log file modified time or file size attributes change.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.
Throttle Events/Sec	Type the maximum number of events the Microsoft Exchange protocol forwards every second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default value is 100 EPS.

9 Click **Save**.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

LOGbinder EX Event Collection from Microsoft Exchange Server

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

Microsoft IAS Server

The Microsoft IAS Server DSM for SIEM accepts RADIUS events using syslog. You can integrate Internet Authentication Service (IAS) or Network Policy Server (NPS) logs with SIEM using WinCollect. For more information, see the *SIEM WinCollect Users Guide*.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Microsoft Windows IAS Server:

u From the **Log Source Type** list, select the **Microsoft IAS Server** option.

For more information on configuring devices, see the *SIEM Log Sources User Guide*. For more information about your server, see your vendor documentation.

Microsoft DHCP Server

The Microsoft DHCP Server DSM for SIEM accepts DHCP events using the Microsoft DHCP Server protocol or WinCollect.

Configure Your Microsoft DHCP Server

Before you can integrate your Microsoft DHCP Server with SIEM, you must enable audit logging.

To configure the Microsoft DHCP Server:

1 Log in to the DHCP Server Administration Tool.

2 From the DHCP Administration Tool, right-click on the DHCP server and select Properties.

The Properties window is displayed.

3 Click the General tab.

The General panel is displayed.

4 Click Enable DHCP Audit Logging.

The audit log file is created at midnight and must contain a three-character day of the week abbreviation.

Table 139: Microsoft DHCP Log File Examples

Log Type	Example
IPv4	`DhcpSrvLog-Mon.log`
IPv6	`DhcpV6SrvLog-Wed.log`

By default Microsoft DHCP is configured to write audit logs to the %WINDIR%\system32\dhcp\ directory.

5 Restart the DHCP service.

You are now ready to configure the log source and protocol in SIEM:

1 To configure SIEM to receive events from a Microsoft DHCP Server, you must select the Microsoft DHCP Server option from the Log Source Type list.

2 To configure the protocol, you must select the Microsoft DHCP option from the Protocol Configuration list. For more information on configuring the Microsoft DHCP protocol, see the *SIEM Log Sources User Guide*.

NOTE

To integrate Microsoft DHCP Server versions 2000/2003 with SIEM using WinCollect, see the *WinCollect Users Guide*.

Microsoft IIS Server

The Microsoft Internet Information Services (IIS) Server DSM for SIEM accepts FTP, HTTP, NNTP, and SMTP events using syslog.

You can integrate a Microsoft IIS Server with SIEM using one of the following methods:

- Configure SIEM to connect to your Microsoft IIS Server using the IIS Protocol. The IIS Protocol collects HTTP events from Microsoft IIS servers. For more information, see Configure Microsoft IIS Using the IIS Protocol on page 391.
- Configure a Snare Agent with your Microsoft IIS Server to forward event information to SIEM. For more information, see Configuring Microsoft IIS Using a Snare Agent on page 393.
- Configure WinCollect to forward IIS events to SIEM. For more information, see Configuring Microsoft IIS using Adaptive Log Exporter on page 396.

  For more information, see the *WinCollect Users Guide*.

Table 140: Microsoft IIS Supported Log Types

Version	Supported Log Type	Method of Import
Microsoft IIS 6.0	SMTP, NNTP, FTP, HTTP	IIS Protocol
Microsoft IIS 6.0	SMTP, NNTP, FTP, HTTP	WinCollect or Snare
Microsoft IIS 7.0	HTTP	IIS Protocol
Microsoft IIS 7.0	SMTP, NNTP, FTP, HTTP	WinCollect or Snare

Configure Microsoft IIS Using the IIS Protocol

Before you configure SIEM with the Microsoft IIS protocol, you must configure your Microsoft IIS Server to generate the proper log format.

The Microsoft IIS Protocol only supports the W3C Extended Log File format. The Microsoft authentication protocol NTLMv2 Session is not supported by the Microsoft IIS protocol.

Configuring Your IIS Server

To configure the W3C event log format in Microsoft IIS:

1. Log in to your Microsoft Information Services (IIS) Manager.
2. In the IIS Manager menu tree, expand Local Computer.
3. Select Web Sites.
4. Right-click on **Default Web Sites** and select Properties.
   The Default Web Site Properties window is displayed.
5. Select the **Web Site** tab.
6. Select the **Enable logging** check box.
7. From the Active Log Format list, select W3C Extended Log File Format.
8. From the Enable Logging pane, click Properties.

The Logging Properties window is displayed.

9 Click the Advanced tab.

10 From the list of properties, select check boxes for the following W3C properties:

Table 141: Required Properties for IIS Event Logs

IIS 6.0 Required Properties	IIS 7.0 Required Properties
Date (date)	Date (date)
Time (time)	Time (time)
Client IP Address (c-ip)	Client IP Address (c-ip)
User Name (cs-username)	User Name (cs-username)
Server IP Address (s-ip)	Server IP Address (s-ip)
Server Port (s-port)	Server Port (s-port)
Method (cs-method)	Method (cs-method)
URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)
URI Query (cs-uri-query)	URI Query (cs-uri-query)
Protocol Status (sc-status)	Protocol Status (sc-status)
Protocol Version (cs-version)	User Agent (cs(User-Agent))
User Agent (cs(User-Agent))	

11 Click OK.

You are now ready to configure the log source in SIEM.

Configuring the Microsoft IIS Protocol in SIEM

To configure the log source

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 From the Log Source Type list, select Microsoft IIS Server.

7 From the **Protocol Configuration** list, select **Microsoft IIS**.

8 Configure the following values:

Table 142: Microsoft IIS Protocol Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source.

Table 142: Microsoft IIS Protocol Parameters (Continued)

Parameter	Description
Server Address	Type the IP address of the Microsoft IIS server.
Username	Type the username required to access the Microsoft IIS server.
Password	Type the password required to access the Microsoft IIS server.
Confirm Password	Confirm the password required to access the Microsoft IIS server.
Domain	Type the domain required to access the Microsoft IIS server.
Folder Path	Type the directory path to access the IIS log files. The default is `/WINDOWS/system32/LogFiles/W3SVC1/` Parameters that support file paths allow you to define a drive letter with the path information. For example, you can use `c$/LogFiles/` for an administrative share or `LogFiles/` for a public share folder path, but not `c:/LogFiles`. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the proper access required to read the log files. Local or domain administrators have sufficient privileges to access log files that reside on administrative shares.
File Pattern	Type the regular expression (regex) required to filter the filenames. All matching files are included in the processing. The default is `(?:u_)?ex.*\.(?:log|LOG)` For example, to list all files starting with the word log, followed by one or more digits and ending with tar.gz, use the following entry: log[0-9]+\.tar\.gz. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.
Polling Interval (s)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.

9 Click **Save**.

10 The Microsoft IIS protocol configuration is complete.

Configuring Microsoft IIS Using a Snare Agent

If you want to use a snare agent to integrate the Microsoft IIS server with SIEM, you must configure a Snare Agent to forward events.

Configuring Microsoft IIS using a Snare Agent with SIEM requires the following:

1 Configure Your Microsoft IIS Server for Snare (page 14)

2 Configure the Snare Agent (page 15)

3 Configure a Microsoft IIS log source (page 15)

Configure Your Microsoft IIS Server for Snare

To configure a Snare Agent to integrate a Microsoft IIS server with SIEM:

1 Log in to your Microsoft Information Services (IIS) Manager.

2 In the IIS Manager menu tree, expand Local Computer.

3 Select Web Sites.

4 Right-click on **Default Web Sites** and select Properties.
The Default Web Site Properties window is displayed.

5 Select the **Web Site** tab.

6 Select the **Enable logging** check box.

7 From the Active Log Format list, select W3C Extended Log File Format.

8 From the Enable Logging panel, click Properties.
The Logging Properties window is displayed.

9 Click the Advanced tab.

10 From the list of properties, select check boxes for the following W3C properties:

Table 143: Required Properties for IIS Event Logs

IIS 6.0 Required Properties	IIS 7.0 Required Properties
Date (date)	Date (date)
Time (time)	Time (time)
Client IP Address (c-ip)	Client IP Address (c-ip)
User Name (cs-username)	User Name (cs-username)
Server IP Address (s-ip)	Server IP Address (s-ip)
Server Port (s-port)	Server Port (s-port)
Method (cs-method)	Method (cs-method)
URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)
URI Query (cs-uri-query)	URI Query (cs-uri-query)
Protocol Status (sc-status)	Protocol Status (sc-status)
Protocol Version (cs-version)	User Agent (cs(User-Agent))
User Agent (cs(User-Agent))	

11 Click OK.

12 You are now ready to configure the Snare Agent.

Configure the Snare Agent

To configure your Snare Agent:

1 Access the InterSect Alliance website:
http://www.intersectalliance.com/projects/SnareIIS/

2 Download open source Snare Agent for IIS, version 1.2:
`SnareIISSetup-1.2.exe`

3 Install the open source Snare Agent for IIS.

4 In the Snare Agent, select Audit Configuration.
The Audit Service Configuration window is displayed.

5 In the **Target Host** field, type the IP address of your SIEM.

6 In the **Log Directory** field type the IIS file location:
`\%SystemRoot%\System32\LogFiles\`
By default Snare for IIS is configured to look for logs in `C:\WINNT\System32\LogFiles\`.

7 For **Destination**, select Syslog.

8 For **Delimiter**, select TAB.

9 Select the Display IIS Header Information check box.

10 Click OK.

Configure a Microsoft IIS Log Source

SIEM automatically discovers and creates a log source for syslog events from Microsoft IIS forwarded from a Snare agent. These configuration steps are optional.

To manually create a Microsoft IIS log source in SIEM:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 From the Log Source Type list, select Microsoft IIS Server.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the following values:

Table 144: Microsoft IIS Syslog Configuration

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source.

9 Click Save.

10 On the Admin tab, click Deploy Changes.
The configuration is complete.

Configuring Microsoft IIS using Adaptive Log Exporter

WinCollect is a stand-alone application that allows you to integrate device logs or application event data with SIEM.

To integrate the Adaptive Log Exporter with Microsoft IIS:

1 Log in to your Microsoft Information Services (IIS) Manager.

2 In the IIS Manager menu tree, expand Local Computer.

3 Select Web Sites.

4 Right-click on **Default Web Site** and select Properties.
The Web Sites Properties window is displayed.

5 From the Active Log Format list, select one of the following:

- Select NCSA. Go to Step 9.
- Select IIS. Go to Step 9.
- Select W3C. Go to Step 6.

6 Click Properties.
The Properties window is displayed.

7 Click the Advanced tab.

8 From the list of properties, select all event properties that you want to apply to the Microsoft IIS event log. The selected properties must include the following:
a Select the Method (cs-method) check box.
b Select the Protocol Version (cs-version) check box.

9 Click OK.

10 You are now ready to configure the Adaptive Log Exporter.
For more information on installing and configuring Microsoft IIS for the Adaptive Log Exporter, see the *Adaptive Log Exporter User Guide*.

Microsoft ISA

The Microsoft Internet and Acceleration (ISA) DSM for SIEM accepts events using syslog. You can integrate Microsoft ISA Server with SIEM using WinCollect. For more information, see the *WinCollect Users Guide*.

NOTE

The Microsoft ISA DSM also supports events from Microsoft Threat Management Gateway using WinCollect.

Microsoft Hyper-V

The IBM Security SIEM DSM for Microsoft Hyper-V can collect event logs from your Microsoft Hyper-V servers.

The following table describes the specifications for the Microsoft Hyper-V Server DSM:

Table 145: Microsoft Hyper-V DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM	Microsoft Hyper-V
RPM file name	DSM-MicrosoftHyperV-*build_number*.rpm
Supported versions	v2008 and v2012
Protocol	WinCollect
SIEM recorded events	All relevant events
Automatically discovered	No
Includes identity	No
More information	http://technet.microsoft.com/en-us/windowsserver/dd448604.aspx

Microsoft Hyper-V DSM Integration Process

To integrate Microsoft Hyper-V DSM with SIEM, use the following procedures:

1 Download and install the most recent WinCollect RPM on your SIEM Console.

2 Install a WinCollect agent on the Hyper-V system or on another system that has a route to the Hyper-V system. You can also use an existing WinCollect agent. For more information, see the *WinCollect User Guide*.

3 If automatic updates are not enabled, download and install the DSM RPM for Microsoft Hyper-V on your SIEM Console. RPMs need to be installed only one time.

4 For each Microsoft Hyper-V server that you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually installing a DSM (page 6)

Configuring a Microsoft Hyper-V log source in SIEM (page 18)

Configuring a Microsoft Hyper-V Log Source in SIEM

To collect Microsoft Hyper-V events, configure a log source in SIEM.

Before You Begin

Ensure that you have the current credentials for the Microsoft Hyper-V server and the WinCollect agent can access it.

Procedure

1. Log in to SIEM.
2. Click the Admin tab.
3. In the navigation menu, click Data Sources.
4. Click the Log Sources icon.
5. Click Add.
6. From the Log Source Type list, select **Microsoft Hyper-V**.
7. From the **Protocol Configuration** list, select **WinCollect**.
8. From the **Application or Service Log Type** list, select **Microsoft Hyper-V**.
9. From the **WinCollect Agent** list, select the WinCollect agent that accesses the Microsoft Hyper-V server.
10. Configure the remaining parameters.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

Microsoft SharePoint

The Microsoft SharePoint DSM for SIEM collects audit events from the SharePoint database using JDBC to poll an SQL database for audit events.

Audit events allow you to track changes made to sites, files, and content managed by Microsoft SharePoint.

Microsoft SharePoint audit events include:

- Site name and the source from which the event originated
- Item ID, item name, and event location
- User ID associated with the event
- Event type, timestamp, and event action

There are two log source configurations that can be used to collect Microsoft SharePoint database events.

1 Create a database view in your SharePoint database to poll for events with the JDBC protocol. See Configuring a Database View to Collect Audit Events on page 399.

2 Create a JDBC log source and use predefined database queries to collect SharePoint events. This option does not require an administrator to create database view. See Configure a SharePoint Log Source for Predefined Database Queries on page 404.

Configuring a Database View to Collect Audit Events

Before you can integrate Microsoft SharePoint events with SIEM, you must complete the following tasks:

1 Configure the audit events you want to collect for Microsoft SharePoint.

2 Create an SQL database view for SIEM in Microsoft SharePoint.

3 Configure a log source to collect audit events from Microsoft SharePoint.

NOTE

Ensure that no firewall rules are blocking the communication between SIEM and the database associated with Microsoft SharePoint.

Configure Microsoft SharePoint Audit Events

The audit settings for Microsoft SharePoint allow you to define what events are tracked for each site managed by Microsoft SharePoint.

Procedure

1 Log in to your Microsoft SharePoint site.

2 From the **Site Actions** list, select **Site Settings**.

3 From the Site Collection Administration list, click **Site collection audit settings**.

4 From the Documents and Items section, select a check box for each document and item audit event you want to audit.

5 From the Lists, Libraries, and Sites section, select a check box for each content audit event you want to enable.

6 Click **OK**.

You are now ready to create a database view for SIEM to poll Microsoft SharePoint events.

Create a Database View for Microsoft SharePoint

Microsoft SharePoint uses SQL Server Management Studio (SSMS) to manage the SharePoint SQL databases. To collect audit event data, you must create a database view on your Microsoft SharePoint server that is accessible to SIEM.

Procedure

1 Log in to the system hosting your Microsoft SharePoint SQL database.

2 On the desktop, select **Start > Run**.

3 Type the following:

```
ssms
```

4 Click OK.

The Microsoft SQL Server 2008 displays the Connect to Server window.

5 Log in to your Microsoft SharePoint database.

6 Click **Connect**.

7 From the Object Explorer for your SharePoint database, select **Databases > WSS_Logging > Views**.

8 From the navigation menu, click **New Query**.

9 In the Query pane, type the following Transact-SQL statement to create the AuditEvent database view:

```
create view dbo.AuditEvent as select a.siteID
,a.ItemId
,a.ItemType
,u.tp_Title as "User"
,a.MachineName
,a.MachineIp
,a.DocLocation
,a.LocationType
,a.Occurred as "EventTime"
,a.Event as "EventID"
,a.EventName
,a.EventSource
,a.SourceName
,a.EventData
from WSS_Content.dbo.AuditData a, WSS_Content.dbo.UserInfo u
where a.UserId = u.tp_ID and a.SiteId = u.tp_SiteID;
```

10 From the Query pane, right-click and select **Execute**.

If the view is created, the following message is displayed in the results pane:

Command(s) completed successfully.

The dbo.AuditEvent view is created. You are now ready to configure the log source in SIEM to poll the view for audit events.

Configure a SharePoint Log Source for a Database View

SIEM requires a user account with the proper credentials to access the view you created in the Microsoft SharePoint database. To successfully poll for audit data from the Microsoft SharePoint database, you must create a new user or provide the log source with existing user credentials to read from the AuditEvent view. For more information on creating a user account, see your vendor documentation.

To configure SIEM to receive SharePoint events:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select Microsoft SharePoint.

7 From the Protocol Configuration list, select JDBC.

8 Configure the following values:

Table 146: Microsoft SharePoint JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<SharePoint Database>@<SharePoint Database Server IP or Host Name>` Where: `<SharePoint Database>` is the database name, as entered in the Database Name parameter. `<SharePoint Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type WSS_Logging as the name of the Microsoft SharePoint database.
IP or Hostname	Type the IP address or host name of the Microsoft SharePoint SQL Server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SharePoint database. The Microsoft SharePoint database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username the log source can use to access the Microsoft SharePoint database.

Table 146: Microsoft SharePoint JDBC Parameters (Continued)

Parameter	Description
Password	Type the password the log source can use to access the Microsoft SharePoint database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the **Password** field.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type AuditEvent as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type EventTime as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the AuditEvent view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.

Table 146: Microsoft SharePoint JDBC Parameters (Continued)

Parameter	Description
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Use NTLMv2	Select the **Use NTLMv2** check box. This option forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Use SSL	Select this check box if your connection supports SSL communication. This option requires additional configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Microsoft SharePoint log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

Configure a SharePoint Log Source for Predefined Database Queries

Administrators who are not permitted to create a database view due to policy restrictions can collect Microsoft SharePoint events with a log source that uses predefined queries. Predefined queries are customized statements that are capable of joining data from seperate tables when the database is polled by the JDBC protocol. To successfully poll for audit data from the Microsoft SharePoint database, you must create a new user or provide the log source with existing user credentials. For more information on creating a user account, see your vendor documentation.

Procedure

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select Microsoft SharePoint.

7 From the Protocol Configuration list, select JDBC.

8 Configure the following values:

Table 147: Microsoft SharePoint JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<SharePoint Database>@<SharePoint Database Server IP or Host Name>` Where: `<SharePoint Database>` is the database name, as entered in the Database Name parameter. `<SharePoint Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type WSS_Logging as the name of the Microsoft SharePoint database.
IP or Hostname	Type the IP address or host name of the Microsoft SharePoint SQL Server.

Table 147: Microsoft SharePoint JDBC Parameters (Continued)

Parameter	Description
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SharePoint database. The Microsoft SharePoint database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username the log source can use to access the Microsoft SharePoint database.
Password	Type the password the log source can use to access the Microsoft SharePoint database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the **Password** field.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Predefined Query	From the list, select **Microsoft SharePoint**.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time	Optional. Type the start date and time for database polling. If a start date or time is not selected, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the AuditEvent view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.

Table 147: Microsoft SharePoint JDBC Parameters (Continued)

Parameter	Description
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Use NTLMv2	Select the **Use NTLMv2** check box. This option forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Use SSL	Select this check box if your connection supports SSL communication. This option requires additional configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Microsoft SharePoint log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

Microsoft SQL Server

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

LOGbinder SP Event Collection from Microsoft SharePoint

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

Microsoft Windows Security Event Log

The Microsoft Windows Security Event Log DSM for SIEM accepts Windows-based events using syslog.

You can integrate Window Microsoft Security Event Log events with SIEM using one of the following methods:

- Use a WinCollect agent to retrieve Windows-based events from multiple Windows systems in your network. For more information on WinCollect, see the *WinCollect User Guide*.
- Use the Microsoft Security Event Log protocol to collect events using WMI. For more information, see Using WMI on page 407
- Set-up the Snare Agent to forward Microsoft Windows Security Event Logs to SIEM. See Using the Snare Agent on page 408

Using WMI

Before you can configure a log source using the Microsoft Windows Security Event Log protocol, you must configure your system DCOM settings for each host you want to monitor. Ensure the following is configured for each host:

- Make sure you have appropriate administrative permissions. For this process, you must be a member of the Administrators group on the remote computer.
- Make sure you have Windows 2000, Windows 2003, Windows 2008, XP, or Vista software, or Windows 7 installed. The Windows Event Log Protocol supports 32 or 64-bit systems.
- Configure DCOM and enable the host.
- Enable Windows Management Instrumentation on the host.
- Activate the remote registry service.
- If a firewall is installed on the host (for example, Windows firewall) or is located between the host and SIEM (such as a hardware or other intermediary firewall), you must configure the firewall to allow DCOM communication. This includes configuring the firewall to permit port 135 to be accessible on the host, as well as permitting DCOM ports (generally random ports above 1024). If necessary, you can also configure specific ports to be accessible to DCOM. This depends on the version of Windows. For more information, see your Windows documentation.
- Configure a system or domain account that includes security configuration permitting access to the Window event log protocol DCOM components, Windows event log protocol name space, and appropriate access to the remote registry keys.

You are now ready to configure the log source in SIEM:

1 To configure SIEM to receive events from Windows security event logs, you must select the Microsoft Windows Security Event Log option from the Log Source Type list.

2 To configure the Windows Event Log protocol, you must select the Microsoft Security Event Log option from the Protocol Configuration list. Your system must be running the latest version of the Windows Event Log protocol to retrieve File Replication and Directory Service events:

Using the Snare Agent

To configure the Snare Agent to forward Windows security event logs to SIEM:

1 Download and install the Snare Agent.

NOTE

To download a Snare Agent, see the following website:
www.intersectalliance.com/projects/SnareWindows/index.html

2 On the navigation menu, select Network Configuration.

3 Type the IP address of the SIEM system in the **Destination Snare Server** address field.

4 Select the Enable SYSLOG Header check box.

5 Click Change Configuration.

6 On the navigation menu, select Objectives Configuration.

7 In the **Identify the event types to be captured** field, select check boxes to define the event types you want snare to forward to SIEM.

The Microsoft Windows Event Log DSM supports Informational, Warning, Error, Success Audit, and Failure Audit event types.

8 In the **Identify the event logs** field, select check boxes to define the event logs you want snare to forward to SIEM.

The Microsoft Windows Event Log DSM supports Security, System, Application, DNS Server, File Replication and Directory Service log types.

9 Click Change Configuration.

10 On the navigation menu, select Apply the Latest Audit Configuration.

The value entered in the override host name detection with field must match the IP address or hostname assigned to the device configured in the SIEM setup.

You are now ready to configure the log source in SIEM:

1 To configure SIEM to receive events from Windows security event logs, you must select the Microsoft Windows Security Event Log option from the Log Source Type list.

2 To configure the Windows Event Log protocol, you must select the Microsoft Security Event Log option from the Protocol Configuration list. Your system must be running the latest version of the Windows Event Log protocol to retrieve File Replication and Directory Service log types:

For more information on configuring devices, see the *SIEM Log Sources User Guide*. For more information about your server, see your vendor documentation.

Microsoft Operations Manager

The Microsoft Operations Manager DSM for SIEM accepts Microsoft Operations Manager (MOM) events by polling the OnePoint database allowing SIEM to record the relevant events.

Before you configure SIEM to integrate with the Microsoft Operations Manager, you must ensure a database user account is configured with appropriate permissions to access the MOM OnePoint SQL Server database. Access to the OnePoint database SDK views is managed through the MOM SDK View User database role. For more information, please see your Microsoft Operations Manager documentation.

NOTE

Make sure that no firewall rules are blocking the communication between SIEM and the SQL Server database associated with MOM. For MOM installations that use a separate, dedicated computer for the SQL Server database, the SDKEventView view is queried on the database system, not the system running MOM.

To configure SIEM to receive MOM events:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

3 Click the Log Sources icon.
The Log Sources window is displayed.

4 From the Log Source Type list, select Microsoft Operations Manager.

5 From the Protocol Configuration list, select JDBC.
The JDBC protocol parameters appear.

6 Configure the following values:

Table 148: Microsoft Operations Manager JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<MOM Database>@<MOM Database Server IP or Host Name>` Where: `<MOM Database>` is the database name, as entered in the Database Name parameter. `<MOM Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type OnePoint as the name of the Microsoft Operations Manager database.
IP or Hostname	Type the IP address or host name of the Microsoft Operations Manager SQL Server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft Operations Manager database. The Microsoft Operations Manager database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type SDKEventView as the name of the table or view that includes the event records.

Table 148: Microsoft Operations Manager JDBC Parameters (Continued)

Parameter	Description
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type TimeStored as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Microsoft Operations Manager log source with a higher importance compared to other log sources in SIEM.

7 Click Save.

8 On the Admin tab, click Deploy Changes.

For more information on configuring log sources, see the *SIEM Log Sources User Guide.*

Microsoft System Center Operations Manager

A SIEM Microsoft System Center Operations Manager (SCOM) DSM accepts SCOM events by polling the OperationsManager database allowing SIEM to record the relevant events.

Before you configure SIEM to integrate with the Microsoft SCOM, you must ensure a database user account is configured with appropriate permissions to access the SCOM OperationsManager SQL Server database. The appropriate authentication mode might need to be enabled in the Security settings of the SQL Server properties. For more information, please see your Microsoft SCOM documentation.

NOTE

Ensure that no firewall rules are blocking the communication between SIEM and the SQL Server database associated with SCOM. For SCOM installations that use a separate, dedicated computer for the SQL Server database, the EventView view is queried on the database system, not the system running SCOM.

To configure SIEM to receive SCOM events:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

3 Click the Log Sources icon.
The Log Sources window is displayed.

4 From the Log Source Type list, select Microsoft SCOM.

5 From the Protocol Configuration list, select JDBC.
The JDBC protocol is displayed.

6 Configure the following values:

Table 149: Microsoft SCOM JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<SCOM Database>@<SCOM Database Server IP or Host Name>` Where: `<SCOM Database>` is the database name, as entered in the Database Name parameter. `<SCOM Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type OperationsManager as the name of the Microsoft SCOM database.
IP or Hostname	Type the IP address or host name of the Microsoft SCOM SQL Server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SCOM database. The Microsoft SCOM database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type EventView as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).

Table 149: Microsoft SCOM JDBC Parameters (Continued)

Parameter	Description
Compare Field	Type TimeAdded as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Microsoft SCOM log source with a higher importance compared to other log sources in SIEM.

7 Click Save.

8 On the Admin tab, click Deploy Changes.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Microsoft Endpoint Protection

The Microsoft Endpoint Protection DSM for SIEM is capable of collecting malware detection events.

Supported Event Types

Malware detection events are retrieved by SIEM by configuring the JDBC protocol. Adding malware detection events to SIEM allows you to monitor and detect malware infected computers in your deployment.

Malware detection events include:

- Site name and the source from which the malware was detected
- Threat name, threat ID, and severity
- User ID associated with the threat
- Event type, timestamp, and the cleaning action taken on the malware.

Configuration Overview

The Microsoft Endpoint Protection DSM uses JDBC to poll an SQL database for malware detection event data. This DSM does not automatically discover. To integrate Microsoft EndPoint Protection with SIEM, you must:

1 Create an SQL database view for SIEM with the malware detection event data.

2 Configure a JDBC log source to poll for events from the Microsoft EndPoint Protection database.

3 Ensure that no firewall rules are blocking communication between SIEM and the database associated with Microsoft EndPoint Protection.

Creating a Database View

Microsoft EndPoint Protection uses SQL Server Management Studio (SSMS) to manage the EndPoint Protection SQL databases.

Procedure

1 Log in to the system hosting your Microsoft EndPoint Protection SQL database.

2 On the desktop, select **Start > Run**.

3 Type the following:
```
ssms
```

4 Click OK.

5 Log in to your Microsoft Endpoint Protection database.

6 From the Object Explorer, select **Databases.**

7 Select your database and click **Views**.

8 From the navigation menu, click **New Query**.

9 In the Query pane, type the following Transact-SQL statement to create the database view:

```
create view dbo.MalwareView as
select n.Type
, n.RowID
, n.Name
, n.Description
, n.Timestamp
, n.SchemaVersion
, n.ObserverHost
, n.ObserverUser
, n.ObserverProductName
, n.ObserverProductversion
, n.ObserverProtectionType
, n.ObserverProtectionVersion
, n.ObserverProtectionSignatureVersion
, n.ObserverDetection
, n.ObserverDetectionTime
, n.ActorHost
, n.ActorUser
, n.ActorProcess
, n.ActorResource
, n.ActionType
, n.TargetHost
, n.TargetUser
, n.TargetProcess
, n.TargetResource
, n.ClassificationID
, n.ClassificationType
, n.ClassificationSeverity
, n.ClassificationCategory
, n.RemediationType
, n.RemediationResult
, n.RemediationErrorCode
, n.RemediationPendingAction
, n.IsActiveMalware
, i.IP_Addresses0 as 'SrcAddress'
from v_AM_NormalizedDetectionHistory n, System_IP_Address_ARR i,
v_RA_System_ResourceNames s, Network_DATA d where n.ObserverHost
= s.Resource_Names0 and s.ResourceID = d.MachineID and
d.IPEnabled00 = 1 and d.MachineID = i.ItemKey and
i.IP_Addresses0 like '%.%.%.%';
```

10 From the Query pane, right-click and select **Execute**.

If the view is created, the following message is displayed in the results pane:

Command(s) completed successfully.

You are now ready to configure a log source in SIEM.

Configuring a Log Source

SIEM requires a user account with the proper credentials to access the view you created in the Microsoft EndPoint Protection database.

To successfully poll for malware detection events from the Microsoft EndPoint Protection database, you must create a new user or provide the log source with existing user credentials to read from the database view you created. For more information on creating a user account, see your vendor documentation.

Procedure

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 In the **Log Source Name** field, type a name for the log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select Microsoft EndPoint Protection.

7 From the Protocol Configuration list, select JDBC.

8 Configure the following values:

Table 150: Microsoft EndPoint Protection JDBC parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Database>@<Database Server IP or Host Name>` Where: `<Database>` is the database name, as entered in the Database Name parameter. `<Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type the name of the Microsoft EndPoint Protection database. This name must match the database name you selected when creating your view in Step 7.
IP or Hostname	Type the IP address or host name of the Microsoft EndPoint Protection SQL Server.

Table 150: Microsoft EndPoint Protection JDBC parameters (Continued)

Parameter	Description
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft EndPoint Protection database. The Microsoft EndPoint Protection database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username the log source can use to access the Microsoft EndPoint Protection database.
Password	Type the password the log source can use to access the Microsoft EndPoint Protection database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the **Password** field.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define the Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type dbo.MalwareView as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type Timestamp as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.

Table 150: Microsoft EndPoint Protection JDBC parameters (Continued)

Parameter	Description
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Creatinatabase Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.
Use NTLMv2	Select the **Use NTLMv2** check box. This option forces MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Microsoft EndPoint Protection log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The Microsoft EndPoint Protection configuration is complete.

66 NetApp Data ONTAP

SIEM accepts syslog events from a Windows agent installed with the Adaptive Log Exporter.

The Adaptive Log Exporter is an external event collection agent. The Adaptive Log Exporter allows you to collect events using a NetApp Data ONTAP plug-in. The Adaptive Log Exporter can read and process event log messages generated from Common Internet File System (CIFS) auditing on the NetApp Data ONTAP device and forward the events.

For more information on using the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

NOTE

The NetApp Data ONTAP plug-in for the Adaptive Log Exporter only supports CIFS. For information on configuring CIFS on your NetApp Data ONTAP device, see your vendor documentation.

SIEM automatically detects the NetApp Data ONTAP events from the Adaptive Log Exporter. To manually configure SIEM to receive events from NetApp Data ONTAP:

From the Log Source Type list, select the NetApp Data ONTAP option.

67 Name Value Pair

The Name Value Pair (NVP) DSM allows you to integrate SIEM with devices that might not natively send logs using syslog.

SIEMThe NVP DSM provides a log format that allows you to send logs to SIEM. For example, for a device that does not export logs natively with syslog, you can create a script to export the logs from a device that SIEM does not support, format the logs in the NVP log format, and send the logs to SIEM using syslog. The NVP DSM log source configured in SIEM then receives the logs and is able to parse the data since the logs are received in the NVP log format.

NOTE

Events for the NVP DSM are not automatically discovered by SIEM.

The NVP DSM accepts events using syslog. SIEM records all relevant events. The log format for the NVP DSM must be a tab-separated single line list of Name=Parameter. The NVP DSM does not require a valid syslog header.

NOTE

The NVP DSM assumes an ability to create custom scripts or thorough knowledge of your device capabilities to send logs to SIEM using syslog in NVP format.

This section provides information on the following:

NVP Log Format

Table 151 includes a list of tags that the NVP DSM is able to parse:

Table 151: NVP Log Format Tags

Tag	Description
DeviceType	Type `NVP` as the DeviceType. This identifies the log formats as a Name Value Pair log message. This is a required parameter and `DeviceType=NVP` must be the first pair in the list.
EventName	Type the event name that you want to use to identity the event in the Events interface when using the Event Mapping functionality. For more information on mapping events, see the *SIEM Users Guide*. This is a required parameter.
EventCategory	Type the event category you want to use to identify the event in the Events interface. If this value is not included in the log message, the value `NameValuePair` value is used.
SourceIp	Type the source IP address for the message.
SourcePort	Type the source port for the message.
SourceIpPreNAT	Type the source IP address for the message before Network Address Translation (NAT) occurred.
SourceIpPostNAT	Type the source IP address for the message after NAT occurs.
SourceMAC	Type the source MAC address for the message.
SourcePortPreNAT	Type the source port for the message before NAT occurs.
SourcePortPostNAT	Type the source port for the message after NAT occurs.
DestinationIp	Type the destination IP address for the message.
DestinationPort	Type the destination port for the message.
DestinationIpPreNAT	Type the destination IP address for the message before NAT occurs.
DestinationIpPostNAT	Type the IP address for the message after NAT occurs.
DestinationPortPreNAT	Type the destination port for the message before NAT occurs.
DestinationPortPostNAT	Type the destination port for the message after NAT occurs.
DestinationMAC	Type the destination MAC address for the message.
DeviceTime	Type the time that the event was sent, according to the device. The format is: YY/MM/DD hh:mm:ss. If no specific time is provided, the syslog header or DeviceType parameter is applied.
UserName	Type the user name associated with the event.
HostName	Type the host name associated with the event. Typically, this parameter is only associated with identity events.
GroupName	Type the group name associated with the event. Typically, this parameter is only associated with identity events.

Table 151: NVP Log Format Tags (Continued)

Tag	Description
NetBIOSName	Type the NetBIOS name associated with the event. Typically, this parameter is only associated with identity events.
Identity	Type TRUE or FALSE to indicate whether you wish this event to generate an identity event. An identity event is generated if the log message contains the SourceIp (if the IdentityUseSrcIp parameter is set to TRUE) or DestinationIp (if the IdentityUseSrcIp parameter is set to FALSE) and one of the following parameters: UserName, SourceMAC, HostName, NetBIOSName, or GroupName.
IdentityUseSrcIp	Type TRUE or FALSE (default). TRUE indicates that you wish to use the source IP address for identity. FALSE indicates that you wish to use the destination IP address for identity. This parameter is used only if the Identity parameter is set to TRUE.

In addition to the parameters listed above, you can add any NVP parameters to your log. The additional parameters are added to the payload, however, these values are not parsed.

11 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from an NVP DSM:

From the Log Source Type list, select the Name Value Pair option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Examples

Example 1

The following example parses all fields:

```
DeviceType=NVP  EventName=Test DestinationIpPostNAT=172.16.45.10
DeviceTime=2007/12/14 09:53:49  SourcePort=1111 Identity=FALSE
SourcePortPostNAT=3333  DestinationPortPostNAT=6666
HostName=testhost        DestinationIpPreNAT=172.16.10.10
SourcePortPreNAT=2222   DestinationPortPreNAT=5555
SourceMAC=AA:15:C5:BF:C4:9D      SourceIp=172.16.200.10
SourceIpPostNAT=172.16.40.50 NetBIOSName=testbois
DestinationMAC=00:41:C5:BF:C4:9D          EventCategory=Accept
DestinationPort=4444     GroupName=testgroup
SourceIpPreNAT=172.16.70.87UserName=root
DestinationIp=172.16.30.30
```

Example 2

The following example provides identity using the destination IP address:

```
<133>Apr 16 12:41:00 172.16.10.10 namevaluepair:
DeviceType=NVP  EventName=Test  EventCategory=Accept
Identity=TRUE SourceMAC=AA:15:C5:BF:C4:9D
SourceIp=172.15.210.113          DestinationIp=172.16.10.10
UserName=root
```

Example 3

The following example provides identity using the source IP address:

```
DeviceType=NVP  EventName=Test  EventCategory=Accept
DeviceTime=2007/12/14 09:53:49  SourcePort=5014 Identity=TRUE
IdentityUseSrcIp=TRUE     SourceMAC=AA:15:C5:BF:C4:9D
SourceIp=172.15.210.113          DestinationIp=172.16.10.10
DestinationMAC=00:41:C5:BF:C4:9D          UserName=root
```

Example 4

The following example provides an entry with no identity:

```
DeviceType=NVP  EventName=Test  EventCategory=Accept
DeviceTime=2007/12/14 09:53:49  SourcePort=5014 Identity=FALSE
SourceMAC=AA:15:C5:BF:C4:9D      SourceIp=172.15.210.113
DestinationIp=172.16.10.10DestinationMAC=00:41:C5:BF:C4:9D
UserName=root
```

68 Niksun

The Niksun DSM for SIEM records all relevant Niksun events using syslog.

You can integrate NetDetector/NetVCR2005, version 3.2.1sp1_2 with SIEM. Before you configure SIEM to integrate with a Niksun device, you must configure a log source, then enable syslog forwarding on your Niksun appliance. For more information on configuring Niksun, see your Niksun appliance documentation.

Configure a Log Source

To integrate Niksun with SIEM, you must manually create a log source to receive events.

SIEM does not automatically discover or create log sources for syslog events from Niksun appliances. In cases where the log source is not automatically discovered, we recommend you create a log source before forwarding events to SIEM.

To configure a log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Niksun 2005 v3.5.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 152: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Niksun appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM.

69 Nokia Firewall

The Check Point Firewall-1 DSM allows SIEM to accept events Check Point-based Firewall events sent from Nokia Firewall appliances.

The syslog and OPSEC protocols allow two methods for SIEM to collect Check Point events from Nokia Firewall appliances.

This section contains the following topics:

Integrating with a Nokia Firewall using syslog

This method allows you to configure your Nokia Firewall to accept Check Point syslog events forwarded from your Nokia Firewall appliance.

To configure SIEM to integrate with a Nokia Firewall device, you must:

1 Configure iptables on your SIEM Console or Event Collector to receive syslog events from Nokia Firewall.

2 Configure your Nokia Firewall to forward syslog event data.

3 Configure the events logged by the Nokia Firewall.

4 Optional. Configure a log source in SIEM.

Configuring IPtables

Nokia Firewalls require a TCP reset (rst) or a TCP acknowledge (ack) from SIEM on port 256 before forwarding syslog events.

The Nokia Firewall TCP request is an online status request designed to ensure that SIEM is online and able to receive syslog events. If a valid reset or acknowledge is received from SIEM, then Nokia Firewall begins forwarding events to SIEM on UDP port 514. By default, SIEM does not respond to any online status requests from TCP port 256. You must configure IPtables on your SIEM Console or any Event Collectors that receive Check Point events from a Nokia Firewall to respond to an online status request.

Procedure

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

Login: `root`

Password: `<password>`

2 Type the following command to edit the IPtables file:

```
vi /opt/qradar/conf/iptables.pre
```

The IPtables configuration file is displayed.

3 Type the following command to instruct SIEM to respond to your Nokia Firewall with a TCP reset on port 256:

```
-A INPUT -s <IP address> -p tcp --dport 256 -j REJECT --reject-
with tcp-reset
```

Where `<IP address>` is the IP address of your Nokia Firewall. You must include a TCP reset for each Nokia Firewall IP address that sends events to your SIEM Console or Event Collector. For example,

-A INPUT -s 10.10.100.10/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset

-A INPUT -s 10.10.110.11/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset

-A INPUT -s 10.10.120.12/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset

4 Save your IPtables configuration.

5 Type the following command to update IPtables in SIEM:
`./opt/qradar/bin/iptables_update.pl`

6 Repeat step 1 to step 5 to configure any additional Event Collectors in your deployment that receive syslog events from a Nokia Firewall.

You are now ready to configure your Nokia Firewall to forward events to SIEM.

Configuring Syslog

To configure your Nokia Firewall to forward syslog events to SIEM:

Procedure

1 Log in to the Nokia Voyager.

2 Click Config.

3 In the System Configuration pane, click System Logging.

4 In the **Add new remote IP address to log to** field, type the IP address of your SIEM Console or Event Collector.

5 Click Apply.

6 Click Save.

You are now ready to configure which events are logged by your Nokia Firewall to the logger.

Configure the Logged Events Custom Script

To configure which events are logged by your Nokia Firewall and forwarded to SIEM, you must configure a custom script for your Nokia Firewall.

Procedure

1 Using SSH, log in to Nokia Firewall as an administrative user.

If you cannot connect to your Nokia Firewall, SSH may be disabled. You must enable the command-line using the Nokia Voyager web interface or connect directly using a serial connection. For more information, see your Nokia Voyager documentation.

2 Type the following command to edit your Nokia Firewall rc.local file:
`vi /var/etc/rc.local`

3 Add the following command to your rc.local file:

```
$FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
```

4 Save the changes to your rc.local file.

The terminal is displayed.

5 To begin logging immediately, type the following command:

```
nohup $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
```

You are now ready to configure the log source in SIEM.

Configure a Log Source

Events forwarded by your Nokia Firewall are automatically discovered by the Check Point Firewall-1 DSM. The automatic discovery process creates a log source for syslog events from Nokia Firewall appliances. The following steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Check Point Firewall-1.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 153: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from your Nokia Firewall appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The syslog configuration for receiving Check Point events from Nokia Firewalls over syslog is complete. Check Point events from your Nokia Firewall are displayed in the **Log Activity** tab in SIEM.

Integrating with a Nokia Firewall using OPSEC

SIEM can accept Check Point FireWall-1 events from Nokia Firewalls using the Check Point FireWall-1 DSM configured using the OPSEC/LEA protocol. Before you configure SIEM to integrate with a Nokia Firewall device, you must:

1 Configure Nokia Firewall using OPSEC, see Configuring a Nokia Firewall for OPSEC on page 430.

2 Configure a log source in SIEM for your Nokia Firewall using the OPSEC LEA protocol, see Configuring an OPSEC Log Source on page 431.

Configuring a Nokia Firewall for OPSEC

To configure Nokia Firewall using OPSEC:

Procedure

1 To create a host object for your SIEM, open up the Check Point SmartDashboard GUI and select **Manage > Network Objects > New > Node > Host**.

2 type the Name, IP Address, and optional Comment for your SIEM.

3 Click OK.

4 Select Close.

5 To create the OPSEC connection, select **Manage > Servers and OPSEC Applications > New > OPSEC Application Properties**.

6 Type the Name and optional Comment.

The name you type must be different than the name in Step 2.

7 From the Host drop-down menu, select the SIEM host object that you created.

8 From Application Properties, select User Defined as the Vendor Type.

9 From Client Entries, select LEA.

10 Select Communication and enter an activation key to configure the Secure Internal Communication (SIC) certificate.

11 Select OK and then select Close.

12 To install the policy on your firewall, select **Policy > Install > OK**.

For more information on policies, see your vendor documentation. You are now ready to configure a log source for your Nokia Firewall in SIEM.

Configuring an OPSEC Log Source

OPSEC/LEA log sources do not automatically discover in SIEM, you must create an OPSEC log source to collect events.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the **Log Sources** icon.

5 Click **Add**.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the **Log Source Type** list, select **Check Point FireWall-1**.

9 Using the Protocol Configuration list, select OPSEC/LEA.

10 Configure the following values:

Table 154: OPSEC/LEA protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the event source. IP addresses or host names are recommended as they allow SIEM to identify a log file to a unique event source.
Server IP	Type the IP address of the server.
Server Port	Type the port used for OPSEC communication. The valid range is 0 to 65,536 and the default is 18184.
Use Server IP for Log Source	Select this check box if you want to use the LEA server's IP address instead of the managed device's IP address for a log source. By default, the check box is selected.
Statistics Report Interval	Type the interval, in seconds, during which the number of syslog events are recorded in the qradar.log file. The valid range is 4 to 2,147,483,648 and the default is 600.

Table 154: OPSEC/LEA protocol parameters (Continued)

Parameter	Description
Authentication Type	From the list, select the authentication type you want to use for this LEA configuration. The options are sslca (default), sslca_clear, or clear. This value must match the authentication method used by the server. The following parameters appear if sslca or sslca_clear is selected as the authentication type. • OPSEC Application Object SIC Attribute (SIC Name) - Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: `CN=LEA, o=fwconsole..7psasx.` The name can be up to 255 characters in length and is case sensitive. • Log Source SIC Attribute (Entity SIC Name) - Type the SIC name of the server, for example: `cn=cp_mgmt,o=fwconsole..7psasx.` The name can be up to 255 characters in length and is case sensitive. • Specify Certificate - Select this check box if you want to define a certificate for this LEA configuration. SIEM attempts to retrieve the certificate using these parameters when the certificate is required. If you select the **Specify Certificate** check box, the Certificate Filename parameter is displayed: • Certificate Filename - This option only appears if Specify Certificate is selected. Type the directory path of the certificate you want to use for this configuration. If you clear the **Specify Certificate** check box, the following parameters appear: • Certificate Authority IP - Type the IP address of the SmartCenter server from which you want to pull your certificate. • Pull Certificate Password - Type the password you want to use when requesting a certificate. The password can be up to 255 characters in length. • OPSEC Application - Type the name of the application you want to use when requesting a certificate. This value can be up to 255 characters in length.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. As events are received, they are displayed in the **Log Activity** tab in SIEM.

70 Nominum Vantio

The Nominum Vantio DSM for SIEM accepts syslog events in Log Extended Event Format (LEEF) forwarded from Nominum Vantio engines installed with the Nominum Vantio LEEF Adapter.

SIEM accepts all relevant events forwarded from Nominum Vantio.

The Vantio LEEF Adapter creates LEEF messages based on Lightweight View Policy (LVP) matches. In order to generate LVP matches for the Vantio LEEF Adapter to process, you most configure Lightweight Views and the lvp-monitor for the Vantio engine. LVP is an optionally licensed component of the Nominum Vantio product. For more information about configuring LVP, please see the *Vantio Administrator's Manual*.

Before you can integrate Nominum Vantio events with SIEM, you must install and configure the Vantio LEEF adapter. To obtain the Vantio LEEF adapter or request additional information, you can email Nominum at the following address: *leefadapter@nominum.com*.

Configure the Vantio LEEF Adapter

To install and configure your Vantio LEEF Adapter:

1 Using SSH, log in to your Vantio engine server.

2 Install the Vantio LEEF Adapter:
`sudo rpm -I VantioLEEFAdapter-0.1-a.x86_64.rpm`

3 Edit the Vantio LEEF Adapter configuration file.
`usr/local/nom/sbin/VantioLEEFAdapter`

4 Configure the Vantio LEEF Adapter configuration to forward LEEF events to SIEM:
`-qradar-dest-addr=<IP Address>`
Where `<IP Address>` is the IP address of your SIEM Console or Event Collector.

5 Save the Vantio LEEF configuration file.

6 Type the following command to start the Vantio Adapter:
`usr/local/nom/sbin/VantioLEEFAdapter &`
The configuration is complete. The log source is added to SIEM as Nominum Vantio events are automatically discovered. Events forwarded to SIEM by the Vantio LEEF Adapter are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from the Vantio LEEF Adapter. The following configuration steps are optional.

To manually configure a log source for Nominum Vantio:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Nominum Vantio.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 155: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from Nominum Vantio.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

71 Nortel Networks

This section provides information on the following DSMs:

Nortel Multiprotocol Router

The Nortel Multiprotocol Router DSM for SIEM records all relevant Nortel Multiprotocol Router events using syslog.

Before you configure SIEM to integrate with a Nortel Multiprotocol Router device, you must:

1 Log in to your Nortel Multiprotocol Router device.

2 At the prompt, type the following command:
`bcc`
The Bay Command Console prompt is displayed.
Welcome to the Bay Command Console!
* To enter configuration mode, type config
* To list all system commands, type ?
* To exit the BCC, type exit
bcc>

3 Type the following command to access configuration mode:
`config`

4 Type the following command to access syslog configuration:
`syslog`

5 Type the following commands:
`log-host address <IP address>`
Where `<IP address>` is the IP address of your SIEM.

6 View current default settings for your SIEM:
`info`
For example:

```
log-host/10.11.12.210# info
   address 10.11.12.210
   log-facility local0
   state enabled
```

7 If the output of the command entered in step 6 indicates that the state is not enabled, type the following command to enable forwarding for the syslog host:

```
state enable
```

8 Configure the log facility parameter:

```
log-facility local0
```

9 Create a filter for the hardware slots to enable them to forward the syslog events. Type the following command to create a filter with the name WILDCARD:

```
filter name WILDCARD entity all
```

10 Configure the slot-upper bound parameter:

```
slot-upper bound <number of slots>
```

Where `<number of slots>` is the number of slots available on your device. This parameter can require different configuration depending on your version of Nortel Multiprotocol Router device, which determines the maximum number of slots available on the device.

11 Configure the level of syslog messages you want to send to your SIEM:

```
severity-mask all
```

12 View the current settings for this filter:

```
info
```

For example:

```
filter/10.11.12.210/WILDCARD# info
   debug-map debug
   entity all
   event-lower-bound 0
   event-upper-bound 255
   fault-map critical
   info-map info
   name WILDCARD
   severity-mask {fault warning info trace debug}
   slot-lower-bound 0
   slot-upper-bound 1
   state enabled
   trace-map debug
   warning-map warning
```

13 View the currently configured settings for the syslog filters:

```
show syslog filters
```

When the syslog and filter parameters are correctly configured, the Operational State indicates `up`.

For example:

```
syslog# show syslog filters
show syslog filters              Sep 15, 2008 18:21:25 [GMT+8]
```

```
Host          Filter     Entit  Entity Configure  Operationa
IP address    Name       y      Code   d State    l State
                         Name
10.11.12.13   WILDCARD   all    255    enabled    up
0
10.11.12.21   WILDCARD   all    255    enabled    up
0
```

14 View the currently configured syslog host information:

```
show syslog log-host
```

The host log is displayed with the number of packets being sent to the various syslog hosts.

For example:

```
syslog# show syslog log-host
show syslog log-host                Sep 15, 2008 18:21:32 [GMT+8]
Host        Configure  Operationa  Time       UDP   Facilit  #Message
IP address  d State    l State     Sequencin  Port  y Code   s Sent
                                   g
10.11.12.1  enabled    up          disabled   514   local0   1402
30
10.11.12.2  enabled    up          disabled   514   local0   131
10
```

15 Exit the command interface:

a Exit the current command-line to return to the bcc command-line:

```
exit
```

b Exit the bbc command-line:

```
exit
```

c Exit the command-line session:

```
logout
```

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Multiprotocol Router device:

From the Log Source Type list, select the Nortel Multiprotocol Router option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your device, see your vendor documentation.

Nortel Application Switch

Nortel Application Switches integrate routing and switching by forwarding traffic at layer 2 speed using layer 4-7 information.

The Nortel Application Switch DSM for SIEM accepts events using syslog. SIEM records all relevant status and network condition events. Before configuring a Nortel Application Switch device in SIEM, you must configure your device to send syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to the Nortel Application Switch command-line interface (CLI).

2 Type the following command:
`/cfg/sys/syslog/host`

3 At the prompt, type the IP address of your SIEM:
`Enter new syslog host: <IP address>`
Where `<IP address>` is the IP address of your SIEM.

4 Apply the configuration:
`apply`

5 After the new configuration is applied, save your configuration:
`save`

6 Type `y` at the prompt to confirm that you wish to save the configuration to flash. For example:
Confirm saving to FLASH [y/n]: `y`
New config successfully saved to FLASH

7 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Application Switch:

From the Log Source Type list, select the Nortel Application Switch option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about the Nortel Application Switch, see *your vendor documentation*.

Nortel Contivity

A SIEM Nortel Contivity DSM records all relevant Nortel Contivity events using syslog.

Before you configure SIEM to integrate with a Nortel Contivity device, you must:

1 Log in to the Nortel Contivity command-line interface (CLI).

2 Type the following command:
`enable <password>`
Where `<password>` is the Nortel Contivity device administrative password.

3 Type the following command:
`config t`

4 Configure the logging information:
`logging <IP address> facility-filter all level all`
Where `<IP address>` is the IP address of the SIEM.

5 Type the following command to exit the command-line:
`exit`

6 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Contivity device:

From the Log Source Type list, select the Nortel Contivity VPN Switch option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Nortel Contivity device, see your vendor documentation.

Nortel Ethernet Routing Switch 2500/4500/5500

A SIEM Nortel Ethernet Routing Switch (ERS) 2500/4500/5500 DSM records all relevant routing switch events using syslog.

Before configuring a Nortel ERS 2500/4500/5500 device in SIEM, you must configure your device to send syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to the Nortel ERS 2500/4500/5500 user interface.

2 Type the following commands to access global configuration mode:
`ena`
`config term`

3 Type `informational` as the severity level for the logs you wish to send to the remote server:
`logging remote level {critical|informational|serious|none}`
Where `informational` sends all logs to the syslog server.

4 Enable the host:

```
host enable
```

5 Type the remote logging address:
```
logging remote address <IP address>
```
Where `<IP address>` is the IP address of the SIEM system.

6 Ensure that remote logging is enabled:
```
logging remote enable
```

7 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel ERS 2500/4500/5500 device:

From the Log Source Type list, select the Nortel Ethernet Routing Switch 2500/4500/5500 option.

For more information on configuring log sources, see the *Log Sources User Guide*.

For more information about the Nortel ERS 2500/4500/5500, see http://www.nortel.com/support.

Nortel Ethernet Routing Switch 8300/8600

A SIEM Nortel Ethernet Routing Switch (ERS) 8300/8600 DSM records all relevant events using syslog.

Before configuring a Nortel ERS 8600 device in SIEM, you must configure your device to send syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to the Nortel ERS 8300/8600 command-line interface (CLI).

2 Type the following command:
```
config sys syslog host <ID>
```
Where `<ID>` is the ID of the host you wish to configure to send syslog events to SIEM.
For the syslog host ID, the valid range is 1 to 10.

3 Type the IP address of your SIEM system:
```
address <IP address>
```
Where `<IP address>` is the IP address of your SIEM system.

4 Type the facility for accessing the syslog host.
```
host <ID> facility local0
```
Where `<ID>` is the ID specified in Step 2.

5 Enable the host:
```
host enable
```

6 Type the severity level for which syslog messages are sent:
```
host <ID> severity info
```
Where `<ID>` is the ID specified in Step 2.

7 Enable the ability to send syslog messages:
```
state enable
```
8 Verify the syslog configuration for the host:
```
sylog host <ID> info
```
For example, the output might resemble the following:
```
ERS-8606:5/config/sys/syslog/host/1# info
Sub-Context:
Current Context:
address : 10.10.10.1
create : 1
delete : N/A
facility : local6
host : enable
mapinfo : info
mapwarning : warning
maperror : error
mapfatal : emergency
severity : info|warning|error|fatal
udp-port : 514
ERS-8606:5/config/sys/syslog/host/1#
```
9 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel ERS 8300/8600 device:

From the Log Source Type list, you must select the Nortel Ethernet Routing Switch 8300/8600 option.

For more information on configuring log sources, see the *Log Sources User Guide*.

For more information about the Nortel ERS 8300/8600, see http://www.nortel.com/support.

Nortel Secure Router

A SIEM Nortel Secure Router DSM records all relevant router events using syslog.

Before configuring a Nortel Secure Router device in SIEM, you must configure your device to send syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to the Nortel Secure Router command-line interface (CLI).

2 Type the following to access global configuration mode:
```
config term
```
3 Type the following command:
```
system logging syslog
```
4 Type the IP address of the syslog server (SIEM system):

```
host_ipaddr <IP address>
```

Where `<IP address>` is the IP address of the SIEM system.

5 Ensure that remote logging is enabled:

```
enable
```

6 Verify that the logging levels are configured, as appropriate:

```
show system logging syslog
```

The following shows an example of the output:

```
-----------------------------------
Syslog Setting
-----------------------------------
Syslog:                              Enabled
Host IP Address:                    10.10.10.1
Host UDP Port:                      514
Facility Priority Setting:
          facility                   priority
          ========                   ========
          auth:                       info
          bootp:                      warning
          daemon:                     warning
          domainname:                warning
          gated:                      warning
          kern:                       info
          mail:                       warning
          ntp:                        warning
          system:                    info
          fr:                         warning
          ppp:                        warning
          ipmux:                     warning
          bundle:                    warning
          qos:                        warning
          hdlc:                       warning
          local7:                    warning
          vpn:                        warning
          firewall:                  warning
```

7 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Secure Router device:

u From the **Log Source Type** list, select the **Nortel Secure Router** option.

For more information on configuring log sources, see the *Log Sources User Guide*.

For more information about the Nortel Secure Router, see http://www.nortel.com/support.

Nortel Secure Network Access Switch

A SIEM Nortel Secure Network Access Switch (SNAS) DSM records all relevant switch events using syslog.

Before configuring a Nortel SNAS device in SIEM, you must:

1 Log in to the Nortel SNAS user interface.

2 Select the Config tab.

3 Select Secure Access Domain and Syslog from the Navigation pane.
The Secure Access Domain window is displayed.

4 From the Secure Access Domain list, select the secure access domain. Click Refresh.

5 Click Add.
The Add New Remote Server window is displayed.

6 Click Update.
The server is displayed in the secure access domain table.

7 Using the toolbar, click Apply to send the current changes to the Nortel SNAS.

8 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel SNAS device:

From the Log Source Type list, select the Nortel Secure Network Access Switch (SNAS) option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

For more information about the Nortel SNA, see www.nortel.com/support.

Nortel Switched Firewall 5100

A SIEM Nortel Switched Firewall 5100 DSM records all relevant firewall events using either syslog or OPSEC.

Before configuring a Nortel Switched Firewall device in SIEM, you must configure your device to send events to SIEM.

This section provides information on configuring a Nortel Switched Firewall using one the following methods:

- Integrate Nortel Switched Firewall using syslog (page 12)
- Integrate Nortel Switched Firewall using OPSEC (page 13)

Integrate Nortel Switched Firewall Using Syslog

This method ensures the SIEM Nortel Switched Firewall 5100 DSM accepts events using syslog.

To configure your Nortel Switched Firewall 5100:

1 Log into your Nortel Switched Firewall device command-line interface (CLI).

2 Type the following command:

```
/cfg/sys/log/syslog/add
```

3 Type the IP address of your SIEM system at the following prompt:

```
Enter IP address of syslog server:
```

A prompt is displayed to configure the severity level.

4 Configure `info` as the desired severity level. For example:

```
Enter minimum logging severity
(emerg | alert | crit | err | warning | notice | info | debug):
info
```

A prompt is displayed to configure the facility.

5 Configure `auto` as the local facility. For example:

```
Enter the local facility (auto | local0-local7): auto
```

6 Apply the configuration:

```
apply
```

7 Repeat for each firewall in your cluster.

8 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Switched Firewall 5100 device using syslog:

From the Log Source Type list, select the Nortel Switched Firewall 5100 option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information, see www.nortel.com/support.

Integrate Nortel Switched Firewall Using OPSEC

This method ensures the SIEM Nortel Switched Firewall 5100 DSM accepts Check Point FireWall-1 events using OPSEC.

NOTE

Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and SIEM integration, you must:

1 Reconfigure Check Point SmartCenter Server.

2 Configure the log source in SIEM.

Reconfigure Check Point SmartCenter Server

This section describes how to reconfigure the Check Point SmartCenter Server. In the Check Point SmartCenter Server, create a host object representing the SIEM system. The leapipe is the connection between the Check Point SmartCenter Server and SIEM.

To reconfigure the Check Point SmartCenter Server:

1 To create a host object, open the Check Point SmartDashboard user interface and select **Manage > Network Objects > New > Node > Host**.

2 Type the Name, IP Address, and optional Comment for your host.

3 Click OK.

4 Select Close.

5 To create the OPSEC connection, select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.

6 Type the Name and optional Comment.
The name you type must be different than the name in Step 2.

7 From the Host drop-down menu, select the host object you have created in Step 1.

8 From Application Properties, select User Defined as the vendor.

9 From Client Entries, select LEA.

10 Click **Communication.**

11 Choose a password in the provide field. This password is necessary when pulling the certificate to the Firewall Director.

12 Click **OK and then click** Close.

13 To install the Security Policy on your firewall, select **Policy > Install > OK**.

Configure a Log Source

You are now ready to configure the log source in SIEM.

1 To configure SIEM to receive events from a Nortel Switched Firewall 5100 device using OPSEC, you must select the Nortel Switched Firewall 5100 option from the Log Source Type list.

2 To configure SIEM to receive events from a Check Point SmartCenter Server using OPSEC LEA, you must select the LEA option from the Protocol Configuration list when configuring your protocol configuration.

For more information, see the *SIEM Log Sources User Guide*.

Nortel Switched Firewall 6000

A SIEM Nortel Switched Firewall 6000 DSM records all relevant firewall events using either syslog or OPSEC.

Before configuring a Nortel Switched Firewall device in SIEM, you must configure your device to send events to SIEM.

This section provides information on configuring a Nortel Switched Firewall 6000 device with SIEM using one of the following methods:

- Configure syslog for Nortel Switched Firewalls (page 14)
- Configure OPSEC for Nortel Switched Firewalls (page 15)

Configure Syslog for Nortel Switched Firewalls

This method ensures the SIEM Nortel Switched Firewall 6000 DSM accepts events using syslog.

To configure your Nortel Switched Firewall 6000:

1 Log into your Nortel Switched Firewall device command-line interface (CLI).

2 Type the following command:
`/cfg/sys/log/syslog/add`

3 Type the IP address of your SIEM system at the following prompt:
`Enter IP address of syslog server:`
A prompt is displayed to configure the severity level.

4 Configure `info` as the desired severity level. For example:
```
Enter minimum logging severity
(emerg | alert | crit | err | warning | notice | info | debug):
info
```
A prompt is displayed to configure the facility.

5 Configure `auto` as the local facility. For example:
`Enter the local facility (auto | local0-local7): auto`

6 Apply the configuration:

```
apply
```

7 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from an Nortel Switched Firewall 6000 using syslog:

From the Log Source Type list, select the Nortel Switched Firewall 6000 option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information, see www.nortel.com/support.

Configure OPSEC for Nortel Switched Firewalls

This method ensures the SIEM Nortel Switched Firewall 6000 DSM accepts Check Point FireWall-1 events using OPSEC.

NOTE

Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and SIEM integration, you must:

1 Reconfigure Check Point SmartCenter Server. See Reconfigure Check Point SmartCenter Server on page 447.

2 Configure the OPSEC LEA protocol in SIEM.

To configure SIEM to receive events from a Check Point SmartCenter Server using OPSEC LEA, you must select the LEA option from the Protocol Configuration list when configuring LEA.

For more information, see the *Log Sources User Guide*.

3 Configure the log source in SIEM.

To configure SIEM to receive events from a Nortel Switched Firewall 6000 device using OPSEC you must select the Nortel Switched Firewall 6000 option from the Log Source Type list. For more information on configuring log sources, see the *Log Sources User Guide*.

For more information, see http://www.nortel.com/support.

Reconfigure Check Point SmartCenter Server

This section describes how to reconfigure the Check Point SmartCenter Server. In the Check Point SmartCenter Server, create a host object representing the SIEM system. The leapipe is the connection between the Check Point SmartCenter Server and SIEM.

To reconfigure the Check Point SmartCenter Server:

1 To create a host object, open the Check Point SmartDashboard user interface and select **Manage > Network Objects > New > Node > Host**.

2 Type the Name, IP Address, and optional Comment for your host.

3 Click OK.

4 Select Close.

5 To create the OPSEC connection, select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.

6 Type the Name and optional Comment.
The name you type must be different than the name in Step 2.

7 From the Host drop-down menu, select the host object you have created in Step 1.

8 From **Application Properties**, select User Defined as the vendor.

9 From **Client Entries**, select LEA.

10 Click **Communication** to generate a Secure Internal Communication (SIC) certificate and enter an activation key.

11 Click **OK and then click** Close.

12 To install the Security Policy on your firewall, select **Policy > Install > OK**.
The configuration is complete.

Nortel Threat Protection System

A SIEM Nortel Threat Protection System (TPS) DSM records all relevant threat and system events using syslog.

Before configuring a Nortel TPS device in SIEM, you must:

1 Log in to the Nortel TPS user interface.

2 Select **Policy & Response > Intrusion Sensor > Detection & Prevention**.
The Detection & Prevention window is displayed.

3 Click Edit next to the intrusion policy you want to configure alerting option.
The Edit Policy window is displayed.

4 Click Alerting.
The Alerting window is displayed.

5 Under Syslog Configuration, select on next to State to enable syslog alerting.

6 From the listes, select the facility and priority levels.

7 Optional. In the **Logging Host** field, type the IP address of your SIEM system. This configures your SIEM system to be your logging host. Separate multiple hosts with commas.

8 Click Save.
The syslog alerting configuration is saved.

9 Apply the policy to your appropriate detection engines.

10 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel TPS device:

From the Log Source Type list, select the Nortel Threat Protection System (TPS) Intrusion Sensor option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about Nortel TPS, see www.nortel.com/support.

Nortel VPN Gateway

The SIEM Nortel VPN Gateway DSM accetps events using syslog.

SIEM records all relevant operating system (OS), system control, traffic processing, startup, configuration reload, AAA, and IPsec events. Before configuring a Nortel VPN Gateway device in SIEM, you must configure your device to send syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to the Nortel VPN Gateway command-line interface (CLI).

2 Type the following command:
`/cfg/sys/syslog/add`

3 At the prompt, type the IP address of your SIEM system:
Enter new syslog host: `<IP address>`
Where `<IP address>` is the IP address of your SIEM system.

4 Apply the configuration:
`apply`

5 View all syslog servers currently added to your system configuration:
`/cfg/sys/syslog/list`

6 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Nortel VPN Gateway device:

From the Log Source Type list, select the Nortel VPN Gateway option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about the Nortel VPN Gateway, see www.nortel.com/support.

72 Novell eDirectory

The Novell eDirectory DSM for SIEM accepts audit events from Novell eDirectory using syslog.

Before You Begin

To use the Novell eDirectory DSM, you must have the following components installed:

- Novell eDirectory v8.8 with service pack 6 (sp6)
- Novell iManager v2.7
- XDASv2

To configure Novell eDirectory with SIEM, you must:

1 Configure the XDASv2 property file to forward events to SIEM.

2 Load the XDASv2 module on your Linux or Windows Operating System.

3 Configure auditing using Novell iManager.

4 Configure SIEM.

Configure XDASv2 to Forward Events

By default, XDASv2 is configured to log events to a file. To forward events from XDASv2 to SIEM, you must edit the xdasconfig.properties and configure the file for syslog forwarding.

Audit events must be forwarded by syslog to SIEM, instead of being logged to a file.

To configure XDASv2 to forward syslog events:

1 Log in to the server hosting Novell eDirectory.

2 Open the following file for editing:

- **Windows** - `C:\Novell\NDS\xdasconfig.properties`
- **Linux or Solaris** - `etc/opt/novell/configuration/xdasconfig.properties`

3 To set the root logger, remove the comment marker (#) from the following line:

```
log4j.rootLogger=debug, S, R
```

4 To set the appender, remove the comment marker (#) from the following line:
`log4j.appender.S=org.apache.log4j.net.SyslogAppender`

5 To configure the IP address for the syslog destination, remove the comment marker (#) and edit the following lines:

```
log4j.appender.S.Host=<IP address>
log4j.appender.S.Port=<Port>
```

Where,

`<IP address>` is the IP address or hostname of SIEM.

`<Port>` is the port number for the UDP or TCP protocol. The default port for syslog communication is port **514** for SIEM or Event Collectors.

6 To configure the syslog protocol, remove the comment marker (#) and type the protocol (UDP, TCP, or SSL) use in the following line:

`log4j.appender.S.Protocol=TCP`

The encrypted protocol SSL is not supported by SIEM.

7 To set the severity level for logging events, remove the comment marker (#) from the following line:

`log4j.appender.S.Threshold=INFO`

The default value of INFO is the correct severity level for events.

8 To set the facility for logging events, remove the comment marker (#) from the following line:

`log4j.appender.S.Facility=USER`

The default value of USER is the correct facility value for events.

9 To set the facility for logging events, remove the comment marker (#) from the following line:

`log4j.appender.R.MaxBackupIndex=10`

10 Save the xdas.properties file.

After you configure the syslog properties for XDASv2 events, you are ready to load the XDASv2 module.

Load the XDASv2 Module

Before you can configure events in Novell iManager, you must load the changes you made to the XDASv2 module.

To load the XDASv2 module, select your operating system.

- To load the XDASv2 in Linux, see Load the XDASv2 on a Linux Operating System on page 452.
- To load the XDASv2 in Windows, see Load the XDASv2 on a Windows Operating System on page 452.

NOTE

If your Novell eDirectory has Novell Module Authentication Service (NMAS) installed with NMAS auditing enabled, the changes made to XDASv2 modules are loaded automatically. If you have NMAS installed, you should configure event auditing. For information on configuring event auditing, see Configure Event Auditing Using Novell iManager on page 452.

Load the XDASv2 on a Linux Operating System

1 Log in to your Linux server hosting Novell eDirectory, as a root user.

2 Type the following command:

```
ndstrace -c "load xdasauditds"
```

You are now ready to configure event auditing in Novell eDirectory. For more information, see Configure Event Auditing Using Novell iManager on page 452.

Load the XDASv2 on a Windows Operating System

1 Log in to your Windows server hosting Novell eDirectory.

2 On your desktop, click **Start > Run**.

The Run window is displayed.

3 Type the following:

```
C:\Novell\NDS\ndscons.exe
```

This is the default installation path for the Windows Operating System. If you installed Novell eDirectory to a different directory, then the correct path is required.

4 Click **OK**.

The Novell Directory Service console displays a list of available modules.

5 From the **Services** tab, select **xdasauditds**.

6 Click **Start**.

The xdasauditds service is started for Novell eDirectory.

7 Click **Startup**.

The Service window is displayed.

8 In the **Startup Type** panel, select the **Automatic** check box.

9 Click **OK**.

10 Close the Novell eDirectory Services window.

You are now ready to configure event auditing in Novell eDirectory. For more information, see Configure Event Auditing Using Novell iManager on page 452.

Configure Event Auditing Using Novell iManager

To configure event auditing for XDASv2 in Novell iManager:

1 Log in to your Novell iManager console user interface.

2 From the navigation bar, click **Roles and Tasks**.

3 In the left-hand navigation, click **eDirectory Auditing > Audit Configuration**.

The Audit Configuration panel is displayed.

4 In the **NPC Server name** field, type the name of your NPC Server.

5 Click **OK**.

The Audit Configuration for the NPC Server is displayed.

6 Configure the following parameters:
   a On the **Components** panel, select one or both of the following:
      - **DS** - Select this check box to audit XDASv2 events for an eDirectory object.
      - **LDAP** - Select this check box to audit XDASv2 events for a Lightweight Directory Access Protocol (LDAP) object.
   b On the **Log Event's Large Values** panel, select one of the following:
      - **Log Large Values** - Select this option to log events that are larger than 768 bytes.
      - **Don't Log Large Values** - Select this option to log events less than 768 bytes. If a value exceeds 768 bytes, then the event is truncated.
   c On the **XDAS Events Configuration**, select the check boxes of the events you want XDAS to capture and forward to SIEM.
   d Click **Apply**.
7 On the **XDAS** tab, click **XDASRoles**.
   The XDAS Roles Configuration panel is displayed.
8 Configure the following role parameters:
   a Select a check box for each object class to support event collection.
   b From the **Available Attribute(s)** list, select any attributes and click the **arrow** to add these to the **Selected Attribute(s)** list.
   c Click **OK** after you have added the object attributes.
   d Click **Apply**.
9 On the **XDAS** tab, click **XDASAccounts**.
   The XDAS Accounts Configuration panel is displayed.
10 Configure the following account parameters:
   a From the **Available Classes** list, select any classes and click the **arrow** to add these to the **Selected Attribute(s)** list.
   b Click **OK** after you have added the object attributes.
   c Click **Apply**.
   You are now ready to configure SIEM.

Configure a Log Source

SIEM automatically detects syslog events from Novell eDirectory. This configuration step is optional.

- From the Log Source Type list, select Novell eDirectory.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about Novell eDirectory, Novell iManager, or XDASv2, see your vendor documentation.

73 ObserveIT

The ObserveIT DSM for SIEM can collect Log Enhanced Event Format (LEEF) events from ObserveIT using the log file protocol.

About ObserveIT

ObserveIT provides administrators and security professionals the ability to capture and replay video recordings of user interactions with network systems, software, or operating systems.

To integrate ObserveIT with SIEM, you must download and install an interface package from the ObserveIT website. The interface package contains the tools required to monitor the ObserveIT database and write the events to a file in LEEF format. As ObserveIT generates and writes events to a log file, SIEM can poll for the event file and retrieve your ObserveIT event data. SIEM remembers the state of the event file to ensure that duplicate events are not imported the next time SIEM read your event file.

The ObserveIT interface package for SIEM requires the following:

- Active Perl installed on the ObserveIT web server.
- An osql client and access to the ObserveIT database

You can download the ObserveIT interface package (Monitor_Log_SIEM.zip) from the ObserveIT customer support: *support@observeIT.com.*

Supported Versions

SIEM supports ObserveIT v5.6.x and later.

Configuring ObserveIT

The following process outlines the steps required to integrate ObserveIT events with SIEM.

1 Configure the ObserveIT interface package for SIEM on your ObserveIT appliance.

2 Configure a log source to use the log file protocol and download the ObserveIT event log to SIEM.

Configuring the ObserveIT Interface Package

To collect ObserveIT events in SIEM, you must download and configure the ObserveIT interface package.

Procedure

1 Email ObserveIT customer support at *support@observeIT.com* to receive the ObserveIT interface package for SIEM.
`Monitor_Log_SIEM.zip`

2 Copy the ObserveIT interface package to the web server hosting ObserveIT.

3 Extract the interface package to a directory.

4 From the interface package directory, edit the following file:
`Data_Query_v5.bat`

5 In the Data_Query_v5.bat file, edit the osql connection information with the location of the ObserveIT database.

6 From the interface package directory, run the Monitor_Log.pl file.
You must be an administrator or have access to write permissions to the following folder: C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles\qradar\.

7 Verify that ObserveIT events are written to the following folder:
C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles\qradar\

8 Optional. Add Monitor_Log.pl to the Windows Job Scheduler to ensure the script starts automatically when the host is powered on.

Next Steps

You are now ready to configure a log source for ObserveIT in SIEM.

Configuring a Venusense Log Source

To integrate ObserveIT events, you must manually create a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select **ObserveIT**.

9 From the **Protocol Configuration** list, select **Log File**.

10 Configure the following values:

Table 156: Log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names allow SIEM to identify a log file to a unique event source.
Service Type	From the list, select the protocol you want to use to retrieve log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the ObserveIT web server that contains your event log files.
Remote Port	Type the port number for the protocol selected to retrieve the event logs from your ObserveIT web server. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 **NOTE:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, adjust the port value accordingly.
Remote User	Type the user name required to log in to the ObserveIT web server that contains your audit event logs. The username can be up to 255 characters in length.
Remote Password	Type the password to log in to your ObserveIT web server.
Confirm Password	Confirm the password to log in to your ObserveIT web server
SSH Key File	If you select SCP or SFTP as the **Service Type**, use this parameter to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The **Recursive** parameter is ignored if you configure SCP as the **Service Type**.

Table 156: Log file protocol parameters (Continued)

Parameter	Description
FTP File Pattern	If you select SFTP or FTP as the **Service Type**, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All files that match the regular expression are retrieved and processed. The FTP file pattern must match the name you assigned to your ObserveIT event log. For example, to collect files that start with ObserveIT_ and end with a timestamp, type the following value: `ObserveIT_*` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only displays if you select **FTP** as the **Service Type**. From the list, select ASCII. ASCII is required for text event logs retrieved by the log file protocol using FTP.
SCP Remote File	If you select **SCP** as the **Service Type**, type the file name of the remote file.
Start Time	Type a time value to represent the time of day you want the log file protocol to start. Type the start time, based on a 24 hour clock, in the following format: HH:MM. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the **Recurrence** parameter value to establish when and how often the Remote Directory on your ObserveIT web server is scanned for new event log files.
Recurrence	Type the frequency that you want to scan the remote directory on your ObserveIT web server for new event log files. Type this value in hours (H), minutes (M), or days (D). For example, type 2H to scan the remote directory every 2 hours from the start time. The default is 1H and the minimum value is 15M.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the save action completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the **Ignore Previously Processed File** parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	From the list, select **NONE**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded. SIEM can process files in zip, gzip, tar, or tar+gzip archive format.

Table 156: Log file protocol parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed. SIEM examines the log files in the remote directory to determine if a file is already processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file. Only new or unprocessed event log files are downloaded by SIEM. This option only applies to **FTP** and **SFTP** service types.
Change Local Directory?	Select this check box to define a local directory on SIEM to store event log files during processing. We recommend that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which allows you to configure the local directory on SIEM to store event log files. After the event log is processed and the events added to SIEM, the local directory deletes the event log files to retain disk space.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The configuration for ObserveIT is complete. As the log file protocol retrieves events, they are displayed on the **Log Activity** tab of SIEM.

74 OpenBSD

The OpenBSD DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant informational, authentication, and system level events forwarded from OpenBSD operating systems.

Configure a Log Source

To integrate OpenBSD events with SIEM, you must manually create a log source. SIEM does not automatically discover or create log sources for syslog events from OpenBSD operating systems.

To create a log source for OpenBSD:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select OpenBSD OS.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 157: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your OpenBSD appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The log source is added to SIEM. You are now ready to configure your OpenBSD appliance to forward syslog events.

Configure Syslog for OpenBSD

To configure OpenBSD to forward syslog events:

1 Using SHH, log in to your OpenBSD device, as a root user.

2 Open the `/etc/syslog.conf` file.

3 Add the following line to the top of the file. Make sure all other lines remain intact:

```
*.* @<IP address>
```

Where `<IP address>` is the IP address of your SIEM.

4 Save and exit the file.

5 Send a hang-up signal to the syslog daemon to ensure all changes are applied:

```
kill -HUP `cat /var/run/syslog.pid`
```

NOTE

The command later uses the backquote character (‘), which is located to the left of the number one on most keyboard layouts.

The configuration is complete. Events forwarded to SIEM by OpenBSD are displayed on the **Log Activity** tab.

75 Open LDAP

The Open LDAP DSM for SIEM accepts multiline UDP syslog events from Open LDAP installations configured to log stats events using logging level 256.

Before You Begin

Open LDAP events are forwarded to SIEM using port 514, but must be redirected to the port configured in the UDP Multiline protocol. This redirect using iptables is required because SIEM does not support multiline UDP syslog on the standard listen port.

NOTE

UDP multiline syslog events can be assigned to any port other than port 514. The default port assigned to the UDP Multiline protocol is UDP port 517. If port 517 is used in your network, see the *SIEM Common Ports Technical Note* for a list of ports used by SIEM.

Configure a Log Source

SIEM does not automatically discover Open LDAP events forwarded in UDP multiline format. To complete the integration, you must manually create a log source for the UDP Multiline Syslog protocol using the **Admin** tab in SIEM. Creating the log source allows SIEM to establish a listen port for incoming Open LDAP multiline events.

To configure an Open LDAP log source in SIEM:

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.
The Data Sources pane is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Open LDAP Software**.

9 From the **Protocol Configuration** list, select **UDP Multiline Syslog**.

10 Configure the following values:

Table 158: UDP Multiline Protocol Configuration

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Open LDAP server.
Listen Port	Type the port number used by SIEM to accept incoming UDP Multiline Syslog events. The valid port range is 1 to 65536. The default UDP Multiline Syslog listen port is 517. **NOTE:** If you do not see the Listen Port field, you must restart Tomcat on SIEM. For more information on installing a protocol manually, see the SIEM Log Sources User Guide. To edit the Listen Port number: 1 Update IPtables on your SIEM Console or Event Collector with the new UDP Multiline Syslog port number. For more information, see Configure IPtables for Multiline UDP Syslog Events on page 464. 2 In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. 3 Click **Save**. 4 On the **Admin** tab, select **Advanced > Deploy Full Configuration**. **NOTE:** When you click **Deploy Full Configuration**, SIEM restarts all services, resulting in a gap in data collection for events and flows until the deployment completes.
Message ID Pattern	Type the regular expression (regex) required to filter the event payload messages. All matching events are included when processing Open LDAP events. The following regular expression is recommended for Open LDAP events: `conn=(\d+)` For example, Open LDAP starts connection messages with the word conn, followed by the rest of the event payload. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

The log source is created for Open LDAP events. You are now ready to configure IPtables for SIEM to redirect Open LDAP events to the proper UDP multiline syslog port on your SIEM Console or Event Collector.

Configure IPtables for Multiline UDP Syslog Events

Open LDAP requires that you redirect events from your Open LDAP servers from port 514 to another SIEM port for the UDP multiline protocol. You must configure IPtables on your SIEM Console or for each Event Collectors that receives multiline UDP syslog events from an Open LDAP server.

To configure SIEM to redirect multiline UDP syslog events:

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

Login: `root`

Password: `<password>`

2 Type the following command to edit the IPtables file:

```
vi /opt/qradar/conf/iptables-nat.post
```

The IPtables NAT configuration file is displayed.

3 Type the following command to instruct SIEM to redirect syslog events from UDP port 514 to UDP port 517:

```
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-
port> -s <IP address>
```

Where:

`<IP address>` is the IP address of your Open LDAP server.

`<New port>` is the port number configured in the UDP Multiline protocol for Open LDAP.

You must include a redirect for each Open LDAP IP address that sends events to your SIEM Console or Event Collector. For example, if you had three Open LDAP servers communicating to an Event Collect, you would type the following:

```
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s
10.10.10.10
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s
10.10.10.11
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s
10.10.10.12
```

4 Save your IPtables NAT configuration.

You are now ready to configure IPtables on your SIEM Console or Event Collector to accept events from your Open LDAP servers.

5 Type the following command to edit the IPtables file:

```
vi /opt/qradar/conf/iptables.post
```

The IPtables configuration file is displayed.

6 Type the following command to instruct SIEM to allow communication from your Open LDAP servers:

```
-I QChain 1 -m udp -p udp --src <IP address> --dport <New port>
-j ACCEPT
```

Where:

`<IP address>` is the IP address of your Open LDAP server.

<New port> is the port number configured in the UDP Multiline protocol for Open LDAP.

You must include a redirect for each Open LDAP IP address that sends events to your SIEM Console or Event Collector. For example, if you had three Open LDAP servers communicating to an Event Collect, you would type the following:

```
-I QChain 1 -m udp -p udp --src 10.10.10.10 --dport 517 -j
ACCEPT
-I QChain 1 -m udp -p udp --src 10.10.10.11 --dport 517 -j
ACCEPT
-I QChain 1 -m udp -p udp --src 10.10.10.12 --dport 517 -j
ACCEPT
```

7 Type the following command to update IPtables in SIEM:

```
./opt/qradar/bin/iptables_update.pl
```

8 Repeat Step 1 to Step 7 to configure any additional SIEM Consoles or Event Collectors in your deployment that receive syslog events from an Open LDAP server.

You are now ready to configure your Open LDAP server to forward events to SIEM.

Configure Event Forwarding for Open LDAP

To configure syslog forwarding for Open LDAP:

1 Log in to the command-line interface for your Open LDAP server.

2 Edit the following file:

```
/etc/syslog.conf
```

3 Add the following information to the syslog configuration file:

```
<facility>        @<IP address>
```

Where:

<facility> is the syslog facility, for example local4.

<IP address> is the IP address of your SIEM Console or Event Collector.

For example,

```
#Logging for SLAPD
local4.debug          /var/log/messages
local4.debug          @10.10.10.1
```

NOTE

If your Open LDAP server stores event messages in a directory other than /var/log/messages, you must edit the directory path accordingly.

4 Save the syslog configuration file.

5 Type the following command to restart the syslog service:

```
/etc/init.d/syslog restart
```

The configuration for Open LDAP is complete. UDP multiline events forwarded to SIEM are displayed on the **Log Activity** tab.

76 Open Source SNORT

The Open Source SNORT DSM for SIEM records all relevant SNORT events using syslog.

Supported Event Types

The SourceFire VRT certified rules for registered SNORT users are supported. Rule sets for Bleeding Edge, Emerging Threat, and other vendor rule sets might not be fully supported by the Open Source SNORT DSM.

Before You Begin

The below procedure applies to a system operating Red Hat Enterprise. The procedures below can vary for other operating systems.

Configure Open Source SNORT

To configure syslog on an Open Source SNORT device:

1 Configure SNORT on a remote system.

2 Open the `snort.conf` file.

3 Uncomment the following line:

```
output alert_syslog:LOG_AUTH LOG_INFO
```

4 Save and exit the file.

5 Open the following file:

```
/etc/init.d/snortd
```

6 Add an `-s` to the following lines, as shown in the example below:

```
daemon /usr/sbin/snort $ALERTMODE $BINARY_LOG $NO PACKET_LOG
$DUMP_APP -D $PRINT_INTERFACE -i $i -s -u $USER -g $GROUP
$CONF -i $LOGIR/$i $PASS_FIRST
```

```
daemon /usr/sbin/snort $ALERTMODE $BINARY_LOG $NO_PACKET_LOG
$DUMP_APP -D $PRINT_INTERFACE $INTERFACE -s -u $USER -g
$GROUP $CONF -i $LOGDIR
```

7 Save and exit the file.

8 Restart SNORT:

```
/etc/init.d/snortd restart
```

9 Open the `syslog.conf` file.

10 Update the file to reflect the following:

```
auth.info                                   @<IP Address>
```

Where `<IP Address>` is the system to which you want logs sent.

11 Save and exit the file.

12 Restart syslog:

```
/etc/init.d/syslog restart
```

You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates log sources for Open Source SNORT syslog events. The following configuration steps are optional.

To create a log source in SIEM:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Open Source IDS.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 159: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for your Open Source SNORT events.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

For more information about SNORT, see the SNORT documentation at www.snort.org/docs/

77 Oracle

This section provides information on configuring the following DSMs:

Oracle Audit Records

Oracle databases track auditing events, such as, user login and logouts, permission changes, table creation, and deletion and database inserts.

SIEM can collect these events for correlation and reporting purposes through the use of the Oracle Audit DSM. For more information, see your Oracle documentation.

NOTE

Oracle provides two modes of audit logs. SIEM does not support fine grained auditing.

Before You Begin

Oracle RDBMS is supported on Linux only when using syslog. Microsoft Windows hosts and Linux are supported when using JDBC to view database audit tables. When using a Microsoft Windows host, verify database audit tables are enabled. These procedures should be considered guidelines only. We recommend that you have experience with Oracle DBA before performing the procedures in this document. For more information, see your vendor documentation.

Before SIEM can collect Oracle Audit events from an Oracle RDBMS instance, that instance must be configured to write audit records to either syslog or the database audit tables. For complete details and instructions for configuring auditing, see your vendor documentation.

NOTE

Not all versions of Oracle can send audit events using syslog. Oracle v9i and 10g Release 1 can only send audit events to the database. Oracle v10g Release 2 and Oracle v11g can write audit events to the database or to syslog. If you are using v10g Release 1 or v9i, you must use JDBC-based events. If you are using Oracle v10g Release 2, you can use syslog or JDBC-based events.

To configure an Oracle Audit device to write audit logs to SIEM, see Configure Oracle Audit Logs on page 470. If your system includes a large Oracle audit table (greater than 1 GB), see Improve Performance with Large Audit Tables on page 471.

Configure Oracle Audit Logs

To configure the device to write audit logs:

1 Log in to the Oracle host as an Oracle user (This user was used to install Oracle, for example oracle).

2 Make sure the ORACLE_HOME and ORACLE_SID environment variables are configured properly for your deployment.

3 Open the following file:
`${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`

4 Choose one of the following options:
a For database audit trails, type the following command:
`*.audit_trail='DB'`
b For syslog, type the following command:
```
*.audit_trail='os'
*.audit_syslog_level='local0.info'
```
You must make sure the syslog daemon on the Oracle host is configured to forward the audit log to SIEM. For systems running Red Hat Enterprise, the following line in the `/etc/syslog.conf` file effects the forwarding:
`local0.info @SIEM.domain.tld`
Where `SIEM.domain.tld` is the hostname of the SIEM that receives the events. The syslog configuration must be re-loaded for the above command to be recognized. On a system running Red Hat Enterprise, type the following line to reload the syslog configuration:
`kill -HUP /var/run/syslogd.pid`

5 Save and exit the file.

6 To restart the database:
a Connect to SQLplus and log in as sysdba:
For example,
`Enter user-name: sys as sysdba`
b Shut down the database:
`shutdown immediate`
c Restart the database:
`startup`

7 If you are using Oracle v9i or Oracle v10g Release 1, you must create a view, using SQLplus to enable the SIEM integration. If you are using Oracle 10g Release 2 or later, you can skip this step:
```
CREATE VIEW SIEM_audit_view AS SELECT
CAST(dba_audit_trail.timestamp AS TIMESTAMP) AS SIEM_time,
dba_audit_trail.* FROM dba_audit_trail;
```

If you are using the JDBC protocol, see the *SIEM Log Sources User Guide* for more information on configuring the JDBC protocol. When configuring the JDBC protocol within SIEM, use the following specific parameters:

Table 160: Configuring Log Source Parameters

Parameter Name	Oracle v9i or 10g Release 1 Values	Oracle v10g Release 2 and v11g Values
Table Name	SIEM_audit_view	dba_audit_trail
Select List	*	*
Compare Field	SIEM_time	extended_timestamp
Database Name	For all supported versions of Oracle, the Database Name must be the exact service name used by the Oracle listener. You can view the available service names by running the following command on the Oracle host: `lsnrctl status`	

NOTE

Make sure that database user that SIEM uses to query events from the audit log table has the appropriate permissions for the Table Name object.

8 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from an Oracle Database:

u From the **Log Source Type** list, select the **Oracle RDBMS Audit Record** option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Improve Performance with Large Audit Tables

The size of the Oracle audit table affects the amount of time that SIEM requires to process the DBA_AUDIT_TRAIL view. If your sys.sud$ table is large (close or exceeding 1 GB), extended processing time is required. To ensure SIEM processes the large sys.sud$ table quickly, you must create an index and a new view.

NOTE

If auditing is extensive or the database server is very active, you might need to shut down the database to perform the below procedure.

To create an index and a new view:

1 Access the following website to download the required files:
http://support.extremenetworks.com

2 From the **Software** tab, select **Scripts**.

3 Download the appropriate file for your version of Oracle:
a If you are using Oracle 9i or 10g Release 1, download the following file:

`oracle_9i_dba_audit_view.sql`

b If you are using Oracle v10g Release 2 and v11g, download the following file:

`oracle_alt_dba_audit_view.sql`

4 Copy the downloaded file to a local directory.

5 Change the directory to the location where you copied the file in Step 4.

6 Log in to SQLplus and log in as sysdba:

```
sqlplus / as sysdba
```

7 At the SQL prompt, type one of the following commands, depending on your version of Oracle Audit:

To create an index, the file might already be in use and must have exclusive access.

a If you are using Oracle 9i or 10g Release 1, type the following command:

```
@oracle_9i_dba_audit_view.sql
```

b If you are using Oracle v10g Release 2 and v11g, type the following command:

```
@oracle_alt_dba_audit_view.sql
```

8 Make sure the database user configured in SIEM has SELECT permissions on the view.

For example if the user is USER1:

```
grant select on sys.alt_dba_audit_view to USER1;
```

9 Log out of SQLplus.

10 Log in to SIEM.

11 Update the JDBC protocol configuration for this entry to include the following:

- Table Name - Update the table name from DBA_AUDIT_TRAIL to sys.alt_dba_audit_view.
- Compare Field - Update the field from entended_timestamp to ntimestamp.

For more information, see the *Log Sources User Guide*.

12 Click Save.

The configuration is complete.

Oracle DB Listener

The Oracle Database Listener application stores logs on the database server.

To integrate SIEM with Oracle DB Listener, select one of the following methods for event collection:

- Collect Events Using the Oracle Database Listener Protocol on page 473
- Collect Oracle Database Events Using Perl on page 474

Collect Events Using the Oracle Database Listener Protocol

The Oracle Database Listener protocol source allows SIEM to monitor log files generated from an Oracle Listener database. Before you configure the Oracle Database Listener protocol to monitor log files for processing, you must obtain the directory path to the Oracle Listener database log files.

To configure SIEM to monitor log files from Oracle Database Listener:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 From the Log Source Type list, select Oracle Database Listener.

6 Using the Protocol Configuration list, select Oracle Database Listener.

7 Configure the following parameters:

Table 161: Oracle Database Listener Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source.
Server Address	Type the IP address of the Oracle Database Listener.
Domain	Type the domain required to access the Oracle Database Listener. This parameter is optional.
Username	Type the username required to access the host running the Oracle Database Listener.
Password	Type the password required to access the host running the Oracle Database Listener.
Confirm Password	Confirm the password required to access the Oracle Database Listener.
Log Folder Path	Type the directory path to access the Oracle Database Listener log files.
File Pattern	Type the regular expression (regex) required to filter the filenames. All matching files are included in the processing. The default is `listener\.log` This parameter does not accept wildcard or globbing patterns in the regular expression. For example, if you want to list all files starting with the word log, followed by one or more digits and ending with tar.gz, use the following entry: log[0-9]+\.tar\.gz. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

Table 161: Oracle Database Listener Parameters (Continued)

Parameter	Description
Force File Read	Select this check box to force the protocol to read the log file when the timing of the polling interval specifies. When the check box is selected, the log file source is always examined when the polling interval specifies, regardless of the last modified time or file size attribute. When the check box is not selected, the log file source is examined at the polling interval if the last modified time or file size attributes have changed.
Recursive	Select this check box if you want the file pattern to also search sub folders. By default, the check box is selected.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.
Throttle Events/Sec	Type the maximum number of events the Oracle Database Listener protocol forwards per second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default is 100 EPS.

8 Click **Save**.

9 On the **Admin** tab, click **Deploy Changes**.

The configuration of the Oracle Database Listener protocol is complete. For more information, see the *SIEM Log Sources User Guide*.

Collect Oracle Database Events Using Perl

The Oracle Database Listener application stores logs on the database server. To forward these logs from the Oracle server to SIEM, you must configure a Perl script on the Oracle server. The Perl script monitors the listener log file, combines any multi-line log entries into a single log entry, and sends the logs, using syslog (UDP), to SIEM.

Before being sent to SIEM, the logs are processed and re-formatted to ensure the logs are not forwarded line-by-line, as is found in the log file. All of the relevant information is retained.

NOTE

Perl scripts written for Oracle DB listener work on Linux/UNIX servers only. Windows Perl script is not supported.

To install and configure the Perl script:

1 Access the following websites to download the required files:
http://support.extremenetworks.com

2 From the **Software** tab, select **Scripts**.

3 Download the script to forward Oracle DB Listener events.

`oracle_dblistener_fwdr.pl.gz`

4 Extract the file:
`gzip -d oracle_dblistener_fwdr.pl.gz`

5 Copy the Perl script to the server that hosts the Oracle server.

NOTE

Perl 5.8 must be installed on the device that hosts the Oracle server.

6 Log in to the Oracle server using an account that has read/write permissions for the `listener.log` file and the `/var/run` directory.

7 Type the following command and include any additional command parameters to start the Oracle DB Listener script:

`oracle_dblistener_fwdr.pl -h <IP address> -t "tail -F listener.log"`

Where `<IP address>` is the IP address of your SIEM Console or Event Collector.

Table 162: Command Parameters

Parameters	Description
-D	The -D parameter defines that the script is to run in the foreground. Default is to run as a daemon and log all internal messages to the local syslog service.

-t	The -t parameter defines that the command-line is used to tail the log file (monitors any new output from the listener). The log file might be different across versions of the Oracle database; some examples are provided below:
	Oracle 9i:
	`<install_directory>/product/9.2/network/log/listener.log`
	Oracle 10g:
	`<install_directory>/product/10.2.0/db_1/network/log/listener.log`
	Oracle 11g:
	`<install_directory>/diag/tnslsnr/qaoracle11/listener/trace/listener.log`

-f	The -f parameter defines the syslog facility.priority to be included at the beginning of the log. If nothing is specified, `user.info` is used.
-H	The -H parameter defines the host name or IP address for the syslog header. It is recommended that this be the IP address of the Oracle server on which the script is running.
-h	The -h parameter defines the receiving syslog host (the Event Collector host name or IP address being used to receive the logs).
-p	The -p parameter defines the receiving UDP syslog port. If a port is not specified, `514` is used.

Table 162: Command Parameters (Continued)

Parameters	Description
-r	The -r parameter defines the directory name where you wish to create the .pid file. The default is /var/run. This parameter is ignored if -D is specified.
-l	The -l parameter defines the directory name where you wish to create the lock file. The default is /var/lock. This parameter is ignored if -D is specified.

For example, to monitor the listener log on an Oracle 9i server with an IP address of 182.168.12.44 and forward events to SIEM with the IP address of 192.168.1.100, type the following:

```
oracle_dblistener_fwdr.pl -t "tail -f <install_directory>/
product/9.2/network/log/listener.log"
-f user.info -H 192.168.12.44 -h 192.168.1.100 -p 514
```

A sample log from this setup would appear as follows:

```
<14>Apr 14 13:23:37 192.168.12.44 AgentDevice=OracleDBListener
Command=SERVICE_UPDATE   DeviceTime=18-AUG-2006
16:51:43   Status=0   SID=qora9
```

NOTE

The kill command can be used to terminate the script if you need to reconfigure a script parameter or stop the script from sending events to SIEM. For example, `kill -QUIT 'cat /var/run/oracle_dblistener_fwdr.pl.pid'`. The example command uses the backquote character (`), which is located to the left of the number one on most keyboard layouts.

You are now ready to configure the Oracle Database Listener within SIEM.

1 From the **Log Source Type** list, select **Oracle Database Listener**.

2 From the **Protocol Configuration** list, select **syslog**.

3 In the **Log Source Identifier** field, type the IP address of the Oracle Database you specified using the -H option in Step 7.

The configuration of the Oracle Database Listener protocol is complete. For more information on Oracle Database Listener, see your vendor documentation.

Oracle Audit Vault

The Oracle Audit Vault DSM for SIEM accepts events on Oracle v10.2.3.2 and later using Java Database Connectivity (JDBC) to accesses alerts on the JDBC protocol.

SIEM records Oracle Audit Vault alerts from the source database and captures events as configured by the Oracle Audit Policy Setting. When events occur, the alerts are stored in avsys.av$alert_store table. Customized events are created in Oracle Audit Vault by a user with AV_AUDITOR permissions.

See your vendor documentation about configuration of Audit Policy Settings in Oracle Audit Vault.

In Oracle Audit Vault, alert names are not mapped to a SIEM Identifier (QID). Using the Map Event function in the SIEM Events interface a normalized or raw event can be mapped to a high-level and low-level category (or QID). Using the Oracle Audit Vault DSM, category mapping can be done by mapping your high or low category alerts directly to an alert name (ALERT_NAME field) in the payload. For information about the Events interface, see the *SIEM Users Guide*.

Configure a Log Source

To configure a SIEM log source to access the Oracle Audit Vault database using the JDBC protocol:

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.

6 Using the Log Source Type list, select Oracle Audit Vault.

7 Using the Protocol Configuration list, select JDBC.

8 Configure the following values:
   a Database Type: **Oracle**
   b Database Name: <**Audit Vault Database Name**>
   c Table Name: **avsys.av$alert_store**
   d Select List: ***
   e Compare Field: **ALERT_SEQUENCE**
   f IP or Hostname: <**Location of Oracle Audit Vault Server**>
   g Port: <**Default Port**>
   h Username: <**Database Access Username having AV_AUDITOR role**>
   i Password: <**Password**>
   j Polling Interval: <**Default Interval**>

NOTE

Verify the AV_AUDITOR password has been entered correctly before saving the JDBC protocol configuration. Oracle Audit Vault might lock the user account due to repeated failed login attempts. When the AV_AUDITOR account is locked, data in the avsys.av$alert_store cannot be accessed. In order to unlock this user account, it is necessary to first correct the password entry in the protocol configuration. Then log in to Oracle Audit Vault through the Oracle sqlplus prompt as the avadmindva user to perform an alter user <AV_AUDITOR USER> account unlock command.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

NOTE

The local time zone conversion-dependent Oracle timestamps are not supported in earlier versions of the JDBC protocol for SIEM so fields AV_ALERT_TIME, ACTUAL_ALERT_TIME, and TIME_CLEARED in the payload only display object identifiers until your JDBC protocol is updated.

Oracle OS Audit

The Oracle OS Audit DSM for SIEM allows monitoring of the audit records that are stored in the local operating system file.

When audit event files are created or updated in the local operating system directory, a Perl script detects the change, and forwards the data to SIEM. The Perl script monitors the Audit log file, combines any multi-line log entries into a single log entry to ensure the logs are not forwarded line-by-line, as is found in the log file, then sends the logs using syslog to SIEM. Perl scripts written for Oracle OS Audit work on Linux/UNIX servers only. Windows-based Perl installations are not supported.

To integrate the Oracle OS Audit DSM with SIEM:

1 Access the following websites to download the required files:
http://support.extremenetworks.com

2 From the **Software** tab, select **Scripts**.

3 Download the Oracle OS Audit script:
`oracle_osauditlog_fwdr_5.3.tar.gz`

4 Type the following command to extract the file:
`tar -zxvf oracle_osauditlog_fwdr_5.3.tar.gz`

5 Copy the Perl script to the server that hosts the Oracle server.

NOTE

Perl 5.8 must be installed on the device that hosts the Oracle server. If you do not have Perl 5.8 installed, you might be prompted that library files are missing when you attempt to start the Oracle OS Audit script. We recommend you verify you have installed Perl 5.8 before you continue.

6 Log in to the Oracle host as an Oracle user that has SYS or root privilege.

7 Make sure the ORACLE_HOME and ORACLE_SID environment variables are configured properly for your deployment.

8 Open the following file:
`${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`

9 For syslog, add the following lines to the file:
```
*.audit_trail='os'
*.audit_syslog_level='local0.info'
```

10 Verify account has read/write permissions for the following directories:
```
/var/lock/
/var/run/
```

11 Restart the Oracle database instance.

12 Start the OS Audit DSM script:
`oracle_osauditlog_fwdr_5.3.pl -t target_host -d logs_directory`

Table 163: Oracle OS Audit Command Parameters

Parameters	Description
-t	The -t parameter defines the remote host that receives the audit log files.
-d	The -d parameter defines directory location of the DDL and DML log files. **NOTE:** The directory location you specify should be the absolute path from the root directory.
-H	The -H parameter defines the host name or IP address for the syslog header. We recommend that this be the IP address of the Oracle server on which the script is running.
-D	The -D parameter defines that the script is to run in the foreground. Default is to run as a daemon (in the background) and log all internal messages to the local syslog service.
-n	The -n parameter processes new logs, and monitors existing log files for changes to be processed. If the -n option string is absent all existing log files are processed during script execution.
-u	The -u parameter defines UDP.
-f	The -f parameter defines the syslog facility.priority to be included at the beginning of the log. If you do not type a value, `user.info` is used.

Table 163: Oracle OS Audit Command Parameters (Continued)

Parameters	Description
-r	The -r parameter defines the directory name where you want to create the .pid file. The default is /var/run. This parameter is ignored if -D is specified.
-l	The -l parameter defines the directory name where you want to create the lock file. The default is /var/lock. This parameter is ignored if -D is specified.
-h	The -t parameter displays the help message.
-v	The -v parameter displays the version information for the script.

If you restart your Oracle server you must restart the script:

```
oracle_osauditlog_fwdr.pl -t target_host -d logs_directory
```

You are now ready to configure the log sources within SIEM.

1 From the **Log Source Type** list, select Oracle RDBMS OS Audit Record.

2 From the Protocol Configuration list. select syslog.

3 From the Log Source Identifier field type the address specified using the –H option in Step 12. For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

For more information about your Oracle Audit Record, see your vendor documentation.

Oracle BEA WebLogic

The Oracle BEA WebLogic DSM allows SIEM to retrieve archived server logs and audit logs from any remote host, such as your Oracle BEA WebLogic server.

SIEM uses the log file protocol to retrieve events from your Oracle BEA WebLogic server and provide information on application events that occur in your domain or on a single server.

To integrate Oracle BEA WebLogic events, you must:

1 Enable auditing on your Oracle BEA WebLogic server.

2 Configure domain logging on your Oracle BEA WebLogic server.

3 Configure application logging on your Oracle BEA WebLogic server.

4 Configure an audit provider for Oracle BEA WebLogic.

5 Configure SIEM to retrieve log files from Oracle BEA WebLogic.

Enable Event Logs

By default, Oracle BEA WebLogic does not enable event logging.

To enable event logging on your Oracle WebLogic console:

1 Log in to your Oracle WebLogic console user interface.

2 Select **Domain > Configuration > General**.

3 Click **Advanced**.

4 From the **Configuration Audit Type** list, select **Change Log and Audit**.

5 Click **Save**.

You are now ready to configure the collection of domain logs for Oracle BEA WebLogic.

Configure Domain Logging

Oracle BEA WebLogic supports multiple instances. Event messages from instances are collected in a single domain-wide log for the Oracle BEA WebLogic server.

To configure the log file for the domain:

1 From your Oracle WebLogic console, select **Domain > Configuration > Logging**.

2 From the **Log file name** parameter, type the directory path and file name for the domain log. For example, OracleDomain.log.

3 Optional. Configure any additional domain log file rotation parameters.

4 Click **Save**.

You are now ready to configure application logging for the server.

Configure Application Logging

To configure application logging for Oracle BEA WebLogic:

1 From your Oracle WebLogic console, select **Server > Logging > General**.

2 From the **Log file name** parameter, type the directory path and file name for the application log. For example, OracleDomain.log.

3 Optional. Configure any additional application log file rotation parameters.

4 Click **Save**.

You are now ready to configure an audit provider for Oracle BEA WebLogic.

Configure an Audit Provider

To configure an audit provider:

1 Select **Security Realms > Realm Name > Providers > Auditing**.

2 Click **New**.

3 Configure an audit provider:
   a Type a name for the audit provider you are creating.
   b From the **Type** list, select **DefaultAuditor**.
   c Click **OK**.
   The Settings window is displayed.
4 Click the auditing provider you created in Step 3.
5 Click the **Provider Specific** tab.
6 Configure the following parameters:
   a Add any **Active Context Handler Enteries** required.
   b From the **Severity** list, select **INFORMATION**.
   c Click **Save**.
   You are now ready to configure SIEM to pull log files from Oracle BEA WebLogic.

Configure a Log Source

To configure SIEM to retrieve log files from Oracle BEA WebLogic:

1 Log in to SIEM.
2 Click the Admin tab.
3 On the navigation menu, click Data Sources.
   The Data Sources panel is displayed.
4 Click the Log Sources icon.
   The Log Sources window is displayed.
5 From the Log Source Type list, select Oracle BEA WebLogic.
6 Using the Protocol Configuration list, select Log File.
7 Configure the following parameters:

Table 164: Log File Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. This value must match the value configured in the Remote Host IP or Hostname parameter. The log source identifier must be unique for the log source type.
Service Type	From the list, select the File Transfer Protocol (FTP) you want to use for retrieving files. The options are: SSH File Transfer Protocol (SFTP), File Transfer Protocol (FTP), or Secure Copy (SCP). The default is SFTP.
Remote IP or Hostname	Type the IP address or hostname of the host from which you want to receive files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 to 65535.

Table 164: Log File Parameters (Continued)

Parameter	Description
Remote User	Type the username necessary to log in to the host running the selected Service Type. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host running the selected Service Type.
Confirm Password	Confirm the Remote Password to log in to the host running the selected Service Type.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. Also, when you provide an SSH Key File, the Remote Password option is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. For example, if you want to list all files starting with the word server, followed by one or more digits and ending with `.log`, use the following entry: `server[0-9]+\.log`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select a binary FTP transfer mode for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar.gz archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when using ASCII as the FTP Transfer Mode.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.

Table 164: Log File Parameters (Continued)

Parameter	Description
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File(s) parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a .zip, .gzip, .tar, or .tar.gz archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your SIEM system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select Oracle BEA WebLogic.

8 Click **Save**.

9 On the Admin tab, click Deploy Changes.

The configuration is complete.

Oracle Acme Packet Session Border Controller

You can use SIEM to collect events from Oracle Acme Packet Session Border Controller (SBC) installations in your network.

Configuration Overview

The Oracle Acme Packet SBC installations generate events from syslog and SNMP traps. SNMP trap events are converted to syslog and all events are forwarded to to SIEM over syslog. SIEM does not automatically discover syslog events that are forwarded from Oracle Communications SBC. SIEM supports syslog events from Oracle Acme Packet SBC V6.2 and later.

To collect Oracle Acme Packet SBC events, you must complete the following tasks:

1 On your SIEM system, configure a log source with the Oracle Acme Packet Session Border Controller DSM.

2 On your Oracle Acme Packet SBC installation, enable SNMP and configure the destination IP address for syslog events.

3 On your Oracle Acme Packet SBC installation, enable syslog settings on the media-manager object.

4 Restart your Oracle Acme Packet SBC installation.

5 Optional. Ensure that no firewall rules block syslog communication between your Oracle Acme Packet SBC installation and the SIEM Console or managed host that collects syslog events.

Supported Oracle Acme Packet Event Types that are Logged by SIEM

The Oracle Acme Packet SBC DSM for SIEM can collect syslog events from authorization and the system monitor event categories.

Each event category can contain low-level events that describe the action that is taken within the event category. For example, authorization events can have low-level categories of a login success or login failed.

Configuring an Oracle Acme Packet SBC Log Source

To collect syslog events from Oracle Acme Packet SBC, you must configure a log source in SIEM. Oracle Acme Packet SBC syslog events do not automatically discover in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 Optional. In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Oracle Acme Packet SBC**.

9 From the **Protocol Configuration** list, select **Syslog**.

10 Configure the following values:

Table 165: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name as an identifier for events from your Oracle Acme Packet SBC installation. The log source identifier must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

What's next

You are now ready to configure your Oracle Acme Packet SBC installation.

Configuring SNMP to Syslog Conversion on Oracle Acme Packet SBC

To collect events in a format compatible with SIEM, you must enable SNMP to syslog conversion and configure a syslog destination.

Procedure

1 Using SSH, log in to the command-line interface of your Oracle Acme Packet SBC installation as an administrator.

2 Type the following command to start the configuration mode:

```
config t
```

3 Type the following commands to start the system configuration:

```
(configure)# system
(system)#
(system)# system-config
(system-config)# sel
```

The sel command is required to select a single-instance of the system configuration object.

4 Type the following commands to configure your SIEM system as a syslog destination:

```
(system-config)# syslog-servers
(syslog-config)# address <SIEM IP address>
(syslog-config)# done
```

5 Type the following commands to enable SNMP traps and syslog conversion for SNMP trap notifications:

```
(system-config)# enable-snmp-auth-traps enabled
(system-config)# enable-snmp-syslog-notify enabled
(system-config)# enable-snmp-monitor-traps enabled
(system-config)# ids-syslog-facility 4
(system-config)# done
```

6 Type the following commands to return to configuration mode:

```
(system-config)# exit
(system)# exit
(configure)#
```

Enabling Syslog Settings on the Media Manager Object

The media-manager object configuration enables syslog notifications when the Intrusion Detection System (IDS) completes an action on an IP address. The available action for the event might be dependent on your firmware version.

Procedure

1 Type the following command to list the firmware version for your Oracle Acme Packet SBC installation:

```
(configure)# show ver
ACME Net-Net OSVM Firmware SCZ 6.3.9 MR-2 Patch 2 (Build 465)
Build Date=03/13/13
```

The underlined text is the major and minor version number for the firmware.

2 Type the following commands to configure the media-manager object:

```
(configure)# media-manager
(media-manager)#
(media-manager)# media-manager
(media-manager)# sel
(media-manager-config)#
```

The sel command is required to select a single-instance of the media-manager object.

3 Type the following command to enable syslog messages when an IP is demoted by the IDS system to the denied queue.

```
(media-manager-config)# syslog-on-demote-to-deny enabled
```

4 For firmware version C6.3.0 and later, type the following command to enable syslog message when sessions are rejected.

```
(media-manager-config)# syslog-on-call-reject enabled
```

5 For firmware version C6.4.0 and later, type the following command to enable syslog messages when an IP is demoted to the untrusted queue

```
(media-manager-config)# syslog-on-demote-to-untrusted enabled
```

6 Type the following commands to return to configuration mode:

```
(media-manager-config)# done
(media-manager-config)# exit
(media-manager)# exit
(configure)# exit
```

7 Type the following commands to save and activate the configuration:

```
# save
Save complete
# activate
```

8 Type `reboot` to restart your Oracle Acme Packet SBC installation.

After the system restarts, events are forwarded to SIEM and displayed on the **Log Activity** tab.

Oracle Fine Grained Auditing

The Oracle Fine Grained Auditing DSM can poll for database audit events from Oracle 9i and later by using the Java Database Connectivity (JDBC) protocol.

Configuration Overview

To collect events, administrators must enable fine grained auditing on their Oracle databases. Fine grained auditing provides events on select, update, delete, and insert actions that occur in the source database and the records the data changed. The database table dba_fga_audit_trail is updated with a new row each time a change occurs on a database table where the administrator enabled an audit policy.

To configure Oracle fine grained auditing, administators can complete the following tasks:

1 Configure on audit on any tables that require policy monitoring in the Oracle database.

2 Configure a log source for the Oracle Fine Grained Auditing DSM to poll the Oracle database for events.

3 Verify that the events polled are collected and displayed on the Log Activity tab of SIEM.

Configure a Log Source

After the database administrator has configured database polocies, a log source can be configured to access the Oracle database with the JDBC protocol.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 Using the Log Source Type list, select Oracle Fine Grained Auditing.

7 Using the Protocol Configuration list, select JDBC.

8 Configure the following values:

Table 166: Oracle Fine Grained Auditing JDBC parameters

Parameter	Description
Log Source Identifier	Type the log source identifier in the following format: `<database>@<hostname>` or `<table name>|<database>@<hostname>` Where: `<table name>` is the name of the table or view of the database containing the event records. This parameter is optional. If you include the table name, you must include a pipe (|) character and the table name must match the Table Name parameter. `<database>` is the database name, as defined in the Database Name parameter. The database name is a required parameter. `<hostname>` is the hostname or IP address for this log source, as defined in the IP or Hostname parameter. The hostname is a required parameter. The log source identifier must be unique for the log source type.
Database Type	Select **MSDE** as the database type.
Database Name	Type the name of the database to which you want to connect. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
IP or Hostname	Type the IP address or hostname of the database.
Port	Type the port number used by the database server. The default that is displayed depends on the selected Database Type. The valid range is 0 to 65536. The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections enabled to communicate with SIEM. The default port number for all options include: • **DB2** - 50000 • **MSDE** - 1433 • **Oracle** - 1521 **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the database username. The username can be up to 255 alphanumeric characters in length. The username can also include underscores (_).
Password	Type the database password. The password can be up to 255 characters in length.
Confirm Password	Confirm the password to access the database.

Table 166: Oracle Fine Grained Auditing JDBC parameters (Continued)

Parameter	Description
Authentication Domain	If you select MSDE as the Database Type, the **Authentication Domain** field is displayed. If your network is configured to validate users with domain credentials, you must define a Windows Authentication Domain. Otherwise, leave this field blank. The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.).
Database Instance	If you select MSDE as the Database Type, the **Database Instance** field is displayed. Type the type the instance to which you want to connect, if you have multiple SQL server instances on one server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Predefined Query	From the list, select **None**.
Table Name	Type `dba_fga_audit_trail` as the name of the table that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the JDBC protocol.
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `extended_timestamp` to identify new events added between queries to the table by their timestamp.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time	Optional. Configure the start date and time for database polling.
Polling Interval	Type the polling interval in seconds, which is the amount of time between queries to the database table. The default polling interval is 30 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.

Table 166: Oracle Fine Grained Auditing JDBC parameters (Continued)

Parameter	Description
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	If you select MSDE as the Database Type, the **Use Named Pipe Communications** check box is displayed. By default, this check box is clear. Select this check box to use an alternative method to a TCP/IP port connection. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Use NTLMv2	If you select MSDE as the Database Type, the **Use NTLMv2** check box is displayed. Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Use SSL	Select this check box if your connection supports SSL communication. This option requires additional configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.
Database Cluster Name	If you select the **Use Named Pipe Communication** check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

78 OSSEC

The OSSEC DSM for SIEM accepts events forwarded from OSSEC installations using syslog.

OSSEC is an open source Host-based Intrusion Detection System (HIDS) that can provide intrusion events to SIEM. If you have OSSEC agents installed, you must configure syslog on the OSSEC management server. If you have local or stand-alone installations of OSSEC, then you must configure syslog on each stand-alone OSSEC to forward syslog events to SIEM.

Configure OSSEC

To configure syslog for OSSEC on a stand-alone installation or management server:

1 Using SSH, log in to your OSSEC device.

2 Edit the OSSEC configuration file ossec.conf.
`<installation directory>/ossec/etc/ossec.conf`

3 Add the following syslog configuration.

The syslog configuration should be added after the alerts entry and before the localfile entry.

```
</alerts>
<syslog_output>
<server>(SIEM IP Address)</server>
<port>514</port>
</syslog_output>
<localfile>
For example,
<syslog_output>
<server>10.100.100.2</server>
<port>514</port>
</syslog_output>
```

4 Save the OSSEC configuration file.

5 Type the following command to enable the syslog daemon:
`<installation directory>/ossec/bin/ossec-control enable client-syslog`

6 Type the following command to restart the syslog daemon:
`<installation directory>/ossec/bin/ossec-control restart`

The configuration is complete. The log source is added to SIEM as OSSEC events are automatically discovered. Events forwarded to SIEM by OSSEC are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from OSSEC. The following configuration steps are optional.

To manually configure a log source for OSSEC:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select OSSEC.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 167: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your OSSEC installation.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

79 Palo Alto Networks

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

80 Pirean Access: One

The Pirean Access: One DSM for SIEM collects events by polling the DB2 audit database for access management and authentication events.

Supported Versions

SIEM supports Pirean Access: One software installations at v2.2 that use a DB2 v9.7 database to store access management and authentication events.

Before You Begin

Before you configure SIEM to integrate with Pirean Access: One, you can create a database user account and password for SIEM. Creating a SIEM account is not required, but is beneficial as it allows you to secure your access management and authentication event table data for the SIEM user. Your SIEM user must have read permissions for the database table that contains your events. The JDBC protocol allows SIEM to log in and poll for events from the database based on the timestamp to ensure the latest data is retrieved.

NOTE

Ensure that no firewall rules block communication between your Pirean Access: One installation and the SIEM Console or managed host responsible for event polling with JDBC.

Configuring a Log Source

To collect events, you must configure a log source in SIEM to poll your Access: One installation database with the JDBC protocol.

Procedure

1 Click the **Admin** tab.

2 On the navigation menu, click **Data Sources**.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **Pirean Access: One**.

8 Using the Protocol Configuration list, select JDBC.

9 Configure the following values:

Table 168: Pirean Access: One log source parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. The log source identifier must be defined in the following format: `<database>@<hostname>` Where: `<database>` is the database name, as defined in the Database Name parameter. The database name is a required parameter. `<hostname>` is the hostname or IP address for the log source as defined in the IP or Hostname parameter. The hostname is a required parameter. The log source identifier must be unique for the log source type.
Database Type	From the list, select **DB2** as the type of database to use for the event source.
Database Name	Type the name of the database to which you want to connect. The default database name is **LOGINAUD**.
IP or Hostname	Type the IP address or hostname of the database server.
Port	Type the TCP port number used by the audit database DB2 instance. Your DB2 administrator can provide you with the TCP port required for this field.
Username	Type a username that has access to the DB2 database server and audit table. The username can be up to 255 alphanumeric characters in length. The username can also include underscores (_).
Password	Type the database password. The password can be up to 255 characters in length.
Confirm Password	Confirm the password to access the database.
Table Name	Type **AUDITDATA** as the name of the table or view that includes the event records. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **TIMESTAMP** to identify new events added between queries to the table. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).

Table 168: Pirean Access: One log source parameters (Continued)

Parameter	Description
Use Prepared Statements	Select this check box to use prepared statements, which allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clear this check box to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time	Optional. Configure the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Enabled	Select this check box to enable the Pirean Access: One log source.

10 Click Save.

11 On the Admin tab, click Deploy Changes.

The configuration is complete. Access management and authentication events for Pirean Access: One are displayed on the **Log Activity** tab of SIEM.

81 PostFix Mail Transfer Agent

SIEM can collect and categorize syslog mail events from PostFix Mail Transfer Agents (MTA) installed in your network.

Configuration Overview

To collect syslog events, you must configure PostFix MTA installation to forward syslog events to SIEM. SIEM does not automatically discover syslog events that are forwarded from PostFix MTA installations as they are multiline events. SIEM supports syslog events from PostFix MTA V2.6.6.

To configure PostFix MTA, complete the following tasks:

1 On your PostFix MTA system, configure syslog.conf to forward mail events to SIEM.

2 On your SIEM system, create a log source for PostFix MTA to use the UDP multiline syslog protocol.

3 On your SIEM system, configure iptables to redirect events to the port defined for UDP multiline syslog events.

4 On your SIEM system, verify that your PostFix MTA events are displayed on the **Log Activity** tab.

If you have multiple PostFix MTA installations where events go to different SIEM systems, you must configure a log source and IPtables for each SIEM system that receives PostFix MTA multiline UDP syslog events.

Configuring Syslog for PostFix Mail Transfer Agent

To collect events, you must configure syslog on your PostFix MTA installation to forward mail events to SIEM.

Procedure

1 Using SSH, log in to your PostFix MTA installation as a root user.

2 Edit the following file:
`/etc/syslog.conf`

3 To forward all mail events, type the following command to change `-/var/log/maillog/` to an IP address. Make sure all other lines remain intact:
`mail.*  @<IP address>`
Where `<IP address>` is the IP address of the SIEM Console, Event Processor, or Event Collecor, or all-in-one system.

4 Save and exit the file.

5 Restart your syslog daemon to save the changes.

Configuring a PostFix MTA Log Source

To collect syslog events, you must configure a log source for PostFix MTA to use the UDP Multiline Syslog protocol.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select **PostFix Mail Transfer Agent**.

6 From the **Protocol Configuration** list, select **UDP Multiline Syslog**.

7 Configure the following values:

Table 169: PostFix MTA log source parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name to identify your PostFix MTA installation.
Listen Port	Type **517** as the port number used by SIEM to accept incoming UDP Multiline Syslog events. The valid port range is 1 to 65535. To edit a saved configuration to use a new port number: **1** In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. **2** Click **Save**. **3** On the **Admin** tab, select **Advanced > Deploy Full Configuration**. After the full deploy completes, SIEM is capable of receiving events on the updated listen port. **NOTE:** When you click **Deploy Full Configuration**, SIEM restarts all services, which results in a gap in data collection for events and flows until the deployment completes.
Message ID Pattern	Type the following regular expression (regex) required to filter the event payload messages. `postfix/.*?[ \[]\\d+[ \]](?:- - |: )([A-Z0-9]{8,10})`
Enabled	Select this check box to enable or disable the log source.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.

Table 169: PostFix MTA log source parameters (Continued)

Parameter	Description
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Payload Encoding	Select the character encoding required to parse the event logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Log Source Language	Select the language of the events generated by PostFix MTA.

8 Click **Save**.

9 On the **Admin** tab, click **Deploy Changes**.

Configure IPtables for multiline UDP Syslog Events

To collect events, you must redirect events from the standard PostFix MTA port to port 517 for the UDP multiline protocol.

Procedure

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

2 To edit the IPtables file, type the following command:
`vi /opt/qradar/conf/iptables-nat.post`

3 To instruct SIEM to redirect syslog events from UDP port 514 to UDP port 517, type the following command:

`-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>`

Where:

`<IP address>` is the IP address of your PostFix MTA installation.

`<New port>` is the port number configured in the UDP Multiline protocol for PostFix MTA.

For example, if you had three PostFix MTA installations that communicate to SIEM, you can type the following:

`-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s 10.10.10.10`

```
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s
10.10.10.11
-A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s
10.10.10.12
```

4 Save your IPtables NAT configuration.

You are now ready to configure IPtables on your SIEM Console or Event Collector to accept events from your PostFix MTA installation.

5 Type the following command to edit the IPtables file:

```
vi /opt/qradar/conf/iptables.post
```

6 Type the following command to instruct SIEM to allow communication from your PostFix MTA installations:

```
-I QChain 1 -m udp -p udp --src <IP address> --dport <New
port> -j ACCEPT
```

Where:

`<IP address>` is the IP address of your PostFix MTA installation.

`<New port>` is the port number configured in the UDP Multiline protocol.

For example, if you had three PostFix MTA installations communicating to an Event Collector, you can type the following:

```
-I QChain 1 -m udp -p udp --src 10.10.10.10 --dport 517 -j
ACCEPT
-I QChain 1 -m udp -p udp --src 10.10.10.11 --dport 517 -j
ACCEPT
-I QChain 1 -m udp -p udp --src 10.10.10.12 --dport 517 -j
ACCEPT
```

7 To save the changes and update IPtables, type the following command:

```
./opt/qradar/bin/iptables_update.pl
```

82 ProFTPd

SIEM can collect events from a ProFTP server through syslog.

By default, ProFTPd logs authentication related messages to the local syslog using the auth (or authpriv) facility. All other logging is done using the daemon facility. To log ProFTPd messages to SIEM, use the SyslogFacility directive to change the default facility.

Configure ProFTPd

To configure syslog on a ProFTPd device:

1 Open the `/etc/proftd.conf` file.

2 Below the LogFormat directives add the following:

`SyslogFacility <facility>`

Where `<facility>` is one of the following options: AUTH (or AUTHPRIV), CRON, DAEMON, KERN, LPR, MAIL, NEWS, USER, UUCP, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, or LOCAL7.

3 Save the file and exit.

4 Open the `/etc/syslog.conf` file

5 Add the following line at the end of the file:

`<facility> @<SIEM host>`

Where:

`<facility>` matches the facility chosen in step 2. The facility must be typed in lower case.

`<SIEM host>` is the IP address of your SIEM Console or Event Collector.

6 Restart syslog and ProFTPd:

```
/etc/init.d/syslog restart
/etc/init.d/proftpd restart
```

You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from ProFTPd. The following configuration steps are optional.

To manually configure a log source for ProFTPd:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select ProFTPd Server.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 170: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ProFTPd installation.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

83 Proofpoint Enterprise Protection and Enterprise Privacy

SIEM can collect and categorize syslog events from Proofpoint Enterprise Protection and Enterprise Privacy systems that are installed within your network.

The following events types are supported for Proofpoint installations:

- System events for Proofpoint Enterprise Protection
- Email security threat classification events for Proofpoint Enterprise Protection
- System events for Proofpoint Enterprise Privacy
- Email audit and encryption events for Proofpoint Enterprise Privacy

Configuration Overview

To collect syslog events, administrators must configure the Proofpoint appliance to forward syslog events. SIEM does not automatically discover syslog events that are forwarded from Proofpoint installations. SIEM supports syslog events from Proofpoint Enterprise Protection or Proofpoint Enterprise Privacy installations that use software version 7.0.2, 7.1, or 7.2.

To collect events from Proofpoint Enterprise, administrators must complete the following tasks:

1 On your Proofpoint system, configure the log settings to forward syslog events.

2 On your SIEM system, create a log source for Proofpoint Enterprise.

Configuring Syslog for Proofpoint Enterprise

To collect events, you must configure syslog on your Proofpoint installation to forward syslog events.

Procedure

1 Log in to the Proofpoint Enterprise interface.

2 Click **Logs and Reports**.

3 Click **Log Settings**.

4 From the Remote Log Settings pane, configure the following options to enable syslog communication:
   a Select **Syslog** as the communication protocol.
   b Type the IP address of the SIEM Console or Event Collector.
   c In the **Port** field, type **514** as the port number for syslog communication.
   d From the **Syslog Filter Enable** list, select **On**.
   e From the **Facility** list, select **local1**.
   f From the **Level** list, select **Information**.
   g From the **Syslog MTA Enable** list, select **On**.

5 Click Save.

Configuring a Proofpoint Log Source

To collect syslog events, you must configure a log source for Proofpoint Enterprise because the DSM does not support automatic discovery.

Procedure

1 Click the Admin tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 In the **Log Source Description** field, type a description for your log source.

6 From the Log Source Type list, select **Proofpoint Enterprise Protection/Enterprise Privacy**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the following values:

Table 171: Proofpoint Enterprise log source parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name to identify your Proofpoint Enterprise appliance.
Enabled	Select this check box to enable the log source.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Payload Encoding	Select the character encoding that is required to parse the event logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Table 171: Proofpoint Enterprise log source parameters (Continued)

Parameter	Description
Log Source Language	Select the language of the events that are generated by the Proofpoint Enterprise appliance.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

84 Radware DefensePro

The Radware DefensePro DSM for SIEM accepts events using syslog. Event traps can also be mirrored to a syslog server.

Before you configure SIEM to integrate with a Radware DefensePro device, you must configure your Radware DefensePro device to forward syslog events to SIEM. You must configure the appropriate information using the **Device > Trap and SMTP option**.

Any traps generated by the Radware device are mirrored to the specified syslog server. The current Radware Syslog server enables you to define the status and the event log server address.

You can also define additional notification criteria, such as Facility and Severity, which are expressed by numerical values:

- Facility is a user-defined value indicating the type of device used by the sender. This criteria is applied when the device sends syslog messages. The default value is 21, meaning Local Use 6.
- Severity indicates the importance or impact of the reported event. The Severity is determined dynamically by the device for each message sent.

In the Security Settings window, you must enable security reporting using the connect and protect/security settings. You must enable security reports to syslog and configure the severity (syslog risk).

You are now ready to configure the log source in SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Radware DefensePro. The following configuration steps are optional.

To manually configure a log source for Radware DefensePro:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Radware DefensePro.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 172: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Radware DefensePro installation.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

85 Raz-Lee iSecurity

SIEM that can collect and parse syslog events forwarded from Raz-Lee iSecurity installations on IBM iSeries® infrastructure.

Supported Versions

SIEM supports events from Raz-Lee iSecurity installations with Firewall v15.7 and Audit v11.7.

Supported Event Types

Raz-Lee iSecurity installations on IBM AS/400 iSeries are can forward syslog events for security, compliance, and auditing to SIEM.

All syslog events forwarded by Raz-Lee iSecurity automatically discover and the events are parsed and categorized with the IBM AS/400 iSeries DSM.

Configuring Raz-Lee iSecurity

To collect security and audit events, you must configure your Raz-Lee iSecurity installation to forward syslog events to SIEM.

Procedure

1 Log in to the IBM System i command-line interface.

2 Type the following command to access the audit menu options:
`STRAUD`

3 From the Audit menu, select **81. System Configuration**.

4 From the iSecurity/Base System Configuration menu, select **31. SYSLOG Definitions**.

5 Configure the following parameters:
   a **Send SYSLOG message** - Select **Yes**.
   b **Destination address** - Type the IP address of SIEM.
   c **"Facility" to use** - Type a facility level.
   d **"Severity" range to auto send** - Type a severity level.
   e **Message structure** - Type any additional message structure parameters required for your syslog messages.

Next steps

Syslog events forwarded by Raz-Lee iSecurity are automatically discovered by SIEM by the IBM AS/400 iSeries DSM. In most cases, the log source is automatically created in SIEM after a small number of events are detected. If the event rate is extremely low, then you might be required to manually create a log source for Raz-Lee iSecurity in SIEM. Until the log source is automatically discovered and identified, the event type displays as Unknown

on the **Log Activity** tab of SIEM. Automatically discovered log sources can be viewed on the **Admin** tab of SIEM by clicking the Log Sources icon.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events forwarded from Raz-Lee i Security. This procedure is optional.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select IBM AS/400 iSeries.

7 Using the Protocol Configuration list, select **Syslog**.

8 Configure the following values:

Table 173: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM AS/400 iSeries device with Raz-Lee iSecurity.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.

Table 173: Syslog Parameters (Continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

86 Redback ASE

The Redback ASE DSM for SIEM accepts events using syslog.

The Redback ASE device can send log messages to the Redback device console or to a log server that is integrated with SIEM to generate deployment specific reports. Before configuring a Redback ASE device in SIEM, you must configure your device to forward syslog events.

Configure Redback ASE

To configure the device to send syslog events to SIEM:

1 Log in to your Redback ASE device user interface.

2 Start the CLI configuration mode.

3 In global configuration mode, configure the default settings for the security service:

```
asp security default
```

4 In ASP security default configuration mode, configure the IP address of the log server and the optional transport protocol:

```
log server <IP address> transport udp port 9345
```

Where `<IP address>` is the IP address of the SIEM.

5 Configure the IP address that you want to use as the source IP address in the log messages:

```
log source <source IP address>
```

Where `<source IP address>` is the IP address of the loopback interface in context local.

6 Commit the transaction.

For more information about Redback ASE device configuration, see your vendor documentation.

For example, if you want to configure:

- Log source server IP address 10.172.55.55
- Default transport protocol: UDP
- Default server port: 514

The source IP address used for log messages is 10.192.22.24. This address must be an IP address of a loopback interface in context local.

```
asp security default
log server 10.172.55.55
log source 10.192.22.24
```

You are now ready to configure the log sources SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from Redback ASE. The following configuration steps are optional.

To manually configure a log source for Redback ASE:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Redback ASE.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 174: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Redback ASE appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

87 Riverbed SteelCentral NetProfiler (Audit and Alert)

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

88 RSA Authentication Manager

An RSA Authentication Manager DSM allows you to integrate SIEM with an RSA Authentication Manager using syslog or the log file protocol.

Before you configure SIEM to integrate with RSA Authentication Manager, select your configuration preference:

- Configuring syslog for RSA (page 3)
- Configuring the log file protocol for RSA (page 5)

NOTE

You must apply the most recent hot fix on RSA Authentication Manager 7.1 primary, replica, node, database and radius installations before configuring syslog.

Configuring Syslog for RSA

The procedure to configure your RSA Authentication Manager using syslog depends on the operating system version for your RSA Authentication Manager or SecureID 3.0 appliance:

- If you are using RSA Authentication Manager on Linux, see Configuring Linux on page 518.
- If you are using RSA Authentication Manager on Windows, see Configuring Windows on page 519.

Configuring Linux

To configure RSA Authentication Manager for syslog on Linux-based operating systems:

1 Log in to the RSA Security Console command-line interface (CLI).

2 Open the following file for editing based on your operating system:

```
/usr/local/RSASecurity/RSAAuthenticationManager/utils/resources
/ims.properties
```

3 Add the following enteries to the `ims.properties` file:

```
ims.logging.audit.admin.syslog_host          = <IP address>
ims.logging.audit.admin.use_os_logger       = true
ims.logging.audit.runtime.syslog_host       = <IP address>
ims.logging.audit.runtime.use_os_logger     = true
ims.logging.system.syslog_host                = <IP address>
ims.logging.system.use_os_logger              = true
```

Where `<IP address>` is the IP address or hostname of SIEM.

4 Save the `ims.properties` files.

5 Open the following file for editing:

```
/etc/syslog.conf
```

6 Type the following command to add SIEM as a syslog entry:

```
*.* @<IP address>
```

Where `<IP address>` is the IP address or hostname of SIEM.

7 Type the following command to restart the syslog services for Linux.

```
service syslog restart
```

You are now ready to configure the log sources and protocol in SIEM: To configure SIEM to receive events from your RSA Authentication Manager:

8 From the Log Source Type list, select the RSA Authentication Manager option.

For more information, see the *SIEM Log Sources User Guide.* For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

Configuring Windows

To configure RSA Authentication Manager for syslog using Microsoft Windows:

1 Log in to the system hosting your RSA Security Console.

2 Open the following file for editing based on your operating system:

```
/Program Files/RSASecurity/RSAAuthenticationManager/utils/
resources/ims.properties
```

3 Add the following enteries to the `ims.properties` file:

```
ims.logging.audit.admin.syslog_host         = <IP address>
ims.logging.audit.admin.use_os_logger      = true
ims.logging.audit.runtime.syslog_host      = <IP address>
ims.logging.audit.runtime.use_os_logger    = true
ims.logging.system.syslog_host               = <IP address>
ims.logging.system.use_os_logger             = true
```

Where `<IP address>` is the IP address or hostname of SIEM.

4 Save the `ims.properties` files.

5 Restart RSA services.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from your RSA Authentication Manager:

- From the Log Source Type list, select the RSA Authentication Manager option.

For more information, see the *SIEM Log Sources User Guide.* For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

Configuring the Log File Protocol for RSA

The log file protocol allows SIEM to retrieve archived log files from a remote host. The RSA Authentication Manager DSM supports the bulk loading of log files using the log file protocol source.

The procedure to configure your RSA Authentication Manager using the log file protocol depends on the version of RSA Authentication Manager:

- If you are using RSA Authentication Manager v7.x, see Configuring RSA Authentication Manager 7.x on page 520.
- If you are using RSA Authentication Manager v6.x, see Configuring RSA Authentication Manager 6.x on page 521.

Configuring RSA Authentication Manager 7.x

To configure your RSA Authentication Manager v7.x device:

1 Log in to the RSA Security Console.

2 Click **Administration > Log Management > Recurring Log Archive Jobs**.

3 In the Schedule section, configure values for the Job Starts, Frequency, Run Time, and Job Expires parameters.

4 For the **Operations** field, select Export Only or Export and Purge for the following settings: **Administration Log Settings**, **Runtime Log Settings**, and **System Log Settings**.

NOTE

The Export and Purge operation exports log records from the database to the archive and then purges the logs form the database. The Export Only operation exports log records from the database to the archive and the records remain in the database.

5 For **Administration**, **Runtime**, and **System**, configure an Export Directory to which you want to export your archive files.

We recommend you make sure you can access the Administration Log, Runtime Log, and System Log using FTP before you continue.

6 For Administration, Runtime, and System parameters, set the Days Kept Online parameter to 1. Logs older than 1 day are exported. If you selected Export and Purge, the logs are also purged from the database.

7 Click Save.

You are now ready to configure the log sources and protocol within SIEM:

1 To configure SIEM to receive events from a RSA device, you must select the RSA Authentication Manager option from the Log Source Type list.

2 To configure the log file protocol, you must select the Log File option from the Protocol Configuration list.

For more information on configuring log sources and protocols, see the *Log Sources User Guide*.

Configuring RSA Authentication Manager 6.x

To configure your RSA Authentication Manager v6.x device:

1 Log in to the RSA Security Console.

2 Log in to the RSA Database Administration tool:
   a Click the Advanced tool.
   The system prompts you to login again.
   b Click Database Administration.
   For complete information on using SecurID, see your vendor documentation.

3 From the Log list, select Automate Log Maintenance.
   The Automatic Log Maintenance window is displayed.

4 Select the Enable Automatic Audit Log Maintenance check box.

5 Select Delete and Archive.

6 Select Replace files.

7 Type an archive filename.

8 In the Cycle Through Version(s) field, type a value.
   For example, 1.

9 Select Select all Logs.

10 Select a frequency.

11 Click OK.

You are now ready to configure the log sources and protocol in SIEM:

1 To configure SIEM to receive events from a RSA device, you must select the RSA Authentication Manager option from the Log Source Type list.

2 To configure the log file protocol, you must select the Log File option from the Protocol Configuration list.

For more information on configuring log sources and protocols, see the *SIEM Log Sources User Guide*.

89 Safenet/DataSecure

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

90 Salesforce Security Auditing and Monitoring

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

91 Samhain Labs

The Samhain Labs Host-Based Intrusion Detection System (HIDS) monitors changes to files on the system.

The Samhain HIDS DSM for SIEM supports Samhain version 2.4 when used for File Integrity Monitoring (FIM).

You can configure the Samhain HIDS DSM to accept one of the following log types:

- Configuring Syslog to Collect Samhain Events on page 526
- Configuring JDBC to Collect Samhain Events on page 527

Configuring Syslog to Collect Samhain Events

Before you configure SIEM to integrate with Samhain HIDS using syslog, you must configure the Samhain HIDS system to forward logs to your SIEM system.

NOTE

The following procedure is based on the default samhainrc file. If the samhainrc file has been modified, some values might be different, such as the syslog facility,

Procedure

1 Log in to Samhain HIDS from the command-line interface.

2 Open the following file:
`/etc/samhainrc`

3 Remove the comment marker (`#`) from the following line:
`SetLogServer=info`

4 Save and exit the file.
Alerts are sent to the local system using syslog.

5 Open the following file:
`/etc/syslog.conf`

6 Add the following line:
`local2.* @<IP Address>`
Where `<IP Address>` is the IP address of your SIEM.

7 Save and exit the file.

8 Restart syslog:
`/etc/init.d/syslog restart`
Samhain sends logs using syslog to SIEM. You are now ready to configure Samhain HIDS DSM in SIEM.

To configure SIEM to receive events from Samhain:

From the Log Source Type list, select the Samhain HIDS option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Configuring JDBC to Collect Samhain Events

You can configure Samhain HIDS to send log alerts to a database. Oracle, PostgreSQL, and MySQL are natively supported by Samhain. You can also configure SIEM to collect events from these databases using the JDBC protocol.

NOTE

SIEM does not include a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the platform independent MySQL Connector/J from http://dev.mysql.com/downloads/connector/j/. For instruction on installing MySQL Connector/J for the JDBC protocol, see the *SIEM Log Sources User Guide*.

Procedure

1 Log into SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select the Samhain HIDS option.

7 Using the Protocol Configuration list, select JDBC.

8 Update the JDBC configuration to include the following values:
   a Database Type: `<Samhain Database Type>`
   b Database Name: `<Samhain SetDBName>`
   c Table Name: `<Samhain SetDBTable>`
   d Select List: `*`
   e Compare Field: `log_index`
   f IP or Hostname: `<Samhain SetDBHost>`
   g Port: `<Default Port>`
   h Username: `<Samhain SetDBUser>`
   i Password: `<Samhain SetDBPassword>`
   j Polling Interval: `<Default Interval>`

Where:

`<Samhain Database Type>` is the database type used by Samhain (see your Samhain system administrator).

`<Samhain SetDBName>` is the database name specified in the samhainrc file.

`<Samhain SetDBTable>` is the database table specified in the samhainrc file.

<Samhain SetDBHost> is the database host specified in the samhainrc file.

<Samhain SetDBUser> is the database user specified in the samhainrc file.

<Samhain SetDBPassword> is the database password specified in the samhainrc file.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from Samhain:

From the Log Source Type list, select the Samhain HIDS option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about Samhain, see http://www.la-samhna.de/samhain/manual.

92 Imperva SecureSphere

The Imperva SecureSphere DSM for SIEM records all relevant events forwarded using syslog.

Configuration Overview

To collect syslog events, you must configure your Imperva SecureSphere appliance with an alert and a system event action that can be associated to a firewall or system policy. Each time a firewall policy triggers an alert action or a system event policy triggers an event action a syslog event is sent to SIEM.

To configure events for your SecureSphere appliance, complete the following tasks:

1 On your Imperva SecureSphere appliance, create an alert action and associate the alert action to your SecureSphere firewall policies.

2 your Imperva SecureSphere appliance, create a system alert action and associate the action to your SecureSphere system event policies.

3 On your SIEM system, verify that the syslog events are forwarded and that a log source is automatically discovered.

Configuring an Alert Action for Imperva SecureSphere

You can configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to SIEM.

Procedure

1 Log in to your SecureSphere device user interface using administrative privileges.

2 Click the Policies tab.

3 Click the Action Sets tab.

4 To generate events for each alert generated by the SecureSphere device:
   a Click **New** to create a new action set for an alert.
   b Move the action to the Selected Actions list.
   c Expand the **System Log** action group.
   d In the **Action Name** field, type a name for your alert action.
   e Configure the following parameters:
   - Syslog host - Type the IP address of SIEM to which you want to send events.
   - Syslog log level - Select INFO.
   - Message - Define a message string for your event type from Table 175.

Table 175: Imperva SecureSphere alert message strings

Type	Version	Message string
Database alerts	V9.5 and V10	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}| ${Alert.alertType} ${Alert.immediateAction}\|Alert ID=${Alert.dn}|devTimeFormat=**[see note]**|devTime=${Alert.createTime}\|Alert type=${Alert.alertType}|src=${Alert.sourceIp} \|usrName=${Event.struct.user.user}|Application name=${Alert.applicationName}\|dst=${Event.destInfo.serverIp}|Alert Description=${Alert.description}\|Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}\|SecureSphere Version=${SecureSphereVersion}
File server alerts	V9.5 and V10	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}| ${Alert.alertType} ${Alert.immediateAction}\|Alert ID={Alert.dn}\|devTimeFormat=**[see note]** \|devTime=${Alert.createTime}|Alert type=${Alert.alertType}\|src=${Alert.sourceIp} |usrName=${Event.struct.user.username}\|Domain=${Event.struct.user.domain} |Application name=${Alert.applicationName}\|dst=${Event.destInfo.serverIp} |Alert Description=${Alert.description}\|Severity=${Alert.severity} |Immediate Action=${Alert.immediateAction} \|SecureSphere Version=${SecureSphereVersion}
Web application firewall alerts	V9.5 and V10	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}| ${Alert.alertType} ${Alert.immediateAction}\|Alert ID=${Alert.dn}|devTimeFormat=**[see note]**|devTime=${Alert.createTime}\|Alert type=${Alert.alertType}|src=${Alert.sourceIp} \|usrName=${Alert.username}|Application name=${Alert.applicationName} \|Service name=${Alert.serviceName}|Alert Description=${Alert.description} \|Severity=${Alert.severity}|Simulation Mode=${Alert.simulationMode} \|Immediate Action=${Alert.immediateAction}
All alerts	v6.2 and v7.x Release Enterprise Edition	DeviceType=ImpervaSecuresphere Alert|an=$!{Alert.alertMetadata.alertName}\|at=Securesphere Alert\|sp=$!{Event.sourceInfo.sourcePort}|s=$!{Event.sourceInfo.sourceIp}\|d=$!{ Event.destInfo.serverIp}|dp=$!{Event.destInfo.serverPort}\|u=$!{Alert.username} |g=$!{Alert.serverGroupName}\|ad=$!{Alert.description}

NOTE

The devTimeFormat does not include a value as the time format can be configured on the SecureSphere appliance. Administrators must review the time format of their SecureSphere appliance and specify the appropriate time format. For example, `dd MMM yyyy HH:mm:ss` or `yyyy-MM-dd HH:mm:ss.S`.

f Select the Run on Every Event check box.

g Click Save.

h Repeat this process to create an alert with another message type from Table 175.

5 To trigger syslog events, you must associate your firewall policies to use your alert actions.

a From the navigation menu, select **Policies > Security > Firewall Policy**.

b Select the policy you want to edit to use the alert action.
c Click the Policy tab.
d From the Followed Action list, select your new action.
e Ensure your policy is configured as enabled and is applied to the appropriate server groups.
f Click Save.
g Repeat this step for all policies that require an alert.

Configuring a System Event Action for Imperva SecureSphere

You can configure your Imperva SecureSphere appliance to forward syslog system policy events to SIEM.

1 Click the Policies tab.

2 Click the Action Sets tab.

3 To generate events for each event generated by the SecureSphere device:
a Click **New** to create a new action set for an event.
b Move the action to the Selected Actions list.
c Expand the System Log action group.
d In the **Action Name** field, type a name for your event action.
e Configure the following parameters:
- Syslog host - Type the IP address of SIEM to which you want to send events.
- Syslog log level - Select INFO.
- Message - Define a message string for your event type from Table 176.

Table 176: Imperva SecureSphere system event message strings

Type	Version	Message string
System events	V9.5 and V10	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Event.eventType}|Event ID=${Event.dn}\|devTimeFormat=**[see note]**\|devTime=${Event.createTime}|Event Type=${Event.eventType}\|Message=${Event.message}|Severity=${Event.severity.displayName}\|usrName=${Event.username}| SecureSphere Version=${SecureSphereVersion}

Table 176: Imperva SecureSphere system event message strings (Continued)

Type	Version	Message string
Database audit records	V9.5 and V10	LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Event.struct.eventType}|Server Group=${Event.serverGroup}\|Service Name=${Event.serviceName}|Application Name=${Event.applicationName}\|Source Type=${Event.sourceInfo.eventSourceType} |User Type=${Event.struct.user.userType}\|usrName=${Event.struct.user.user}|User Group=${Event.struct.userGroup}\|Authenticated=${Event.struct.user.authenticated} |App User=${Event.struct.applicationUser}\|src=${Event.sourceInfo.sourceIp}| Application=${Event.struct.application.application} \|OS User=${Event.struct.osUser.osUser}|Host=${Event.struct.host.host} \|Service Type=${Event.struct.serviceType}|dst=${Event.destInfo.serverIp} \|Event Type=${Event.struct.eventType}|Operation=${Event.struct.operations.name} \|Operation type=${Event.struct.operations.operationType} |Object name=${Event.struct.operations.objects.name} \|Object type=${Event.struct.operations.objectType}| Subject=${Event.struct.operations.subjects.name}\| Database=${Event.struct.databases.databaseName} |Schema=${Event.struct.databases.schemaName} \|Table Group=${Event.struct.tableGroups.displayName}| Sensitive=${Event.struct.tableGroups.sensitive}\| Privileged=${Event.struct.operations.privileged} |Stored Proc=${Event.struct.operations.storedProcedure} \|Completed Successfully=${Event.struct.complete.completeSuccessful} |Raw Data=${Event.struct.rawData.rawData} \|Parsed Query=${Event.struct.query.parsedQuery} |Bind Vaiables=${Event.struct.rawData.bindVariables}\| Error=${Event.struct.complete.errorValue} |Response Size=${Event.struct.complete.responseSize} \|Response Time=${Event.struct.complete.responseTime} |Affected Rows=${Event.struct.query.affectedRows}\| devTimeFormat=**[see note]**\|devTime=${Event.createTime}
All events	v6.2 and v7.x Release Enterprise Edition	DeviceType=ImpervaSecuresphere Event|et=$!{Event.eventType}\|dc=Securesphere System Event\|sp=$!{Event.sourceInfo.sourcePort}|s=$!{Event.sourceInfo.sourceIp}\| d=$!{Event.destInfo.serverIp}|dp=$!{Event.destInfo.serverPort}\|u=$!{Event.user name}| t=$!{Event.createTime}\|sev=$!{Event.severity}|m=$!{Event.message}

NOTE

The devTimeFormat does not include a value as the time format can be configured on the SecureSphere appliance. Administrators must review the time format of their SecureSphere appliance and specify the appropriate time format. For example, `dd MMM yyyy HH:mm:ss` or `yyyy-MM-dd HH:mm:ss.S`.

f Select the Run on Every Event check box.
g Click Save.
h Repeat this process to create an alert with another message type from Table 176.

4 To enable the action, you must edit your system event policies to use the action.

The below procedure details the steps to configure the action for a system event policy. Repeat this procedure for all required policies.

a Go to **Policies > System Events**.
b Select or create the system event policy you want to edit to use the event action.
c Click the Followed Action tab.
d From the Followed Action list, select your system event action.
e Click Save.
f Repeat this step for all system event policies that require an action.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Imperva SecureSphere. The following configuration steps are optional.

Procedure

1 Log in to SIEM.
2 Click the **Admin** tab.
3 Click the Log Sources icon.
4 Click Add.
5 In the **Log Source Name** field, type a name for your log source.
6 From the Log Source Type list, select Imperva SecureSphere.
7 Using the Protocol Configuration list, select **Syslog**.
8 Configure the following values:

Table 177: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Imperva SecureSphere appliance.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.

Table 177: Syslog protocol parameters (Continued)

Parameter	Description
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

93 Sentrigo Hedgehog

You can integrate a Sentrigo Hedgehog device with SIEM.

A Sentrigo Hedgehog device accepts LEEF events using syslog. Before you configure SIEM to integrate with a Sentrigo Hedgehog device, you must:

1 Log in to the Sentrigo Hedgehog command-line interface (CLI).

2 Open the following file for editing:
`<Installation directory>/conf/sentrigo-custom.properties`
Where `<Installation directory>` is the directory containing your Sentrigo Hedgehog installation.

3 Add the following log.format entries to the custom properties file:

NOTE

Depending on your Sentrigo Hedgehog configuration or installation, you might be required to replace or overwrite the existing log.format entry.

```
sentrigo.comm.ListenAddress=1996
log.format.body.custom=usrName=$osUser:20$|duser=$execUser:20$|
severity=$severity$|identHostName=$sourceHost$|src=$sourceIP$|
dst=$agent.ip$|devTime=$logonTime$|devTimeFormat=EEE MMM dd
HH:mm:ss z yyyy|cmdType=$cmdType$|externalId=$id$|
execTime=$executionTime.time$|dstServiceName=$database.name:20$|sr
cHost=$sourceHost:30$|execProgram=$execProgram:20$|
cmdType=$cmdType:15$|oper=$operation:225$|
accessedObj=$accessedObjects.name:200$
log.format.header.custom=LEEF:1.0|Sentrigo|Hedgehog|$serverVersion
$|$rules.name:150$|
log.format.header.escaping.custom=\\|
log.format.header.seperator.custom=,
log.format.header.escape.char.custom=\\
log.format.body.escaping.custom=\=
log.format.body.escape.char.custom=\\
log.format.body.seperator.custom=|
log.format.empty.value.custom=NULL
log.format.length.value.custom=10000
log.format.convert.newline.custom=true
```

4 Save the custom properties file.

5 Stop and restart your Sentrigo Hedgehog service to implement the log.format changes.
You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Sentrigo Hedgehog device:

From the Log Source Type list, select the Sentrigo Hedgehog option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about Sentrigo Hedgehog see your vendor documentation.

94 Secure Computing Sidewinder

The Sidewinder DSM for SIEM records all relevant Sidewinder events using syslog.

Before you configure SIEM to integrate with a Sidewinder device, you must configure syslog within your Sidewinder device. When configuring the Sidewinder device to forward syslog to SIEM, make sure that the logs are exported in Sidewinder Export format (SEF).

For more information on configuring Sidewinder, see your vendor documentation.

After you configure syslog to forward events to SIEM, you are ready to configure the log source in SIEM.

To configure SIEM to receive events from a Sidewinder device:

From the **Log Source Type** list, select Sidewinder G2 Security Appliance option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

95 SolarWinds Orion

The SolarWinds Orion DSM for SIEM supports SNMPv2 and SNMPv3 configured alerts from the SolarWinds Alert Manager.

The events are sent to SIEM using syslog. Before you can integrate SIEM, you must configure the SolarWinds Alert Manager to create SNMP traps and forward syslog events.

To configure SNMP traps in the SolarWinds Orion Alert Manager:

1 Select **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.

The Alert Manager Quick Start is displayed.

2 Click **Configure Alerts**.

The Manage Alerts window is displayed.

3 Select an existing alert and click **Edit**.

4 Select the **Triggered Actions** tab.

5 Click **Add New Action**.

The Select an Action window is displayed.

6 Select Send an SNMP Trap and click **OK**.

7 Configure the following values:

a **SNMP Trap Definitions** - Type the IP address of the SIEM Console or Event Collector.

b **Trap Template** - Select **ForwardSyslog**.

c **SNMP Version** - Select the SNMP Version to use to forward the event. SIEM supports SNMPv2c or SNMPv3.

- **SNMPv2c** - Type the **SNMP Community String** to use for SNMPv2c authentication. The default Community String value is public.
- **SNMPv3** - Type the **Username** and select the **Authentication Method** to use for SNMPv3.

SIEM supports MD5 or SH1 as methods of authentication and DES56 or AES128 bit encryption.

8 Click OK to save the SNMP trigger action.

The Manage Alerts window is displayed.

NOTE

To verify that your SNMP trap is configured properly, select an alert you've edited and click **Test**. The action should trigger and forward the syslog event to SIEM.

9 Repeat Step 3 to Step 8 to configure the Alert Manager with all of the SNMP trap alerts you want to monitor in SIEM.

You are now ready to configure the log source in SIEM.

SIEM automatically detects syslog events from properly configured SNMP trap alert triggers. However, if you want to manually configure SIEM to receive events from SolarWinds Orion:

From the **Log Source Type** list, select **SolarWinds Orion**.

For more information on configuring log sources, see the *SIEM Log Sources Users Guide*.

96 SonicWALL

The SonicWALL SonicOS DSM accepts events using syslog.

SIEM records all relevant syslog events forwarded from SonicWALL appliances using SonicOS firmware. Before you can integrate with a SonicWALL SonicOS device, you must configure syslog forwarding on your SonicWALL SonicOS appliance.

Configure SonicWALL to Forward Syslog Events

SonicWALL captures all SonicOS event activity. The events can be forwarded to SIEM using SonicWALL's default event format.

Procedure

1 Log in to your SonicWALL web interface.

2 From the navigation menu, select **Log > Syslog**.

3 From the Syslog Servers pane, click **Add**.

4 In the **Name or IP Address** field, type the IP address of your SIEM Console or Event Collector.

5 In the **Port** field, type **514**.

SonicWALL syslog forwarders send events to SIEM using UDP port 514.

6 Click **OK**.

7 From the **Syslog Format** list, select **Default**.

8 Click **Apply**.

Syslog events are forwarded to SIEM. SonicWALL events forwarded to SIEM are automatically discovered and log sources are created automatically. For more information on configuring your SonicWALL appliance or for information on specific events, see your vendor documentation.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from SonicWALL appliances. The following configuration steps are optional.

To manually configure a log source for SonicWALL syslog events:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select SonicWALL SonicOS.

8 Using the Protocol Configuration list, select **Syslog**.

9 Configure the following values:

Table 178: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from SonicWALL appliances. Each log source you create for your SonicWALL SonicOS appliance should include a unique identifier, such as an IP address or host name.

10 Click Save.

11 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by SonicWALL SonicOS appliances are displayed on the **Log Activity** tab. For more information, see the *SIEM Users Guide*.

97 Sophos

This section provides information on the following:

Sophos Enterprise Console

SIEM has two options for gathering events from a Sophos Enterprise Console using JDBC.

Select the method that best applies to your Sophos Enterprise Console installation:

NOTE

To use the Sophos Enterprise Console protocol, you must ensure that the Sophos Reporting Interface is installed with your Sophos Enterprise Console. If you do not have the Sophos Reporting Interface, you must configure SIEM using the JDBC protocol. For information on installing the Sophos Reporting Interface, see your Sophos Enterprise Console documentation.

Configure SIEM Using the Sophos Enterprise Console Protocol

The Sophos Enterprise Console DSM for SIEM accepts events using Java Database Connectivity (JDBC).

The Sophos Enterprise Console DSM works in coordination with the Sophos Enterprise Console protocol to combine payload information from anti-virus, application control, device control, data control, tamper protection, and firewall logs in the vEventsCommonData table and provide these events to SIEM. You must install the Sophos Enterprise Console protocol before configuring SIEM.

To configure SIEM to access the Sophos database using the JDBC protocol:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 From the Log Source Type list, select Sophos Enterprise Console.

7 From the Protocol Configuration list, select Sophos Enterprise Console JDBC.

NOTE

You must refer to the Configure Database Settings on your Sophos Enterprise Console to define the parameters required to configure the Sophos Enterprise Console JDBC protocol in SIEM.

8 Configure the following values:

Table 179: Sophos Enterprise Console JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Sophos Database>@<Sophos Database Server IP or Host Name>` Where: `<Sophos Database>` is the database name, as entered in the Database Name parameter. `<Sophos Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. **NOTE:** When defining a name for your log source identifier, you must use the values of the Sophos Database and Database Server IP address or hostname from the Management Enterprise Console.
Database Type	From the list, select MSDE.
Database Name	Type the exact name of the Sophos database.
IP or Hostname	Type the IP address or host name of the Sophos SQL Server.
Port	Type the port number used by the database server. The default port for MSDE in Sophos Enterprise Console is 1168. The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.

Table 179: Sophos Enterprise Console JDBC Parameters (Continued)

Parameter	Description
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type vEventsCommonData as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **InsertedAt** as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

Table 179: Sophos Enterprise Console JDBC Parameters (Continued)

Parameter	Description
Use NTLMv2	If you select MSDE as the Database Type, the **Use NTLMv2** check box is displayed. Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Sophos log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

Configure SIEM Using the JDBC Protocol

The Sophos Enterprise Console DSM for SIEM accepts events using Java Database Connectivity (JDBC).

SIEM records all relevant anti-virus events. This document provides information on configuring SIEM to access the Sophos Enterprise Console database using the JDBC protocol.

Configure the Database View

To integrate SIEM with Sophos Enterprise Console:

1 Log in to your Sophos Enterprise Console device command-line interface (CLI).

2 Type the following command to create a custom view in your Sophos database to support SIEM:

```
CREATE VIEW threats_view AS SELECT t.ThreatInstanceID,
t.ThreatType, t.FirstDetectedAt, c.Name, c.LastLoggedOnUser,
c.IPAddress, c.DomainName, c.OperatingSystem, c.ServicePack,
t.ThreatSubType, t.Priority, t.ThreatLocalID,
t.ThreatLocalIDSource, t.ThreatName, t.FullFilePathCheckSum,
t.FullFilePath, t.FileNameOffset, t.FileVersion, t.CheckSum,
t.ActionSubmittedAt, t.DealtWithAt, t.CleanUpable, t.IsFragment,
t.IsRebootRequired, t.Outstanding, t.Status, InsertedAt FROM
<Database Name>.dbo.ThreatInstancesAll t, <Database
Name>.dbo.Computers c WHERE t.ComputerID = c.ID;
```

Where `<Database Name>` is the name of the Sophos database.

NOTE

The database name must not contain any spaces.

After you have created your custom view, you must configure SIEM to receive event information using the JDBC protocol.

To configure the Sophos Enterprise Console DSM with SIEM, see Configure a JDBC Log Source in SIEM on page 547.

Configure a JDBC Log Source in SIEM

To configure SIEM to access the Sophos database using the JDBC protocol:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

6 Using the Log Source Type list, select Sophos Enterprise Console.

7 Using the Protocol Configuration list, select JDBC.

NOTE

You must refer to the Configure Database Settings on your Sophos Enterprise Console to define the parameters required to configure the Sophos Enterprise Console DSM in SIEM.

8 Configure the following values:

Table 180: Sophos Enterprise Console JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Sophos Database>@<Sophos Database Server IP or Host Name>` Where: `<Sophos Database>` is the database name, as entered in the Database Name parameter. `<Sophos Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. **NOTE:** When defining a name for your log source identifier, you must use the values of the Sophos Database and Database Server IP address or hostname from the Management Enterprise Console.
Database Type	From the list, select MSDE.
Database Name	Type the exact name of the Sophos database.
IP or Hostname	Type the IP address or host name of the Sophos SQL Server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type threats_view as the name of the table or view that includes the event records.

Table 180: Sophos Enterprise Console JDBC Parameters (Continued)

Parameter	Description
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **ThreatInstanceID** as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Sophos log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Sophos PureMessage

The Sophos PureMessage DSM for SIEM accepts events using Java Database Connectivity (JDBC).

SIEM records all relevant quarantined email events. This document provides information on configuring SIEM to access the Sophos PureMessage database using the JDBC protocol.

SIEM supports the following Sophos PureMessage versions:

- Sophos PureMessage for Microsoft Exchange - Stores events in a Microsoft SQL Server database specified as savexquar.
- Sophos PureMessage for Linux - Stores events in a PostgreSQL database specified as pmx_quarantine.

This section provides information on the following:

- Integrate SIEM with Sophos PureMessage for Microsoft Exchange on page 550
- Integrate SIEM with Sophos PureMessage for Linux on page 553

Integrate SIEM with Sophos PureMessage for Microsoft Exchange

To integrate SIEM with Sophos PureMessage for Microsoft Exchange:

1 Log in to the Microsoft SQL Server command-line interface (CLI):

```
osql -E -S localhost\sophos
```

2 Type which database you want to integrate with SIEM:

```
use savexquar;
go
```

3 Type the following command to create a SIEM view in your Sophos database to support SIEM:

```
create view siem_view as select 'Windows PureMessage' as
application, id, reason, timecreated, emailonly as sender,
filesize, subject, messageid, filename  from dbo.quaritems,
dbo.quaraddresses  where ItemID = ID and Field = 76;
Go
```

After you create your SIEM view, you must configure SIEM to receive event information using the JDBC protocol.

To configure the Sophos PureMessage DSM with SIEM, see Configure a JDBC Log Source for Sophos PureMessage on page 551.

Configure a JDBC Log Source for Sophos PureMessage

To configure SIEM to access the Sophos PureMessage for Microsoft Exchange database using the JDBC protocol:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 From the Log Source Type list, select Sophos PureMessage.

7 From the Protocol Configuration list, select JDBC.

NOTE

You must refer to the database configuration settings on your Sophos PureMessage device to define the parameters required to configure the Sophos PureMessage DSM in SIEM.

8 Configure the following values:

Table 181: Sophos PureMessage JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Sophos PureMessage Database>@<Sophos PureMessage Database Server IP or Host Name>` Where: `<Sophos PureMessage Database>` is the database name, as entered in the Database Name parameter. `<Sophos PureMessage Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. When defining a name for your log source identifier, you must use the values of the Database and Database Server IP address or hostname of the Sophos PureMessage device.

Table 181: Sophos PureMessage JDBC Parameters (Continued)

Parameter	Description
Database Type	From the list, select MSDE.
Database Name	Type `savexquar`.
IP or Hostname	Type the IP address or host name of the Sophos PureMessage server.
Port	Type the port number used by the database server. The default port for MSDE is 1433. Sophos installations typically use 24033. You can confirm port usage using the SQL Server Configuration Manager utility. For more information, see your vendor documentation. The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a database instance in the Database Instance parameter, you must leave the Port parameter blank. You can only define a database instance if the database server uses the default port of 1433. This is not the standard Sophos configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you define a port number other than the default in the Port parameter, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank.
Table Name	Type `siem_view` as the name of the table or view that includes the event records.
Select List	Type `*` for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `ID`. The Compare Field parameter is used to identify new events added between queries to the table.

Table 181: Sophos PureMessage JDBC Parameters (Continued)

Parameter	Description
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24-hour clock. If the Start Date and Time parameter is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Sophos PureMessage log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Integrate SIEM with Sophos PureMessage for Linux

To integrate SIEM with Sophos PureMessage for Linux:

1 Navigate to your Sophos PureMessage PostgreSQL database directory:
```
cd /opt/pmx/postgres-8.3.3/bin
```
2 Access the pmx_quarantine database SQL prompt:
```
./psql -d pmx_quarantine
```
3 Type the following command to create a SIEM view in your Sophos database to support SIEM:
```
create view siem_view as select 'Linux PureMessage' as
application, id, b.name, m_date, h_from_local, h_from_domain,
m_global_id, m_message_size, outbound, h_to, c_subject_utf8 from
message a, m_reason b where a.reason_id = b.reason_id;
```
After you create your database view, you must configure SIEM to receive event information using the JDBC protocol.

Configure a Log Source for Sophos PureMessage for Microsoft Exchange

To configure SIEM to access the Sophos PureMessage database using the JDBC protocol:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 From the Log Source Type list, select Sophos PureMessage.

7 From the Protocol Configuration list, select JDBC.

NOTE

You must refer to the Configure Database Settings on your Sophos PureMessage to define the parameters required to configure the Sophos PureMessage DSM in SIEM.

8 Configure the following values:

Table 182: Sophos PureMessage JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<Sophos PureMessage Database>@<Sophos PureMessage Database Server IP or Host Name>` Where: `<Sophos PureMessage Database>` is the database name, as entered in the Database Name parameter. `<Sophos PureMessage Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. When defining a name for your log source identifier, you must use the values of the Database and Database Server IP address or hostname of the Sophos PureMessage device.
Database Type	From the list, select Postgres.
Database Name	Type `pmx_quarantine`.
IP or Hostname	Type the IP address or host name of the Sophos PureMessage server.
Port	Type the port number used by the database server. The default port is 1532. The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with SIEM.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type `siem_view` as the name of the table or view that includes the event records.
Select List	Type `*` for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).

Table 182: Sophos PureMessage JDBC Parameters (Continued)

Parameter	Description
Compare Field	Type **ID**. The Compare Field parameter is used to identify new events added between queries to the table.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24-hour clock. If the Start Date and Time parameter is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Sophos PureMessage log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Sophos Astaro Security Gateway

The Sophos Astaro Security Gateway DSM for SIEM accepts events using syslog, enabling SIEM to record all relevant events.

Configure Syslog for Sophos Astaro

To configure syslog for Sophos Astaro Security Gateway:

1 Log in to the Sophos Astaro Security Gateway console.

2 From the navigation menu, select **Logging > Settings**.

3 Click the **Remote Syslog Server** tab.
The Remote Syslog Status window is displayed.

4 From **Syslog Servers** panel, click the + icon.
The Add Syslog Server window is displayed.

5 Configure the following parameters:
   a **Name** - Type a name for the syslog server.
   b **Server** - Click the folder icon to add a pre-defined host, or click **+** and type in new network definition.
   c **Port** - Click the folder icon to add a pre-defined port, or click **+** and type in a new service definition.

   By default, SIEM communicates using the syslog protocol on UDP/TCP port 514.

6 Click Save.

7 From the Remote syslog log selection field, you must select check boxes for the following logs:
   a **POP3 Proxy** - Select this check box.
   b **Packet Filter** - Select this check box.
   c **Intrusion Prevention System** - Select this check box.
   d **Content Filter(HTTPS)** - Select this check box.
   e **High availability** - Select this check box.
   f **FTP Proxy** - Select this check box.
   g **SSL VPN** - Select this check box.
   h **PPTP daemon**- Select this check box.
   i **IPSEC VPN** - Select this check box.
   j **HTTP daemon** - Select this check box.
   k **User authentication daemon** - Select this check box.
   l **SMTP proxy** - Select this check box.

8 Click **Apply**.

9 From **Remote syslog status** section, click **Enable**.

10 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from your Sophos Astaro Security Gateway device:

u From the **Log Source Type** list, select **Sophos Astaro Security Gateway**.

For more information on configuring log sources, see *SIEM Log Sources User Guide*.

Sophos Web Security Appliance

The Sophos Web Security Appliance (WSA) DSM for SIEM accepts events using syslog.

SIEM records all relevant events forwarded from the transaction log of the Sophos Web Security Appliance. Before configuring SIEM, you must configure your Sophos WSA appliance to forward syslog events.

Configure Syslog for Sophos Web Security Appliance

To configure your Sophos Web Security Appliance to forward syslog events:

1 Log in to your Sophos Web Security Appliance.

2 From the menu, select **Configuration > System > Alerts & Monitoring**.

3 Select the **Syslog** tab.

4 Select the **Enable syslog transfer of web traffic** check box.

5 In the **Hostname/IP** text box, type the IP address or hostname of SIEM.

6 In the **Port** text box, type **514**.

7 From the **Protocol** list, select a protocol. The options are:

- **TCP** - The TCP protocol is supported with SIEM on port 514.
- **UDP** - The UDP protocol is supported with SIEM on port 514.
- **TCP - Encrypted** - TCP Encrypted is an unsupported protocol for SIEM.

8 Click **Apply**.

You are now ready to configure the Sophos Web Security Appliance DSM in SIEM.

SIEM automatically detects syslog data from a Sophos Web Security Appliance. To manually configure SIEM to receive events from Sophos Web Security Appliance:

u From the **Log Source Type** list, select **Sophos Web Security Appliance**.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

98 Sourcefire

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

99 SSH CryptoAuditor

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

100 Splunk

SIEM accepts and parses multiple event types forwarded from Splunk appliances.

NOTE

For Check Point events forwarded from Splunk, see Integrating Check Point Firewall Events from External Syslog Forwarders on page 109.

Collect Windows Events Forwarded from Splunk Appliances

To collect events, you can configure your Windows end points to forward events to your SIEM Console and your Splunk indexer.

Forwarding Windows events from aggregation nodes in your Splunk deployment is not suggested. Splunk indexers that forward events from multiple Windows end points to SIEM can obscure the true source of the events with the IP address of the Splunk indexer. To prevent a situation where an incorrect IP address association might occur in the log source, you can update your Windows end point systems to forward to both the indexer and your SIEM Console.

Splunk events are parsed by using the Microsoft Windows Security Event Log DSM with the TCP multiline syslog protocol. The regular expression configured in the protocol defines where a Splunk event starts or ends in the event payload. The event pattern allows SIEM to assemble the raw Windows event payload as a single-line event that is readable by SIEM. The regular expression required to collect Windows events is outlined in the log source configuration.

To configure event collection for Splunk syslog events, you must complete the following tasks:

1 On your SIEM appliance, configure a log source to use the Microsoft Windows Security Event Log DSM.

NOTE

You must configure one log source for Splunk events. SIEM can use the first log source to autodiscover additional Windows end points.

2 On your Splunk appliance, configure each Splunk Forwarder on the Windows instance to send Windows event data to your SIEM Console or Event Collector.

To configure a Splunk Forwarder, you must edit the props, transforms, and output configuration files. For more information on event forwarding, see your Splunk documentation.

3 Ensure that no firewall rules block communication between your Splunk appliance and the SIEM Console or managed host that is responsible for retrieving events.

4 On your SIEM appliance, verify the **Log Activity** tab to ensure that the Splunk events are forwarded to SIEM.

Configuring a Log Source for Splunk Forwarded Events

To collect raw events forwarded from Splunk, you must configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 Optional. In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **Microsoft Windows Security Event Log**.

9 From the **Protocol Configuration** list, select **TCP Multiline Syslog**.

10 Configure the following values:

Table 183: Protocol parameters for TCP multiline syslog

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Splunk appliance. The log source identifier must be unique value.
Listen Port	Type the port number used by SIEM to accept incoming TCP multiline syslog events from Splunk. The default listen port is 12468. The port number you configure must match the port that you configured on your Splunk Forwarder. You can use the listen port to collect events from up to 50 event sources that have a common event pattern. You cannot specify port 514 in this field.
Event Formatter	From the list, select **Windows Multiline.** The event formatter ensures the format of the TCP multiline event matches the event pattern for the event type you selected.
Event Start Pattern	Type the following regular expression (regex) to identify the start of your Splunk windows event: `(?:<(\d+)>\s?(\w{3} \d{2} \d{2}:\d{2}:\d{2}) (\S+) )?(\d{2}/\d{2}/\d{4} \d{2}:\d{2}:\d{2} [AP]M)` The TCP multiline syslog protocol captures all the information between each occurrence of the defined regex pattern to create single-line syslog events.
Event End Pattern	This field can be cleared of any regex patterns.

Table 183: Protocol parameters for TCP multiline syslog (Continued)

Parameter	Description
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

13 Optional. If you have 50 or more Windows sources, you must repeat this process to create another log source.

Events provided by the Splunk Forwarder to SIEM are displayed on the **Log Activity** tab.

101 Squid Web Proxy

The Squid Web Proxy DSM for SIEM records all cache and access log events using syslog.

To integrate SIEM with Squid Web Proxy, you must configure your Squid Web Proxy to forward your cache and access logs using syslog.

Configure Syslog Forwarding

To configure Squid Web Proxy to forward your access and cache events using syslog:

1 Using SSH, log in to the Squid device command-line interface (CLI).

2 Open the following file:
`/etc/rc3.d/S99local`

3 Add the following line:
`tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &`
Where:
`<facility>` is any valid syslog facility (such as, authpriv, daemon, local0 to local7, or user) written in lowercase.
`<priority>` is any valid priority (such as, err, warning, notice, info, debug) written in lowercase.

4 Save and close the file.
Logging begins the next time the system is rebooted.

5 To begin logging immediately, type the following command:
`nohup tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &`
Where `<facility>` and `<priority>` are the same values entered in step 3.

6 Open the following file:
`/etc/squid/squid.conf`

7 Add the following line to send the logs to the SIEM:
`<prioirty>.<facility> @<SIEM_IP_address>`
Where:
`<priority>` is the priority of your Squid messages
`<facility>` is the facility of your Squid messages
`<SIEM_IP_address>` is the IP address or hostname of your SIEM.
For example:
`info.local4 @172.16.210.50`

8 Add the following line to squid.conf to turn off Squid httpd log emulation:
`emulate_httpd_log off`

9 Save and close the file.

10 Type the following command to restart the syslog daemon:

```
/etc/init.d/syslog restart
```

For more information on configuring Squid Web Proxy, consult your vendor documentation. After you configure syslog forwarding your cache and access logs, the configuration is complete. SIEM can automatically discover syslog events forwarded from Squid Web Proxy.

Create a Log Source

SIEM automatically discovers and creates a log source for syslog events forwarded from Squid Web Proxy appliances. These configuration steps for creating a log source are optional.

To manually configure a log source for Squid Web Proxy:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for the log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Squid Web Proxy.

9 From the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 184: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from the Squid Web Proxy.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The configuration is complete.

102 Starent Networks

The Starent Networks DSM for SIEM accepts Event, Trace, Active, and Monitor events.

Before configuring a Starent Networks device in SIEM, you must configure your Starent Networks device to forward syslog events to SIEM.

To configure the device to send syslog events to SIEM:

1 Log in to your Starent Networks device.

2 Configure the syslog server:

The following table provides the necessary parameters:

Table 185: Syslog Server Parameters

Parameter	Description
syslog <IP address>	Type the IP address of your SIEM
facility <facilities>	Type the local facility for which the logging options shall be applied. The options are: • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 The default is local7.
rate value	Type the rate that you want log entries to be sent to the system log server. This value must be an integer from 0 to 100000. The default is 1000 events per second.
pdu-verbosity <pdu-level>	Type the level of verboseness you want to use in logging the Protocol Data Units (PDUs). The range is 1 to 5 where 5 is the most detailed. This parameter only affects protocol logs.
pdu-data <format>	Type the output format for the PDU when logged as one of following formats: • none - Displays results in raw or unformatted text. • hex - Displays results in hexadecimal format. • hex-ascii - Displays results in hexadecimal and ASCII format similar to a main frame dump.

Table 185: Syslog Server Parameters (Continued)

Parameter	Description
event-verbosity <event_level>	Type the level of detail you want to use in logging of events, including: • min - Provides minimal information about the event, such as, event name, facility, event ID, severity level, data, and time. • concise - Provides detailed information about the event, but does not provide the event source. • full - Provides detailed information about the event including the source information identifying the task or subsystem that generated the event.

3 From the root prompt for the Exec mode, identify the session for which the trace log is to be generated:

The following table provides the necessary parameters:

Table 186: Trace Log Parameters

Parameter	Description
callid <call_id>	Indicates a trace log is generated for a session identified by the call identification number. This value is a 4-byte hexadecimal number.
ipaddr <IP address>	Indicates a trace log is generated for a session identified by the specified IP address.
msid <ms_id>	Indicates a trace log is generated for a session identified by the mobile station identification (MSID) number. This value must be from 7 to 16 digits, specified as an IMSI, MIN, or RMI.
name <username>	Indicates a trace log is generated for a session identified by the username. This value is the name of the subscriber that was previously configured.

4 To write active logs to the active memory buffer, in the config mode:

5 Configure a filter for the active logs:

The following table provides the necessary parameters:

Table 187: Active Log Parameters

Parameter	Description
facility <facility>	Type the facility message level. A facility is a protocol or task that is in use by the system. The local facility defines which logging options shall be applied for processes running locally. The options are: • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 The default is local7.
level <report_level>	Type the log severity level, including: • critical - Logs only those events indicating a serious error has occurred that is causing the system or a system component to cease functioning. This is the highest level severity. • error - Logs events that indicate an error has occurred that is causing the system or a system component to operate in a degraded date. This level also logs events with a higher severity level. • warning - Logs events that can indicate a potential problem. This level also logs events with a higher severity level. • unusual - Logs events that are very unusual and might need to be investigated. This level also logs events with a higher severity level. • info - Logs informational events and events with a higher severity level. • debug - Logs all events regardless of the severity. We recommend that a level of error or critical can be configured to maximize the value of the logged information while minimizing the quantity of logs generated.
critical-info	The critical-info parameter identifies and displays events with a category attribute of critical information. Examples of these types of events can be seen at bootup when system processes or tasks are being initiated.
no-critical-info	The no-critical-info parameter specifies that events with a category attribute of critical information are not displayed.

6 Configure the monitor log targets:

The following table provides the necessary parameters:

Table 188: Monitor Log Parameters

Parameter	Description
msid <md_id>	Type an msid to define that a monitor log is generated for a session identified using the Mobile Station Identification (MDID) number. This value must be between 7 and 16 digits specified as a IMSI, MIN, or RMI.
username <username>	Type username to identify a monitor log generated for a session by the username. The username is the name of the subscriber that was previously configured.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Starent device:

From the Log Source Type list, select the Starent Networks Home Agent (HA) option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about the device, see your vendor documentation.

103 STEALTHbits StealthINTERCEPT

The SIEM DSM for STEALTHbits StealthINTERCEPT can collect event logs from your STEALTHbits StealthINTERCEPT servers.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT DSM:

Table 189: STEALTHbits StealthINTERCEPT DSM specifications

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM	STEALTHbits StealthINTERCEPT
RPM file name	DSM-STEALTHbitsStealthINTERCEPT-*build_number*.noarch.rpm
Supported versions	
Protocol	Syslog LEEF
SIEM recorded events	Active Directory Audit Events
Automatically discovered	Yes
Includes identity	No
More information	www.stealthbits.com/resources

STEALTHbits StealthINTERCEPT DSM Integration Process

To integrate STEALTHbits StealthINTERCEPT DSM with SIEM, use the following procedure:

1 If automatic updates are not enabled, download and install the most recent RPM files on your SIEM Console. RPMs need to be installed only one time. The most recent version of the following RPM files are required:

- DSMCommon RPM
- STEALTHbits StealthINTERCEPT RPM

2 For each instance of STEALTHbits StealthINTERCEPT, configure you STEALTHbits StealthINTERCEPT system to enable communication with SIEM.

3 If SIEM does not automatically discover the log source, for each STEALTHbits StealthINTERCEPT server that you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually installing a DSM (page 6)

Configuring your STEALTHbits StealthINTERCEPT system for communication with SIEM (page 4)

Configuring a STEALTHbits StealthINTERCEPT log source in SIEM (page 5)

Configuring your STEALTHbits StealthINTERCEPT System for Communication with SIEM

To collect all audit logs and system events from STEALTHbits StealthINTERCEPT, you must specify SIEM as the syslog server and configure the message format.

Procedure

1 Log in to your STEALTHbits StealthINTERCEPT server.

2 Start the Administration Console.

3 Click **Configuration > Syslog Server**.

4 Configure the following parameters:

Table 190: STEALTHbits Parameters

Parameter	Description
Host Address	The IP address of the SIEM Console
Port	514

5 Click **Import mapping file**.

6 Select the `SyslogLeefTemplate.txt` file and press Enter.

7 Click **Save**.

8 On the Administration Console, click **Actions**.

9 Select the mapping file that you imported, and then select the **Send to Syslog** check box.

Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.

10 Click **Add**.

Configuring a STEALTHbits StealthINTERCEPT Log Source in SIEM

To collect STEALTHbits StealthINTERCEPT events, configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **STEALTHbits StealthINTERCEPT**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

104 Stonesoft Management Center

The Stonesoft Management Center DSM for SIEM accepts events using syslog.

SIEM records all relevant LEEF formatted syslog events. Before configuring SIEM, you must configure your Stonesoft Management Center to export LEEF formatted syslog events.

This document includes the steps required to edit LogServerConfiguration.txt file. Configuring the text file allows Stonesoft Management Center to export event data in LEEF format using syslog to SIEM. For detailed configuration instructions, see the *StoneGate Management Center Administrator's Guide*.

Configuring Stonesoft Management Center

To configure Stonesoft Management Center:

Procedure

1 Log in to the appliance hosting your Stonesoft Management Center.

2 Stop the Stonesoft Management Center Log Server:

- **Windows** - Select one of the following methods to stop the Log Server:
  - Stop the Log Server in the Windows Services list.
  - Run the batch file `<installation path>/bin/sgStopLogSrv.bat`.
- **Linux** - To stop the Log Server in Linux, run the script `<installation path>/bin/sgStopLogSrv.sh`.

3 Edit the LogServerConfiguration.txt file. The configuration file is located in the following directory:
`<installation path>/data/LogServerConfiguration.txt`

4 Configure the following parameters in the LogServerConfiguration.txt file:

Table 191: Log Server Configuration Options

Parameter	Value	Description
SYSLOG_EXPORT_FORMAT	LEEF	Type LEEF as the export format to use for syslog.
SYSLOG_EXPORT_ALERT	YES | NO	Type one of the following values: • **Yes** - Exports alert entries to SIEM using syslog. • **No** - Alert entries are not exported using syslog.
SYSLOG_EXPORT_FW	YES | NO	Type one of the following values: • **Yes** - Exports firewall and VPN entries to SIEM using syslog. • **No** - Firewall and VPN entries are not exported using syslog.

Table 191: Log Server Configuration Options (Continued)

Parameter	Value	Description
SYSLOG_EXPORT_IPS	YES | NO	Type one of the following values: • **Yes** - Exports IPS log file entries to SIEM using syslog. • **No** - IPS entries are not exported using syslog.
SYSLOG_PORT	514	Type 514 as the UDP port for forwarding syslog events to SIEM.
SYSLOG_SERVER_ADDRESS	SIEM IPv4 Address	Type the IPv4 address of your SIEM Console or Event Collector.

5 Save the LogServerConfiguration.txt file.

6 Start the Log Server:

- **Windows** - Type `<installation path>/bin/sgStartLogSrv.bat`.
- **Linux** - Type `<installation path>/bin/sgStartLogSrv.sh`.
  You are now ready to configure a traffic rule for syslog.

NOTE

A firewall rule is only required if your SIEM Console or Event Collector is separated by a firewall from the Stonesoft Management Server. If no firewall exists between the Management Server and SIEM, you need to configure the log source in SIEM.

Configure a Syslog Traffic Rule

If the Stonesoft Management Center and SIEM are separated by a firewall in your network, you must modify your firewall or IPS policy to allow traffic between the Stonesoft Management Center and SIEM.

Procedure

1 From the Stonesoft Management Center, select one of the following methods for modifying a traffic rule:

- **Firewall policies** - Select **Configuration > Configuration > Firewall**.
- **IPS policies** - Select **Configuration > Configuration > IPS**.

2 Select the type of policy to modify:

- **Firewall** - Select **Firewall Policies > Edit Firewall Policy**.
- **IPS** - Select **IPS Policies > Edit Firewall Policy**.

3 Add an IPv4 Access rule with the following values to the firewall policy:
   a **Source** - Type the IPv4 address of your Stonesoft Management Center Log Server.
   b **Destination** - Type the IPv4 address of your SIEM Console or Event Collector.

c **Service** - Select **Syslog (UDP)**.
d **Action** - Select **Allow**.
e **Logging** - Select **None**.

NOTE

In most cases, we recommend setting the logging value to **None**. Logging syslog connections without configuring a syslog filter can create a loop. For more information, see the *StoneGate Management Center Administrator's Guide*.

4 Save your changes and refresh the policy on the firewall or IPS.

You are now ready to configure the log source in SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Stonesoft Management Center. The following configuration steps are optional.

Procedure

1 Log in to SIEM.
2 Click the **Admin** tab.
3 On the navigation menu, click **Data Sources**.
4 Click the Log Sources icon.
5 Click Add.
6 In the **Log Source Name** field, type a name for your log source.
7 In the **Log Source Description** field, type a description for the log source.
8 From the Log Source Type list, select **Stonesoft Management Center**.
9 Using the Protocol Configuration list, select **Syslog**.
10 Configure the following values:

Table 192: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Stonesoft Management Center appliance.

11 Click Save.
12 On the Admin tab, click Deploy Changes.

The configuration is complete.

105 Sun Solaris

This section provides DSM configuration information on the following:

Sun Solaris

The Sun Solaris DSM for records all relevant Solaris authentication events using syslog.

Configuring Sun Solaris

To collect authentication events from Sun Solaris, you must configure syslog to forward events to SIEM.

Procedure

1 Log in to the Sun Solaris command-line interface.

2 Open the `/etc/syslog.conf` file.

3 To forward system authentication logs to SIEM, add the following line to the file:

```
*.err;auth.notice;auth.info                    @<IP address>
```

Where `<IP address>` is the IP address of your SIEM. Use tabs instead of spaces to format the line.

NOTE

Depending on the version of Solaris you are running, you might need to add additional log types to the file. Contact your system administrator for more information.

4 Save and exit the file.

5 Type the following command:

```
kill -HUP `cat /etc/syslog.pid`
```

You are now ready to configure the log source SIEM.

Configuring a Sun Solaris DHCP Log Source

SIEM automatically discovers and creates a log source for syslog events from Sun Solaris DHCP installations. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Solaris Operating System Authentication Messages.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 193: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Sun Solaris installations. Each additional log source you create when you have multiple installations should include a unique identifier, such as an IP address or host name.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Solaris Sendmail is displayed on the **Log Activity** tab.

Sun Solaris DHCP

The Sun Solaris DHCP DSM for SIEM records all relevant DHCP events using syslog.

Configuring Sun Solaris DHCP

To collect events from Sun Solaris DHCP, you must configure syslog to forward events to SIEM.

Procedure

1 Log in to the Sun Solaris command-line interface.

2 Edit the `/etc/default/dhcp` file.

3 Enable logging of DHCP transactions to syslog by adding the following line:

`LOGGING_FACILITY=X`

Where `X` is the number corresponding to a local syslog facility, for example, a number from 0 to 7.

4 Save and exit the file.

5 Edit the `/etc/syslog.conf` file.

6 To forward system authentication logs to SIEM, add the following line to the file:

`localX.notice @<IP address>`

Where:

`X` is the logging facility number you specified in Step 3.

`<IP address>` is the IP address of your SIEM. Use tabs instead of spaces to format the line.

7 Save and exit the file.

8 Type the following command:

`kill -HUP 'cat /etc/syslog.pid'`

You are now ready to configure the log source in SIEM.

Configuring a Sun Solaris DHCP Log Source

1 SIEM automatically discovers and creates a log source for syslog events from Sun Solaris DHCP installations. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Solaris Operating System DHCP Logs.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 194: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Sun Solaris DHCP installations. Each additional log source you create when you have multiple installations should include a unique identifier, such as an IP address or host name.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Solaris Sendmail is displayed on the **Log Activity** tab.

Sun Solaris Sendmail

The Sun Solaris Sendmail DSM for SIEM accepts Solaris authentication events using syslog and records all relevant sendmail events.

Configuring Syslog for Sun Solaris Sendmail

To collect events from Sun Solaris Sendmail, you must configure syslog to forward events to SIEM.

Procedure

1 Log in to the Sun Solaris command-line interface.

2 Open the `/etc/syslog.conf` file.

3 To forward system authentication logs to SIEM, add the following line to the file:

```
mail.*; @<IP address>
```

Where `<IP address>` is the IP address of your SIEM. Use tabs instead of spaces to format the line.

NOTE

Depending on the version of Solaris you are running, you might need to add additional log types to the file. Contact your system administrator for more information.

4 Save and exit the file.

5 Type the following command:

```
kill -HUP `cat /etc/syslog.pid`
```

You are now ready to configure the log source SIEM.

Configuring a Sun Solaris Sendmail Log Source

SIEM automatically discovers and creates a log source for syslog events from Sun Solaris Sendmail appliances. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Solaris Operating System Sendmail Logs.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 195: Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Sun Solaris Sendmail installations. Each additional log source you create when you have multiple installations should include a unique identifier, such as an IP address or host name.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. Events forwarded to SIEM by Solaris Sendmail is displayed on the **Log Activity** tab.

Sun Solaris Basic Security Mode (BSM)

Sun Solaris Basic Security Mode (BSM) is an audit tracking tool for system administrator to retrieve detailed auditing events from Sun Solaris systems.

SIEM retrieves Sun Solaris BSM events using the Log File protocol. To you configure SIEM to integrate with Solaris Basic Security Mode, you must:

1 Enable Solaris Basic Security Mode.

2 Convert audit logs from binary to a human-readable format.

3 Schedule a cron job to run the conversion script on a schedule.

4 Collect Sun Solaris events in SIEM using the Log File protocol.

Enabling Basic Security Mode

To configure Sun Solaris BSM, you must enable Solaris Basic Security Mode and configure the classes of events the system logs to an audit log file.

Procedure

1 Log in to your Solaris console as a superuser or root user.

2 Enable single-user mode on your Solaris console.

3 Type the following command to run the bsmconv script and enable auditing:
`/etc/security/bsmconv`
The bsmconv script enables Solaris Basic Security Mode and starts the auditing service auditd.

4 Type the following command to open the audit control log for editing:
`vi /etc/security/audit_control`

5 Edit the audit control file to contain the following information:
```
dir:/var/audit
flags:lo,ad,ex,-fw,-fc,-fd,-fr
naflags:lo,ad
```

6 Save the changes to the audit_control file, then reboot the Solaris console to start auditd.

7 Type the following command to verify auditd has started:
`/user/sbin/auditconfig -getcond`
If the auditd process is started, the following string is returned:
audit condition = auditing
You are now ready to convert the binary Solaris Basic Security Mode logs to a human-readable log format.

Converting Sun Solaris BSM Audit Logs

SIEM cannot process binary files directly from Sun Solaris BSM. You must convert the audit log from the existing binary format to a human-readable log format using praudit before the audit log data can be retrieved by SIEM.

Procedure

1 Type the following command to create a new script on your Sun Solaris console:

```
vi /etc/security/newauditlog.sh
```

2 Add the following information to the newauditlog.sh script:

```
#!/bin/bash
#
# newauditlog.sh - Start a new audit file and expire the old
logs
#

AUDIT_EXPIRE=30
AUDIT_DIR="/var/audit"
LOG_DIR="/var/log/"

/usr/sbin/audit -n

cd $AUDIT_DIR # in case it is a link

# Get a listing of the files based on creation date that are
not current in use
FILES=$(ls -lrt | tr -s " " | cut -d" " -f9 | grep -v
"not_terminated")

# We just created a new audit log by doing 'audit -n', so we
can
# be sure that the last file in the list will be the latest
# archived binary log file.
lastFile=""
for file in $FILES; do
          lastFile=$file
done

# Extract a human-readable file from the binary log file
echo "Beginning praudit of $lastFile"
praudit -l $lastFile > "$LOG_DIR$lastFile.log"
echo "Done praudit, creating log file at: $LOG_DIR$lastFile.log"

/usr/bin/find . $AUDIT_DIR -type f -mtime +$AUDIT_EXPIRE \
-exec rm {} > /dev/null 2>&1 \;
# End script
```

The script outputs log files in the <starttime>.<endtime>.<hostname>.log format.

For example, the log directory in /var/log would contain a file with the following name:

20111026030000.20111027030000.qasparc10.log

3 Optional. Edit the script to change the default directory for the log files.
   a **AUDIT_DIR="/var/audit"** - The Audit directory must match the location specified by the audit control file you configured in Step 5.
   b **LOG_DIR="/var/log/"** - The log directory is the location of the human-readable log files of your Sun Solaris system that are ready to be retrieved by SIEM.

4 Save your changes to the newauditlog.sh script.

   You are now ready to automate the this script using CRON to convert the Sun Solaris Basic Security Mode log to human-readable format.

Creating a Cron Job

Cron is a Solaris daemon utility that automates scripts and commands to run system-wide on a scheduled basis.

The following steps provide an example for automating newauditlog.sh to run daily at midnight. If you need to retrieve log files multiple times a day from your Solaris system, you must alter your cron schedule accordingly.

Procedure

1 Type the following command to create a copy of your cron file:
```
crontab -l > cronfile
```
2 Type the following command to edit the cronfile:
```
vi cronfile
```
3 Add the following information to your cronfile:
```
0 0 * * * /etc/security/newauditlog.sh
```
4 Save the change to the cronfile.

5 Type the following command to add the cronfile to crontab:
```
crontab cronfile
```
6 You are now ready to configure the log source in SIEM to retrieve the Sun Solaris BSM audit log files.

What to do next

You are now ready to configure a log source in SIEM.

Configuring a Log Source for Sun Solaris BSM

A log file protocol source allows SIEM to retrieve archived log files from a remote host. Sun Solaris BSM supports the bulk loading of audit log files using the log file protocol.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 From the Log Source Type list, select Solaris BSM.

6 Using the Protocol Configuration list, select Log File.

7 Configure the following parameters:

Table 196: Log File Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service types requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or hostname of the Sun Solaris BSM system.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 to 65535.
Remote User	Type the username necessary to log in to your Sun Solaris system. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to your Sun Solaris system.
Confirm Password	Confirm the Remote Password to log in to your Sun Solaris system.
SSH Key File	If you select SCP or SFTP from the **Service Type** field you can define a directory path to an SSH private key file. The SSH Private Key File allows you to ignore the **Remote Password** field.
Remote Directory	Type the directory location on the remote host from which the files are retrieved. By default, the newauditlog.sh script writes the human-readable logs files to the **/var/log/** directory.

Table 196: Log File Parameters (Continued)

Parameter	Description
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. For example, if you want to retrieve all files in the <starttime>.<endtime>.<hostname>.log format, use the following entry: `\d+\.\d+\.\w+\.log`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the **Processor** field and **LINEBYLINE** the **Event Generator** field when using ASCII as the transfer mode.
SCP Remote File	If you select SCP as the Service Type, you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File(s) parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a .zip, .gzip, .tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.

Table 196: Log File Parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your SIEM system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LINEBYLINE.

8 Click **Save**.

The configuration is complete. Events that are retrieved using the log file protocol are displayed on the **Log Activity** tab of SIEM.

106 Sybase ASE

You can integrate a Sybase Adaptive Server Enterprise (ASE) device with SIEM to record all relevant events using JDBC.

To configure a Sybase ASE device:

1 Configure Sybase auditing.

For information about configuring Sybase auditing, see your Sybase documentation.

2 Log in to the Sybase database as an `sa` user:

```
isql -Usa -P<password>
```

Where `<password>` is the password necessary to access the database.

3 Switch to the security database:

```
use sybsecurity
go
```

4 Create a view for SIEM.

```
create view audit_view
as
select audit_event_name(event) as event_name, * from
<audit_table_1>
union
select audit_event_name(event) as event_name, * from
<audit_table_2>
go
```

5 For each additional audit table in the audit configuration, make sure the union select parameter is repeated for each additional audit table.

For example, if you want to configure auditing with four audit tables (sysaudits_01, sysaudits_02,sysaudits_03, sysaudits_04), type the following:

```
create view audit_view as select audit_event_name(event) as
event_name, * from sysaudits_01
union select audit_event_name(event) as event_name, * from
sysaudits_02,
union select audit_event_name(event) as event_name, * from
sysaudits_03,
union select audit_event_name(event) as event_name, * from
sysaudits_04
```

You are now ready to configure the log source SIEM.

To configure SIEM to receive events from a Sybase ASE device:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

4 Click the Log Sources icon.

The Log Sources window is displayed.

5 Click Add.

The Add a log source window is displayed.

1 From the Log Source Type list, select the Sybase ASE option.

2 Using the Protocol Configuration list, select JDBC.

The JDBC protocol configuration is displayed.

3 Update the JDBC configuration to include the following values:

a Database Name: `sybsecurity`

b Port: `5000` (Default)

c Username: `sa`

d Table Name: `audit_view`

e Compare Field: `eventtime`

The Database Name and Table Name parameters are case sensitive.

For more information on configuring log sources and protocols, see the *SIEM Log Sources User Guide*. For more information about the Sybase ASE device, see your vendor documentation.

107 Symantec

This section provides information on the following DSMs:

Symantec Endpoint Protection

The Symantec Endpoint Protection DSM for SIEM accepts events using syslog.

SIEM records all Audit and Security log events. Before configuring a Symantec Endpoint Protection device in SIEM, you must configure your device to forward syslog events.

Procedure

1 Log in to the Symantec Endpoint Protection Manager

2 On the left panel, click the Admin icon.
The View Servers option is displayed.

3 From the bottom of the View Servers panel, click Servers.

4 From the View Servers panel, click Local Site.

5 From the Tasks panel, click Configure External Logging.

6 On the **Generals** tab:
   a Select the Enable Transmission of Logs to a Syslog Server check box.
   b In the Syslog Server field, type the IP address of your SIEM you want to parse the logs.
   c In the **UDP Destination Port** field, type 514.
   d In the **Log Facility** field, type 6.

7 In the Log Filter tab:
   a Under the Management Server Logs, select the Audit Logs check box.
   b Under the Client Log panel, select the Security Logs check box.
   c Under the Client Log panel, select the Risks check box.

8 Click OK.
You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Symantec Endpoint Protection device:

From the Log Source Type list, select the Symantec Endpoint Protection option.
For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Symantec SGS

The Symantec Gateway Security (SGS) Appliance DSM for SIEM accepts SGS events using syslog.

SIEM records all relevant events from SGS. Before you configure SIEM to integrate with an SGS, you must configure syslog within your SGS appliance. For more information on Symantec SGS, see your vendor documentation.

After you configure syslog to forward events to SIEM, the configuration is complete. Events forward from Symantec SGS to SIEM using syslog are automatically discovered. However, if you want to manually create a log source for Symantec SGS:

From the Log Source Type list, select the Symantec Gateway Security (SGS) Appliance option.

For more information on configuring devices, see the *SIEM Log Sources User Guide.*

Symantec System Center

The Symantec System Center (SSC) DSM for SIEM retrieves events from an SSC database using a custom view created for SIEM.

SIEM records all SSC events. You must configure the SSC database with a user that has read and write privileges for the custom SIEM view to be able to poll the view for information. Symantec System Center (SSC) only supports the JDBC protocol.

Configuring a database view for Symantec System Center

A database view is required by the JDBC protocol to poll for SSC events.

Procedure

1 In the Microsoft SQL Server database used by the SSC device, configure a custom default view to support SIEM:

```
The database name must not contain any spaces.
CREATE VIEW dbo.vw_SIEM AS SELECT
dbo.alerts.Idx AS idx,
dbo.inventory.IP_Address AS ip,
dbo.inventory.Computer AS computer_name,
dbo.virus.Virusname AS virus_name,
dbo.alerts.Filepath AS filepath,
dbo.alerts.NoOfViruses AS no_of_virus,
dbo.actualaction.Actualaction AS [action],
dbo.alerts.Alertdatetime AS [date],
dbo.clientuser.Clientuser AS user_name FROM
dbo.alerts INNER JOIN
```

```
dbo.virus ON dbo.alerts.Virusname_Idx = dbo.virus.Virusname_Idx
INNER JOIN
dbo.inventory ON dbo.alerts.Computer_Idx =
dbo.inventory.Computer_Idx INNER JOIN
dbo.actualaction ON dbo.alerts.Actualaction_Idx =
dbo.actualaction.Actualaction_Idx INNER JOIN
dbo.clientuser ON dbo.alerts.Clientuser_Idx =
dbo.clientuser.Clientuser_Idx
```

After you create your custom view, you must configure SIEM to receive event information using the JDBC protocol.

Configuring a Log Source

To configure SIEM to access the SSC database using the JDBC protocol.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 Using the Log Source Type list, select Symantec System Center.

7 Using the Protocol Configuration list, select JDBC.

8 Configure the following:

Table 197: Symantec System Center JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: `<SSC Database>@<SSC Database Server IP or Host Name>` Where: `<SSC Database>` is the database name, as entered in the Database Name parameter. `<SSC Database Server IP or Host Name>` is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.
Database Type	From the list, select MSDE.
Database Name	Type Reporting as the name of the Symantec System Center database.
IP or Hostname	Type the IP address or host name of the Symantec System Center SQL Server.

Table 197: Symantec System Center JDBC Parameters (Continued)

Parameter	Description
Port	Type the port number used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Symantec System Center database. The Symantec System Center database must have incoming TCP connections enabled to communicate with SIEM. **NOTE:** If you define a Database Instance when using MSDE as the database type, you must leave the Port parameter blank in your configuration.
Username	Type the username required to access the database.
Password	Type the password required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.
Authentication Domain	If you select MSDE as the Database Type and the database is configured for Windows, you must define a Windows Authentication Domain. Otherwise, leave this field blank.
Database Instance	Optional. Type the database instance, if you have multiple SQL server instances on your database server. **NOTE:** If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type vw_SIEM as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma separated list to define specific tables or views, if required for your configuration. The comma separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type idx as the compare field. The compare field is used to identify new events added between queries to the table.
Start Date and Time	Optional. Type the start date and time for database polling. The Start Date and Time parameter must be formatted as yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.

Table 197: Symantec System Center JDBC Parameters (Continued)

Parameter	Description
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	Clear the Use Named Pipe Communications check box. When using a Named Pipe connection, the username and password must be the appropriate Windows authentication username and password and not the database username and password. Also, you must use the default Named Pipe.
Database Cluster Name	If you select the Use Named Pipe Communication check box, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

NOTE

Selecting a value for the Credibility parameter greater than 5 will weight your Symantec System Center log source with a higher importance compared to other log sources in SIEM.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

Symantec Data Loss Prevention (DLP)

The Symantec Data Loss Protection (DLP) DSM for SIEM accepts events from a Symantec DLP appliance using syslog.

Before configuring SIEM, you must configure response rules on your Symantec DLP. The response rule allows the Symantec DLP appliance to forward syslog events to SIEM when a data loss policy violation occurs. Integrating Symantec DLP requires you to create two protocol response rules (SMTP and None of SMTP) for SIEM. These protocol response rules create an action to forward the event information, using syslog, when an incident is triggered.

To configure Symantec DLP with SIEM, you must:

1 Create an SMTP response rule.

2 Create a None of SMTP response rule.

3 Configure a log source in SIEM.

4 Map Symantec DLP events in SIEM.

Creating an SMTP Response Rule

To configure an SMTP response rule in Symantec DLP:

Procedure

1 Log in to your Symantec DLP user interface.

2 From the menu, select the **Manage > Policies > Response Rules**.

3 Click **Add Response Rule**.

4 Select one of the following response rule types:

- **Automated Response** - Automated response rules are triggered automatically as incidents occur. This is the default value.
- **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.

5 Click Next.

6 Configure the following values:
   a **Rule Name** - Type a name for the rule you are creating. This name should be descriptive enough for policy authors to identify the rule. For example, **`SIEM Syslog SMTP`**.
   b **Description** - Optional. Type a description for the rule you are creating.

7 Click **Add Condition**.

8 On the **Conditions** panel, select the following conditions:

- From the first list, select **Protocol or Endpoint Monitoring**.
- From the second list, select **Is Any Of**.
- From the third list, select **SMTP**.

9 On the **Actions** panel, click **Add Action**.

10 From the **Actions** list, select **All: Log to a Syslog Server**.

11 Configure the following options:
   a **Host** - Type the IP address of your SIEM.
   b **Port** - Type **514** as the syslog port.
   c **Message** -Type the following string to add a message for SMTP events.

```
LEEF:1.0|Symantec|DLP|2:medium|$POLICY$|suser=$SENDER$|duser=$R
ECIPIENTS$|rules=$RULES$|matchCount=$MATCH_COUNT$|blocked=$BLOC
KED$|incidentID=$INCIDENT_ID$|incidentSnapshot=$INCIDENT_SNAPSH
OT$|subject=$SUBJECT$|fileName=$FILE_NAME$|parentPath=$PARENT_P
ATH$|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$|
scan=$SCAN$|target=$TARGET$
```

   d **Level** - From this list, select **6 - Informational**.

12 Click **Save**.

You are now ready to configure your None Of SMTP response rule.

Creating a None of SMTP Response Rule

To configure a None Of SMTP response rule in Symantec DLP:

Procedure

1 From the menu, select the **Manage > Policies > Response Rules**.

2 Click **Add Response Rule**.

3 Select one of the following response rule types:

- **Automated Response** - Automated response rules are triggered automatically as incidents occur. This is the default value.
- **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.

4 Click Next.

5 Configure the following values:
   a **Rule Name** - Type a name for the rule you are creating. This name should be descriptive enough for policy authors to identify the rule. For example, **`SIEM`** `Syslog None Of SMTP`.
   b **Description** - Optional. Type a description for the rule you are creating.

6 Click **Add Condition**.

7 On the **Conditions** panel, select the following conditions:

- From the first list, select **Protocol or Endpoint Monitoring**.
- From the second list, select **Is Any Of**.
- From the third list, select **None Of SMTP**.

8 On the **Actions** panel, click **Add Action**.

9 From the **Actions** list, select **All: Log to a Syslog Server**.

10 Configure the following options:
   a **Host** - Type the IP address of your SIEM.
   b **Port** - Type **514** as the syslog port.
   c **Message** -Type the following string to add a message for None Of SMTP events.

```
LEEF:1.0|Symantec|DLP|2:medium|$POLICY$|src=$SENDER$|dst=$RECIP
IENTS$|rules=$RULES$|matchCount=$MATCH_COUNT$|blocked=$BLOCKED$
|incidentID=$INCIDENT_ID$|incidentSnapshot=$INCIDENT_SNAPSHOT$|
subject=$SUBJECT$|fileName=$FILE_NAME$|parentPath=$PARENT_PATH$
|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$|scan
=$SCAN$|target=$TARGET$
```

   d **Level** - From this list, select **6 - Informational**.

11 Click **Save**.

   You are now ready to configure SIEM.

Configuring a Log Source

You are now ready to configure the log source in SIEM.

SIEM automatically detects syslog events for the SMTP and None of SMTP response rules you created. However, if you want to manually configure SIEM to receive events from a Symantec DLP appliance:

From the Log Source Type list, select the Symantec DLP option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about Symantec DLP, see your vendor documentation.

Creating an Event Map for Symantec DLP Events

Event mapping is required for a number of Symantec DLP events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined SIEM Identifier (QID) map to categorize security events.

You can individually map each event for your device to an event category in SIEM. Mapping events allows SIEM to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for Symantec DLP are categorized as unknown. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

Discovering Unknown Events

As your device forwards events to SIEM, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we recommend you repeat this search until you are comfortable that you have identified the majority of your events.

Procedure

1 Log in to SIEM.

1 Click the **Log Activity** tab.

2 Click **Add Filter**.

3 From the first list, select **Log Source**.

4 From the **Log Source Group** list, select the log source group or **Other**.
Log sources that are not assigned to a group are categorized as Other.

5 From the **Log Source** list, select your Symantec DLP log source.

6 Click **Add Filter**.
The **Log Activity** tab is displayed with a filter for your log source.

7 From the **View** list, select **Last Hour**.
Any events generated by the Symantec DLP DSM in the last hour are displayed. Events displayed as unknown in the Event Name column or Low Level Category column require event mapping in SIEM.

NOTE

You can save your existing search filter by clicking **Save Criteria**.

You are now ready to modify the event map.

Modifying the Event Map

Modifying an event map allows you to manually categorize events to a SIEM Identifier (QID) map. Any event categorized to a log source can be remapped to a new SIEM Identifier (QID).

NOTE

Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1 On the Event Name column, double-click an unknown event for Symantec DLP.

The detailed event information is displayed.

2 Click **Map Event**.

3 From the Browse for QID pane, select any of the following search options to narrow the event categories for a SIEM Identifier (QID):

a From the **High-Level Category** list, select a high-level event categorization.

For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *SIEM Administration Guide*.

b From the **Low-Level Category** list, select a low-level event categorization.

c From the **Log Source Type** list, select a log source type.

The **Log Source Type** list allows you to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, Symantec provides policy and data loss prevention events, you might select another product that likely captures similar events.

d To search for a QID by name, type a name in the **QID/Name** field.

The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, policy.

4 Click **Search**.

A list of QIDs are displayed.

5 Select the QID you want to associate to your unknown event.

6 Click **OK**.

SIEM maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by SIEM.

If you update an event with a new SIEM Identifier (QID) map, past events stored in SIEM are not updated. Only new events are categorized with the new QID.

Symantec PGP Universal Server

The PGP Universal Server DSM for SIEM accepts syslog events from PGP Universal Servers.

Supported Event Types

SIEM accepts all relevant events from the following categories:

- Administration
- Software updates
- Clustering
- Backups
- Web Messenger
- Verified Directory
- Postfix
- Client logs
- Mail

Before you can integrate PGP Universal Server events with SIEM, you must enable and configure PGP Universal Server to forward syslog events to SIEM.

Configure Syslog for PGP Universal Server

To enable external logging to forward syslog events to SIEM:

Procedure

1 In a web browser, log in to your PGP server's administrative interface.
`https://<PGP Server IP address>:9000`

2 Click **Settings**.

3 Select the **Enable External Syslog** check box.

4 From the **Protocol** list, select the either **UDP** or **TCP**.
By default, SIEM uses port 514 to receive UDP syslog or TCP syslog event messages.

5 In the **Hostname** field, type the IP address of your SIEM Console or Event Collector.

6 In the **Port** field, type **514**.

7 Click **Save**.
The configuration is complete. The log source is added to SIEM as PGP Universal Server events are automatically discovered. Events forwarded to SIEM by the PGP Universal Servers are displayed on the **Log Activity** tab of SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events from PGP Universal Servers. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select PGP Universal Server.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 198: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your PGP Universal Server.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

108 Motorola Symbol AP

The Motorola Symbol AP DSM for SIEM records all relevant events forwarded from Motorola Symbol AP devices using syslog.

Configure a Log Source

To integrate Motorola SymbolAP with SIEM, you must manually create a log source to receive events.

SIEM does not automatically discover or create log sources for syslog events from Motorola SymbolAP appliances. In cases where the log source is not automatically discovered, we recommend you create a log source before forwarding events to SIEM.

To configure a log source:

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.
The Data Sources panel is displayed.

4 Click the Log Sources icon.
The Log Sources window is displayed.

5 Click Add.
The Add a log source window is displayed.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Motorola SymbolAP.

9 Using the Protocol Configuration list, select **Syslog**.
The syslog protocol configuration is displayed.

10 Configure the following values:

Table 199: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Motorola SymbolAP appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.
The log source is added to SIEM.

Configure Syslog Events for Motorola Symbol AP

To configure the device to forward syslog events to SIEM:

1 Log in to your Symbol AP device user interface.

2 From the menu, select **System Configuration > Logging Configuration**.

The Access Point window is displayed.

3 Using the Logging Level list, select the desired log level for tracking system events. The options are:

0 - Emergency

1- Alert

2 - Critical

3 - Errors

4 - Warning

5 - Notice

6 - Info. This is the default.

7 - Debug

4 Select the Enable logging to an external syslog server check box.

5 In the **Syslog Server IP Address** field, type the IP address of an external syslog server, such as SIEM.

This is required to route the syslog events to SIEM.

6 Click Apply.

7 Click Logout.

A confirmation window is displayed.

8 Click OK to exit the application.

The configuration is complete. Events forwarded to SIEM are displayed on the **Log Activity** tab.

109 Symantec Critical System Protection

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

110 Symark

Symark PowerBroker logs all events to a multi-line format in a single event log file, which is viewed using Symark's pblog utility.

PowerBroker pblogs must be re-formatted using a script and forwarded to SIEM. This configuration requires you download and configure a script for your Symark PowerBroker appliance before you can forward events to SIEM.

Configure Symark PowerBroker

To configure a Symark PowerBroker device to forward syslog to SIEM:

1 On the IBM support website, download the following file:
`pbforwarder.pl.gz`
The script can be downloaded from the following website:
http://support.extremenetworks.com

2 Copy the file to the device that hosts Symark PowerBroker.

NOTE

Perl 5.8 must be installed on the device that hosts Symark PowerBroker.

3 Type the following command to extract the file:
`gzip -d pbforwarder.pl.gz`

4 Type the following command to set the script file permissions:
`chmod +x pbforwarder.pl`

5 Using SSH, log in to the device that hosts Symark PowerBroker.
The credentials used to log in must have read, write, and execute permissions for the log file.

6 Type the appropriate parameters:

Table 200: Command Parameters

Parameters	Description
-h	The -h parameter defines the syslog host receiving the events from Symark PowerBroker. This is the IP address of your SIEM or Event Collector.
-t	The -t parameter defines that the command-line is used to tail the log file and monitor for new output from the listener. For PowerBroker this must be specified as `"pblog -l -t"`.
-p	The -p parameter defines the TCP port to be used when forwarding events. If nothing is specified, the default is port `514`.

Table 200: Command Parameters (Continued)

Parameters	Description
-H	The -H parameter defines the hostname or IP address for the syslog header of all sent events. It is recommended that this be the IP address of the Symark PowerBroker.
-r	The -r parameter defines the directory name where you want to create the process ID (.pid) file. The default is /var/run. This parameter is ignored if -D is specified.
-l	The -l parameter defines the directory name where you want to create the lock file. The default is /var/lock. This parameter is ignored if -D is specified.
-D	The -D parameter defines that the script should run in the foreground. The default setting is to run as a daemon and log all internal messages to the local syslog service.
-f	The -f parameter defines the syslog facility and (optionally) the severity for messages sent to the Event Collector. If no value is specified, `user.info` is used.
-a	The -a parameter enables an AIX compatible ps method. This command is only required when using Symark PowerBroker on AIX systems.
-d	The -d parameter enables debug logging.
-v	The -v parameter displays the script version information.

7 Type the following command to start the pbforwarder.pl script.

```
pbforwarder.pl -h <IP address> -t "pblog -l -t"
```

Where `<IP address>` is the IP address of your SIEM or Event Collector.

8 Type the following command to stop the pbforwarder.pl script:

```
kill -QUIT `cat /var/run/pbforwarder.pl.pid`
```

9 Type the following command to reconnect the pbforwarder.pl script:

```
kill -HUP `cat /var/run/pbforwarder.pl.pid`
```

SIEM automatically detects and creates a log source from the syslog events forwarded from a Symark PowerBroker.

Configure a Log Source

SIEM automatically discovers and identifies most incoming syslog events from external sources. The following configuration steps are optional.

To create a log source:

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.
The Data Sources panel is displayed.

3 Click the Log Sources icon.
The Log Sources window is displayed.

4 In the **Log Source Name** field, type a name for your Symark PowerBroker log source.

5 In the **Log Source Description** field, type a description for the log source.

6 From the Log Source Type list, select Symark PowerBroker.

7 From the Protocol Configuration list, select Syslog.
The syslog protocol parameters are displayed.

8 Configure the following values:

Table 201: Adding a Syslog Log Source

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your Symark PowerBroker appliance.
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** list in the **System Settings** window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on Settings, see the *SIEM Administration Guide*.

Table 201: Adding a Syslog Log Source (Continued)

Parameter	Description
Store Event Payload	Select this check box to enable or disable SIEM from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list in the **System Settings** window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on Settings, see the *SIEM Administration Guide*.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

The configuration is complete.

111 ThreatGRID Malware Threat Intelligence Platform

The ThreatGRID Malware Threat Intelligence Platform DSM for SIEM collects malware events by using the log file protocol or syslog.

Supported Versions of ThreatGRID Malware Threat Intelligence

SIEM supports ThreatGRID Malware Threat Intelligence Platform appliances with v2.0 software that use the SIEM Log Enhanced Event Format (LEEF) Creation script.

Supported Event Collection Protocols for ThreatGRID Malware Threat Intelligence

ThreatGRID Malware Threat Intelligence Platform writes malware events that are readable by SIEM.

The LEEF creation script is configured on the ThreatGRID appliance and queries the ThreatGRID API to write LEEF events that are readable by SIEM. The event collection protocol your log source uses to collect malware events is based on the script you install on your ThreatGRID appliance.

Two script options are available for collecting LEEF formatted events:

- **Syslog** - The syslog version of the LEEF creation script allows your ThreatGRID appliance to forward events directly to SIEM. Events that are forwarded by the syslog script are automatically discovered by SIEM.
- **Log File** - The Log File protocol version of the LEEF creation script allows the ThreatGRID appliance to write malware events to a file. SIEM uses the Log File protocol to communicate with the event log host to retrieve and parse malware events.

The LEEF creation script is available from ThreatGRID customer support. For more information, see the ThreatGRID website (www.threatgrid.com) or email ThreatGRID support at *support@threatgrid.com*.

ThreatGRID Malware Threat Intelligence Configuration Overview

To integrate ThreatGRID Malware Threat Intelligence events with SIEM, you must complete the following tasks:

1 Download the SIEM Log Enhanced Event Format Creation script for your collection type from the ThreatGRID support website to your appliance.

2 On your ThreatGRID appliance, install and configure the script to poll the ThreatGRID API for events.

3 On your SIEM appliance, configure a log source to collect events based on the script you installed on your ThreatGRID appliance.

4 Ensure that no firewall rules block communication between your ThreatGRID installation and the SIEM Console or managed host that is responsible for retrieving events.

Configuring a ThreatGRID Syslog Log Source

SIEM automatically discovers and creates a log source for malware events that are forwarded from the ThreatGRID Malware Threat Intelligence Platform. This procedure is optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select ThreatGRID Malware Intelligence Platform.

9 From the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 202: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ThreatGRID Malware Intelligence Platform. The log source identifier must be unique for the log source type.
Enabled	Select this check box to enable the log source. By default, the check box is selected.

Table 202: Syslog protocol parameters (Continued)

Parameter	Description
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

Malware events that are forwarded to SIEMce are displayed on the **Log Activity** tab of SIEM.

Configuring a ThreatGRID Log File Protocol Log Source

To use the log file protocol to collect events, you must configure a log source in SIEM to poll for the event log that contains your malware events.

Procedure

1 Click the Admin tab.

2 On the navigation menu, click Data Sources.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for the log source.

6 In the **Log Source Description** field, type a description for the log source.

7 From the Log Source Type list, select **ThreatGRID Malware Threat Intelligence Platform**.

8 From the **Protocol Configuration** list, select **Log File**.

9 Configure the following values:

Table 203: Log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use to retrieve log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy Protocol The SCP and SFTP service type requires that the host server in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the ThreatGRID server that contains your event log files.
Remote Port	Type the port number for the protocol that is selected to retrieve the event logs from your ThreatGRID server. The valid range is 1 - 65535. The list of default service type port numbers: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22
Remote User	Type the user name that is required to log in to the ThreatGRID web server that contains your audit event logs. The user name can be up to 255 characters in length.
Remote Password	Type the password to log in to your ThreatGRID server.
Confirm Password	Confirm the password to log in to your ThreatGRID server
SSH Key File	If you select SCP or SFTP as the **Service Type**, use this parameter to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **NOTE:** For FTP only. If your log files are in the remote user's home directory, you can leave the remote directory blank. Blank values in the **Remote Directory** field support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The **Recursive** parameter is ignored if you configure SCP as the **Service Type**.

Table 203: Log file protocol parameters (Continued)

Parameter	Description
FTP File Pattern	Type the regular expression (regex) required to filter the list of files that are specified in the Remote Directory. All files that match the regular expression are retrieved and processed. The FTP file pattern must match the name that you assigned to your ThreatGRID event log. For example, to collect files that start with leef or LEEF and ends with a text file extension, type the following value: `(leef|LEEF)+.*\.txt` Use of this parameter requires knowledge of regular expressions (regex). This parameter applies to log sources that are configured to use FTP or SFTP.
FTP Transfer Mode	If you select **FTP** as the **Service Type**, from the list, select ASCII. ASCII is required for text-based event logs.
SCP Remote File	If you select **SCP** as the **Service Type**, type the file name of the remote file.
Start Time	Type a time value to represent the time of day you want the log file protocol to start. The start time is based on a 24 hour clock and uses the following format: HH:MM. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the **Recurrence** field value to establish when your ThreatGRID server is polled for new event log files.
Recurrence	Type the frequency that you want to scan the remote directory on your ThreatGRID server for new event log files. Type this value in hours (H), minutes (M), or days (D). For example, type 2H to scan the remote directory every 2 hours from the start time. The default recurrence value is 1H. The minimum time interval is 15M.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the save action completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the **Ignore Previously Processed File** parameter.
EPS Throttle	Type the number of events per second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.
Processor	From the list, select **NONE**. Processors allow event file archives to be expanded and processed for their events. Files are processed after they are downloaded. SIEM can process files in *zip*, *gzip*, *tar*, or *tar+gzip* archive format.

Table 203: Log file protocol parameters (Continued)

Parameter	Description
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed. SIEM examines the log files in the remote directory to determine whether the event log was processed by the log source. If a previously processed file is detected, the log source does not download the file. Only new or unprocessed event log files are downloaded by SIEM. This option applies to **FTP** and **SFTP** service types.
Change Local Directory?	Select this check box to define a local directory on your SIEM appliance to store event log files during processing. In most scenarios, you can leave this check box not selected. When this check box is selected, the **Local Directory** field is displayed. You can configure a local directory to temporarily store event log files. After the event log is processed, the events added to SIEM and event logs in the local directory are deleted.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies extra processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.

Malware events that are retrieved by the log source are displayed on the **Log Activity** tab of SIEM.

112 Tipping Point

This section provides information on the following DSMs:

Tipping Point Intrusion Prevention System

The Tipping Point Intrusion Prevention System (IPS) DSM for SIEM accepts Tipping Point events using syslog.

SIEM records all relevant events from either a Local Security Management (LMS) device or multiple devices with a Security Management System (SMS).

Before you configure SIEM to integrate with Tipping Point, you must configure your device based on type:

- If you are using an SMS, see Configure Remote Syslog for SMS on page 613.
- If you are using an LSM, see Configure Notification Contacts for LSM on page 614.

Configure Remote Syslog for SMS

To configure Tipping Point for SMS, you must enable and configure your appliance to forward events to a remote host using syslog.

To configure your Tipping Point SMS:

1 Log in to the Tipping Point system.

2 On the Admin Navigation menu, select Server Properties.

3 Select the Management tab.

4 Click Add.

The Edit Syslog Notification window is displayed.

5 Select the Enable check box.

6 Configure the following values:

a Syslog Server - Type the IP address of the SIEM to receive syslog event messages.

b Port - Type 514 as the port address.

c Log Type - Select SMS 2.0 / 2.1 Syslog format from the list.

d Facility - Select Log Audit from the list.

e Severity - Select Severity in Event from the list.

f Delimiter - Select TAB as the delimiter for the generated logs.

g Include Timestamp in Header - Select Use original event timestamp.

7 Select the Include SMS Hostname in Header check box.

8 Click OK.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Tipping Point device:

From the Log Source Type list, select the Tipping Point Intrusion Prevention System (IPS) option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Tipping Point device, see your vendor documentation.

Configure Notification Contacts for LSM

To configure LSM notification contacts:

1 Log in to the Tipping Point system.

2 From the LSM menu, select **IPS > Action Sets**.
The IPS Profile - Action Sets window is displayed.

3 Click the Notification Contacts tab.

4 In the Contacts List, click Remote System Log.
The Edit Notification Contact page is displayed.

5 Configure the following values:
   a Syslog Server - Type the IP address of the SIEM to receive syslog event messages.
   b Port - Type 514 as the port address.
   c Alert Facility - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   d **Block Facility** - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   e Delimiter - Select TAB from the list.

6 Click Add to table below.

7 Configure a Remote system log aggregation period in minutes.

NOTE

If your SIEM resides in a different subnet than your Tipping Point device, you might have to add static routes. For more information, see your vendor documentation.

8 Click Save.
You are now ready to configure the action set for your LSM, see Configuring an Action Set for LSM on page 614.

Configuring an Action Set for LSM

To configure an action set for your LSM:

1 Log in to the Tipping Point system.

2 From the LSM menu, select I**PS > Act**ion Sets.
The IPS Profile - Action Sets window is displayed.

3 Click **Create Action Set**.
The Create/Edit Action Set window is displayed.

4 Type the Action Set Name.

5 For Actions, select a flow control action setting:

- Permit - Allows traffic.
- Rate Limit - Limits the speed of traffic. If you select Rate Limit, you must also select the desired rate.
- Block - Does not permit traffic.
- TCP Reset - When used with the Block action, resets the source, destination, or both IP addresses of an attack. This option resets blocked TCP flows.
- Quarantine - When used with the Block action, blocks an IP address (source or destination) that triggers the filter.

6 Select the Remote System Log check box for each action you have selected.

7 Click Create.

8 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Tipping Point device.

From the Log Source Type list, select the Tipping Point Intrusion Prevention System (IPS) option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Tipping Point device, see your vendor documentation.

Tipping Point X505/X506 Device

The Tipping Point X505/X506 DSM for SIEM accepts events using syslog.

Supported Event Types

SIEM records all relevant system, audit, VPN, and firewall session events.

Configure Syslog

To configure your device to forward events to SIEM:

1 Log in to the Tipping Point X505/X506 device.

2 From the LSM menu, select **System > Configuration > Syslog Servers**.
The Syslog Servers window is displayed.

3 For each log type you want to forward, select a check box and type the IP address of your SIEM.

NOTE

If your SIEM resides in a different subnet than your Tipping Point device, you might have to add static routes. For more information, see your vendor documentation.

4 You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Tipping Point X505/X506 device:

u From the **Log Source Type** list, select the **Tipping Point X Series Appliances** option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

NOTE

If you have a previously configured Tipping Point X505/X506 DSM installed and configured on your SIEM, the Tipping Point X Series Appliances option is still displayed in the Log Source Type list. However, any new Tipping Point X505/X506 DSM you configure, you must select the Tipping Point Intrusion Prevention System (IPS) option.

113 Top Layer IPS

The Top Layer IPS DSM for SIEM accepts Top Layer IPS events using syslog.

SIEM records and processes Top Layer events. Before you configure SIEM to integrate with a Top Layer device, you must configure syslog within your Top Layer IPS device. For more information on configuring Top Layer, see your Top Layer documentation.

The configuration is complete. The log source is added to SIEM as Top Layer IPS events are automatically discovered. Events forwarded to SIEM by Top Layer IPS are displayed on the **Log Activity** tab of SIEM.

To configure SIEM to receive events from a Top Layer IPS device:

From the Log Source Type list, select the Top Layer Intrusion Prevention System (IPS) option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Top Layer device, see your vendor documentation.

114 Trend Micro

This section provides information on the following DSMs:

Trend Micro InterScan VirusWall

The Trend Micro InterScan VirusWall DSM for SIEM accepts events using syslog.

You can integrate InterScan VirusWall logs with SIEM using the Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *SIEM Adaptive Log Exporter Users Guide*.

After you configure the Adaptive Log Exporter, the configuration is complete. The log source is added to SIEM as Trend Micro InterScan VirusWall events are automatically discovered. Events forwarded to SIEM by Trend Micro InterScan VirusWall are displayed on the **Log Activity** tab of SIEM.

To manually configure SIEM to receive events from an InterScan VirusWall device:

From the Log Source Type list, select the Trend InterScan VirusWall option.

For more information on configuring devices, see the *SIEM Log Sources User Guide*. For more information about your Trend Micro InterScan VirusWall device, see your vendor documentation.

Trend Micro Control Manager

You can integrate a Trend Micro Control Manager device with SIEM.

A Trend Micro Control Manager accepts events using SNMPv1 or SNMPv2. Before you configure SIEM to integrate with a Trend Micro Control Manager device, you must configure a log source, then configure SNMP trap settings for your Trend Micro Control Manager.

Configure a Log Source

SIEM does not automatically discover SNMP events from Trend Micro Control Manager.

You must configure an SNMP log source for your Trend Micro Control Manager to use the SNMPv1 or SNMPv2 protocol. SNMPv3 is not supported by Trend Micro Control Manager.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Trend Micro Control Manager.

9 Using the Protocol Configuration list, select **SNMPv2**.
SNMPv3 is not supported by Trend Micro Control Manager.

10 Configure the following values:

Table 204: SNMPv2 protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Trend Micro Control Manager appliance.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Clear the **Include OIDs in Event Payload** check box, if selected. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Configure SNMP Traps

To configure SNMP traps for Trend Micro Control Manager:

NOTE

Trend Micro Control Manager v5.5 requires hotfix 1697 or hotfix 1713 after Service Pack 1 Patch 1 to provide correctly formatted SNMPv2c events. For more information, see your vendor documentation.

Procedure

1 Log in to the Trend Micro Control Manager device.

2 Select **Administration > Settings > Event Center Settings**.

3 Set the SNMP trap notifications:
   a In the **SNMP Trap Settings** field, type the Community Name.
   b Type the SIEM server IP address.

4 Click Save.
   You are now ready to configure events in the Event Center.

1 Select **Administration > Event Center**.

2 From the Event Category list, expand Alert.

3 Click Recipients for an alert.

4 In Notification methods, select the SNMP Trap Notification check box.

5 Click Save.
   The Edit Recipients Result window is displayed.

6 Click OK.

7 Repeat Step 2 to Step 6 for every alert that requires an SNMP Trap Notification.
   The configuration is complete. Events from Trend Micro Control Manager are displayed on the **Log Activity** tab of SIEM. For more information on Trend Micro Control Manager, see your vendor documentation.

Trend Micro Office Scan

A Trend Micro Office Scan DSM for SIEM accepts events using SNMPv2.

SIEM records events relevant to virus and spyware events. Before configuring a Trend Micro device in SIEM, you must configure your device to forward SNMPv2 events.

SIEM has two options for integrating with a Trend Micro device depending on your device version:

- Integrating with Trend Micro Office Scan 8.x on page 621
- Integrating with Trend Micro Office Scan 10.x on page 622

Integrating with Trend Micro Office Scan 8.x

To integrate a Trend Micro Office Scan 8.x device with SIEM:

Procedure

1 Log in to the Office Scan Administration interface.

2 Select Notifications.

3 Configure the General Settings for SNMP Traps:
   a In the **Server IP Address** field, type the IP address of the SIEM.

NOTE

Do not change the community trap information.

   b Click Save.

4 Configure the Standard Alert Notification:
   a Select Standard Notifications.
   b Click the SNMP Trap tab.
   c Select the Enable notification via SNMP Trap for Virus/Malware Detections check box.
   d Type the following message in the field (this should be the default):

```
Virus/Malware: %v
Computer: %s
Domain: %m
File: %p
Date/Time: %y
Result: %a
```

   e Select the Enable notification via SNMP Trap for Spyware/Grayware Detections check box.
   f Type the following message in the field (this should be the default):

```
Spyware/Grayware: %v
Computer: %s
Domain: %m
Date/Time: %y
Result: %a
```

5 Click Save.

6 Configure Outbreak Alert Notifications:
   a Select Out Notifications.
   b Click the SNMP Trap tab.
   c Select the Enable notification via SNMP Trap for Virus/Malware Outbreaks check box.
   d Type the following message in the field (this should be the default):

```
Number of viruses/malware: %CV
Number of computers: %CC
Log Type Exceeded: %A
Number of firewall violation logs: %C
Number of shared folder sessions: %S
Time Period: %T
```

   e Select the Enable notification via SNMP Trap for Spyware/Grayware Outbreaks check box.
   f Type the following message in the field (this should be the default):

```
Number of spyware/grayware: %CV
Number of computers: %CC
Log Type Exceeded: %A
Number of firewall violation logs: %C
Number of shared folder sessions: %S
Time Period: %T
```

   g Click Save.

7 You are now ready to configure the log sources in SIEM.

To configure the Trend Micro Office Scan device:

1 From the Log Source Type list, select the Trend Micro Office Scan option.

2 From the Protocol Configuration list, select the SNMPv2 option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Integrating with Trend Micro Office Scan 10.x

Before you configure SIEM to integrate with a Trend Micro Office Scan 10.x device, you must:

1 Configure the SNMP settings for Trend Micro Office Scan 10.x.

2 Configure standard notifications.

3 Configure outbreak criteria and alert notifications.

Configure General Settings

To integrate a Trend Micro Office Scan 10.x device with SIEM:

1 Log in to the Office Scan Administration interface.

2 Select **Notifications > Administrator Notifications > General Settings**.

3 Configure the General Settings for SNMP Traps:
   a In the **Server IP Address** field, type the IP address of your SIEM.
   b Type a community name for your Trend Micro Office Scan device.
   c Click Save.

   You must now configure the Standard Notifications for Office Scan.

Configure Standard Notifications

To configure standard notifications:

1 Select **Notifications > Administrator Notifications > Standard Notifications**.

2 Define the Criteria settings.
   a Click the Criteria tab.
   b Select the option to alert administrators on the detection of virus/malware and spyware/grayware, or when the action on these security risks is unsuccessful.

3 To enable notifications:
   a Configure the SNMP Trap tab.
   b Select the Enable notification via SNMP Trap check box.
   c Type the following message in the field:

```
Virus/Malware: %v
Spyware/Grayware: %T
Computer: %s
IP address: %i
Domain: %m
File: %p
Date/Time: %y
Result: %a
User name: %n
```

4 Click Save.

   You must now configure Outbreak Notifications.

Configure Outbreak Criteria and Alert Notifications

To configure outbreak criteria and alert notifications:

1 Select **Notifications > Administrator Notifications > Outbreak Notifications**.

2 Click the Criteria tab.

3 Type the number of detections and detection period for each security risk.

Notification messages are sent to an administrator when the criteria exceeds the specified detection limit.

NOTE

Trend Micro recommends using the default values for the detection number and detection period.

4 Select Shared Folder Session Link and enable Office Scan to monitor for firewall violations and shared folder sessions.

NOTE

To view computers on the network with shared folders or computers currently browsing shared folders you can select the number link in the interface.

5 Click the SNMP Trap tab.

a Select the Enable notification via SNMP Trap check box.

b Type the following message in the field:

```
Number of viruses/malware: %CV
Number of computers: %CC
Log Type Exceeded: %A
Number of firewall violation logs: %C
Number of shared folder sessions: %S
Time Period: %T
```

6 Click Save.

7 You are now ready to configure the log source in SIEM.

To configure the Trend Micro Office Scan device:

1 From the Log Source Type list, select the Trend Micro Office Scan option.

2 From the Protocol Configuration list, select the SNMPv2 option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

Trend Micro Deep Discovery

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

115 Tripwire

The Tripwire DSM for SIEM accepts resource additions, removal, and modification events using syslog.

Procedure

1 Log in to the Tripwire interface.

2 On the left-hand navigation, click Actions.

3 Click New Action.

4 Configure the new action.

5 Select Rules and click on the desired rule you wish to monitor.

6 Select the Actions tab.

7 Make sure the new action is selected.

8 Click OK.

9 Repeat step 5 to step 8 for each rule you want to monitor.

You are now ready to configure the log source in SIEM.

To configure SIEM to receive events from a Tripwire device:

From the Log Source Type list, select the Tripwire Enterprise option.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*. For more information about your Tripwire device, see your vendor documentation.

116 Tropos Control

The Tropos Control DSM for SIEM accepts events using syslog.

SIEM is capable of recording all fault management, login and logout events, provisioning events, and device image upload events. Before configuring SIEM, you must configure your Tropos Control to forward syslog events.

You can configure Tropos Control to forward logs using syslog to SIEM.

Procedure

1 Using SSH, log in to your Tropos Control device as a root user.

2 Open the following file for editing:

`/opt/ControlServer/ems/conf/logging.properties`

3 To enable syslog, remove the comment marker (#) from the following line:

```
#log4j.category.syslog = INFO, syslog
```

4 To configure the IP address for the syslog destination, edit the following line:

```
log4j.appender.syslog.SyslogHost = <IP address>
```

Where `<IP address>` is the IP address or hostname of SIEM.

By default, Tropos Control uses a facility of USER and a default log level of INFO. These default settings are correct for syslog event collection from a Tropos Control device.

5 Save and exit the file.

You are now ready to configure the Tropos Control DSM in SIEM.

To configure SIEM to receive events from Tropos Control:

From the Log Source Type list, select **Tropos Control**.

For more information on configuring log sources, see the *SIEM Log Sources User Guide*.

117 Trusteer Apex Local Event Aggregator

SIEM can collect and categorize malware, exploit, and data exfiltration detection events from Trusteer Apex Local Event Aggregator.

Configuration Overview

To collect syslog events, you must configure your Trusteer Apex Local Event Aggregator to forward syslog events to SIEM. Administrators can use the Apex L.E.A. management console interface to configure a syslog target for events. SIEM automatically discovers and creates log sources for syslog events that are forwarded from Trusteer Apex Local Event Aggregator appliances. SIEM supports syslog events from Trusteer Apex Local Event Aggregator V1304.x and later.

To integrate events with SIEM, administrators can complete the following tasks:

1 On your Trusteer Apex Local Event Aggregator appliance, configure syslog server.

2 On your SIEM system, verify that the forwarded events are automatically discovered.

Configuring Syslog for Trusteer Apex Local Event Aggregator

To collect events, you must configure a syslog server on your Trusteer Apex Local Event Aggregator to forward syslog events.

Procedure

1 Log in to the Trusteer Apex L.E.A. management console.

2 From the navigation menu, select **Configuration**.

3 To export the current Trusteer Apex Local Event Aggregator configuration, click **Export** and save the file.

4 Open the configuration file with a text editor.

5 From the `syslog.event_targets` section, add the following information:

```
{
  "host": "<SIEM IP address>",
  "port": "514",
  "proto": "tcp"
}
```

6 Save the configuration file.

7 From the navigation menu, select **Configuration**.

8 Click **Choose file** and select the new configuration file that contains the event target IP address.

9 Click **Import**.

Result

As syslog events are generated by the Trusteer Apex Local Event Aggregator, they are forwarded to the target specified in the configuration file. The log source is automatically discovered after enough events are forwarded to SIEM. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the SIEM Console and verify that the log source is created. The **Log Activity** tab displays events from Trusteer Apex Local Event Aggregator.

118 Universal DSM

SIEM can collect and correlates events from any network infrastructure or security device using the Universal DSM.

After the events are collected and before the correlation can begin. The individual events from your devices must be properly parsed to determine the event name, IP addresses, protocol, and ports. For common network devices, such as Cisco Firewalls, predefined DSMs have been engineered for SIEM to properly parse and classify the event messages from the respective devices. After the events from a device have been parsed by the DSM, SIEM can continue to correlate events into offenses.

If an enterprise network has one or more network or security devices that are not officially supported, where no specific DSM for the device exists, you can use the Universal DSM. The Universal DSM allows you to forward events and messages from unsupported devices and use the Universal DSM to categorize the events for SIEM. SIEM can integrate with virtually any device or any common protocol source using the Universal DSM. For more information on the available protocols for retrieving events or logs from devices, see the *SIEM Log Sources User Guide*.

To configure the Universal DSM, you must use device extensions to associate a Universal DSM to devices. Before you define device extension information using the log sources window in the **Admin** tab, you must create an extensions document for the log source.

119 Universal LEEF

The Universal LEEF DSM for SIEM can accept events from devices that produce events using the Log Event Extended Format (LEEF).

The LEEF event format is a proprietary event format, which allows hardware manufacturers and software product manufacturers to read and map device events specifically designed for SIEM integration.

LEEF formatted events sent to SIEM outside of the partnership program require you to have installed the Universal LEEF DSM and manually identify each event forwarded to SIEM by mapping unknown events. The Universal LEEF DSM can parse events forwarded from syslog or files containing events in the LEEF format polled from a device or directory using the Log File protocol.

To configure events in SIEM using Universal LEEF, you must:

1 Configure a Universal LEEF log source in SIEM.

2 Send LEEF formatted events from your device to SIEM. For more information on forwarding events, see your vendor documentation.

3 Map unknown events to SIEM Identifiers (QIDs).

Configuring a Universal LEEF Log Source

Before you configure your device to send events to SIEM, you must add a log source for the device providing LEEF events.

SIEM can receive events from a real-time source using syslog or files stored on a device or in a repository using the Log File protocol.

Configuring Syslog to Collect Universal LEEF Events

To configure a log source for Universal LEEF using syslog:

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Universal LEEF.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 205: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for Universal LEEF events.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to forward LEEF events to SIEM.

Configuring the Log File Protocol to Collect Universal LEEF Events

The Log File protocol allows SIEM to retrieve archived event or log files from a remote host or file repository.

The files are transferred, one at a time, to SIEM for processing. SIEM reads the event files and updates the log source with new events. Due to the Log File protocol polling for archive files, the events are not provided in real-time, but added in bulk. The log file protocol can manage plain text, compressed files, or archives.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 On the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 In the **Log Source Name** field, type a name for the Universal LEEF log source.

6 In the **Log Source Description** field, type a description for the Universal LEEF log source.

7 From the Log Source Type list, select Universal LEEF.

8 Using the Protocol Configuration list, select Log File.

9 Configure the following parameters:

Table 206: Log file protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for your Universal LEEF log source. This value must match the value configured in the **Remote Host IP or Hostname** parameter. The log source identifier must be unique for the log source type.

Table 206: Log file protocol parameters (Continued)

Parameter	Description
Service Type	From the list, select the protocol you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy **NOTE:** The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or hostname of the host from which you want to receive files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 to 65535.
Remote User	Type the username necessary to log in to the host running the selected Service Type. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host containing the LEEF event files.
Confirm Password	Confirm the Remote Password to log in to the host containing the LEEF event files.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the Remote Password option is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved. **NOTE:** For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is clear. The Recursive parameter is not used if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. For example, if you want to list all files starting with the word log, followed by one or more digits and ending with `tar.gz`, use the following entry: `log[0-9]+\.tar\.gz`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

Table 206: Log file protocol parameters (Continued)

Parameter	Description
FTP Transfer Mode	This option is only displayed if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list, select the transfer mode you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** as the Processor and **LINEBYLINE** as the Event Generator when using ASCII as the FTP Transfer Mode.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed that you do not want to be processed a second time. This only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your SIEM system that you want to use for storing downloaded files during processing. We recommend that you leave this check box clear. When the check box is selected, the Local Directory field is displayed, allowing you to configure the local directory to use for storing files.

Table 206: Log file protocol parameters (Continued)

Parameter	Description
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. The LineByLine option reads each line of the file as single event. For example, if a file has 10 lines of text, 10 separate events are created.

10 Click Save.

11 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. You are now ready to write LEEF events that can be retrieved using the Log File protocol.

Forwarding Events to SIEM

After you have created your log source, you are ready to forward or retrieve events for SIEM. Forwarding events using syslog might require additional configuration from your network device.

As events are discovered by SIEM, either using syslog or polling for log files, events are displayed in the **Log Activity** tab. The events for your device forwarding LEEF events are identified by the name you typed in the **Log Source Name** field. The events for your log source are not categorized by default in SIEM and require categorization. For more information on categorizing your Universal LEEF events, see Creating a Universal LEEF Event Map on page 634.

Creating a Universal LEEF Event Map

Event mapping is required for the Universal LEEF DSM, as Universal LEEF events do not contain a predefined SIEM Identifier (QID) map to categorize security events.

Members of the SIPP partner program have QID maps designed for their network devices, the configuration documented, and the QID maps tested by IBM Corp.

The Universal LEEF DSM requires that you individually map each event for your device to an event category in SIEM. Mapping events allows SIEM to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for the Universal LEEF DSM are categorized as unknown. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

Discovering Unknown Events

As your device forwards events to SIEM, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we recommend you repeat this search until you are comfortable that you have identified the majority of your Universal LEEF events.

Procedure

1 Log in to SIEM.

1 Click the **Log Activity** tab.

2 Click **Add Filter**.

3 From the first list, select **Log Source**.

4 From the **Log Source Group** list, select the log source group or **Other**.

Log sources that are not assigned to a group are categorized as Other.

5 From the **Log Source** list, select your Universal LEEF log source.

6 Click **Add Filter**.

The **Log Activity** tab is displayed with a filter for your Universal LEEF DSM.

7 From the **View** list, select **Last Hour**.

Any events generated by your Universal LEEF DSM in the last hour are displayed. Events displayed as unknown in the Event Name column or Low Level Category column require event mapping in SIEM.

NOTE

You can save your existing search filter by clicking **Save Criteria**.

You are now ready to modify the event map for your Universal LEEF DSM.

Modifying an Event Map

Modifying an event map allows you to manually categorize events to a SIEM Identifier (QID) map. Any event categorized to a log source can be remapped to a new SIEM Identifier (QID). By default, the Universal LEEF DSM categorizes all events as unknown.

NOTE

Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1 On the Event Name column, double-click an unknown event for your Universal LEEF DSM.

The detailed event information is displayed.

2 Click **Map Event**.

3 From the Browse for QID pane, select any of the following search options to narrow the event categories for a SIEM Identifier (QID):

a From the **High-Level Category** list, select a high-level event categorization.

For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *SIEM Administration Guide*.

b From the **Low-Level Category** list, select a low-level event categorization.

c From the **Log Source Type** list, select a log source type.

The **Log Source Type** list allows you to search for QIDs from other individual log sources. Searching for QIDs by log source is useful when the events from your Universal LEEF DSM are similar to another existing network device. For example, if your Universal DSM provides firewall events, you might select Cisco ASA, as another firewall product that likely captures similar events.

d To search for a QID by name, type a name in the **QID/Name** field.

The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, MySQL.

4 Click **Search**.

A list of QIDs are displayed.

5 Select the QID you want to associate to your unknown Universal LEEF DSM event.

6 Click **OK**.

SIEM maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by SIEM.

NOTE

If you update an event with a new SIEM Identifier (QID) map, past events stored in SIEM are not updated. Only new events are categorized with the new QID.

120 Venustech Venusense

The Venustech Venusense DSM for SIEM can collect events from Venusense appliances using syslog.

Supported Venusense Events and Appliances

SIEM records all relevant unified threat, firewall, or network intrusion prevention events forwarded using syslog on port 514.

The following Venustech appliances are supported by SIEM:

- Venustech Venusense Security Platform
- Venusense Unified Threat Management (UTM)
- Venusense Firewall
- Venusense Network Intrusion Prevention System (NIPS)

Venusense Configuration Overview

SIEM can collect events from Venustech appliances that are configured to forward filtered event logs in syslog format to SIEM.

The following process outlines the steps required to collect events from a Venustech Venusense appliance:

1 Configure the syslog server on your Venusense appliance.

2 Configure a log filter on your Venusense appliance to forward specific event logs.

3 Configure a log source in SIEM to correspond to the filtered log events.

Configuring a Venusense Syslog Server

To forward events to SIEM, you must configure and enable a syslog server on your Venusense appliance with the IP address of your SIEM Console or Event Collector.

Procedure

1 Log in to the configuration interface for your Venusense appliance.

2 From the navigation menu, select **Logs > Log Configuration > Log Servers**.

3 In the **IP Address** field, type the IP address of your SIEM Console or Event Collector.

4 In the **Port** field, type **514**.

5 Select the **Enable** check box.

6 Click **OK**.

Next Steps

You are ready to configure your Venusense appliance to filter which events are forwarded to SIEM.

Configuring Venusense Event Filtering

Event filtering allows you to determine which events your Venusense appliance forwards to SIEM.

Procedure

1 From the navigation menu, select **Logs > Log Configuration > Log Filtering**.

2 In the Syslog Log column, select a check box for each event log you want to forward to SIEM.

3 From the list, select a syslog facility for the event log you enabled.

4 Repeat Step 2 and Step 3 to configure any additional syslog event filters.

5 Click **OK**.

Next Steps

You are now ready to configure a log source for your Venusense appliance in SIEM. SIEM does not automatically discover or create log sources for syslog events from Venusense appliances.

Configuring a Venusense Log Source

To integrate Venusense syslog events, you must manually create a log source in SIEM as Venusense events to not automatically discover.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select your Venustech Venusense appliance.

The type of log source you select is determined by the event filtering configured on your Venusense appliance. The options include:

- **Venustech Venusense Security Platform** - Select this option if you enabled all event filtering options.

- **Venustech Venusense UTM** - Select this option if you enabled unified filtering events.
- **Venustech Venusense Firewall** - Select this option if you enabled filtering for firewall events.
- **Venustech Venusense NIPS** - Select this option if you enabled filtering for firewall events.

9 From the Protocol Configuration list, select **Syslog**.

10 In the **Log Source Identifier** field, type the IP address or host name for the log source as an identifier for your Venusense appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete. Events forwarded to SIEM by your Venusense appliance are displayed on the **Log Activity** tab.

121 Verdasys Digital Guardian

The Verdasys Digital Guardian DSM for SIEM accepts and categorizes all alert events from Verdasys Digital Guardian appliances.

About Verdasys Digital Guardian

Verdasys Digital Guardian is a comprehensive Enterprise Information Protection (EIP) platform. Digital Guardian serves as a cornerstone of policy driven, data-centric security by enabling organizations to solve the information risk challenges that exist in today's highly collaborative and mobile business environment. Digital Guardian's endpoint agent architecture makes it possible to implement a data-centric security framework.

Verdasys Digital Guardian allows business and IT managers to:

- Discover and classify sensitive data by context and content
- Monitor data access and usage by user or process
- Automatically implement policy driven information protection
- Alert, block, and record high risk behavior to prevent costly and damaging data loss incidents.

Digital Guardian's integration with SIEM provides context from the endpoint and enables a new level of detection and mitigation for Insider Threat and Cyber Threat (Advanced Persistent Threat).

Digital Guardian provides SIEM with a rich data stream from the end-point which includes; visibility of every data access by users or processes including the file name, file classification, application used to access the data and other contextual variables.

Supported Event Types

SIEM supports all SIEM LEEF or syslog formatted alert events you configure in your data export from Verdasys Digital Guardian.

Supported Versions

SIEM supports Verdasys Digital Guardian versions:

- v6.1.1 and later with the SIEM LEEF event format
- v6.0.x with the Syslog event format

Configuring IPtables

Before configuring your Verdasys Digital Guardian to forward events, you must configure IPtables in SIEM to allow ICMP requests from Verdasys Digital Guardian.

Procedure

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

Login: `root`

Password: `<password>`

2 Type the following command to edit the IPtables file:

```
vi /opt/qradar/conf/iptables.post
```

The IPtables configuration file is displayed.

3 Type the following command to allow SIEM to accept ICMP requests from Verdasys Digital Guardian:

```
-I QChain 1 -m icmp -p icmp --src <IP address> -j ACCEPT
```

Where `<IP address>` is the IP address of your Verdasys Digital Guardian appliance. For example,

```
-I QChain 1 -m icmp -p icmp --src 10.100.100.101 -j ACCEPT
```

4 Save your IPtables configuration.

5 Type the following command to update IPtables in SIEM:

```
./opt/qradar/bin/iptables_update.pl
```

6 To verify SIEM accepts ICMP traffic from your Verdasys Digital Guardian, type the following command:

```
iptables --list --line-numbers
```

The following output is displayed:

```
[root@Qradar bin]# iptables --list --line-numbers
Chain QChain (1 references)
num target  prot   opt   source           destination
1   ACCEPT  icmp   --    10.100.100.101   anywhere       icmp any
2   ACCEPT  tcp    --    anywhere         anywhere       state
NEW tcp dpt:https
3   ACCEPT  tcp    --    anywhere         anywhere       state
NEW tcp dpt:http
```

The IPtables configuration for SIEM is complete.

Configuring a Data Export

Data exports allow you to configure the events Verdasys Digital Guardian forwards to SIEM.

Procedure

1 Log in to the Digital Guardian Management Console.

2 Select **Workspace > Data Export > Create Export**.

3 From the **Data Sources** list, select **Alerts** or **Events** as the data source.

4 From the **Export type** list, select **SIEM LEEF**.

If your Verdasys Digital Guardian is v6.0.x, you can select **Syslog** as the **Export Type**. SIEM LEEF is the preferred export type format for all Verdasys Digital Guardian appliances with v6.1.1 and later.

5 From the **Type** list, select **UDP** or **TCP** as the transport protocol.

SIEM can accept syslog events from either transport protocol. If the length of your alert events typically exceed 1024 bytes, then you should select **TCP** to prevent the events from being truncated.

6 In the **Server** field, type the IP address of your SIEM Console or Event Collector.

7 In the **Port** field, type **514**.

8 From the **Severity Level** list, select a severity level.

9 Select the **Is Active** check box.

10 Click **Next**.

11 From the list of available fields, add the following Alert or Event fields for your data export:

- Agent Local Time
- Application
- Computer Name
- Detail File Size
- IP Address
- Local Port
- Operation (required)
- Policy
- Remote Port
- Rule
- Severity
- Source IP Address
- User Name
- Was Blocked
- Was Classified

12 Select a Criteria for the fields in your data export and click **Next**.

By default, the Criteria is blank.

13 Select a group for the criteria and click **Next**.

By default, the Group is blank.

14 Click **Test Query**.

A Test Query ensures the database runs properly.

15 Click **Next**.

16 Save the data export.

The configuration is complete.

Next steps

The data export from Verdasys Digital Guardian occurs on a 5 minute interval. You can adjust this timing with the job scheduler in Verdasys Digital Guardian, if required. Events exported to SIEM by Verdasys Digital Guardian are displayed on the **Log Activity** tab.

Configuring a Log Source

SIEM automatically discovers and creates a log source for data exports from Verdasys Digital Guardian appliances. The following procedure is optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Verdasys Digital Guardian.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 207: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Verdasys Digital Guardian appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM.

122 Vericept Content 360 DSM

The Vericept Content 360 DSM for SIEM accepts Vericept events using syslog.

SIEM records all relevant and available information from the event. Before configuring a Vericept device in SIEM, you must configure your device to forward syslog. For more information on configuring your Vericept device, consult your vendor documentation.

After you configure syslog to forward events to SIEM the configuration is complete. The log source is added to SIEM as Vericept Content 360 events are automatically discovered. Events forwarded to SIEM by your Vericept Content 360 appliance are displayed on the **Log Activity** tab.

To manually configure a log source for SIEM to receive events from a Vericept device:

From the Log Source Type list, select the Vericept Content 360 option.

For more information on configuring devices, see the *SIEM Log Sources User Guide*.

123 VMWare

The VMWare DSM for SIEM can collect events from VMWare ESX and ESXi, vCenter, vCloud Director, vShield servers.

VMware ESX and ESXi

The EMC VMware DSM for SIEM collects ESX and ESXi server events by using the VMware protocol or syslog. The EMC VMware DSM supports events from VMware ESX or ESXi 3.x, 4.x, or 5.x servers.

To collect VMware ESX or ESXi events, you can select one of the following event collection methods:

- Configuring Syslog on VMWare ESX and ESXi Servers on page 645
- Configuring the VMWare Protocol for ESX or ESXi Servers on page 648

Configuring Syslog on VMWare ESX and ESXi Servers

To collect syslog events for VMWare, you must configure the server to forward events by using syslogd from your ESXi server to SIEM.

Procedure

1 Log in to your VMWare vSphere Client.

2 Select the host that manages your VMWare inventory.

3 Click the **Configuration** tab.

4 From the Software panel, click **Advanced Settings**.

5 In the navigation menu, click **Syslog**.

6 Configure values for the following parameters:

Table 208: VMWare syslog protocol parameters

Parameter	ESX version	Description
Syslog.Local.DatastorePath	ESX or ESXi 3.5.x or 4.x	Type the directory path for the local syslog messages on your ESXi server. The default directory path is `[] /scratch/log/messages`.
Syslog.Remote.Hostname	ESX or ESXi 3.5.x or 4.x	Type the IP address or host name of SIEM.
Syslog.Remote.Port	ESX or ESXi 3.5.x or 4.x	Type the port number the ESXi server uses to forward syslog data. The default is port 514.

Table 208: VMWare syslog protocol parameters (Continued)

Parameter	ESX version	Description
Syslog.global.logHost	ESXi v5.x	Type the URL and port number that the ESXi server uses to forward syslog data. Examples: udp://<SIEM IP address>:514 tcp://<SIEM IP address>:514

7 Click **OK** to save the configuration.

Firewall Settings for VMWare Products

The default firewall configuration on VMWare ESXi v5.x servers disable outgoing connections by default. Disabled outgoing syslog connections restrict the internal syslog forwarder from sending security and access events to SIEM

By default, the syslog firewall configuration for VMWare products allow only outgoing syslog communications. To prevent security risks, do not edit the default syslog firewall rule to enable incoming syslog connections.

Enabling Syslog Firewall Settings on vSphere Clients

To forward syslog events from ESXi v5.x server, you must edit your security policy to enable outgoing syslog connections for events.

Procedure

1 Log in to your ESXi v5.x Server from a vSphere client.

2 From the inventory list, select your ESXi Server.

3 Click the **Manage** tab and select **Security Profile**.

4 In the Firewall section, click **Properties**.

5 In the Firewall Properties window, select the **syslog** check box.

6 Click **OK**.

Configuring a Syslog Log Source for VMware ESX or ESXi

SIEM automatically discovers and creates a log source for syslog events from VMWare. The following configuration steps are optional.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select **EMC VMWare**.

6 Using the Protocol Configuration list, select **Syslog**.

7 Configure the following values:

Table 209: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your EMC VMWare server.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

Configuring the VMWare Protocol for ESX or ESXi Servers

You can configure the VMWare protocol to read events from your VMWare ESXi server. The VMware protocol uses HTTPS to poll for ESX and ESXi servers for events.

Before you configure your log source to use the VMWare protocol, we suggest you create a unique user to poll for events. This user can be created as a member of the root or administrative group, but you must provide the user with an assigned role of read-only permission. This ensures that SIEM can collect the maximum number of events and retain a level of security for your virtual servers. For more information on user roles, see your VMWare documentation.

To integrate EMC VMWare with SIEM, you must complete the following tasks:

1 Create an ESX account for SIEM.

2 Configure account permissions for the SIEM user.

3 Configure the VMWare protocol in SIEM.

Creating a user who is not part of the root or an administrative group might lead to some events not being collected by SIEM. We suggest that you create your SIEM user to include administrative privileges, but assign this custom user a read-only role.

Creating an Account for SIEM in ESX

You can create a SIEM user account for EMC VMWare to allow the protocol to properly poll for events.

Procedure

1 Log in to your ESX host by using the vSphere Client.

2 Click the **Local Users & Groups** tab.

3 Click **Users**.

4 Right-click and select **Add**.

5 Configure the following parameters:
   a **Login** - Type a login name for the new user.
   b **UID** - Optional. Type a user ID.
   c **User Name** - Optional. Type a user name for the account.
   d **Password** - Type a password for the account.
   e **Confirm Password** - Type the password again as confirmation.
   f **Group** - From the **Group** list, select **root**.

6 Click **Add**.

7 Click **OK**.

Configuring Read-only Account Permissions

For security reasons, we suggest you configure your SIEM user account as a member of your root or admin group, but select an assigned role of read-only permissions.

Read-only permission allows the SIEM user account to view and collect events by using the VMWare protocol.

Procedure

1 Click the **Permissions** tab.

2 Right-click and select Add Permissions.

3 On the Users and Groups window, click **Add**.

4 Select your SIEM user and click **Add**.

5 Click **OK**.

6 From the **Assigned Role** list, select **Read-only**.

7 Click **OK**.

Configuring a Log Source for the VMWare Protocol

You can configure a log source with the VMWare protocol to poll for EMC VMWare events.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select EMC VMWare.

6 Using the Protocol Configuration list, select **EMC** VMWare.

7 Configure the following values:

Table 210: VMWare protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. This value must match the value configured in the **ESX IP** field.
ESX IP	Type the IP address of the VMWare ESX or ESXi server. For example, `1.1.1.1`. The VMware protocol prepends the IP address of your VMware ESX or ESXi server with HTTPS before the protocol requests event data.
User Name	Type the username required to access the VMWare server.
Password	Type the password required to access the VMWare server.

8 Click Save.

9 On the Admin tab, click Deploy Changes.

VMware vCenter

The VMware vCenter DSM for SIEM collects vCenter server events by using the VMware protocol.

The VMware protocol uses HTTPS to poll for vCenter appliances for events. You must configure a log source in SIEM to collect VMware vCenter events.

Before you configure your log source to use the VMWare protocol, we suggest you create a unique user to poll for events. This user can be created as a member of the root or administrative group, but you must provide the user with an assigned role of read-only permission. This ensures that SIEM can collect the maximum number of events and retain a level of security for your virtual servers. For more information on user roles, see your VMWare documentation.

Configuring a Log Source for the VMWare vCenter

To collect vCenter events with the VMware protocol, you must configure a log source in SIEM.

Procedure

1 Click the **Admin** tab.

2 Click the Log Sources icon.

3 Click Add.

4 In the **Log Source Name** field, type a name for your log source.

5 From the Log Source Type list, select VMWare vCenter.

6 Using the Protocol Configuration list, select **EMC** VMWare.

7 The syslog protocol is listed in the

8 Configure the following values:

Table 211: VMware protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source. This value must match the value configured in the **ESX IP** field.
ESX IP	Type the IP address of the VMWare vCenter server. For example, `1.1.1.1`. The VMware protocol prepends the IP address of your VMware vCenter server with HTTPS before the protocol requests event data.
User Name	Type the username required to access the VMWare vCenter server.
Password	Type the password required to access the VMWare vCenter server.

9 Click Save.

10 On the Admin tab, click Deploy Changes.

VMware vCloud Director

You can use the VMware vCloud Director DSM and the vCloud protocol for SIEM to poll the vCloud REST API for events.

Configuration Overview

SIEM supports polling for VMware vCloud Director events from vCloud Directory 5.1 appliances. Events collected by using the vCloud REST API are assembled as Log Extended Event Format (LEEF) events.

To integrate vCloud events with SIEM, you must complete the following tasks:

1. On your vCloud appliance, configure a public address for the vCloud REST API.
2. On your SIEM appliance, configure a log source to poll for vCloud events.
3. Ensure that no firewall rules block communication between your vCloud appliance and the SIEM Console or the managed host that is responsible for polling the vCloud REST API.

Supported vCloud Event Types Logged by SIEM

The VMware vCloud DSM for SIEM can collect events from several categories.

Each event category contains low level events that describe the action taken within the event category. For example, user events can have user created or user deleted as low level event.

The following list are the default event categories collected by SIEM from vCloud Director:

- User events
- Group events
- User role events
- Session events
- Organization events
- Network events
- Catalog events
- Virtual data center (VDC) events
- Virtual application (vApp) events
- Virtual machine (VM) events
- Media events
- Task operation events

Configuring the vCloud REST API Public Address

SIEM collects security data from the vCloud API by polling the REST API of the vCloud appliance for events. Before SIEM can collect any data, you must configure the public REST API base URL.

Procedure

1 Log in to your vCloud appliance as an administrator.

2 Click the **Administration** tab.

3 From the Administration menu, select **System Settings > Public Addresses**.

4 In the **VCD public REST API base URL** field, type an IP address or host name.

The address that you specify becomes a publically available address outside of the firewall or NAT on your vCloud appliance. For example, `https://1.1.1.1/`.

5 Click **Apply**.

The public API URL is created on the vCloud appliance.

What to do next

You are now ready to configure a log source in SIEM.

Configuring a vCloud Log Source in SIEM

To collect vCloud events, you must configure a log source in SIEM with the location and credentials that are required to poll the vCloud API.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 Optional. In the **Log Source Description** field, type a description for your log source.

8 From the Log Source Type list, select **VMware vCloud Director**.

9 From the **Protocol Configuration** list, select **VMware vCloud Director**.

10 Configure the following values:

Table 212: VMware vCloud Director log source parameters

Parameter	Description
Log Source Identifier	Type the IP address, host name, or name that identifies the vCloud appliance events to SIEM.

Table 212: VMware vCloud Director log source parameters (Continued)

Parameter	Description
vCloud URL	Type the URL configured on your vCloud appliance to access the REST API. The URL you type must match the address you configured in the **VCD public REST API base URL** field on your vCloud Server. For example, `https://10.10.10.1`.
User Name	Type the user name that is required to remotely access the vCloud Server. For example, `console/user@organization`. If you want to configure a read-only account to use with SIEM, you can create a vCloud user in your organization who has the **Console Access Only** permission.
Password	Type the password that is required to remotely access the vCloud Server.
Confirm Password	Confirm the password that is required to remotely access the vCloud Server.
Polling Interval	Type a polling interval, which is the amount of time between queries to the vCloud Server for new events. The default polling interval is 10 seconds.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

11 Click **Save**.

12 On the **Admin** tab, click **Deploy Changes**.

vCloud events that are forwarded to SIEMce are displayed on the **Log Activity** tab of SIEM.

VMware vShield

The SIEM DSM for VMware vShield can collect event logs from your VMware vShield servers.

The following table identifies the specifications for the VMware vShield Server DSM:

Table 213: VMware vShield DSM specifications

Specification	Value
Manufacturer	VMware
DSM	vShield
RPM file name	DSM-VMwarevShield-*build_number*.noarch.rpm
Supported versions	
Protocol	Syslog
SIEM recorded events	All events
Automatically discovered	Yes
Includes identity	No
More information	www.vmware.com/

VMware vShield DSM Integration Process

To integrate VMware vShield DSM with SIEM, use the following procedures:

1 If automatic updates are not enabled, download and install the most recent version of the VMware vShield RPM on your SIEM Console.

2 For each instance of VMware vShield, configure your VMware vShield system to enable communication with SIEM. This procedure must be performed for each instance of VMware vShield.

3 If SIEM does not automatically discover the log source, for each VMware vShield server that you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually Installing a DSM on page 4

Configuring your VMware vShield System for Communication with SIEM on page 655

Configuring a VMware vShield Log Source in SIEM on page 655

Configuring your VMware vShield System for Communication with SIEM

To collect all audit logs and system events from VMware vShield, you must configure the vShield Manager. When you configure VMware vShield, you must specify SIEM as the syslog server.

Procedure

1 Access your vShield Manager inventory panel.

2 Click **Settings & Reports**.

3 Click **Configuration > General**.

4 Click **Edit** next to the **Syslog Server** option.

5 Type the IP address of your SIEM Console.

6 Optional. Type the port for your SIEM Console. If you do not specify a port, the default UDP port for the IP address/host name of your SIEM Console is used.

7 Click **OK**.

Configuring a VMware vShield Log Source in SIEM

To collect VMware vShield events, configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **VMware vShield**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

124 Vormetric Data Security

The Vormetric Data Security DSM for SIEM can collect event logs from your Vormetric Data Security servers.

The following table identifies the specifications for the Vormetric Data Security DSM:

Table 214: Vormetric Data Security DSM specifications

Specification	Value
Manufacturer	Vormetric, Inc.
DSM	Vormetric Data Security
RPM file name	DSM-VormetricDataSecurity-7.1-804377.noarch.rpm DSM-VormetricDataSecurity-7.2-804381.noarch.rpm
Supported versions	Vormetric Data Security Manager v5.1.3 and later Vormetric Data Firewall FS Agent v5.2 and later
Protocol	Syslog (LEEF)
SIEM recorded events	Audit, Alarm, Warn, Learn Mode, System
Auto discovered	Yes
Includes identity	No
More information	Vormetric website (www.vormetric.com)

Vormetric Data Security DSM Integration Process

To integrate Vormetric Data Security DSM with SIEM, use the following procedures:

1 If automatic updates are not enabled, download and install the most recent version of the following RPMs on your SIEM Console:

- Syslog protocol RPM
- DSMCommon RPM
  The minimum version of the DSMCommon RPM that you can use are the DSM-DSMCommon-7.1-530016.noarch.rpm or DSM-DSMCommon-7.2-572972.noarch.rpm
- Vormetric Data Security RPM

2 For each instance of Vormetric Data Security, configure your Vormetric Data Security system to enable communication with SIEM.

3 If SIEM does not automatically discover the DSM, for each Vormetric Data Security server you want to integrate, create a log source on the SIEM Console.

Related tasks

Manually Installing a DSM on page 4

Configuring your Vormetric Data Security Systems for Communication with SIEM on page 657

Configuring a Vormetric Data Security Log Source in SIEM on page 659

Configuring your Vormetric Data Security Systems for Communication with SIEM

To collect all audit logs and system events from Vormetric Data Security, you must configure your Vormetric Data Security Manager to enable communication with SIEM.

Before You Begin

Your Vormetric Data Security Manager user account must have System Administrator permissions.

Procedure

1 Log in to your Vormetric Data Security Manager as an administrator that is assigned System Administrator permissions.

2 On the navigation menu, click **Log > Syslog**.

3 Click **Add**.

4 In the **Server Name** field, type the IP address or host name of your SIEM system.

5 From the **Transport Protocol** list, select `TCP` or a value that matches the log source protocol configuration on your SIEM system.

6 In the **Port Number** field, type `514` or a value that matches the log source protocol configuration on your SIEM system.

7 From the **Message Format** list, select **LEEF**.

8 Click **OK**.

9 On the Syslog Server summary screen, verify the details you have entered for your SIEM system. If the **Logging to SysLog** value is **OFF**, complete the following steps.
   a On the navigation menu, click **System > General Preferences**.
   b Click the **System** tab.
   c In the **Syslog Settings** pane, select the **Syslog Enabled** check box.

What to do next

Configuring Vormetric Data Firewall FS Agents to Bypass Vormetric Data Security Manager on page 658

Configuring Vormetric Data Firewall FS Agents to Bypass Vormetric Data Security Manager

When the Vormetric Data Security Manager is enabled to communicate with SIEM, all events from the Vormetric Data Firewall FS Agents are also forwarded to the SIEM system through the Vormetric Data Security Manager. To bypass the Vormetric Data Security Manager, you can configure Vormetric Data Firewall FS Agents to send LEEF events directly to the SIEM system.

Before You Begin

Your Vormetric Data Security Manager user account must have System Administrator permissions.

Procedure

1 Log in to your Vormetric Data Security Manager.

2 On the navigation menu, click **System > Log Preferences**.

3 Click the **FS Agent Log** tab.

4 In the Policy Evaluation row, configure the following parameters:
   a Select the **Log to Syslog/Event Log** check box.
   b Clear the **Upload to Server** check box.
   c From the **Level** list, select **INFO**.

   This set up enables a full audit trail from the policy evaluation module to be sent directly to a syslog server, and not to the Security Manager. Leaving both destinations enabled may result in duplication of events to the SIEM system.

5 Under the Syslog Settings section, configure the following parameters.
   a In the **Server** field, use the following syntax to type the IP address or host name and port number of your SIEM system.

   ```
   SIEM_IP address_or_host:port
   ```

   b From the **Protocol** list, select TCP or a value that will match the log source configuration on your SIEM system.
   c From the **Message Format** list, select **LEEF**.

What to do next

This configuration is applied to all hosts or host groups subsequently added to the Vormetric Data Security Manager. For each existing host or host group, select the required host or host group from the **Hosts** list and repeat the procedure.

Configuring a Vormetric Data Security Log Source in SIEM

To collect Vormetric Data Security events, configure a log source in SIEM.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 In the navigation menu, click Data Sources.

4 Click the Log Sources icon.

5 Click Add.

6 From the Log Source Type list, select **Vormetric Data Security**.

7 From the **Protocol Configuration** list, select **Syslog**.

8 Configure the remaining parameters.

9 Click **Save**.

10 On the **Admin** tab, click **Deploy Changes**.

125 WatchGuard Fireware OS

For instructions about how to integrate this DSM, see the *DSM Configuration Guide Addendum*.

126 Websense V-Series

This section provides information on the following DSMs:

Websense TRITON

The Websense V-Series Content Gateway DSM for SIEM supports events for web content from several Websense TRITON solutions, including Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series™ appliances.

Websense TRITON collects and streams event information to SIEM using the Websense Multiplexer component. Before configuring SIEM, you must configure the Websense TRITON solution to provide LEEF formatted syslog events.

Before You Begin

Before you can configure Websense TRITON Web Security solutions to forward events to SIEM, you must ensure your deployment contains a Websense Multiplexer.

The Websense Multiplexer is supported on Windows, Linux, and on Websense V-Series appliances.

To configure a Websense Multiplexer on a Websense Triton or V-Series appliance:

1 Install an instance of Websense Multiplexer for each Websense Policy Server component in your network.

- **For Microsoft Windows** - To install the Websense Multiplexer on Windows, use the TRITON Unified Installer. The Triton Unified Installer is available for download at www.mywebsense.com.
- **For Linux** - To install the Websense Multiplexer on Linux, use the Web Security Linux Installer. The Web Security Linux Installer is available for download at www.mywebsense.com.

  For information on adding a Websense Multiplexer to software installations, see your *Websense Security Information Management (SIEM) Solutions* documentation.

2 Enable the Websense Multiplexer on a V-Series appliance configured as a full policy source or user directory and filtering appliance:
   a Log in to your Websense TRITON Web Security Console or V-Series appliance.
   b From the Appliance Manager, select **Administration > Toolbox > Command Line Utility**.
   c Click the **Websense Web Security** tab.
   d From the **Command** list, select **multiplexer**, then use the **enable** command.

3 Repeat Step 1 and Step 2 to enable one Multiplexer instance for each Policy Server instance in your network.

If more than one Multiplexer is installed for a Policy Server, only the last installed instance of the Websense Multiplexer is used. The configuration for each Websense Multiplexer instance is stored by its Policy Server.

You are now ready to configure your Websense TRITON appliance to forward syslog events in LEEF format to SIEM.

Configuring Syslog for Websense TRITON

To collect events, you must configure syslog forwarding for Websense TRITON.

Procedure

1. Log in to your Websense TRITON Web Security Console.
2. On the **Settings** tab, select **General > SIEM Integration**.
3. Select the **Enable SIEM integration for this Policy Server** check box.
4. In the **IP address or hostname** field, type the IP address of your SIEM.
5. In the **Port** field, type **514**.
6. From the **Transport protocol** list, select either the **TCP** or **UDP** protocol option.
   SIEM supports syslog events for TCP and UDP protocols on port 514.
7. From the **SIEM format** list, select **syslog/LEEF (SIEM)**.
8. Click **OK** to cache any changes.
9. Click **Deploy** to update your Websense Triton security components or V-Series appliances.

The Websense Multiplexer connects to Websense Filtering Service and ensures that event log information is provided to SIEM.

Configure a Log Source

SIEM automatically discovers and creates a log source for syslog events in LEEF format from Websense TRITON and V-Series appliances. The configuration steps for creating a log source are optional.

Procedure

1. Log in to SIEM.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the Log Sources icon.
5. Click Add.
6. In the **Log Source Name** field, type a name for your log source.
7. In the **Log Source Description** field, type a description for the log source.
8. From the Log Source Type list, select Websense V Series Content Gateway.

NOTE

Websense TRITON uses the Websense V Series Content Gateway DSM for parsing events. When you manually add a log source to SIEM for Websense TRITON, you should select the Websense V Series Content Gateway.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 215: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Websense TRITON or V-Series appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The log source is added to SIEM.

Websense V-Series Data Security Suite

The Websense V-Series Data Security Suite DSM for SIEM supports Websense V-Series appliances and the Data Security Suite (DSS) software.

Configuring Syslog for Websense V-Series DSS

The Websense V-Series Data Security Suite DSM accepts events using syslog. Before you can integrate SIEM you, must enable the Websense V-Series appliance to forward syslog events in the Data Security Suite (DSS) Management Console.

Procedure

1 Select **Policies > Policy Components > Notification Templates**.

2 Select an existing Notification Template or create a new template.

3 Click the General tab.

4 Click Send Syslog Message.

5 Select **Options > Settings > Syslog** to access the Syslog window.

The syslog window enables administrators to define the IP address/hostname and port number of the syslog in their organization. The defined syslog receives incident messages from the Websense Data Security Suite DSS Manager.

6 The syslog is composed of the following fields:

DSS Incident|ID={value}|action={display value - max}|urgency= {coded}|policy categories={values,,,}|source={value-display

name}|destinations={values...}|channel={display name}|matches={value}|detaills={value}

- Max length for policy categories is 200 characters.
- Max length for destinations is 200 characters.
- Details and source are reduced to 30 characters.

7 Click Test Connection to verify that your syslog is accessible.

You are now ready to configure the log source in SIEM.

The configuration is complete. The log source is added to SIEM as OSSEC events are automatically discovered. Events forwarded to SIEM by OSSEC are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Websense V-Series Data Security Suite. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Websense V Series.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 216: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Websense V-Series Data Security Suite DSM

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Websense V-Series Content Gateway

The Websense V-Series Content Gateway DSM for SIEM supports events for web content on Websense V-Series appliances with the Content Gateway software.

The Websense V-Series Content Gateway DSM accepts events using syslog to stream events or using the Log File protocol to provide events to SIEM. Before you can integrate your appliance with SIEM, you must select one of the following configuration methods:

- To configure syslog for your Websense V-Series, see Configure Syslog for Websense V-Series Content Gateway on page 665.
- To configure the log file protocol for your Websense V-Series, see Configuring a Log File Protocol for Websense V-Series Content Gateway on page 667.

Configure Syslog for Websense V-Series Content Gateway

The Websense V-Series DSM supports Websense V-Series appliances running the Websense Content Gateway on Linux software installations.

Before configuring SIEM, you must configure the Websense Content Gateway to provide LEEF formatted syslog events.

Configure the Management Console

To configure event logging in the Content Gateway Manager:

1 Log into your Websense Content Gateway Manager.

1 Click the Configure tab.

2 Select **Subsystems > Logging**.

The General Logging Configuration window is displayed.

3 Select Log Transactions and Errors.

4 Select **Log Directory** to specify the directory path of the stored event log files.

The directory you define must already exist and the Websense user must have read and write permissions for the specified directory. The default directory is `/opt/WGC/logs`

5 Click Apply.

6 Click the Custom tab.

7 In the **Custom Log File Definitions** window, type the following text for the LEEF format.

```
<LogFormat>
     <Name = "leef"/>
     <Format =
"LEEF:1.0|Websense|WCG|7.6|%<wsds>|cat=%<wc>     src=%<chi>
 devTime=%<cqtn>     devTimeFormat=dd/MMM/yyyy:HH:mm:ss
Z     http-username=%<caun>     url=%<cquc>
     method=%<cqhm>     httpversion=%<cqhv>     cachecode=%<crc
>     dstBytes=%<sscl>     dst=%<pqsi>
     srcBytes=%<pscl>     proxy-status-code=%<pssc>     server-
```

```
status-code=%<sssc>     usrName=%<wui>     duration=%<ttms>"/>
</LogFormat>
<LogObject>
   <Format = "leef"/>
   <Filename = "leef"/>
</LogObject>
```

NOTE

The fields in the LEEF format string are tab separated. You might be required to type the LEEF format in a text editor and then cut and paste it into your web browser to retain the tab separations.The definitions file ignores extra white space, blank lines, and all comments.

8 Select **Enabled** to enable the custom logging definition.

9 Click Apply.

You are now ready to enable event logging for your Websense Content Gateway.

Enable Event Logging

If you are using a Websense V-Series appliance, you need to contact Websense Technical Support to enable this feature.

Procedure

1 Log in to the command-line Interface (CLI) of the server running Websense Content Gateway.

2 Add the following lines to the end of the /etc/rc.local file:

```
( while [ 1 ] ; do
         tail -n1000 -F /opt/WCG/logs/leef.log | nc <IP Address>
514
         sleep 1
done ) &
```

Where `<IP Address>` is the IP address for SIEM.

3 To start logging immediately, type the following command:

```
nohup /bin/bash –c "while [ 1 ] ; do tail -F /opt/WCG/logs/
leef.log | nc <IP Address> 514; sleep 1; done" &
```

NOTE

You might need to type the logging command in Step 3 or copy the command to a text editor to interpret the quotation marks.

The configuration is complete. The log source is added to SIEM as syslog events from Websense V-Series Content Gateway are automatically discovered. Events forwarded by Websense V-Series Content Gateway are displayed on the **Log Activity** tab of SIEM.

Configuring a Log Source

SIEM automatically discovers and creates a log source for syslog events from Websense V-Series Content Gateway. The following configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select Websense V Series.

9 Using the Protocol Configuration list, select **Syslog**.

10 Configure the following values:

Table 217: Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Websense V-Series Content Gateway appliance.

11 Click Save.

12 On the Admin tab, click Deploy Changes.

The configuration is complete.

Configuring a Log File Protocol for Websense V-Series Content Gateway

The log file protocol allows SIEM to retrieve archived log files from a remote host.

The Websense V-Series DSM supports the bulk loading of log files from your Websense V-Series Content Gateway using the log file protocol to provide events on a scheduled interval. The log files contain transaction and error events for your Websense V-Series Content Gateway:

Configure the Management Console

To configure event logging in the Content Management Console:

1 Log into your Websense Content Gateway interface.

1 Click the Configure tab.

2 Select **Subsystems > Logging**.

3 Select Log Transactions and Errors.

4 Select **Log Directory** to specify the directory path of the stored event log files.

The directory you define must already exist and the Websense user must have read and write permissions for the specified directory. The default directory is `/opt/WGC/logs`.

5 Click Apply.

6 Click the Formats tab.

7 Select Netscape Extended Format as your format type.

8 Click Apply.

You are now ready to enable event logging for your Websense V-Series Content Gateway.

Configuring a Log File Protocol Log Source

When configuring your Websense V-Series DSM to use the log file protocol, make sure the hostname or IP address configured in the Websense V-Series is the same as configured in the Remote Host parameter in the Log File protocol configuration.

Procedure

1 Log in to SIEM.

2 Click the **Admin** tab.

3 On the navigation menu, click **Data Sources**.

4 Click the Log Sources icon.

5 Click Add.

6 In the **Log Source Name** field, type a name for your log source.

7 In the **Log Source Description** field, type a description for the log source.

8 From the Log Source Type list, select the Websense V Series.

9 From the Protocol Configuration list, select the Log File.

10 From the Service Type list, select the Secure File Transfer Protocol (SFTP) option.

11 In the FTP File Pattern field, type extended.log_.*.old.

12 In the Remote Directory field, type /opt/WCG/logs.

This is the default directory for storing the Websense V-Series log files you specified in Step 4.

13 From the Event Generator list, select LINEBYLINE.

14 Click Save.

15 On the Admin tab, click Deploy Changes.

The log source is added to SIEM. For the entire list of Log File protocol parameters, see the *SIEM Log Sources User Guide.*

127 Zscaler Nanolog Streaming Service

SIEM can collect and categorize events from Zscaler Nanolog Streaming Service (NSS) log feeds that forward syslog event to SIEM.

Configuration Overview

To collect syslog events, you must configure your Zscaler NSS with an NSS feed to forward TCP syslog events to SIEM. SIEM automatically discovers and creates log sources for syslog events that are forwarded from Zscaler NSS log feeds. SIEM supports syslog events from Zscaler NSS V4.1.

To configure Zscaler NSS, complete the following tasks:

1 On your Zscaler NSS appliance, create a log feed for SIEM.

2 On your SIEM system, verify that the forwarded events are automatically discovered.

Supported Event Types for Zscaler NSS

The ZScaler NSS DSM for SIEM collects information about web browsing events from Zscaler NSS installations.

Each Zscaler NSS event contains information on the action that is taken on the web browsing in the event category. For example, web browsing events can have a category that is allowed or blocked website traffic. Each event defines the website that was allowed or blocked and includes all of the event details in the event payload.

Configuring a Syslog Feed in Zscaler NSS

To collect events, you must configure a log feed on your Zscaler NSS to forward syslog events to SIEM.

Procedure

1 Log in to the administration portal for Zscaler NSS.

2 In the navigation menu, select **Policy > Administration > Configure Nanolog Streaming Service**.

3 Click **Add Feed**.

4 In the **Feed Name** field, type a name for the NSS feed.

5 From the **NSS Name** list, select the ZScaler NSS system.

6 From the **Status** list, select **Enabled**.

7 In the **SIEM IP** field, type the IP address of your SIEM system.

8 In the **TCP Port** field, type the 514.

9 From the **Log Type** list, select **Web Log**.

10 From the **Feed Output Type** list, select **Custom**.

11 In the **Feed Output Format** field, type the following custom format:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss:
LEEF:1.0|Zscaler|NSS|4.1|%s{reason}|cat=%s{action}\tdevTime=
%s{mon} %02d{dd} %d{yy}
%02d{hh}:%02d{mm}:%02d{ss}%s{tz}\tdevTimeFormat=MMM dd yyyy
HH:mm:ss z\tsrc=%s{cip}\tdst=%s{sip}
\tsrcPostNAT=%s{cintip}\trealm=%s{location}\tusrName=%s{login}\tsr
cBytes=%d{reqsize}\tdstBytes=%d{respsize}\trole=%s{dept}\tpolicy=%
s{reason}\turl=%s{url}\trecordid=%d{recordid}\tbwthrottle=%s{bwthr
ottle}\tuseragent=%s{ua}\treferer=%s{referer}\thostname=%s{host}\t
appproto=%s{proto}\turlcategory=%s{urlcat}\turlsupercategory=%s{ur
lsupercat}\turlclass=%s{urlclass}\tappclass=%s{appclass}\tappname=
%s{appname}\tmalwaretype=%s{malwarecat}\tmalwareclass=%s{malwarecl
ass}\tthreatname=%s{threatname}\triskscore=%d{riskscore}\tdlpdict=
%s{dlpdict}\tdlpeng=%s{dlpeng}\tfileclass=%s{fileclass}\tfiletype=
%s{filetype}\treqmethod=%s{reqmethod}\trespcode=%s{respcode}\n
```

12 Click **Done**.

SIEM automatically discovers and creates a log source for Zscaler NSS appliances. Events that are forwarded to SIEM are viewable on the **Log Activity** tab.

Configuring a Zscaler NSS Log Source

SIEM automatically discovers and creates a log source for syslog events that are forwarded from Zscaler NSS. These configuration steps are optional.

Procedure

1 Log in to SIEM.

2 Click the Admin tab.

3 Click the Log Sources icon.

4 Click Add.

5 In the **Log Source Name** field, type a name for your log source.

6 Optional. In the **Log Source Description** field, type a description for your log source.

7 From the Log Source Type list, select **Zscaler NSS**.

8 From the **Protocol Configuration** list, select **Syslog**.

9 Configure the following values:

Table 218: Syslog protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address as an identifier for events from your Zscaler NSS installation. The log source identifier must be unique value.

Table 218: Syslog protocol parameters (Continued)

Parameter	Description
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in SIEM. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Log Source Language	Select the language of the events generated by zScaler NSS.

10 Click **Save**.

11 On the **Admin** tab, click **Deploy Changes**.