85 SafeNet DataSecure/KeySecure

The SafeNet DataSecure DSM for IBM Security QRadar receives syslog events from your SafeNet DataSecure and KeySecure devices. QRadar supports SafeNet DataSecure and KeySecure v6.3.0 and later.

Supported event types

SafeNet DataSecure and KeySecure create the following event logs:

Activity log

Contains a record of each request that is received by the key server.

Audit log

Contains a record of all configuration changes and user input errors that are made to KeySecure, whether through the management console or the command line interface.

Client event log

Contains a record of all client requests that have the <RecordEventRequest> element.

System log

Contains a record of all system events, such as the following events:

- Service starts, stops, and restarts
- SNMP traps
- Hardware failures
- Successful or failed cluster replication and synchronization
- Failed log transfers
- License errors

Configuration overview

To integrate SafeNet DataSecure/KeyStore with QRadar, you must perform the following tasks:

1. Enable syslog on the SafeNet device.
2. Configure a SafeNet DataSecure/KeyStore log source on your QRadar Console.

Enabling syslog on SafeNet DataSecure or KeySecure

Before you add the DSM for SafeNet DataSecure/KeySecure, enable syslog on your SafeNet device.

Procedure

Step 1 Log in to the SafeNet management console as an administrator with logging access control.

Step 2 Select **Device** > **Log Configuration**.

Step 3 Select the **Rotation & Syslog** tab.

Step 4 Select a log in the **Syslog Settings** section and click **Edit**.

Step 5 Select **Enable Syslog**.

Step 6 Configure the parameters:

Parameter	Description
Syslog Server #1 IP	The IP address or host name of the target QRadar Event Collector.
Syslog Server #1 Port	The listening port for QRadar. Use Port 514.
Syslog Server #1 Proto	QRadar can receive syslog messages by using either UDP or TCP.

Step 7 Optional. Type an IP address, port, and protocol for a Syslog Server #2. When two servers are configured, SafeNet sends messages to both servers.

Step 8 Type the Syslog Facility or accept the default value of local1.

Step 9 Click **Save**.

Add a log source

QRadar automatically detects syslog events forwarded by SafeNet. In most cases, QRadar automatically adds the log source after a small number of events are detected. If required, you can manually add the log source.

Procedure

Step 1 Log in to QRadar.

Step 2 Click the **Admin** tab.

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

Step 4 Click the **Log Sources** icon.

Step 5 Click **Add**.

Step 6 From the **Log Source Type** list box, select the **SafeNet DataSecure/KeySecure** option.

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

Step 8 Configure the remaining parameters.

The following table describes some SafeNet DataSecure/KeySecure log source parameters:

Table 85-9 SafeNet DataSecure/KeySecure parameters

Parameter	Description
Log Source Identifier	The IP address or hostname to identify the log source. The value must be unique to the log source type.
Credibility	Indicates the integrity of an event or offense as determined by the credibility rating from the log source. Credibility increases if multiple log sources report the same event.
Incoming Payload Encoding	The character encoding that is required to parse the event logs.
Store Event Payload	Enables the log source to store event payload information. Automatically discovered log sources inherit the value in the **Store Event Payload** list from your system settings. When you manually create or edit a log source, you can override the default value by configuring this option.

Step 9 Optional. Clear the **Enable** check box if you want to disable the log source.

Step 10 Select any groups that you want this log source to be a member of.

Step 11 Click **Save**.