IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

DSM Configuration Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page page 67.

CONTENTS

ABOUT THIS GUIDE

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

DSMs allow QRadar to integrate events from security appliances, software, and devices in your network that forward events to IBM Security QRadar or IBM Security QRadar Log Manager. All references to QRadar or IBM Security QRadar is intended to refer both the QRadar and QRadar Log Manager product. For information on DSMs supported in IBM Security QRadar Network Anomaly Detection, see the *IBM Security QRadar Network Anomaly Detection DSM Configuration Guide.*

Intended audience

This guide is intended for the system administrator responsible for setting up event collection for QRadar in your network.

This guide assumes that you have administrative access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation	For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacting customer support	For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)
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. IBM 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. IBM 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 QRadar Network Anomaly Detection.

Device Support Modules (DSMs) parse event information for QRadar Network Anomaly Detection 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 *IBM Security QRadar Network Anomaly Detection Users Guide.*

Note: Information found in this documentation about configuring Device Support Modules (DSMs) is based on the latest RPM files located on the Qmmunity website at *https://qmmunity.q1labs.com/* or the IBM website at *http://www.ibm.com/support.*

To configure QRadar Network Anomaly Detection to receive events from devices, you must:

1. Configure the device to send events to QRadar Network Anomaly Detection.
2. Configure log sources for QRadar Network Anomaly Detection to receive events from specific devices. For more information, see the *IBM Security QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 *IBM Security QRadar Network Anomaly Detection Administration Guide*.

CAUTION: *Uninstalling a Device Support Module (DSM) is not supported in QRadar Network Anomaly Detection. If you need technical assistance, contact Customer Support. For more information, see* **Contacting customer support***.*

Schedule Automatic Updates

You can schedule when automatic updates are downloaded and installed on your QRadar Network Anomaly Detection Console.

QRadar Network Anomaly Detection 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

- For detailed information on each update, select the update. A description and any error messages are displayed in the right pane of the window.

To schedule an update:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Auto Update** icon.

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

Step 5 From the **Schedule** list box, 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 *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*.

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

Step 7 Click **OK**.

The selected updates are now scheduled.

View Pending Updates

You can view or install any pending software updates for QRadar Network Anomaly Detection through the **Admin** tab.

To view your pending updates:

Step 1 Click the **Admin** tab.

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

Step 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 2-1 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

Table 2-1 Check for Updates Window Parameters (continued)

Parameter	Description
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 2-2 Check for Updates Page Parameters Toolbar Functions

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 *IBM Security QRadar Network Anomaly Detection Administrator Guide*.
Install	From this list box, you can manually install updates. When you manually install updates, the installation process starts within a minute. For more information, see the *IBM Security QRadar Network Anomaly Detection Administrator Guide*.
Schedule	From this list box, 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. For more information, see the *IBM Security QRadar Network Anomaly Detection Administrator Guide*.
Unschedule	From this list box, you can remove preconfigured schedules for manually installing updates on your Console. For more information, see the *IBM Security QRadar Network Anomaly Detection Administrator Guide*.
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.

Step 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 Install a DSM

You can use one of the following websites to download and manually install the latest RPM files for QRadar Network Anomaly Detection.

- *https://qmmunity.q1labs.com/*
- *http://www.ibm.com/support*

Most users do not need to visit the Qmmunity website or *http://www.ibm.com/support* 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 Qmmunity website, or through auto updates contain improved event parsing for network security products and enhancements for event categorization in the QRadar Network Anomaly Detection Identifier Map (QID map).

CAUTION: *Uninstalling a Device Support Module (DSM) is not supported in QRadar Network Anomaly Detection. If you need technical assistance, contact Customer Support. For more information, see* **Contacting customer support***.*

Install a single DSM

The Qmmunity website and *http://www.ibm.com/support* website contain individual DSMs that you can download and install using the command-line.

To use the command-line to install an individual DSM:

Step 1 Download the DSM file to your system hosting QRadar Network Anomaly Detection.

Step 2 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **`root`**

Password: **`<password>`**

Step 3 Navigate to the directory that includes the downloaded file.

Step 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
```

Step 5 Log in to QRadar Network Anomaly Detection.

https://**`<IP Address>`**

Where **`<IP Address>`** is the IP address of the QRadar Network Anomaly Detection Console or Event Collector.

Step 6 On the **Admin** tab, click **Deploy Changes**.

The installation is complete.

Install a DSM Bundle

The Qmmunity and *http://www.ibm.com/support* websites contain a DSM bundle which is updated daily with the latest DSM versions that you can install.

To use the command-line to install the DSM bundle:

Step 1 Download the DSM bundle to your system hosting QRadar Network Anomaly Detection.

Step 2 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Step 3 Navigate to the directory that includes the downloaded file.

Step 4 Type the following command to extract the DSM bundle:

```
tar -zxvf QRadar Network Anomaly
Detection_bundled-DSM-<version>.tar.gz
```

Where **<version>** is your version of QRadar Network Anomaly Detection.

Step 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.

Step 6 Log in to QRadar Network Anomaly Detection.

https://**<IP Address>**

Where **<IP Address>** is the IP address of QRadar Network Anomaly Detection.

Step 7 On the **Admin** tab, click **Deploy Changes**.

The installation is complete.

3 ARRAY NETWORKS SSL VPN

The Array Networks SSL VPN DSM for IBM Security QRadar Network Anomaly Detection collects events from an ArrayVPN appliance using syslog.

Supported event types

QRadar Network Anomaly Detection records all relevant SSL VPN events forwarded using syslog on TCP port 514 or UDP port 514.

Configure a log source

To integrate Array Networks SSL VPN events with QRadar Network Anomaly Detection, you must manually create a log source. QRadar Network Anomaly Detection does not automatically discover or create log sources for syslog events from Array Networks SSL VPN.

To create a log source for Array Networks SSL VPN:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

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

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 3-1 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.

Step 11 Click **Save**.

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

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

Configure Array Networks SSL VPN

For details of configuring ArrayVPN appliances for remote syslog, please consult Array Networks documentation.

4 Cisco

This section provides information on the following DSMs:

- **Cisco NAC**
- **Cisco VPN 3000 Concentrator**

Cisco NAC

The Cisco NAC DSM for IBM Security QRadar Network Anomaly Detection accepts events using syslog.

Supported event types

QRadar Network Anomaly Detection records all relevant audit, error, and failure events as well as quarantine and infected system events. Before configuring a Cisco NAC device in QRadar Network Anomaly Detection, you must configure your device to forward syslog events.

Configure Cisco NAC to forward events

To configure the device to forward syslog events:

Step 1 Log in to the Cisco NAC user interface.

Step 2 In the Monitoring section, select **Event Logs**.

Step 3 Click the **Syslog Settings** tab.

Step 4 In the **Syslog Server Address** field, type the IP address of your QRadar Network Anomaly Detection.

Step 5 In the **Syslog Server Port** field, type the syslog port. The default is 514.

Step 6 In the **System Health Log Interval** field, type the frequency, in minutes, for system statistic log events.

Step 7 Click **Update**.

You are now ready to configure the log source in QRadar Network Anomaly Detection.

Configure a log source

To integrate Cisco NAC events with QRadar Network Anomaly Detection, you must manually create a log source to receive Cisco NAC events. QRadar Network Anomaly Detection does not automatically discover or create log sources for syslog events from Cisco NAC appliances.

To create a log source:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **Cisco NAC Appliance**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 4-2 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 NAC appliance.

Step 11 Click **Save**.

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

The log source is added to QRadar Network Anomaly Detection. Events forwarded to QRadar Network Anomaly Detection by Cisco NAC are displayed on the **Log Activity** tab.

Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Concentrator DSM for IBM Security QRadar Network Anomaly Detection accepts

Cisco VPN Concentrator events using syslog. QRadar Network Anomaly Detection records all relevant events. Before you can integrate with a Cisco VPN concentrator, you must configure your device to forward syslog events to QRadar Network Anomaly Detection.

Configure a Cisco VPN 3000 Concentrator

To configure your Cisco VPN 3000 Concentrator:

Step 1 Log in to the Cisco VPN 3000 Concentrator command-line interface (CLI).

Step 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 QRadar Network Anomaly Detection or your Event Collector.

Step 3 Type the following command to enable system message logging to the configured syslog servers:

```
set logging server enable
```

Step 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 QRadar Network Anomaly Detection as Cisco VPN Concentrator events are automatically discovered. Events forwarded to QRadar Network Anomaly Detection are displayed on the **Log Activity** tab of QRadar Network Anomaly Detection.

Configure a log source

QRadar Network Anomaly Detection 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:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **Cisco VPN 3000 Series Concentrator**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 4-3 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 Cisco VPN 3000 Series Concentrators.

Step 11 Click **Save**.

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

The configuration is complete.

5 GENERIC FIREWALL

The generic firewall server DSM for IBM Security QRadar Network Anomaly Detection accepts events using syslog. QRadar Network Anomaly Detection records all relevant events.

Configure event properties

To configure QRadar Network Anomaly Detection to interpret the incoming generic firewall events:

Step 1 Forward all firewall logs to your QRadar Network Anomaly Detection.

For information on forwarding firewall logs from your generic firewall to QRadar Network Anomaly Detection, see your firewall vendor documentation.

Step 2 Open the following file:

```
/opt/qradar/conf/genericFirewall.conf
```

Make sure you copy this file to systems hosting the Event Collector and the QRadar Network Anomaly Detection Console.

Step 3 Restart the Tomcat server:

```
service tomcat restart
```

A message is displayed indicating that the Tomcat server has restarted.

Step 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 QRadar Network Anomaly Detection, 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 /+/)**.

Step 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**.

Step 6 Add the following to the file:

```
accept_pattern=<accept pattern>
```

Where <accept pattern> is the pattern determined in**Step 5**. For example:

```
accept pattern=Packet accepted
```

Patterns are case insensitive.

Step 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.**

Step 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.

Step 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**.

Step 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.

Step 11 Save and exit the file.

You are now ready to configure the log source in QRadar Network Anomaly Detection.

Configure a log source

To integrate generic firewalls with QRadar Network Anomaly Detection, you must manually create a log source to receive the events as QRadar Network Anomaly Detection does not automatically discover or create log sources for events from generic firewall appliances.

To configure a log source:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **Configurable Firewall Filter**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 5-1 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.

Step 11 Click **Save**.

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

The log source is added to QRadar Network Anomaly Detection. Events forwarded to QRadar Network Anomaly Detection by generic firewalls are displayed on the **Log Activity** tab.

6 GENERIC AUTHORIZATION SERVER

The generic authorization server DSM for IBM Security QRadar Network Anomaly Detection records all relevant generic authorization events using syslog.

Configure event properties

To configure QRadar Network Anomaly Detection to interpret the incoming generic authorization events:

Step 1 Forward all authentication server logs to your QRadar Network Anomaly Detection system.

For information on forwarding authentication server logs to QRadar Network Anomaly Detection, see your generic authorization server vendor documentation.

Step 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.

Step 3 Restart the Tomcat server:

```
service tomcat restart
```

A message is displayed indicating that the Tomcat server has restarted.

Step 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 QRadar Network Anomaly Detection, 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 /+/)**.

Step 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**.

Step 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.

Step 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**.

Step 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.

Step 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.**

Step 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.

Step 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`.

Step 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
```

Step 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`.

Step 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 QRadar Network Anomaly Detection.

Configure a log source

To integrate generic authorization appliance event with QRadar Network Anomaly Detection, you must manually create a log source to receive the events as QRadar Network Anomaly Detection does not automatically discover or create log sources for events from generic authorization appliances.

To configure a log source:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **Configurable Authentication message filter**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 6-1 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.

Step 11 Click **Save**.

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

The log source is added to QRadar Network Anomaly Detection. Events forwarded to QRadar Network Anomaly Detection by generic authorization appliances are displayed on the **Log Activity** tab.

7 IBM

This section provides information on the following DSMs:

- **IBM AIX Server**
- **IBM AS/400 iSeries**
- **IBM Proventia Management SiteProtector**
- **IBM ISS Proventia**
- **IBM Security Network Protection (XGS)**

IBM AIX Server

IBM Security QRadar Network Anomaly Detection supports two separate event collection methods for IBM AIX®. The following methods of event collection are supported:

- **Syslog** - Event collection using syslog allows you to configure IBM AIX to forward system events to QRadar Network Anomaly Detection. For more information, see **Configure syslog protocol for system events**
- **Log File Protocol** - Event collection using the log file protocol allows you to collect audit events written to a file by the audit.pl script. The log file protocol import and parses the file containing audit events on a schedule you specify in QRadar Network Anomaly Detection. For more information, see **Configure the log file protocol for audit events**.

Configure syslog protocol for system events

The IBM AIX DSM for IBM Security QRadar Network Anomaly Detection accepts system events from IBM AIX using syslog.

QRadar Network Anomaly Detection records all relevant login, logoff, session opened, session closed, and accepted/failed password events. If you are using syslog on a UNIX host, we recommend that you upgrade the standard syslog to a more recent syslog forwarder, such as, syslog-ng.

- To configure syslog events in IBM AIX, see **Configure syslog**.
- To configure a log source in QRadar Network Anomaly Detection, see **Configure a log source**.

Configure syslog

To configure syslog forwarding for IBM AIX:

Step 1 Log in to your IBM AIX system as a root user.

Step 2 Open the **/etc/syslog.conf** file.

Step 3 Forward the system authentication logs to QRadar Network Anomaly Detection by adding the following line to the file:

```
auth.info            @<IP address>
```

Where **<IP address>** is the IP address of the QRadar Network Anomaly Detection.

Note: A tab is required between **auth.info** and **@<IP address>** to configure syslog for IBM AIX.

For example,

```
##### begin /etc/syslog.conf
mail.debug /var/adm/maillog
mail.none /var/adm/maillog
auth.notice /var/adm/authlog
lpr.debug /var/adm/lpd-errs
kern.debug /var/adm/messages
*.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info
/var/adm/messages
auth.info            @<10.100.100.1>
##### end /etc/syslog.conf
```

Step 4 Save and exit the file.

Step 5 Restart syslog:

```
refresh -s syslogd
```

After the syslog server restarts, the configuration is complete. QRadar Network Anomaly Detection automatically discovers syslog events forwarded from IBM AIX.

Configure a log source

QRadar Network Anomaly Detection automatically discovers and creates a log source for syslog events from IBM AIX. The following configuration steps are optional.

To manually configure a syslog log source for IBM AIX:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **IBM AIX Server**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 7-1 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 AIX.

Step 11 Click **Save**.

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

The configuration is complete.

Configure the log file protocol for audit events

The log file protocol reads events created from the audit.pl script by converting binary logs on your IBM AIX server in to single line events that are readable by QRadar Network Anomaly Detection.

The audit.pl script should be schedule to run each time you want to convert your audit logs to a readable format. The audit script determines which audit logs to read based on the configuration of your auditing configuration in the /etc/security/audit/config file on your IBM AIX server. This allows you to determine which classes and folders are read by the script and written to an event file on your system. The log file protocol then retrieves the event file and imports the events to QRadar Network Anomaly Detection.

Note: We recommend that you configure auditing as defined in your IBM AIX Server documentation. As auditing all events can produce a large volume of data.

Configure auditing in IBM AIX

Step 1 Edit the following audit configuration file on your IBM AIX server to determine the folders and classes that are required for auditing:

```
/etc/security/audit/config
```

Step 2 In the Start section of the audit file, edit the configuration to enable binmode.

For example,

```
binmode = on
```

Step 3 In the Start section of the audit file, edit the configuration to determine which directories contain the binary audit logs.

In most cases, you do not have to edit the binary file (bin1 and bin2) directories.

For example, the default configuration for IBM AIX auditing writes binary logs to the following directories:

```
trail = /audit/trail
bin1 = /audit/bin1
bin2 = /audit/bin2
binsize = 10240
cmds = /etc/security/audit/bincmds
```

Step 4 In the Classes section of the audit file, edit the configuration to determine which classes are audited.

For information on configuring classes, see your IBM AIX documentation.

CAUTION: *The default classes configured in IBM AIX captures a large number of audit events. We recommend you configure the classes in the audit configuration on your IBM AIX system to prevent performance issues.*

Step 5 Save the auditing configuration changes.

Step 6 Type the following command to start auditing on your IBM AIX system:

```
audit start
```

Configure the audit script

To configure IBM AIX for auditing:

Step 1 From the Qmmunity website or *http://www.ibm.com/support*, download the following archive file:

```
audit.pl.gz
```

Step 2 Copy the audit script to a folder on your IBM AIX server.

Note: The audit.pl script requires a minimum version of Perl 5.8 installed on your IBM AIX server.

Step 3 Type the following command to extract the file:

```
tar -zxvf audit.pl.gz
```

Step 4 Type the following command and include any additional command parameters to start the audit script:

```
./audit.pl
```

Table 7-2 Command Parameters

Parameters	Description
-r	The -r parameter defines the results directory where the audit script writes the event files that have been converted in to a format readable by QRadar Network Anomaly Detection. If you do not specify a results directory, the script writes the events to the following directory: **`/audit/results/`** The directory you specift for your audit result files is required in the **Remote Directory** field when you configure a log source using the log file protocol. ***Note:*** *To prevent errors, you must verify that any directory you specify exists on your IBM AIX system.*
-n	The -n parameter renames the audit files processed by the script. By default, audit files are processed as **`AIX_AUDIT_<timestamp>`**. The value you specify using the -n parameter must also be configured in the **FTP File Pattern** field when you configure a log source using the log file protocol.
-l	The -l parameter defines the name of the last record file. By default, the last record file is named lastrecord.txt. The last record file is used by the script to determine the last event processed by the audit script. The last record file ensures the audit script processes events where it left off and prevents duplicate events from being added to the results file.
-m	The -m parameter defines the maximum number of audit files to retain on your IBM AIX system. By default, the script keeps 30 audit files. When the number of audit files exceeds the value of the -m parameter, the script deletes the audit file with the oldest timestamp.
-t	The -t parameter defines the directory that contains the audit trail file. The default is /audit/trail.
-h	The -h parameter displays the help and usage information.
-v	The -v parameter displays the script version information.

The script converts the binary audit records to event files readable by QRadar Network Anomaly Detection. The configuration is complete.

Note: We recommend you configure a cronjob for the audit.pl script. Adding **`0 * * * * /audit.pl`** allows the audit script to run hourly. Any configuration parameters required must be added after you specify audit.pl. For more information, see your system documentation.

You are now ready to configure a log source for IBM AIX in QRadar Network Anomaly Detection.

Configure a log source

A log file protocol source allows QRadar Network Anomaly Detection to retrieve archived audit log files from a remote host.

The IBM AIX DSM supports the bulk loading of log files using the log file protocol source. When configuring your IBM AIX to use the log file protocol, make sure the log file protocol is reading the archived audit log.

You are now ready to configure the log source and protocol in QRadar Network Anomaly Detection:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **IBM AIX Audit**.

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

Step 10 Configure the following values:

Table 7-3 IBM AIX Audit 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 QRadar Network Anomaly Detection to identify a log file to a unique event source.
Service Type	From the list box, 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 7-3 IBM AIX Audit 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 IBM AIX.
Confirm Password	Confirm the password necessary to log in to IBM AIX.
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 7-3 IBM AIX Audit 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 AIX_Audit_<timestamp>.gz The FTP file pattern you specify must match the name you assigned to your AIX audit files by the -n parameter of the audit script. For example, to collect files starting with AIX_AUDIT and ending with your timestamp value, type the following: **`AIX_Audit_*`** 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 box, 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 7-3 IBM AIX Audit Log File Parameters (continued)

Parameter	Description
Processor	From the list box, select **NONE**. Processors allow event file archives to be expanded and contents processed for events. Files are only processed after they are downloaded. QRadar Network Anomaly Detection 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. QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection 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 box, 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.

Step 11 Click **Save**.

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

The configuration is complete. As the log file protocol retrieves events, they are displayed on the **Log Activity** tab of QRadar Network Anomaly Detection.

IBM AS/400 iSeries

IBM Security QRadar Network Anomaly Detection 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** - 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 QRadar Network Anomaly Detection using the Log File protocol source.

  For more information, see **Integrating an IBM AS/400 iSeries DSM**.

  For more information on configuring log sources and protocols, see **Pulling Data Using Log File Protocol**.

- **LogAgent for System i** - Accepts all Common Event Format (CEF) formatted syslog messages. You can integrate an IBM OS/400 device and above 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**.

- **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.

  For more information, see your PowerTech Interact documentation.

- **Raz-Lee iSecurity** - Accepts iSecurity formatted events using the Log Enhanced Event Format protocol (LEEF). After you configure your iSecurity software, the syslog events are automatically discovered by QRadar Network Anomaly Detection. For more information, see **Configure Raz-Lee iSecurity**.

Integrating an IBM AS/400 iSeries DSM

The QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection can retrieve the records using FTP.

To integrate IBM iSeries events into QRadar Network Anomaly Detection:

Step 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 QRadar Network Anomaly Detection.

Step 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.

Step 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**.

Configure an IBM iSeries to integrate with QRadar Network Anomaly Detection

To integrate an IBM iSeries with QRadar Network Anomaly Detection:

Step 1 From the Qmmunity website or *http://www.ibm.com/support*, download the following files:

AJLIB.SAVF

Step 2 Copy the **AJLIB.SAVF** file onto a computer or terminal that has FTP access to the IBM AS/400 iSeries.

Step 3 Create a generic online SAVF file on the iSeries using the command:

CRTSAVF QGPL/SAVF

Step 4 Using FTP on the computer or terminal, replace the iSeries generic **SAVF** with the **AJLIB.SAVF** file downloaded from Qmmunity or *http://www.ibm.com/support*:

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.

Step 5 Restore the AJLIB library on the IBM iSeries:

RSTLIB

Step 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.

Step 7 Run **AJLIB/DATETIME.**

This updates the IBM AS/400 iSeries with the data collection start date and time if you made changes.

Step 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 QRadar Network Anomaly Detection:

Step 1 To configure QRadar Network Anomaly Detection to receive events from an IBM AS/400 iSeries, you must select the **IBM AS/400 iSeries** option from the **Log Source Type** list box.

Step 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 box 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 box.

Step 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 *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*.

Configure Raz-Lee iSecurity

The Raz-Lee iSecurity for System i user interface allows detailed security audits of systems for compliance and securing iSeries infrastructure. You can integrate QRadar Network Anomaly Detection to read iSecurity events using the Log

Enhanced Event Protocol (LEEF). Before configuring your device in QRadar Network Anomaly Detection, you must:

1. Configure the Raz-Lee iSecurity user interface to forward syslog events to QRadar Network Anomaly Detection. For more information, see **Configure iSecurity to Forward Syslog Events**.
2. Configure the log source in QRadar Network Anomaly Detection. For more information, see **Configure a log source**.

Configure iSecurity to Forward Syslog Events

To integrate the device with QRadar Network Anomaly Detection:

Step 1 Log in to the IBM System i command-line interface.

Step 2 Type the following command to access the audit menu options:

```
STRAUD
```

Step 3 From the Audit menu, select **81. System Configuration**.

The iSecurity/Base System Configuration window is displayed.

Step 4 From the iSecurity/Base System Configuration menu, select **31. SYSLOG Definitions**.

The SYSLOG Definitions window is displayed.

Step 5 Configure the following parameters:

a. **Send SYSLOG message** - Select **Yes**.

b. **Destination address** - Type the IP address of QRadar Network Anomaly Detection.

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.

Step 6 You are now ready to configure the log source in QRadar Network Anomaly Detection.

Configure a log source

You are now ready to configure the log source in QRadar Network Anomaly Detection. QRadar Network Anomaly Detection automatically detects syslog events from iSecurity on the System i. If you want to manually configure QRadar Network Anomaly Detection to receive events from a System i device:

- From the **Log Source Type** list box, select the **IBM iSecurity** option.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about Raz-Lee iSecurity, see your vendor documentation.

IBM Proventia Management SiteProtector

The IBM Proventia® Management SiteProtector™ DSM for IBM Security QRadar Network Anomaly Detection accepts SiteProtector events by polling the SiteProtector database.

The DSM allows QRadar Network Anomaly Detection 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 IBM Security QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection to integrate with SiteProtector, we recommend you create a database user account and password in SiteProtector for QRadar Network Anomaly Detection. Your QRadar Network Anomaly Detection user must have read permissions for the SensorData1 table, which stores SiteProtector events. The JDBC - SiteProtector protocol allows QRadar Network Anomaly Detection to log in and poll for events from the database. Creating a QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection.

Configure a log source

To configure QRadar Network Anomaly Detection to poll for IBM SiteProtector events:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

The Data Sources panel is displayed.

Step 3 Click the **Log Sources** icon.

The Log Sources window is displayed.

Step 4 Click **Add**.

The Add a log source window is displayed.

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

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

Step 7 Select the **IBM Proventia Management SiteProtector** option from the **Log Source Type** list box.

Step 8 Using the **Protocol Configuration** list box, select **JDBC - SiteProtector**.

The JDBC - SiteProtector protocol configuration is displayed.

Step 9 Configure the following values:

Table 7-4 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: **<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 box, 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**. 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 server.

Table 7-4 JDBC 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 QRadar Network Anomaly Detection. 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 table or view that includes the event records. The default table name is **`SensorData1.`** 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(.).

Table 7-4 JDBC 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 ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **`SensorDataRowID`** to identify new events added between queries to the table. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), 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.
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.
Include Audit Events	Select this check box to collect audit events from IBM SiteProtector. By default, this check box is clear.
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.

Step 10 Click **Save**.

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

The configuration is complete.

IBM ISS Proventia

The IBM Integrated Systems Solutions® (ISS) Proventia DSM for IBM Security QRadar Network Anomaly Detection records all relevant IBM Proventia® events using SNMP.

To configure IBM Proventia:

Step 1 In the Proventia Manager user interface navigation pane, expand the System node.

Step 2 Select **System**.

Step 3 Select **Services**.

The Service Configuration page is displayed.

Step 4 Click the **SNMP** tab.

Step 5 Select **SNMP Traps Enabled**.

Step 6 In the **Trap Receiver** field, type the IP address of your QRadar Network Anomaly Detection you wish to monitor incoming SNMP traps.

Step 7 In the **Trap Community** field, type the appropriate community name.

Step 8 From the **Trap Version** list, select the trap version.

Step 9 Click **Save Changes**.

You are now ready to configure QRadar Network Anomaly Detection to receive SNMP traps.

To configure QRadar Network Anomaly Detection to receive events from an ISS Proventia device:

- From the **Log Source Type** list box, select **IBM Proventia Network Intrusion Prevention System (IPS)**.

For information on configuring SNMP in the QRadar Network Anomaly Detection, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about your ISS Proventia device, see your vendor documentation.

IBM Security Network Protection (XGS)

The IBM Security Network Protection (XGS) DSM accepts events by using the Log Enhanced Event Protocol (LEEF), enabling QRadar Network Anomaly Detection to record all relevant events.

Before you configure an Network Security Protection (XGS) appliance in QRadar Network Anomaly Detection, you must configure remote syslog alerts for your IBM

Security Network Protection (XGS) rules or policies to forward events to QRadar Network Anomaly Detection.

Supported event types

IBM Security Network Protection (XGS) appliances provides three types of event to QRadar Network Anomaly Detection:

- System events
- Access events
- Security events

To integrate the device with QRadar Network Anomaly Detection see the Network Security Protection (XGS) online documentation: *http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.alps.doc/tasks/alps_configuring_system_alerts.htm.*

Configure IBM Security Network Protection (XGS) Alerts

All event types are sent to QRadar Network Anomaly Detection 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:

Step 1 Click **New > Alert > Remote Syslog**.

Step 2 Select an existing remote syslog alert object, and then click **Edit**.

Step 3 Configure the following options:

Table 7-1 Syslog Configuration Parameters

Option	Description
Name	Type a name for the syslog alert configuration.
Remote Syslog Collector	Type the IP address of your QRadar Network Anomaly Detection Console or Event Collector.
Remote Syslog Collector Port	Type **514** for the Remote Syslog Collector Port.

Table 7-1 Syslog Configuration Parameters (continued)

Option	Description
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.

Step 4 Click **Save Configuration**.

The alert is added to the Available Objects list.

Step 5 Click **Deploy** to update your IBM Security Network Protection (XGS) appliance.

The remote syslog alert object you created is now ready to be added to your system, access, or security policies to forward events to QRadar Network Anomaly Detection

Step 6 To make your IBM Security Network Protection (XGS) device send an event to QRadar Network Anomaly Detection, you must:

- Add the LEEF alert object for QRadar Network Anomaly Detection to one or more rules in a policy.
- Add the LEEF alert object for QRadar Network Anomaly Detection to the Added Objects pane n the System Alerts page.

Step 7 Click **Deploy** to update your IBM Security Network Protection (XGS) appliance.

Further support information about the Network Security Protection (XGS) device can be found by clicking help in the Network Security Protection (XGS) local management interface browser client window or by accessing the online Network Security Protection (XGS) documentation.

The configuration is complete. The log source is added to QRadar Network Anomaly Detection as events IBM Security Network Protection (XGS) are automatically discovered. Events forwarded to QRadar Network Anomaly Detection by IBM Security Network Protection (XGS) are displayed on the **Log Activity** tab of QRadar Network Anomaly Detection.

Configuring a Log Source in QRadar Network Anomaly Detection

QRadar Network Anomaly Detection automatically discovers and creates a log source for LEEF-enabled syslog events from IBM Security Network Protection (XGS). The following configuration steps are optional.

To manually configure a log source:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

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

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

Step 8 From the **Log Source Type** list box, select **IBM Security Network Protection (XGS)**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 7-1 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).

Step 11 Click **Save**.

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

The configuration is complete.

8 JUNIPER NETWORKS SECURE ACCESS

The Juniper Networks Secure Access DSM for IBM Security QRadar Network Anomaly Detection accepts login and session information using syslog in WebTrends Enhanced Log File (WELF) format. You can integrate Juniper SA and Juniper IC with QRadar Network Anomaly Detection.

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**.
- Syslog. See **Use the syslog format**.

Use the WELF:WELF format

To integrate a Juniper Networks Secure Access device with QRadar Network Anomaly Detection using the WELF:WELF format:

Step 1 Log in to your Juniper device administration user interface:

`https://10.xx.xx.xx/admin`

Step 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**.

The Filter menu is displayed.

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 box, select the facility.

j From the **Filter** list box, select **WELF:WELF**.

k Click **Add**, then click **Save Changes**.

Step 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**.

The Filter menu is displayed.

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 box, select the facility.

i From the **Filter** list box, select **WELF:WELF**.

j Click **Add** and click **Save Changes.**

Step 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**.

The Filter menu is displayed.

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 box, select the facility.

j From the **Filter** list box, select **WELF:WELF**.

k Click **Add**, then click **Save Changes**.

Step 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 box, select the facility.

i From the **Filter** list box, select **WELF:WELF**.

j Click **Add**, then click **Save Changes**.

Step 6 You are now ready to configure the log source in QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection to receive events from Juniper Networks Secure Access device:

- From the **Log Source Type** list box, select **Juniper Networks Secure Access (SA) SSL VPN**.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about your Juniper device, see your vendor documentation.

Use the syslog format

To integrate a Juniper Networks Secure Access device with QRadar Network Anomaly Detection using syslog:

Step 1 Log in to your Juniper device administration user interface:

```
https://10.xx.xx.xx/admin
```

Step 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.

Step 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.

Step 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.

Step 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 QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection to receive events from Juniper Networks Secure Access device:

- From the **Log Source Type** list box, select **Juniper Networks Secure Access (SA) SSL VPN**.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about your Juniper device, see your vendor documentation.

9 LINUX DHCP

The Linux DHCP Server DSM for IBM Security QRadar Network Anomaly Detection accepts DHCP events using syslog.

QRadar Network Anomaly Detection records all relevant events from a Linux DHCP Server. Before you configure QRadar Network Anomaly Detection to integrate with a Linux DHCP Server, you must configure syslog within your Linux DHCP Server to forward syslog events to QRadar Network Anomaly Detection.

For more information on configuring your Linux DHCP Server, consult the man pages or associated documentation for your DHCP daemon.

QRadar Network Anomaly Detection automatically discovers and creates log sources for syslog events forwarded from Linux DHCP Servers. The following configuration steps for creating a log source are optional.

To manually create a log source in QRadar Network Anomaly Detection:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

The Data Sources panel is displayed.

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

The Log Sources window is displayed.

Step 5 Click **Add**.

The Add a log source window is displayed.

Step 6 In the **Log Source Name** field, type a name for your Linux DHCP Server.

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

Step 8 From the **Log Source Type** list box, select **Linux DHCP Server**.

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

The syslog protocol configuration is displayed.

Step 10 Configure the following values:

Table 9-1 Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from your Linux DHCP Server.

Step 11 Click **Save**.

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

The configuration is complete.

10 MICROSOFT

This section provides information on the following DSMs:

- **Microsoft DHCP Server**
- **Microsoft Windows Security Event Log**

Microsoft DHCP Server

The Microsoft DHCP Server DSM for IBM Security QRadar Network Anomaly Detection accepts DHCP events using the Microsoft DHCP Server protocol or the Adaptive Log Exporter.

Configure your Microsoft DHCP Server

Before you can integrate your Microsoft DHCP Server with QRadar Network Anomaly Detection, you must enable audit logging.

To configure the Microsoft DHCP Server:

Step 1 Log in to the DHCP Server Administration Tool.

Step 2 From the DHCP Administration Tool, right-click on the DHCP server and select **Properties**.

The Properties window is displayed.

Step 3 Click the **General** tab.

The General panel is displayed.

Step 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 10-2 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.

Step 5 Restart the DHCP service.

You are now ready to configure the log source and protocol in QRadar Network Anomaly Detection:

Step 1 To configure QRadar Network Anomaly Detection to receive events from a Microsoft DHCP Server, you must select the **Microsoft DHCP Server** option from the **Log Source Type** list box.

Step 2 To configure the protocol, you must select the **Microsoft DHCP** option from the **Protocol Configuration** list box. For more information on configuring the Microsoft DHCP protocol, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*.

Note: To integrate Microsoft DHCP Server versions 2000/2003 with QRadar Network Anomaly Detection using the Adaptive Log Exporter Microsoft DHCP devices, see the Adaptive Log Exporter Users Guide.

Microsoft Windows Security Event Log

The Microsoft Windows Security Event Log DSM for IBM Security QRadar Network Anomaly Detection accepts Windows-based events using syslog.

You can integrate Window Microsoft Security Event Log events with QRadar Network Anomaly Detection 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 Adaptive Log Exporter. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.
- Use the Microsoft Security Event Log protocol to collect events using WMI. For more information, see **Using WMI**
- Set-up the Snare Agent to forward Microsoft Windows Security Event Logs to QRadar Network Anomaly Detection. See **Using the Snare Agent**

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 QRadar Network Anomaly Detection (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 QRadar Network Anomaly Detection:

Step 1 To configure QRadar Network Anomaly Detection to receive events from Windows security event logs, you must select the **Microsoft Windows Security Event Log** option from the **Log Source Type** list box.

Step 2 To configure the Windows Event Log protocol, you must select the **Microsoft Security Event Log** option from the **Protocol Configuration** list box. 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 QRadar Network Anomaly Detection:

Step 1 Download and install the Snare Agent.

Note: To download a Snare Agent, see the following website: http://www.intersectalliance.com/projects/SnareWindows/index.html

Step 2 On the navigation menu, select **Network Configuration**.

Step 3 Type the IP address of the QRadar Network Anomaly Detection system in the **Destination Snare Server** address field.

Step 4 Select the **Enable SYSLOG Header** check box.

Step 5 Click **Change Configuration**.

Step 6 On the navigation menu, select **Objectives Configuration**.

Step 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 QRadar Network Anomaly Detection.

The Microsoft Windows Event Log DSM supports Informational, Warning, Error, Success Audit, and Failure Audit event types.

Step 8 In the **Identify the event logs** field, select check boxes to define the event logs you want snare to forward to QRadar Network Anomaly Detection.

The Microsoft Windows Event Log DSM supports Security, System, Application, DNS Server, File Replication and Directory Service log types.

Step 9 Click **Change Configuration**.

Step 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 QRadar Network Anomaly Detection setup.

You are now ready to configure the log source in QRadar Network Anomaly Detection:

Step 1 To configure QRadar Network Anomaly Detection to receive events from Windows security event logs, you must select the **Microsoft Windows Security Event Log** option from the **Log Source Type** list box.

Step 2 To configure the Windows Event Log protocol, you must select the **Microsoft Security Event Log** option from the **Protocol Configuration** list box. 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 *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about your server, see your vendor documentation.

11 NORTEL NETWORKS

This section provides information on the following DSMs:

- **Nortel Secure Network Access Switch**
- **Nortel VPN Gateway**

Nortel Secure Network Access Switch

A QRadar Network Anomaly Detection Nortel Secure Network Access Switch (SNAS) DSM records all relevant switch events using syslog.

Before configuring a Nortel SNAS device in QRadar Network Anomaly Detection, you must:

Step 1 Log in to the Nortel SNAS user interface.

Step 2 Select the **Config** tab.

Step 3 Select **Secure Access Domain** and **Syslog** from the Navigation pane.

The Secure Access Domain window is displayed.

Step 4 From the Secure Access Domain list, select the secure access domain. Click **Refresh**.

Step 5 Click **Add**.

The Add New Remote Server window is displayed.

Step 6 Click **Update**.

The server is displayed in the secure access domain table.

Step 7 Using the toolbar, click **Apply** to send the current changes to the Nortel SNAS.

Step 8 You are now ready to configure the log source in QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection to receive events from a Nortel SNAS device:

- From the **Log Source Type** list box, select the **Nortel Secure Network Access Switch (SNAS)** option.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*.

For more information about the Nortel SNA, see *http://www.nortel.com/support*.

Nortel VPN Gateway

The IBM Security QRadar Network Anomaly Detection Nortel VPN Gateway DSM accetps events using syslog.

QRadar Network Anomaly Detection 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 QRadar Network Anomaly Detection, you must configure your device to send syslog events to QRadar Network Anomaly Detection.

To configure the device to send syslog events to QRadar Network Anomaly Detection:

Step 1 Log in to the Nortel VPN Gateway command-line interface (CLI).

Step 2 Type the following command:

```
/cfg/sys/syslog/add
```

Step 3 At the prompt, type the IP address of your QRadar Network Anomaly Detection system:

```
Enter new syslog host: <IP address>
```

Where **<IP address>** is the IP address of your QRadar Network Anomaly Detection system.

Step 4 Apply the configuration:

```
apply
```

Step 5 View all syslog servers currently added to your system configuration:

```
/cfg/sys/syslog/list
```

Step 6 You are now ready to configure the log source in QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection to receive events from a Nortel VPN Gateway device:

- From the **Log Source Type** list box, select the **Nortel VPN Gateway** option.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about the Nortel VPN Gateway, see *http://www.nortel.com/support*.

12 SUN SOLARIS DHCP

The Sun Solaris DHCP DSM for IBM Security QRadar Network Anomaly Detection records all relevant DHCP events using syslog.

To configure syslog for Solaris DHCP:

Step 1 Log in to the Sun Solaris command-line interface.

Step 2 Open the **/etc/default/dhcp** file.

Step 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.

Step 4 Save and exit the file.

Step 5 Open the **/etc/syslog.conf** file.

Step 6 To forward system authentication logs to QRadar Network Anomaly Detection, 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 QRadar Network Anomaly Detection. Use tabs instead of spaces to format the line.

Step 7 Save and exit the file.

Step 8 Type the following command:

kill -HUP `cat /etc/syslog.pid`

You are now ready to configure the log source in QRadar Network Anomaly Detection.

To configure QRadar Network Anomaly Detection to receive events from a Solaris device:

- From the **Log Source Type** list box, select the **Solaris Operating System DHCP Logs** option.

For more information on configuring log sources, see the *IBM Security QRadar Network Anomaly Detection Log Sources User Guide*. For more information about Solaris, see your vendor documentation.

13 UNIVERSAL DSM

QRadar 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 QRadar to properly parse and classify the event messages from the respective devices. After the events from a device have been parsed by the DSM, QRadar 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 QRadar. QRadar 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 *IBM Security QRadar 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.

Note: For more information on writing and testing a Universal DSM, see our Qmmunity forum at *https://qmmunity.q1labs.com/* or *http://www.ibm.com/support*.

14 SUPPORTED DSMS

Table 14-1 provides information on the DSMs supported for IBM Security QRadar Network Anomaly Detection.

IBM Security QRadar Network Anomaly Detection integrates with many manufacturers and vendors of security products. Our list of supported DSMs and documentation is constantly increasing. If your device or appliance is not listed in this document, contact your sales representative.

Table 14-1 Supported DSMs

Manufacturer	DSM	Version	Events Accepted	QRadar Network Anomaly Detection Recorded Events	Option in QRadar Network Anomaly Detection	Auto Discovered	Includes Identity	For More Information
Array Networks	SSL VPN	ArraySP v7.3	Syslog	All relevant events	Array Networks SSL VPN Access Gateways	No	Yes	http://www.arraynetworks.net
Cisco	NAC Appliance	v4.x and above	Syslog	All relevant audit, error, failure, quarantine, and infected events	Cisco NAC Appliance	No	No	http://www.cisco.com
Cisco	VPN 3000 Concentrator	VPN 3005, 4.1.7.H	Syslog	All relevant events	Cisco VPN 3000 Series Concentrator	Yes	Yes	http://www.cisco.com
IBM	AIX	5.x and 6.x	Syslog, Log File Protocol	All relevant events	IBM AIX Server	Yes	Yes	http://www.ibm.com
IBM	AS/400 iSeries DSM	V5R3 and above	Log File Protocol	All relevant events	IBM AS/400 iSeries	No	Yes	http://www.ibm.com
IBM	AS/400 iSeries - Robert Townsend Security Solutions	V5R1 and above	Syslog	All CEF formatted messages	IBM AS/400 iSeries	Yes	Yes	http://www.ibm.com http://www.patownsend.com

Table 14-1 Supported DSMs (continued)

Manufacturer	DSM	Version	Events Accepted	QRadar Network Anomaly Detection Recorded Events	Option in QRadar Network Anomaly Detection	Auto Discovered	Includes Identity	For More Information
IBM	AS/400 iSeries - Powertech Interact	V5R1 and above	Syslog	All CEF formatted messages	IBM AS/400 iSeries	Yes	Yes	http://www.ibm.com http://www.powertech.com
IBM	AS/400 iSeries - Raz-Lee iSecurity	Firewall 15.7 and Audit 11.7	Syslog	All relevant events	IBM AS/400 iSeries	Yes	Yes	http://www.ibm.com http://www.razlee.com
IBM	ISS Proventia	M10 v2.1_2004 .1122_15. 13.53	SNMP	All relevant events	IBM Proventia Network Intrusion Prevention System (IPS)	No	No	http://www.ibm.com
IBM	Proventia Management SiteProtector	v2.0 and v2.9	JDBC	All relevant IPS and audit events	IBM Proventia Management SiteProtector	No	No	http://www.ibm.com
IBM	Security Network Protection (XGS)	v5.0 with fixpack 7	Syslog	All relevant system, access, and security events	IBM Security Network Protection (XGS)	Yes	No	http://www.ibm.com
Juniper Networks	Secure Access RA	Juniper SA version 6.1R2 and Juniper IC version 2.1	Syslog	All relevant events	Juniper Networks Secure Access (SA) SSL VPN	Yes	Yes	http://www.juniper.net
Linux	DHCP Server	v2.4 and above	Syslog	All relevant events from a DHCP server	Linux DHCP Server	Yes	Yes	

Table 14-1 Supported DSMs (continued)

Manufacturer	DSM	Version	Events Accepted	QRadar Network Anomaly Detection Recorded Events	Option in QRadar Network Anomaly Detection	Auto Discovered	Includes Identity	For More Information
Microsoft	Microsoft Windows Event Security Log	2000, 2003, 2008, XP, Vista, and Windows 7 (32 or 64-bit systems supported)	Syslog or Microsoft Windows Event Log Protocol Source	All relevant events	Microsoft Windows Security Event Log	Yes	Yes	http://www.microsoft.com
Microsoft	DHCP Server	2000/2003	Syslog	All relevant events	Microsoft DHCP Server	Yes	Yes	http://www.microsoft.com
Nortel	VPN Gateway	v6.0, 7.0.1 and above, v8.x	Syslog	All relevant events	Nortel VPN Gateway	Yes	Yes	http://www.nortel.com
Nortel	Secure Network Access Switch	v1.6 and v2.0	Syslog	All relevant events	Nortel Secure Network Access Switch (SNAS)	Yes	Yes	http://www.nortel.com
Sun	Solaris DHCP	v2.8	Syslog	All relevant events	Solaris Operating System DHCP Logs	Yes	Yes	http://www.sun.com
Universal	Syslog and SNMP		Syslog, SNMP, or SDEE	All relevant events	Universal DSM	No	Yes	
Universal	Authentication Server		Syslog	All relevant events	Configurable Authentication message filter	No	Yes	
Universal	Firewall		Syslog	All relevant events	Configurable Firewall Filter	No	No	

* These devices are auto discovered as Cisco IOS devices.
** These devices are auto discovered as a Juniper JunOS Platform devices.
*** PCAP Syslog Combination protocol is only available on the Juniper Networks SRX Series appliance.

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX