IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

Log Sources User Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 93.

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar Network Anomaly Detection Log Sources User Guide* provides you with information for configuring log sources and the associated protocols in QRadar Network Anomaly Detection.

Log Sources enable you to integrate events and logs from external devices (Device Support Modules (DSMs)) with QRadar Network Anomaly Detection and QRadar Log Manager. All references to QRadar Network Anomaly Detection or QRadar Network Anomaly Detection is intended to refer to the other products that support log sources, such as QRadar Network Anomaly Detection or IBM Security QRadar Log Manager.

Intended audience

This guide is intended for the system administrator responsible for setting up QRadar Network Anomaly Detection in your network. This guide assumes that you have QRadar Network Anomaly Detection 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 Network Anomaly Detection 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 MANAGE LOG SOURCES

You can configure IBM Security QRadar Network Anomaly Detection or IBM Security QRadar Log Manager to log and correlate events received from external sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers).

Log sources allow you to integrate QRadar Network Anomaly Detection or QRadar Log Manager with these external devices. Unless otherwise noted, all references to QRadar Network Anomaly Detection in this guide refer to both QRadar Network Anomaly Detection and QRadar Log Manager.

Note: Information found in this documentation about configuring log sources is based on the latest RPM files located on the Qmmunity website located at *https://qmmunity.q1labs.com/* or *http://www.ibm.com/support*.

This section provides information on the following:

Configure QRadar Network Anomaly Detection to receive events

QRadar Network Anomaly Detection automatically discovers many log sources in your deployment that are sending syslog messages.

Any log sources that are automatically discovered by QRadar Network Anomaly Detection appear in the Log Sources window. You can configure automatically discovered log sources on a per Event Collector basis using the Autodetection Enabled parameter in the Event Collector configuration. For more information, see the *IBM Security QRadar Network Anomaly Detection Administration Guide, Using the Deployment Editor.*

Note: For more information about auto discovered log sources and configurations specific to your device or appliance, see the *IBM Security QRadar Network Anomaly Detection DSM Configuration Guide*.

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

Step 1 Configure the external Device Support Module (DSM) to send events to QRadar Network Anomaly Detection.

For information on configuring DSMs, see the *IBM Security QRadar Network Anomaly Detection Configuring DSMs Guide* and your vendor documentation.

Step 2 Configure log sources in QRadar Network Anomaly Detection to receive events from the DSMs. See **Manage log sources**.

Note: You must have administrative privileges to configure log sources in QRadar Network Anomaly Detection. For more information on accessing the **Admin** tab, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Manage log sources

A log source provides events to your deployment through DSMs. Using the **Admin** tab, you can:

- View log sources. See **View log sources**.
- Add a log source. See **Add a log source**.
- Edit an existing log source. See **Edit a log source**.
- Enable or disable a log source. See **Enable or disable a log source**.
- Delete a log source. See **Delete a log source**.
- Add a bulk log source. See **Adde multiple log sources**.
- Edit a bulk log source. See **Edit multiple log sources**.

View log sources

To view existing log sources, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

If a log source has not received any events within the configured syslog timeout period, the Status column displays Error. If you manually configure a log source that uses syslog, the Status column displays a status of Error until that log source has received an event. For more information about the Syslog Event Timeout parameter, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Note: Bulk added log sources display N/A in the **Status** column.

Add a log source

To add a log source to your deployment, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

The Log Sources window is displayed.

Step 4 Click **Add**.

Step 5 Type values for the following parameters:

Table 1-1 Add a Log Source Parameters

Parameter	Description
Log Source Name	Type a suitable name of the log source. The name can be up to 255 characters in length.
Log Source Description	Type a description for the log source (optional).
Log Source Type	From the list box, select the type of log source to add.
Protocol Configuration	From the list box, select the protocol configuration for the log source. The Protocol Configuration allows you to define protocol parameters for communication with the log source, such as JDBC, syslog, SNMP, or vendor specific protocols. The available protocols displayed in the Protocol Configuration list box are based on the Log Source Type selected. For information about specific protocols and parameters, see **Configure log source protocols**.
Log Source Identifier	Type an IP address or hostname to identify the log source. The identifier address should be the source device that generated the event. For example, if your network contains multiple devices and a management console, you should specify the IP address of the individual device in the Log Source Identifier field. This allows events forwarded to QRadar Network Anomaly Detection to contain the IP address or hostname of the event source, instead of the management console.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list box, select the Event Collector to use as the target for the log source.

Table 1-1 Add a Log Source Parameters (continued)

Parameter	Description
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** drop-down in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Store Event Payload	Select this check box to enable or disable QRadar Network Anomaly Detection from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** drop-down in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Log Source Extension	The Log Source Extension parameter only appears if you have a log source extension configured in your deployment. Log source extensions allow you to immediately extend the parsing routines of specific log sources, which ensures DSMs send valid data to QRadar Network Anomaly Detection. For more information on log source extensions, see **Manage Log Source Extensions**. From the list box, select the log source extension to use for this log source.

Table 1-1 Add a Log Source Parameters (continued)

Parameter	Description
Extension Use Condition	The Extension Use Condition parameter only appears if you have a log source extension configured in your deployment. For more information on log source extensions, see **Manage Log Source Extensions**. From the list box, select the Extension Use Condition to apply to this log source: • **Parsing Enhancement** - When the DSM is unable to parse correctly and the event is categorized as *stored*, the selected log source extension extends the failing parsing by creating a new event as if the new event came from the DSM. This is the default setting. • **Parsing Override** - When a DSM parses correctly for most fields but needs one or more fields added or modified, the fields specified in the log source extension are overwritten. We recommend that you enable the Parsing Override parameter for Universal DSMs.
Groups	Select one or more groups for the log source.

Step 6 Click **Save**.

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

Edit a log source

To edit a log source, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the log source to edit.

Note: To edit the log source name, log source description, log source identifier, or group of a log source, double-click the log source.

Step 5 Click **Edit**.

Step 6 Edit values for the parameters, as necessary:

Table 1-2 Edit a Log Source Parameters

Parameter	Description
Log Source Name	Type a suitable name of the log source. The name can be up to 255 characters in length.
Log Source Description	Type a description for the log source (optional).
Log Source Type	From the list box, select the type of log source to add.

Table 1-2 Edit a Log Source Parameters (continued)

Parameter	Description
Protocol Configuration	From the list box, select the protocol to use for this log source. Only the protocols that are available for the selected Log Source Type appear in the list. The required configuration parameters appear. For more information about protocol parameters, see **Configure log source protocols**.
Log Source Identifier	Type an IP address or hostname to identify the log source. The identifier address should be the source device that generated the event. For example, if your network contains multiple devices and a management console, you should specify the IP address of the individual device in the Log Source Identifier field. This allows events forwarded to QRadar Network Anomaly Detection to contain the IP address or hostname of the event source, instead of the management console.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list box, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** list box in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Table 1-2 Edit a Log Source Parameters (continued)

Parameter	Description
Store Event Payload	Select this check box to enable or disable storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list box in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Log Source Extension	The Log Source Extension parameter only appears if you have a log source extension configured in your deployment. Log source extensions allow you to immediately extend the parsing routines of specific log sources, which ensures DSMs send valid data to QRadar Network Anomaly Detection. For more information on log source extensions, see **Manage Log Source Extensions**. From the list box, select the log source extension to use for this log source.
Extension Use Condition	The Extension Use Condition parameter only appears if you have a log source extension configured in your deployment. For more information on log source extensions, see **Manage Log Source Extensions**. From the list box, select a use condition to apply to this log source: • **Parsing Enhancement** - When the DSM is unable to parse correctly and the event is categorized as *stored*, the selected log source extension extends the failed parsing by creating a new event as if the new event came from the DSM. This is the default setting. • **Parsing Override** - When a DSM parses correctly for most fields but needs one or more fields added or modified, the fields specified in the log source extension are overwritten. We recommend that you enable the Parsing Override parameter for Universal DSMs.
Groups	Select one or more groups for the log source.

Step 7 Click **Save**.

The changes are saved and the Log Sources window is displayed.

Enable or disable a log source

To enable or disable a log source, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the log source that you want to enable or disable.

Step 5 Click **Enable/Disable**.

When a log source is enabled, the Enabled column indicates true. When a log source is disabled, the **Status** column indicates **Disabled**.

Note: If you cannot enable a log source, you might have exceeded your license restrictions. For more information about your license limits, see the Managing the System section of the *IBM Security QRadar Network Anomaly Detection Administration Guide*. If you require additional license limits, contact your sales representative.

Delete a log source

To delete a log source. perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the log source you want to delete.

You can delete multiple log sources by pressing the Shift key to select multiple log sources.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **OK**.

Adde multiple log sources

You can add multiple log sources to QRadar Network Anomaly Detection that share a configuration protocol.

Log sources allow you to bulk add and configure hosts by uploading a text file, using a domain query, or typing a host name or IP address. A maximum of 500 active hosts or IP addresses can share a single protocol configuration. If you attempt to add more than 500 hosts, an error message is displayed.

To add multiple log sources to your deployment, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Using the **Bulk Actions** list box, select **Bulk Add**.

Step 5 Type values for the parameters, as necessary:

Table 1-3 Adding a Bulk Log Source Parameters

Parameter	Description
Bulk Log Source Name	Type a suitable name for the group or bulk log source. The name can be up to 255 characters in length. ***Note:*** *Adding a bulk log source automatically creates a log source group using the name you input into this field.*
Log Source Type	From the list box, select the type of log source to add.
Protocol Configuration	From the list box, select the protocol to use for this log source. Only the protocols that are available for the selected Log Source Type appear in the list. The required configuration parameters appear. For more information about protocol parameters, see **Configure log source protocols**.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list box, select the credibility of the bulk log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list box, select the Event Collector to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value configured in the **Coalescing Events** list box in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Table 1-3 Adding a Bulk Log Source Parameters (continued)

Parameter	Description
Store Event Payload	Select this check box to enable or disable QRadar Network Anomaly Detection from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list box in the QRadar Network Anomaly Detection Settings window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.
File Upload tab	Enables you to upload a text file containing a maximum of 500 IP addresses or host names of log sources you want to bulk add. The text file should contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters result in an error indicating a log source from the host list could not be added.
Domain Query tab	Enables you to search a domain to add bulk log sources from a domain controller. To search a domain you must add the domain, username, and password before polling the domain for hosts to add. Type values for the following parameters: • **Domain Controller** - Type the IP address of the domain controller. • **Full Domain Name** - Type a valid domain name.
Manual tab	Enables you to manually add an individual IP address or host name to the host list.
Add	The add field is displayed when you have at least one log source in the host list. By default, the check box is selected. Clearing the check box from the add field allows you to ignore a log source. ***Note:*** *You are not required to clear check boxes for log sources that already exist. Duplicate host names or IP addresses are ignored.*

Step 6 Click **Save**.

A summary of the added log sources is displayed.

Step 7 Click **Continue**.

Edit multiple log sources

Log sources that share a common protocol can be edited as a group as they share a configuration.

Note: You can use bulk editing to update host names or IP addresses, but not delete log sources. For more information, see **Delete a log source**.

To edit a bulk log source to your deployment, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select a bulk log source to edit from the list.

You must select one or more bulk log source from your active log sources list for the **Bulk Edit** list box to be available.

Note: To edit the log source name, log source description, log source identifier, or group, double-click the bulk log source.

Step 5 Using the **Bulk Actions** list box, select **Bulk Edit**.

Step 6 Type values for the parameters you want to edit.

For more information, see **Adding a Bulk Log Source Parameters**.

Step 7 Click **Save**.

A summary of the added log sources is displayed.

Step 8 Click **Continue**.

Configure log source protocols

When you select the type of log source from the Log Source Type list box, the protocol options for the selected log source are displayed in the Protocol Configuration list box.

This section provides information on configuring the following protocols:

- **Syslog**
- **JDBC**
- **JDBC - SiteProtector**
- **SNMPv1**
- **SNMPv2**
- **SNMPv3**
- **Log File protocol**
- **Microsoft Security Event Log**
- **Microsoft Security Event Log Custom**
- **Microsoft DHCP**
- **SMB Tail**

- **Forwarded Protocol**
- **TLS Syslog Protocol**

Syslog

To configure the syslog protocol, you must define the IP address or hostname for the device in the Log Source Identifier field.

The identifier address should be the source device providing events to QRadar Network Anomaly Detection. For example, if your network contains multiple devices and a management console, you should specify the IP address of the individual device in the Log Source Identifier field. This allows events forwarded to QRadar Network Anomaly Detection to contain the IP address or hostname of the event source, instead of the management console.

Table 1-4 Syslog Parameters

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

JDBC To configure the JDBC protocol, define values for the following parameters:

Table 1-5 JDBC Parameters

Parameter	Description
Log Source Identifier	Type the log source identifier in the following format: **<database>@<hostname>** or **<table name>|<database>@<hostname>** Where: **<table name>** is the name of the table or view of the database containing the event records. This parameter is optional. If you include the table name, you must include a pipe (|) character and the table name must match the Table Name parameter. **<database>** is the database name, as defined in the Database Name parameter. The database name is a required parameter. **<hostname>** is the hostname or IP address for this log source, as defined in the IP or Hostname parameter. The hostname is a required parameter. The log source identifier must be unique for the log source type.
Database Type	From the list box, select the type of database to use for the event source. The options include MSDE, Postgres, MySQL, Sybase, and Oracle. The default is MSDE.
Database Name	Type the name of the database to which you want to connect. The name can be up to 255 alphanumeric characters in length. The 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.
Port	Type the port number used by the database server. The default displayed depends on the selected Database Type. The valid range is 0 to 65536. The defaults include: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Oracle - 1521 • Sybase - 1521 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. ***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 include underscores (_).

Table 1-5 JDBC Parameters (continued)

Parameter	Description
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 table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type the list of fields to include in the events. You can use a comma separated list or type * for all fields from the table or view. You can use a comma-separated list to define specific fields from the tables or views. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type a numeric value or timestamp field to use 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 following 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.

Table 1-5 JDBC Parameters (continued)

Parameter	Description
Use Prepared Statements	Select this check box to use prepared statements. Prepared statements allow the JDBC protocol source to setup the SQL statement, and then execute the SQL statement numerous 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.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.
Use Named Pipe Communication	If you select MSDE as the database type, select the 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.
Use NTLMv2	If you select MSDE as the Database Type, the **Use NTLMv2** check box is displayed. Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when communicating with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

Install the MySQL Connector/J Driver

IBM Security QRadar Network Anomaly Detection Maintenance Release 3 and above are not installed with a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the platform independent MySQL Connector/J from *http://dev.mysql.com/downloads/connector/j/.*

To install the MySQL JDBC driver:

Step 1 Download the MySQL JDBC driver from the following website:

http://dev.mysql.com/downloads/connector/j/

Step 2 Copy the MySQL Connector/J .zip file or tar.gz file to your QRadar Network Anomaly Detection or your Event Collector.

Step 3 Type the following to extract the .zip file or tar.gz file on your appliance:

- For .zip files: **`gzip -d mysql-connector-java-<version>.zip`**
- For tar.gz files : **`tar -zxvf mysql-connector-java-<version>.tar.gz`**

The extracted .zip or tar.gz contains the file mysql-connector-java-<version>.jar. The extracted files are located in a mysql-connector-java-<version> folder.

Step 4 Navigate to the mysql-connector-java-<version> folder.

Step 5 Type the following to copy the MySQL Connector/J jar to the proper directory:

`cp mysql-connector-java-<version>-bin.jar /opt/qradar/jars`

Step 6 Type the following command to restart Tomcat:

`service tomcat restart`

Step 7 Type the following command to restart the Event Collection System (ECS):

`service ecs restart`

CAUTION: *Restarting the Event Collection System (ECS) service stops all event collection for QRadar Network Anomaly Detection until the service restarts.*

After the service restarts, the installation of the MySQL driver is complete. For more information on installing or using MySQL Connector/J, see http://dev.mysql.com/downloads/connector/j/.

JDBC - SiteProtector

The JDBC - SiteProtector protocol combines information from the SensorData1 and SensorDataAVP1 tables in the creation of the log source payload.

The SensorData1 and SensorDataAVP1 tables are located in the IBM Proventia® Management SiteProtector® database.

Note: The maximum number of rows that the JDBC - SiteProtector protocol can poll in a single query is 30,000 rows.

To configure the JDBC - SiteProtector protocol, define values for the following parameters:

Table 1-6 JDBC Parameters

Parameter	Description
Log Source Identifier	Type the identifier for the log source 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.
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 (_).

Table 1-6 JDBC Parameters (continued)

Parameter	Description
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 ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type **`*`** to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), 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.

Table 1-6 JDBC Parameters (continued)

Parameter	Description
Use Prepared Statements	Select this check box to use prepared statements, which allows the JDBC protocol source to setup the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements. Clear this check box to use an alternative method of querying that does not use pre-compiled statements.
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.

SNMPv1 To configure the SNMPv1 protocol, you must type the IP address for the log source in the Log Source Identifier parameter. The log source identifier must be unique for the log source type.

SNMPv2 To configure the SNMPv2 protocol, define values for the following parameters:

Table 1-7 SNMPv2 Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the SNMPv2 event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.

Table 1-7 SNMPv2 Parameters (continued)

Parameter	Description
Include OIDs in Event Payload	This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs. For more information, see the *DSM Configuration Guide*.

SNMPv3 To configure the SNMPv3 protocol, define values for the following parameters:

Table 1-8 SNMPv3 Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the SNMPv3 event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source.
Authentication Protocol	From the list box, select the algorithm you want to use to authenticate SNMP traps. This parameter is required if you are using SNMPv3. The default is MD5.
Authentication Password	Type the password you want to use to authenticate SNMP. This parameter is required if you are using SNMPv3. The password can be up to 64 characters in length. ***Note:*** *Your authentication password must include a minimum of 8 characters.*
Decryption Protocol	From the list box, select the protocol you want to use to decrypt SNMP traps. This parameter is required if you are using SNMPv3. The default is AES256.
Decryption Password	Type the password used to decrypt SNMP traps. This parameter is required if you are using SNMPv3. The password can be up to 64 characters in length.
User	Type the user access for this protocol. The default is AdminUser. The username can be up to 255 characters in length.

Log File protocol

The log file protocol source allows QRadar Network Anomaly Detection to retrieve archived log files containing events from a remote host.

Log files are transferred, one at a time, to QRadar Network Anomaly Detection for processing. The log file protocol can manage plain text, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. When a protocol source downloads a file for processing, QRadar Network Anomaly Detection processes the information received in the file to generate events. If additional information is written to the file after the download is complete, that information is not processed by QRadar Network Anomaly Detection.

Note: The Log File protocol is intended for files that write daily event logs. It is not recommended to use the Log File protocol for devices that appended additional information to their event files.

To configure the Log File protocol, define values for the following parameters:

Table 1-9 Log File Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source. For example, if your network contains multiple devices, such as a management console or a file repository, you should specify the IP address or hostname of the device that created the event. This allows events to be identified at the device level in your network, instead of identifying the event for the management console or file repository.
Service Type	From the list box, select the protocol you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy ***Note:*** *The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the* ***Remote IP or Hostname*** *field has the SFTP subsystem enabled.*
Remote IP or Hostname	Type the IP address or hostname of the device storing your event log files.

Table 1-9 Log File Parameters (continued)

Parameter	Description
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 ***Note:*** *If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.*
Remote User	Type the user name necessary to log in to the host containing your event files. The username can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. 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. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. For example, if you want to list all files starting with the word log, followed by one or more digits and ending with **`tar.gz`**, use the following entry: **`log[0-9]+\.tar\.gz`**. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: *http://download.oracle.com/javase/tutorial/essential/regex/*

Table 1-9 Log File Parameters (continued)

Parameter	Description
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. From the list box, select the transfer mode you want to apply to this log source: • **Binary** - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • **ASCII** - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when using ASCII as the FTP Transfer Mode.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your QRadar Network Anomaly Detection that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.

Table 1-9 Log File Parameters (continued)

Parameter	Description
Event Generator	The Event Generator applies additional processing to the retrieved event files. From the **Event Generator** list box, select one of the following options: • **LineByLine** - Each line of the file is processed as a single event. For example, if a file has 10 lines of text, 10 separate events are created. • **HPTandem** - The file is processed as a HPTandem/NonStop binary audit log. Each record in the log file (whether primary or secondary) is converted into text and processed as a single event. HPTandem audit logs use the following filename pattern: **"[aA]\d{7}"**. • **WebSphere Application Server** - Processes the log files containing WebSphere Application Server events generated from the WebSphere Application Server DSM. The remote directory must define the file path configured in the DSM. • **W3C** - Processes log files from sources using the w3c format. The header of the log file identifies the order and data contained in each line of the file. • **Fair Warning** - Processes log files from Fair Warning devices protecting patient identity and medical information. The remote directory must define the file path containing the event log files generated by your Fair Warning device. • **DPI Subscriber Data** - The file is processed as a DPI statistic log produced by a Juniper Networks MX router. The header of the file identifies the order and data contained in each line of the file. Each line in the file after the header is formatted to a tab-delimited name=value pair event to be processed by QRadar Network Anomaly Detection. • **SAP Audit Logs** - Process files for SAP Audit Logs to keep a record of security-related events in SAP systems. Each line of the file is formatted to be processed by QRadar Network Anomaly Detection. • **Oracle BEA WebLogic** - Processes files for Oracle BEA WebLogic application log files. Each line of the file is formatted to be processed by QRadar Network Anomaly Detection. • **Juniper SBR** - Processes event log files from Juniper Steel-belted RADIUS. Each line of the file is formatted to be processed by QRadar Network Anomaly Detection.

Microsoft Security Event Log

The Microsoft Security Event Log protocol provides remote agentless Windows event log collection for Windows using the Microsoft Windows Management Instrumentation (WMI) API.

Supported operating systems

QRadar Network Anomaly Detection supports the following Microsoft Windows Management Instrumentation (WMI) API:

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Supported event types

The Microsoft Windows Security Event Log protocol is capable of collecting the following log types:

- Application
- Security
- System
- DNS Server
- File Replication
- Directory Service logs

Before you begin

You must configure your firewall to accept incoming external communications on port 135 and any dynamic ports required for DCOM. For more information on configuring DCOM, see your Microsoft Support documentation.

The following log source limitations apply when deploying the Microsoft Security Event Log Protocol in your environment:

- A QRadar Network Anomaly Detection all-in-one installation can support up to 250 log sources using the Microsoft Security Event Log Protocol.
- A dedicated Event Collector can support up to 500 log sources using the Microsoft Security Event Log Protocol.

Note: The Microsoft Security Event Log protocol is not recommended for remote servers accessed over network links with high round-trip delay times, such as satellite or slow WAN networks. Round-trip delay can be confirmed by examining request and response time between servers using ping. Network delays created by slow connections decrease the EPS throughput available to those remote servers. In addition, event collection from busy servers or Domain Controllers rely on low

round-trip delay times to keep up with incoming events. If it is not possible to decrease your network round-trip delay time, we recommend you consider using the Adaptive Log Exporter or Snare. For more information on the Adaptive Log Exporter, see the Adaptive Log Exporter Users Guide.

Configure the Microsoft Windows Security Event Log protocol

To configure the Microsoft Security Event Log protocol, define values for the following parameters:

Table 1-10 Microsoft Security Event Log Parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname of the Windows host. The log source identifier must be unique for the log source type.
Domain	Type the Windows domain that includes the Windows Machine specified above. This parameter is optional.
User Name	Type the username required to access the Windows host.
Password	Type the password required to access the Windows host.
Confirm Password	Confirm the password required to access the Windows host.
Standard Log Types	Select any check boxes for the Windows log type you want QRadar Network Anomaly Detection to monitor. At least one check box must be selected. The log types include: • Security • System • Application • DNS Server • File Replication Service • Directory Service
Event Types	Select any check boxes for the event type you want QRadar Network Anomaly Detection to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit

Microsoft Security Event Log Custom

The Microsoft Security Event Log protocol provides remote agentless Windows event log collection of customized EVT files using the Microsoft Windows Management Instrumentation (WMI) API.

Supported operating systems

QRadar Network Anomaly Detection supports the following Microsoft Windows Management Instrumentation (WMI) API:

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Supported event types

The Microsoft Security Event Log Custom protocol can process Windows EVT log files and is used in conjunction with the Universal DSM. For information on configuring custom EVT files with events for your Windows operating system, see your Microsoft documentation.

Before you begin

You must configure your firewall to accept incoming external communications on port 135 and any dynamic ports required for DCOM. For more information on configuring DCOM, see your Microsoft Support documentation.

The following log source limitations apply when deploying the Microsoft Security Event Log Custom protocol in your environment:

- A QRadar Network Anomaly Detection all-in-one installation can support up to 250 log sources using the Microsoft Security Event Log Custom protocol.
- A dedicated Event Collector can support up to 500 log sources using the Microsoft Security Event Log Custom protocol.

Note: The Microsoft Security Event Log Custom protocol is not recommended for remote servers accessed over network links with high round-trip delay times, such as satellite or slow WAN networks. Round-trip delay can be confirmed by examining request and response time between servers using ping. Network delays created by slow connections decrease the EPS throughput available to those remote servers. In addition, event collection from busy servers or Domain Controllers rely on low round-trip delay times to keep up with incoming events. If it is not possible to decrease your network round-trip delay time, we recommend you consider using the Adaptive Log Exporter or Snare. For more information on the Adaptive Log Exporter, see the *Adaptive Log Exporter Users Guide*.

Configure the Microsoft Windows Security Event Log Custom protocol

To configure the Windows Event Log Custom protocol, define values for the following parameters:

Table 1-11 Windows Event Log Custom Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the Windows event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source.
Domain	Type the Windows domain that includes the Windows Machine specified above. This parameter is optional.
User Name	Type the username required to access the Windows host.
Password	Type the password required to access the Windows host.
Confirm Password	Confirm the password required to access the Windows host.
Monitored Event Logs	Type the display name of the Windows event logs you want to process. Type multiple event logs in a comma separated list.
Event Types	Select any check boxes for the event type you want QRadar Network Anomaly Detection to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit

Microsoft DHCP

The Microsoft DHCP protocol only supports a single connection to a Microsoft DHCP server.

The Microsoft authentication protocol NTLMv2 Session is not supported in the Microsoft DHCP Log Source. To configure the Microsoft DHCP protocol, define values for the following parameters:

Table 1-12 Microsoft DHCP Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the Microsoft DHCP event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source.
Server Address	Type the IP address of the Microsoft DHCP server.
Domain	Type the domain required to access the Microsoft DHCP server. This parameter is optional.
Username	Type the username required to access the Microsoft DHCP server.
Password	Type the password required to access the Microsoft DHCP server.
Confirm Password	Confirm the password required to access the Microsoft DHCP server.
Folder Path	Type the directory path to access the DHCP log files. The default is **`/WINDOWS/system32/dhcp/.`** Users with NetBIOS access on the administrative share (C$) have the proper access to read DHCP log files in **`/WINDOWS/system32/dhcp/.`** Local or domain administrators have sufficient privileges to access DHCP log files.
File Pattern	Type the regular expression (regex) required to filter the filenames. All matching files are included in the processing. ***Note:*** *Your Microsoft DHCP audit log files must contain a three-character abbreviation for a day of the week.* The default IPv4 file pattern: **`DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** Optional. IPv6 file pattern: **`DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** Optional. IPv4 and IPv6 file pattern: **`Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`** Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: *http://download.oracle.com/javase/tutorial/essential/regex/*
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is clear.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.

Table 1-12 Microsoft DHCP Parameters (continued)

Parameter	Description
Throttle Events/Sec	Type the maximum number of events the Microsoft DHCP protocol forwards every second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default value is 100 EPS.

SMB Tail

The SMB Tail protocol allows you to configure QRadar Network Anomaly Detection to poll specific files on a remote event sources.

To configure the SMB Tail protocol, define values for the following parameters:

Table 1-13 SMB Tail Parameters

Parameter	Description
Log Source Identifier	Type an IP address, hostname, or name to identify the SMB Tail event source. IP addresses or hostnames are recommended as they allow QRadar Network Anomaly Detection to identify a log file to a unique event source.
Server Address	Type the IP address of the server.
Domain	Type the domain required to access the server. This parameter is optional.
Username	Type the username required to access the server.
Password	Type the password required to access the server.
Confirm Password	Confirm the password required to access the server.
Log Folder Path	Type the directory path to access the log files. Parameters that support file paths allow you to define a drive letter with the path information. For example, you can use **`c$/LogFiles/`** for an administrative share, or **`LogFiles/`** for a public share folder path, but not **`c:/LogFiles`**. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the proper access required to read the log files. Local or domain administrators have sufficient privileges to access log files that reside on administrative shares.
File Pattern	Type the regular expression (regex) required to filter the filenames. All matching files are included in the processing. For example, if you want to list all files starting with the word log, followed by one or more digits and ending with **`tar.gz`**, use the following entry: **`log[0-9]+\.tar\.gz`**. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: *http://download.oracle.com/javase/tutorial/essential/regex/*

Table 1-13 SMB Tail Parameters (continued)

Parameter	Description
Force File Read	Select this check box to force the protocol to read the log file. By default, the check box is selected. If the check box is clear, the log file is read only when QRadar Network Anomaly Detection detects a change in the modified time or file size.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds.
Throttle Events/Sec	Type the maximum number of events the SMB Tail protocol forwards per second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default is 100 EPS.

Forwarded Protocol

The Forwarded protocol enables you to receive a forwarded log source from another QRadar Network Anomaly Detection Console in your deployment.

The forwarded protocol is typically used in a scenario where you want to forward a log source to another QRadar Network Anomaly Detection Console. In this scenario, Console A is configured with an off-site target in the deployment editor, which points to Console B. Log sources that are automatically discovered in QRadar Network Anomaly Detection are automatically added to Console B. Any log sources from Console A that are not automatically discovered must be added to Console B by selecting **Forwarded** from the **Protocol Configuration** list box. This allows Console B to know that it is receiving forwarded log source events from another Console. For example, see **Figure 1-1**.

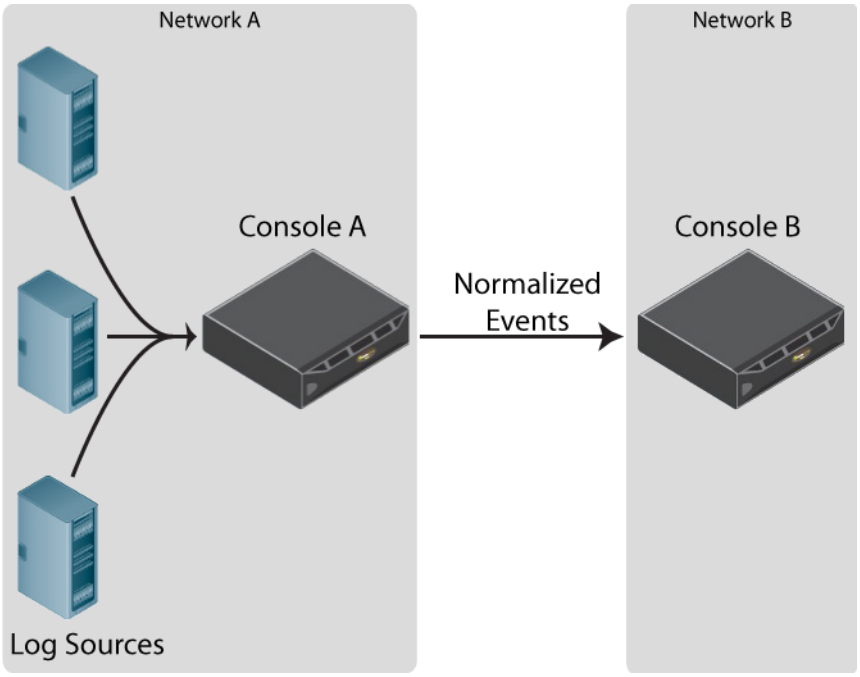

Figure 1-1 Console B Receives Forwarded Events from Console A.

In most cases, log sources that are automatically discovered are added to Console B without having to configure a log source manually. However, if you have a log source that does not automatically discover, you must manually configure Console B to receive the forwarded log source.

To configure a forwarded log source:

Step 1 Log in to the QRadar Network Anomaly Detection Console receiving the forwarded events.

Step 2 Click the **Admin** tab.

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

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

Step 5 Click **Add**.

Step 6 From the **Log Source Type** list box, select a log source type.

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

Step 8 Configure the following values:

Table 1-14 Forwarded Protocol Configuration

Parameter	Description
Log Source Identifier	Type an IP address or hostname for the originating log source. For example, this would be the IP address or hostname of the log source in Network A.

Step 9 Click **Save**.

Step 10 Repeat **Step 5** to **Step 9** for any other log sources that do not automatically discover in QRadar Network Anomaly Detection.

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

The configuration to receive forwarded events is complete. For more information on configuring an off-site target in the deployment editor, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

TLS Syslog Protocol

TLS Syslog protocol allows QRadar Network Anomaly Detection to receive encrypted syslog events from up to 50 network devices that support TLS Syslog event forwarding.

After you create an initial TLS Syslog log source and configure a listening port for TLS syslog, QRadar Network Anomaly Detection generates a syslog-tls certificate. This certificate can be copied to any device on your network that is capable of forwarding encrypted syslog. Additional network devices with a syslog-tls certificate file and the TLS listen port number can be automatically discovered as a TLS syslog log source in QRadar Network Anomaly Detection.

Note: Your network device might require additional configuration after copying the certificate to enable TLS Syslog event forwarding. For more information, see your vendor documentation.

To configure the TLS Syslog protocol, you must:

1. Install the TLS Syslog protocol.
2. Create a TLS Syslog log source.
3. Copy the TLS Syslog certificate to your network device.

Creating a TLS Syslog Log Source

Before QRadar Network Anomaly Detection can accept incoming encrypted syslog events from a network device, you must create a log source that uses the TLS Syslog protocol. Creating the log source allows QRadar Network Anomaly Detection to establish a port for incoming TLS Syslog events and generate a certificate file for your network devices. Any log source that supports syslog also includes a protocol configuration option for TLS Syslog, but not all network devices are capable of forwarding TLS Syslog events to QRadar Network Anomaly Detection.

Note: To determine if your device supports TLS Syslog, see the vendor documentation for your network device.

To configure a TLS Syslog log source:

Step 1 Log in to QRadar Network Anomaly Detection.

Step 2 Click the **Admin** tab.

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

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

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 your log source.

Step 8 From the **Log Source Type** list box, select a log source type that supports TLS syslog encryption.

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

Step 10 Configure the following values:

Table 1-15 Forwarded Protocol Configuration

Parameter	Description
Log Source Identifier	Type the IP address or hostname of the network device forwarding encrypted syslog.

Table 1-15 Forwarded Protocol Configuration (continued)

Parameter	Description
TLS Listen Port	Type the port number used by QRadar Network Anomaly Detection to accept incoming TLS Syslog events. The valid port range is 1 to 65536. The default TLS listen port is 6514. The port number specified as the listen port for TLS events can be used by up to 50 log sources. If multiple network devices are forwarding TLS syslog events, they can also use 6514 as their default TLS syslog port. ***Note:*** *If you do not see the TLS Listen Port field, you must restart Tomcat on QRadar Network Anomaly Detection. For more information, see* **Manually install a log source protocol**,**Step 8***.* To edit the Incoming TLS Listen Port number: **1** In the **Incoming TLS Listen Port** field, type the new port number for receiving TLS syslog events. **2** Click **Save**. **3** On the **Admin** tab, select **Advanced > Deploy Full Configuration**. ***Note:*** *When you click Deploy Full Configuration, QRadar Network Anomaly Detection restarts all services, resulting in a gap in data collection for events and flows until the deployment completes.*

Step 11 Click **Save**.

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

After you create your initial TLS Syslog log source, you must copy the TLS certificate from QRadar Network Anomaly Detection to your network device providing TLS Syslog events.

Copying the TLS Syslog Certificate

After you configure a TLS Syslog log source, QRadar Network Anomaly Detection creates a generic syslog-tls certificate file that can be used with multiple network devices that are capable of forwarding encrypted syslog.

To copy the QRadar Network Anomaly Detection syslog-tls certificate file:

Step 1 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: `root`

Password: `<password>`

Step 2 Navigate to the trusted certificates directory in QRadar Network Anomaly Detection.

`/opt/qradar/conf/trusted_certificates/`

Step 3 This directory contains the following two syslog files:

- **syslog-tls.cert** - The certificate file that you copy to your network devices so they can communicate with QRadar Network Anomaly Detection.
- **syslog-tls.key** - The private key file allowing network devices to communicate with QRadar Network Anomaly Detection. This file does not get copied.

Step 4 Copy the syslog-tls.cert file to your network device.

The directory path for certificate files varies between network devices. For the proper certificate path, see the vendor documentation for your network device.

The TLS Syslog configuration for QRadar Network Anomaly Detection is complete.

Once one TLS Syslog log source has been created and deployed, which will generate a syslog-tls certificate, other devices can be configured to send events to the same port using the same certificate. Provided that the log source supports auto discovery, log sources will be created automatically for additional event streams sent to the TLS Syslog listen port. The maximum number of TLS Syslog log sources that can be associated with a single TLS Listen Port is 50. To add more log sources after the first 50, you must configure your additional log sources to use a different TLS Listen Port number. You can then configure your devices to forward events for your additional log sources to the alternate TLS Listen Port.

Grouped log sources

You can view log sources based on functionality. Categorizing your log sources into groups allows you to efficiently view and track your log sources. For example, you can view all log sources by name. Each group can display a maximum of 1,000 log sources.

You must have administrative access to create, edit, or delete groups. For more information on user roles, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

View log sources using groups

To view log sources using groups, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 From the **Search For** list box, select the group option to display.

Step 5 Select your group criteria.

Step 6 Click **Go**.

The group results are displayed.

Create a log source group

To create a group, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Groups** icon.

Step 4 From the menu tree, select the group under which you want to create a new group.

Note: Alternatively, click **Assign** to access the log source group menu option.

Step 5 Click **New Group**.

Step 6 Define values for the parameters:

- **Name** - Type a name to assign to the new group. The name can be up to 255 characters in length and is case sensitive.
- **Description** - Type a description to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 To change the location of the new group, click the new group and drag the folder to a chosen location in your menu tree.

Step 9 Close the Groups Properties window.

Note: When you create the group, you can drag and drop menu tree items to change the organization of the tree items.

Edit a log source group

To edit a group, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Groups** icon.

Step 4 From the menu tree, select the group to edit.

Step 5 Click **Edit**.

Step 6 Update values for the parameters, as necessary:

- **Name** - Type a name to assign to the new group. The name can be up to 255 characters in length and is case sensitive.
- **Description** - Type a description to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 To change the location of the group, click the new group and drag the folder to a suitable location in your menu tree.

Step 9 Close the Groups window.

Copy a log source to another group

Using the groups functionality, you can copy a log source to one or more groups.

To copy a log source:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Groups** icon.

Step 4 From the Log Source Groups tree, select the group from which you want to copy the log source.

A list of log sources is displayed in the Group Content Frame.

Step 5 From the Group Content Frame, select the log source you want to copy to another group.

Step 6 Click **Copy**.

Step 7 Select the group to which you want to copy the log source.

Step 8 Click **Assign Groups**.

Step 9 Close the Groups window.

Remove a log source from a group

Removing a log source group does not delete the log source from QRadar Network Anomaly Detection, just removes the group association.

To remove a log source from a group:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Groups** icon.

Step 4 From the menu tree, select the a group with items to be removed.

Step 5 From the Group Content Frame, select the item to remove.

Step 6 Click **Remove**.

A confirmation window is displayed.

Step 7 Click **OK**.

Step 8 Close the Groups window.

Define the log source parsing order

You can configure the order that you want each Event Collector in your deployment to parse events from log sources (Device Support Modules (DSMs)). If a DSM has multiple incoming log sources under the same IP address or host name, you can order the importance of these incoming log sources by defining the parsing order.

Defining the parsing order for log sources ensures that the required log sources are parsed in a specific order, regardless of changes to the log source configuration. This ensures system performance is not affected by changes to log source configuration by preventing unnecessary parsing.

To define the parsing order:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Parsing Ordering** icon.

Note: If no log sources are configured for the selected Event Collector, only the **Selected Event Collector** list box is displayed.

Step 4 Define values for the following parameters:

- **Selected Event Collector** - From the list box, select the Event Collector to define the log source parsing order.
- **Log Source Host** - From the list box, select which log source host sends events to the Selected Event Collector.

  If multiple hosts exist on the Event Collector, a list of available hosts is displayed. Select the host from the **Filter** parameter or select from the list below.

Step 5 To prioritize the order of log source parsing:

a Select the log source you want to prioritize.

b Prioritize the log source order using the available buttons:

Up - Moves the log source higher in the parsing order.

Down - Moves the log source lower in the parsing order.

Top - Moves the log source to the top of the parsing order.

Bottom - Moves the log source to the bottom of the parsing order.

Note: To move a log source to a specific order in the parsing list, select the log source and use the **Move to** parameter.

Step 6 Click **Save**.

Step 7 Repeat for all desired log sources.

2 MANAGE LOG SOURCE EXTENSIONS

Log source extensions allow you to immediately extend or modify the parsing routines of specific devices.

For example, you can use a log source extension to detect an event that has missing or incorrect fields. A log source extension can also parse an event when the DSM to which it is attached fails to produce a result.

For information on configuring log sources, see **Manage Log Sources**.

This section provides information on the following topics:

About log source extensions

A log source extension allows a DSM to parse logs even if the DSM has not received an update or if the DSM does not exist for this log source type. Information about log source extensions is accessed from the **Admin** tab.

You can also create log source extension reports that can be sent to Customer Support. This capability is a mechanism for reporting parsing issues and potential fixes to our Customer Support department, so that they can be evaluated for inclusion in future DSM updates.

Create a log source extension document

Before defining a log source extension within QRadar Network Anomaly Detection, you must create the extension document. The extension document is an XML document that you create or edit using any common word processing application. Multiple extension documents can be created, uploaded, and associated to various log source types.

The format of the extension document must conform to a standard XML schema document (XSD). To develop an extension document, knowledge of and experience with XML coding is required.

For more information on creating an extensions document, see **Create an Extensions Document**.

The name of the extension document must be in the following format:

```
<filename>.xml
```

When you select an extension document for uploading, QRadar Network Anomaly Detection validates the document against the internal XSD. QRadar Network Anomaly Detection also verifies the validity of the document before uploading to the system. The following is an example of a valid log source extension document:

```
<?xml version="1.0" encoding="UTF-8" ?>
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventName" xmlns=""><![CDATA[
%FWSM[a-zA-Z\-]*\d-(\d{1,6}) ]]></pattern>
  <pattern id="SourceIp" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="EventNameId"
xmlns=""><![CDATA[(\d{1,6})]]></pattern>
  <match-group order="1" description="FWSM Test"
device-type-id-override="6" xmlns="">
  <matcher field="EventName" order="1" pattern-id="EventName"
capture-group="1"    enable-substitutions="false" />
  <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
  <event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco Firewall"
severity="7" send-identity="OverrideAndNeverSend" />
</match-group>
</device-extension>
```

Note: All characters between the start tag <pattern> and end tag </pattern> are considered part of the pattern. Do not use extra spaces and hard returns inside or around your pattern or <CDATA> expression. Extra characters or spaces can prevent the DSM extension from matching your intended pattern.

View a log source extensions

A list of log source extensions, their status and description is displayed in the Log Source Extensions window.

To view configured log source extensions, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

The Log Source Extensions window provides the following details for each log source extension:

Table 2-1 Log Source Extension Parameters

Parameter	Description
Extension Name	The name of the log source extension. After you have added a log source extension, click **Extension Name** to download the xml file associated with the parsing override or enhancement.
Description	The description for the log source extension. The description must not exceed 255 characters.
Enabled	Specifies if the log source extension is enabled (true) or disabled (false).
Default for Log Source Types	The log source types the log source extension is overriding or enhancing. A single log source extension file can be applied to several log sources. The parsing of all the log sources listed are being enhanced or have parsing overrides applied.

Add a log source extension

To add a log source extension:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 Click **Add**.

Step 5 Configure values for the following parameters:

Table 2-2 Add a Log Source Extension Parameters

Parameter	Description
Name	Type a name for the log source extension. The name can be a maximum of 255 alphanumeric characters including an underscore (_).
Description	Type a description for the log source extension. The description can be a maximum of 255 characters.

Table 2-2 Add a Log Source Extension Parameters (continued)

Parameter	Description
Use Condition	From the list box, select one of the following: • **Parsing Enhancement** - Select this option when the DSM correctly parses most fields for the log source, but needs either one or two fields corrected. The incorrectly parsed field values are enhanced with the new XML values. This is the default setting. • **Parsing Override** - Select this option when the DSM is unable to parse correctly or is unable to retrieve specific required device information. The log source extension completely overrides the failed parsing by the DSM and substitutes the parsing with the new XML values.
Log Source Types	Select log sources to add or remove from the extension parsing. The options include: • **Available** - Select a log source type and click the right arrow to add the log source to the **Set to default for** list. • **Set to default for** - Select a log source type and click the left arrow to remove a log source type from the **Set to default for** list. Repeat this step for each log source type you want the extension to override or enhance.

Step 6 From the **Upload Extension** field, click **Browse** and locate a log source extension document (`<filename>.xml`) to be uploaded.

Step 7 Click **Upload**.

The contents of the extension file is displayed. This displayed content is not editable.

Step 8 Click **Save**.

The new log source extension is created. The Event Collector automatically detects changes and enforces the revised log source extension.

By default, new log source extensions are enabled. If you want to disable the log source extension, see **Enabe or disable a log source extension**.

If you want to report the log source extension document back to Customer Support, see **Report a log source extension**.

Edit a log source extension

This section provides information on how to edit a log source extension, such as modifying the definition of a log source extension or changing the device to which it is the default log source extension.

To edit a log source extension, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 From the list of log source extensions, select the log source extension that you want to edit.

Step 5 Click **Edit**.

Step 6 Edit your extension parameters, as necessary:

Table 2-3 Edit Log Source Extension Parameters

Parameter	Description
Name	Type the name for the log source extension. The name can be a maximum of 255 alphanumeric characters plus the underscore (_).
Description	Type the description for the log source extension. The description can be a maximum of 255 characters.
Use Condition	From the list box, select one of the following: • **Parsing Enhancement** - Select this option when the DSM correctly parses most fields for the log source, but needs either one or two fields corrected. The incorrectly parsed field values are enhanced with the new XML values. This is the default setting. • **Parsing Override** - Select this option when the DSM is unable to parse correctly or is unable to retrieve specific required device information. The log source extension completely overrides the failed parsing by the DSM and substitutes the parsing with the new XML values.
Log Source Types	Select log sources to add or remove from the extension parsing. The options include: • **Available** - Select a log source type and click the right arrow to add the log source to the **Set to default for** list. • **Set to default for** - Select a log source type and click the left arrow to remove a log source type from the **Set to default for** list. Repeat this step for each log source type you want the extension to override or enhance.

Step 7 Click **Browse** and locate a log source extension document (`<filename>.xml`) if you want to upload an extension document to replace the existing extension document.

Step 8 Click **Upload**.

Step 9 Click **Save**.

The log source extension is revised. The Event Collector automatically detects changes and enforces the revised log source extension.

Copy a log source extension

This section provides information on how to copy a log source extension.

Use this function if you want to create a new log source extension that has some or all of the parameters of an existing log source extension. You can use an existing log source extension as a template.

To copy a log source extension:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 From the list of log source extensions, select the log source extension that you want to copy.

Step 5 Click **Copy**.

Step 6 Type values for the parameters:

Table 2-4 Copy Log Source Extension Parameters

Parameter	Description
Name	Type a name for the log source extension. The name can be a maximum of 255 alphanumeric characters plus the underscore (_).
Description	Type a description for the log source extension. The description can be a maximum of 255 characters.
Use Condition	From the list box, select one of the following: • **Parsing Enhancement** - Select this option when the DSM correctly parses most fields for the log source, but needs either one or two fields corrected. The incorrectly parsed field values are enhanced with the new XML values. This is the default setting. • **Parsing Override** - Select this option when the DSM is unable to parse correctly or is unable to retrieve specific required device information. The log source extension completely overrides the failed parsing by the DSM and substitutes the parsing with the new XML values.
Log Source Types	Select log sources to add or remove from the extension parsing. The options include: • **Available** - Select a log source type and click the right arrow to add the log source to the **Set to default for** list. • **Set to default for** - Select a log source type and click the left arrow to remove a log source type from the **Set to default for** list. Repeat this step for each log source type you want the extension to override or enhance.

Step 7 Click **Save**.

The new log source extension is created. The Event Collector automatically detects changes and picks up a new or revised log source extension.

Delete a log source extension

Deleting a log source extension removes any additional parsing enhancements or overrides from the log source.

If you delete a log source extension, the parsing changes are applied immediately to the incoming events for the log sources impacted by the parsing change.

To delete a log source extension, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 From the list of log source extensions, select the log source extension that you want to delete.

Step 5 Click **Delete**.

A confirmation window is displayed.

Step 6 Click **Yes** to confirm the deletion.

Enabe or disable a log source extension

You can enable an existing log source extension or disable an existing log source extension (without deleting the extension). This section provides information on how to enable and disable a log source extension.

To enable or disable a log source extension, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 From the list of log source extensions, select the log source extension that you want to enable or disable.

Step 5 Click **Enable/Disable**.

The status (true or false) is displayed in the Enabled column.

The log source extension is enabled or disabled. The Event Collector automatically detects changes and enforces the revised log source extension.

Report a log source extension

After you create a log source extension, you have the option of sending information about that log source extension to IBM Corp.

Customer Support. Sending this information to IBM Corp. Customer Support facilitates the process of providing you with support.

To send a report of the log source extension to IBM Corp. Customer Support:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Log Source Extensions** icon.

Step 4 From the list of log source extensions, select the log source extension that you want to send to IBM Corp. Customer Support.

Step 5 Click **Report**.

The Report Log Source Extensions menu is displayed with the extension document in the Extension Document field.

Step 6 Type values for the parameters:

Table 2-5 Reporting a Log Source Extension Parameters

Parameter	Description
Customer Name	Type your company or organization name.
Technical Contact Name	Type the name of the technical contact.
Comments	Type any comments that can be useful in understanding the issue.

Step 7 Click **Send**.

A Create an Extensions Document

Log source extensions allow you to repair an event with missing or incorrect information.

You can also use log source extensions to parse an event when the associated DSM fails to produce a result. Any new events produced by the log source extensions are associated to the device that failed to parse the original payload. Creating an extension prevents unknown or uncategorized events from being stored as unknown in QRadar Network Anomaly Detection.

Note: This document assumes an advanced knowledge of Java-based regular expressions and XML coding.

For more information on configuring log source extensions, see **Manage Log Source Extensions**.

Before you define a log source extension, you must build an extension document.

This section provides information on the following:

- **About Extension Documents**
- **Understand extension document elements**
- **Create an extension document**
- **Log Source Type IDs**

About Extension Documents

An extension document is specified in Extensible Markup Language (XML) format and can be created or edited using any common word processing application. You can create multiple extension documents and associate an extension document to various log source types.

Using XML format requires that all regular expressions be contained in character data (CDATA) sections to prevent the special characters required by regular expressions from interfering with the markup format. For example:

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[(tcp|udp|icmp|gre)]]></pattern>
```

Where `(tcp|udp|icmp|gre)` is the actual regular expression pattern.

The configuration consists of two sections: patterns and match groups. For more information, see **Understand extension document elements**.

Understand extension document elements

This section explains the two main divisions of the extension document:

- **Patterns**
- **Match groups**

Patterns

Rather than associating a regular expression directly with a particular field name, patterns (**patterns**) are declared separately at the top of the extension document and can be subsequently referenced multiple times within the file.

Note: All characters between the start tag <pattern> and end tag </pattern> are considered part of the pattern. Do not use extra spaces and hard returns inside or around your pattern or <CDATA> expression. Extra characters or spaces can prevent the DSM extension from matching your intended pattern.

Table A-1 Pattern Parameters

Parameter	Description
id (Required)	Type a regular string that is unique within the extension document.
case-insensitive (Optional)	Type a pattern to ignore character case when doing a match, for example **abc** is the same as **ABC**. If not specified, this parameter defaults to false.
trim-whitespace (Optional)	Type if you want the pattern to ignore white space and carriage returns. If the CDATA sections are split onto different lines, this parameter ensures that any extra spaces and carriage returns are not interpreted as part of the pattern. If not specified, this parameter defaults to false.

Match groups

A match group (**match-group**) is a set of patterns used for parsing or modifying one or more types of events. A matcher is an entity within a match group that is parsed (for example, EventName) and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.

Table A-2 Match Group Parameters

Parameter	Description
order (Required)	Type an integer greater than zero to define the order in which the match groups are executed. It must be unique within the extension document.
description (Optional)	Type a description for the match group, which can be any string. This information can appear in the logs. If not specified, this parameter defaults to empty.

Table A-2 Match Group Parameters (continued)

Parameter	Description
device-type-id-override (Optional)	Define a different device ID to override the QID. Allows the particular match group to search in the specified device for the event type. It must be a valid log source type ID, represented as an integer. A list of log source type IDs is presented in **Table A-6**. If not specified, this parameter defaults to the log source type of the log source to which the extension is attached.

Match groups can have up to three different types of entities:

- **Matcher (matcher)**
- **Single-event modifier (event-match-single)**
- **Multi-event modifier (event-match-multiple)**

Matcher (`matcher`)

A matcher entity is a field that is parsed (for example, EventName) and is paired with the appropriate pattern and group for parsing. Matchers have an associated order, so if multiple matchers are specified for the same field name, the matchers are executed in the order presented until a successful parse is found or a failure occurs.

Table A-3 Matcher Entity Parameters

Parameter	Description
field (Required)	Type the field to which you want the pattern to apply, for example, EventName, or SourceIp. See **Table A-4** for a list of valid field names.
pattern-id (Required)	Type the pattern you want to use when parsing the field out of the payload. This value must match (including case) the ID parameter of the pattern previously defined in a pattern ID parameter (**Table A-1**).
order (Required)	Type the order that you want this pattern to attempt among matchers assigned to the same field. If there are two matchers assigned to the EventName field, the one with the lowest order is attempted first.

Table A-3 Matcher Entity Parameters (continued)

Parameter	Description
capture-group (Optional)	Define a capture group, as denoted in the regular expression inside parenthesis ( ). These captures are indexed starting at one and processed from left to right in the pattern. The **capture-group** field must be a positive integer less than or equal to the number of capture groups contained in the pattern. The default value is zero, which is the entire match. For example, you can define a single pattern for a source IP address and port; where the SourceIp matcher can use a capture group of 1, and the SourcePort matcher can use a capture group of 2, but only one pattern needs to be defined. This field has a dual purpose when combined with the **enable-substitutions** parameter.
enable-substitutions (Optional)	Type this Boolean parameter as **true** when a field cannot be adequately represented with a straight group capture. Allows you to combine multiple groups together with extra text to form a value. This parameter changes the meaning of the **capture-group** parameter. The **capture-group** parameter creates the new value, and group substitutions are specified using **\x** where **x** is a group number from 1 to 9. You can use groups multiple times, and any free-form text can also be inserted into the value. For example, if you need to form a value out of group 1, followed by an underscore, followed by group 2, an @, and then group 1 again, the appropriate capture-group syntax is: **capture-group="\1_\2@\1"** In another example, a MAC address is separated by colons, but QRadar Network Anomaly Detection assumes that MAC addresses are hyphen separated. The syntax to parse and capture the individual portions is: **capture-group="\1:\2:\3:\4:\5:\6"** If no groups are specified in the capture-group when substitutions are enabled, a direct text replacement occurs. Default is false.

Table A-3 Matcher Entity Parameters (continued)

Parameter	Description
`ext-data` (Optional)	Type an extra-data parameter to define any extra field information or formatting that a Matcher Field can provide in the extension. For example, you might have a device that sends events using a unique timestamp, but you want the event to be reformatted to a standard device time. The ext-data parameter included with the DeviceTime field allows you to reformat the date and timestamp of the event. For more information, see **Table A-4**.

Table A-4 provides a list of valid field names for use in the matcher field parameter (see **Table A-2**).

Table A-4 Matcher Field Names

Field Name	Description
EventName (Required)	Type the event name to be retrieved from the QID to identify the event.
EventCategory	Type an event category for any event with a category not handled by an **`event-match-single`** entity or an **`event-match-multiple`** entity. Combined with EventName, EventCategory is used to search for the event in the QID.
SourceIp	Type the source IP address for the message.
SourcePort	Type the source port for the message.
SourceIpPreNAT	Type the source IP address for the message before Network Address Translation (NAT) occurs.
SourceIpPostNAT	Type the source IP address for the message after NAT occurs.
SourceMAC	Type the source MAC address for the message.
SourcePortPreNAT	Type the source port for the message before NAT occurs.
SourcePortPostNAT	Type the source port for the message after NAT occurs.
DestinationIp	Type the destination IP address for the message.
DestinationPort	Type the destination port for the message.
DestinationIpPreNAT	Type the destination IP address for the message before NAT occurs.
DestinationIpPostNAT	Type the destination IP address for the message after NAT occurs.
DestinationPortPreNAT	Type the destination port for the message before NAT occurs.
DestinationPortPostNAT	Type the destination port for the message after NAT occurs.
DestinationMAC	Type the destination MAC address for the message.

Table A-4 Matcher Field Names (continued)

Field Name	Description
DeviceTime	Type the time and format used by the device. This date and timestamp represents the time that the event was sent, according to the device (this is NOT the time that the event arrived). The DeviceTime field supports the ability to use a custom date and timestamp for the event by calling the ext-data Matcher Entity. The following list contains examples of date and timestamp formats that can be used in the DeviceTime field: • ext-data="dd/MMM/YYYY:hh:mm:ss" • ext-data="MMM dd YYYY / hh:mm:ss" • ext-data="hh:mm:ss:dd/MMM/YYYY" For more information on the possible values for the data and timestamp format, see http://download.oracle.com/javase/1.4.2/docs/api/java/text/SimpleDateFormat.html. ***Note:*** *DeviceTime is the only event field that uses the ext-data optional parameter.*
Protocol	Type the protocol associated with the event; for example, TCP, UDP, or ICMP. If a protocol is not properly parsed out of a message, ports that were parsed can not appear in QRadar Network Anomaly Detection (it only displays ports for port-based protocols).
UserName	Type the username associated with the event.
HostName	Type the host name associated with the event. Typically, this field is associated with identity events.
GroupName	Type the group name associated with the event. Typically, this field is associated with identity events.
NetBIOSName	Type the NetBIOS name associated with the event. Typically, this field is associated with identity events.
ExtraIdentityData	Type any user-specific data associated with the event. Typically, this field is associated with identity events.
SourceIpv6	Type the IPv6 source IP address for the message.
DestinationIpv6	Type the IPv6 destination IP address for the message.

Single-event modifier (`event-match-single`)

Single-event modifier (**`event-match-single`**) matches (and subsequently modifies) exactly one type of event, as specified by the required, case-sensitive EventName parameter. This entity allows mutation of successful events by changing the device event category, severity, or the method for sending identity events.

When events matching this event name are parsed, the device category, severity, and identity properties are imposed upon the resulting event. An event-match-single entity consists of three optional properties:

Table A-5 Single-Event Modifier Parameters

Parameter	Description
device-event-category	Type a new category for searching in the QID for the event. This is an optimizing parameter, since some devices have the same category for all events.
severity	Type the severity of the event. This parameter must be an integer value between 1 and 10. If a severity of less than 1 or greater than 10 is specified, the system defaults to 5. If not specified, the default is whatever is found in the QID.
send-identity	Specifies the sending of identity change information from the event. Choose one of the following options: • **UseDSMResults** – If the DSM returns an identity event, the event is passed on. If the DSM does not return an identity event, the DSM does not create or modify the identity information. This is the default value if no value is specified. • **SendIfAbsent** – If the DSM creates identity information, the identity event is passed through unaffected. If no identity event is produced by the DSM, but there is enough information in the event to create an identity event, an event is generated with all the relevant fields set. • **OverrideAndAlwaysSend** – Ignores any identity event returned by the DSM and creates a new identity event, if there is enough information. • **OverrideAndNeverSend** – Suppress any identity information returned by the DSM.

Multi-event modifier (**event-match-multiple**)

The multi-event modifier (**event-match-multiple**) matches a range of event types (and subsequently modifies) as specified by the **pattern-id** parameter and the **capture-group-index** parameter.

Note: This match is not performed against the payload, but is performed against the results of the EventName matcher previously parsed out of the payload.

This entity allows mutation of successful events by changing the device event category, severity, or the method the event uses to send identity events. The **capture-group-index** must be an integer value (substitutions are not supported) and pattern-ID must reference an existing pattern entity. All other properties are identical to their counterparts in the single-event modifier

Create an extension document

This section provides information on the following:

- **Writing a complete extension document**
- **Upload extension documents**
- **Solve specific parsing issues**

Writing a complete extension document

The example of an extension document included in this section provides information on how to parse one particular type of Cisco FWSM so that events are not sent with an incorrect event name. For example, if you want to resolve the word **session**, which is embedded in the middle of the event name:

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015: Built UDP
connection for faddr 38.116.157.195/80 gaddr
129.15.127.254/31696 laddr 10.194.2.196/2157 duration 0:00:00
bytes 57498 (TCP FINs)
```

This condition causes the DSM to not recognize any events and all the events are un-parsed and associated with the generic logger.

Although only a portion of the text string (**302015**) is used for the QID search, the entire text string (**%FWSM-session-0-302015**) identifies the event as coming from a Cisco FWSM. Since the entire text string is not valid, the DSM assumes that the event is not valid.

An FWSM device has a large number of event types, many with unique formats. The following extension document example indicates how to parse one event type.

Note: The pattern IDs do not have to match the field names that they are parsing. Even though the following example duplicates the pattern, the SourceIp field and the SourceIpPreNAT field could use the exact same pattern in this case (this might not be true in all FWSM events).

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">

<pattern id="EventNameFWSM"
xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT" xmlns=""><![CDATA[gaddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT" xmlns=""><![CDATA[laddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp" xmlns=""><![CDATA[faddr
(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol" case-insensitive="true"
xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6" case-insensitive="true"
xmlns=""><![CDATA[ protocol=6]]></pattern>
```

```
<pattern id="EventNameId"
xmlns=""><![CDATA[(\d{1,6})]]></pattern>

<match-group order="1" description="FWSM Test"
device-type-id-override="6" xmlns="">
 <matcher field="EventName" order="1"
pattern-id="EventNameFWSM" capture-group="1"/>
 <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
 <matcher field="SourcePort" order="1" pattern-id="SourceIp"
capture-group="2" />
 <matcher field="SourceIpPreNAT" order="1"
pattern-id="SourceIpPreNAT" capture-group="1" />
 <matcher field="SourceIpPostNAT" order="1"
pattern-id="SourceIpPostNAT" capture-group="1" />
 <matcher field="SourcePortPreNAT" order="1"
pattern-id="SourceIpPreNAT" capture-group="2" />
 <matcher field="SourcePortPostNAT" order="1"
pattern-id="SourceIpPostNAT" capture-group="2" />
 <matcher field="DestinationIp" order="1"
pattern-id="DestinationIp" capture-group="1" />
 <matcher field="DestinationPort" order="1"
pattern-id="DestinationIp" capture-group="2" />
 <matcher field="Protocol" order="1" pattern-id="Protocol"
capture-group="1" />
 <matcher field="Protocol" order="2" pattern-id="Protocol_6"
capture-group="TCP" enable-substitutions=”true”/>

 <event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco
Firewall"/>
</match-group>

</device-extension>
```

The above extension document example demonstrates some of the basic aspects of parsing:

- IP addresses
- Ports
- Protocol
- Multiple fields using the same pattern with different groups

This example parses all FWSM events that follow the specified pattern, although the fields that are parsed might not be present in those events (if the events include different content).

The information that was necessary to create this configuration that was not available from the event:

- The event name is only the last six digits (`302015`) of the `%FWSM-session-0-302015` portion of the event.
- The FWSM has a hard-coded log source type category of `Cisco Firewall`.
- The FWSM uses the Cisco Pix QID and therefore includes the `device-type-id-override="6"` parameter in the match group (the Pix firewall's log source type ID is 6, see **Table A-6**).

Note: If the QID information is not specified or is unavailable, you can modify the event mapping. For more information, see the Modifying Event Mapping section in the *IBM Security QRadar Network Anomaly Detection Users Guide*.

An event name and a device event category is required when looking for the event in the QID. This device event category is a grouping parameter within the database that helps define like events within a device. The `event-match-multiple` at the end of the match group includes hard-coding of the category. The `event-match-multiple` uses the EventNameId pattern on the parsed event name to match up to six digits. This pattern is not run against the full payload, just that portion parsed as the EventName field.

The EventName pattern references the `%FWSM` portion of the events; all Cisco FWSM events contain the `%FWSM` portion. The pattern in the example matches `%FWSM` followed by any number (zero or more) of letters and dashes. This pattern match resolves the word `session` that is embedded in the middle of the event name that needs to removed. The event severity (according to Cisco), followed by a dash and then the true event name as expected by QRadar Network Anomaly Detection. The only string with a capture group (that is, bounded by parenthesis) is this pattern of digits `(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`.

The IP addresses and ports for the event all follow the same basic pattern: an IP address followed by a slash followed by the numeric port number. This pattern parses two pieces of data (the IP address and the port), and specifies different capture groups in the matcher section.

```
   <matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourceIp"
capture-group="2" />
```

Thus, the IP address/port patterns are four sets of one to three digits, separated by periods followed by a slash and the port number. The IP address section is in a group, as is the port number (but not the slash). As was previously mentioned, the matcher sections for these fields reference the same pattern name, but a different capture group (the IP address is group 1 and the port is group 2).

The protocol is a common pattern that searches the payload for the first instance of TCP, UDP, ICMP, or GRE (the pattern is marked with the case-insensitive parameter so that any occurrence matches).

Note: You must search for the protocol when writing extension documents, as QRadar Network Anomaly Detection might not display port numbers if the event is not based on a port-based protocol. See **Convert a protocol** for an example of how to search for a protocol.

Although a second protocol pattern does not occur in the event being used as an example, there is a second protocol pattern defined with an order of two. If the lowest-ordered protocol pattern does not match, the next one is attempted (and so on). The second protocol pattern also demonstrates the cpt of a direct substitution; there are no match groups in the pattern, but with the enable-substitutions parameter enabled, the text TCP can be used in place of protocol=6.

Upload extension documents

Multiple extension documents can be created, uploaded, and associated to various log source types. Extension documents can be stored anywhere prior to uploading to QRadar Network Anomaly Detection. When you select an extension document for uploading, QRadar Network Anomaly Detection validates the document against the internal XSD. QRadar Network Anomaly Detection also verifies the validity of the document before uploading to the system.

Solve specific parsing issues

This section provides you with XML examples that can be used when resolving specific parsing issues.

- **Convert a protocol**
- **Make a single substitution**
- **Generating a colon-separated MAC address**
- **Combining IP address and port**
- **Modifying an event category**
- **Modifying multiple event categories**
- **Suppressing identity change events**
- **Encoding logs**

Convert a protocol

The following example shows a typical protocol conversion that searches for TCP, UDP, ICMP, or GRE anywhere in the payload, surrounded by any word boundary (for example, tab, space, end-of-line). Also, character case is ignored:

```
<pattern id="Protocol" case-insensitive="true"
xmlns=""><![CDATA[\b(tcp|udp|icmp|gre)\b]]> </pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol"
capture-group="1" />
```

Make a single substitution

The following is an example of a straight substitution that parses the source IP address, and then overrides the result and sets the IP address to 10.100.100.100, ignoring the IP address in the payload. This example assumes that the source IP

address matches something similar to SrcAddress=10.3.111.33 followed by a comma:

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]></p
attern>

<matcher field="SourceIp" order="1"
pattern-id="SourceIp_AuthenOK" capture-group="100.100.100.100"
enable-substitutions="true"/>
```

Generating a colon-separated MAC address

QRadar Network Anomaly Detection detects MAC addresses in a colon-separated form. Since all devices do not use this form, the following example shows how to correct that situation:

```
<pattern id="SourceMACWithDashes"
xmlns=""><![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-(
[0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{
2})]]></pattern>

<matcher field="SourceMAC" order="1" pattern-id="
SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

In the above example `SourceMAC=12-34-56-78-90-AB` is converted to a MAC address of `12:34:56:78:90:AB`.

If the dashes are removed from the pattern, the pattern converts a MAC address with no separators. If spaces are inserted, the pattern converts a space-separated MAC address, and so on.

Combining IP address and port

Typically an IP address and port are combined in one field, separated by a colon or a slash. The following example uses multiple capture groups with one pattern:

```
pattern id="SourceIPColonPort" xmlns=""><!
[CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]
]></pattern>

<matcher field="SourceIp" order="1"
pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1"
pattern-id="SourceIPColonPort" capture-group="2" />
```

Modifying an event category

A device event category can be hard-coded, or the severity needs to be adjusted. The following example adjusts the severity for a single event type:

```
<event-match-single event-name="TheEvent"
device-event-category="Actual Category" severity="6"
send-identity="UseDSMResults" />
```

Modifying multiple event categories

The following example is similar to the above single event example, except that this example matches all event codes starting with `7` and followed by one to five digits:

```
<pattern id="EventNameId"
xmlns=""><![CDATA[(7\d{1,5})]]></pattern>

<event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Actual Category"
severity="6" send-identity="UseDSMResults"/>
```

Suppressing identity change events

A DSM might unnecessarily send identity change events. The following are two examples; one is a method of how to suppress identity change events from being sent from a single event type. The other is a method of how to suppress identity change events from being sent from a group of events.

```
// Never send identity for the event with an EventName of
“Authen OK”
<event-match-single event-name="Authen OK"
device-event-category="ACS" severity="6"
send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name
starting with 7, followed by one to five other digits:
<pattern id="EventNameId"
xmlns=""><![CDATA[(7\d{1,5})]]></pattern>

<event-match-multiple pattern-id="EventNameId"
capture-group-index="1" device-event-category="Cisco Firewall"
severity="7" send-identity="OverrideAndNeverSend"/>
```

Encoding logs

The following encoding formats are supported:

- US-ASCII
- UTF-8

Logs can be forwarded to the system in an encoding that does not match US-ASCII or UTF-8 formats. You can configure an advanced flag to ensure input can be re-encoded to UTF-8 for parsing and storage purposes.

For example, if you want to ensure that the source logs arrive in SHIFT-JIS (ANSI/OEM Japanese) encoding, type the following:

```
<device-extension source-encoding=”SHIFT-JIS”
xmlns=”event_parsing/device_extension”>
```

The logs are enclosed in UTF-8 format.

Formatting event dates and timestamps

A log source extension for QRadar Network Anomaly Detection can detect several different date and timestamp formats on events. Since device manufacturers do not conform to a standard date and timestamp format, the ext-data optional parameter is included in the log source extension to allow the DeviceTime to be reformatted. The following example shows how an event can be reformatted to correct the date and timestamp formatting:

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern
id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]
</pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
<matcher field="EventName" order="1" pattern-id="EventName1"
capture-group="1"/>
<matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
<matcher field="UserName" order="1" pattern-id="Username"
capture-group="1"/></match-group>
```

Log Source Type IDs

Table A-6 lists the Log Source Type IDs that can be used in a `match-group` statement:

Table A-6 Log Source Type ID Numbers

ID	Log Source Type
2	Snort Open Source IDS
3	Check Point Firewall-1
4	Configurable Firewall Filter
5	Juniper Networks Firewall and VPN
6	Cisco PIX Firewall
7	Configurable Authentication message filter
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	Linux OS
12	Microsoft Windows Security Event Log
13	Windows IIS
14	Linux iptables Firewall
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks Intrusion Detection and Prevention (IDP)
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
21	Nortel Contivity VPN Switch
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 Series Cntrator
24	Solaris Operating System Authentication Messages
25	McAfee IntruShield Network IPS Appliance
26	Cisco CSA
28	Enterasys Matrix E1 Switch
29	Solaris Operating System Sendmail Logs
30	Cisco Intrusion Prevention System (IDS)
31	Cisco Firewall Services Module (FWSM)
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS Family
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN Switch
38	Top Layer Intrusion Prevention System (IPS)
39	Universal DSM

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
48	Oracle RDBMS Audit Records
49	F5 Networks BIG-IP LTM
50	Solaris Operating System DHCP Logs
55	Array Networks SSL VPN Access Gateway
56	Cisco CatOS for Catalyst Switches
57	ProFTPD Server
58	Linux DHCP Server
59	Juniper Networks Infranet Controller
64	Juniper JunOS Platform
68	Enterasys Matrix K/N/S Series Switch
70	Extreme Networks ExtremeWare Operating System (OS)
71	Sidewinder G2 Security Appliance
73	Fortinet FortiGate Security Gateway
78	SonicWall UTM/Firewall/VPN device
79	Vericept Content 360
82	Symantec Gateway Security (SGS) Appliance
83	Juniper Steel Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	CiscoNAC Appliance
96	TippingPoint X Series Appliances
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend Interscan VirusWall
101	Microsoft SQL Server

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
102	MAC OS X
103	Bluecoat SG Appliance
104	Nortel Switched Firewall 6000
106	3Com 8800 Series Switch
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Nortel Application Switch
111	Juniper DX Application Acceleration Platform
112	SNARE Reflector Server
113	Cisco 12000 Series Routers
114	Cisco 6500 Series Switches
115	Cisco 7600 Series Routers
116	Cisco Carrier Routing System
117	Cisco Integrated Services Router
118	Juniper M-Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Juniper MX-Series Ethernet Services Router
123	Juniper T-Series Core Platform
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex-Series Ethernet Switch
140	Sysmark Power Broker
141	Oracle Database Listener
142	Samhain HIDS
143	Bridgewater Systems AAA Service Controller
144	Name Value Pair
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Juniper SRX Series Services Gateway
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Aruba Mobility Controller

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Enterasys XSR Security Routers
167	Enterasys Stackable and Standalone Switches
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys A-Series
171	Enterasys B2-Series
172	Enterasys B3-Series
173	Enterasys C2-Series
174	Enterasys C3-Series
175	Enterasys D-Series
176	Enterasys G-Series
177	Enterasys I-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS Audit Record
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility (ACF2)
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Sophos Web Security Appliance
241	Sophos Astaro Security Gateway
243	Infoblox NIOS
244	Tropos Control

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
245	Novell eDirectory
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Digital China Networks DCS and DCRS Series switch
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
282	OSSEC
283	Huawei AR Series Router
286	IBM AIX Audit
287	Symantec PGP Universal Server
289	IBM Tivoli Endpoint Manager
290	Juniper Mykonos Web Security
291	Nominum Vantio
292	Enterasys 800-Series Switch
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP Advanced Firewall Manager (AFM)

Table A-6 Log Source Type ID Numbers (continued)

ID	Log Source Type
298	Fidelis XPS
300	Barracuda Web Filter

B INSTALL PROTOCOL SOURCES

QRadar Network Anomaly Detection is preconfigured to perform weekly automatic software updates. This includes DSMs, protocols, and scanner module updates.

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 more information on scheduling pending updates, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

This section includes the following topics:

Schedule Automatic Updates

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.

Auto 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.

▶ 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

The Schedule the Updates window is displayed.

Note: Protocol updates installed automatically require you to restart Tomcat manually. For more information on manually restarting Tomcat, see **Manually install a log source protocol**.

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

If you are having connection issues with a protocol, you might need to install a protocol update.

You can view any pending software updates for QRadar Network Anomaly Detection through the **Admin** tab. You can select and install a pending update from the Auto Update window.

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 B-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 B-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 B-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 log source protocol

You can install a protocol source that allows you to access additional or updated protocols for use with your Device Support Modules (DSMs) and log sources.

You can download and automatically install updates using the Auto Updates icon on the **Admin** tab or manually install a protocol update.

Install a single protocol

To install a single protocol using the command line:

Step 1 Download the protocol file from one of the following websites to your system hosting QRadar Network Anomaly Detection:

https://qmmunity.q1labs.com/

http://www.ibm.com/support

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 PROTOCOL-SNMP-7.0-201509.noarch.rpm**

The protocols are installed. To complete the installation, you must run a Full Deploy and restart Tomcat.

Step 5 Log in to QRadar Network Anomaly Detection.

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

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

Step 6 Click the **Admin** tab.

Step 7 Select **Advanced > Deploy Full Configuration**.

CAUTION: *Deploying Full Configuration restarts multiple services on the QRadar Network Anomaly Detection system. Event collection is unavailable on QRadar Network Anomaly Detection until the Deploy Full Configuration completes.*

Step 8 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Step 9 Restart the Tomcat service:

service tomcat restart

Note: Restarting Tomcat on QRadar Network Anomaly Detection forces every user to immediately log out. Verify all users are logged out of the system before restarting the Tomcat service.

Install a log source protocol bundle

The Qmmunity or *http://www.ibm.com/support* website contain a protocol bundle that is updated with the latest protocol versions.

To install the protocol bundle using the command line:

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

https://qmmunity.q1labs.com/

http://www.ibm.com/support

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 protocol bundle:

```
tar -zxvf QRadar_bundled-PROTOCOL-<version>.tar.gz
```

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

Step 5 Type the following command:

```
for FILE in *Common*.rpm PROTOCOL-*.rpm; do rpm -Uvh "$FILE"; done
```

The protocols are installed. To complete the installation, you must run a Full Deploy and restart Tomcat.

Step 6 Log in to QRadar Network Anomaly Detection.

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

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

Step 7 Click the **Admin** tab.

Step 8 Select **Advanced > Deploy Full Configuration**.

CAUTION: *Deploying Full Configuration restarts multiple services on QRadar Network Anomaly Detection. Event collection is unavailable on QRadar Network Anomaly Detection until the Deploy Full Configuration completes.*

Step 9 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Step 10 Restart the Tomcat service:

```
service tomcat restart
```

Note: Restarting Tomcat on QRadar Network Anomaly Detection forces every user to immediately log out. Verify all users are logged out of the system before restarting the Tomcat service.

C DCOM CONFIGURATION

The Microsoft Security Event Log and Microsoft Security Event Log Custom protocols provide remote agentless Windows event log collection using the Microsoft Windows Management Instrumentation (WMI) API.

To configure DCOM, select your operating system from the options below:

- To Configure DCOM and WMI for Windows Server 2003. For more information, see **Configuring Windows Server 2003**.
- To Configure DCOM and WMI for Windows Server 2008. For more information, see **Configure Windows Server 2008**.

Supported operating systems

QRadar Network Anomaly Detection supports the following Microsoft Windows Management Instrumentation (WMI) API:

- Microsoft Windows 2000
- Microsoft WIndows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R2
- Microsoft Windows XP
- Microsoft WIndows Vista
- Microsoft Windows 7

Before you begin

Before you install the Windows 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:

- Configure and enable DCOM on the host.
- Enable Windows Management Instrumentation on the host.
- Activate the remote registry service.
- Ensure you have appropriate administrative or user permissions for DCOM and WMI. For this process, you must be a member of the Administrators group, or you must create a group with the necessary permissions to access the remote computer. If the system is part of a domain, you must be a member of the Domain Administrators group.

- You have configured any firewalls to permit traffic on TCP port 135, as well as permitting DCOM communications TCP ports above 1024 on your network.

Configuring Windows Server 2003

To configure DCOM on Windows Server 2003, perform the following steps:

1. Verify the required Windows Server 2003 services are started. For more information, see **Required DCOM and WMI services for Windows Server 2003**.
2. Enabling DCOM for Windows Server 2003. For more information, see **Enable DCOM for Windows Server 2003**.
3. Configure DCOM communications for Windows Server 2003. For more information, see **Configure DCOM communications in Windows Server 2003**.
4. Configure user accounts for DCOM. For more information, see **Configure Windows Server 2003 user accounts for DCOM**.
5. Configure WMI for Windows Server 2003. For more information, see **Configuring WMI User Access for Server 2003**.
6. Test the WMI configuration. For more information, see **Verifying WMI communications**.

Required DCOM and WMI services for Windows Server 2003

The following Windows services for DCOM must be started and configured for automatic startup:

- Server
- Remote Registry
- Windows Management Instrumentation

To configure the Server and Remote Registry services for automatic startup, you must:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
services.msc
```

Step 3 Click **OK**.

The Services window is displayed.

Step 4 In the details pane, verify the following services are started and set to automatic startup:

- Server
- Remote Registry

Step 5 To change a service property, right-click on the service name, and then click **Properties**.

Step 6 Using the **Startup type** list box, select **Automatic**.

Step 7 If the Service status is not started, click **Start**.

Step 8 Click **OK**.

Step 9 Close the Services window.

You are now ready to enable DCOM on your Windows Server 2003.

Enable DCOM for Windows Server 2003

To enable DCOM on your Windows Server 2003 , perform the following steps:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under **Console root**, expand **Component Services**, expand **Computers**, and select **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **Default Properties** tab.

Step 7 Configure the following Default Properties:

a Select the **Enable Distributed COM on this computer** check box.

b Using the **Default Authentication Level** list box, select **Connect**.

c Using the **Default Impersonation Level** list box, select **Identify**.

Note: You can define the TCP ports DCOM uses to communicate on your network by configuring the Properties for Connection-oriented TCP/IP. For more information, see **Configure DCOM communications in Windows Server 2003**.

Step 8 Click **Apply**, then click **OK**.

The Component Services window is displayed.

Step 9 Close the Component Services window.

You are now ready to configure DCOM ports on your Windows Server 2003.

Configure DCOM communications in Windows Server 2003

Windows Server 2003 requires TCP/IP communications for DCOM.

To configure DCOM TCP/IP communications, you must:

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under **Console root**, expand **Component Services**, expand **Computers**, and select **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **Default Protocols** tab.

Step 7 Configure the following options:

a If Connection-oriented TCP/IP is listed in the DCOM Protocols window, go to **Step 8**.

b If Connection-oriented TC/IP is not listed in the DCOM Protocol window, select **Add**.

The Select DCOM protocol window is displayed.

c From the list box, select **Connection-oriented TC/IP**.

Step 8 Click **OK**.

Step 9 Click **OK**.

Step 10 Close the Component Services window.

You are now ready to configure a user account with permission to access the host. For more information, see **Configure Windows Server 2003 user accounts for DCOM**.

Configure Windows Server 2003 user accounts for DCOM

After you have enabled DCOM, you must assign an account the proper permission to access DCOM on the host.

You must select an existing account with administrative access or create a normal user account that is a member of an administrative group to access the host.

To configure a user account for DCOM on Windows Server 2003, perform the following steps:

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under **Console root**, expand **Component Services**, expand **Computers**, and select **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **COM Security** tab.

Step 7 In **Access Permissions**, click **Edit Default**.

Step 8 Select the user or group requiring DCOM access.

Note: If the user or group requiring DCOM access is not listed in the permissions list, you must add the user to the configuration.

Step 9 Select the check boxes for the following permissions:

- **Local Access** - Select the **Allow** check box.
- **Remote Access** - Select the **Allow** check box.

Step 10 Click **OK**.

The My Computer Properties window is displayed.

Step 11 In **Launch and Activation Permissions**, click **Edit Default**.

Step 12 Select the user or group requiring DCOM access.

Step 13 Configure the following permissions:

- **Local Launch** - Select the **Allow** check box.
- **Remote Launch** - Select the **Allow** check box.
- **Local Activation** - Select the **Allow** check box.
- **Remote Activation** - Select the **Allow** check box.

Step 14 Click **OK**.

Step 15 Click **OK**.

Step 16 Close the Component Services window.

You are now ready to configure Windows Management Instrumentation (WMI) on your Windows Server 2003.

Configuring WMI User Access for Server 2003

The user or group you configured for DCOM access must also have Windows Management Instrumentation (WMI) permission to access the Windows event logs required by QRadar Network Anomaly Detection.

To configure WMI User Access, perform the following steps:

Step 1 On your desktop, select **Start > Run**.

The Run window is displayed.

Step 1 Type the following:

```
wmimgmt.msc
```

Step 2 Click **OK**.

The Windows Management Infrastructure window is displayed.

Step 3 Right-click on **WMI Control (Local)**, and then click **Properties**.

Step 4 Click the **Security** tab.

Step 5 In the Namespace navigation, expand **Root**.

Step 6 In the menu tree, click **CIMV2**.

Step 7 Click **Security**.

The Security for ROOT\CIMV2 window is displayed.

Step 8 Select the user or group requiring WMI access.

Note: If the user or group requiring WMI access is not listed in the permissions list, you must add the user to the configuration.

Step 9 Configure the following user permissions:

- **Execute Methods** - Select the **Allow** check box.
- **Provider Write** - Select the **Allow** check box.
- **Enable Account** - Select the **Allow** check box.
- **Remote Enable** - Select the **Allow** check box.

Note: If the user or group you are configuring is an Administrator, the allow permission check boxes might already be selected.

Step 10 Click **OK**.

The My Computer Properties window is displayed.

Step 11 Click **OK** to close the My Computer Properties window.

You must querying the Windows Server 2003 for event or security logs to complete the DCOM configuration by verify WMI communications.

Configure Windows Server 2008

To configure DCOM on Windows Server 2008, perform the following steps:

1. Verify the required Windows Server 2008 services are started. For more information, see **Required DCOM and WMI services for Windows Server 2008**.
2. Enable DCOM for Windows Server 2008. For more information, see **Enable DCOM for Windows Server 2008**.
3. Configure DCOM communications for Windows Server 2008. For more information, see **Configuring DCOM communications for Windows Server 2008**.
4. Configure User Accounts for DCOM. For more information, see **Configure Windows Server 2008 user accounts for DCOM**.
5. Configure Windows Server 2008 Firewall. For more information, see **Configure the Windows Server 2008 Firewall**.
6. Configure WMI for Windows Server 2008. For more information, see **Configuring WMI user access for Windows Server 2008**.
7. Test the WMI configuration. For more information, see **Verifying WMI communications**.

Required DCOM and WMI services for Windows Server 2008

The following Windows services for DCOM and WMI must be started and configured for automatic startup:

- Server
- Remote Registry
- Windows Management Instrumentation

To configure the Server and Remote Registry services for automatic startup, perform the following steps:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
services.msc
```

Step 3 Click **OK**.

The Services window is displayed.

Step 4 In the details pane, verify the following services are started and set to automatic startup:

- Server
- Remote Registry
- Windows Management Instrumentation

Step 5 To change a service property, right-click on the service name, and then click **Properties**.

Step 6 From the **Startup type** list box, select **Automatic**.

Step 7 If the Service status is not started, click **Start**.

Step 8 Click **OK**.

Step 9 Close the Services window.

You are now ready to enable DCOM on your Windows Server 2008.

Enable DCOM for Windows Server 2008

To enable DCOM on your Windows Server 2008, you must:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under **Component Services**, expand **Computers**, and then click **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **Default Properties** tab.

Step 7 Configure the following Default Properties:

a Select the **Enable Distributed COM on this computer** check box.

b Using the **Default Authentication Level** list box, select **Connect**.

c Using the **Default Impersonation Level** list box, select **Identify**.

Step 8 Click **OK**.

Step 9 Click **OK**.

Step 10 Close the Component Services window.

You are now ready to configure DCOM ports on your Windows Server 2008.

Configuring DCOM communications for Windows Server 2008

Windows Server 2008 requires TCP/IP communications for DCOM.

To configure DCOM TCP/IP communications, perform the following steps:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under Component Services, expand **Component Services**, expand **Computers**, and then click **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **Default Protocols** tab.

Step 7 Configure the following options:

a If Connection-oriented TCP/IP is listed in the DCOM Protocols window, go to Step **d**.

b If Connection-oriented TC/IP is not listed in the DCOM Protocol window, select **Add**.

The Select DCOM protocol window is displayed.

c From the **Protocol Sequence** list box, select **Connection-oriented TC/IP**.

d Click **OK**.

Step 8 Click **OK**.

Step 9 Close the Component Services window.

You are now ready to configure a user account with permission to access the host.

Configure Windows Server 2008 user accounts for DCOM

After you have enabled DCOM, you must assign an account the proper permission to access DCOM on the host. You must select an existing account with administrative access or create a normal user account that is a member of an administrative group to access the host.

To configure a user account for DCOM on Windows Server 2008, you must:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
dcomcnfg
```

Step 3 Click **OK**.

The Component Services window is displayed.

Step 4 Under Console Root, expand **Component Services**, expand **Computers**, and select **My Computer**.

Step 5 On the **Action** menu, click **Properties**.

Step 6 Select the **COM Security** tab.

Step 7 In **Access Permissions**, click **Edit Default**.

Step 8 Select the user or group requiring DCOM access.

Note: If the user or group requiring DCOM access is not listed in the permissions list, you must add the user to the configuration.

Step 9 Configure the following user permissions:

- **Local Access** - Select the **Allow** check box.
- **Remote Access** - Select the **Allow** check box.

Step 10 Click **OK**.

The My Computer Properties window is displayed.

Step 11 In **Launch and Activation Permissions**, click **Edit Default**.

Step 12 Select the user or group requiring DCOM access.

Note: If the user or group requiring DCOM access is not in the permissions list, you must add the user to the configuration.

Step 13 Configure the following user permissions:

- **Local Launch** - Select the **Allow** check box.
- **Remote Launch** - Select the **Allow** check box.
- **Local Activation** - Select the **Allow** check box.
- **Remote Activation** - Select the **Allow** check box.

Step 14 Click **OK**.

Step 15 Click **OK**.

Step 16 Close the Component Services window.

You are now ready to configure the firewall in Windows Server 2008. For more information, see **Configure the Windows Server 2008 Firewall**.

Configure the Windows Server 2008 Firewall

If you are using the Windows Server 2008 firewall on a firewall is located between the your Windows 2008 Server and QRadar Network Anomaly Detection, you must configure the firewall with an exception to permit DCOM communications.

Note: You must be an administrator to change Windows Firewall settings or add an exception to the Windows Firewall.

To add a Windows Firewall exception, you must:

Step 1 Click **Start > All Programs > Administrative Tools > Server Manager**.

Step 2 In the Server Manager menu, expand **Configuration**, expand **Windows Firewall with Advanced Security**.

Step 3 Select **Inbound Rules**.

Step 4 On the **Action** menu, click **New Rule**.

Step 5 Select **Custom** and click **Next**.

The Program window is displayed.

Step 6 Select **All programs**, and click **Next**.

The Protocol and Ports window is displayed.

Step 7 From the **Protocol type** list box, select **TCP** and click **Next**.

Note: We recommend you do not limit Local and Remote ports or local IP addresses, but define firewall connection rules by remote IP address.

Step 8 Under **Which remote IP addresses does this rule apply to?**, select **These IP addresses**.

Step 9 Select **These IP addresses**, click **Add**.

Step 10 In the **This IP address or subnet** text box, type the IP address of QRadar Network Anomaly Detection, click **OK**.

The Action window is displayed.

Step 11 Select **Allow the connection**, click **Next**.

The Profile window is displayed.

Step 12 Type the network profile to which the rule applies, click **Next**.

Step 13 Type a name and description for the firewall rule, click **Finish**.

Step 14 Close the Server Manager window.

You are now ready to configure Windows Management Instrumentation (WMI) on your Windows Server 2008.

Configuring WMI user access for Windows Server 2008

The user or group you configured for DCOM access must also have Windows Management Instrumentation (WMI) permission to access the Windows event logs required by QRadar Network Anomaly Detection.

To configure WMI User Access, you must:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
wmimgmt.msc
```

Step 3 Click **OK**.

The Windows Management Infrastructure window is displayed.

Step 4 Right-click on **WMI Control (Local)**, select **Properties**.

Step 5 Click the **Security** tab.

Step 6 In **Namespace navigation**, expand **Root**, click **CIMV2**.

Step 7 Click **Security**.

The Security for ROOT\CIMV2 window is displayed.

Step 8 Select the user or group requiring WMI access.

Note: If the user or group requiring WMI access is not listed in the permissions list, you must add the user to the configuration.

Step 9 Select the check boxes to add the following permissions:

- **Execute Methods** - Select the **Allow** check box.
- **Provider Write** - Select the **Allow** check box.
- **Enable Account** - Select the **Allow** check box.
- **Remote Enable** - Select the **Allow** check box.

Note: If the user or group you are configuring is a system administrator, the allow permission check boxes might be selected as the permissions are inherited.

Step 10 Click **OK**.

Step 11 Click **OK**.

Step 12 Close the WMIMGMT - WMI Control (Local) window.

Configuring Windows Server 2008 R2 64-bit Trusted Installer

Windows Server 2008 R2 64-bit incorporated a security feature called the Trusted Installer that can affect the connection to the DCOM object.

To add a Trusted Installer permission to the DCOM object:

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following:

```
regedit
```

Step 3 Click **OK**.

Note: You must be a system administrator to edit registry settings.

The Registry Editor window is displayed.

Step 4 Locate the following registry location:

```
HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
```

Step 5 Right-click the entry `{76A64158-CB41-11D1-8B02-00600806D9B6}`, then click **Permissions**.

The Permissions window is displayed.

Step 6 Click **Advanced**.

Step 7 Click the **Owner** tab.

The Trusted Installer is shown as the current owner.

Step 8 Select the **Administrators** group, click **OK**.

The Permissions window is displayed.

Step 9 Select the QRadar Network Anomaly Detection user, select the **Allow** check box for **Full Control** permission, and click **Apply**.

Note: If the QRadar Network Anomaly Detection user is not listed in the permissions list, you must add the user to the configuration.

Step 10 Click **Advanced**.

Step 11 Click the **Owner** tab.

Administrators is shown as the current owner.

Step 12 Select or add your QRadar Network Anomaly Detection user, click **OK**.

Note: If the QRadar Network Anomaly Detection user is not listed in the Change owner to permission list, you must select **Other users or groups** to add the user to the configuration.

Step 13 Click **OK** to return to the Registry Editor.

Step 14 Repeat **Step 5** to **Step 13** for the following registry key:

```
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
```

Step 15 Close the Registry Editor.

You must verify WMI communications by querying the Windows Server 2008 for security event logs to complete your DCOM configuration.

Verifying WMI communications

To assist with verifying your WMI communications, the Microsoft Windows Event Log protocol RPM includes a test tool that allows QRadar Network Anomaly Detection to query the remote server for Windows event log information.

To use this test tool, Your system must be running the latest version of the Windows Event Log protocol.

To query your Windows server, you must:

Step 1 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: `root`

Password: `<password>`

Step 2 Type the following command:

```
cd /opt/qradar/jars
```

Step 3 Type the following command:

```
java -jar WMITestTool-<date>.jar
```

Where `<date>` is the date of release for the WMI test tool.

Step 4 Configure the following parameters:

a **Remote Windows Host** - Type the IP address of your Windows server.

b **Active Directory Domain, or Hostname if in a Workgroup** - Type the domain or workgroup for your Windows server.

c **Username** - Type the username required to access the remote Windows server.

d **Password** - Type the username required to access the remote Windows server.

The test tool will attempt to connect to your remote Windows server.

Step 5 In the **WQL Query** parameter, type the following:

```
Select NumberOfRecords From Win32_NTEventLogFile WHERE
LogFileName='Security'
```

Note: The example query provided functions with 32-bit and 64-bit versions of Windows Server 2003 and Windows Server 2008.

If QRadar Network Anomaly Detection can successfully query your Windows server, the results of the security event log are returned.

For example:

```
-----
instance of Win32_NTEventlogFile
Name = C:\Windows\System32\Winevt\Logs\Security.evtx
NumberOfRecords = 5786
-----
```

If the returned query states total records = 0, or if there is an error, you must verify the proper services are running, your DCOM configuration, the WMI configuration, and your Windows firewall settings. If you have verified the configuration of your Windows server, contact support.

If you are having connection issues, we recommend using the test tool with the Windows Firewall temporarily disabled. If the test tool returns security event log results, enable the Windows Firewall and see your Network Administrator.

D 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.

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

INDEX

T

W

X