IBM Security QRadar SIEM
Version 7.1.0 MR1

Administration Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 307.

CONTENTS

3 MANAGING THE SYSTEM

4 MANAGING HIGH AVAILABILITY

5 SETTING UP QRADAR SIEM

C EVENT CATEGORIES

D NOTICES AND TRADEMARKS

INDEX

About This Guide

The *IBM Security QRadar SIEM Administration Guide* provides you with information for managing QRadar SIEM functionality requiring administrative access.

Intended Audience

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

Conventions

The following conventions are used throughout this guide:

- ▶ Indicates that the procedure contains a single instruction.

NOTE

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

CAUTION

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

WARNING

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

Technical Documentation

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

Contacting Customer Support

For information on contacting customer support, see the ***Support and Download Technical Note***.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 OVERVIEW

This overview includes general information on how to access and use the QRadar SIEM user interface and the **Admin** tab.

This section includes the following topics:

Supported Web Browsers

You can access the Console from a standard web browser. When you access the system, a prompt is displayed asking for a user name and a password, which must be configured in advance by the QRadar SIEM administrator.

Table 1-1 Supported Web Browsers

Web Browser	Supported Versions
Mozilla Firefox	• 10.0 Due to Mozilla's short release cycle, we cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.
Microsoft® Windows Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0 For instructions on how to enable Compatibility View, see **Enabling Compatibility View for Internet Explorer**.

Enabling Compatibility View for Internet Explorer

To enable Compatibility View for Internet Explorer 8.0 and 9.0:

Step 1 Press F12 to open the Developer Tools window.

Step 2 Configure the following compatibility settings:

Table 1-2 Internet Explorer Compatibility Settings

Browser Version	Option	Description
Internet Explorer 8.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 8.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**
Internet Explorer 9.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 9.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**

About the User Interface

You must have administrative privileges to access administrative functions. To access administrative functions, click the **Admin** tab on the QRadar SIEM user interface.

The **Admin** tab provides access to the following functions:

- Manage users. See **Managing User Roles and Accounts**.
- Manage your network settings. See **Managing the System**.
- Manage high availability. See **Managing High Availability**.
- Manage QRadar SIEM settings. See **Setting Up QRadar SIEM**.
- Manage references sets. See **Managing Reference Sets**.
- Manage authorized services. See **Managing Authorized Services**.
- Backup and recover your data. See **Managing Backup and Recovery**.
- Manage your deployment views. See **Using the Deployment Editor**.
- Manage flow sources. See **Managing Flow Sources**.
- Configure remote networks and remote services. See **Configuring Remote Networks and Services**.
- Discover servers. See **Discovering Servers**.
- Configure syslog forwarding. See **Forwarding Event Data**.
- Managing vulnerability scanners. For more information, see the *Managing Vulnerability Assessment Guide*.
- Configure plug-ins. For more information, see the associated documentation.

- Configure the IBM Security QRadar Risk Manager. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.
- Manage log sources. For more information, see the *IBM Security QRadar Log Sources Users Guide.*

Using the Admin Tab

The **Admin** tab provides several tab and menu options that allow you to configure QRadar SIEM, including:

- **System Configuration** - Provides access to administrative functionality, such as automatic updates, backup and recovery, Console configuration, global system notifications, network hierarchy, system and license management, system settings, reference set management, user management, authentication, and authorized services.
- **Data Sources** - Provides access to log source management, forwarding destinations, routing rules, custom event and flow properties, event and flow retention buckets, flow sources management, and vulnerability scanner management.
- **Remote Networks and Services Configuration** - Provides access to QRadar SIEM remote networks and services.
- **Plug-ins** - Provides access to plug-in components, such as the plug-in for the IBM Security QRadar Risk Manager. This option is only displayed if there are plug-ins installed on your Console.

The **Admin** tab also includes several menu options, including:

Table 1-3 Admin Tab Menu Options

Menu Option	Description
Deployment Editor	Opens the Deployment Editor window. For more information, see **Using the Deployment Editor**.
Deploy Changes	Deploys any configuration changes from the current session to your deployment. For more information, see **Deploying Changes**.
Advanced	The Advanced menu provides the following options: **Clean SIM Model** - Resets the SIM module. See **Resetting SIM**. **Deploy Full Configuration** - Deploys all configuration changes. For more information, see **Deploying Changes**.

Deploying Changes

When you update your configuration settings using the **Admin** tab, your changes are saved to a staging area where they are stored until you manually deploy the changes.

Each time you access the **Admin** tab and each time you close a window on the **Admin** tab, a banner at the top of the **Admin** tab displays the following message: **`Checking for undeployed changes.`**

If undeployed changes are found, the banner updates to provide information about the undeployed changes.

To view the detailed undeployed changes:

Step 1 Click **View Details**.

The details are displayed in groups.

Step 2 Choose one of the following options:

- To expand a group to display all items, click the plus sign (+) beside the text. When done, you can click the minus sign (-).
- To expand all groups, click **Expand All**. When done, you can click **Collapse All**.

If the list of undeployed changes is lengthy, a scroll bar is provided to allow you to scroll through the list.

Step 3 Click **Hide Details** to hide the details from view again.

The banner message also recommends which type of deployment change to make. The two options are:

- **Deploy Changes** - Click the **Deploy Changes** icon on the **Admin** tab toolbar to deploy any configuration changes from the current session to your deployment.
- **Deploy Full Configuration** - Select **Advanced > Deploy Full Configuration** from the **Admin** tab menu to deploy all configuration settings to your deployment. All deployed changes are then applied throughout your deployment.

CAUTION

*When you click **Deploy Full Configuration**, QRadar SIEM restarts all services, resulting in a gap in data collection for events and flows until deployment completes.*

After you deploy your changes, the banner clears the list of undeployed changes and checks the staging area again for any new undeployed changes. If none are present, the following message is displayed: **`There are no changes to deploy.`**

Updating User Details

You can access your administrative user details through the main QRadar SIEM interface.

▶ To access your user details, click **Preferences**.

The User Details window is displayed, providing information such as your user name and email address. You can edit your administrative user details, if required. For more information on the pop-up notifications, see the *IBM Security QRadar SIEM Users Guide*.

Resetting SIM

Using the **Admin** tab, you can reset the SIM module, which allows you to remove all offense, source IP address, and destination IP address information from the database and the disk. This option is useful after tuning your deployment to avoid receiving any additional false positive information.

To reset the SIM module:

Step 1 Click the **Admin** tab.

Step 2 From the **Advanced** menu, select **Clean SIM Model**.

Step 3 Read the information on the Reset SIM Data Module window.

Step 4 Select one of the following options:

- **Soft Clean** - Closes all offenses in the database. If you select the **Soft Clean** option, you can also select the **Deactivate all offenses** check box.
- **Hard Clean** - Purges all current and historical SIM data including offenses, source IP addresses, and destination IP addresses.

Step 5 If you want to continue, select the **Are you sure you want to reset the data model?** check box.

Step 6 Click **Proceed**.

A message is displayed, indicating that the SIM reset process has started. This process can take several minutes, depending on the amount of data in your system.

Step 7 Click **Close**.

Step 8 When the SIM reset process is complete, reset your browser.

NOTE If you attempt to navigate to other areas of the QRadar SIEM user interface during the SIM reset process, an error message is displayed.

About High Availability

The High Availability (HA) feature ensures availability of QRadar SIEM data in the event of a hardware or network failure. Each HA cluster consists of a primary host and a standby secondary host. The secondary host maintains the same data as the primary host by either replicating the data on the primary host or accessing a shared external storage. At regular intervals, every 10 seconds by default, the secondary host sends a heartbeat ping to the primary host to detect hardware or network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host. HA is not supported in an IPv6 environment.

For more information on managing HA clusters, see **Managing High Availability**.

Monitoring QRadar SIEM Systems with SNMP

QRadar SIEM supports the monitoring of our appliances through SNMP polling. QRadar SIEM uses the Net-SNMP agent, which supports a variety of system resource monitoring MIBs that can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information on Net-SNMP, refer to Net-SNMP documentation.

2 MANAGING USER ROLES AND ACCOUNTS

When you initially configure IBM Security QRadar SIEM, you must create user accounts for all users that require access to QRadar SIEM.

This section includes the following topics:

User Management Overview

A user account defines the user name, default password, and email address for a user. For each new user account you create, you must assign the following items:

- **User Role** - Determines the privileges the user is granted to access functionality and information in QRadar SIEM. QRadar SIEM includes two default user roles: Admin and All. Before you add user accounts, you must create additional user roles to meet the specific permission requirement of your users.
- **Security Profile** - Determines the networks and log sources the user is granted access to. QRadar SIEM includes one default security profile for administrative users. The Admin security profile includes access to all networks and log sources. Before you add user accounts, you must create additional security profiles to meet the specific access requirements of your users.

After initial configuration, you can edit user accounts to ensure that user information is current. You can also add and delete user accounts as required.

Managing Roles

Before you can create user accounts, you must create the user roles required for your deployment. By default, QRadar SIEM provides a default administrative user role, which provides access to all areas of QRadar SIEM.

Users who are assigned an administrative user role cannot edit their own account. This restriction applies to the default Admin user role. Another administrative user must make any account changes.

This section includes the following topics:

Creating a Role

To create a role:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **User Roles** icon.

NOTE

You can also access the User Role Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

Two default user roles are listed in the left pane of the window: **Admin** and **All**. You can select a role in the left pane to view the associated role permissions in the right pane.

Step 4 On the toolbar, click **New**.

After you click **New**, the parameters in the right pane are cleared, allowing you to create a new user role.

Step 5 Configure the following parameters:

Table 2-1 User Role Management Window Parameters

Parameter	Description
User Role Name	Type a unique name for the role. The user role name must meet the following requirements: • Minimum of three characters • Maximum of 30 characters

Table 2-1 User Role Management Window Parameters (continued)

Parameter	Description
Admin	Select this check box to grant the user administrative access to the QRadar SIEM user interface. After you select the **Admin** check box, all permissions check boxes are selected by default. Within the Admin role, you can grant individual access to the following Admin permissions: • **Administrator Manager** - Select this check box to allow users to create and edit other administrative user accounts. If you select this check box, the **System Administrator** check box is automatically selected. • **Remote Networks and Services Configuration** - Select this check box to allow users to configure remote networks and services on the **Admin** tab. • **System Administrator** - Select this check box to allow users to access all areas of QRadar SIEM. Users with this access are not able to edit other administrator accounts.
Offenses	Select this check box to grant the user access to all **Offenses** tab functionality. Within the Offenses role, you can grant individual access to the following permissions: • **Assign Offenses to Users** - Select this check box to allow users to assign offenses to other users. • **Customized Rule Creation** - Select this check box to allow users to create custom rules. • **Manage Offense Closing Reasons** - Select this check box to allow users to manage offense closing reasons. For more information on the **Offenses** tab, see the *IBM Security QRadar SIEM Users Guide*.
Log Activity	Select this check box to grant the user access to all **Log Activity** tab functionality. Within the Log Activity role, you can also grant users individual access to the following permissions: • **Customized Rule Creation** - Select this check box to allow users to create rules using the **Log Activity** tab. • **Manage Time Series** - Select this check box to allow users to configure and view time series data charts. • **User Defined Event Properties** - Select this check box to allow users to create custom event properties. For more information on custom event properties, see the *IBM Security QRadar SIEM Users Guide*. For more information on the **Log Activity** tab, see the *IBM Security QRadar SIEM Users Guide*.

Table 2-1 User Role Management Window Parameters (continued)

Parameter	Description
Admin	Select this check box to grant the user administrative access to the QRadar SIEM user interface. After you select the **Admin** check box, all permissions check boxes are selected by default. Within the Admin role, you can grant individual access to the following Admin permissions: • **Administrator Manager** - Select this check box to allow users to create and edit other administrative user accounts. If you select this check box, the **System Administrator** check box is automatically selected. • **Remote Networks and Services Configuration** - Select this check box to allow users to configure remote networks and services on the **Admin** tab. • **System Administrator** - Select this check box to allow users to access all areas of QRadar SIEM. Users with this access are not able to edit other administrator accounts.
Offenses	Select this check box to grant the user access to all **Offenses** tab functionality. Within the Offenses role, you can grant individual access to the following permissions: • **Assign Offenses to Users** - Select this check box to allow users to assign offenses to other users. • **Customized Rule Creation** - Select this check box to allow users to create custom rules. • **Manage Offense Closing Reasons** - Select this check box to allow users to manage offense closing reasons. For more information on the **Offenses** tab, see the *IBM Security QRadar SIEM Users Guide*.
Log Activity	Select this check box to grant the user access to all **Log Activity** tab functionality. Within the Log Activity role, you can also grant users individual access to the following permissions: • **Customized Rule Creation** - Select this check box to allow users to create rules using the **Log Activity** tab. • **Manage Time Series** - Select this check box to allow users to configure and view time series data charts. • **User Defined Event Properties** - Select this check box to allow users to create custom event properties. For more information on custom event properties, see the *IBM Security QRadar SIEM Users Guide*. For more information on the **Log Activity** tab, see the *IBM Security QRadar SIEM Users Guide*.

Table 2-1 User Role Management Window Parameters (continued)

Parameter	Description
Assets	Select this check box to grant the user access to all **Assets** tab functionality. Within the Assets role, you can grant individual access to the following permissions: • **Perform VA Scans** - Select this check box to allow users to perform vulnerability assessment scans. For more information on vulnerability assessment, see the *Managing Vulnerability Assessment* guide. • **Remove Vulnerabilities** - Select this check box to allow user to remove vulnerabilities from assets. • **Server Discovery** - Select this check box to allow users to discover servers. • **View VA Data** - Select this check box to allow users access to vulnerability assessment data. For more information on vulnerability assessment, see the *Managing Vulnerability Assessment* guide.
Network Activity	Select this check box to grant the user access to all **Network Activity** tab functionality. Within the Network Activity role, you can grant individual access to the following permissions: • **Customized Rule Creation** - Select this check box to allow users to create rules using the **Network Activity** tab. • **Manage Time Series -** Select this check box to allow users to configure and view time series data charts. • **User Defined Flow Properties** - Select this check box to allow users to create custom flow properties. • **View Flow Content** - Select this check box to allow users access to flow data. For more information on viewing flows, see the *IBM Security QRadar SIEM Users Guide*. For more information on the **Network Activity** tab, see the *IBM Security QRadar SIEM Users Guide.*
Reports	Select this check box to grant the user access to all **Reports** tab functionality. Within the Reports role, you can grant users individual access to the following permissions: • **Distribute Reports via Email** - Select this check box to allow users to distribute reports through email. • **Maintain Templates** - Select this check box to allow users to edit reporting templates. For more information, see the *IBM Security QRadar SIEM Users Guide.*
IP Right Click Menu Extensions	Select this check box to grant the user access to options added to the right-click menu.

Table 2-1 User Role Management Window Parameters (continued)

Parameter	Description
Risks	This option is only available if IBM Security QRadar Risk Manager is activated. Select this check box to grant users access to IBM Security QRadar Risk Manager functionality. For more information, see the *IBM Security QRadar Risk ManagerUsers Guide.*

Step 6 Click **Save**.

The user role is added to the list in the left pane of the User Role Management window. The following message is displayed next to the **Save** icon: `User Role <role_name> saved`, where `<role_name>` is the name of the user role you added.

Step 7 Close the User Role Management window.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Editing a Role

To edit a role:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **User Roles** icon.

NOTE

You can also access the User Role Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

The left pane provides a list of user roles. You can select a role in the left pane to view the associated role permissions in the right pane.

Step 4 In the left pane, select the role you want to edit.

NOTE

You can locate a role by typing a role name in the **Type to filter** text box, which is located above the left pane.

Step 5 Update the parameters (see **Table 2-1**), as necessary.

Step 6 Click **Save**.

If you changed the name of the user role, the user role name is updated in the left pane. The user role parameters are updated in the right pane. The following message is displayed next to the **Save** icon: `User Role <role_name> saved`, where `<role_name>` is the name of the user role you edited.

Step 7 Close the User Role Management window.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a Role

To delete a role:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **User Roles** icon.

NOTE

You can also access the User Role Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

The left pane provides a list of user roles. You can select a role in the left pane to view the associated role permissions in the right pane.

Step 4 In the left pane, select the role you want to delete.

NOTE

You can locate a role by typing a role name in the **Type to filter** text box, which is located above the left pane.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

If user accounts are assigned to this user role, the **Users are Assigned to this User Role** window is displayed. Go to **Step 7**.

If no user accounts are assigned to this role, the user role is successfully deleted. go to **Step 8**.

Step 7 Reassign the listed user accounts to another user role:

a From the **User Role to assign** list box, select a user role.

b Click **Confirm**.

The user role is deleted and all listed user accounts are reassigned to the selected user role.

Step 8 Close the User Role Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Managing Security Profiles

The Security Profile Management feature allows you to create and manage security profiles. Security profiles define which networks and log sources a user can access. Using the Security Profile Management window, you can view, create, update, and delete security profiles.

This section includes the following topics:

- **Creating a Security Profile**
- **Editing a Security Profile**
- **Duplicating a Security Profile**
- **Deleting a Security Profile**

Creating a Security Profile

QRadar SIEM includes one default security profile for administrative users. The Admin security profile includes access to all networks and log sources. Before you add user accounts, you must create additional security profiles to meet the specific access requirements of your users.

To add a security profile:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Security Profiles** icon.

NOTE

You can also access the Security Profile Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

The left pane provides a list of security profiles. You can select a security profile in the left pane to view the associated Security Profile details in the right pane.

Step 4 On the toolbar, click **New**.

After you click **New**, the parameters in the right pane are cleared, allowing you to create a new security profile.

Step 5 Configure the following parameters:

Table 2-2 Security Profile Management Window Parameters

Parameter	Description
Security Profile Name	Type a unique name for the security profile. The security profile name must meet the following requirements: • Minimum of three characters • Maximum of 30 characters
Description	Optional. Type a description of the security profile. The maximum number of characters is 255.

The **Summary** tab is displayed; however, the summary is not editable. After you create this security profile, the **Summary** tab is populated.

Step 6 Click the **Permission Precedence** tab.

Permission precedence determines which Security Profile components to consider when displaying events in the **Log Activity** tab and flows in the **Network Activity** tab.

Step 7 In the Permission Precedence Setting pane, select a permission precedence option. Options include:

- **No Restrictions** - Select this option if you do not want to place restrictions on which events are displayed in the **Log Activity** tab and which flows are displayed in the **Network Activity** tab. This is the default permission precedence.

- **Network Only** - Select this option to restrict the user to only view events and flows associated with the networks specified in this security profile.
- **Log Sources Only** - Select this option to restrict the user to only view events associated with the log sources specified in this security profile.
- **Networks AND Log Sources** - Select this option to allow the user to only view events and flows associated with the log sources and networks specified in this security profile.

  For example, if an event is associated with a log source the security profile allows access to, but the destination network is restricted, the event is not displayed in the **Log Activity** tab. The event must match both requirements.
- **Networks OR Log Sources** - Select this option to allow the user to only view events and flows associated with the log sources or networks specified in this security profile.

  For example, if an event is associated with a log source the security profile allows access to, but the destination network is restricted, the event is displayed in the **Log Activity** tab. The event only needs to match one requirement.

Step 8 Configure the networks you want to assign to the security profile:

a Click the **Networks** tab.

b From the navigation tree in the left pane, locate and select the network you want this security profile to have access to. Choose one of the following options:

- From the **All Networks** list box, select a network group or network.
- Select the network group or network in the navigation tree.

NOTE

You can also select multiple network or network groups by holding the Control key while you select each network or network group you want to add.

c Click the Add (>) icon.

The added network is displayed in the Assigned Networks pane. To remove the network from the Assigned Networks pane, select the network and click the Remove (<) icon. To remove all selected networks, click **Remove All**.

d Repeat for each network you want to add.

Step 9 Configure the log sources you want to assign to the security profile:

a Click the **Log Sources** tab.

b From the navigation tree in the left pane, locate and select the log source group or log source you want this security profile to have access to. Choose one of the following options:

- From the **Log Sources** list box, select a log source group or log source.
- Double-click the folder icons in the navigation tree to navigate to a specific log source group or log source.

NOTE

You can also select multiple log source or log source groups by holding the Control key while you select each log source or log source groups you want to add.

c Click the Add (>) icon.

The added log source is displayed in the Assigned Log Sources pane. To remove the log source from the Assigned Log Sources pane, select the log source and click the Remove (<) icon. To remove all selected log sources, click **Remove All**.

d Repeat for each log source you want to add.

Step 10 Click **Save**.

Step 11 Close the Security Profile Management window.

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

Editing a Security Profile

To edit a security profile:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Security Profiles** icon.

NOTE

You can also access the Security Profiles Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

The left pane provides a list of security profiles. You can select a security profile in the left pane to view the associated Security Profile details in the right pane.

Step 4 In the left pane, select the security profile you want to edit.

NOTE

You can locate a security profile by typing a security profile name in the **Type to filter** text box, which is located above the left pane.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters as required. For more information on the Security Profile Management window parameters, see **Creating a Security Profile**.

Step 7 Click **Save**.

NOTE

If the **Security Profile Has Time Series Data** window is displayed, see **Step 8**.

The security profile is added to the list in the left pane of the Security Profile Management window. The following message is displayed next to the **Save** icon: `<security_profile_name> saved`, where `<security_profile_name>` is the name of the security profile you edited.

Step 8 If the **Security Profile Has Time Series Data** window is displayed, select one of the following options:

- **Keep Old Data and Save** - Select this option to keep previously accumulated time series data. Choosing this option can cause issues when users associated with this security profile views time series charts.
- **Hide Old Data and Save** - Select this option to hiding the time-series data. Choosing this option restarts time series data accumulation after you deploy your configuration changes.

If you changed the name of the security profile, the security profile name is updated in the left pane. The security profile parameters are updated in the right pane. The following message is displayed next to the **Save** icon: `<security_profile_name> saved`, where `<security_profile_name>` is the name of the security profile you edited.

Step 9 Close the Security Profile Management window.

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

Duplicating a Security Profile

To duplicate a security profile:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Security Profiles** icon.

NOTE

You can also access the Security Profiles Management window from the User Details window. The User Details window allows you to configure a user account. For more information on user accounts, see **Managing User Accounts**.

The left pane provides a list of security profiles. You can select a security profile in the left pane to view the associated Security Profile details in the right pane.

Step 4 In the left pane, select the security profile you want to duplicate.

NOTE

You can locate a security profile by typing a security profile name in the **Type to filter** text box, which is located above the left pane.

Step 5 On the toolbar, click **Duplicate**.

A confirmation window is displayed, requesting you to enter a name for the duplicated security profile.

Step 6 Type a unique name for the duplicated security profile.

Step 7 Click **OK**.

Step 8 Close the Security Profile Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a Security Profile

To delete a security profile:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Security Profiles** icon.

Step 4 In the left pane, select the security profile you want to delete.

NOTE

You can locate a security profile by typing a security profile name in the **Type to filter** text box, which is located above the left pane.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

If user accounts are assigned to this security profile, the **Users are Assigned to this Security Profile** window is displayed. Go to **Step 7**.

If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to **Step 8**.

Step 7 Reassign the listed user accounts to another security profile:

a From the **User Security Profile to assign** list box, select a security profile.

b Click **Confirm**.

The security profile is deleted and the user accounts are reassigned to the selected security profile.

Step 8 Close the Security Profile Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Managing User Accounts

When you initially configure QRadar SIEM, you must create user accounts for each of your users. After initial configuration, you may be required to create additional user accounts or edit existing user accounts.

When you create a new user account, you must assign access credentials, a user role, and a security profile to the user. User Roles define what actions the user has permission to perform. Security Profiles define what data the user has permission to access.

You can create multiple user accounts that include administrative privileges; however, any Administrator Manager user accounts can create other administrative user accounts.

This section includes the following topics:

- **Viewing User Accounts**
- **Creating a User Account**

- Editing a User Account
- Deleting a User Account

Viewing User Accounts

To view user accounts:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Users** icon.

The User Management window is displayed, providing the following information:

Table 2-3 User Management Window Parameters

Parameter	Description
Username	Displays the user name of this user account.
Description	Displays the description of the user account.
E-mail	Displays the email address of this user account.
User Role	Displays the user role assigned to this user account. User Roles define what actions the user has permission to perform.
Security Profile	Displays the security profile assigned to this user account. Security Profiles define what data the user has permission to access.

The User Management window toolbar provides the following functions:

Table 2-4 User Management Window Toolbar Functions

Function	Description
New	Click this icon to create a user account. For more information on creating a user account, see Creating a User Account.
Edit	Click this icon to edit the selected user account. For more information on editing a user account, see Editing a User Account.
Delete	Click this icon to delete the selected user account. For more information on deleting a user account, see Deleting a User Account.
Search Users	In this text box, you can type a keyword and then press Enter to locate a specific user account.

Creating a User Account

To create a user account:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Users** icon.

Step 4 On the toolbar, click **New**.

Step 5 Enter values for the following parameters:

Table 2-5 User Details Window Parameters

Parameter	Description
Username	Type a unique user name for the new user. The user name must contain a maximum 30 characters
E-mail	Type the user's email address. The email address must meet the following requirements: • Must be a valid email address • Minimum of 10 characters • Maximum of 255 characters
Password	Type a password for the user to gain access. The password must meet the following criteria: • Minimum of five characters • Maximum of 255 characters
Confirm Password	Type the password again for confirmation.
Description	Optional. Type a description for the user account. The maximum number of characters is 2,048.
User Role	From the list box, select the user role you want to assign to this user. To add, edit, or delete user roles, you can click the **Manage User Roles** link. For information on user roles, see **Managing Roles**.
Security Profile	From the list box, select the security profile you want to assign to this user. To add, edit, or delete security profiles, you can click the **Manage Security Profiles** link. For information on security profiles, see **Managing Security Profiles**.

Step 6 Click **Save**.

The following message is displayed next to the **Save** icon: `User <username> saved`, where `<username>` is the name of the user account you added. The user account is added to the User Management window.

Step 7 Close the User Details window.

Step 8 Close the User Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Editing a User Account

To edit a user account:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Users** icon.

Step 4 Select the user account you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update parameters, as necessary. See **Table 2-5**

Step 7 Click **Save**.

The following message is displayed next to the **Save** icon: `User <username> saved`, where `<username>` is the name of the user account you edited. The user account is updated in the User Management window.

Step 8 Close the User Details window.

Step 9 Close the User Management window.

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

Deleting a User Account

To delete a user account:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Users** icon.

Step 4 Select the user you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

Step 7 Close the User Management window.

This user no longer has access to the QRadar SIEM user interface. If this user attempts to log in to QRadar SIEM, the following message is displayed: **The username and password you supplied are not valid. Please try again**.

After you delete a user, items the user created, such as saved searches, reports, and assigned offenses, remain associated with the deleted user.

Authenticating Users

You can configure authentication to validate QRadar SIEM users and passwords. QRadar SIEM supports the following user authentication types:

- **System Authentication** - Users are authenticated locally by QRadar SIEM. This is the default authentication type.
- **RADIUS Authentication** - Users are authenticated by a Remote Authentication Dial-in User Service (RADIUS) server. When a user attempts to log in, QRadar SIEM encrypts the password only, and forwards the user name and password to the RADIUS server for authentication.
- **TACACS Authentication** - Users are authenticated by a Terminal Access Controller Access Control System (TACACS) server. When a user attempts to log in, QRadar SIEM encrypts the user name and password, and forwards this information to the TACACS server for authentication. TACACS Authentication uses Cisco Secure ACS Express as a TACACS server. QRadar SIEM supports

up to Cisco Secure ACS Express 4.3.

- **Active Directory** - Users are authenticated by a Lightweight Directory Access Protocol (LDAP) server using Kerberos.
- **LDAP** - Users are authenticated by a Native LDAP server.

To configure RADIUS, TACACS, Active Directory, or LDAP as the authentication type, you must:

- Configure the authentication server before you configure authentication in QRadar SIEM.
- Ensure the server has the appropriate user accounts and privilege levels to communicate with QRadar SIEM. See your server documentation for more information.
- Ensure the time of the authentication server is synchronized with the time of the QRadar SIEM server. For more information on setting QRadar SIEM time, see **Setting Up QRadar SIEM**.
- Ensure all users have appropriate user accounts and roles in QRadar SIEM to allow authentication with the vendor servers.

When authentication is configured and a user enters an invalid user name and password combination, a message is displayed indicating the login was invalid. If the user attempts to access the system multiple times using invalid information, the user must wait the configured amount of time before attempting to access the system again. For more information on configuring Console settings for authentication, see **Setting Up QRadar SIEM** - **Configuring the Console Settings**.

An administrative user can access QRadar SIEM through a vendor authentication module or by using the local QRadar SIEM Admin password. The QRadar SIEM Admin password still functions if you have set up and activated a vendor authentication module, however, you cannot change the QRadar SIEM Admin password while the authentication module is active. To change the QRadar SIEM admin password, you must temporarily disable the vendor authentication module, reset the password, and then reconfigure the vendor authentication module.

To configure authentication:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select the authentication type you want to configure.

Step 5 Configure the selected authentication type:

a If you selected **System Authentication,** go to **Step 6**.

b If you selected **RADIUS Authentication**, enter values for the following parameters:

Table 2-6 RADIUS Authentication Parameters

Parameter	Description
RADIUS Server	Type the host name or IP address of the RADIUS server.
RADIUS Port	Type the port of the RADIUS server.
Authentication Type	From the list box, select the type of authentication you want to perform. The options are: • **CHAP** (Challenge Handshake Authentication Protocol) - Establishes a Point-to-Point Protocol (PPP) connection between the user and the server. • **MSCHAP** (Microsoft® Challenge Handshake Authentication Protocol) - Authenticates remote Windows workstations. • **ARAP** (Apple Remote Access Protocol) - Establishes authentication for AppleTalk network traffic. • **PAP** (Password Authentication Protocol) - Sends clear text between the user and the server.
Shared Secret	Type the shared secret that QRadar SIEM uses to encrypt RADIUS passwords for transmission to the RADIUS server.

c If you selected **TACACS Authentication**, enter values for the following parameters:

Table 2-7 TACACS Authentication Parameters

Parameter	Description
TACACS Server	Type the host name or IP address of the TACACS server.
TACACS Port	Type the port of the TACACS server.
Authentication Type	From the list box, select the type of authentication you want to perform. The options are: • **ASCII** • **PAP** (Password Authentication Protocol) - Sends clear text between the user and the server. This is the default authentication type. • **CHAP** (Challenge Handshake Authentication Protocol) - Establishes a PPP connection between the user and the server. • **MSCHAP** (Microsoft Challenge Handshake Authentication Protocol) - Authenticates remote Windows workstations. • **MSCHAP2** (Microsoft Challenge Handshake Authentication Protocol version 2) - Authenticates remote Windows workstations using mutual authentication. • **EAPMD5** (Extensible Authentication Protocol using MD5 Protocol) - Uses MD5 to establish a PPP connection.
Shared Secret	Type the shared secret that QRadar SIEM uses to encrypt TACACS passwords for transmission to the TACACS server.

d If you selected **Active Directory**, enter values for the following parameters:

Table 2-8 Active Directory Parameters

Parameter	Description
Server URL	Type the URL used to connect to the LDAP server. For example, ldap://<host>:<port>
LDAP Context	Type the LDAP context you want to use, for example, DC=Q1LABS,DC=INC.
LDAP Domain	Type the domain you want to use, for example q1labs.inc.

e If you selected **LDAP**, enter values for the following parameters:

Table 2-9 LDAP Parameters

Parameter	Description
Server URL	Type the URL used to connect to the LDAP server. For example, ldap://<host>:<port> You can use a space-separated list to specify multiple LDAP servers.
SSL Connection	From the list box, select **True** to use Secure Socket Layer (SSL) encryption when connecting to the LDAP server. The default is True. Before enabling the SSL connection to your LDAP server, you must import the SSL certificate from the LDAP server to the your QRadar SIEM system. For more information on how to configure the SSL certificate, see **Configuring Your SSL Certificate**.
TLS Authentication	From the list box, select **True** to start Transport Layer Security (TLS) encryption when connecting to the LDAP server. The default is True.
Search Entire Base	From the list box, select one of the following options: • **True** - Enables searching all subdirectories of the specified Directory Name (DN). • **False** - Enables searching the immediate contents of the Base DN. The subdirectories are not searched. The default is True.
LDAP User Field	Type the user field identifier you want to search on, for example, uid. You can use a comma-separated list to search for multiple user identifiers.
Base DN	Type the base DN for performing searches, for example, DC=Q1LABS,DC=INC.

Step 6 Click **Save**.

Your authentication is now configured.

Configuring Your SSL Certificate

If you use LDAP for user authentication and you want to enable SSL, you must configure your SSL certificate.

To configure your SSL certificate for connection to your LDAP server:

Step 1 Using SSH, log in to QRadar SIEM as the root user.

User Name: **root**

Password: **<password>**

Step 2 Type the following command to create the /opt/qradar/conf/trusted_certificates/ directory:

```
mkdir -p /opt/qradar/conf/trusted_certificates
```

Step 3 Copy the SSL certificate from the LDAP server to the /opt/qradar/conf/trusted_certificates directory on your QRadar SIEM system.

Step 4 Verify that the certificate file name extension is .cert, which indicates that the certificate is trusted. QRadar SIEM only loads `.cert` files.

3 MANAGING THE SYSTEM

Using features in the System Configuration pane of the **Admin** tab, you can manage your license keys, restart or shut down your system, and configure access settings.

This section includes the following topics:

Managing Your License Keys

For your QRadar SIEM Console, a default license key provides you access to the QRadar SIEM user interface for 5 weeks. You must manage your license key using the System and License Management window, which you can access using the **Admin** tab. This window provides the status of the license key for each system (host) in your deployment. Statuses include:

- **Valid** - The license key is valid.
- **Expired** - The license key has expired. To update your license key, see **Updating your License Key**.
- **Override Console License** - This host is using the Console license key. You can use the Console key or apply a license key for this system. If you want to use the Console license for any system in your deployment, click **Revert to Console** on the License window.

A license key allows a certain number of log sources to be configured in your system. If you exceed the limit of configured logs sources, as established by the license key, an error message is displayed. If additional log sources are auto-discovered, they are automatically disabled. To extend the number of log sources allowed, contact your marketing representative.

This section includes the following topics:

Updating your License Key

For your QRadar SIEM Console, a default license key provides you with access to the QRadar SIEM user interface for 5 weeks. Choose one of the following options for assistance with your license key:

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

If you log in to QRadar SIEM and your Console license key has expired, you are automatically directed to the System and License Management window. You must update the license key before you can continue. If one of your non-Console systems includes an expired license key, a message is displayed when you log in indicating a system requires a new license key. You must navigate to the System and License Management window to update that license key.

To update your license key:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

The System and License Management window provides a list of all hosts in your deployment.

Step 4 Select the host for which you want to view the license key.

Step 5 From the **Actions** menu, select **Manage License**.

The License window provides the current license key limits. If you want to obtain additional licensing capabilities, contact your sales representative.

Step 6 Click **Browse** beside the **New License Key File** field and select the license key.

Step 7 Click **Open**.

Step 8 Click **Save**.

Step 9 On the System and License Management window, click **Deploy License Key**.

NOTE If you want to revert back to the previous license key, click **Revert to Deployed.** If you revert to the license key used by the QRadar SIEM Console system, click **Revert to Console**.

The license key information is updated in your deployment.

Exporting Your License Key Information

To export your license key information for all systems in your deployment:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

The System and License Management window provides a list of all hosts in your deployment.

Step 4 Select the system that includes the license you want to export.

Step 5 From the **Actions** menu, select **Export Licenses**.

Step 6 Select one of the following options:

- **Open with** - Opens the license key data using the selected application.
- **Save File** - Saves the file to your desktop.

Step 7 Click **OK**.

Restarting a System

To restart a QRadar SIEM system:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the system you want to restart.

Step 5 From the **Actions** menu, select **Restart System**.

NOTE

Data collection stops while the system is shutting down and restarting.

Shutting Down a System

To shutdown a QRadar SIEM system:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the system you want to shut down.

Step 5 From the **Actions** menu, select **Shutdown**.

NOTE

Data collection stops while the system is shutting down.

Configuring Access Settings

The System and License Management window provides access to the System Setup window, which allows you to configure firewall rules, interface roles, passwords, and system time.

This section includes the following topics:

- **Configuring Firewall Access**
- **Updating Your Host Setup**

- **Configuring Interface Roles**
- **Changing Passwords**
- **Updating System Time**

NOTE

If you require network setting changes, such as changing an IP address, to your Console and non-Console systems after your deployment is initially installed, you must use the **`qchange_netsetup`** utility to make these changes. For more information on changing network settings, see the *IBM Security QRadar SIEM Installation Guide*.

Configuring Firewall Access

You can configure local firewall access to enable communications between devices and QRadar SIEM. Also, you can define access to the System Setup window.

To enable QRadar SIEM managed hosts to access specific devices or interfaces:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure firewall access settings.

Step 5 From the **Actions** menu, select **Manage System.**

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE

The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > Local Firewall.**

Step 8 In the **Device Access** box, you must include any QRadar SIEM systems you want to access to this managed host. Only the listed managed hosts have access. For example, if you only enter one IP address, only that IP address is granted access to the managed host. All other managed hosts are blocked.

To configure access:

a In the **IP Address** field, type the IP address of the managed host you want to have access.

b From the **Protocol** list box, select the protocol you want to enable access for the specified IP address and port. Options include:

- **UDP** - Allows UDP traffic.
- **TCP** - Allows TCP traffic.
- **Any** - Allows any traffic.

c In the **Port** field, type the port on which you want to enable communications.

NOTE

If you change the **External Flow Source Monitoring Port** parameter in the QFlow configuration, you must also update your firewall access configuration. For more information about QFlow configuration, see **Using the Deployment Editor**.

d Click **Allow**.

Step 9 In the **System Administration Web Control** box, type the IP addresses of managed hosts that you want to allow access to the System Setup window in the **IP Address** field. Only IP addresses listed have access to the QRadar SIEM user interface. If you leave the field blank, all IP addresses have access. Click **Allow**.

NOTE

Make sure you include the IP address of your client desktop you want to use to access the QRadar SIEM user interface. Failing to do so may affect connectivity.

Step 10 Click **Apply Access Controls**.

Wait for the System Setup window to refresh before continuing to another task.

Updating Your Host Setup

You can use the System Setup window to configure the mail server you want QRadar SIEM to use and the global password for QRadar SIEM configuration:

To configure your host setup:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to update your host setup settings.

Step 5 From the **Actions** menu, select **Manage System.**

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE

The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > QRadar Setup**.

Step 8 In the **Mail Server** field, type the address for the mail server you want QRadar SIEM to use. QRadar SIEM uses this mail server to distribute alerts and event messages. To use the mail server provided with QRadar SIEM, type **localhost**.

Step 9 In the **Enter the global configuration password**, type the password you want to use to access the host. Type the password again for confirmation.

The global configuration password does not accept special characters. The global configuration password must be the same throughout your deployment. If you edit this password, you must also edit the global configuration password on all systems in your deployment.

Step 10 Click **Apply Configuration**.

Configuring Interface Roles

You can assign specific roles to the network interfaces on each managed host.

To assign roles:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure interface role settings.

Step 5 From the **Actions** menu, select **Manage System.**

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > Network Interfaces**.

The Network Interfaces page provides a list of each interface on your managed host.

NOTE For assistance with determining the appropriate role for each interface, contact Customer Support.

Step 8 For each interface listed, select the role you want to assign to the interface from the **Role** list box.

Step 9 Click **Save Configuration**.

Step 10 Wait for the System Setup window to refresh before continuing.

Changing Passwords

To change the passwords:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure interface role settings.

Step 5 From the **Actions** menu, select **Manage System**.

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > Root Password**.

Step 8 Update the passwords:

Make sure you record the entered values. The root password does not accept the following special characters: apostrophe (‘), dollar sign ($), exclamation mark (!).

- **New Root Password** - Type the root password necessary to access the System Setup window.
- **Confirm New Root Password** - Type the password again for confirmation.

Step 9 Click **Update Password**.

Updating System Time

You are able to change the time for the following options:

- System time
- Hardware time
- Time Zone
- Time Server

NOTE

All system time changes must be made within the System Time page. You can only change the system time information on the host operating the Console. The change is then distributed to all managed hosts in your deployment.

You can configure time for your system using one of the following methods:

- **Configuring Your Time Server Using RDATE**
- **Manually Configuring Time Settings For Your System**

Configuring Your Time Server Using RDATE

To update the time settings using RDATE:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure system time settings.

Step 5 From the **Actions** menu, select **Manage System**.

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE

The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > System Time**.

Step 8 Configure the time zone:

a Click the **Change time zone** tab.

b From the **Change timezone to** list box, select the time zone in which this managed host is located.

c Click **Save**.

Step 9 Configure the time server:

a Click the **Time server sync** tab.

b Configure the following parameters:

Table 3-1 Time Server Parameters

Parameter	Description
Timeserver hostnames or addresses	Type the time server host name or IP address.
Set hardware time too	Select the check box if you want to set the hardware time.
Synchronize on schedule?	Select one of the following options: • **No** - Select this option if you do not want to synchronize the time. Go to **c**. • **Yes** - Select this option if you want to synchronize the time.
Simple Schedule	Select this option if you want the time update to occur at a specific time. After you select this option, select a simple schedule from the list box.
Times and dates are selected below	Select this option to specify time you want the time update to occur. After you select this option, select the times and dates in the list boxes.

c Click **Sync and Apply**.

Manually Configuring Time Settings For Your System

To update the time settings for your system:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure system time settings.

Step 5 From the **Actions** menu, select **Manage System**.

Step 6 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

NOTE The user name and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > System Time**.

Step 8 Click the **Set time** tab.

The Set Time page is divided into tabs. You must save each setting before continuing. For example, when you configure system time, you must click **Apply** in the System Time pane before continuing.

Step 9 Set the system time:

a Choose one of the following options:

- In the System Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
- Click **Set system time to hardware time**.

b Click **Apply**.

Step 10 Set the hardware time:

a Choose one of the following options:

- In the Hardware Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
- Click **Set hardware time to system time**.

b Click **Save**.

Step 11 Configure the time zone:

a Click the **Change time zone** tab.

b From the **Change Timezone To** list box, select the time zone in which this managed host is located.

c Click **Save**.

4 MANAGING HIGH AVAILABILITY

The High Availability (HA) feature ensures QRadar SIEM data remains available in the event of a hardware or network failure. Before you begin, we recommend that you review the requirements and considerations for deploying an HA solution in your environment. For more information, see the *Managing High Availability Guide*.

This section includes the following topics:

Adding an HA Cluster

The System and License Management window allows you to manage your HA clusters.

To add an HA cluster:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the host for which you want to configure HA.

Step 5 From the **Actions** menu, select **Add HA Host**.

If the primary host is a Console, a warning message indicates that the QRadar SIEM user interface restarts after you add the HA host. Click **OK** to proceed.

NOTE If you do not want to view the Welcome to the High Availability page again, select the **Skip this page when running the High Availability wizard** check box.

Step 6 Read the introductory text. Click **Next**.

The Select the High Availability Wizard Options page automatically displays the Cluster Virtual IP address, which is the IP address of the primary host (Host IP).

Step 7 To configure the HA host information, configure the following parameters:

Table 4-1 HA Host Information Parameters

Parameter	Description
Primary Host IP Address	Type a new primary host IP address. The new primary host IP address is assigned to the primary host, replacing the previous IP address. The current IP address of the primary host becomes the Cluster Virtual IP address. If the primary host fails and the secondary host becomes active, the Cluster Virtual IP address is assigned to the secondary host. The new primary host IP address must be on the same subnet as the Host IP.
Secondary Host IP Address	Type the IP address of the secondary host you want to add. The secondary host must be in the same subnet as the primary host.
Enter the root password of the host	Type the root password for the secondary host.
Confirm the root password of the host	Type the root password for the secondary host again for confirmation.

Step 8 Optional. To configure advanced parameters:

a Click the arrow beside **Show Advanced Options**.

The advanced option parameters are displayed.

b Configure the following parameters:

Table 4-2 Advanced Options Parameters

Parameter	Description
Heartbeat Intervals (seconds)	Type the time, in seconds, you want to elapse between heartbeat messages. The default is 10 seconds. At the specified interval, the secondary host sends a heartbeat ping to the primary host to detect hardware and network failure. For more information on failover scenarios, see the *Managing High Availability Guide*.
Heartbeat Timeout (seconds)	Type the time, in seconds, you want to elapse before the primary host is considered unavailable if there is no heartbeat detected. The default is 30 seconds. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host. For more information on failover scenarios, see the *Managing High Availability Guide*.

Table 4-2 Advanced Options Parameters (continued)

Parameter	Description
Network Connectivity Test List peer IP addresses (comma delimited)	Type the IP addresses of the hosts you want the secondary host to ping, as a means to test it's own network connection. The default is all other managed hosts in your deployment. For more information on network connectivity testing, see the *Managing High Availability Guide*.
Disk Synchronization Rate (MB/s)	Type or select the disk synchronization rate. The default is 100 MB/s. When you initially add an HA cluster, the first disk synchronization can take an extended period of time to complete, depending on size of your /store partition and your disk synchronization speed. For example, the initial disk synchronization can take up to 24 hours or more. The secondary host only assumes the Standby status after the initial disk synchronization is complete. We require that the connection between the primary host and secondary host have a minimum bandwidth of 1 gigabits per second (Gbps).
Disable Disk Replication	Select this option if you want to disable disk replication. This option is only visible for non-Console hosts.

c Click **Next**.

The HA Wizard connects to the primary and secondary host to perform the following validations:

- Verifies that the secondary host has a valid HA activation key.
- Verifies that the secondary host is not already added to another HA cluster.
- Verifies that the software versions on the primary and secondary hosts are the same.
- Verifies that the primary and secondary hosts support the same Device Support Module (DSM), scanner, and protocol RPMs.
- Verifies if the primary host has an externally mounted storage system. If it does, the HA wizard then verifies that the secondary host also has an externally mounted storage system.

If any of these validations fail, the HA wizard displays an error message and then closes.

CAUTION

If the primary host is configured with external storage, you must configure the secondary host with the same external storage before continuing.

Step 9 Review the information. Click **Finish**.

If Disk Synchronization is enabled, it can take 24 hours or more for the data to initially synchronize.

NOTE

If required, click **Back** to return to the Confirm the High Availability Wizard Options page to edit the information.

The System and License Management window displays the HA cluster you added. Use the **Arrow** icon to display or hide the secondary host.

The System and License Management window provides the status of your HA clusters, including:

Table 4-3 HA Status Descriptions

Status	Description
Active	Specifies that the host is acting as the active system with all services running. Either the primary or secondary host can display the Active status. If the secondary host is displaying the Active status, failover has occurred.
Standby	Specifies that the host is acting as the standby system. This status will only display for a secondary host. The standby system has no services running. If disk replication is enabled, the standby system is replicating data from the primary host. If the primary host fails, the standby system automatically assumes the active role.
Failed	Specifies that the host is in a failed state. Both the primary or secondary host can display the Failed status: • If the primary host displays the Failed status, the secondary host takes over the services and should now display the Active status. • If the secondary host displays the Failed status, the primary host remains active, but is not protected by HA. A system in the failed state must be manually repaired (or replaced), and then restored. See **Restoring a Failed Host**. ***Note:*** *Depending on the type of failure that caused the failover, you may not be able to access a failed system from the Console.*

Table 4-3 HA Status Descriptions (continued)

Status	Description
Synchronizing	Specifies that the host is synchronizing data on the local disk of the host to match the currently active system. ***Note:*** *This status is only displayed if disk replication is enabled.*
Online	Specifies that the host is online.
Offline	Specifies that the host is offline. All processes are stopped and the host is not monitoring the heartbeat from the active system. Both the primary and the secondary can display the Offline status. While in the Offline state, disk replication continues if it is enabled.
Restoring	After you select **High Availability > Restore System** to restore a failed host (see **Restoring a Failed Host**), this status specifies that system is in the process of restoring.
Needs License	Specifies that a license key is required for the HA cluster. See **Managing the System** - **Updating your License Key**. In the Needs License state, no processes are running.
Setting Offline	Specifies that the host is in the process of changing state from online to offline.
Setting Online	Specifies that the host is in the process of changing state from offline to online.
Needs Upgrade	Specifies that the host requires a software upgrade, because the primary host has been upgraded to a newer software version. If the secondary host displays the Needs Upgrade status, the primary host remains active, but is not protected by HA. Heartbeat monitoring and disk replication, if enabled, continue to function. ***Note:*** *Only a secondary host can display a Needs Upgrade status.*

Table 4-3 HA Status Descriptions (continued)

Status	Description
Upgrading	Specifies that the host is in the process of upgrading software. If the secondary host displays the Upgrading status, the primary host remains active, but is not protected by HA. Heartbeat monitoring and disk replication, if enabled, continue to function. ***Note:*** *After Device Service Modules (DSMs) or protocols are installed on a Console and the configuration changed are deployed, the Console replicates the DSM and protocol updates to its managed hosts. Then, when HA replication occurs between a primary and secondary hosts, DSM and protocols updates are installed on the secondary host.* ***Note:*** *Only a secondary host can display an Upgrading status.*

Editing an HA Cluster

Using the Edit HA Host feature, you can edit the advanced options for your HA cluster.

To edit an HA cluster:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the row for the HA cluster you want to edit.

Step 5 From the **High Availability** menu, select **Edit HA Host**.

Step 6 Edit the parameters in the advanced options section. See **Table 4-2**.

Step 7 Click **Next**.

Step 8 Review the information. Click **Finish**.

The secondary host restarts and your HA cluster continues functioning.

Removing an HA Host

You can remove an HA host from a cluster. You cannot remove a host from an HA cluster when the primary HA host is in the Failed, Offline, or Synchronizing state.

To remove an HA host:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the HA host you want to set to remove.

Step 5 From the **High Availability** menu, select **Remove HA Host**.

A confirmation message is displayed, indicating that removing an HA host reboots the QRadar SIEM user interface.

Step 6 Click **OK**.

After you remove an HA host, the host restarts and becomes available to be added to another cluster.

Setting an HA Host Offline

You can set either the primary or secondary host to Offline from the Active or Standby state. If you set the active system to Offline, the standby system becomes the active system, thereby forcing a failover. If you set the standby system to Offline, the standby system no longer monitors the heartbeat of the active system, however, continues to synchronize data from the active system.

To set an HA host offline:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the HA host you want to set to offline.

Step 5 From the **High Availability** menu, select **Set System Offline**.

The status for the host changes to Offline.

Setting an HA Host Online

When you set the secondary host to online, the secondary host becomes the standby system. If you set the primary host to Online while the secondary system is currently the active system, the primary host becomes the active system and the secondary host automatically becomes the standby system.

To set an HA host online:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System and License Management** icon.

Step 4 Select the offline HA host you want to set to online.

Step 5 From the **High Availability** menu, select **Set System Online**.

The status for the host changes to Online.

Restoring a Failed Host

If a host displays a status of Failed, a hardware or network failure occurred for that host. Before you can restore the host using the QRadar SIEM user interface, you must manually repair the host. For more information, see your network administrator.

To restore a failed system:

Step 1 Recover the failed host.

NOTE

Recovering a failed host involves re-installing QRadar SIEM. For more information on recovering a failed host, see the *IBM Security QRadar SIEM Installation Guide*. If you are recovering a primary host and your HA cluster uses shared storage, you must manually configure iSCSI. For more information on configuring iSCSI, see the *Configuring iSCSI Technical Note*.

Step 2 Click the **Admin** tab.

Step 3 On the navigation menu, click **System Configuration**.

Step 4 Click the **System and License Management** icon.

Step 5 Select the failed HA host you want to restore.

Step 6 From the **High Availability** menu, select **Restore System**.

The system restores the HA configuration on the failed host. The status of the host changes through the following sequence:

a Restoring

b Synchronizing (if disk synchronization is enabled)

c Standby (secondary host) or Offline (primary host)

If the restored host is the primary system, you must manually set the primary system to the Online state. See **Setting an HA Host Online**.

5 SETTING UP QRADAR SIEM

Using various options on the **Admin** tab, you can configure your network hierarchy, automatic updates, system settings, event and flow retention buckets, system notifications, console settings, offense close reasons, and index management.

This section includes the following topics:

Creating Your Network Hierarchy

QRadar SIEM uses the network hierarchy to understand your network traffic and provide you with the ability to view network activity for your entire deployment.

When you develop your network hierarchy, you should consider the most effective method for viewing network activity. The network you configure in QRadar SIEM does not have to resemble the physical deployment of your network. QRadar SIEM supports any network hierarchy that can be defined by a range of IP addresses. You can create your network based on many different variables, including geographical or business units.

Best Practices

Consider the following best practices when defining your network hierarchy:

- To create a clear view of your network, group together systems and user groups that have similar behavior.
- If your deployment is processing more than 600,000 flows, create multiple top-level groups.
- Organize your systems and networks by role or similar traffic patterns. For example, mail servers, departmental users, labs, or development groups. This

organization allows you to differentiate network behavior and enforce network management security policies.

- Do not group a server that has unique behavior with other servers on your network. Placing a unique server alone provides the server greater visibility in QRadar SIEM, allowing you to manage specific policies.
- Within a group, place servers with high volumes of traffic, such as mail servers, at the top of the group. This provides you with a clear visual representation when a discrepancy occurs.
- Do not configure a network group with more than 15 objects. Large network groups can cause you difficulty in viewing detailed information for each object.
- Combine multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network group to conserve disk space. For example:

Group	Description	IP Address
1	Marketing	10.10.5.0/24
2	Sales	10.10.8.0/21
3	Database Cluster	10.10.1.3/32
		10.10.1.4/32
		10.10.1.5/32

- Add key servers as individual objects and group other major but related servers into multi-CIDR objects.
- Define an all-encompassing group so when you define new networks, the appropriate policies and behavioral monitors are applied. For example:

Group	Subgroup	IP Address
Cleveland	Cleveland misc	10.10.0.0/16
Cleveland	Cleveland Sales	10.10.8.0/21
Cleveland	Cleveland Marketing	10.10.1.0/24

If you add a new network to the above example, such as 10.10.50.0/24, which is an HR department, the traffic is displayed as Cleveland-based and any rules applied to the Cleveland group are applied by default.

Defining Your Network Hierarchy

To define your network hierarchy:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Network Hierarchy** icon.

Step 4 From the menu tree, select the area of the network in which you want to add a network object.

Step 5 Click **Add**.

Step 6 Configure the following parameters:

Table 5-1 Add New Object Parameters

Parameter	Action
Group	From the list box, select the group in which you want to add the new network object. If required, you can create a new group. **1** Click **Add Group**. **2** Type a unique name for the group. **3** Click **OK**.
Name	Type a unique name for the object.
Weight	Type or select the weight of the object. The range is 0 to 100 and indicates the importance of the object in the system.
IP/CIDR(s)	Type the CIDR range for this object and click **Add**. For more information on CIDR values, see **Acceptable CIDR Values**.
Description	Type a description for this network object.
Color	Click **Select Color** and select a color for this object.
Database Length	From the list box, select the database length.

Step 7 Click **Save**.

Step 8 Repeat for all network objects.

Step 9 Click **Re-Order**.

Step 10 Organize the network objects as required.

Step 11 Click **Save**.

Acceptable CIDR Values

The following table provides a list of the CIDR values that QRadar SIEM accepts:

Table 5-2 Acceptable CIDR Values

CIDR Length	Mask	Number of Networks	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176

Table 5-2 Acceptable CIDR Values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 subnets	124
/26	255.255.255.192	4 subnets	62
/27	255.255.255.224	8 subnets	30
/28	255.255.255.240	16 subnets	14
/29	255.255.255.248	32 subnets	6
/30	255.255.255.252	64 subnets	2
/31	255.255.255.254	none	none
/32	255.255.255.255	1/256 C	1

For example, a network is called a supernet when the prefix boundary contains fewer bits than the natural (or classful) mask of the network. A network is called a subnet when the prefix boundary contains more bits than the natural mask of the network:

- 209.60.128.0 is a class C network address with a mask of /24.
- 209.60.128.0 /22 is a supernet that yields:

  209.60.128.0 /24

  209.60.129.0 /24

  209.60.130.0 /24

  209.60.131.0 /24
- 192.0.0.0 /25

  Subnet Host Range

0 192.0.0.1-192.0.0.126

1 192.0.0.129-192.0.0.254

- 192.0.0.0 /26

  Subnet Host Range

  0 192.0.0.1 - 192.0.0.62

  1 192.0.0.65 - 192.0.0.126

  2 192.0.0.129 - 192.0.0.190

  3 192.0.0.193 - 192.0.0.254

- 192.0.0.0 /27

  Subnet Host Range

  0 192.0.0.1 - 192.0.0.30

  1 192.0.0.33 - 192.0.0.62

  2 192.0.0.65 - 192.0.0.94

  3 192.0.0.97 - 192.0.0.126

  4 192.0.0.129 - 192.0.0.158

  5 192.0.0.161 - 192.0.0.190

  6 192.0.0.193 - 192.0.0.222

  7 192.0.0.225 - 192.0.0.254

Managing Automatic Updates

QRadar SIEM uses system configuration files to provide useful characterizations of network data flows. You can automatically or manually update your configuration files to ensure your configuration files contain the latest network security information.

In HA deployments, the Automatic Update functionality is disabled on a secondary HA system if the system is the active host during a failover. Automatic updates are performed on the secondary HA system after the primary HA system is restored and set to the Online status.

Update files are available for manual download from the Qmmunity website:

https://qmmunity.q1labs.com

QRadar SIEM update files can include the following updates:

- Configuration updates, which include configuration file changes, vulnerability, QID map, and security threat information updates.
- DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, which include items such as updated JAR files.

- Minor updates, which include items such as additional Online Help content or updated scripts.

QRadar SIEM allows you to either replace your existing configuration files or integrate the updated files with your existing files to maintain the integrity of your current configuration and information.

After you install updates on your Console and deploy your changes, the Console updates its managed hosts if your deployment is defined in your deployment editor. For more information on using the deployment editor, see **Using the Deployment Editor**.

CAUTION

Failing to build your system and event views in the deployment editor before you configure automatic or manual updates results in your managed hosts not being updated.

The Console must be connected to the Internet to receive the updates. If your Console is not connected to the Internet, you must configure an internal update server for your Console to download the files from. For more information on setting up an automatic update server, see the *Setting Up a QRadar Update Server Technical Note*.

In a High Availability (HA) deployment, after you update your configuration files on a primary host and deploy your changes, the updates are automatically performed on the secondary host. If you do not deploy your changes, the updates are performed on the secondary host through an automated process that runs hourly.

This section includes the following topics:

- **Viewing Your Pending Updates**
- **Configuring Automatic Update Settings**
- **Scheduling an Update**
- **Clearing Scheduled Updates**
- **Checking for New Updates**
- **Manually Installing Automatic Updates**
- **Viewing Your Update History**
- **Restoring Hidden Updates**
- **Viewing the Autoupdate Log**

Viewing Your Pending Updates

Your system is preconfigured to perform weekly automatic 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 checking for new updates, see **Checking for New Updates**.

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 automatically displays the Check for Updates page, providing the following information:

Table 5-3 Check for Updates Window Parameters

Parameter	Description
Updates were installed	Specifies the date and time the last update was installed. If no updates have been installed, this following text is displayed: `No updates have been installed`.
Next Check for Updates	Specifies the date and time the next update is scheduled to be installed. If auto updates are disabled, the following text is displayed: `Auto Update Schedule is disabled`.
Name	Specifies the name of the update.
Type	Specifies the type of update. Types include: • DSM, Scanner, Protocol Updates • Minor Updates
Status	Specifies the status of the update. Status types include: • **New** - The update is not yet scheduled to be installed. • **Scheduled** - The update is scheduled to be installed. • **Installing** - The update is currently installing. • **Failed** - The updated failed to install.
Date to Install	Specifies the date on which this update is scheduled to be installed.

The Check for Updates page toolbar provides the following functions:

Table 5-4 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 **Restoring Hidden Updates**.

Table 5-4 Check for Updates Page Parameters Toolbar Functions (continued)

Function	Description
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 **Manually Installing Automatic Updates**.
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 **Scheduling an Update**.
Unschedule	From this list box, you can remove preconfigured schedules for manually installing updates on your Console. For more information, see **Scheduling an Update**.
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.

Configuring Automatic Update Settings

You can customize the automatic update settings to change the frequency, update type, server configuration, and backup settings.

To configure automatic updates settings:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Change Settings**.

Step 5 In the Auto Update Schedule pane, configure the schedule for updates:

Table 5-5 Schedule Update Pane Parameters

Parameter	Description
Frequency	From this list box, select the frequency with which you want to receive updates. Options include: • Disabled • Weekly • Monthly • Daily The default frequency is Weekly.
Hour	From this list box, select the time of day you want your system to update. The default hour is 3 am.
Week Day	This option is only available if you select **Weekly** as the update frequency. ▶ From this list box, select the day of the week you want to receive updates. The default week day is Monday.
Month Day	This option is only active when you select Monthly as the update frequency. ▶ From this list box, select the day of the month you want to receive updates. The default month day is 1.

Step 6 In the Update Types pane, configure the types of updates you want to install:

Table 5-6 Choose Updates Pane Parameters

Parameter	Description
Configuration Updates	From this list box, select the method you want to use for updating your configuration files: • **Auto Integrate** - Select this option to integrate the new configuration files with your existing files and maintain the integrity of your information. This is the default setting. • **Auto Update** - Select this option to replace your existing configuration files with the new configuration files. • **Disable** - Select this option to prevent configuration updates.

Table 5-6 Choose Updates Pane Parameters (continued)

Parameter	Description
DSM, Scanner, Protocol Updates	From this list box, select one of the following options for DSM updates: • **Disable** - Select this option to prevent DSM, scanner, and protocol updates being installed on your system. • **Manual Install** - Select this option to download the DSM, scanner, and protocol updates to the designated download path location. If you choose this option, you must manually install the updates. See **Manually Installing Automatic Updates**. • **Auto Install** - Select this option to download the DSM, scanner, and protocol updates to the designated download path location and automatically install the update. This is the default setting.
Major Updates	From this list box, select one of the following options for major updates: • **Disable** - Select this option to prevent major updates being installed on your system. This is the default setting. • **Download** - Select this option to download the major updates to the designated download path location. If you choose this option, you must manually install the updates from a command line interface (CLI). See the readme file in the download files for installation instructions. ***Note:*** *Major updates cause service interruptions during installation.*
Minor Updates	From this list box, select one of the following options for minor updates: • **Disable** - Select this option to prevent minor updates being installed on your system. • **Manual Install**- Select this option to download the minor updates to the designated download path location. if you choose this option, you must manually install the updates. See **Manually Installing Automatic Updates**. • **Auto Install** - Select this option to automatically install minor updates on your system. This is the default setting.

Step 7 Select the **Auto Deploy** check box if you want to deploy update changes automatically after updates are installed.

If this check box is clear, a system notification is displayed on the **Dashboard** tab indicating that you must deploy changes after updates are installed. By default, the check box is selected.

Step 8 Select the **Auto Restart Service** check box if you want to restart the user interface service automatically after updates are installed.

When this option is enabled, automatic updates that require the user interface to restart is automatically performed. A user interface disruption occurs when the

service restarts. When this option is disabled, updates that require your user interface to restart are prevented from automatically installing. You can manually install the updated from the Check for Updates window.

Step 9 Click the **Advanced** tab.

Step 10 In the Server Configuration pane, configure the server settings:

Table 5-7 Server Configuration Pane Parameters

Parameter	Description
Web Server	Type the web server from which you want to obtain the updates. The default web server is: *https://qmmunity.q1labs.com*
Directory	Type the directory location on which the web server stores the updates. The default directory is autoupdates/.
Proxy Server	Type the URL for the proxy server. The proxy server is only required if the application server uses a proxy server to connect to the Internet.
Proxy Port	Type the port for the proxy server. The proxy port is only required if the application server uses a proxy server to connect to the Internet.
Proxy Username	Type the user name for the proxy server. A user name is only required if you are using an authenticated proxy.
Proxy Password	Type the password for the proxy server. A password is only required if you are using an authenticated proxy.

Step 11 In the Other Settings pane, configure the update settings:

Table 5-8 Update Settings Pane Parameters

Parameter	Description
Send feedback	Select this check box if you want to send feedback to IBM regarding the update. Feedback is sent automatically using a web form when errors occur with the update. By default, this check box is clear.
Backup Retention Period (days)	Type or select the length of time, in days, that you want to store files that are replaced during the update process. The files are stored in the location specified in the **Backup Location** parameter. The default backup retention period is 30 days. The minimum is 1 day and the maximum is 65535 years.
Backup Location	Type the location where you want to store backup files.
Download Path	Type the directory path location to which you want to store DSM, minor, and major updates. The default directory path is /store/configservices/staging/updates.

Step 12 Click **Save**.

Scheduling an Update

QRadar SIEM performs automatic updates on a recurring schedule according to the settings on the Update Configuration page; however, if you want to schedule an update or a set of updates to run at a specific time, you can schedule an update using the Schedule the Updates window. This 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

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.

Clearing Scheduled Updates

Scheduled updates display a status of **Scheduled** in the **Status** field. If required, you can clear a scheduled update.

To clear scheduled updates:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Optional. If you want to clear specific scheduled updates, select the updates you want to clear.

Step 6 From the **Unschedule** list box, select the type of scheduled update you want to clear. Options include:

- All Updates
- Selected Updates

- DSM, Scanner, Protocol Updates
- Minor Updates

Step 7 Click **OK**.

The selected updates are now cleared. The status of the update now displays as **New**.

Checking for New Updates

IBM provides updates on a regular basis. By default, the Auto Update feature is scheduled to automatically download and install updates. If you require an update at a time other than the preconfigured schedule, you can download new updates using the **Get new updates** icon.

To check for new updates:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Click **Get new updates**.

Step 6 Click **OK**.

The system retrieves the new updates from the Qmmunity website. This may take an extended period of time. When complete, new updates are listed on the Updates window.

Manually Installing Automatic Updates

IBM provides updates on a regular basis. By default, the Auto Update feature is scheduled to automatically download and install updates. If you want to install an update at a time other than the preconfigured schedule, you can install an update using the **Install** list box on the toolbar.

To manually install automatic updates:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Optional. If you want to install specific updates, select the updates you want to schedule.

Step 6 From the **Install** list box, select the type of update you want to install. Options include:

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

Viewing Your Update History

After an update was successfully installed or failed to install, the update is displayed on the View Update History page.

To view your update history:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **View Update History**.

The View Update History page provides the following information:

Table 5-9 View Update Window Parameters

Parameter	Description
Name	Specifies the name of the update.
Type	Specifies the type of update. Types include: • DSM, Scanner, Protocol Updates • Minor Updates
Status	Specifies the status of the update. Status types include: • Installed • Failed
Installed Date	Specifies the date on which the update was installed or failed.

Step 5 Optional. Using the **Search by Name** text box, you can type a keyword and then press Enter to locate a specific update by name.

Step 6 To investigate a specific update, select the update.

A description of the update and any installation error messages are displayed in the right pane.

Restoring Hidden Updates

Using the **Hide** icon, you can remove selected updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page.

To restore hidden updates:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Restore Hidden Updates**.

Step 5 Optional. To locate an update by name, type a keyword in the **Search by Name** text box and press Enter.

Step 6 Select the hidden update you want to restore.

Step 7 Click **Restore**.

Viewing the Autoupdate Log

The Autoupdate feature logs the most recent automatic update run on your system. You can view the Autoupdate log on the QRadar SIEM user interface using the View Log feature.

To view the Autoupdate log:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **View Log**.

The Autoupdate Log page is displayed.

Configuring System Settings

To configure system settings:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Settings** icon.

Step 4 Configure the following parameters:

Table 5-10 System Settings Parameters

Parameter	Description
System Settings	
Administrative Email Address	Type the email address of the designated system administrator. The default email address is root@localhost.
Alert Email From Address	Type the email address from which you want to receive email alerts. This address is displayed in the **From** field of the email alerts. A valid address is required by most email servers. The default email address is root@<hostname.domain>.
Resolution Interval Length	Resolution interval length determines at what interval the QRadar QFlow Collectors and Event Collectors send bundles of information to the Console. From the list box, select the interval length, in minutes. The options include: • 30 seconds • 1 minute (default) • 2 minutes ***Note:*** *If you select the **30 seconds** option, results are displayed on the QRadar SIEM user interface as the data enters the system. However, with shorter intervals, the volume of time series data is larger and the system may experience delays in processing the information.*

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Delete Root Mail	Root mail is the default location for host context messages. From the list box, select one of the following options: • **Yes** - Delete the local administrator email. This is the default setting. • **No** - Do not delete the local administrator email.
Temporary Files Retention Period	From the list box, select the period of time you want the system to retain temporary files. The default storage location for temporary files is the /store/tmp directory. The default retention period is 6 hours. The minimum is 6 hours and the maximum is 2 years.
Asset Profile Reporting Interval	Type or select the interval, in seconds, that the database stores new asset profile information. The default reporting interval is 900 seconds. The minimum is zero (0) and the maximum is 4294967294.
Asset Profile Query Period	From the list box, select the period of time for an asset search to process before a time-out occurs. The default query period is 1 day. The minimum is 1 day and 1 week.
VIS Passive Asset Profile Interval	Type or select the interval, in seconds, that the database stores all passive asset profile information. The default interval is 86400 seconds. The minimum is zero (0) and the maximum is 4294967294.
TNC Recommendation Enable	Trusted Network Computing (TNC) recommendations enable you to restrict or deny access to the network based on user name or other credentials. From the list box, select one of the following options: • **Yes** - Enables the TNC recommendation functionality. • **No** - Disables the TNC recommendation functionality. The default setting is No.
Coalescing Events	From the list box, select one of the following options: • **Yes** - Enables log sources to coalesce (bundle) events. • **No** - Prevents log sources from coalescing (bundling) events. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the **Coalescing Event** parameter in the log source configuration. For more information, see the *Managing Log Sources Guide*. The default setting is Yes.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Store Event Payload	From the list box, select one of the following options: • **Yes** - Enables log sources to store event payload information. • **No** - Prevents log sources from storing event payload information. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the **Event Payload** parameter in the log source configuration. For more information, see the *IBM Security QRadar Log Sources Users Guide*. The default setting is Yes.
Global Iptables Access	Type the IP addresses of non-Console systems that do not have iptables configuration to which you want to enable direct access. To enter multiple systems, type a comma-separated list of IP addresses.
Syslog Event Timeout (minutes)	Type or select the amount of time, in minutes, that the status of a syslog device is recorded as error if no events have been received within the timeout period. The status is displayed on the Log Sources window (for more information, see the *IBM Security QRadar Log Sources Users Guide*). The default setting is 720 minutes (12 hours). The minimum value is zero (0) and the maximum value is 4294967294.
Partition Tester Timeout (seconds)	Type or select the amount of time, in seconds, for a partition test to perform before a time-out occurs. The default setting is 30. The minimum is zero (0) and the maximum is 4294967294. The default setting is 86400.
Max Number of TCP Syslog Connections	Type or select the maximum number of Transmission Control Protocol (TCP) syslog connections you want to allow your system. The minimum is 0 and the maximum is 4294967294. The default is 2500.
Export Directory	Type the location where offense, event, and flow exports are stored. The default location is /store/exports.
Database Settings	
User Data Files	Type the location of the user profiles. The default location is /store/users.
Accumulator Retention - Minute-By-Minute	From the list box, select the period of time you want to retain minute-by-minute data accumulations. The default setting is 1 week. The minimum is 1 day and the maximum is 2 years. Every 60 seconds, the data is aggregated into a single data set.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Accumulator Retention - Hourly	From the list box, select the period of time you want to retain hourly data accumulations. The default setting is 33 days. The minimum is 1 day and the maximum is 2 years. At the end of every hour, the minute-by minute data sets are aggregated into a single hourly data set.
Accumulator Retention - Daily	From the list box, select the period of time you want to retain daily data accumulations. The default setting is 1 year. The minimum is 1 day and the maximum is 2 years. At the end of every day, the hourly data sets are aggregated into a single daily data set.
Payload Index Retention	From the list box, select the amount of time you want to store event and flow payload indexes. The default setting is 1 week. The minimum is 1 day and the maximum is 2 years. For more information on payload indexing, see the *Enabling Payload Indexing for Quick Filtering Technical Note*.
Offense Retention Period	From the list box, select the period of time you want to retain closed offense information. The default setting is 30 days. The minimum is 1 day and the maximum is 2 years. After the offense retention period has elapsed, closed offenses are purged from the database. ***Note:*** *Offenses can be retained indefinitely as long as they are not closed and they are still receiving events. The magistrate automatically closes an offense if the offense has not received an event for 5 days. This 5-day period is known as the dormant time. If an event is received during the dormant time, the dormant time is reset back to zero. When an offense is closed either by you or the magistrate, the* ***Offense Retention Period*** *setting is applied.*
Attacker History Retention Period	From the list box, select the amount of time that you want to store the attacker history. The default setting is 6 months. The minimum is 1 day and the maximum is 2 years.
Ariel Database Settings	
Flow Data Storage Location	Type the location that you want to store the flow log information. The default location is /store/ariel/flows. ***Note:*** *This is a global setting, applied to all Consoles and managed hosts in your deployment.*
Asset Profile Storage Location	Type the location where you want to store asset profile information. The default location is /store/ariel/hprof.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Asset Profile Retention Period	From the list box, select the period of time, in days, that you want to store the asset profile information. The default setting is 30 days. The minimum is 1 day and the maximum is 2 years.
Log Source Storage Location	Type the location where you want to store the log source information. The default location is /store/ariel/events. ***Note:*** *This is a global setting, applied to Consoles and managed hosts in your deployment.*
Search Results Retention Period	From the list box, select the amount of time you want to store event and flow search results. The default setting is 1 day. The minimum is 1 day and the maximum is 3 months.
Reporting Max Matched Results	Type or select the maximum number of results you want a report to return. This value applies to the search results on the **Offenses**, **Log Activity**, and **Network Activity** tabs. The default setting is 1,000,000. The minimum value is zero (0) and the maximum value is 4294967294.
Command Line Max Matched Results	Type or select the maximum number of results you want the AQL command line to return. The default setting is 0. The minimum value is zero (0) and the maximum value is 4294967294.
Web Execution Time Limit	Type or select the maximum amount of time, in seconds, you want a query to process before a time-out occurs. This value applies to the search results on the **Offenses**, **Log Activity**, and **Network Activity** tabs. The default setting is 600 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Reporting Execution Time Limit for Manual Reports	Type or select the maximum amount of time, in seconds, you want a reporting query to process before a time-out occurs. The default setting is 57600 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Command Line Execution Time Limit	Type or select the maximum amount of time, in seconds, you want a query in the AQL command line to process before a time-out occurs. The default setting is 0 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Web Last Minute (Auto refresh) Execution Time Limit	From the list box, select the maximum amount of time, in seconds, you want an auto refresh to process before a time-out occurs. The default setting is 10 seconds. The maximum is 40 seconds.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Flow Log Hashing	From the list box, select one of the following options: • **Yes** - Enables QRadar SIEM to store a hash file for every stored flow log file. • **No** - Prevents QRadar SIEM from storing a hash file for every stored flow log file. The default setting is No.
Event Log Hashing	From the list box, select one of the following options: • **Yes** - Enables QRadar SIEM to store a hash file for every stored event log file. • **No** - Prevents QRadar SIEM from storing a hash file for every stored event log file. The default setting is No.
HMAC Encryption	This parameter is only displayed when the **Event Log Hashing** or **Flow Log Hashing** system setting is enabled. From the list box, select one of the following options: • **Yes** - Enables QRadar SIEM to encrypt the integrity hashes on stored event and flow log files. • **No** - Prevents QRadar SIEM from encrypting the integrity hashes on stored event and flow log files. The default setting is No.
HMAC Key	This parameter is only displayed when the **HMAC Encryption** system setting is enabled. Type the key you want to use for HMAC encryption. The maximum character length is 128 characters. The key must be unique.
Verify	This parameter is only displayed when the **HMAC Encryption** system setting is enabled. Retype the key you want to use for HMAC encryption. The key must match the key you typed in the **HMAC Key** field.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Hashing Algorithm	You can use a hashing algorithm for database integrity. QRadar SIEM uses the following hashing algorithm types: • **Message-Digest Hash Algorithm** - Transforms digital signatures into shorter values called Message-Digests (MD). • **Secure Hash Algorithm (SHA) Hash Algorithm** - Standard algorithm that creates a larger (60 bit) MD. ▶ From the list box, select the log hashing algorithm you want to use for your deployment. If the **HMAC Encryption** parameter is disabled, the following options are displayed: • **MD2** - Algorithm defined by RFC 1319. • **MD5** - Algorithm defined by RFC 1321. • **SHA-1** - Algorithm defined by Secure Hash Standard (SHS), NIST FIPS 180-1. This is the default setting. • **SHA-256** - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-256 is a 255-bit hash algorithm intended for 128 bits of security against security attacks. • **SHA-384** - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-384 is a bit hash algorithm, created by truncating the SHA-512 output. • **SHA-512** - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-512 is a bit hash algorithm intended to provide 256 bits of security. If the **HMAC Encryption** parameter is enabled, the following options are displayed: • **HMAC-MD5 -** An encryption method based on the MD5 hashing algorithm. • **HMAC-SHA-1** - An encryption method based on the SHA-1 hashing algorithm. • **HMAC-SHA-256 -** An encryption method based on the SHA-256 hashing algorithm. • **HMAC-SHA-384 -** An encryption method based on the SHA-384 hashing algorithm. • **HMAC-SHA-512** An encryption method based on the SHA-512 hashing algorithm.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Transaction Sentry Settings	
Transaction Max Time Limit	A transaction sentry detects unresponsive applications using transaction analysis. If an unresponsive application is detected, the transaction sentry attempts to return the application to a functional state. From the list box, select the length of time you want the system to check for transactional issues in the database. The default setting is 10 minutes. The minimum is 1 minute and the maximum is 30 minutes.
Resolve Transaction on Non-Encrypted Host	From the list box, select whether you want the transaction sentry to resolve all error conditions detected on the Console or non-encrypted managed hosts. If you select No, the conditions are detected and logged but you must manually intervene and correct the error. The default setting is Yes.
Resolve Transaction on Encrypted Host	From the list box, select whether you want the transaction sentry to resolve all error conditions detected on the encrypted managed host. If you select No, the conditions are detected and logged but you must manually intervene and correct the error. The default setting is Yes.
SNMP Settings	
SNMP Version	From the list box, choose one of the following options: • **Disabled** - Select this option if you do not want SNMP responses in the QRadar SIEM custom rules engine. Disabling SNMP indicates that you do not want to accept events using SNMP. This the default. • **SNMPv3** - Select this option if you want to use SNMP version 3 in your deployment. • **SNMPv2c** - Select this option if you want to use SNMP version 2 in your deployment.
SNMPv2c Settings	
Destination Host	Type the IP address to which you want to send SNMP notifications.
Destination Port	Type the port number to which you want to send SNMP notifications. The default port is 162.
Community	Type the SNMP community, such as public.
SNMPv3 Settings	
Destination Host	Type the IP address to which you want to send SNMP notifications.
Destination Port	Type the port to which you want to send SNMP notifications. The default port is 162.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
Username	Type the name of the user you want to access SNMP related properties.
Security Level	From the list box, select the security level for SNMP. The options are: • **NOAUTH_NOPRIV** - Indicates no authorization and no privacy. This the default. • **AUTH_NOPRIV** - Indicates authorization is permitted but no privacy. • **AUTH_PRIV** - Allows authorization and privacy.
Authentication Protocol	From the list box, select the algorithm you want to use to authenticate SNMP traps.
Authentication Password	Type the password you want to use to authenticate SNMP traps.
Privacy Protocol	From the list box, select the protocol you want to use to decrypt SNMP traps.
Privacy Password	Type the password used to decrypt SNMP traps.
Embedded SNMP Daemon Settings	
Enabled	From the list box, select one of the following options: • **Yes** - Enables access to data from the SNMP Agent using SNMP requests. • **No** - Disables access to data from the SNMP Agent using SNMP requests. The default setting is Yes. After you enable the embedded SNMP daemon, you must access the host specified in the **Destination Host** parameter and type **qradar** in the **Username** field. A password is not required. The location where you configure a destination host to communicate with QRadar SIEM can vary depending on the vendor host. For more information on configuring your destination host to communicate with QRadar SIEM, see your vendor documentation.
Daemon Port	Type the port you want to use for sending SNMP requests.
Community String	Type the SNMP community, such as **`public`**. This parameter only applies if you are using SNMPv2 and SNMPv3.
IP Access List	Type the systems that can access data from the SNMP agent using an SNMP request. If the **Enabled** option is set to Yes, this option is enforced.

Table 5-10 System Settings Parameters (continued)

Parameter	Description
IF-MAP Client/Server Settings	
IF-MAP Version	The Interface For Metadata Access Points (IF-MAP) rule response enables QRadar SIEM to publish alert and offense data derived from events, flows, and offense data on an IF-MAP server. From the list box, select one of the following options: • **Disabled** - Select this option if you want to disable access to the IF-MAP Server. This is the default setting. When disabled, the other IF-MAP Client/Server settings are not displayed. • **1.1** - Select this option if you want to use IF-MAP version 1.1 in your deployment. • **2.0** - Select this option if you want to use IF-MAP version 2.0 in your deployment.
Server Address	Type the IP address of the IF-MAP server.
Basic Server Port	Type or select the port number for the basic IF-MAP server. The default port is 8443.
Credential Server Port	Type or select the port number for the credential server. The default port is 8444.
Authentication	Before you can configure IF-MAP authentication, you must configure your IF-MAP server certificate. For more information on how to configure your IF-MAP certificate, see **Configuring your IF-MAP Server Certificates**. Using the list box, select the authentication type from the following options: • **Basic** - Select this option to use basic authentication. When you select this option, the **Username** and **User Password** parameters are displayed. • **Mutual** - Select this option to use mutual authentication. When you select this option, the **Key Password** parameter is displayed. The default authentication type is **Mutual**.
Key Password	This setting is displayed only when you select the **Mutual** option for the **Authentication** setting. Type the key password to be shared between the IF-MAP client and server.
Username	This setting is displayed only when you select the **Basic** option for the **Authentication** setting. Type the user name required to access the IF-MAP server.
User Password	This setting is displayed only when you select the **Basic** option for the **Authentication** setting. Type the password required to access the IF-MAP server.

Step 5 Click **Save**.

Step 6 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Configuring your IF-MAP Server Certificates

Before you can configure IF-MAP authentication, you must configure your IF-MAP server certificate.

This section includes the following topics:

- **Configuring IF-MAP Server Certificate for Basic Authentication**
- **Configuring IF-MAP Server Certificate for Mutual Authentication**

Configuring IF-MAP Server Certificate for Basic Authentication

To configure your IF-MAP certificate for basic authentication:

Step 1 Contact your IF-MAP server administrator to obtain a copy of the IF-MAP server public certificate. The certificate must have the **.cert** file extension, for example, ifmapserver.cert.

Step 2 Log in to QRadar SIEM as root and copy the certificate to the /opt/qradar/conf/trusted_certificates directory.

Configuring IF-MAP Server Certificate for Mutual Authentication

Mutual authentication requires certificate configuration on your QRadar SIEM Console and your IF-MAP server. For assistance configuring the certificate on your IF-MAP server, contact your IF-MAP server administrator.

To configure your IF-MAP certificate for mutual authentication:

Step 1 Contact your IF-MAP server administrator to obtain a copy of the IF-MAP server public certificate. The certificate must have the .cert file extension, for example, ifmapserver.cert.

Step 2 Using SSH, log in to QRadar SIEM as the root user and access the certificate to the /opt/qradar/conf/trusted_certificates directory

Step 3 Copy the SSL intermediate certificate and SSL Verisign root certificate to your IF-MAP server as CA certificates. For assistance, contact your IF-MAP server administrator.

Step 4 Type the following command to create the Public-Key Cryptography Standards file with the .pkcs12 file extension using the following command:

```
openssl pkcs12 -export -inkey <private_key> -in <certificate>
-out <pkcs12_filename.pkcs12> -name "IFMAP Client"
```

Step 5 Type the following command to copy the pkcs12 file to the /opt/qradar/conf/key_certificates directory:

```
cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates
```

Step 6 Create a client on the IF-MAP server with the Certificate authentication and upload the SSL certificate. For assistance, contact your IF-MAP server administrator.

Step 7 Change the permissions of the directory by typing the following commands:

```
chmod 755 /opt/qradar/conf/trusted_certificates
chmod 644 /opt/qradar/conf/trusted_certificates/*.cert
```

Step 8 Type the following command to restart the Tomcat service:

```
service tomcat restart
```

Using Event and Flow Retention Buckets

Using the Event Retention and Flow Retention features available on the **Admin** tab, you can configure retention buckets. Each retention bucket defines a retention policy for events and flows that match custom filter requirements. As QRadar SIEM receives events and flows, each event and flow is compared against retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the retention policy time period is reached. This feature enables you to configure multiple retention buckets.

Retention buckets are sequenced in priority order from the top row to the bottom row on the Event Retention and Flow Retention windows. A record is stored in the bucket that matches the filter criteria with highest priority. If the record does not match any of your configured retention buckets, the record is stored in the default retention bucket, which is always located below the list of configurable retention buckets.

This section includes the following topics:

- **Configuring Event Retention Buckets**
- **Configuring Flow Retention Buckets**
- **Managing Retention Buckets**

Configuring Event Retention Buckets

By default, the Event Retention feature provides a default retention bucket and 10 unconfigured retention buckets. Until you configure an event retention bucket, all events are stored in the default retention bucket.

To configure an event retention bucket:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Event Retention** icon.

The Event Retention window provides the following information for each retention bucket:

Table 5-11 Event Retention Window Parameters

Parameter	Description
Order	Specifies the priority order of the retention buckets.
Name	Specifies the name of the retention bucket.
Retention	Specifies the retention period of the retention bucket.
Compression	Specifies the compression policy of the retention bucket.

Table 5-11 Event Retention Window Parameters (continued)

Parameter	Description
Deletion Policy	Specifies the deletion policy of the retention bucket.
Filters	Specifies the filters applied to the retention bucket. Move your mouse pointer over the **Filters** parameter for more information on the applied filters.
Distribution	Specifies the retention bucket usage as a percentage of total event retention in all your retention buckets.
Enabled	Specifies whether the retention bucket is enabled (true) or disabled (false). The default setting is true.
Creation Date	Specifies the date and time the retention bucket was created.
Modification Date	Specifies the date and time the retention bucket was last modified.

The Event Retention toolbar provides the following functions:

Table 5-12 Event Retention Window Toolbar

Function	Description
Edit	Click **Edit** to edit a retention bucket. For more information on editing a retention bucket, see **Editing a Retention Bucket**.
Enable/Disable	Click **Enable/Disable** to enable or disable a retention bucket. For more information on enabling and disabling retention buckets, see **Enabling and Disabling a Retention Bucket**.
Delete	Click **Delete** to delete a retention bucket. For more information on deleting retention buckets, see **Deleting a Retention Bucket**.

Step 4 Double-click the first available retention bucket.

Step 5 Configure the following parameters:

Table 5-13 Retention Properties Window Parameters

Parameter	Description
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	From the list box, select a retention period. When the retention period is reached, events are deleted according to the **Delete data in this bucket** parameter. The default setting is 1 month. The minimum is 1 day and the maximum is 2 years.
Allow data in this bucket to be compressed	Select the check box to enable data compression, and then select a time frame from the list box. When the time frame is reached, all events in the retention bucket are eligible to be compressed. This increases system performance by guaranteeing that no data is compressed within the specified time period. Compression only occurs when used disk space reaches 83% for payloads and 85% for records. The default setting is 1 week. The minimum is Never and the maximum is 2 weeks.

Table 5-13 Retention Properties Window Parameters (continued)

Parameter	Description
Delete data in this bucket	From the list box, select a deletion policy. Options include: • **When storage space is required** - Select this option if you want events that match the **Keep data placed in this bucket for** parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. When storage is required, only events that match the Keep data placed in this bucket for parameter are deleted. • **Immediately after the retention period has expired** - Select this option if you want events to be deleted immediately on matching the **Keep data placed in this bucket for** parameter. The events are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.
Description	Type a description for the retention bucket. This field is optional.
Current Filters	In the Current Filters pane, configure your filters. To add a filter: **1** From the first list box, select a parameter you want to filter for. For example, Device, Source Port, or Event Name. **2** From the second list box, select the modifier you want to use for the filter. The list of modifiers depends on the attribute selected in the first list. **3** In the text field, type specific information related to your filter. **4** Click **Add Filter**. The filters are displayed in the **Current Filters** text box. You can select a filter and click **Remove Filter** to remove a filter from the **Current Filter** text box.

Step 6 Click **Save**.

Your event retention bucket configuration is saved.

Step 7 Click **Save**.

Your event retention bucket starts storing events that match the retention parameters immediately.

Configuring Flow Retention Buckets

By default, the Flow Retention feature provides a default retention bucket and 10 unconfigured retention buckets. Until you configure a flow retention bucket, all flows are stored in the default retention bucket.

To configure a flow retention bucket:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Flow Retention** icon.

The Flow Retention window is provides the following information for each retention bucket:

Table 5-14 Flow Retention Window Parameters

Parameter	Description
Order	Specifies the priority order of the retention buckets.
Name	Specifies the name of the retention bucket.
Retention	Specifies the retention period of the retention bucket.
Compression	Specifies the compression policy of the retention bucket.
Deletion Policy	Specifies the deletion policy of the retention bucket.
Filters	Specifies the filters applied to the retention bucket. Move your mouse pointer over the **Filters** parameter for more information on the applied filters.
Distribution	Specifies the retention bucket usage as a percentage of total event or flow retention in all your retention buckets.
Enabled	Specifies whether the retention bucket is enabled (true) or disabled (false). The default setting is true.
Creation Date	Specifies the date and time the retention bucket was created.
Modification Date	Specifies the date and time the retention bucket was last modified.

The Event Retention toolbar provides the following functions:

Table 5-15 Event Retention Window Toolbar

Function	Description
Edit	Click **Edit** to edit a retention bucket. For more information on editing a retention bucket, see **Editing a Retention Bucket**.
Enable/Disable	Click **Enable/Disable** to enable or disable a retention bucket. By default, retention buckets are enabled. For more information on disabling retention buckets, see **Enabling and Disabling a Retention Bucket**.
Delete	Click **Delete** to delete a retention bucket. For more information on deleting retention buckets, see **Deleting a Retention Bucket**.

Step 4 Double-click the first available retention bucket.

Step 5 Configure the following parameters:

Table 5-16 Retention Properties Window Parameters

Parameter	Description
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	From the list box, select a retention period. When the retention period is reached, flows are deleted according to the **Delete data in this bucket** parameter. The default setting is 1 month. The minimum is 1 day and the maximum is 2 years.
Allow data in this bucket to be compressed	Select the check box to enable data compression, and then select a time frame from the list box. When the time frame is reached, all flows in the retention bucket are eligible to be compressed. This increases system performance by guaranteeing that no data is compressed within the specified time period. Compression only occurs when used disk space reaches 83% for payloads and 85% for records. The default setting is 1 week. The minimum is Never and the maximum is 2 weeks.
Delete data in this bucket	From the list box, select a deletion policy. Options include: • **When storage space is required** - Select this option if you want flows that match the **Keep data placed in this bucket for** parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. When storage is required, only events that match the Keep data placed in this bucket for parameter are deleted. • **Immediately after the retention period has expired** - Select this option if you want flows to be deleted immediately on matching the **Keep data placed in this bucket for** parameter. The events are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.
Description	Type a description for the retention bucket. This field is optional.

Table 5-16 Retention Properties Window Parameters (continued)

Parameter	Description
Current Filters	In the Current Filters pane, configure your filters. To add a filter: **1** From the first list box, select a parameter you want to filter for. For example, Device, Source Port, or Event Name. **2** From the second list box, select the modifier you want to use for the filter. The list of modifiers depends on the attribute selected in the first list. **3** In the text field, type specific information related to your filter. **4** Click **Add Filter**. The filters are displayed in the **Current Filters** text box. You can select a filter and click **Remove Filter** to remove a filter from the **Current Filter** text box. ***Note:*** *This parameter is not displayed when editing the default retention bucket.*

Step 6 Click **Save**.

Your flow retention bucket is saved and starts storing flows that match the retention parameters immediately.

Managing Retention Buckets

After you configure your retention buckets, you can manage the buckets using the Event Retention and Flow Retention windows.

This section includes the following topics:

- **Managing Retention Bucket Sequence**
- **Editing a Retention Bucket**
- **Enabling and Disabling a Retention Bucket**
- **Deleting a Retention Bucket**

Managing Retention Bucket Sequence

Retention buckets are sequenced in priority order from the top row to the bottom row on the Event Retention and Flow Retention windows. A record is stored in the first retention bucket that matches the record parameters. You can change the order of the retention buckets to ensure that events and flows are being matched against the retention buckets in the order that matches your requirements.

To manage the retention bucket sequence:

Step 1 Click the **Admin** tab.

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

Step 3 Choose one of the following options:

a To manage the event retention bucket sequence, click the **Event Retention** icon. The Event Retention window is displayed.

b To manage the flow retention bucket sequence, click the **Flow Retention** icon. The Flow Retention window is displayed.

Step 4 Select the retention bucket you want to move, and then click one of the following icons:

- **Up** - Click this icon to move the selected retention bucket up one row in priority sequence.
- **Down** - Click this icon to move the selected retention bucket down one row in priority sequence.
- **Top** - Click this icon to move the selected retention bucket to the top of the priority sequence.
- **Bottom** - Click this icon to move the selected retention bucket to the bottom of the priority sequence.

NOTE

You cannot move the default retention bucket. It always resides at the bottom of the list.

Editing a Retention Bucket

To edit a retention bucket:

Step 1 Click the **Admin** tab.

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

Step 3 Choose one of the following options:

- To edit an event retention bucket, click the **Event Retention** icon. The Event Retention window is displayed.
- To edit a flow retention bucket, click the **Flow Retention** icon. The Flow Retention window is displayed.

Step 4 Select the retention bucket you want to edit, and then click **Edit**.

Step 5 Edit the parameters. For more information on event retention parameters, see Table 5-13. For more information on flow retention parameters, see Table 5-16.

NOTE

On the Retention Parameters window, the Current Filters pane is not displayed when editing a default retention bucket.

Step 6 Click **Save**.

Your changes are saved.

Enabling and Disabling a Retention Bucket

When you configure and save a retention bucket, it is enabled by default. You can tune your event or flow retention by disabling a bucket.

When you disable a bucket, any new events or flows that match the requirements for the disabled bucket are stored in the next bucket that matches the event or flow properties.

To enable or disable a retention bucket:

Step 1 Click the **Admin** tab.

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

Step 3 Choose one of the following options:

- **a** To disable an event retention bucket, click the **Event Retention** icon. The Event Retention window is displayed.
- **b** To disable a flow retention bucket, click the **Flow Retention** icon. The Flow Retention window is displayed.

Step 4 Select the retention bucket you want to disable, and then click **Enable/Disable**.

The retention bucket is disabled. You can click **Enable/Disable** to enable the retention bucket again.

Deleting a Retention Bucket

When you delete a retention bucket, the events or flows contained in the retention bucket are not removed from the system, only the criteria defining the bucket is deleted. All events or flows are maintained in storage.

To delete a retention bucket:

Step 1 Click the **Admin** tab.

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

Step 3 Choose one of the following options:

- **a** To delete an event retention bucket, click the **Event Retention** icon. The Event Retention window is displayed.
- **b** To delete a flow retention bucket, click the **Flow Retention** icon. The Flow Retention window is displayed.

Step 4 Select the retention bucket you want to delete, and then click **Delete**.

The retention bucket is deleted.

Configuring System Notifications

You can configure system performance alerts for thresholds using the **Admin** tab. This section provides information on configuring your system thresholds.

To configure system thresholds:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Global System Notifications** icon.

Step 4 Enter values for the parameters. For each parameter, you must select the following options:

- **Enabled** - Select the check box to enable the option.
- **Respond if value is** - From the list box, select one of the following options:
  - **Greater Than** - An alert occurs if the parameter value exceeds the configured value.
  - **Less Than** - An alert occurs if the parameter value is less than the configured value.
- **Resolution Message** - Type a description of the preferred resolution to the alert.

Table 5-17 Global System Notifications Parameters

Parameter	Description
System load over 1 minute	Type the threshold system load average over the last minute. The default setting is 15.
System load over 5 minutes	Type the threshold system load average over the last 5 minutes. The default setting is 10.
System load over 15 minutes	Type the threshold system load average over the last 15 minutes. The default setting is 8.
Percentage of swap used	Type the threshold percentage of used swap space. The default setting is 80.
Received packets per second	Type the threshold number of packets received per second. This setting is disabled by default.
Transmitted packets per second	Type the threshold number of packets transmitted per second. This setting is disabled by default.
Received bytes per second	Type the threshold number of bytes received per second. This setting is disabled by default.
Transmitted bytes per second	Type the threshold number of bytes transmitted per second. This setting is disabled by default.
Receive errors	Type the threshold number of corrupted packets received per second. The default setting is 1.
Transmit errors	Type the threshold number of corrupted packets transmitted per second. The default setting is 1.

Table 5-17 Global System Notifications Parameters (continued)

Parameter	Description
Packet collisions	Type the threshold number of collisions that occur per second while transmitting packets. The default setting is 1.
Dropped receive packets	Type the threshold number of received packets that are dropped per second due to a lack of space in the buffers. The default setting is 1.
Dropped transmit packets	Type the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers. The default setting is 1.
Transmit carrier errors	Type the threshold number of carrier errors that occur per second while transmitting packets. The default setting is 1.
Receive frame errors	Type the threshold number of frame alignment errors that occur per second on received packets. The default setting is 1.
Receive fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets. The default setting is 1.
Transmit fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets. The default setting is 1.

Step 5 Click **Save**.

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

Configuring the Console Settings

The QRadar SIEM Console provides the user interface for QRadar SIEM. The Console provides real-time views, reports, alerts, and in-depth investigation of flows for network traffic and security threats. You can configure the Console to manage distributed QRadar SIEM deployments.

To configure QRadar SIEM Console settings:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Console** icon.

Step 4 Enter values for the parameters:

Table 5-18 QRadar SIEM Console Parameters

Parameter	Description
Console Settings	
ARP - Safe Interfaces	Type the interfaces you want to be excluded from ARP resolution activities.

Table 5-18 QRadar SIEM Console Parameters (continued)

Parameter	Description
Results Per Page	Type the maximum number of results you want to display on the main QRadar SIEM user interface. This parameter applies to the **Offenses**, **Log Activity**, **Assets**, **Network Activity**, and **Reports** tabs. For example, if the **Default Page Size** parameter is configured to 50, the **Offenses** tab displays a maximum of 50 offenses. The default setting is 40. The minimum is 0 and the maximum is 4294967294.
Authentication Settings	
Persistent Session Timeout (in days)	Type the length of time, in days, that a user system will be persisted. The default setting is 0, which disables this feature. The minimum is 0 and the maximum is 4294967294.
Maximum Login Failures	Type the number of times a login attempt can fail. The default setting is 5. The minimum is 0 and the maximum is 4294967294.
Login Failure Attempt Window (in minutes)	Type the length of time during which a maximum number of login failures can occur before the system is locked. The default setting is 10 minutes. The minimum is 0 and the maximum is 4294967294.
Login Failure Block Time (in minutes)	Type the length of time that the system is locked if the maximum login failures value is exceeded. The default setting is 30 minutes. The minimum is 0 and the maximum is 4294967294.
Login Host Whitelist	Type a list of hosts who are exempt from being locked out of the system. Enter multiple entries using a comma-separated list.
Inactivity Timeout (in minutes)	Type the amount of time that a user will be automatically logged out of the system if no activity occurs. The default setting is 0. The minimum is 0 and the maximum is 4294967294.
Login Message File	Type the location and name of a file that includes content you want to display on the QRadar SIEM login window. The contents of the file are displayed below the current log in window. The login message file must be located in the opt/qradar/conf directory on your system. This file may be in text or HTML format.

Table 5-18 QRadar SIEM Console Parameters (continued)

Parameter	Description
Event Permission Precedence	From the list box, select the level of network permissions you want to assign to users. This parameter affects the events that are displayed on the **Log Activity** tab. The options include: • **Network Only** - A user must have access to either the source network or the destination network of the event to have that event display on the **Log Activity** tab. • **Devices Only** - A user must have access to either the device or device group that created the event to have that event display on the **Log Activity** tab. • **Networks and Devices** - A user must have access to both the source or the destination network and the device or device group to have an event display on the **Log Activity** tab. • **None** - All events are displayed on the **Log Activity** tab. Any user with Log Activity role permissions is able to view all events. For more information on managing users, see **Managing User Roles and Accounts**.
DNS Settings	
Enable DNS Lookups for Asset Profiles	From the list box, select whether you want to enable or disable the ability for QRadar SIEM to search for DNS information in asset profiles. When enabled, this information is available in the right-click menu for the IP address or host name located in the **Host Name (DNS Name)** field in the asset profile. The default setting is False.
Enable DNS Lookups for Host Identity	From the list box, select whether you want to enable or disable the ability for QRadar SIEM to search for host identity information. When enabled, this information is available in the right-click menu for any IP address or asset name. The default setting is True.
WINS Settings	
WINS Server	Type the location of the Windows Internet Naming Server (WINS) server.
Reporting Settings	
Report Retention Period	Type the period of time, in days, that you want the system to maintain reports. The default setting is 30 days. The minimum is 0 and the maximum is 4294967294.
Data Export Settings	
Include Header in CSV Exports	From the list box, select whether you want to include a header in a CSV export file.
Maximum Simultaneous Exports	Type the maximum number of exports you want to occur at one time. The default setting is 1. The minimum is 0 and the maximum is 4294967294.

Step 5 Click **Save**.

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

Managing Custom Offense Close Reasons

When a user closes an offense on the **Offenses** tab, the Close Offense window is displayed. The user is prompted to select a reason from the **Reason for Closing** list box. Three default options are listed:

- False-positive, tuned
- Non-issue
- Policy violation

Administrators can add, edit, and delete custom offense close reasons from the **Admin** tab.

This section includes the following topics:

Adding a Custom Offense Close Reason

When you add a custom offense close reason, the new reason is listed on the Custom Close Reasons window and in the **Reason for Closing** list box on the Close Offense window of the **Offenses** tab.

To add a custom offense close reason:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Custom Offense Close Reasons** icon.

The Custom Offense Close Reasons window provides the following parameters.

Table 5-19 Custom Close Reasons Window Parameters

Parameter	Description
Reason	Specifies the reason that is displayed in the **Reason for Closing** list box on the Close Offense window of the **Offenses** tab.
Created by	Specifies the user that created this custom offense close reason.
Date Created	Specifies the date and time of when the user created this custom offense close reason

NOTE

You can also access the Custom Offense Close Reasons window by clicking the **Manage Close Reasons** icon on the Close Offense window of the **Offenses** tab.

Step 4 Click **Add**.

Step 5 Type a unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.

Step 6 Click **OK**.

Your new custom offense close reason is now listed in the Custom Close Reasons window. The **Reason for Closing** list box on the Close Offense window of the **Offenses** tab also displays the custom reason you added.

Editing Custom Offense Close Reason

Editing a custom offense close reason updates the reason in the Custom Close Reasons window and the **Reason for Closing** list box on the Close Offense window of the **Offenses** tab.

To edit a custom offense close reason:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Custom Offense Close Reasons** icon.

Step 4 Select the reason you want to edit.

Step 5 Click **Edit**.

Step 6 Type a new unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.

Step 7 Click **OK**.

The custom offense close reason is now edited.

Deleting a Custom Offense Close Reason

Deleting a custom offense close reason removes the reason from the Custom Close Reasons window and the **Reason for Closing** list box on the Close Offense window of the **Offenses** tab.

To delete a custom offense close reason:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Custom Offense Close Reasons** icon.

Step 4 Select the reason you want to delete.

Step 5 Click **Delete**.

Step 6 Click **OK**.

The custom offense close reason is now deleted.

Index Management

The Index Management feature allows you to control database indexing on event and flow properties. Indexing event and flow properties allows you to optimize your searches. You can enable indexing on any property that is listed in the Index Management window and you can enable indexing on more than one property. The Index Management feature also provides statistics, such as:

- The percentage of saved searches running in your deployment that include the indexed property
- The volume of data that is written to the disk by the index during the selected time frame

NOTE

To enable payload indexing, you must enable indexing on the Quick Filter property. For more information on payload indexing, see the *Enable Payload Indexing for Quick Filtering Technical Note*.

This section includes the following topics:

- **Viewing the Index Management Window**
- **Enabling Indexes**

Viewing the Index Management Window

The Index Management window lists all event and flow properties that can be indexed and provides statistics for the properties. Toolbar options allow you to enable and disable indexing on selected event and flow properties.

NOTE

Modifying database indexing may decrease system performance, therefore, we recommend that you monitor the statistics after enabling indexing on multiple properties.

To view the Index Management window:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Index Management** icon.

The Index Management window provides the following parameters.

Table 5-20 Index Management Window Parameters

Parameter	Description
Display	Displays the time range used to calculate the statistics for each property. From the list box, you can select a new time range. The minimum time range is **Last Hour** and the maximum time range is **Last 30 Days**. The default time range is **Last 24 Hours**. After you select a new time range option, the statistics are refreshed.
View	Allows you to display properties filtered on the **Indexed** parameter. From the list box, select one of the following options: • **All** - Displays all properties in the Index Management list. • **Enabled** - Displays only indexed properties in the Index Management list. • **Disabled** - Displays only properties that are not indexed in the Index Management list.

Table 5-20 Index Management Window Parameters (continued)

Parameter	Description
Database	Allows you to display properties filtered on the **Database** parameter. From the list box, select one of the following options: • **All** - Displays all properties in the Index Management list. • **Events** - Displays only event properties in the Index Management list. • **Flows** - Displays only flow properties in the Index Management list.
Show	Allows you to display all properties or only custom properties. Options include: • **All** - Displays all properties in the Index Management list. • **Custom** - Displays only custom event and flow properties. Custom properties are properties that you can create by extracting from unnormalized data using RegEx statements or calculated properties that are created by performing operations on existing properties. For more information on custom properties, see the *IBM Security QRadar SIEM Users Guide*.
Indexed	Indicates whether the property is indexed or not: • **Green dot** - Indicates that the property is indexed. • **Empty cell** - Indicates that the property is not indexed.
Property	Displays the name of the property.
% of Searches Using Property	Displays the percentage of searches that include this property that have performed in the specified time range.
% of Searches Hitting Index	Displays the percentage of searches that include this property that have performed in the specified time range and successfully used the index.
% of Searches Missing Index	Displays the percentage of searches that include this property that have performed in the specified time range and did not use the index.
Data Written	Displays the volume of data written to the disk by the index in the time range specified in the **Display** list box.
Database	Displays the name of the database the property is stored in. Databases include: • **Event** - Specifies that the property is stored in the event database. • **Flow** - Specifies that the property is stored in the flow database.

The Index Management toolbar provides the following options:

Table 5-21 Index Management Window Parameters

Option	Description
Enable Index	Select one or more properties in the Index Management list, and then click this icon to enable indexing on the selected parameters.
Disable Index	Select one or more properties in the Index Management list, and then click this icon to disable indexing on the selected parameters.
Quick Search	Type your keyword in the **Quick Search** field and click the **Quick Filter** icon or press Enter on the keyboard. All properties that match your keyword are displayed in the Index Management list.

Enabling Indexes

To enable indexing on selected properties:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Index Management** icon.

Step 4 Select one or more properties from the Index Management list.

Step 5 Click **Enable Index**.

NOTE You can also right-click a property and select **Enable Index** from the menu.

Step 6 Click **Save**.

Step 7 Click **OK**.

The selected properties are now indexed. In lists that include event or flow properties, indexed property names are appended with the following text: `[Indexed]`. Examples of such lists include the search parameters on the **Log Activity** and **Network Activity** tab search criteria pages and the Add Filter window.

Disabling Indexes

To disable indexing on selected properties:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Index Management** icon.

Step 4 Select one or more properties from the Index Management list.

Step 5 Click **Disable Index**.

NOTE You can also right-click a property and select **Disable Index** from the menu.

Step 6 Click **Save**.

Step 7 Click **OK**.

The selected properties are no longer indexed. In lists that include event or flow properties, indexed property names are no longer appended with the following text: `[Indexed]`.

6 MANAGING REFERENCE SETS

The Reference Set Management feature allows you to create and manage reference sets. You can also import elements into a reference set from an external file.

This section includes the following topics:

Reference Set Overview

A reference set is a set of elements, such as a list of IP addresses or user names, that are derived from events and flows occurring on your network.

After you create a reference set, you can create rules in the Rule Wizard to detect when log or network activity associated with the reference set occurs on your network. For example, you can create a rule to detect when a terminated user attempts to access your network resources. You can also configure a rule to add an element to a reference set when log activity or network activity matches the rule conditions. For example, you can create a rule to detect when an employee has accessed a prohibited website and add that employee's IP address to a reference set. For more information on configuring rules, see the *IBM Security QRadar Risk Manager Users Guide*.

Viewing Reference Sets

To view reference sets:

Step 1 Log in to the QRadar SIEM user interface.

Step 2 Click the **Admin** tab.

Step 3 From the navigation menu, select **System Configuration**.

Step 4 Click **Reference Set Management**.

The Reference Set Management window provides the following information:

Table 6-1 Reference Set Management Window Parameters

Parameter	Description
Name	Displays the name of this reference set.
Number of Elements	Displays the number of elements that this reference set contains.
Type	Displays the data type of this reference set. Options include: • AlphaNumeric • Numeric • IP • Port • AlphaNumeric_Ignore_Case
Associated Rules	Displays the number of rules that are configured to contribute elements to this reference set.
Capacity	Displays a visual indication of the reference set capacity used by the elements contained in the set. Reference sets can contain up to 100,000 elements.

The Reference Set Management toolbar provides the following functions:

Table 6-2 Reference Set Management Toolbar Function

Function	Description
New	Click this icon to create a new reference set. See **Adding a Reference Set**.
Edit	Select a reference set, and then click this icon to edit the reference set. See **Editing a Reference Set**.
View Contents	Select a reference set, and then click this icon to view the elements and associated rules for this reference set. See **Viewing the Contents of a Reference Set**.
Delete	Select a reference set, and then click this icon to delete the reference set. See **Deleting Reference Sets**.

Table 6-2 Reference Set Management Toolbar Function (continued)

Function	Description
Delete Listed	Use the **Quick Search** field to filter for specific reference sets, and then click the **Delete Listed** icon to delete these reference sets. See **Deleting Reference Sets**.
Quick Search	Type your keyword in the **Quick Search** field, and then click the **Quick Search** icon or press Enter on the keyboard. All reference sets that match your keyword are displayed in the Reference Set Management list. To display all reference sets again, click the eraser icon.

Adding a Reference Set

To add a reference set:

Step 1 On the Reference Set Management window, click **New**.

Step 2 Configure the following parameters:

Table 6-3 New Reference Set Dialog Box Parameters

Parameter	Description
Name	Type a unique name for this reference set. The maximum length is 255 characters.
Type	Using the list box, select a reference set type from the following options: • AlphaNumeric • Numeric • IP • Port • AlphaNumeric_Ignore_Case ***Note:*** *You cannot edit the* ***Type*** *parameter after you create a reference set.*
Time to Live of Elements	Using the list boxes, select the amount of time that you want to maintain each element in the reference set or select **Lives Forever**. If you specify an amount of time, you must also indicate when you want to start tracking time for an element. Select one of the following options: • Since first seen • Since last seen **Lives Forever** is the default setting.

Step 3 Click **Create**.

The reference set that you created is listed on the Reference Set Management window. In the Rule Wizard, this reference set is now listed as an option on the Rule Response page. After you configure one or more rules to send elements to this reference set, the **Number of Elements**, **Associated Rules**, and **Capacity** parameters are automatically updated.

Editing a Reference Set

To edit a reference set:

Step 1 On the Reference Set Management window, select a reference set, and then click **Edit**.

Step 2 Edit the parameters, as required. See **Table 6-3**.

Step 3 Click **Submit**.

The reference set that you edited is now updated.

Deleting Reference Sets

When deleting reference sets, a confirmation window indicates if the reference sets that you want to delete have rules associated with them. After you delete a reference set, the **Add to Reference Set** configuration is cleared from the associated rules. Before you delete a reference set, you can view associated rules in the **Reference** tab. See **Viewing the Contents of a Reference Set**.

To delete a reference set:

Step 1 Choose one of the following:

- On the Reference Set Management window, select a reference set, and then click **Delete**.
- On the Reference Set Management window, use the **Quick Search** text box to display only the reference sets that you want to delete, and then click **Delete Listed**.

Step 2 Click **Delete**.

The reference sets that you deleted is removed from the list.

Viewing the Contents of a Reference Set

To view the contents of a reference set:

Step 1 On the Reference Set Management window, select a reference set, and then click **View Contents**.

NOTE You can also double-click a reference set to view the contents.

Step 2 Click the **Content** tab.

The **Content** tab is provides a list of the elements that are included in this reference set. The **Content** tab provides the following information:

Table 6-4 Content Tab Parameters

Parameter	Description
Value	Displays the value for this element. For example, if the reference set contains a list of IP addresses, this parameter displays an IP address.
Origin	Indicates the source of this element. Options include: • **<rulename>** - This element was placed in this reference set as a response to a rule. The • **User** - This element was imported from an external file or manually added to the reference set.
Time to Live	Displays the time remaining until this element is removed from the reference set.
Date Last Seen	Displays the date and time that this element was last detected on your network.

The **Content** tab toolbar provides the following functions:

Table 6-5 Content Tab Toolbar Functions

Function	Description
New	Click this icon to manually add an element to the reference set. See **Adding a New Element to a Reference Set**.
Delete	Select an element, and then click this icon to delete the element.
Delete Listed	Use the **Quick Search** field to filter for specific elements, and then click the **Delete Listed** icon to delete these elements.
Import	Click this icon to import elements from a Comma-Separated Value (CSV) or text file. See **Importing Elements into a Reference Set**.
Export	Click this icon to export the contents of this reference set to a CSV file.
Refresh Table	Click this icon to refresh the **Content** tab.
Quick Search	Type your keyword in the **Quick Search** field, and then click the **Quick Search** icon or press Enter on the keyboard. All elements that match your keyword are displayed in the Content list. To display all elements again, click the eraser icon.

Step 3 Click the **References** tab.

The **References** tab is provides a list of rules that are configured to add elements to this reference set. The **References** tab provides the following information:

Table 6-6 References Tab Parameters

Parameter	Description
Rule Name	Displays the name of this rule.
Group	Displays the name of the group this rule belongs to.
Category	Displays the category of this rule. Options include Custom Rule or Anomaly Detection Rule.
Type	Displays the type of this rule. Options include: Event, Flow, Common, or Offense.
Enabled	Indicates whether the rule is enabled or disabled: • **true** - Indicates that this rule is enabled. • **false** - Indicates that this rule is disabled.
Response	Specifies the responses configured for this rule.
Origin	Indicates the origin of this rule. Options include: • **System** - Indicates that this is a default rule. • **Modified** - Indicates that this is a default rule that has been customized. • **User** - Indicates that this is a user-created rule.

The **References** tab toolbar provides the following functions:

Table 6-7 References Tab Toolbar Functions

Function	Description
Edit	Click this icon to edit the rule in the Rule Wizard. You can also double-click the rule to open the Rule Wizard.
Refresh Table	Click this icon to refresh the References list.

Step 4 To view or edit an associated rule, double-click the rule in the **References** list.

In the Rule Wizard, you can edit rule configuration settings, if required.

Adding a New Element to a Reference Set

To add a new element to a reference set:

Step 1 On the Reference Set Management window, select a reference set, and then click **View Contents**.

Step 2 Click the **Content** tab.

Step 3 On the toolbar, click **New**.

Step 4 Configure the following parameters:

Table 6-8 Add Reference Set Data Dialog Box Parameters

Parameter	Description
Value(s)	Type the value for the element that you want to add. If you want to type multiple values, include a separator character between each value, and then specify the separator character in the **Separator Character** field.
Separator Character	Type the separator character that you used in the **Value(s)** field.

Step 5 Click **Add**.

The elements you added are now displayed on the **Content** tab.

Deleting Elements from a Reference Set

To delete elements from a reference set:

Step 1 On the Reference Set Management window, select a reference set, and then click **View Contents**.

Step 2 Click the **Content** tab.

Step 3 Choose one of the following:

- Select an element, and then click **Delete**.
- Use the **Quick Search** text box to display only the elements that you want to delete, and then click **Delete Listed**.

Step 4 Click **Delete**.

The element you deleted is removed from the list.

Importing Elements into a Reference Set

You can import elements from an external CSV or text file. Before you begin, ensure that the CSV or text file that you want to import is stored on your local desktop.

To import a CSV or text file into a reference set:

Step 1 On the Reference Set Management window, select a reference set, and then click **View Contents**.

Step 2 Click the **Content** tab.

Step 3 On the toolbar, click **Import**.

Step 4 Click **Browse**.

Step 5 Select the CSV or text file that you want to import.

Step 6 Click **Import**.

The elements in the CSV or text file you imported are now displayed in the list.

Exporting Elements from a Reference Set

You can export reference set elements to an external CSV or text file.

To export the contents of a reference set to a CSV or text file:

Step 1 On the Reference Set Management window, select a reference set, and then click **View Contents**.

Step 2 Click the **Content** tab.

Step 3 On the toolbar, click **Export**.

Step 4 Choose one of the following options:

- If you want to open the list for immediate viewing, select the **Open with** option and select an application from the list box.
- If you want to save the list, select the **Save File** option.

Step 5 Click **OK**.

7 MANAGING AUTHORIZED SERVICES

You can configure authorized services on the **Admin** tab to pre-authenticate a customer support service for your QRadar SIEM deployment.

This section includes the following topics:

Authorized Services Overview

Authenticating a customer support service allows the service to connect to your QRadar SIEM user interface and either dismiss or update notes to an offense using a web service. You can add or revoke an authorized service at any time.

Viewing Authorized Services

To view authorized services for your QRadar SIEM deployment:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Authorized Services** icon.

The Manage Authorized Services window provides the following information:

Table 7-1 Manage Authorized Services Parameters

Parameter	Description
Service Name	Specifies the name of the authorized service.
Authorized By	Specifies the name of the user or administrator that authorized the addition of the service.
Authentication Token	Specifies the token associated with this authorized service.
User Role	Specifies the user role associated with this authorized service.
Created	Specifies the date that this authorized service was created.

Table 7-1 Manage Authorized Services Parameters (continued)

Parameter	Description
Expires	Specifies the date and time that the authorized service will expire. Also, this field indicates when a service has expired.

Step 4 To select a token from an authorized service, select the appropriate authorized service. The token is displayed in the **Selected Token** field in the top bar. This allows you to copy the token into your vendor software to authenticate with QRadar SIEM.

Adding an Authorized Service

To add an authorized service:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Authorized Services** icon.

Step 4 Click **Add Authorized Service**.

Step 5 Enter values for the parameters:

Table 7-2 Add Authorized Services Parameters

Parameter	Description
Service Name	Type a name for this authorized service. The name can be up to 255 characters in length.
User Role	From the list box, select the user role you want to assign to this authorized service. The user roles assigned to an authorized service determines the functionality on the QRadar SIEM user interface this service can access.
Expiry Date	Type or select a date you want this service to expire or select the **No Expiry** check box if you do not want this service to expire. By default, the authorized service is valid for 30 days.

Step 6 Click **Create Service**.

The confirmation message contains a token field that you must copy into your vendor software to authenticate with QRadar SIEM. For more information on setting up your vendor software to integrate with QRadar SIEM, contact your system administrator.

Revoking Authorized Services

To revoke an authorized service:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Authorized Services** icon.

Step 4 Select the service you want to revoke.

Step 5 Click **Revoke Authorization**.

Step 6 Click **OK**.

Configuring the Customer Support Service

After you have configured an authorized service in QRadar SIEM, you must configure your customer support service to access QRadar SIEM offense information. For example, you can configure QRadar SIEM to send an SNMP trap that includes the offense ID information. Your service must be able to authenticate to QRadar SIEM using the provided authorized token by passing the information through an HTTP query string. When authenticated, the service should interpret the authentication token as the user name for the duration of the session.

Your customer support service must use a query string to update notes, dismiss, or close an offense.

This section includes the following topics:

- **Dismissing an Offense**
- **Closing an Offense**
- **Adding Notes to an Offense**

Dismissing an Offense

To dismiss an offense, your customer support service must use the following query string:

```
https://<IP address >/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId=
OffenseList&nextForward=offensesearch&attribute=dismiss&daoName
=offense&value=1&authenticationToken=<Token>
```

Where:

<IP address> is the IP address of your QRadar SIEM system.

<Offense ID> is the identifier assigned to the QRadar SIEM offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide.*

<Token> is the token identifier provided to the authorized service on the QRadar SIEM user interface.

Closing an Offense

To close an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId=
OffenseList&nextForward=offensesearch&attribute=dismiss&daoName
=offense&value=2&authenticationToken=<Token>
```

Where:

<IP address> is the IP address of your QRadar SIEM system.

<Offense ID> is the identifier assigned to the QRadar SIEM offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide.*

<Token> is the token identifier provided to the authorized service on the QRadar SIEM user interface.

Adding Notes to an Offense

To add notes to an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId=
OffenseList&nextForward=offensesearch&attribute=notes&daoName
=offense&value=<NOTES>&authenticationToken=<Token>
```

Where:

<IP address> is the IP address of your QRadar SIEM system.

<Offense ID> is the identifier assigned to the QRadar SIEM offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide.*

<Token> is the token identifier provided to the authorized service on the QRadar SIEM user interface.

8 MANAGING BACKUP AND RECOVERY

Using the Backup and Recovery feature, you can backup and recover QRadar SIEM configuration information and data.

This section includes the following topics:

Backup and Recovery Overview

QRadar SIEM enables you to perform two types of backup:

- Configuration backups, which include the following components:
  - Assets
  - Certificates
  - Custom logos
  - Custom rules
  - Device Support Modules (DSMs)
  - Event categories
  - Flow sources
  - Flow and event searches
  - Groups
  - License key information
  - Log sources
  - Offenses
  - Store and Forward schedules
  - User and user roles information
  - Vulnerability data
- Data backups, which include the following information:
  - Audit log information

- Event data
- Flow data
- Report data
- Indexes
- Reference set elements

NOTE

You can back up your event and flow data using the Backup and Recovery feature, however, you must restore event and flow data manually. For assistance in restoring your event and flow data, see the *Restoring Your Data Technical Note*.

Managing Backup Archives

By default, QRadar SIEM creates a backup archive of your configuration information daily at midnight. The backup archive includes configuration information, data, or both from the previous day. QRadar SIEM lists all successful backup archives on the Backup Archives window, which is the first window displayed when you access the Backup and Recovery feature from the **Admin** tab. From this window, you can view and manage all successful backup archives.

This section includes the following topics:

- **Viewing Backup Archives**
- **Importing a Backup Archive**
- **Deleting a Backup Archive**

Viewing Backup Archives

To view all successful backup archives:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

If a backup is in progress, a status pane provides the following Information:

- **Host** - Specifies the host on which the backup is currently running.
- **Name** - Specifies the user-defined name of the backup archive.
- **Backup Type** - Specifies the type of backup that is in progress.
- **Initiated by** - Specifies the user account that initiated the backup process.
- **Initiated at** - Specifies the date and time the backup process was initiated.
- **Duration** - Specifies the elapsed time since the backup process was initiated.

Until the backup is complete, you are unable to start any new backup or restore processes.

- Existing backup archives are displayed on the window. Each archive file includes the data from the previous day. The list of archives is sorted by the **Time Initiated** column in descending order. If a backup file is deleted, it is

removed from the disk and from the database. Also, the entry is removed from this list and an audit event is generated to indicate the removal.

The Existing Backups pane on the Backup Archives window provides the following information for each backup archive:

Table 8-1 Existing Backups Pane Parameters

Parameter	Description
Host	Specifies the host that initiated the backup process.
Name	Specifies the name of the backup archive. To download the backup file, click the name of the backup.
Type	Specifies the type of backup. The options include: • **config** - Configuration data • **data** - Events, flows, asset, and offense information
Size	Specifies the size of the archive file.
Time Initiated	Specifies the time that the backup file was initiated.
Duration	Specifies the time to complete the backup process.
Initialized By	Specifies whether the backup file was created by a user or through a scheduled process.

Importing a Backup Archive

You can import a backup archive into the Existing Backups pane on your Backup Archives window. This is useful if you want to restore a backup archive that was created on another QRadar SIEM host.

NOTE

If you place a QRadar SIEM backup archive file in the `/store/backupHost/inbound` directory on the Console server, the backup archive file is automatically imported.

To import a QRadar SIEM backup archive file:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 In the **Upload Archive** field, click **Browse**.

Step 5 Locate and select the archive file you want to upload. The archive file must include a .tgz extension.

Step 6 Click **Open**.

Step 7 Click **Upload**.

The imported archive file is displayed in the Existing Backups pane.

Deleting a Backup Archive

To delete a backup archive file, the backup archive file and the Host Context component must reside on the same system. The system must also be in communication with the Console and no other backup can be in progress. If a backup file is deleted, it is removed from the disk and from the database. Also, the entry is removed from this list and an audit event is generated to indicate the removal.

To delete a backup archive:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 In the Existing Backups pane, select the archive you want to delete.

Step 5 Click **Delete**.

Step 6 Click **OK**.

Backing Up Your Configuration Information and Data

By default, QRadar SIEM creates a backup archive of your configuration information daily at midnight. The backup archive includes your configuration information, data, or both from the previous day. Using the Backup and Recovery feature on the **Admin** tab, you can customize this nightly backup and create an on-demand configuration backup, as required.

This section includes the following topics:

- **Configuring Your Scheduled Nightly Backup**
- **Creating an On-demand Configuration Backup Archive**

Configuring Your Scheduled Nightly Backup

By default, the nightly backup process includes only your configuration files. You can customize your nightly backup process to include data from your Console and selected managed hosts. You can also customize your backup retention period, backup archive location, the time limit for a backup to process before timing out, and the backup priority in relation to other QRadar SIEM processes.

To configure your scheduled nightly backup:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 On the toolbar, click **Configure**.

Step 5 To customize your nightly backup, configure the values for the following parameters, as required:

Table 8-2 Backup Recovery Configuration Parameters

Parameter	Description
General Backup Configuration	
Backup Repository Path	Type the location where you want to store your backup file. The default location is `/store/backup`. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts. If you modify this path, make sure the new path is valid on every system in your deployment. ***Note:*** *Active data is stored on the /store directory. If you have both active data and backup archives stored in the same directory, data storage capacity may easily be reached and your scheduled backups may fail. We recommend you specify a storage location on another system or copy your backup archives to another system after the backup process is complete. You can use a Network File System (NFS) storage solution in your QRadar SIEM deployment. For more information on using NFS, see the Configuring Offboard Storage Guide.*
Backup Retention Period (days)	Type or select the length of time, in days, that you want to store backup files. The default is 2 days. This period of time only affects backup files generated as a result of a scheduled process. On-demand backups or imported backup files are not affected by this value.
Nightly Backup Schedule	Select one of the following options: • **No Nightly Backups** - Disables the nightly scheduled backup process. • **Configuration Backup Only** - Enables a nightly backup archive that includes configuration information only. This is the default option. • **Configuration and Data Backups** - Enables a nightly backup that includes configuration information and data.
Select the managed hosts you would like to run data backups:	This option is only displayed if you select the **Configuration and Data Backups** option. All hosts in your deployment are listed. The first host in the list is your Console; it is enabled for data backup by default, therefore no check box is displayed. If you have managed hosts in your deployment, the managed hosts are listed below the Console and each managed host includes a check box. Select the check box for the managed hosts you want to run data backups on. For each host (Console or managed hosts), you can optionally clear the data items you want to exclude from the backup archive. Choices include **Event Data** and **Flow Data**. Both options are selected by default.

Table 8-2 Backup Recovery Configuration Parameters (continued)

Parameter	Description
Configuration Only Backup	
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 180 minutes. If the backup process exceeds the configured time limit, the backup process is automatically canceled.
Backup Priority	From this list box, select the level of importance that you want the system to place on the configuration backup process compared to other processes. Options include: • LOW • MEDIUM • HIGH A priority of medium or high have a greater impact on system performance.
Data Backup	
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 1020 minutes. If the backup process exceeds the configured time limit, the backup is automatically canceled.
Backup Priority	From the list box, select the level of importance you want the system to place on the data backup process compared to other processes. Options include: • LOW • MEDIUM • HIGH A priority of medium or high have a greater impact on system performance.

Step 6 Click **Save**.

The Backup Recovery Configuration window closes.

Step 7 Close the Backup Archives window.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Creating an On-demand Configuration Backup Archive

To backup your configuration files at a time other than your nightly scheduled backup, you can create an on-demand backup archive. On-demand backup archives include only configuration information.

CAUTION

We recommend that you initiate an on-demand backup archive during a period when QRadar SIEM has low processing load, such as after normal office hours. During the backup process, system performance is affected.

To create an on-demand backup:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 From the toolbar, click **On Demand Backup**.

Step 5 Enter values for the following parameters:

- **Name** - Type a unique name you want to assign to this backup archive. The name can be up to 100 alphanumeric characters in length. Also, the name can contain following characters: underscore (_), dash (-), or period (.).
- **Description** - Optional. Type a description for this configuration backup archive. The description can be up to 255 characters in length.

Step 6 Click **Run Backup**.

Step 7 Click **OK**.

The on-demand backup process begins. Information about the backup is displayed, including:

- **Host** - Specifies the host on which the backup is currently running.
- **Name** - Specifies the user-defined name of the backup archive.
- **Backup Type** - Specifies that this is a configuration backup.
- **Initiated by** - Specifies the user account that initiated the backup process.
- **Initiated at** - Specifies the date and time the backup process was initiated.
- **Duration** - Specifies the elapsed time since the backup process was initiated.

Until the backup is complete, you are unable to start any new backup or restore processes.

When the on-demand backup is complete, the backup process information is no longer displayed and the backup archive is listed in the Existing Backups pane.

Restoring Your Backup Archives

Using the Restore a Backup window, you can restore a backup archive. This is useful if you want to restore previously archived configuration files, asset data, and offense data on your QRadar SIEM system.

Reasons to restore a backup archive include:

- You have had a system hardware failure.
- You want to store a backup archive on a replacement appliance.

Before you begin, note the following considerations:

- You can only restore a backup archive created within the same release of software, including the patch level. For example, if you are running IBM Security QRadar SIEM 7.1.0 (MR1), the backup archive must have been created in IBM Security QRadar SIEM 7.1.0 (MR1).
- The restore process only restores your configuration information, asset data, and offense data. For assistance in restoring your event or flow data, see the *Restoring Your Data Technical Note*.
- If the backup archive originated on a NATed Console system, you can only restore that backup archive on a NATed system.

This section includes the following topics:

Restoring a Backup Archive

To restore your backup archive:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 Select the archive you want to restore.

Step 5 Click **Restore**.

Step 6 Configure the following parameters, as required:

Table 8-3 Restore a Backup Window Parameters

Parameter	Description
Name	Displays the name of the backup archive.
Description	Displays the description, if any, of the backup archive.
Type	Specifies the type of backup. Only configuration backups can be restored, therefore, this parameter displays **config**.

Table 8-3 Restore a Backup Window Parameters (continued)

Parameter	Description
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive. This check box is selected by default. To clear all configuration items, clear the check box.
Restore Configuration	The Restore Configuration pane lists the configuration items to include in the restoration of the backup archive. All items are selected by default. To remove items, you can clear the check boxes for each item you want to remove or clear the **Select All Configuration Items** check box. Options include: • Custom Rules Configuration • Deployment Configuration, which includes: Assets Certificates Custom logos Device Support Modules (DSMs) Event categories Flow sources Flow and event searches Groups Log sources Offenses Store and Forward schedules Vulnerability data • User and user roles information • License key information
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive. This check box is selected by default. To clear all data items, clear this check box.
Restore Data	The Restore Data pane lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore. Options include: • Assets • Offenses

Step 7 Click **Restore**.

Step 8 Click **OK**.

The restore process begins.

Do not restart the Console until the restore process is complete. During the restore process, the following steps are taken on the Console:

- Existing files and database tables are backed up.
- Tomcat is shut down.
- All system processes are shut down.
- Files are extracted from the backup archive and restored to disk.
- Database tables are restored.
- All system processes are restarted.
- Tomcat restarts.

The restore process can take up to several hours depending on the size of the backup archive being restored. When complete, a confirmation message is displayed.

Step 9 Click **OK**.

Step 10 Choose one of the following options:

- If the QRadar SIEM user interface was closed during the restore process, open a browser and log in to QRadar SIEM.
- If the QRadar SIEM user interface has not been closed, the login window is displayed. Log in to QRadar SIEM.

A window provides the status of the restore process. This window provides any errors for each host and instructions for resolving the errors.

Step 11 Follow the instructions on the status window.

NOTE

After you have verified that your data is restored to your system, you must re-apply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

NOTE

If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after backup was performed, the secondary host displays a Failed status on the System and License Management window.

Restoring a Backup Archive Created on a Different QRadar SIEM System

Each backup archive includes IP address information of the system from which the backup archive was created. When restoring a backup archive from a different QRadar SIEM system, the IP address of the backup archive and the system you are restoring the backup are mismatched. This procedure provides steps to correct this.

To restore your backup archive that was created on a different QRadar SIEM system:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Backup and Recovery** icon.

Step 4 Select the archive you want to restore.

Step 5 Click **Restore**.

The Restore a Backup window includes a message asking you to stop the iptables service on each managed host in your deployment. The Iptables service is a Linux®-based firewall.

Step 6 Stop IP tables:

a Using SSH, log into the managed host as the root user.

User Name: **root**

Password: **<password>**

b Type the following command:

```
service iptables stop
```

c Repeat for all managed hosts in your deployment.

Step 7 On the Restore a Backup window, click **Test Hosts Access**.

The Restore a Backup (Managed Hosts Accessibility) window provides the following information.

Table 8-4 Restore a Backup (Managed Host Accessibility Parameters

Parameter	Description
Host Name	Specifies the managed host name.
IP Address	Specifies the IP address of the managed host.
Access Status	Specifies the access status to the managed host. The options include: • **Testing Access** - Specifies the test to determine access status is not complete. • **No Access** - Specifies the managed host cannot be accessed. • **OK** - Specifies the managed host is accessible.

Step 8 After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**.

If the **Access Status** column indicates a status of **No Access** for a host, stop iptables (see **Step 6**) again, and then click **Test Host Access** again to attempt a connection.

Step 9 Configure the following parameters, as required:

Table 8-5 Restore a Backup Window Parameters

Parameter	Description
Name	Displays the name of the backup archive.
Description	Displays the description, if any, of the backup archive.
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive. This check box is selected by default. To clear all configuration items, clear this check box.
Restore Configuration	The Restore Configuration pane lists the configuration items to include in the restoration of the backup archive. All items are selected by default. To remove items, you can clear the check boxes for each item you want to remove or clear the **Select All Configuration Items** check box. Options include: • Custom Rules Configuration • Deployment Configuration, which includes: Assets Custom logos Device Support Modules (DSMs) Event categories Flow sources Flow and event searches Groups Log sources Offenses Certificates Vulnerability data • User and user roles information • License key information
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive. This check box is selected by default. To clear all data items, clear the check box.

Table 8-5 Restore a Backup Window Parameters (continued)

Parameter	Description
Restore Data	The Restore Data pane lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore. Options include: • Assets • Offenses

Step 10 Click **Restore**.

Step 11 Click **OK**.

The restore process begins. Do not restart the Console until the restore process is complete.

The restore process can take up to several hours depending on the size of the backup archive being restored. When complete, a message is displayed.

Step 12 Click **OK** to log in. Choose one of the following options:

- If the QRadar SIEM user interface has been closed during the restore process, open a browser and log in to QRadar SIEM.
- If the QRadar SIEM user interface has not been closed, the login window is automatically displayed. Log in to QRadar SIEM.

A window provides the status of the restore process. This window provides any errors for each host. This window also provides instructions for resolving errors that have occurred.

Step 13 View the results of the restore process and follow the instructions to resolve errors, if required.

Step 14 Refresh your browser window.

Step 15 From the **Admin** tab, select **Advanced > Deploy Full Configuration**.

NOTE

After you have verified that your data is restored to your system, you must re-apply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

NOTE

If the backup archive originated on an HA cluster and disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after backup was performed, the secondary host displays a **Failed** status on the System and License Management window.

9 USING THE DEPLOYMENT EDITOR

Using the deployment editor, you can manage the individual components of your QRadar SIEM deployment.

This section includes the following topics:

Deployment Editor Overview

After you configure your deployment, you can access and configure the individual components of each managed host in your deployment.

NOTE

The Deployment Editor requires Java™ Runtime Environment (JRE). You can download Java™ 1.6.0_u24 at the following website: *http://www.java.com*. Also, If you are using the Firefox browser, you must configure your browser to accept Java™ Network Language Protocol (JNLP) files.

CAUTION

*Many Web browsers that use the Internet Explorer engine, such as Maxthon or MyIE, install components that may be incompatible with the **Admin** tab. You may be required to disable any Web browsers installed on your system. For further assistance, contact Customer Support.*

To access the deployment editor from behind a proxy server or firewall, you must configure the appropriate proxy settings on your desktop. This allows the software to automatically detect the proxy settings from your browser.

To configure the proxy settings:

- ▶ Open the Java ™ configuration located in your Control Pane and configure the IP address of your proxy server.

For more information on configuring proxy settings, see your Microsoft® documentation.

About the Deployment Editor User Interface

You can access the deployment editor using the **Admin** tab. You can use the deployment editor to create your deployment, assign connections, and configure each component.

The deployment editor provides the following views of your deployment:

- **System View** - Use the System View page to assign software components, such as a QRadar QFlow Collector, to managed hosts in your deployment. The System View page includes all managed hosts in your deployment. A managed host is a system in your deployment that has QRadar SIEM software installed. By default, the System View page also includes the following components:
  - **Host Context** - Monitors all QRadar SIEM components to ensure that each component is operating as expected.
  - **Accumulator** - Analyzes flows, events, reporting, writing database data, and alerting a DSM. An accumulator resides on any host that contains an Event Processor.
- **Event View** - Use the Event View page to create a view of your components including QRadar QFlow Collectors, Event Processors, Event Collectors, Off-site Sources, Off-site Targets, and Magistrate components.

On the Event View page, the left pane provides a list of components you can add to the view, and the right pane provides a view of your deployment.

On the System View page, the left pane provides a list of managed hosts, which you can view and configure. The deployment editor polls your deployment for updates to managed hosts. If the deployment editor detects a change to a managed host in your deployment, a message is displayed notifying you of the change. For example, if you remove a managed host, a message is displayed, indicating that the assigned components to that host must be re-assigned to another host. Also, if you add a managed host to your deployment, the deployment editor displays a message indicating that the managed host has been added.

Accessing the Deployment Editor

On the **Admin** tab, click **Deployment Editor**. The deployment editor is displayed. After you update your configuration settings using the deployment editor, you must save those changes to the staging area. You must manually deploy all changes using the **Admin** tab menu option. All deployed changes are then enforced throughout your deployment.

Using the Editor

The deployment editor provides you with several menu and toolbar options when configuring your views, including:

- **Menu Options**
- **Toolbar Functions**

Menu Options

The displayed menu options depend on the selected component in your view. Table 9-1 provides a list of the menu options.

Table 9-1 Deployment Editor Menu Options

Menu Option	Sub Menu Option	Description
File	Save to staging	Saves deployment to the staging area.
	Save and close	Saves deployment to the staging area and closes the deployment editor.
	Open staged deployment	Opens a deployment that was previously saved to the staging area.
	Open production deployment	Opens a deployment that was previously saved.
	Close current deployment	Closes the current deployment.
	Revert	Reverts current deployment to the previously saved deployment.
	Edit Preferences	Opens the Deployment Editor Settings window.
	Close editor	Closes the deployment editor.
Edit	Delete	Deletes a component, host, or connection.
Actions	Add a managed host	Opens the Add a Managed Host wizard.
	Manage NATed Networks	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
	Rename component	Renames an existing component. This option is only available when a component is selected.
	Configure	Configures QRadar SIEM components. This option is only available when a QRadar QFlow Collector, Event Collector, Event Processor, or Magistrate is selected.
	Assign	Assigns a component to a managed host. This option is only available when a QRadar QFlow Collector, Event Collector, Event Processor, or Magistrate is selected.
	Unassign	Unassigns a component from a managed host. This option is only available when a QRadar QFlow Collector is selected. The host for the selected component must be running the version of QRadar SIEM software as the managed host.

Toolbar Functions

The toolbar functions include:

Table 9-2 Toolbar Functions

Function	Description
Save and Close	Saves deployment to the staging area and closes the deployment editor.
Open Current Deployment	Opens current production deployment.
Open Staged Deployment	Opens a deployment that was previously saved to the staging area.
Discard	Discards recent changes and reloads last saved model.
Remove	Deletes selected item from the deployment view. This option is only available when the selected component has a managed host running a compatible version of QRadar SIEM software.
Add Managed Host	Opens the Add a Managed Host wizard, which allows you to add a managed host to your deployment.
Manage NATed Networks	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
Reset the zoom	Resets the zoom to the default.
Zoom in	Zooms in.
Zoom Out	Zooms out.

Building Your Deployment

To build your deployment, you must:

1. Build your Event View. See **Building Your Event View**.
2. Build your System View. See **Managing Your System View**.
3. Configure components. See **Configuring QRadar SIEM Components**.
4. Stage your deployment change. From the deployment editor menu, select **File > Save to Staging**.
5. Deploy all configuration changes. On the **Admin** tab menu, select **Advanced > Deploy Changes**.

   For more information on the **Admin** tab, see the **Overview**.

Before you Begin

Before you begin, you must:

- Install all necessary hardware and QRadar SIEM software.
- Install the Java™ Runtime Environment (JRE). You can download Java 1.6.0_u24 at the following website: *http://www.java.com*.

- If you are using the Firefox browser, you must configure your browser to accept Java™ Network Language Protocol (JNLP) files.
- Plan your QRadar SIEM deployment, including the IP addresses and login information for all devices in your QRadar SIEM deployment.

NOTE

If you require assistance, contact Customer Support.

Configuring Deployment Editor Preferences

To configure the deployment editor preferences:

Step 1 Select **File > Edit Preferences**.

Step 2 Configure the parameters:

- **Presence Poll Frequency** - Type how often, in milliseconds, you want the managed host to monitor your deployment for updates, for example, a new or updated managed host.
- **Zoom Increment** - Type the increment value when the zoom option is selected. For example. 0.1 indicates 10%.

Building Your Event View

The Event View page allows you to create and manage the components for your deployment, including the following components:

- **QRadar QFlow Collector** - Collects data from devices, and various live and recorded feeds, such as network taps, span/mirror ports, NetFlow, and QRadar SIEM flow logs. When the data is collected, the QRadar QFlow Collector groups related individual packets into a flow. QRadar SIEM defines these flows as a communication session between two pairs of unique IP address and ports that use the same protocol. A flow starts when the QRadar QFlow Collector detects the first packet with a unique source IP address, destination IP address, source port, destination port, and other specific protocol options that determine the start of a communication. Each additional packet is evaluated. Counts of bytes and packets are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to an Event Collector and statistical counters for the flow are reset. A flow ends when no activity for the flow is detected within the configured period of time.

  Flow reporting generates records of all active or expired flows during a specified period of time. If the protocol does not support port-based connections, QRadar SIEM combines all packets between the two hosts into a single flow record. However, a QRadar QFlow Collector does not record flows until a connection is made to another QRadar SIEM component and data is retrieved.

- **Event Collector** - Collects security events from various types of security devices, known as log sources, in your network. The Event Collector gathers events from local and remote log sources. The Event Collector then normalizes the events and sends the information to the Event Processor. The Event Collector also bundles all virtually identical events to conserve system usage.
- **Event Processor** - An Event Processor processes event and flow data from the Event Collector. The events are bundled to conserve network usage. When received, the Event Processor correlates the information from QRadar SIEM and distributes to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by QRadar SIEM to indicate any behavioral changes or policy violations for that event. Rules are then applied to the events that allow the Event Processor to process according to the configured rules. When complete, the Event Processor sends the events to the Magistrate.

  A non-Console Event Processor can be connected to the Event Processor on the Console or connected to another Event Processor in your deployment. The Accumulator is responsible for gathering flow and event information from the Event Processor.

NOTE

The Event Processor on the Console is always connected to the magistrate. This connection cannot be deleted.

See **Figure 9-1** for an example QRadar SIEM deployment that includes SIEM components.

- **Off-site Source** - Indicates an off-site event or flow data source that forwards normalized data to an Event Collector. You can configure an off-site source to receive flows or events and allows the data to be encrypted before forwarding.
- **Off-site Target** - Indicates an off-site device that receives event or flow data. An off-site target can only receive data from an Event Collector.
- **Magistrate** - The Magistrate component provides the core processing components of the security information and event management (SIEM) system. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the events or flows against the defined custom rules to create an offense. If no custom rules exist, the Magistrate uses the default rule set to process the offending event or flow. An offense is an event or flow that has been processed through QRadar SIEM using multiple inputs, individual events or flows, and combined events or flows with analyzed behavior and vulnerabilities. Magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including the amount of offenses, severity, relevance, and credibility.

  When processed, the Magistrate produces a list for each offense source, providing you with a list of attackers and their offense for each event or flow. After the Magistrate establishes the magnitude, the Magistrate then provides multiple options for resolution.

By default, the Event View page includes a Magistrate component. **Figure 9-1** shows an example of a QRadar SIEM deployment that includes SIEM components. The example shows a QRadar QFlow Collector, an Event Collector, and an Event Processor connected to the Magistrate, which allows for the collection, categorizing, and processing of flow and event information.

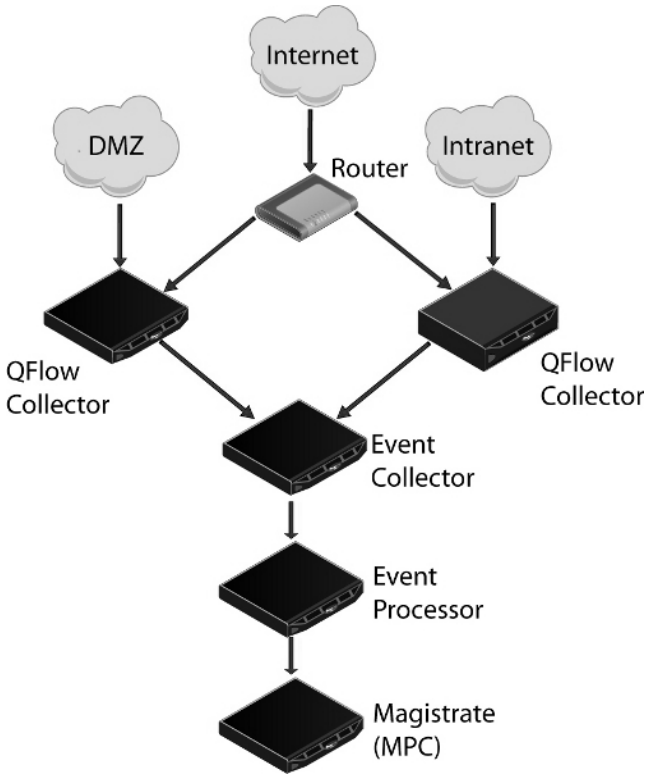

Figure 9-1 Example of SIEM Components in your QRadar SIEM Deployment

To build your Event View:

1. Add SIEM components to your view. See **Adding Components**.
2. Connect the components. See **Connecting Components**.
3. Connect deployments. See **Forwarding Normalized Events and Flows**.
4. Rename the components so each component has a unique name. See **Renaming Components**.

Adding Components

You can add the following QRadar SIEM components to your Event View:

- Event Collector
- Event Processor
- Off-site Source
- Off-site Target
- QRadar QFlow Collector

NOTE

The procedures in the section provide information on adding QRadar SIEM components using the Event View page.

You can also add components using the System View page. For information on the System View page, see **Managing Your System View**.

To add components to your Event View:

Step 1 On the **Admin** tab, click **Deployment Editor**.

Step 2 In the Event Components pane, select a component you want to add to your deployment.

Step 3 Type a unique name for the component you want to add. The name can be up to 20 characters in length and may include underscores or hyphens. Click **Next**.

Step 4 From the **Select a host to assign to** list box, select a managed host you want to assign the new component to. Click **Next**.

Step 5 Click **Finish**.

Step 6 Repeat for each component you want to add to your view.

Step 7 From the deployment editor menu, select **File > Save to staging**.

The deployment editor saves your changes to the staging area and automatically closes.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Connecting Components

After you add all the necessary components in your Event View page, you must connect them. The Event View page only allows you to connect appropriate components together. For example, you can connect an Event Collector to an Event Processor, but not a Magistrate component.

To connect components:

Step 1 In the Event View page, select the component for which you want to establish a connection.

Step 2 From the menu, select **Actions > Add Connection**.

NOTE

You can also right-click a component to access the **Action** menu item.

An arrow is displayed in your map. The arrow represents a connection between two components.

Step 3 Drag the end of the arrow to the component you want to establish a connection to. **Table 9-3** provides a list of components you are able to connect.

Table 9-3 Component Connections

You can connect a...	To	Connection Guide
QRadar QFlow Collector	Event Collector	A QRadar QFlow Collectorcan only be connected to an Event Collector.
		The number of connections is not restricted.
Event Collector	Event Processor	An Event Collector can only be connected to one Event Processor.
		A Console Event Collector can only be connected to a Console Event Processor. This connection cannot be removed.
		A non-Console Event Collector can be connected to an Event Processor on the same system.
		A non-Console Event Collector can be connected to a remote Event Processor, but only if the Event Processor does not already exist on the Console.
Event Collector	Off-site Target	The number of connections is not restricted.
Off-site Source	Event Collector	The number of connections is not restricted.
		An Event Collector connected to an Event-only appliance cannot receive an off-site connection from system hardware that has the **Receive Flows** feature enabled. For more information, see **Forwarding Normalized Events and Flows**.
		An Event Collector connected to a QFlow-only appliance cannot receive an off-site connection from a remote system if the system has the Receive Events feature enabled. For more information, see **Forwarding Normalized Events and Flows**.
Event Processor	Magistrate (MPC)	Only one Event Processor can connect to a Magistrate.

Table 9-3 Component Connections (continued)

You can connect a...	To	Connection Guide
Event Processor	Event Processor	A Console Event Processor cannot connect to a non-Console Event Processor.
		A non-Console Event Processor can be connected to another Console or non-Console Event Processor, but not both at the same time.
		A non-Console Event Processor is connected to a Console Event Processor when a non-Console managed host is added.

Step 4 Optional. Configure flow filtering on a connection between a QRadar QFlow Collector and an Event Collector.

a Right-click the arrow between the QRadar QFlow Collector and the Event Collector and select **Configure**.

b In the text field for the **Flow Filter** parameter, type the IP addresses or CIDR addresses for the Event Collectors you want the QRadar QFlow Collector to send flows to.

c Click **Save**.

Step 5 Repeat for all remaining components that require connections.

Forwarding Normalized Events and Flows

To forward normalized events and flows, you must configure an off-site Event Collector (target) in your current deployment to receive events and flows from an associated off-site Event Collector in the receiving deployment (source).

You can add the following components to your Event View page:

- **Off-site Source** - An off-site Event Collector from which you want to receive event and flow data. The off-site source must be configured with appropriate permissions to send event or flow data to the off-site target.
- **Off-site Target** - An off-site Event Collector to which you want to send event data.

For example:

To forward normalized events between two deployments (A and B), where deployment B wants to receive events from deployment A:

1. Configure deployment A with an off-site target to provide the IP address of the managed host that includes Event Collector B.
2. Connect Event Collector A to the off-site target.
3. In deployment B, configure an off-site source with the IP address of the managed host that includes Event Collector A and the port that Event Collector A is monitoring.

   If you want to disconnect the off-site source, you must remove the connections from both deployments. From deployment A, remove the off-site target and in deployment B, remove the off-site source.

   To enable encryption between deployments, you must enable encryption on both off-site source and target. Also, you must ensure the SSH public key for the off-site source (client) is available to the target (server) to ensure appropriate access. For example, if you want to enable encryption between the off-site source and Event Collector B, you must copy the public key (located at /root/.ssh/id_rsa.pub) from the off-site source to Event Collector B (add the contents of the file to /root/.ssh/authorized_keys).

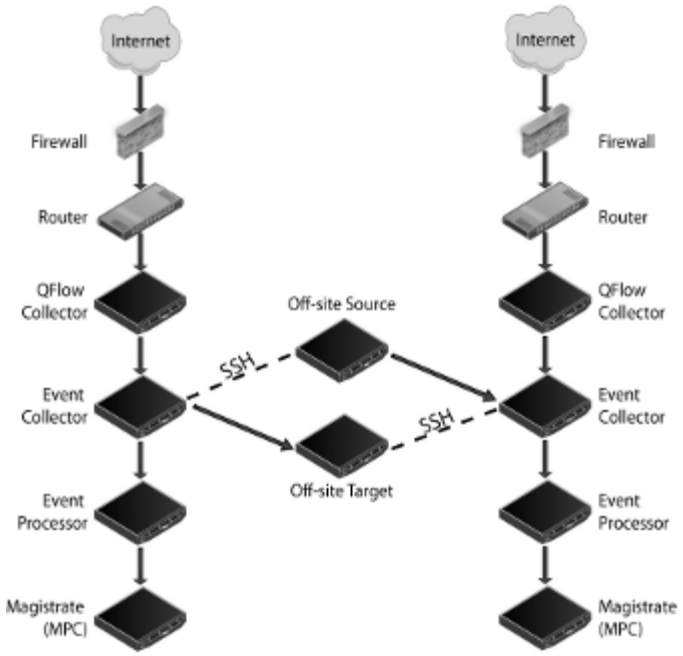

Figure 9-2 Forwarding events between deployments using SSH.

NOTE

If the off-site source or target is an all-in-one system, the public key is not automatically generated, therefore, you must manually generate the public key. For more information on generating public keys, see your Linux® documentation.

To forward normalized events and flows:

Step 1 On the **Admin** tab, click **Deployment Editor**.

Step 2 In the Event Components pane, select one of the following options:

- **Off-site Source**
- **Off-site Target**

Step 3 Type a unique name for the off-site source or off-site target. The name can be up to 20 characters in length and may include underscores or hyphens. Click **Next**.

Step 4 Enter values for the parameters:

- **Enter a name for the off-site host** - Type the name of the off-site host. The name can be up to 20 characters in length and may include the underscores or hyphens characters.
- **Enter the IP address of the source server** - Type the IP address of the managed host you want to connect the off-site host to.
- **Receive Events** - Select the check box to enable the off-site host to receive events.
- **Receive Flows** - Select the check box to enable the off-site host to receive flows.
- **Encrypt traffic from off-site source** - Select the check box to encrypt traffic from an off-site source. When enabling encryption, you must select this check box on the associated off-site source and target.

Step 5 Click **Next**.

Step 6 Click **Finish**.

Step 7 Repeat for all remaining off-site sources and targets.

Step 8 From the deployment editor menu, select **File > Save to staging**.

The deployment editor saves your changes to the staging area and automatically closes.

Step 9 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

NOTE

If you update your Event Collector configuration or the monitoring ports, you must manually update your source and target configurations to maintain the connection between deployments.

Renaming Components

You can rename a component in your view to uniquely identify components through your deployment.

To rename a component:

Step 1 In the Event Components pane, select the component you want to rename.

Step 2 From the menu, select **Actions > Rename Component**.

NOTE

You can also right-click a component to access the **Action** menu items.

Step 3 Type a new name for the component. The name must be alphanumeric with no special characters.

Step 4 Click **OK**.

Managing Your System View

The System View page allows you to manage all managed hosts in your network. A managed host is a component in your network that includes QRadar SIEM software. If you are using a QRadar SIEM appliance, the components for that appliance model are displayed on the System View page. If your QRadar SIEM software is installed on your own hardware, the System View page includes a Host Context component. The System View page allows you to select which components you want to run on each managed host.

Using the System View page, you can:

- Set up managed hosts in your deployment. See **Setting Up Managed Hosts**.
- Use QRadar SIEM with NATed networks in your deployment. See **Using NAT with QRadar SIEM**.
- Update the managed host port configuration. See **Configuring a Managed Host**.
- Assign a component to a managed host. See **Assigning a Component to a Host**.
- Configure Host Context. See **Configuring Host Context**.
- Configure an Accumulator. See **Configuring an Accumulator**.

Setting Up Managed Hosts

Using the deployment editor, you can manage all hosts in your deployment, including:

- Add a managed host to your deployment. See **Adding a Managed Host**.
- Edit an existing managed host. See **Editing a Managed Host**.
- Remove a managed host. See **Removing a Managed Host**.

You cannot add, assign or configure components on a non-Console managed host when the QRadar SIEM software version is incompatible with the software version that the Console is running. If a managed host has previously assigned components and is running an incompatible software version, you can still view the components, however, you are not able to update or delete the components. For more information, contact Customer Support.

Encryption provides greater security for all QRadar SIEM traffic between managed hosts. To provide enhanced security, QRadar SIEM also provides integrated support for OpenSSH software. OpenSSH software provides a FIPS 140-2 certified encryption solution. When integrated with QRadar SIEM, OpenSSH

provides secure communication between QRadar SIEM components.

Encryption occurs between managed hosts in your deployment, therefore, your deployment must consist of more than one managed host before encryption is possible. Encryption is enabled using SSH tunnels (port forwarding) initiated from the client. A client is the system that initiates a connection in a client/server relationship. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host to provide protected access to the respective servers. If you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console.

Figure 9-3 shows the movement of traffic within a QRadar SIEM deployment, including flows and event traffic and the client/server relationships within the deployment. When enabling encryption on a managed host, the encryption SSH tunnel is created on the client host. For example, if you enable encryption for the Event Collector in the deployment depicted in the figure below, the connection between the Event Processor and Event Collector and the connection between the Event Processor and Magistrate are encrypted. Figure 9-3 also displays the client/server relationship between the Console and the Ariel database. When you enable encryption on the Console, an encryption tunnel is used when performing event searches through the **Offenses** tab.

NOTE

You can right-click a component to enable encryption between components.

CAUTION

Enabling encryption reduces the performance of a managed host by at least 50%.

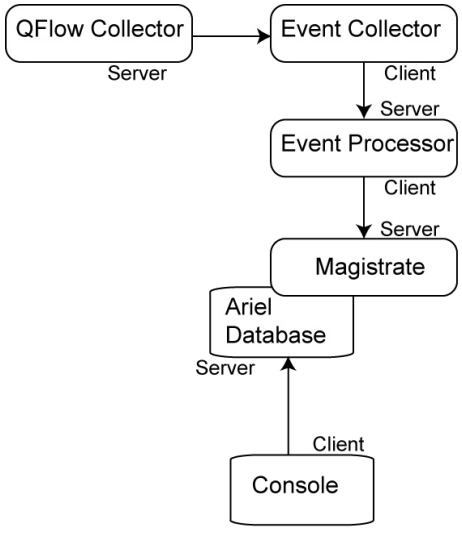

Figure 9-3 Encryption Tunnels

Adding a Managed Host

To add a managed host:

NOTE

Before you add a managed host, make sure the managed host includes QRadar SIEM software.

Step 1 From the menu, select **Actions > Add a Managed Host**.

Step 2 Click **Next**.

Step 3 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of the host you want to add to your System View.
- **Enter the root password of the host** - Type the root password for the host.
- **Confirm the root password of the host** - Type the password again.
- **Host is NATed** - Select the check box to use an existing Network Address Translation (NAT) on this managed host. For more information on NAT, see **Using NAT with QRadar SIEM**.

NOTE

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see **Using NAT with QRadar SIEM**.

- **Enable Encryption** - Select the check box to create an SSH encryption tunnel for the host.
- **Enable Compression** - Select the check box to enable data compression between two managed hosts.

If you selected the Host is NATed check box, the Configure NAT Settings page is displayed. Go to **Step 4**. Otherwise, go to **Step 5**.

NOTE

If you want to add a non-NATed managed host to your deployment when the Console is NATed, you must change the Console to a NATed host (see **Changing the NAT Status for a Managed Host**) before adding the managed host to your deployment.

Step 4 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use.
  - If the managed host is on the same subnet as the Console, select the Console of the NATed network.
  - If the managed host is not on the same subnet as the Console, select the managed host of the NATed network.

NOTE

For information on managing your NATed networks, see **Using NAT with QRadar SIEM**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

NOTE

If your deployment included undeployed changes, a window is displayed requesting you to deploy all changes.

The System View is displayed, including the host in the Managed Hosts pane.

Editing a Managed Host

To edit an existing managed host:

Step 1 Click the **System View** tab.

Step 2 Right-click the managed host you want to edit and select **Edit Managed Host**.

NOTE

This option is only available when the selected component has a managed host running a compatible version of QRadar SIEM software.

Step 3 Click **Next**.

Step 4 Edit the following values, as necessary:

- **Host is NATed** - Select the check box if you want to use existing Network Address Translation (NAT) on this managed host. For more information on NAT, see **Using NAT with QRadar SIEM**.

NOTE

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see **Using NAT with QRadar SIEM**.

- **Enable Encryption** - Select the check box if you want to create an encryption tunnel for the host.

If you selected the Host is NATed check box, the Configure NAT settings page is displayed. Go to **Step 5**. Otherwise, go to **Step 6**.

Step 5 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use. For information on managing your NATed networks, see **Using NAT with QRadar SIEM**.

Step 6 Click **Next**.

Step 7 Click **Finish**.

The System View page is displayed, including the updated host in the Managed Hosts pane.

Removing a Managed Host

You can remove non-Console managed hosts from your deployment. You cannot remove a managed host that is hosting the QRadar SIEM Console.

To remove a managed host:

Step 1 Click the **System View** tab.

Step 2 Right-click the managed host you want to delete and select **Remove host**.

NOTE

This option is only available when the selected component has a managed host running a compatible version of QRadar SIEM software.

Step 3 Click **OK**.

Step 4 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Using NAT with QRadar SIEM

Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and essentially hides internal IP addresses.

Before you enable NAT for a QRadar SIEM managed host, you must set up your NATed networks using static NAT translation. This ensures communications between managed hosts that exist within different NATed networks. For example, in **Figure 9-4**, the QFlow 1101 in Network 1 has an internal IP address of 10.100.100.1. When the QFlow 1101 wants to communicate with the Event Collector in Network 2, the NAT router translates the IP address to 192.15.2.1.

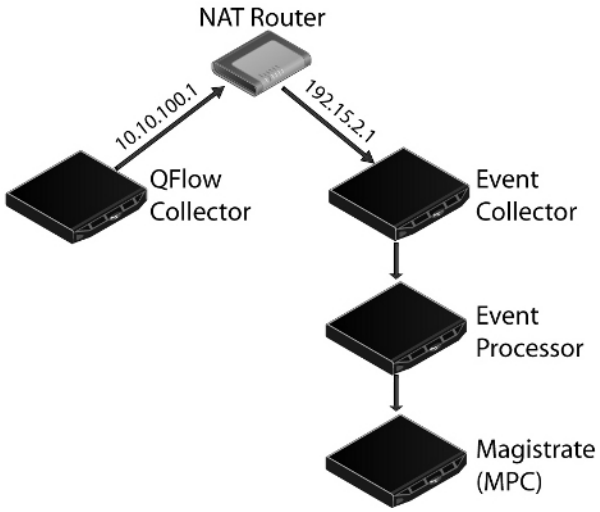

Figure 9-4 Using NAT with QRadar SIEM

NOTE

Before you enable NAT using QRadar SIEM, your static NATed networks must be set up and configured on your network. For more information, see your network administrator.

You can add a non-NATed managed host using inbound NAT for a public IP address. You can also use a dynamic IP address for outbound NAT. However, both must be located on the same switch as the Console or managed host. You must configure the managed host to use the same IP address for the public and private IP addresses.

When adding or editing a managed host, you can enable NAT for that managed host. You can also use the deployment editor to manage your NATed networks, including:

- **Adding a NATed Network to QRadar SIEM**
- **Editing a NATed Network**
- **Deleting a NATed Network From QRadar SIEM**
- **Changing the NAT Status for a Managed Host**

Adding a NATed Network to QRadar SIEM

To add a NATed network to your QRadar SIEM deployment:

Step 1 In the deployment editor, click the **NATed Networks** icon.

NOTE

You can also select the **Actions > Manage NATed Networks** menu option to access the Manage NATed Networks window.

Step 2 Click **Add**.

Step 3 Type a name for a network you want to use for NAT.

Step 4 Click **OK**.

The Manage NATed Networks window is displayed, including the added NATed network.

Step 5 Click **OK**.

Step 6 Click **Yes**.

Editing a NATed Network

To edit a NATed network:

Step 1 In the deployment editor, click the **NATed Networks** icon.

NOTE

You can also select the **Actions > Manage NATed Networks** menu option to access the Manage NATed Networks window.

Step 2 Select the NATed network you want to edit. Click **Edit.**

Step 3 Type a new name for of the NATed network.

Step 4 Click **OK**.

The Manage NATed Networks window is displayed, including the updated NATed networks.

Step 5 Click **OK**.

Step 6 Click **Yes**.

Deleting a NATed Network From QRadar SIEM

To delete a NATed network from your deployment:

Step 1 In the deployment editor, click the **NATed Networks** icon.

NOTE

You can also select the **Actions > Manage NATed Networks** menu option to access the Manage NATed Networks window.

Step 2 Select the NATed network you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Step 5 Click **Yes**.

Changing the NAT Status for a Managed Host

To change your NAT status for a managed host, make sure you update the managed host configuration within QRadar SIEM before you update the device. This prevents the host from becoming unreachable and allows you to deploy changes to that host.

To change the status of NAT (enable or disable) for an existing managed host:

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Right-click the managed host you want to edit and select **Edit Managed Host**.

Step 3 Click **Next**.

Step 4 Choose one of the following options:

a If you want to enable NAT for the managed host, select the **Host is NATed** check box and click **Next**. Go to **Step 5**.

NOTE

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation.

b If you want to disable NAT for the managed host, clear the **Host is NATed** check box. Go to **Step 6**.

Step 5 To select a NATed network, enter values for the following parameters:

- **Change public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.

- **Select NATed network** - From the list box, select the network you want this managed host to use.
- **Manage NATs List** - Click this icon to update the NATed network configuration. For more information, see **Using NAT with QRadar SIEM**.

Step 6 Click **Next**.

Step 7 Click **Finish**.

The System View page is displayed, including the updated host in the Managed Hosts pane.

NOTE

When you change the NAT status for an existing managed host, error messages may be displayed. Ignore these error messages.

Step 8 Update the configuration for the device (firewall) to which the managed host is communicating.

Step 9 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Configuring a Managed Host

To configure a managed host:

Step 1 From the System View page, right-click the managed host you want to configure and select **Configure**.

Step 2 Enter values for the parameters:

- **Minimum port allowed** - Type the minimum port for which you want to establish communications.
- **Maximum port allowed** - Type the maximum port for which you want to establish communications.
- **Ports to exclude** - Type the ports you want to exclude from communications. Separate multiple ports using a comma.

Step 3 Click **Save**.

Assigning a Component to a Host

You can assign the QRadar SIEM components that you added in the Event View page to the managed hosts in your deployment.

NOTE

This section provides information on assigning a component to a host using the System View page, however, you can also assign components to a host on the Event View page.

To assign a host:

Step 1 Click the **System View** tab.

Step 2 From the **Managed Host** list, select the managed host you want to assign a QRadar SIEM component to.

Step 3 Select the component you want to assign to a managed host.

Step 4 From the menu, select **Actions > Assign**.

NOTE You can also right-click a component to access the **Actions** menu items.

Step 5 From the **Select a host** list box, select the host that you want to assign to this component. Click **Next**.

NOTE The list box only displays managed hosts that are running a compatible version of QRadar SIEM software.

Step 6 Click **Finish**.

Configuring Host Context

The Host Context component monitors all QRadar SIEM components to make sure that each component is operating as expected.

To configure the Host Context component:

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Select the managed host that includes the host context you want to configure.

Step 3 Select the Host Context component.

Step 4 From the menu, select **Actions > Configure**.

NOTE You can also right-click a component to access the **Actions** menu item.

Step 5 Enter values for the parameters:

Table 9-4 Host Context Parameters

Parameter	Description
Disk Usage Sentinel Settings	
Warning Threshold	When the configured threshold of disk usage is exceeded, an email is sent to the administrator indicating the current state of disk usage. The default warning threshold is 0.75, therefore, when disk usage exceeds 75%, an email is sent indicating that disk usage is exceeding 75%. If disk usage continues to increase above the configured threshold, a new email is sent after every 5% increase in usage. By default, Host Context monitors the following partitions for disk usage: • / • /store • /store/tmp Type the warning threshold for disk usage. ***Note:*** *Notification emails are sent from the email address specified in the* ***Alert Email From Address*** *parameter to the email address specified in the* ***Administrative Email Address*** *parameter. These parameters are configured on the System Settings window. For more information, see* **Setting Up QRadar SIEM**.
Recovery Threshold	When the system has exceeded the shutdown threshold, disk usage must fall below the recovery threshold before QRadar SIEM processes are restarted. The default is 0.90, therefore, processes are not restarted until disk usage is below 90%. Type the recovery threshold. ***Note:*** *Notification emails are sent from the email address specified in the* ***Alert Email From Address*** *parameter to the email address specified in the* ***Administrative Email Address*** *parameter. These parameters are configured on the System Settings window. For more information, see* **Setting Up QRadar SIEM**.

Table 9-4 Host Context Parameters (continued)

Parameter	Description
Shutdown Threshold	When the system exceeds the shutdown threshold, all QRadar SIEM processes are stopped. An email is sent to the administrator indicating the current state of the system. The default is 0.95, therefore, when disk usage exceeds 95%, all QRadar SIEM processes stop. Type the shutdown threshold. ***Note:*** *Notification emails are sent from the email address specified in the* ***Alert Email From Address*** *parameter to the email address specified in the* ***Administrative Email Address*** *parameter. These parameters are configured on the System Settings window. For more information, see* **Setting Up QRadar SIEM**.
Inspection Interval	Type the frequency, in milliseconds, that you want to determine disk usage.
SAR Sentinel Settings	
Inspection Interval	Type the frequency, in milliseconds, that you want to inspect SAR output. The default is 300,000 ms.
Alert Interval	Type the frequency, in milliseconds, that you want to be notified that the thresholds have been exceeded. The default is 7,200,000 ms.
Time Resolution	Type the time, in seconds, that you want the SAR inspection to be engaged. The default is 60 seconds.
Log Monitor Settings	
Inspection Interval	Type the frequency, in milliseconds, that you want to monitor the log files. The default is 60,000 ms.
Monitored SYSLOG File Name	Type a filename for the SYSLOG file. The default is /var/log/qradar.error.
Alert Size	Type the maximum number of lines you want to monitor from the log file. The default is 1000.

Step 6 Click **Save**.

Configuring an Accumulator

The accumulator component assists with data collection and anomaly detection for the Event Processor on a managed host. The accumulator component is responsible for receiving streams of flows and events from the local Event Processor, writing database data, and contains the Anomaly Detection Engine (ADE).

To configure an accumulator:

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Select the managed host you want to configure.

Step 3 Select the accumulator component.

Step 4 From the menu, select **Actions > Configure**.

NOTE

You can also right-click a component to access the **Actions** menu item.

The Accumulator Configuration window provides the following parameters.

Table 9-5 Accumulator Parameters

Parameter	Description
Central Accumulator	Specifies if the current component is a central accumulator. A central accumulator only exists on a Console system. Options include: • **True** - Specifies that the component is a central accumulator on the Console and receives TCP data from non-central accumulators. • **False** - Specifies that the component is not a central accumulator, but is deployed on the Event Processor and forwards data to a central accumulator on the Console.
Anomaly Detection Engine	Type the address and port of the ADE. The ADE is responsible for analyzing network data and forwarding the data to the rule system for resolution. For the central accumulator, type the address and port using the following syntax: **<Console>:<port>** For a non-central accumulator, type the address and port using the following syntax: **<non-Console IP Address>:<port>**
Streamer Accumulator Listen Port	Type the listen port of the accumulator responsible for receiving streams of flows from the event processor. The default value is 7802.
Alerts DSM Address	Type the DSM address for forwarding alerts from the accumulator using the following syntax: **<DSM_IP address>:<DSM port number>**.

Step 5 Click **Save**.

Configuring QRadar SIEM Components

This section includes the following topics:

Configuring a QRadar QFlow Collector

This section provides information on how to configure a QRadar QFlow Collector. For an overview of the QRadar QFlow Collector component, see **Building Your Event View**.

NOTE

You can configure a flow filter on the connection from a QRadar QFlow Collector and multiple Event Collectors. A flow filter controls which flows a component receives. The **Flow Filter** parameter is available on the Flow Connection Configuration window. Right-click the arrow between the component you want to configure for flow filtering and select **Configure**. For more information on configuring a flow filter, see **Connecting Components**.

To configure a QRadar QFlow Collector:

Step 1 From either the Event View or System View pages, select the QRadar QFlow Collector you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE

You can also right-click a component to access the **Actions** menu items.

Step 3 Enter values for the parameters:

Table 9-6 QRadar QFlow Collector Parameters

Parameter	Description
Event Collector Connections	Specifies the Event Collector component connected to this QRadar QFlow Collector. The connection is displayed in the following format: <Host IP Address>:<Port>. If the QRadar QFlow Collector is not connected to an Event Collector, the parameter is empty.
QFlow CollectorID	Type a unique ID for the QRadar QFlow Collector.
Maximum Content Capture	Type the capture length, in bytes, to attach to a flow. The range is from 0 to 65535. A value of 0 disables content capture. The default is 64 bytes. QRadar QFlow Collectors capture a configurable number of bytes at the start of each flow. Transferring large amounts of content across the network may affect network and QRadar SIEM performance. On managed hosts where the QRadar QFlow Collectors are located on close high-speed links, you can increase the content capture length. ***Note:*** *Increasing content capture length increases disk storage requirements for recommended disk allotment.*

Table 9-6 QRadar QFlow Collector Parameters (continued)

Parameter	Description
Alias Autodetection	Type one of the following values: • **Yes** - Enables the QRadar QFlow Collector to detect external flow source aliases. When a QRadar QFlow Collector receives traffic from a device with an IP address, but no current alias, the QRadar QFlow Collector attempts a reverse DNS lookup to determine the host name of the device. If the lookup is successful, the QRadar QFlow Collector adds this information to the database and reports this information to all QRadar QFlow Collectors in your deployment. • **No** - Prevents the QRadar QFlow Collector from detecting external flow sources aliases. For more information on flow sources, see **Managing Flow Sources**.

Step 4 On the toolbar, click **Advanced** to display the advanced parameters.

The advanced configuration parameters are displayed.

Step 5 Enter values for the parameters, as necessary:

Table 9-7 QRadar QFlow Collector Parameters

Parameter	Description
Event Collector Connections	Type the Event Collector connected to this QRadar QFlow Collector. The connection is displayed in the following format: <Host IP Address>:<Port>. If the QRadar QFlow Collector is not connected to an Event Collector, the parameter is empty.
Flow Routing Mode	Type one of the following values: • **0** - Type **0** to enable Distributor Mode, which allows QRadar QFlow Collector to group flows that have similar properties. • **1** - Type **1** to enable Flow Mode, which prevents the bundling of flows.
Maximum Data Capture/Packet	Type the amount of bytes and packets you want the QRadar QFlow Collector to capture.
Time Synchronization Server IP Address	Type the IP address or host name of the time server.
Time Synchronization Timeout Period	Type the length of time you want the managed host to continue attempting to synchronize the time before timing out. The default is 15 minutes.

Table 9-7 QRadar QFlow Collector Parameters (continued)

Parameter	Description
Endace DAG Interface Card Configuration	Type the Endace Network Monitoring Interface card parameters. For more information on the required input for this parameter, see the Qmmunity website or contact Customer Support.
Flow Buffer Size	Type the amount of memory, in MB, that you want to reserve for flow storage. The default is 400 MB.
Maximum Number of Flows	Type the maximum number of flows you want to send from the QRadar QFlow Collector to an Event Collector.
Remove duplicate flows	Type one of the following values: • **Yes** - Enables the QRadar QFlow Collector to remove duplicate flows. • **No** - Prevents the QRadar QFlow Collector from removing duplicate flows.
Verify NetFlow Sequence Numbers	Type one of the following values: • **Yes** - Enables the QRadar QFlow Collector to check the incoming NetFlow sequence numbers to ensure that all packets are present and in order. A notification is displayed if a packet is missing or received out-of-order. • **No** - Prevents the QRadar QFlow Collector from checking the incoming NetFlow sequence numbers to ensure that all packets are present and in order.
External Flow De-duplication method	Type the method you want to use to remove duplicate external flow sources (de-duplication). Options include: • **Source** - Enables the QRadar QFlow Collector to compare originating flow sources. This method compares the IP address of the device that exported the current external flow record to that of the IP address of the device that exported the first external record of the particular flow. If the IP addresses do not match, the current external flow record is discarded. • **Record** - Enables the QRadar QFlow Collector to compare individual external flow records. This method logs a list of every external flow record detected by a particular device and compares each subsequent record to that list. If the current record is found in the list, that record is discarded.
Flow Carry-over Window	Type the number of seconds before the end of an interval that you want one-sided flows to be held over until the next interval if the flow. This allows time for the inverse side of the flow to arrive before being reported.

Table 9-7 QRadar QFlow Collector Parameters (continued)

Parameter	Description
External flow record comparison mask	***Note:*** *This parameter is only valid if you typed* ***Record*** *in the* ***External Flow De-duplication method*** *parameter.* Type the external flow record fields you want to use to remove duplicate flows. Valid options include: • **D** - Direction • **B** - ByteCount • **P** - (PacketCount You can combine these options. Possible combinations of the options include: • **DBP** - Uses direction, byte count, and packet count when comparing flow records. • **XBP** - Uses byte count and packet count when comparing flow records. • **DXP** - Uses direction and packet count when comparing flow records. • **DBX** - Uses direction and byte count when comparing flow records. • **DXX** - Uses direction when comparing flow records. • **XBX** - Uses byte count when comparing records. • **XXP** - Uses packet count when comparing records.
Create Superflows	Type one of the following options: • **Yes** - Enables the QRadar QFlow Collector to create Superflows from group flows that have similar properties. • **No** - Prevents the creation of Superflows.
Type A Superflows	Type the threshold for type A superflows. A type A superflow is a group of flows from one host to many hosts. This is a unidirectional flow that is an aggregate of all flows that have the same different destination hosts, but following parameters are the same: • Protocol • Source bytes • Source hosts • Destination network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)

Table 9-7 QRadar QFlow Collector Parameters (continued)

Parameter	Description
Type B Superflows	Type the threshold for type B superflows. A type B superflow is group of flows from many hosts to one host. This is unidirectional flow that is an aggregate of all flows that have different source hosts, but the following parameters are the same: • Protocol • Source bytes • Source packets • Destination host • Source network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)
Type CSuperflows	Type the threshold for type C superflows. Type C superflows are a group of flows from one host to another host. This is a unidirectional flow that is an aggregate of all non-ICMP flows have different source or destination ports, but the following parameters are the same: • Protocol • Source host • Destination host • Source bytes • Destination bytes • Source packets • Destination packets
Recombine Asymmetric Superflows	In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This is called asymmetric routing. You can combine flows received from one or more QRadar QFlow Collectors. However, if you want to combine flows from multiple QRadar QFlow Collectors, you must configure flow sources in the **Asymmetric Flow Source Interface(s**) parameter in the QRadar QFlow Collector configuration. Choose one of the following options: • **Yes** - Enables the QRadar QFlow Collector to recombine asymmetric flows. • **No** - Prevents the QRadar QFlow Collector from recombining asymmetric flows.

Table 9-7 QRadar QFlow Collector Parameters (continued)

Parameter	Description
Ignore Asymmetric Superflows	Type one of the following options: • **Yes** - Enables the QRadar QFlow Collector to create superflows while asymmetric flows are enabled. • **No** - Prevents the QRadar QFlow Collector from creating superflows while asymmetric flows are enabled.
Minimum Buffer Data	Type the minimum amount of data, in bytes, that you want the Endace Network Monitoring Interface Card to receive before the captured data is returned to the QRadar QFlow Collector process. For example, if this parameter is 0 and no data is available, the Endace Network Monitoring Interface Card allows non-blocking behavior.
Maximum Wait Time	Type the maximum amount of time, in microseconds, that you want the Endace Network Monitoring Interface Card to wait for the minimum amount of data, as specified in the **Minimum Buffer Data** parameter.
Polling Interval	Type the interval, in microseconds, that you want the Endace Network Monitoring Interface Card to wait before checking for additional data. A polling interval avoids excessive polling traffic to the card and, therefore, conserves bandwidth and processing time.

Step 6 Click **Save**.

Step 7 Repeat for all QRadar QFlow Collectors in your deployment you want to configure.

Configuring an Event Collector

This section provides information on how to configure an Event Collector. For an overview of the Event Collector component, see **Building Your Event View**.

To configure an Event Collector:

Step 1 From either the Event View or System View pages, select the Event Collector you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE You can also right-click a component to access the **Action** menu items.

Step 3 Enter values for the parameters:

Table 9-8 Event Collector Parameters

Parameter	Description
Destination Event Processor	Specifies the Event Processor component connected to this QRadar QFlow Collector. The connection is displayed in the following format: <Host IP Address>:<Port>. If the QRadar QFlow Collector is not connected to an Event Processor, the parameter is empty.

Table 9-8 Event Collector Parameters (continued)

Parameter	Description
Flow Listen Port	Type the listen port for flows.
Event Forwarding Listen Port	Type the Event Collector event forwarding port.
Flow Forwarding Listen Port	Type the Event Collector flow forwarding port.

Step 4 On the toolbar, click **Advanced** to display the advanced parameters.

The advanced configuration parameters are displayed.

Step 5 Enter values for the parameters:

Table 9-9 Event Collector Advanced Parameters

Parameter	Description
Primary Collector	Specifies one of the following values: • **True** - Specifies that the Event Collector is located on a Console system. • **False** - Specifies that the Event Collector is located on a non-Console system.
Autodetection Enabled	Type of the following values: • **Yes** - Enables the Event Collector to automatically analyze and accept traffic from previously unknown log sources. The appropriate firewall ports are opened to enable Autodetection to receive events. This is the default. • **No** - Prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources. For more information on configuring log sources, see the *Managing Log Sources Guide.*
Flow Deduplication Filter	Type the amount of time in seconds flows are buffered before they are forwarded.
Asymmetric Flow Filter	Type the amount of time in seconds asymmetric flows will be buffered before they are forwarded.
Forward Events Already Seen	Type one of the following options: • **True** - Enables the Event Collector to forward events that have already been detected on the system. • **False** - Prevents the Event Collector from forwarding events that have already been detected on the system. This prevents event looping on your system.

Step 6 Click **Save**.

Step 7 Repeat for all Event Collectors in your deployment you want to configure.

Configuring an Event Processor

This section provides information on how to configure an Event Processor. For an overview of the Event Processor component, see **Building Your Event View**.

To configure an Event Processor:

Step 1 From either the Event View or System View pages, select the Event Processor you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE

You can also right-click a component to access the **Action** menu items.

Step 3 Enter values for the parameters:

Table 9-10 Event Processor Parameters

Parameter	Description
Event Collector Connections Listen Port	Type the port that the Event Processor monitors for incoming Event Collector connections. The default value is port 32005.
Event Processor Connections Listen Port	Type the port that the Event Processor monitors for incoming Event Processor connections. The default value is port 32007.

Step 4 On the toolbar, click **Advanced** to display the advanced parameters.

The advanced configuration parameters are displayed.

Step 5 Enter values for the parameters, as necessary:

Table 9-11 Event Processor Advanced Parameters

Parameter	Description
Test Rules	***Note:** The **test rules** list box in the Deployment Editor is available for non-Console Event Processors only.* Type one of the following options: • **Locally** - Rules are tested on the Event Processor and not shared with the system. Testing rules locally is the default for Console Event Processors. • **Globally** - Allows individual rules for every Event Processor to be shared and tested system wide. Each rule in **Offenses > Rules** can be toggled to **Global** for detection by any Event Processor on the system. ***Note:** If a rule is configured to test locally, the Globally option does not override the rule setting.* For example, you can create a rule to alert you when there is five failed login attempts within 5 minutes. The default for the rule is set to local. When the Event Processor containing the local rule observes five failed login attempts, the rule generates a response. When the rule in the example above is set to Global, when five failed login attempts within 5 minutes is detected on any Event Processor, the rule generates a response. This means that when rules are shared globally, the rule can detect when one failed login attempt comes from five separate event processors. Testing rules globally is the default for non-Console Event Processors, with each rule on the Event Processor set to test locally.
Overflow Event Routing Threshold	Type the events per second threshold that the Event Processor can manage. Events over this threshold are placed in the cache.
Overflow Flow Routing Threshold	Type the flows per minute threshold that the Event Processor can manage. Flows over this threshold are placed in the cache.
Events database path	Type the location you want to store events. The default is **`/store/ariel/events`**.
Payloads database length	Type the location you want to store payload information. The default is **`/store/ariel/payloads`**.

Step 6 Click **Save**.

Step 7 Repeat for all Event Processors in your deployment you want to configure.

Configuring the Magistrate

This section provides information on how to configure the Magistrate. For an overview of the Magistrate component, see **Building Your Event View**.

To configure the Magistrate component:

Step 1 From either the Event View or System View pages, select the Magistrate component you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE You can also right-click a component to access the **Action** menu items.

Step 3 On the toolbar, click **Advanced** to display the advanced parameters.

The advanced configuration parameters are displayed.

Step 4 In the **Overflow Routing Threshold** field, type the events per second threshold that the Magistrate can manage events. Events over this threshold are placed in the cache. The default is 20,000.

Step 5 Click **Save**.

Configuring an Off-site Source

This section provides information on how to configure an off-site source. For an overview of the off-site source component, see **Building Your Event View**.

NOTE When configuring off-site source and target components, we recommend that you deploy the Console with the off-site source first and the Console with the off-site target second to prevent connection errors.

To configure an off-site source component:

Step 1 From either the Event View or System View pages, select the off-site source you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE You can also right-click a component to access the **Action** menu items.

Step 3 Enter values for the parameters:

Table 9-12 Off-site Source Parameters

Parameter	Description
Receive Events	Type one of the following values: • **True** - Enables the system to receive events from the off-site source host. • **False** - Prevents the system from receiving events from the off-site source host.

Table 9-12 Off-site Source Parameters (continued)

Parameter	Description
Receive Flows	Type one of the following values: • **True** - Enables the system to receive flows from the off-site source host. • **False** - Prevents the system from receiving flows from the off-site source host.

Step 4 Click **Save**.

Step 5 Repeat for all off-site sources in your deployment you want to configure.

Configuring an Off-site Target

This section provides information on how to configure an off-site target. For an overview of the off-site target component, see **Building Your Event View**.

NOTE

When configuring off-site source and target components, we recommend that you deploy the Console with the off-site source first and the Console with the off-site target second to prevent connection errors.

To configure an off-site target component:

Step 1 From either the Event View or System View pages, select the off-site target you want to configure.

Step 2 From the menu, select **Actions > Configure**.

NOTE

You can also right-click a component to access the **Action** menu items.

Step 3 Enter values for the parameters:

Table 9-13 Off-site Target Parameters

Parameter	Description
Event Collector Listen Port	Type the Event Collector listen port for receiving event data. The default listen port for events is 32004. ***Note:*** *If the off-site target system has been upgraded from a previous QRadar SIEM software version, you must change the port from the default (32004) to the port specified in the* ***Event Forwarding Listen Port*** *parameter for the off-site target. For more information on how to access the Event Forwarding Listen port on the off-site target, see* **Configuring an Event Collector***.*
Flow Collector Listen Port	Type the Event Collector listen port for receiving flow data. The default listen port for flows is 32000.

Step 4 Click **Save**.

10 MANAGING FLOW SOURCES

Using the Flow Sources feature, you can manage the flow sources in your deployment.

This section includes the following topics:

Flow Sources Overview

QRadar SIEM allows you to integrate flow sources. Flow sources are classed as either internal or external:

- **Internal flow sources** - Includes any additional hardware installed on a managed host, such as a Network Interface Card (NIC). Depending on the hardware configuration of your managed host, the internal flow sources may include:
  - Network interface Card
  - Endace Network Monitoring Interface Card
  - Napatech Interface
- **External flow sources** - Includes any external flow sources that send flows to the QRadar QFlow Collector. If your QRadar QFlow Collector receives multiple flow sources, you can assign each flow source a distinct name, providing the ability to distinguish one source of external flow data from another when received on the same QRadar QFlow Collector. External flow sources may include:
  - NetFlow
  - IPFIX
  - sFlow
  - J-Flow
  - Packeteer
  - Flowlog File

QRadar SIEM can forward external flows source data using the spoofing or non-spoofing method:

- **Spoofing** - Resends the inbound data received from flow sources to a secondary destination. To ensure flow source data is sent to a secondary destination, configure the Monitoring Interface in the Flow Source configuration (see **Adding a Flow Source**) to the port on which data is being received (management port). When you use a specific interface, the QRadar QFlow Collector uses a promiscuous mode capture to obtain flow source data, rather than the default UDP listening port on port 2055. This allows the QRadar QFlow Collector to capture flow source packets and forward the data.
- **Non-Spoofing** - For the non-spoofing method, configure the **Monitoring Interface** parameter in the Flow Source Configuration (see **Adding a Flow Source**) as **Any**. The QRadar QFlow Collector opens the listening port, which is the port configured as the Monitoring Port to accept flow source data. The data is processed and forwarded to another flow source destination. The source IP address of the flow source data becomes the IP address of the QRadar SIEM system, not the original router that sent the data.

NetFlow A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. The process of sending data from NetFlow is often referred to as a NetFlow Data Export (NDE). You can configure QRadar SIEM to accept NDE's and thus become a NetFlow collector. QRadar SIEM supports NetFlow versions 1, 5, 7, and 9. For more information on NetFlow, see *http://www.cisco.com*.

While NetFlow expands the amount of the network that is monitored, NetFlow uses a connection-less protocol (UDP) to deliver NDEs. After an NDE is sent from a switch or router, the NetFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, NetFlow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for NetFlow, you must:

- Make sure the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the QRadar QFlow Collector configuration, you must also update your firewall access configuration. For more information about QRadar QFlow Collector configuration, see **Using the Deployment Editor**.
- Make sure the appropriate ports are configured for your QRadar QFlow Collector

If you are using NetFlow version 9, make sure the NetFlow template from the NetFlow source includes the following fields:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

IPFIX Internet Protocol Flow Information Export (IPFIX) is an accounting technology that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a IPFIX collector. IBM Security Network Protection XGS 5000, a next generation IPS, is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE). IPFIX provides more flow information and deeper insight than NetFlow v9. You can configure QRadar SIEM to accept NDE's and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After a NDE is sent from the IPFIX forwarding device, the IPFIX record may be purged.

To configure QRadar SIEM to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows using the same process.

NOTE

Your QRadar SIEM system may include a default NetFlow flow source; therefore, you may not be required to configure a Netflow flow source. To confirm that your system includes a default NetFlow flow source, select **Admin > Flow Sources**. If **default_Netflow** is listed in the flow source list, IPFIX is already configured.

When you configure an external flow source for IPFIX, you must:

- Ensure the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the QRadar QFlow Collector configuration, you must also update your firewall access configuration. For more information on QRadar QFlow Collector configuration, see the *IBM Security QRadar SIEM Administration Guide*.
- Ensure the appropriate ports are configured for your QRadar QFlow Collector.
- Ensure the IPFIX template from the IPFIX source includes the following fields:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

sFlow A multi-vendor and end-user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously. sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. QRadar SIEM supports sFlow versions 2, 4, and 5. Note that sFlow traffic is based on sampled data and, therefore, may not represent all network traffic. For more information on sFlow, see *http://www.sflow.org*.

sFlow uses a connection-less protocol (UDP). When data is sent from a switch or router, the sFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, sFlow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for sFlow, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure the appropriate ports are configured for your QRadar QFlow Collector.

J-Flow A proprietary accounting technology used by Juniper® Networks that allows you to collect IP traffic flow statistics. J-Flow enables you to export data to a UDP port on a J-Flow collector. Using J-Flow, you can also enable J-Flow on a router or interface to collect network statistics for specific locations on your network. Note that J-Flow traffic is based on sampled data and, therefore, may not represent all network traffic. For more information on J-Flow, see *http://www.juniper.net*.

J-Flow uses a connection-less protocol (UDP). When data is sent from a switch or router, the J-Flow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, J-Flow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for J-Flow, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure the appropriate ports are configured for your QRadar QFlow Collector.

Packeteer

Packeteer devices collect, aggregate, and store network performance data. After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to QRadar SIEM.

Packeteer uses a connection-less protocol (UDP). When data is sent from a switch or router, the Packeteer record is purged. As UDP is used to send this information and does not guarantee the delivery of data, Packeteer records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

To configure Packeteer as an external flow source, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure that you configure Packeteer devices to export flow detail records and configure the QRadar QFlow Collector as the destination for the data export.
- Make sure the appropriate ports are configured for your QRadar QFlow Collector.
- Make sure the class IDs from the Packeteer devices can automatically be detected by the QRadar QFlow Collector.
- For additional information on mapping Packeteer applications into QRadar SIEM, see the *Mapping Packeteer Applications into QRadar Technical Note*.

Flowlog File

A file generated from the QRadar SIEM flow logs.

Napatech Interface

If you have a Napatech Network Adapter installed on your QRadar SIEM system, the **Naptatech Interface** option is displayed as a configurable packet-based flow source on the QRadar SIEM user interface. The Napatech Network Adapter provides next-generation programmable and intelligent network adapter for your network. For more information regarding Napatech Network Adapters, see your Napatech vendor documentation.

Managing Flow Sources

For QRadar SIEM appliances, QRadar SIEM automatically adds default flow sources for the physical ports on the appliance. Also, QRadar SIEM also includes a default NetFlow flow source. If QRadar SIEM is installed on your own hardware, QRadar SIEM attempts to automatically detect and add default flow sources for any physical devices, such as a Network Interface Card (NIC). Also, when you assign a QRadar QFlow Collector, QRadar SIEM includes a default NetFlow flow source.

This section includes the following topics:

Adding a Flow Source

To add a flow source:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

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

Step 5 Click **Add**.

Step 6 Enter values for the parameters:

Table 10-1 Add Flow Source Window Parameters

Parameter	Description
Build from existing flow source	Select the check box if you want to create this flow source using an existing flow source as a template. After you select the check box, use the list box to select a flow source and click **Use as Template**.
Flow Source Name	Type a name for the flow source. We recommend that for an external flow source that is also a physical device, you use the device name as the flow source name. If the flow source is not a physical device, ensure you use a an appropriate and recognizable name. For example, if you want to use IPFIX traffic, type **`ipf1`**. If you want to use NetFlow traffic, type **`nf1`**.
Target Collector	Using the list box, select the Event Collector you want to use for this flow source.
Flow Source Type	Using the list box, select the flow source type for this flow source. The options are: • Flowlog File • JFlow • Netflow v.1, v5, v7, or v9 • Network Interface • Packeteer FDR • SFlow v.2, v.4, or v.5 • Napatech, if applicable • Endace, if applicable

Table 10-1 Add Flow Source Window Parameters (continued)

Parameter	Description
Enable Asymmetric Flows	In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This is asymmetric routing. Select this check box is you want to enable asymmetric flows for this flow source.
Source File Path	Type the source file path for the flowlog file.

Step 7 Choose one of the following options:

a If you select the **Flowlog File** option in the **Flow Source Type** parameter, configure the **Source File Path**, which is the source path location for the flow log file.

b If you select the **JFlow**, **Netflow**, **Packeteer FDR**, or **sFlow** options in the **Flow Source Type** parameter, configure the following parameters:

Table 10-2 External Flow parameters

Parameter	Description
Monitoring Interface	Using the list box, select the monitoring interface you want to use for this flow source.
Monitoring Port	Type the port you want this flow source to use. For the first NetFlow flow source configured in your network, the default port is 2055. For each additional NetFlow flow source, the default port number increments by 1. For example, the default NetFlow flow source for the second NetFlow flow source is 2056.
Enable Flow Forwarding	Select the check box to enable flow forwarding for this flow source. When you select the check box, the following options are displayed: • **Forwarding Port** - Type the port you want to forward flows. The default is 1025. • **Forwarding Destinations** - Type the destinations you want to forward flows to. You can add or remove addresses from the list using the **Add** and **Remove** icons.

c If you select the **Napatech Interface** option in the **Flow Source Type** parameter, type the Flow Interface you want to assign to this flow source.

NOTE

The Napatech Interface option is only displayed if you have a Napatech Network Adapter installed in your system.

d If you select the **Network Interface** option as the **Flow Source Type** parameter, configure the following parameters:

Table 10-3 Network Interface Parameters

Parameter	Description
Flow Interface	Using the list box, select the log source you want to assign to this flow source. ***Note:*** *You can only configure one log source per Ethernet Interface. Also, you cannot send different flow types to the same port.*
Filter String	Type the filter string for this flow source.

Step 8 Click **Save**.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Editing a Flow Source

To edit a flow source:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

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

Step 5 Select the flow source you want to edit.

Step 6 Click **Edit**.

Step 7 Edit values, as necessary. For more information on values for flow source types, see **Adding a Flow Source**.

Step 8 Click **Save**.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Enabling and Disabling a Flow Source

To enable or disable a flow source:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

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

Step 5 Select the flow source you want to enable or disable.

Step 6 Click **Enable/Disable**.

The **Enabled** column indicates if the flow source is enabled or disabled. If the flow source was previously disabled, the column now indicates True to indicate the flow source is now enabled. If the flow source was previously enabled, the column now indicates False to indicate the flow source is now disabled.

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

Deleting a Flow Source

To delete a flow source:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

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

Step 5 Select the flow source you want to delete.

Step 6 Click **Delete**.

Step 7 Click **OK**.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Managing Flow Source Aliases

You can configure a virtual name (or alias) for flow sources. You can identify multiple sources being sent to the same QRadar QFlow Collector, using the source IP address and virtual name. An alias allows a QRadar QFlow Collector to uniquely identify and process data sources being sent to the same port.

When a QRadar QFlow Collector receives traffic from a device with an IP address but no current alias, the QRadar QFlow Collector attempts a reverse DNS lookup to determine the host name of the device. If the lookup is successful, the QRadar QFlow Collector adds this information to the database and is reported to all QRadar QFlow Collectors in your deployment.

NOTE

Using the deployment editor, you can configure the QRadar QFlow Collector to automatically detect flow source aliases. For more information, see **Managing Flow Sources**.

This section includes the following topics:

- **Adding a Flow Source Alias**
- **Editing a Flow Source Alias**
- **Deleting a Flow Source Alias**

Adding a Flow Source Alias

To add a flow source alias:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

Step 4 Click the **Flow Source Aliases** icon.

Step 5 Click **Add**.

Step 6 Enter values for the parameters:

- **IP** - Type the IP address of the flow source alias.
- **Name** - Type a unique name for the flow source alias.

Step 7 Click **Save**.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Editing a Flow Source Alias

To edit a flow source alias:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

Step 4 Click the **Flow Source Aliases** icon.

Step 5 Select the flow source alias you want to edit.

Step 6 Click **Edit**.

Step 7 Update values, as necessary.

Step 8 Click **Save**.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Deleting a Flow Source Alias

To delete a flow source alias:

Step 1 Click the **Admin** tab.

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

Step 3 On the navigation menu, click **Flows**.

Step 4 Click the **Flow Source Aliases** icon.

Step 5 Select the flow source alias you want to delete.

Step 6 Click **Delete**.

Step 7 Click **OK**.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

11 CONFIGURING REMOTE NETWORKS AND SERVICES

On the **Admin** tab, you can group remote networks and services for use in the custom rules engine, flow and event searches, and in IBM Security QRadar Risk Manager (if available).

This section includes the following topics:

Remote Networks and Services Overview

Remote network and service groups enable you to represent traffic activity on your network for a specific profile. All remote network and service groups have group levels and leaf object levels.

You can edit remote network and service groups by adding objects to existing groups or changing pre-existing properties to suit your environment.

CAUTION

*If you move an existing object to another group (select a new group and click **Add Group**), the object name moves from the existing group to the newly selected group; however, when the configuration changes are deployed, the object data stored in the database is lost and the object ceases to function. We recommend that you create a new view and re-create the object (that exists with another group).*

Managing Remote Networks

Remote networks groups display user traffic originating from named remote networks. After you create remote network groups, you can aggregate flow and event search results on remote network groups, and create rules that test for activity on remote network groups.

This section includes the following topics:

Default Remote Network Groups

QRadar SIEM includes the following default remote network groups:

Table 11-1 Default Remote Network Groups

Group	Description
BOT	Specifies traffic originating from BOT applications.
Bogon	Specifies traffic originating from un-assigned IP addresses. For more information on bogons, see *http://www.team-cymru.org/Services/Bogons/*
HostileNets	Specifies traffic originating from known hostile networks. HostileNets has a set of 20 (rank 1 to 20 inclusive) configurable CIDR ranges.
Neighbours	This group is blank by default. You must configure this group to classify traffic originating from neighboring networks.
Smurfs	Specifies traffic originating from Smurf attacks. A Smurf attack is a type of denial-of-service attack that floods a destination system with spoofed broadcast ping messages.
Superflows	This group is non-configurable. A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.
TrustedNetworks	This group is blank by default. You must configure this group to classify traffic originating from trusted networks.
Watchlists	This group is blank by default. You can configure this group to classify traffic originating from networks you want monitor.

NOTE

Groups and objects that include superflows are for informational purposes only and cannot be edited. Groups and objects that include bogons are configured by the Automatic Update function.

Adding a Remote Networks Object

To add a remote network object:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Remote Networks and Services Configuration.**

Step 3 Click the **Remote Networks** icon.

Step 4 Click **Add**.

Step 5 Enter values for the following parameters:

Table 11-2 Remote Networks - Add New Object Parameters

Parameter	Description
Group	From the list box, select a group for this object or click **Add Group** to add a new group.
Name	Type a unique name for the object.
Weight	Type or select a weight for the object.
IP/CIDR(s)	Type the IP address or CIDR range for the object. Click **Add**.
Description	Type a description for the object.
Database Length	From the list box, select the database length.

Step 6 Click **Save**.

Step 7 Click **Return**.

Step 8 Close the Remote Networks window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

All changes are deployed.

Editing a Remote Networks Object

To edit an existing Remote Networks object:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Remote Networks and Services Configuration.**

Step 3 Click the **Remote Networks** icon.

The Remote Networks window provides the following information in the Manage Group pane.

Table 11-3 Manage Group Pane Parameters

Parameter	Description
Name	Specifies the name assigned to the view.
Actions	Click the **Open** icon to view the properties window.

Step 4 Click the group you want to display.

The Manage Group pane refreshes, displaying a list of objects in the group you selected.

Table 11-4 Manage Group Pane Parameters for Selected Group

Parameter	Description
Name	Specifies the name assigned to the object.
Value(s)	Specifies IP addresses or CIDR ranges assigned to this object.

Table 11-4 Manage Group Pane Parameters for Selected Group (continued)

Parameter	Description
Actions	Specifies the actions available for each object, including: • **Edit** - Click the **Edit** icon to edit object properties. • **Delete** - Click the **Delete** icon to delete object.

Step 5 Click the **Edit** icon.

Step 6 Edit values as necessary. See **Table 11-2**.

Step 7 Click **Save**.

Step 8 Click **Return**.

Step 9 Close the Remote Networks window.

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

All changes are deployed.

Managing Remote Services

Remote services groups organize traffic originating from user-defined network ranges or the IBM automatic update server. After you create remote service groups, you can aggregate flow and event search results, and create rules that test for activity on remote service groups.

This section includes the following topics:

- **Default Remote Service Groups**
- **Adding a Remote Services Object**
- **Editing a Remote Services Object**

Default Remote Service Groups

QRadar SIEM includes the following default remote service groups:

Table 11-5 Default Remote Service Groups

Parameter	Description
IRC_Servers	Specifies traffic originating from addresses commonly known as chat servers.
Online_Services	Specifies traffic originating from addresses commonly known online services that may involve data loss.
Porn	Specifies traffic originating from addresses commonly known to contain explicit pornographic material.
Proxies	Specifies traffic originating from commonly known open proxy servers.
Reserved_IP_ Ranges	Specifies traffic originating from reserved IP address ranges.
Spam	Specifies traffic originating from addresses commonly known to produce SPAM or unwanted email.

Table 11-5 Default Remote Service Groups (continued)

Parameter	Description
Spy_Adware	Specifies traffic originating from addresses commonly known to contain spyware or adware.
Superflows	Specifies traffic originating from addresses commonly known to produce superflows.
Warez	Specifies traffic originating from addresses commonly known to contain pirated software.

Adding a Remote Services Object

To add a Remote Services Object:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Remote Networks and Services Configuration**.

Step 3 Click the **Remote Services** icon.

Step 4 Click **Add**.

Step 5 Enter values for the following parameters:

Table 11-6 Remote Services - Add New Object Parameters

Parameter	Description
Group	From the list box, select a group for the object or click **Add Group** to add a new group.
Name	Type the name for the object.
Weight	Type or select a weight for the object.
IP/CIDR(s)	Type the IP address or CIDR range for the object. Click **Add**.
Description	Type a description for the object.
Database Length	From the list box, select the database length.

Step 6 Click **Save**.

Step 7 Click **Return**.

Step 8 Close the Remote Services window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

All changes are deployed.

Editing a Remote Services Object

To edit an existing Remote Services object:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Remote Networks and Services Configuration.**

Step 3 Click the **Remote Services** icon.

The Remote Services window provides a list of groups in the Manage Group pane.

Table 11-7 Manage Group Parameters

Parameter	Description
Name	Specifies the name assigned to the group.
Actions	Click the **Open** icon to view properties.

Step 4 Click the group you want to display.

The Manage Group pane is refreshed, providing a list of the objects in group you selected.

Table 11-8 Manage Group Parameters

Parameter	Description
Name	Specifies the name assigned to the object.
Value	Specifies ports assigned to this object:
Actions	Specifies the actions available for each object, including: • **Edit** - Click the **Edit** icon to edit the object properties. • **Delete** - Click the **Delete** icon to delete the object.

Step 5 Click the **Edit** icon.

Step 6 Edit values as necessary. See **Table 11-6**.

Step 7 Click **Save**.

Step 8 Click **Return**.

Step 9 Close the Remote Services window.

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

All changes are deployed.

Using Best Practices

Given the complexities and network resources required for QRadar SIEM in large structured networks, we recommend the following best practices:

- Bundle objects and use the **Network Activity** and **Log Activity** tabs to analyze your network data. Fewer objects create less input and output to your disk.
- Typically, no more than 200 objects per group (for standard system requirements). More objects may impact your processing power when investigating your traffic.

12 DISCOVERING SERVERS

The Server Discovery function uses the Asset Profile database to discover different server types based on port definitions, and then allows you to select which servers to add to a server-type building block for rules.

This section includes the following topics:

Server Discovery Overview

This feature makes the discovery and tuning process simpler and faster by providing a quick mechanism to insert servers into building blocks.

The Server Discovery function is based on server-type building blocks. Ports are used to define the server type so that the server-type building block essentially functions as a port-based filter when searching the Asset Profile database.

For more information on building blocks, see the *IBM Security QRadar SIEM User Guide*.

Discovering Servers

To discover servers:

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Server Discovery**.

Step 3 From the **Server Type** list box, select the server type you want to discover.

Step 4 Select the option to determine the servers you want to discover, including:

- **All** - Search all servers in your deployment with the currently selected Server Type.
- **Assigned** - Search servers in your deployment that have been previously assigned to the currently selected Server Type.
- **Unassigned** - Search servers in your deployment that have not been previously assigned.

Step 5 From the **Network** list box, select the network you want to search.

Step 6 Click **Discover Servers**.

The discovered servers are displayed.

Step 7 In the **Matching Servers** table, select the check boxes of all servers you want to assign to the server role.

NOTE

If you want to modify the search criteria, click either **Edit Port** or **Edit Definition**. For more information on the rules wizard, see the *IBM Security QRadar SIEM User Guide*.

Step 8 Click **Approve Selected Servers**.

13 FORWARDING EVENT DATA

You can configure QRadar SIEM to forward event data to one or more vendor systems, such as ticketing or alerting systems.

This section includes the following topics:

Event Forwarding Overview

QRadar SIEM allows you to forward raw log data received from log sources and QRadar SIEM-normalized event data to one or more vendor systems, such as ticketing or alerting systems. On the QRadar SIEM user interface, these vendor systems are called forwarding destinations. QRadar SIEM ensures that all forwarded data is unaltered.

To configure QRadar SIEM to forward events, you must first configure one or more forwarding destinations. Then you can configure routing rules, custom rules, or both to determine what log data you want to forward and what routing options apply to the log data.

For example, you can configure all log data from a specific event collector to forward to a specific vendor ticketing system. You can also choose from various routing options such as removing the log data that matches a routing rule from your QRadar SIEM system and bypassing correlation. Correlation is the process of matching events to rules, which in turn can generate offenses.

Add Forwarding Destinations

Before you can configure bulk or select event forwarding, you must add forwarding destinations on the Forwarding Destinations window.

To add a forwarding destination:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

Step 4 On the toolbar, click **Add**.

Step 5 Enter values for the parameters:

Table 13-1 Forwarding Destinations Parameters

Parameter	Description
Name	Type a unique name for the forwarding destination.
Event Format	From the list box, select an event format. Options include: • **Raw event** - Raw event data is event data in the format that the log source sent. This is the default option. • **Normalized event** - Normalized data is raw event data that QRadar SIEM has parsed and prepared for the display as readable information on the QRadar SIEM user interface. ***Note:*** *Normalized event data cannot transmit using the UDP protocol. If you select the* ***Normalized Event*** *option, the* ***UDP*** *option in the* ***Protocol*** *list box is disabled.*
Destination Address	Type the IP address or host name of the vendor system you want to forward event data to.
Destination Port	Type the port number of the port on the vendor system you want to forward event data to. The default port is 514.

Table 13-1 Forwarding Destinations Parameters (continued)

Parameter	Description
Protocol	Using the list box, select the protocol you want to use to forward event data. Choices include: • **TCP** - Transmission Control Protocol. To send normalized event data using the TCP protocol, you must create an off-site source at the destination address on port 32004. For more information on creating off-site sources, see **Using the Deployment Editor**. • **UDP** - User Datagram Protocol Normalized event data cannot transmit using the UDP protocol. If you select the UDP option, the **Normalized Event** option in the **Event Format** list box is disabled. The default protocol is TCP.
Prefix a syslog header if it is missing or invalid	When QRadar SIEM forwards syslog messages, the outbound message is verified to ensure it has a proper syslog header. ▶ Select this check box to prefix a syslog header if a header is not detected on the original syslog message. The prefixed syslog header includes the QRadar SIEM appliance host name in the **Hostname** field of the syslog header. If this check box is clear, the syslog message is sent unmodified.

Step 6 Click **Save**.

The forwarding destination you added is now displayed on the Forwarding Destinations window. The forwarding destination is enabled by default and is available for you to include in routing rules and custom rules. For more information on managing forwarding destinations, see **Managing Forwarding Destinations**.

Configuring Bulk Event Forwarding

After you have added one or more forwarding destinations, you can create filter-based routing rules to allow QRadar SIEM to forward large quantities of event data.

To configure bulk event forwarding:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Routing Rules** icon.

Step 4 On the toolbar, click **Add**.

Step 5 Enter values for the parameters:

Table 13-2 Event Routing Rules Parameters

Parameter	Description
Name	Type a unique name for the routing rule.
Description	Type a description for the routing rule.
Forwarding Event Collector	From the list box, select the event collector you want to forward events from.
Current Filters	
Match All Incoming Events	Select this check box to specify that you want this rule to forward all incoming events. If you select this option, the **Add Filter** functionality is no longer displayed.
Add Filter	Using the options in the Current Filters pane, configure your filters: **1** From the first list box, select a property you want to filter for. Options include all normalized and custom event properties. **2** From the second list box, select an operator. Choices include **Equals** and **Equals any of**. **3** In the text box, type the value you want to filter for. **4** Click **Add Filter**. **5** Repeat for each filter you want to add.
Routing Options	
Forward	Select this check box to forward log data that matches the current filters, and then select the check box for each forwarding destination that forward log data to. If you select the **Forward** check box, you can also select either the **Drop** or **Bypass Correlation** check boxes, but not both of them. If you want to edit, add, or delete a forwarding destination, click the **Manage Destinations** link. For more information, see **Managing Forwarding Destinations**.
Drop	Select this check box if you to remove the log data that matches the current filters from the QRadar SIEM database. ***Note:*** *If you select the* ***Drop*** *check box, the* ***Bypass Correlation*** *check box is automatically cleared.*

Table 13-2 Event Routing Rules Parameters (continued)

Parameter	Description
Bypass Correlation	Select this check box if you want the log data that matches the current filters to bypass correlation. When correlation is bypassed, the log data that matches the current filter is stored in the QRadar SIEM database, but it is not tested in the CRE. ***Note:*** *If you select the* ***Bypass Correlation*** *check box, the* ***Drop*** *check box is automatically cleared.*

Step 6 Click **Save**.

The routing rule is now displayed on the Event Routing Rules window. The routing rule is enabled by default and automatically starts processing events for bulk forwarding. For more information on managing routing rules, see **Managing Routing Rules**.

Configuring Selective Event Forwarding

Using the Custom Rule Wizard, you can configure rules to forward event data to one or more forwarding destinations as a rule response. The criteria for what data gets forwarded to a forwarding destination is based on the tests and building blocks included in the rule. This method provides you a means to configure highly selective event forwarding.

To configure selective event forwarding:

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, select **Rules**.

Step 3 Edit or add a rule, ensuring that you select the **Send to Forwarding Destinations** option on the Rule Response page in the Rule Wizard. For more information on how to edit or add a rule, see the *IBM Security QRadar SIEM Users Guide*.

When the rule is configured and enabled, all events matching the rule tests are automatically forwarded to the specified forwarding destinations.

Managing Forwarding Destinations

This section includes the following topics:

- **Viewing Forwarding Destinations**
- **Editing a Forwarding Destination**
- **Delete a Forwarding Destination**

Viewing Forwarding Destinations

The Forwarding Destinations window provides valuable information on your forwarding destinations, including statistics for the data sent to each forwarding destination.

To view your forwarding destinations:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

The Forwarding Destinations window provides the following information:

Table 13-3 Forwarding Destination Window Parameters

Parameter	Description
Name	Specifies the name of this forwarding destination.
Event Format	Specifies whether raw event data or normalized event data is sent to this forwarding destination.
Host / IP Address	Specifies the IP address or host name of this forwarding destination host.
Port	Specifies the receiving port on this forwarding destination host.
Protocol	Specifies whether the protocol for this forwarding event data is TCP or UDP.
Seen	Specifies how many total number events were seen for this forwarding destination.
Sent	Specifies how many events have actually been sent to this forwarding destination.
Dropped	Specifies how many events have been dropped before reaching this forwarding destination.
Enabled	Specifies whether this forwarding destination is enabled or disabled. For more information, see **Enabling and Disabling a Forwarding Destination**.
Creation Date	Specifies the date that this forwarding destination was created.
Modification Date	Specifies the date that this forwarding destination was last modified.

The Forwarding Destinations window toolbar provides the following functions:

Table 13-4 Forwarding Destinations Window Toolbar

Function	Description
Add	Click **Add** to add a new forwarding destination. See **Add Forwarding Destinations**.
Edit	Click **Edit** to edit a selected forwarding destination. See **Editing a Forwarding Destination**.

Table 13-4 Forwarding Destinations Window Toolbar (continued)

Function	Description
Enable/Disable	Click **Enable/Disable** to enable or disable a selected forwarding destination. For more information, see **Enabling and Disabling a Forwarding Destination**.
Delete	Click **Delete** to delete a selected forwarding destination. See **Delete a Forwarding Destination**.
Reset Counters	Click **Reset Counters** to reset the **Seen**, **Sent**, and **Dropped** parameters for all forwarding destinations back to zero (0). See **Resetting the Counters**.

Enabling and Disabling a Forwarding Destination

When you create a forwarding destination, it is enabled by default. Using the **Enable/Disable** icon, you can toggle the forwarding destination on or off.

To enable or disable a forwarding destination:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to enable or disable.

Step 5 On the toolbar, click **Enable/Disable**.

Depending on the current status of the forwarding destination, the result of clicking **Enable/Disable** is as follows:

- If the **Enabled** status is **False**, the forwarding destination is now enabled.
- If the **Enabled** status is **True**, a confirmation message is displayed. A confirmation message is displayed, providing a list of associated rules. Click **OK** to confirm you want to disable the forwarding destination.

Resetting the Counters

The **Seen**, **Sent**, and **Dropped** parameters provide counts that continue to accumulate until you reset the counters. You may want to reset the counters to provide a more targeted view of how your forwarding destinations are performing.

To reset the counters:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

Step 4 On the toolbar, click **Reset Counters**.

The **Seen**, **Sent**, and **Dropped** parameters display a value of zero (0), until the counters start accumulating again.

Editing a Forwarding Destination

You can edit a forwarding destination to change the configured name, format, IP address, port, or protocol.

To edit a forwarding destination:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters, as necessary. See **Table 13-1**.

Step 7 Click **Save**.

Delete a Forwarding Destination

You can delete a forwarding destination. If the forwarding destination is associated with any active rules, you must confirm that you want to delete the forwarding destination.

To delete a forwarding destination:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

Managing Routing Rules

This section includes the following topics:

- **Viewing Routing Rules**
- **Enabling or Disabling a Routing Rule**
- **Deleting a Routing Rule**

Viewing Routing Rules

The Event Routing Rules window provides valuable information on your routing rules, such as the configured filters and actions that are performed when event data matches each rule.

To view your routing rules:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Routing Rules** icon.

The Event Routing Rules window provides the following information:

Table 13-5 Event Routing Rules Window Parameters

Parameter	Description
Name	Specifies the name of this routing rule.
Event Collector	Specifies the Event Collector you want this routing rule process data from.
Filters	Specifies the configured filters for this routing rule.
Routing Options	Specifies the configured routing options for this routing rule. Options include: • **Forward** - Event data is forwarded to the specified forwarding destination. Event data is also stored in the QRadar SIEM database and processed by the Custom Rules Engine (CRE). • **Forward & Drop** - Event data is forwarded to the specified forwarding destination. Event data is not stored in the QRadar SIEM database, but it is processed by the CRE. • **Forward & Bypass** - Event data is forwarded to the specified forwarding destination. Event data is also stored in the QRadar SIEM database, but it is not processed by the CRE. • **Drop** - Event data is not stored in the QRadar SIEM database. The event data is not forwarded to a forwarding destination, but it is processed by the CRE. • **Bypass** - Event data is not processed by the CRE, but it is stored in the QRadar SIEM database. The event data is not forwarded to a forwarding destination.
Enabled	Specifies whether this routing rule is enabled or disabled.
Creation Date	Specifies the date that this routing rule was created.
Modification Date	Specifies the date that this routing rule was modified.

The Event Routing Rules window toolbar provides the following functions:

Table 13-6 Event Routing Rules Window Toolbar

Function	Description
Add	Click **Add** to add a new routing rule. See **Configuring Bulk Event Forwarding**.
Edit	Click **Edit** to edit a selected routing rule. See **Editing a Routing Rule**.
Enable/Disable	Click **Enable/Disable** to enable or disable a selected routing rule. See **Enabling or Disabling a Routing Rule**.
Delete	Click **Delete** to delete a selected routing rule. For more information, see **Deleting a Routing Rule**.

Editing a Routing Rule

You can edit a routing rule to change the configured name, Event Collector, filters, or routing options.

To edit a routing rule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Routing Rules** icon.

Step 4 Select the routing rule you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters, as necessary. See **Table 13-5**.

Step 7 Click **Save**.

Enabling or Disabling a Routing Rule

When you first create a routing rule, it is enabled by default. Using the **Enable/Disable** icon, you can toggle the routing rule on or off. To enable or disable a routing rule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Routing Rules** icon.

Step 4 Select the routing rule you want to enable or disable.

Step 5 On the toolbar, click **Enable/Disable**.

Depending on the current status of the routing rule, the result of clicking **Enable/Disable** is as follows:

- If the **Enabled** status is **True**, the routing rule is disabled.
- If the **Enabled** status is **False** and the routing rule is configured to drop events, a confirmation message is displayed. Click **OK**.

Deleting a Routing Rule

You can delete a routing rule. You are required to confirm that you want to delete the routing rule.

To delete a routing rule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Routing Rules** icon.

Step 4 Select the routing rule you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

14 STORING AND FORWARDING EVENTS

The Store and Forward feature allows you to manage schedules that control when to start and stop forwarding events from your dedicated Event Collector appliances to Event Processors in your deployment.

This section includes the following topics:

Store and Forward Overview

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590 appliances. For more information on these appliances, see the *QRadar Hardware Guide*.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect using the Deployment Editor. The Store and Forward feature allows you to schedule a time range for when you want the Event Collector to forward events. During the period of time when events are not forwarding, the events are stored locally on the appliance and are not accessible using the Console user interface.

This scheduling feature allows you to store events during your business hours and then forward the events to an Event Processor during periods of time when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to only forward events to an Event Processor during non-business hours, such as midnight until 6 AM.

Viewing the Store and Forward Schedule List

The Store and Forward window provides a list of schedules that includes statistics to help you evaluate the status, performance, and progress of your schedules.

NOTE

By default, no schedules are listed the first time you access the Store and Forward window. For more information on adding a schedule, see **Creating a New Store and Forward Schedule**.

You can use options on the toolbar and the **Display** list box to change your view of the schedule list. Changing your view of the list allows you to focus on the statistics from various points of view. For example, if you want to view the statistics for a particular Event Collector, you can select **Event Collectors** from the **Display** list box. The list then groups by the **Event Collector** column and makes it easier for you to locate the Event Collector you want to investigate.

To view the schedule list:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Store and Forward** icon.

By default, the Store and Forward list is configured to display the list organized by the schedule (**Display > Schedules**) and provides the following information:

Table 14-1 Store and Forward Window Parameters

Parameter	Description
Display	From the **Display** list box, select one of the following options: • **Schedules** - When you select **Schedules** from the **Display** list box, the list displays a hierarchy tree that shows the parent-child relationship between the Schedules, Event Processors, and the associated Event Collectors. • **Event Collectors** - When you select **Event Collectors** from the **Display** list box, the list displays the lowest level in the hierarchy, which is a list of Event Collectors. Therefore, the list does not display a hierarchy tree. • **Event Processors** - When you select **Event Processors** from the **Display** list box, the list displays a hierarchy tree that shows the parent-child relationship between the Event Processors and the associated Event Collectors.

Table 14-1 Store and Forward Window Parameters (continued)

Parameter	Description
Name	Displays the name of the schedule, Event Collector, or Event Processor, depending on the level of the hierarchy tree. When you select **Schedules** from the **Display** list box, the values in the **Name** column are displayed as follows. • **First Level** - Displays the name of the schedule. • **Second Level** - Displays the name of the Event Processor. • **Third Level** - Displays the name of the Event Collector. When you select **Event Processors** from the **Display** list box, the values in the **Name** column are displayed as follows: • **First Level** - Displays the name of the Event Processor. • **Second Level** - Displays the name of the Event Collector. ***Note:*** *This parameter is displayed only when you select* ***Schedules*** *or* ***Event Processors*** *from the* ***Display*** *list box.* You can use the plus symbol (+) and minus symbol (-) beside the name or options on the toolbar to expand and collapse the hierarchy tree. You can also expand and collapse the hierarchy tree using options on the toolbar. See **Table 14-2**.
Schedule Name	Displays the name of the schedule. ***Note:*** *This parameter is displayed only when you select* ***Event Collectors*** *or* ***Event Processors*** *from the* ***Display*** *list box.* If an Event Processor is associated with more than one schedule, the **Schedule Name** parameter displays the following text: `Multiple(n)`, where `n` is the number of schedules. You can click the plus symbol (+) to view the associated schedules.
Event Collector	Displays the name of the Event Collector. ***Note:*** *This parameter is displayed only when you select* ***Event Collectors*** *from the* ***Display*** *list box.*
Event Processor	Displays the name of the Event Processor. ***Note:*** *This parameter is displayed only when you select* ***Event Collectors*** *or* ***Event Processors*** *from the* ***Display*** *list box.*

Table 14-1 Store and Forward Window Parameters (continued)

Parameter	Description
Last Status	Displays the status of the Store and Forward process. Statuses include: • **Forwarding** - Indicates that event forwarding is in progress. • **Forward Complete** - Indicates that event forwarding has successfully completed and events are currently being stored locally on the Event Collector. The stored events will be forwarded when the schedule indicates that forwarding can start again. • **Warn** - Indicates that the percentage of events remaining in storage exceeds the percentage of time remaining in the Store and Forward schedule. • **Error** - Indicates that event forwarding ceased before all stored events were forwarded. • **Inactive** - Indicates that this schedule is inactive, because no Event Collectors are assigned to it or the assigned Event Collectors are not receiving any events. You can move your mouse pointer over the **Last Status** column to view a summary of the status. The summary includes the following information: • **Total Events to be Transferred** - Displays the total number of events that were stored during the period of time between the configured **Forward End** and the **Forward Start** times. • **Number of Events Transferred** - Displays the number of events successfully forwarded. • **Events Remaining** - Displays the number of events remaining to be transferred. • **Percentage Transferred** - Displays the percentage of events successfully forwarded.
	• **Forward Start** - Displays the actual time that forwarding started. The time is displayed in the following format: `yyyy-mm-dd hh:mm:ss`. • **Forward Last Update** - Displays the time when the status was last updated. The time is displayed in the following format: `yyyy-mm-dd hh:mm:ss`. • **Forwarding Time Remaining** - Displays the amount of time remaining in the Store and Forward schedule.
Percent Complete	Displays the percentage of events forwarded during the current session.
Forwarded Events	Displays the number of events (in K, M, or G) forwarded in the current session. You can move your mouse pointer over the value in the **Forwarded Events** column to view the actual number of events.

Table 14-1 Store and Forward Window Parameters (continued)

Parameter	Description
Remaining Events	Displays the number of events (in K, M, or G) remaining to be forwarded in the current session. You can move your mouse pointer over the value in the **Remaining Events** column to view the actual number of events.
Time Elapsed	Displays the amount of time that has elapsed since the current forwarding session started.
Time Remaining	Displays the amount of time remaining in the current forwarding session.
Average Event Rate	Displays the average Event Per Second (EPS) rate during this session. The EPS rate is the rate at which events are forwarding from the Event Collector to the Event Processor. You can move your mouse pointer over the value in the **Average Event Rate** column to view the actual average EPS.
Current Event Rate	Displays the current Event Per Second (EPS) rate during this session. The EPS rate is the rate at which events are forwarding from the Event Collector to the Event Processor. You can move your mouse pointer over the value in the **Current Event Rate** column to view the actual current EPS.
Forward Schedule	Displays the time at which events are scheduled to start forwarding.
Transfer Rate Limit	Displays the rate at which events are forwarding. The transfer rate limit is configurable. The transfer rate limit can be configured to display in Kilobits per second (Kps), Megabits per second (Mps), or Gigabits per second (Gps). To edit the transfer rate limit, see **Editing a Store and Forward Schedule**.
Owner	Displays the user name that created this schedule.
Creation Date	Displays the date when this schedule was created.
Last Modified	Displays the date when this schedule was last edited.

The toolbar provides the following options:

Table 14-2 Store and Forward - Schedules Window Parameters

Option	Description
Actions	Click **Actions** to perform the following actions: • **Create** - Click this option to create a new schedule. See **Creating a New Store and Forward Schedule**. • **Edit** - Click this option to edit an existing schedule. See **Editing a Store and Forward Schedule**. • **Delete** - Click this option to delete a schedule. See **Deleting a Store and Forward Schedule**.
Expand All	Click **Expand All** to expand the list to display all levels in the hierarchy tree, including the schedule, Event Processor, and Event Collector levels.

Table 14-2 Store and Forward - Schedules Window Parameters (continued)

Option	Description
Collapse All	Click **Collapse All** to display only the first level of the hierarchy tree.
Search Schedules	Type your search criteria in the **Search Schedules** field and click the **Search Schedules** icon or press Enter on your keyboard. The list updates to display search results based on which option is selected in the **Display** list box: • **Schedules** - When you select **Schedules** from the **Display** list box, schedules that match your search criteria are displayed in the list. • **Event Collectors** - When you select **Event Collectors** from the **Display** list box, Event Collectors that match your search criteria are displayed in the list. • **Event Processors** - When you select **Event Processors** from the **Display** list box, Event Processors that match your search criteria are displayed in the list.
Last Refresh	Indicates the amount of time that has elapsed since this window was refreshed.
Pause	Click the **Pause** icon to pause the timer on the Store and Forward window. Click the **Play** icon to restart the timer.
Refresh	Click the **Refresh** icon to refresh the Store and Forward window.

Creating a New Store and Forward Schedule

The Store and Forward Schedule Wizard allows you to create a schedule that controls when your Event Collector starts and stops forwarding data to an Event Processor for event processing. You can create and manage multiple schedules to control event forwarding from multiple Event Collectors in a geographically distributed deployment.

The connection between an Event Collector and an Event Processor is configured in the Deployment Editor. Before you can create a new schedule, you must ensure that your dedicated Event Collector is added to your deployment and connected to an Event Processor. For more information on adding and connecting an Event Processor to your deployment, see **Building Your Event View**.

To create a new schedule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Store and Forward** icon.

Step 4 From the **Actions** menu, select **Create**.

Step 5 Click **Next** to move to the Select Collectors page.

Step 6 On the Select Collectors page, configure the following parameters:

Table 14-3 Store and Forward Schedule Wizard - Select Collectors Page Parameters

Parameter	Description
Schedule Name	Type a unique name for the schedule. You can type a maximum of 255 characters.
Available Event Collectors	Select one or more Event Collectors from the **Available Event Collectors** list and click the Add Event Collector (>) icon. When you add an Event Collector, the Event Collector is displayed in the **Selected Event Collectors** list. ***Note:*** *You can filter the* ***Available Event Collectors*** *list by typing a keyword in the* ***Type to filter*** *field.* If the Event Collector you want to configure is not listed, the Event Collector may not have been added to your deployment. If this occurs, you need to access the Deployment Editor to add the Event Collector before you proceed. See **Using the Deployment Editor**.
Selected Event Collectors	Displays a list of selected Event Collectors. You can remove Event Collectors from this list. To remove an Event Collector from the **Selected Event Collectors** list: ▶ Select the Event Collector from the **Selected Event Collectors** list and click the Remove Event Collector (<) icon. ***Note:*** *You can filter the* ***Selected Event Collectors*** *list by typing a keyword in the* ***Type to filter*** *field.* When you remove an Event Collector from the **Selected Event Collectors** list, the removed Event Collector is displayed in the **Available Event Collectors** list.

Step 7 Click **Next** to move to the Schedule Options page.

Step 8 On the Schedule Options page, configure the following parameters:

Table 14-4 Store and Forward Schedule Wizard - Schedule Options Page Parameters

Parameter	Description
Forward Transfer Rate (0 for unlimited)	Configure the forward transfer rate you want this schedule to use when forwarding events from the Event Collector to the Event Processor. To configure the forward transfer rate: **1** From the first list box, type or select a number. The minimum transfer rate is 0. The maximum transfer rate is 9,999,999. A value of 0 means that the transfer rate is unlimited. **2** From the second list box, select a unit of measurement. Options include: Kilobits per second, Megabits per second, and Gigabits per second.
Scheduling Information	Select this check box to display the following scheduling options: • Forward Time Zone • Forward Start • Forward End
Forward Time Zone	From this list box, select your time zone. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.*
Forward Start	Configure what time you want event forwarding to start: **1** From the first list box, select the hour of the day when you want to start forwarding events. **2** From the second list box, select AM or PM. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.* ***Note:*** *If the* ***Forward Start*** *and* ***Forward End*** *parameters specify the same time, events are always forwarded. For example, if you configure a schedule to forward events from 1 AM to 1 AM, event forwarding does not cease.*

Table 14-4 Store and Forward Schedule Wizard - Schedule Options Page Parameters

Parameter	Description
Forward End	Configure what time you want event forwarding to end: **1** From the first list box, select the hour of the day when you want to stop forwarding events. **2** From the second list box, select AM or PM. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.* ***Note:*** *If the* ***Forward Start*** *and* ***Forward End*** *parameters specify the same time, events are always forwarded. For example, if you configure a schedule to forward events from 1 AM to 1 AM, event forwarding does not cease.*

Step 9 Click **Next** to move to the Summary page.

Step 10 On the Summary page, confirm the options you configured for this Store and Forward schedule.

Step 11 Click **Finish**.

Your Store and Forward schedule is saved and you can now view the schedule in the Store and Forward window. After you create a new schedule, it may take up to 10 minutes for statistics to start displaying in the Store and Forward window. For more information on viewing the Store and Forward window, see **Viewing the Store and Forward Schedule List**.

Editing a Store and Forward Schedule

You can edit a Store and Forward schedule to add or remove Event Collectors and change the schedule parameters. After you edit a Store and Forward schedule, the schedule's statistics displayed in the Store and Forward list are reset.

To edit a schedule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Store and Forward** icon.

Step 4 Select the schedule you want to edit.

Step 5 From the **Actions** menu, select **Edit**.

NOTE You can also double-click a schedule for editing.

Step 6 Click **Next** to move to the Select Collectors page.

Step 7 On the Select Collectors page, edit the parameters. For more information on the Select Collectors page parameters, see **Table 14-3**.

Step 8 Click **Next** to move to the Schedule Options page.

Step 9 On the Schedule Options page, edit the scheduling parameters. For more information on the Schedule Options page parameters, see **Table 14-4**.

Step 10 Click **Next** to move to the Summary page.

Step 11 On the Summary page, confirm the options you edited for this schedule.

Step 12 Click **Finish**.

The Store and Forward Schedule Wizard closes. Your edited schedule is saved and you can now view the updated schedule in the Store and Forward window. After you edit a schedule, it may take up to 10 minutes for statistics to update in the Store and Forward window. For more information on the Store and Forward window, see **Viewing the Store and Forward Schedule List**.

Deleting a Store and Forward Schedule

You can delete a Store and Forward schedule. After you delete a schedule, the associated Event Collectors continuously forward events to the Event Processor.

To edit a schedule:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **Store and Forward** icon.

Step 4 Select the schedule you want to delete.

Step 5 From the **Actions** menu, select **Delete**.

The deleted schedule is removed from the Store and Forward window. After the schedule is deleted, the associated Event Collectors resume continuous forwarding of events to their assigned Event Processor.

A ENTERPRISE TEMPLATE

The Enterprise template includes settings with emphasis on internal network activities.

This section includes the following topics:

Default Rules

Default rules for the Enterprise template include:

Table 15-1 Default Rules

Rule	Group	Rule Type	Enabled	Description
Anomaly: Devices with High Event Rates	Anomaly	Event	False	Monitors devices for high event rates. Typically, the default threshold is low for most networks and we recommend that you adjust this value before enabling this rule. To configure which devices will be monitored, edit the BB:DeviceDefinition: Devices to Monitor for High Event Rates BB.
Anomaly: DMZ Jumping	Anomaly	Common	False	Reports when connections are bridged across your Demilitarized Zone (DMZ).
Anomaly: DMZ Reverse Tunnel	Anomaly	Common	False	Reports when connections are bridged across your DMZ through a reverse tunnel.
Anomaly: Excessive Database Connections	Anomaly	Event	True	Reports an excessive number of successful database connections.
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Anomaly	Event	False	Reports excessive firewall accepts across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.
Anomaly: Excessive Firewall Accepts Across Multiple Sources to a Single Destination	Anomaly	Event	False	Reports excessive firewall accepts from multiple hosts to a single destination. Detects more than 100 firewall accepts across more than 100 sources IP addresses within 5 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Anomaly: Excessive Firewall Denies from Single Source	Anomaly	Event	True	Reports excessive firewall denies from a single host. Detects more than 400 firewall deny attempts from a single source to a single destination within 5 minutes.
Anomaly: Long Duration Flow Involving a Remote Host	Anomaly	Flow	True	Reports a flow communicating to or from the Internet with a sustained duration of more than 48 hours.
Anomaly: Long Duration ICMP Flows	Anomaly	Flow	False	Reports a flow communicating using ICMP with a sustained duration of more than 60 minutes.
Anomaly: Outbound Connection to a Foreign Country	Anomaly	Event	False	Reports successful logins or access from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries with no Remote Access BB.
Anomaly: Potential Honeypot Access	Anomaly	Event	False	Reports an event that has a source or destination IP address defined as a honeypot or tarpit address. Before enabling this rule, you must configure the BB:HostDefinition: Honeypot like addresses BB.
Anomaly: Remote Access from Foreign Country	Anomaly	Event	False	Reports successful logins or access from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries with no Remote Access BB.
Anomaly: Remote Inbound Communication from a Foreign Country	Anomaly	Flow	False	Reports a flow communicating from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries with no Remote Access BB.
Anomaly: Single IP with Multiple MAC Addresses	Anomaly	Event	False	Reports when the MAC address of a single IP address changes multiple times over a period of time.
Authentication: Login Failure to Disabled Account	Authentication	Event	False	Reports a host login failure message from a disabled user account. If the user is no longer a member of your organization, we recommend that you investigate other received authentication messages from the same user.
Authentication: Login Failure to Expired Account	Authentication	Event	False	Reports a host login failure message from an expired user account known. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages from the same user.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Authentication: Login Failures Followed By Success to the same Destination IP	Authentication	Event	True	Reports multiple login failures to a single destination IP address, followed by a successful login to the destination IP address.
Authentication: Login Failures Followed By Success From Single Source IP	Authentication	Event	True	Reports multiple login failures from a single source IP address, followed by a successful login.
Authentication: Login Failures Followed By Success to the same Username	Authentication	Event	True	Reports multiple login failures followed by a successful login from the same user.
Authentication: Login Successful After Scan Attempt	Authentication	Common	True	Reports a successful login to a host after reconnaissance has been detected on this network.
Authentication: Multiple Login Failures for Single Username	Authentication	Event	True	Reports authentication failures for the same user name.
Authentication: Multiple Login Failures from the Same Source	Authentication	Event	True	Reports authentication failures from the same source IP address to more than three destination IP address more than ten times within 5 minutes.
Authentication: Multiple Login Failures to the Same Destination	Authentication	Event	True	Reports authentication failures to the same destination IP address from more than ten source IP addresses more than ten times within 10 minutes.
Authentication: Multiple VoIP Login Failures	Authentication	Event	False	Reports multiple login failures to a VoIP PBX host.
Authentication: No Activity for 60 Days	Authentication	Event	False	Reports when the configured users have not logged in to the host for over 60 days
Authentication: Possible Shared Accounts	Authentication	Event	False	Reports when an account is shared. We recommend that you add system accounts, such as root and admin to the following negative test: and NOT when the event user name matches the following.
Authentication: Repeat Non-Windows Login Failures	Authentication	Event	False	Reports when a source IP address causes an authentication failure event at least seven times to a single destination IP address within 5 minutes.
Authentication: Repeat Windows Login Failures	Authentication	Event	False	Reports when a source IP address causes an authentication failure event at least nine times to a single Windows host within 1 minute.
Botnet: Local Host on Botnet CandC List (SRC)	Botnet	Common	True	Reports when a source IP address is a member of a known Botnet CandC host.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Botnet: Local host on Botnet CandC List (DST)	Botnet	Common	True	Reports when a local destination IP address is a member of a known Botnet CandC host.
Botnet: Potential Botnet Connection (DNS)	Botnet	Common	False	Reports a host connecting or attempting to connect to a DNS server on the Internet. This may indicate a host connecting to a Botnet.
Botnet: Potential Botnet Events Become Offenses	Botnet	Event	True	Enable this rule if you want all events categorized as exploits to create an offense.
Botnet: Potential connection to known Botnet CandC	Botnet	Common	True	Reports when a potential connection to a know BotNet CandC host is detected. To reduce false positive offenses, connections on ports 25 and 53 are removed from the rule.
Botnet: Successful Inbound Connection from a Known Botnet CandC	Botnet	Common	True	Reports when a successful inbound connection from a BotNet CandC host in detected.
Policy: Remote: IRC Connections	Botnet, Policy	Common	True	Reports a local host issuing an excessive number of IRC connections to the Internet.
Compliance: Auditing Services Stopped on Compliance Host	Compliance	Event	False	Reports when auditing services are stopped on a compliance host. Before enabling this rule, define the hosts in the compliance definition BBs and verify that the events for the audit service stopped for your host are in the BB: CategoryDefinition: Auditing Stopped building block.
Compliance: Compliance Events Become Offenses	Compliance	Event	False	Reports compliance-based events, such as clear text passwords.
Compliance: Configuration Change Made to Device in Compliance network	Compliance	Event	False	Reports configuration change made to device in compliance network. Before you enable this rule, edit the device list to include the devices you want reported.
Compliance: Excessive Failed Logins to Compliance IS	Compliance	Event	False	Reports excessive authentication failures to a compliance server within 10 minutes.
Compliance: Multiple Failed Logins to a Compliance Asset	Compliance	Event	False	Reports multiple failed logins to a compliance asset.
Compliance: Traffic from DMZ to Internal Network	Compliance	Common	True	Reports traffic from the DMZ to an internal network. This is typically not allowed under compliance regulations. Before enabling this rule, make sure the DMZ object is defined in your network hierarchy.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Compliance: Traffic from Untrusted Network to Trusted Network	Compliance	Common	True	Reports traffic from an untrusted network to a trusted network. Before enabling this rule, edit the following BBs: BB:NetworkDefinition: Untrusted Network Segment and BB:NetworkDefinition: Trusted Network Segment.
Database: Attempted Configuration Modification by a remote host	Compliance	Event	True	Reports when a configuration modification is attempted to a database server from a remote network.
Database: Concurrent Logins from Multiple Locations	Compliance	Event	True	Reports when several authentications to a database server occur across multiple remote IP addresses.
Vulnerabilities: Vulnerability Reported by Scanner	Compliance	Event	False	Reports when a vulnerability is discovered on a local host.
Database: Attempted Configuration Modification by a remote host	Database	Event	True	Reports when a configuration modification is attempted to a database server from a remote network.
Database: Concurrent Logins from Multiple Locations	Database	Event	True	Reports when multiple remote IP addresses concurrently login to a database server.
Database: Failures Followed by User Changes	Database	Event	True	Reports when login failures are followed by the addition or change of a user account.
Database: Groups changed from Remote Host	Database	Event	True	Monitors changes to groups on a database when the change is initiated from a remote network.
Database: Multiple Database Failures Followed by Success	Database	Event	True	Reports when there are multiple database failures followed by a success within a short period of time.
Database: Remote Login Failure	Database	Event	True	Reports when a login failure from a remote source IP address to a database server is detected.
Database: Remote Login Success	Database	Event	True	Reports when a successful authentication occurs to a database server from a remote network.
Database: User Rights Changed from Remote Host	Database	Event	True	Reports when changes to database user privileges are made from a remote network.
DDoS: DDoS Attack Detected	D\DoS	Event	True	Reports network Distributed Denial of Service (DDoS) attacks on a system.
DDoS: DDoS Events with High Magnitude Become Offenses	D\DoS	Event	True	Reports when offenses are created for DoS-based events with high magnitude.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
DDoS: Potential DDoS Against Single Host (ICMP)	D\DoS	Flow	False	Reports when more than 500 hosts send packets to a single destination using ICMP in one minute and there is no response.
DDoS: Potential DDoS Against Single Host (Other)	D\DoS	Flow	False	Reports when more than 500 hosts send packets to a single destination using IPSec or an uncommon protocol in one minute and there is no response.
DDoS: Potential DDoS Against Single Host (TCP)	D\DoS	Flow	True	Reports when more than 500 hosts send packets to a single destination using TCP in one minute and there is no response.
DDoS: Potential DDoS Against Single Host (UDP)	D\DoS	Flow	False	Detects when more than 500 hosts send packets to a single destination using UPD in one minute and there is no response.
DoS: DoS Events from Darknet	D/DoS	Event	False	Reports when DoS attack events are identified on Darknet network ranges.
DoS: DoS Events with High Magnitude Become Offenses	D\DoS	Event	True	Rule forces the creation of an offense for DoS based events with a high magnitude.
DoS: Local Flood (ICMP)	D\DoS	Flow	False	Reports when a single local host sends more than three flows containing 60,000 packets to an Internet destination using ICMP in 5 minutes.
DoS: Local Flood (Other)	D\DoS	Flow	False	Reports when a single local host sends more than three flows containing 60,000 packets to an Internet destination using IPSec or an uncommon protocol in 5 minutes.
DoS: Local Flood (TCP)	D\DoS	Flow	True	Reports when a single local host sends more than 60,000 packets at a packet rate of 1,000 packets per second to an Internet destination using TCP.
DoS: Local Flood (UDP)	D\DoS	Flow	False	Reports when a single local host sends more than three flows containing 60,000 packets to an Internet destination using UDP in 5 minutes.
DoS: Network DoS Attack Detected	D\DoS	Event	True	Reports network Denial of Service (DoS) attacks on a system.
DoS: Remote Flood (ICMP)	D\DoS	Flow	False	Reports when a single host on the Internet containing than 60,000 packets to an Internet destination using ICMP in 5 minutes.
DoS: Remote Flood (Other)	D\DoS	Flow	False	Reports when a single host on the Internet sends more than three flows containing 60,000 packets to an Internet destination using IPSec or an uncommon protocol in 5 minutes.
DoS: Remote Flood (TCP)	D\DoS	Flow	False	Reports when a single host on the Internet sends more than three flows containing than 60,000 packets to an Internet destination using TCP in 5 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
DoS: Remote Flood (UDP)	D\DoS	Flow	False	Reports when a single host on the Internet sends more than three flows containing 60,000 packets to an Internet destination using UDP in 5 minutes.
DoS: Service DoS Attack Detected	D\DoS	Event	True	Reports a DoS attack against a local destination IP address that is known to exist and the target port is open.
Botnet: Potential Botnet Connection (DNS)	Exploit	Common	False	Reports a host connecting or attempting to connect to a DNS server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code. Before you enable this rule, configure the BB:HostDefinition: DNS Servers BB. ***Note:*** *Notebooks that include wireless adapters may cause this rule to generate alerts since the laptops may attempt to communicate with another IDPs DNS server. If this occurs, define the ISPs DNS server in the BB:HostDefinition: DNS Servers BB.*
Exploit:All Exploits Become Offenses	Exploit	Event	False	Reports all exploit events. By default, this rule is disabled. Enable this rule if you want all events categorized as exploits to create an offense.
Exploit: Attack followed by Attack Response	Exploit	Event	False	Reports when exploit events are followed by typical responses, which may indicate a successful exploit.
Exploit: Chained Exploit Followed by Suspicious Events	Exploit	Event	True	Reports exploit activity from a source IP address followed by suspicious account activity to a third host from the same destination IP address as the original exploit within 15 minutes.
Exploit: Destination Vulnerable to Detected Exploit	Exploit	Event	True	Reports an exploit against a vulnerable local destination IP address, where the destination IP address is known to exist, and the host is vulnerable to the exploit.
Exploit: Destination Vulnerable to Detected Exploit on a Different Port	Exploit	Event	True	Reports an exploit against a vulnerable local destination IP address, where the destination IP address is known to exist, and the host is vulnerable to the exploit on a different port.
Exploit: Destination Vulnerable to Different Exploit than Attempted on Targeted Port	Exploit	Event	False	Reports an exploit against a vulnerable local destination IP address, where the target is known to exist, and the host is vulnerable to some exploit but not the one being attempted.
Exploit: Exploit Followed by Suspicious Host Activity	Exploit	Event	False	Reports an exploit from a source IP address followed by suspicious account activity on the destination host within 15 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Exploit: Exploit/Malware Events Across Multiple Destinations	Exploit	Event	True	Reports a source IP address generating multiple (at least five) exploits or malicious software (malware) events in the last 5 minutes. These events are not targeting hosts that are vulnerable and may indicate false positives generating from a device.
Exploit: Exploits Events with High Magnitude Become Offenses	Exploit	Event	True	Rule generates offenses for exploit-based events with a high magnitude.
Exploit: Exploits Followed by Firewall Accepts	Exploit	Event	False	Reports when exploit events are followed by firewall accept events, which may indicate a successful exploit.
Exploit: Multiple Exploit Types Against Single Destination	Exploit	Event	True	Reports a destination IP address being exploited using multiple types of exploit types from one or more source IP address.
Exploit: Multiple Vector Attack Source	Exploit	Event	False	Reports when a source IP address attempts multiple attack vectors. This may indicate a source IP address specifically targeting an asset.
Exploit: Potential VoIP Toll Fraud	Exploit	Event	False	Reports when at least three failed login attempts within 30 seconds followed by sessions being opened are detected on your VoIP hardware. This action can indicate that illegal users are executing VoIP sessions on your network.
Exploit: Recon followed by Exploit	Exploit	Event	True	Reports reconnaissance events followed by an exploit from the same source IP address to the same destination port within 1 hour.
Exploit: Source Vulnerable to any Exploit	Exploit	Event	False	Reports an exploit from a local host where the source IP address has at least one vulnerability to any exploit. It is possible the source IP address was a destination IP address in an earlier offense.
Exploit: Source Vulnerable to this Exploit	Exploit	Event	False	Reports an attack from a local host where the source IP address has at least one vulnerability to the exploit being used. It is possible the source IP address was a destination IP address in an earlier offense.
FalsePositive: False Positive Rules and Building Blocks	False Positive	Event	True	Reports events that include false positive rules and BBs, such as, BB:FalsePositive: Windows Server False Positive Events. Events that match the rule are stored and dropped from the event pipeline. If you add any new BBs or rules to remove events from becoming offenses, you must add these new rules or BBs to this rule.
Magnitude Adjustment: Context is Local to Local	Magnitude Adjustment	Common	True	Adjusts the relevance of flows and events when there is local to local communication

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Magnitude Adjustment: Context is Local to Remote	Magnitude Adjustment	Common	True	Adjusts the relevance of flows and events when there is local to remote communication.
Magnitude Adjustment: Context is Remote to Local	Magnitude Adjustment	Common	True	Adjusts the relevance of flows and events when there is remote to local communication.
Magnitude Adjustment: Destination Asset Exists	Magnitude Adjustment	Common	True	Adjusts the relevance and credibility of flows and events where the destination is a local asset.
Magnitude Adjustment: Destination Asset Port is Open	Magnitude Adjustment	Common	True	Adjusts the relevance and credibility of events and flows when the destination port is known to be active.
Magnitude Adjustment: Destination Network Weight is High	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the destination network weight is high.
Magnitude Adjustment: Destination Network Weight is Low	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the destination network weight is low.
Magnitude Adjustment: Destination Network Weight is Medium	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the destination network weight is medium.
Magnitude Adjustment: Source Address is a Bogon IP	Magnitude Adjustment	Common	True	Adjusts the severity of events and flows when the source IP is a known bogon address. Traffic from known bogon addresses may indicate the possibility of the source IP address being spoofed.
Magnitude Adjustment: Source Address is a Known Questionable IP	Magnitude Adjustment	Common	True	Adjusts the severity of events and flows when the source IP is a known questionable host.
Magnitude Adjustment: Source Asset Exists	Magnitude Adjustment	Common	True	Adjusts the relevance and credibility of flows and events where the source is a local asset.
Magnitude Adjustment: Source Network Weight is High	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the source network weight is high.
Magnitude Adjustment: Source Network Weight is Low	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the source network weight is low.
Magnitude Adjustment: Source Network Weight is Medium	Magnitude Adjustment	Common	True	Adjusts the relevance of events and flows if the source network weight is medium.
Malware: Communication with a site that has been involved in previous SQL injection	Malware	Flow	False	Reports communication with a website that has been involved in previous SQL injection.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Malware: Communication with a site that is listed on a known blacklist or uses fast flux	Malware	Flow	True	Reports communication with a website that is listed on a known blacklist or uses fast flux.
Malware: Communication with a website known to aid in distribution of malware	Malware	Flow	False	Reports communication with a website known to aid in distribution of malware.
Malware: Communication with a website known to be a phishing or fraud side	Malware	Flow	False	Reports communication with a website known to be a phishing or fraud site. ***Note:*** *Phishing is the process of attempting to acquire information such as user names, passwords and credit card details by pretending to be a trustworthy entity.*
Malware: Communication with a website known to be associated with the Russian business network	Malware	Flow	True	Reports communication with a website known to be associated with the Russian business network.
Malware: Communication with a website known to be delivering code which may be a trojan	Malware	Flow	False	Reports communication with a website known to be delivering code which may be a trojan.
Malware: Communication with a website known to be involved in botnet activity	Malware	Flow	False	Reports communication with a website known to be involved in botnet activity.
Malware: Local Host Sending Malware	Malware	Event	False	Reports malware being sent from local hosts.
Malware: Remote: Client Based DNS Activity to the Internet	Malware	Flow	True	Reports when a host is attempting to connect to a DNS server that is not defined as a local network.
Malware: Treat Backdoor, Trojans and Virus Events as Offenses	Malware	Event	False	Reports events categorized as backdoor, virus, and trojan. Enable this rule if you want all events categorized as backdoor, virus, and trojan to create an offense.
Malware: Treat Key Loggers as Offenses	Malware	Event	False	Reports events categorized as key loggers. Enable this rule if you want all events categorized as key logger to create an offense.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Malware: Treat Non-Spyware Malware as Offenses	Malware	Event	False	Reports non-spyware malware events. Enable this rule if you want all events categorized as malware to create an offense.
Malware: Treat Spyware and Virus as Offenses	Malware	Event	False	Reports spyware and a virus events. Enable this rule if you want all events categorized as Virus or Spyware to create an offense.
Policy: Connection to a remote proxy or anonymization service	Policy	Common	True	Reports events or flows associated with remote proxy and anonymization services.
Policy: Connection to Internet on Unauthorized Port	Policy	Common	False	Reports events or flows connecting to the Internet on unauthorized ports.
Policy: Create Offenses for All Chat Traffic based on Flows	Policy	Flow	False	Reports flows associated with chat traffic.
Policy: Create Offenses for All Instant Messenger Traffic	Policy	Event	False	Reports Instant Messenger traffic or any event categorized as Instant Messenger traffic where the source is local and the destination IP address is remote.
Policy: Create Offenses for All P2P Usage	Policy	Event	False	Reports Peer-to-Peer (P2P) traffic or any event categorized as P2P.
Policy: Create Offenses for All Policy Events	Policy	Event	False	Reports policy events. By default, this rule is disabled. Enable this rule if you want all events categorized as policy to create an offense.
Policy: Create Offenses for All Porn Usage	Policy	Event	False	Reports any traffic that contains illicit materials or any event categorized as porn. By default, this rule is disabled. Enable this rule if you want all events categorized as porn to create an offense.
Policy: Host has SANS Top 20 Vulnerability	Policy	Event	False	Reports when an event is detected on an asset that is vulnerable to a vulnerability identified in the SANS Top 20 Vulnerabilities. (*http://www.sans.org/top20/*)
Policy: Large Outbound Transfer High Rate of Transfer	Policy	Flow	True	Reports a single host sending more data out of the network than received. This rule detects over 2 MB of data transferred over 12 minutes.
Policy: Large Outbound Transfer Slow Rate of Transfer	Policy	Flow	True	Reports a single host sending more data out of the network than received. This rule detects over 2 MB of data transferred over 2 hour. This is fairly slow and can indicate stealthy data leakage.
Policy: Local: Clear Text Application Usage	Policy	Flow	False	Reports flows to or from the Internet where the application type uses clear text passwords. This may include applications such as Telnet or FTP.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Policy: Local: Hidden FTP Server	Policy	Flow	True	Reports a FTP server on a non-standard port. The default port for FTP is TCP port 21. Detecting FTP on other ports may indicate an exploited host, where this server provides backdoor access to the host.
Policy: Local: SSH or Telnet Detected on Non-Standard Port	Policy	Flow	True	Reports a SSH or Telnet server on a non-standard port. The default port for SSH and Telnet servers is TCP ports 22 and 23. Detecting SSH or Telnet operating on other ports may indicate an exploited host, where these servers provide backdoor access to the host.
Policy: New DHCP Server Discovered	Policy	Flow	False	Reports when a DHCP server is discovered on the network.
Policy: New Host Discovered	Policy	Event	False	Reports when a new host has been discovered on the network.
Policy: New Host Discovered in DMZ	Policy	Event	False	Reports when a new host has been discovered in the DMZ.
Policy: New Service Discovered	Policy	Event	False	Reports when a new service is discovered on an existing host.
Policy: New Service Discovered in DMZ	Policy	Event	False	Reports when a new service has been discovered on an existing host in the DMZ.
Policy: Possible Local IRC Server	Policy	Common	True	Reports a local host running a service on a typical IRC port or a flow that was detected as IRC. This is not typical for enterprises and should be investigated.
Policy: Remote: Clear Text Application Usage based on Flows	Policy	Flow	True	Reports flows to or from the Internet where the application type uses clear text passwords. This may include applications such as Telnet or FTP.
Policy: Remote: Hidden FTP Server	Policy	Flow	True	Reports an FTP server on a non-standard port. The default port for FTP is TCP port 21. Detecting FTP on other ports may indicate an exploited host, where this server to provide backdoor access to the host.
Policy: Remote: IM/Chat	Policy	Flow	True	Reports an excessive amount of IM and Chat traffic from a single source.
Policy: Remote: IRC Connections	Policy	Common	False	Reports a local host issuing an excessive number of IRC connections to the Internet.
Policy: Remote: Local P2P Client Connected to more than 100 Servers	Policy	Flow	True	Reports local hosts operating as a P2P client. This indicates a violation of local network policy and may indicate illegal activities, such as copyright infringement.
Policy: Remote: Local P2P Client Detected	Policy	Flow	False	Reports local hosts operating as a P2P client. This indicates a violation of local network policy and may indicate illegal activities, such as copyright infringement.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Policy: Remote: Local P2P Server connected to more than 100 Clients	Policy	Flow	True	Reports local hosts operating as a P2P server. This indicates a violation of local network policy and may indicate illegal activities, such as copyright infringement.
Policy: Remote: Local P2P Server Detected	Policy	Flow	False	Reports local hosts operating as a P2P server. This indicates a violation of local network policy and may indicate illegal activities, such as copyright infringement.
Policy: Remote: Long Duration Flow Detected	Policy	Flow	True	Reports a flow communicating to the Internet with a sustained duration of more than 48 hours. This is not typical behavior for most applications. Investigate the host for potential malware infections.
Policy: Remote: Potential Tunneling	Policy	Flow	True	Reports potential tunneling that can be used to bypass policy or security controls.
Policy: Remote: Remote Desktop Access from the Internet	Policy	Flow	True	Reports the Microsoft ®Remote Desktop Protocol from the Internet communicating to a local host. Most companies consider this a violation of corporate policy. If this is normal activity on your network, you should disable this rule.
Policy: Remote: SMTP Mail Sender	Policy	Flow	True	Reports a local host sending a large number of SMTP flows from the same source to the Internet in one interval. This may indicate a mass mailing, worm, or spam relay is present.
Policy: Remote: SSH or Telnet Detected on Non-Standard Port	Policy	Flow	True	Reports a SSH or Telnet server on a non-standard port. The default port for SSH and Telnet servers is TCP port 22 and 23. Detecting SSH or Telnet operating on other ports may indicate an exploited host, where these servers provide backdoor access to the host.
Policy: Remote: Usenet Usage	Policy	Flow	True	Reports flows to or from a Usenet server. It is uncommon for legitimate business communications to use Usenet or NNTP services. The hosts involved may be violating corporate policy.
Policy: Remote: VNC Access from the Internet to a Local Host	Policy	Flow	True	Reports when VNC (a remote desktop access application) is communicating from the Internet to a local host. Many companies consider this a policy issue that should be addressed. If this is normal activity on your network, disable this rule.
Policy: Upload to Local WebServer	Policy	Event	False	Reports potential file uploads to a local web server. To edit the details of this rule, edit the BB:CategoryDefinition: Upload to Local WebServer BB.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Aggressive Local L2L Scanner Detected	Recon	Common	True	Reports an aggressive scan from a local source IP address, scanning other local IP addresses. More than 400 destination IP addresses received reconnaissance or suspicious events in less than 2 minutes. This may indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm is present on the system.
Recon: Aggressive Local L2R Scanner Detected	Recon	Common	True	Reports an aggressive scan from a local source IP address, scanning remote IP addresses. More than 400 destination IP addresses received reconnaissance or suspicious events in less than 2 minutes. This may indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm is present on the system.
Recon: Aggressive Remote Scanner Detected	Recon	Common	True	Reports an aggressive scan from a remote source IP address, scanning other local or remote IP addresses. More than 50 destination IP addresses received reconnaissance or suspicious events in less than 3 minutes. This may indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm on a system.
Recon: Excessive Firewall Denies From Local Hosts	Recon	Common	True	Reports excessive attempts, from local hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Recon: Excessive Firewall Denies From Remote Hosts	Recon	Common	True	Reports excessive attempts, from remote hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Recon: Host Port Scan Detected by Remote Host	Recon	Common	True	Reports when more than 400 ports are scanned from a single source IP address in under 2 minutes.
Recon: Increase Magnitude of High Rate Scans	Recon	Event	True	If a high rate flow-based scanning attack is detected, this rule increases the magnitude of the current event.
Recon: Increase Magnitude of Medium Rate Scans	Recon	Event	True	If a medium rate flow-based scanning attack is detected, this rule increases the magnitude of the current event.
Recon: Local L2L LDAP Server Scanner	Recon	Common	True	Reports a source local IP address attempting reconnaissance or suspicious connections on common local LDAP ports to more than 60 hosts in 10 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Local L2R LDAP Server Scanner	Recon	Common	True	Reports a source local IP address attempting reconnaissance or suspicious connections on common remote LDAP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Database Scanner	Recon	Common	True	Reports a scan from a local host against other local destination IP addresses. At least 30 host were scanned in 10 minutes.
Recon: Local L2R Database Scanner	Recon	Common	True	Reports a scan from a local host against remote destination IP addresses. At least 30 host were scanned in 10 minutes.
Recon: Local L2L DHCP Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local DHCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R DHCP Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote DHCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local DNS ports to more than 60 hosts in 10 minutes.
Recon: Local L2R DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote DNS ports to more than 60 hosts in 10 minutes.
Recon: Local L2L FTP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local FTP ports to more than 30 hosts in 10 minutes.
Recon: Local L2R FTP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote FTP ports to more than 30 hosts in 10 minutes.
Recon: Local L2L Game Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local game server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Game Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote game server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L ICMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local ICMP ports to more than 60 hosts in 10 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Local L2R ICMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote ICMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L IM Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local IM server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R IM Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote IM server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L IRC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local IRC server ports to more than 10 hosts in 10 minutes.
Recon: Local L2R IRC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote IRC server ports to more than 10 hosts in 10 minutes.
Recon: Local L2L Mail Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local mail server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Mail Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote mail server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L P2P Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local P2P server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R P2P Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote P2P server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Proxy Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local proxy server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Proxy Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote proxy server ports to more than 60 hosts in 10 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Local L2L RPC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local RPC server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R RPC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote RPC server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Scanner Detected	Recon	Common	True	Reports a scan from a local host against other local destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Local L2R Scanner Detected	Recon	Common	True	Reports a scan from a local host against remote destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Local L2L SNMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local SNMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R SNMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote SNMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L SSH Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local SSH ports to more than 30 hosts in 10 minutes.
Recon: Local L2R SSH Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote SSH ports to more than 30 hosts in 10 minutes.
Recon: Local L2L Suspicious Probe Events Detected	Recon	Common	False	Reports when various suspicious or reconnaissance events have been detected from the same local source IP address to more than five local destination IP address in 4 minutes. This can indicate various forms of host probing, such as Nmap reconnaissance, which attempts to identify the services and operation systems of the host.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Local L2R Suspicious Probe Events Detected	Recon	Common	False	Reports when various suspicious or reconnaissance events have been detected from the same remote source IP address to more than five local destination IP address in 4 minutes. This can indicate various forms of host probing, such as Nmap reconnaissance, which attempts to identify the services and operation systems of the host.
Recon: Local L2L TCP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local TCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R TCP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote TCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L UDP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local UDP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R UDP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common Remote UDP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Web Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Web Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote web server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Windows Server Scanner to Internet	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local Windows server ports to more than 60 hosts in 20 minutes.
Recon: Local L2R Windows Server Scanner to Internet	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote Windows server ports to more than 60 hosts in 20 minutes.
Recon: Local Windows Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common Windows server ports to more than 200 hosts in 20 minutes.
Recon: Potential Local Port Scan Detected	Recon	Common	True	Reports on potential local port scans.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Potential P2P Traffic Detected	Recon	Common	True	Reports on potential P2P traffic.
Recon: Recon Followed by Accept	Recon	Common	False	Reports when a host that has been performing reconnaissance also has a firewall accept following the reconnaissance activity.
Recon: Remote Database Scanner	Recon	Common	True	Reports a scan from a remote host against other local or remote destination IP addresses. At least 30 hosts were scanned in 10 minutes.
Recon: Remote DHCP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common DHCP ports to more than 30 hosts in 10 minutes.
Recon: Remote DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common DNS ports to more than 60 hosts in 10 minutes.
Recon: Remote FTP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common FTP ports to more than 30 hosts in 10 minutes.
Recon: Remote Game Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common game server ports to more than 30 hosts in 10 minutes.
Recon: Remote ICMP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common ICMP ports to more than 60 hosts in 10 minutes.
Recon: Remote IM Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common IM server ports to more than 60 hosts in 10 minutes.
Recon: Remote IRC Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common IRC server ports to more than 10 hosts in 10 minutes.
Recon: Remote LDAP Server Scanner	Recon	Common	True	Reports a scan from a remote host against other local or remote destination IP addresses. At least 30 hosts were scanned in 10 minutes.
Recon: Remote Mail Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common mail server ports to more than 30 hosts in 10 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Remote Proxy Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common proxy server ports to more than 30 hosts in 10 minutes.
Recon: Remote RPC Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common RPC server ports to more than 30 hosts in 10 minutes.
Recon: Remote Scanner Detected	Recon	Common	True	Reports a scan from a remote host against other hosts or remote destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Remote SNMP Scanner	Recon	Common	True	Reports a remote host scans at least 30 local or remote hosts in 10 minutes.
Recon: Remote SSH Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common SSH ports to more than 30 hosts in 10 minutes.
Recon: Remote Suspicious Probe Events Detected	Recon	Common	False	Reports various suspicious or reconnaissance events from the same remote source IP address to more then five destination IP addresses in 4 minutes. This may indicate various forms of host probing, such as Nmap reconnaissance that attempts to identify the services and operating system of the destination IP addresses.
Recon: Remote TCP Scanner	Recon	Common	False	Reports a remote host attempting reconnaissance or suspicious connections on common TCP ports to more than 60 hosts in 10 minutes.
Recon: Remote UDP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common UDP ports to more than 60 hosts in 10 minutes.
Recon: Remote Web Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Recon: Remote Windows Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common Windows server ports to more than 60 hosts in 10 minutes.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Recon: Single Merged Recon Events Local Scanner	Recon	Common	True	Reports merged reconnaissance events generated by local scanners. This rule causes all these events to create an offense. All devices of this type and their event categories should be added to the BB:ReconDetected: Devices which Merge Recon into Single Events BB.
Recon: Single Merged Recon Events Remote Scanner	Recon	Common	True	Reports merged reconnaissance events generated by remote scanners. This rule causes all these events to create an offense. All devices of this type and their event categories should be added to the BB:ReconDetected: Devices which Merge Recon into Single Events BB.
Default-Response-E-mail: Offense E-mail Sender	Response	Offense	False	Reports any offense matching the severity, credibility, and relevance minimums to email. You must configure the email address. You can limit the number of emails sent by tuning the severity, credibility, and relevance limits. This rule only sends one email every hour, per offense.
Default-Response-Syslog: Offense SYSLOG Sender	Response	Offense	False	Reports any offense matching the severity, credibility, or relevance minimum to syslog.
SuspiciousActivity: Common Non-Local to Remote Ports	Suspicious	Common	False	Rule identifies events that have common internal only ports, communicating outside of the local network.
SuspiciousActivity: Communication with Known Hostile Networks	Suspicious	Common	False	Reports events associated with known hostile networks.
SuspiciousActivity: Communication with Known Online Services	Suspicious	Common	False	Reports events associated with networks identified as websites that may involve data loss.
SuspiciousActivity: Communication with Known Watched Networks	Suspicious	Common	False	Reports events associated with networks you want to monitor.
SuspiciousActivity: Consumer Grade Equipment	Suspicious	Event	False	Reports when discovered assets appear to be consumer grade equipment.
System: 100% Accurate Events	System	Event	True	Creates an offense when an event matches a 100% accurate signature for successful compromises.
System:Critical System Events	System	Event	False	Reports when QRadar SIEM detects critical event.
System: Device Stopped Sending Events	System	Event	False	Reports when a log source has not sent an event to the system in over 1 hour. Edit this rule to add devices you want to monitor.

Table 15-1 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
System: Device Stopped Sending Events (Firewall, IPS, VPN or Switch)	System	Event	True	Reports when a firewall, IPS, VPN or switch log source has not sent an event in over 30 minutes
System: Flow Source Stopped Sending Flows	System	Flow	True	Reports when a flow interface stops generating flows for over 30 minutes.
System: Host Based Failures	System	Event	False	Reports when QRadar SIEM detects events that indicate failures within services or hardware.
System: Load Building Blocks	System	Event	True	Loads the BBs required to assist with reporting. This rule has no actions or responses.
System: Multiple System Errors	System	Event	False	Reports when a source IP address has 10 system errors within 3 minutes.
System:Notification	System	Event	True	Rule ensures that notification events shall be sent to the notification framework.
System: Service Stopped and not Restarted	System	Event	False	Reports when a services has been stopped on a system and not restarted.
WormDetection: Local Mass Mailing Host Detected	Worms	Event	True	Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.
WormDetection: Possible Local Worm Detected	Worms	Event	True	Reports a local host generating reconnaissance or suspicious events across a large number of hosts (greater than 300) in 20 minutes. This may indicate the presence of a worm on the network or a wide spread scan.
WormDetection: Successful Connections to the Internet on Common Worm Ports	Worms	Event	True	Reports when a host is connecting to many hosts on the Internet on ports commonly known for worm propagation.
WormDetection: Worm Detected (Events)	Worms	Event	True	Reports exploits or worm activity on a system for local-to-local or local-to-remote traffic.

Default Building Blocks

Default building blocks for the Enterprise template include:

Table 15-2 Default Building Blocks

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB: CategoryDefinition: Application or Service Installed or Modified	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected when an application or service is installed or modified on a host.	
BB: CategoryDefinition: Auditing Stopped	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected when auditing has stopped on a host.	
BB: CategoryDefinition: Communication with File Sharing Sites	Category Definitions	Flow	Edit this BB to include applications that indicate communication with file sharing sites.	
BB: CategoryDefinition: Communication with Free Email Sites	Category Definitions	Flow	Edit this BB to include applications that indicate communication with free email sites	
BB:CategoryDefinition: Logout Events	Category Definitions	Event	Edit this BB to include all events that indicate successful logout attempts from devices.	
BB: CategoryDefinition: Service Started	Category Definition	Event	Edit the BB to include all event categories that indicate a service has started.	
BB: CategoryDefinition: Service Stopped	Category Definition	Event	Edit the BB to include all event categories that indicate a service has stopped.	
BB: CategoryDefinition: Superuser Accounts	Category Definition	Event	Edit this BB to include user names associated with superuser accounts, such as admin, superuser, and root.	
BB: CategoryDefinition: System or Device Configuration Change	Category Definition	Event	Edit this BB is include event categories associated with system or device configuration changes.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB: CategoryDefinition: Unidirectional Flow	Category Definition	Flow	Edit this BB to include all unidirectional flows.	BB: CategoryDefinition: Unidirectional Flow DST BB: CategoryDefinition: Unidirectional Flow SRC
BB: CategoryDefinition: Unidirectional Flow DST	Category Definition	Flow	Edit this BB to define unidirectional flow from the source IP address to the destination IP address.	
BB: CategoryDefinition: Unidirectional Flow SRC	Category Definition	Flow	Edit this BB to define unidirectional flow from the destination IP address to the source IP address.	
BB:BehaviorDefinition: Compromise Activities	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected during a typical compromise.	
BB:BehaviorDefinition: Post Compromise Activities	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected after a typical compromise.	
BB:CategoryDefinition: Access Denied	Category Definition	Event	Edit this BB to include all event categories that indicate access denied.	
BB:CategoryDefinition: Any Flow	Category Definition	Flow	Edit this BB to include all flow types.	
BB:CategoryDefinition: Authentication Failures	Compliance	Event	Edit this BB to include all events that indicate an unsuccessful attempt to access the network.	
BB:CategoryDefinition: Authentication Success	Compliance	Event	Edit this BB to include all events that indicate successful attempts to access the network.	
BB:CategoryDefinition: Authentication to Disabled Account	Compliance	Event	Edit this BB to include all events that indicate failed attempts to access the network using a disabled account.	
BB:CategoryDefinition: Authentication to Expired Account	Compliance	Event	Edit this BB to include all events that indicate failed attempts to access the network using an expired account.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:CategoryDefinition: Authentication User or Group Added or Changed	Compliance	Event	Edit this BB to include all events that indicate modification to accounts or groups.	
BB:CategoryDefinition: Countries with no Remote Access	Category Definitions	Event	Edit this BB to include any geographic location that typically is not allowed remote access to the enterprise. When configured, you can enable the Anomaly: Remote Access from Foreign Country rule.	
BB:CategoryDefinition: Database Access Denied	Category Definition	Event	Edit this BB to include all events that indicates denied access to the database.	
BB:CategoryDefinition: Database Access Permitted	Category Definition	Event	Edit this BB to include all events that indicates permitted access to the database.	
BB:CategoryDefinition: Database Connections	Category Definitions	Event	Edit this BB to define successful logins to databases. You may be required to add additional device types for this BB.	
BB:CategoryDefinition: DDoS Attack Events	Category Definitions	Event	Edit this BB to include all event categories that you want to categorize as a DDoS attack.	
BB:CategoryDefinition: Exploits, Backdoors, and Trojans	Category Definitions	Event	Edit this BB to include all events that are typically exploits, backdoor, or trojans.	
BB:CategoryDefinition: Failure Service or Hardware	Compliance	Event	Edit this BB that indicate failure within a service or hardware.	
BB:CategoryDefinition: Firewall or ACL Accept	Category Definitions	Event	Edit this BB to include all events that indicate access to the firewall.	
BB:CategoryDefinition: Firewall or ACL Denies	Category Definitions	Event	Edit this BB to include all events that indicate unsuccessful attempts to access the firewall.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:CategoryDefinition: Firewall System Errors	Category Definitions	Event	Edit this BB to include all events that may indicate a firewall system error. By default, this BB applies when an event is detected by one or more of the following devices: • Check Point • Generic Firewall • Iptables • NetScreen Firewall • Cisco Pix	
BB:CategoryDefinition: High Magnitude Events	Category Definitions	Event	Edit this BB to the severity, credibility, and relevance levels you want to generate an event. The defaults are: • Severity = 6 • Credibility = 7 • Relevance = 7	
BB:CategoryDefinition: Inverted Flows	Category Definitions	Flow	Edit this BB to identify flows that may be inverted.	
BB:CategoryDefinition: IRC Detected Based on Application	Category Definitions	Flow	This Building Block to include applications that are typically associated with IRC traffic.	BB:CategoryDefinition: Successful Communication
BB:CategoryDefinition: IRC Detected Based on Event Category	Category Definitions	Event	This Building Block to include event categories that are typically associated with IRC traffic.	
BB:CategoryDefinition: IRC Detection Based on Firewall Events	Category Definitions	Event	This Building Block to include event categories and port definitions that are typically associated with IRC traffic.	BB:CategoryDefinition: Firewall or ACL Accept BB:PortDefinition: IRC Ports
BB:CategoryDefinition: KeyLoggers	Category Definitions	Event	Edit this BB to include all events associated with key logger monitoring of user activities.	
BB:CategoryDefinition: Mail Policy Violation	Compliance	Event	Edit this BB to define mail policy violations.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:CategoryDefinition: Malware Annoyances	Category Definitions	Event	Edit this BB to include event categories that are typically associated with spyware infections.	
BB:CategoryDefinition: Network DoS Attack	Category Definitions	Event	Edit this BB to include all event categories that you want to categorize as a network DoS attack.	
BB:CategoryDefinition: Policy Events	Compliance	Event	Edit this BB to include all event categories that may indicate a violation to network policy.	
BB:CategoryDefinition: Post DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Remote-to-Local (R2L) and a DMZ host jumping scenario.	
BB:CategoryDefinition: Post Exploit Account Activity	Category Definitions	Event	Edit this BB to include all event categories that may indicate exploits to accounts.	
BB:CategoryDefinition: Pre DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Local-to-Local (L2L) and a DMZ host jumping scenario.	
BB:CategoryDefinition: Pre Reverse DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Pre DMZ jump followed by a reverse DMZ jump.	
BB:CategoryDefinition: Recon Event Categories	Category Definitions	Event	Edit this BB to include all event categories that indicate reconnaissance activity.	
BB:CategoryDefinition: Recon Events	Category Definitions	Common	Edit this BB to include all events that indicate reconnaissance activity.	
BB:CategoryDefinition: Recon Flows	Category Definitions	Flow	Edit this BB to include all flows that indicate reconnaissance activity.	
BB:CategoryDefinition: Reverse DMZ Jump	Category Definitions	Common	Edit this BB to define actions that may be seen within a Remote-to-Local (R2L) and a DMZ host reverse jumping scenario.	
BB:CategoryDefinition: Service DoS	Category Definitions	Event	Edit this BB to define Denial of Service (DoS) attack events.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:CategoryDefinition: Session Closed	Category Definition	Event	Edit this BB to define all session closed events.	
BB:CategoryDefinition: Session Opened	Category Definition	Event	Edit this BB to define all session opened events.	
BB:CategoryDefinition: Successful Communication	Category Definitions	Flow	Edit this BB to include all flows that are typical of a successful communication. Tuning this BB to reduce the byte to packet ratio to 64 can cause excessive false positives. Further tuning using additional tests may be required.	
BB:CategoryDefinition: Suspicious Event Categories	Category Definitions	Event	Edit this BB to include all event categories that indicate suspicious activity.	
BB:CategoryDefinition: Suspicious Events	Category Definitions	Common	Edit this BB to include all events that indicate suspicious activity.	
BB:CategoryDefinition: Suspicious Flows	Category Definitions	Flow	Edit this BB to include all flows that indicate suspicious activity.	
BB:CategoryDefinition: System Configuration	Category Definitions	Event	Edits this BB to define system configuration events.	
BB:CategoryDefinition: System Errors and Failures	Category Definitions	Event	Edit this BB to define system errors and failures.	
BB:CategoryDefinition: Upload to Local WebServer	Category Definitions	Event	Typically, most networks are configured to restrict applications that use the PUT method running on their web application servers. This BB detects if a remote host has used this method on a local server. The BB can be duplicated to also detect other unwanted methods or for local hosts using the method connecting to remote servers. This BB is referred to by the Policy: Upload to Local WebServer rule.	
BB:CategoryDefinition: Virus Detected	Category Definition	Event	Edit this BB to define all virus detection events.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:CategoryDefinition: VoIP Authentication Failure Events	Category Definitions	Event	Edit this BB to include all events that indicate a VoIP login failure.	
BB:CategoryDefinition: VoIP Session Opened	Category Definitions	Event	Edit this BB to include all events that indicate the start of a VoIP session.	
BB:CategoryDefinition: VPN Access Accepted	Category Definition	Event	Edit this BB to include all events that indicates permitted access.	
BB:CategoryDefinition: VPN Access Denied	Category Definition	Event	Edit this BB to include all events that are considered Denied Access events.	
BB:CategoryDefinition: Windows Compliance Events	Compliance	Event	Edit this BB to include all event categories that indicate compliance events.	
BB:CategoryDefinition: Windows SOX Compliance Events	Compliance	Event	Edit this BB to include all event categories that indicate SOX compliance events.	
BB:CategoryDefinition: Worm Events	Category Definitions	Event	Edit this BB to define worm events. This BB only applies to events not detected by a custom rule.	
BB:ComplianceDefinition: GLBA Servers	Compliance	Common	Edit this BB to include your GLBA IP systems. You must then apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: HIPAA Servers	Compliance	Common	Edit this BB to include your HIPAA Servers by IP address. You must then apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: PCI DSS Servers	Response	Common	Edit this BB to include your PCI DSS servers by IP address. You must apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: SOX Servers	Compliance	Common	Edit this BB to include your SOX IP Servers. You must then apply this BB to rules related to failed logins such as remote access.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Database: System Action Allow	Compliance	Event	Edit this BB to include any events that indicates successful actions within a database.	
BB:Database: System Action Deny	Compliance	Event	Edit this BB to include any events that indicate unsuccessful actions within a database.	
BB:Database: User Addition or Change	Compliance	Event	Edit this BB to include events that indicate the successful addition or change of user privileges	
BB:DeviceDefinition: Access/Authentication/ Audit	Log Source Definitions	Event	Edit this BB to include all access, authentication, and audit devices.	
BB:DeviceDefinition: AntiVirus	Log Source Definitions	Event	Edit this BB to include all antivirus services on the system.	
BB:DeviceDefinition: Application	Log Source Definitions	Event	Edit this BB to include all application and OS devices on the network.	
BB:DeviceDefinition: Consumer Grade Routers	Log Source Definitions	Event	Edit this BB to include MAC addresses of known consumer grade routers.	
BB:DeviceDefinition: Consumer Grade Wireless APs	Log Source Definitions	Event	Edit this BB to include MAC addresses of known consumer grade wireless access points.	
BB:DeviceDefinition: Database	Log Source Definitions	Event	Edit this BB to define all databases on the system.	
BB:DeviceDefinition: Devices to Monitor for High Event Rates	Log Source Definitions	Event	Edit this BB to include devices you want to monitor for high event rates. The event rate threshold is controlled by the Anomaly: Devices with High Event Rates.	
BB:DeviceDefinition: FW/Router/ Switch	Log Source Definitions	Event	Edit this BB to include all firewall (FW), routers, and switches on the network.	
BB:DeviceDefinition: IDS/IPS	Log Source Definitions	Event	Edit this BB to include all IDS and IPS devices on the network.	
BB:DeviceDefinition:VPN	Log Source Definition	Event	Edit this BB to include all VPNs on the network.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:DoS: Local: Distributed DoS Attack (High Number of Hosts)	D/DoS	Flow	Edit this BB to detect a high number of hosts (greater than 100,000) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Local: Distributed DoS Attack (Low Number of Hosts)	D/DoS	Flow	Edit this BB to detect a low number of hosts (greater than 500) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Local: Distributed DoS Attack (Medium Number of Hosts)	D/DoS	Flow	Edit this BB to detect a medium number of hosts (greater than 5,000) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Local: Flood Attack (High))	D/DoS	Flow	Edit this BB to detect flood attacks above 100,000 packets per second. This activity may indicate an attack.	
BB:DoS: Local: Flood Attack (Low)	D/DoS	Flow	Edit this BB to detect flood attacks above 500 packets per second. This activity may indicate an attack.	
BB:DoS: Local: Flood Attack (Medium))	D/DoS	Flow	Edit this BB to detect flood attacks above 5,000 packets per second. This activity may indicate an attack.	
BB:DoS: Local: Potential ICMP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an ICMP DoS attack attempt.	
BB:DoS: Local: Potential TCP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an TCP DoS attack attempt.	
BB:DoS: Local: Potential UDP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an UDP DoS attack attempt.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:DoS: Local: Potential Unresponsive Server or Distributed DoS	D/DoS	Flow	Edit this BB to detect a low number of hosts sending identical, non-responsive packets to a single destination. In this case, the destination is treated as the source on the **Offenses** tab.	
BB:DoS: Remote: Distributed DoS Attack (High Number of Hosts)	D/DoS	Flow	Edit this BB to detect a high number of hosts (greater than 100,000) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Remote: Distributed DoS Attack (Low Number of Hosts)	D/DoS	Flow	Edit this BB to detect a low number of hosts (greater than 500) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Remote: Distributed DoS Attack (Medium Number of Hosts)	D/DoS	Flow	Edit this BB to detect a medium number of hosts (greater than 5,000) sending identical, non-responsive packets to a single destination IP address.	
BB:DoS: Remote: Flood Attack (High)	D/DoS	Flow	Edit this BB to detect flood attacks above 100,000 packets per second. This activity may indicate an attack.	
BB:DoS: Remote: Flood Attack (Low)	D/DoS	Flow	Edit this BB to detect flood attacks above 500 packets per second. This activity may indicate an attack.	
BB:DoS:Remote: Flood Attack (Medium)	D/DoS	Flow	Edit this BB to detect flood attacks above 5,000 packets per second. This activity may indicate an attack.	
BB:DoS: Remote: Potential ICMP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an ICMP DoS attack attempt.	
BB:DoS: Remote: Potential TCP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an TCP DoS attack attempt.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:DoS: Remote: Potential UDP DoS	D/DoS	Flow	Edit this BB to detect flows that appear to be an UDP DoS attack attempt.	
BB:DoS: Remote: Potential Unresponsive Server or Distributed DoS	D/DoS	Flow	Edit this BB to detect a low number of hosts sending identical, non-responsive packets to a single destination. In this case, the destination is treated as the source in the **Offenses** tab.	
BB:FalseNegative: Events That Indicate Successful Compromise	False Positive	Event	Edit this BB to include events that indicate a successful compromise. These events generally have 100% accuracy.	
BB:FalsePositive: All Default False Positive BBs	False Positive	Common	Edit this BB to include all false positive BBs.	All BB:False Positive BBs
BB:FalsePositive: Broadcast Address False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from the broadcast address space.	
BB:FalsePositive: Database Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from database servers that are defined in the BB:HostDefinition: Database Servers BB.	BB:HostDefinition: Database Servers
BB:FalsePositive: Database Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from database servers that are defined in the BB:HostDefinition: Database Servers BB.	BB:HostDefinition: Database Servers
BB:FalsePositive: Device and Specific Event	False Positive	Event	Edit this BB to include the devices and QID of devices that continually generate false positives.	
BB:FalsePositive: DHCP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from DHCP servers that are defined in the BB:HostDefinition: DHCP Servers BB.	BB:HostDefinition: DHCP Servers

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:FalsePositive: DHCP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DHCP servers that are defined in the BB:HostDefinition: DHCP Servers BB.	BB:HostDefinition: DHCP Servers
BB:FalsePositive: DNS Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from DNS based servers that are defined in the BB:HostDefinition: DNS Servers BB.	BB:HostDefinition: DNS Servers
BB:FalsePositive: DNS Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DNS-based servers that are defined in the BB:HostDefinition: DNS Servers BB.	BB:HostDefinition: DNS Servers
BB:FalsePositive: Firewall Deny False Positive Events	False Positive	Event	Edit this BB to define firewall deny events that are false positives	
BB:FalsePositive: FTP False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from FTP-based servers that are defined in the BB:HostDefinition: FTP Servers BB.	BB:HostDefinition: FTP Servers
BB:FalsePositive: FTP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from FTP based servers that are defined in the BB:HostDefinition: FTP Servers BB.	BB:HostDefinition: FTP Servers
BB:FalsePositive: Global False Positive Events	False Positive	Event	Edit this BB to include any event QIDs that you want to ignore.	
BB:FalsePositive: Large Volume Local FW Events	False Positive	Event	Edit this BB to define specific events that can create a large volume of false positives in general rules.	
BB:FalsePositive: LDAP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from LDAP servers that are defined in the BB:HostDefinition: LDAP Servers BB.	BB:HostDefinition: LDAP Servers

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:FalsePositive: LDAP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from LDAP servers that are defined in the BB:HostDefinition: LDAP Servers BB.	BB:HostDefinition: LDAP Servers
BB:FalsePositive: Local Source to Local Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Local (L2L) based servers.	
BB:FalsePositive: Local Source to Remote Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Remote (L2R) based servers.	
BB:FalsePositive: Mail Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from mail servers that are defined in the BB:HostDefinition: Mail Servers BB.	BB:HostDefinition: Mail Servers
BB:FalsePositive: Mail Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from mail servers that are defined in the BB:HostDefinition: Mail Servers BB.	BB:HostDefinition: Mail Servers
BB:FalsePositive: Network Management Servers Recon	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from network management servers that are defined in the BB:HostDefinition: Network Management Servers BB.	BB:HostDefinition: Network Management Servers
BB:FalsePositive: Proxy Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from proxy servers that are defined in the BB:HostDefinition: Proxy Servers BB.	BB:HostDefinition: Proxy Servers
BB:FalsePositive: Proxy Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from proxy servers that are defined in the BB:HostDefinition: Proxy Servers BB.	BB:HostDefinition: Proxy Servers

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:FalsePositive: Remote Source to Local Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Remote-to-Local (R2L) based servers.	
BB:FalsePositive: RPC Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from RPC servers that are defined in the BB:HostDefinition: RPC Servers BB.	BB:HostDefinition: RPC Servers
BB:FalsePositive: RPC Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from RPC servers that are defined in the BB:HostDefinition: RPC Servers BB.	BB:HostDefinition: RPC Servers
BB:FalsePositive: Reversed Flows	False Positive	Flow	Edit this BB to prevent rules from processing flows that have changed direction.	
BB:FalsePositive: SNMP Sender or Receiver False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from SNMP servers that are defined in the BB:HostDefinition: SNMP Servers BB.	BB:HostDefinition: SNMP Servers
BB:FalsePositive: SNMP Sender or Receiver False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SNMP servers that are defined in the BB:HostDefinition: SNMP Sender or Receiver BB.	BB:HostDefinition: SNMP Sender or Receiver
BB:FalsePositive: Source IP and Specific Event	False Positive	Event	Edit this BB to include source IP addresses or specific events that you want to remove.	
BB:FalsePositive: SSH Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from SSH servers that are defined in the BB:HostDefinition: SSH Servers BB.	BB:HostDefinition: SSH Servers

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:FalsePositive: SSH Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SSH servers that are defined in the BB:HostDefinition: SSH Servers BB.	BB:HostDefinition: SSH Servers
BB:FalsePositive: Syslog Sender False Positive Categories	False Positive	Common	Edit this BB to define all false positive categories that occur to or from syslog sources.	BB:HostDefinition: Syslog Servers and Senders
BB:FalsePositive: Syslog Sender False Positive Events	False Positive	Event	Edit this BB to define all false positive events that occur to or from syslog sources or destinations.	BB:HostDefinitionBB:HostDefinition: Syslog Servers and Senders
BB:FalsePositive: Virus Definition Update Categories	False Positive	Common	Edit this BB to define all the false positive QIDs that occur to or from virus definition or other automatic update hosts that are defined in the BB:HostDefinition: Virus Definition and Other Update Servers BB.	BB:HostDefinition: Virus Definition and Other Update Servers
BB:FalsePositive: Web Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from web servers that are defined in the BB:HostDefinition: Web Servers BB.	BB:HostDefinition: Web Servers
BB:FalsePositive: Web Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Web servers that are defined in the BB:HostDefinition: Web Servers BB.	BB:HostDefinition: Web Servers
BB:FalsePositive: Windows AD Source Authentication Events	False Positive	Event	Edit this BB to add addresses of Windows Authentication and Active Directory (AD) servers. This BB prevents the AD servers from being the source of authentication messages.	
BB:FalsePositive: Windows Server False Positive Categories Local	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from Windows servers that are defined in the BB:HostDefinition: Windows Servers BB.	BB:HostDefinition: Windows Servers

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:FalsePositive: Windows Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Windows servers that are defined in the BB:HostDefinition: Windows Servers BB.	BB:HostDefinition: Windows Servers
BB:Flowshape: Balanced	Flowshape	Flow	This BB detects flows that have a balanced flow bias.	
BB:Flowshape: Inbound Only	Flowshape	Flow	This BB detects flows that have an inbound only flow bias.	
BB:Flowshape: Local Balanced	Flowshape	Flow	This BB detects local flows that have a balanced flow bias.	
BB:Flowshape: Local Unidirectional	Flowshape	Flow	This BB detects unidirectional flows within the local network.	
BB:Flowshape: Mostly Inbound	Flowshape	Flow	This BB detects flows that have a mostly inbound flow bias.	
BB:Flowshape: Mostly Outbound	Flowshape	Flow	This BB detects flows that have a mostly outbound flow bias.	
BB:Flowshape: Outbound Only	Flowshape	Flow	This BB detects flows that have an outbound only flow bias.	
BB:HostBased: Critical Events	Compliance	Event	Edit this BB to define event categories that indicate critical events.	
BB:HostDefinition: Consultant Assets	Host Definitions	Common	Edit this BB to include any consultant assets, which includes any asset connected to your network that is supplied or owned by a consultant and not considered to be your asset.	
BB:HostDefinition: Database Servers	Host Definitions	Common	Edit this BB to define typical database servers.	BB:FalsePositive: Database Server False Positive Categories BB:FalsePositive: Database Server False Positive Events

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:HostDefinition: DHCP Servers	Host Definitions	Common	Edit this BB to define typical DHCP servers.	BB:False Positive: DHCP Server False Positives Categories BB:FalsePositive: DHCP Server False Positive Events
BB:HostDefinition: DMZ Assets	Host Definitions	Common	Edit this BB to include any DMZ assets.	
BB:HostDefinition: DNS Servers	Host Definitions	Common	Edit this BB to define typical DNS servers.	BB:False Positive: DNS Server False Positives Categories BB:FalsePositive: DNS Server False Positive Events
BB:HostDefinition: FTP Servers	Host Definitions	Common	Edit this BB to define typical FTP servers.	BB:False Positive: FTP Server False Positives Categories BB:FalsePositive: FTP Server False Positive Events
BB:HostDefinition: Host with Port Open	Host Definitions	Common	Edit this BB to include a host and port that is actively or passively seen.	
BB:HostDefinition: LDAP Servers	Host Definitions	Common	Edit this BB to define typical LDAP servers.	BB:False Positive: LDAP Server False Positives Categories BB:FalsePositive: LDAP Server False Positive Events
BB:HostDefinition: Local Assets	Host Definitions	Common	Edit this BB to include any local assets.	
BB:HostDefinition: Mail Servers	Host Definitions	Common	Edit this BB to define typical mail servers.	BB:False Positive: Mail Server False Positives Categories BB:FalsePositive: Mail Server False Positive Events
BB:HostDefinition: MailServer Assets	Host Definitions	Common	Edit this BB to include any mail server assets.	
BB:HostDefinition: Network Management Servers	Host Definitions	Common	Edit this BB to define typical network management servers.	
BB:HostDefinition: Protected Assets	Host Definitions	Common	Edit this BB to include any protected assets.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:HostDefinition: Proxy Servers	Host Definitions	Common	Edit this BB to define typical proxy servers.	BB:False Positive: Proxy Server False Positives Categories BB:FalsePositive: Proxy Server False Positive Events
BB:HostDefinition: Regulatory Assets	Host Definitions	Common	Edit this BB to include any regulatory assets.	
BB:HostDefinition: Remote Assets	Host Definitions	Common	Edit this BB to include any remote assets.	
BB:HostDefinition: RPC Servers	Host Definitions	Common	Edit this BB to define typical RPC servers.	BB:False Positive: RPC Server False Positives Categories BB:FalsePositive: RPC Server False Positive Events
BB:HostDefinition: Servers	Host Definitions	Event	Edit this BB to define generic servers.	
BB:HostDefinition: SNMP Sender or Receiver	Host Definitions	Common	Edit this BB to define SNMP senders or receivers.	BB:PortDefinition: SNMP Ports
BB:HostDefinition: SSH Servers	Host Definitions	Common	Edit this BB to define typical SSH servers.	BB:False Positive: SSH Server False Positives Categories BB:FalsePositive: SSH Server False Positive Events
BB:HostDefinition: Syslog Servers and Senders	Host Definitions	Common	Edit this BB to define typical host that send or receive syslog traffic.	BB:FalsePositive: Syslog Server False Positive Categories BB:FalsePositive: Syslog Server False Positive Events
BB:HostDefinition: VA Scanner Source IP	Host Definitions	Common	Edit this BB to include the source IP address of your VA scanner. By default, this BB applies when the source IP address is 127.0.0.2.	
BB:HostDefinition: Virus Definition and Other Update Servers	Host Definitions	Common	Edit this BB to include all servers that include virus protection and update functions.	
BB:HostDefinition: VoIP PBX Server	Host Definitions	Common	Edit this BB to define typical VoIP IP PBX servers.	
BB:HostDefinition: VPN Assets	Host Definitions	Common	Edit this BB to include any VPN assets.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:HostDefinition: Web Servers	Host Definitions	Common	Edit this BB to define typical web servers.	BB:False Positive: Web Server False Positives Categories BB:FalsePositive: Web Server False Positive Events
BB:HostDefinition: Windows Servers	Host Definitions	Common	Edit this BB to define typical Windows servers, such as domain controllers or exchange servers.	BB:False Positive: Windows Server False Positives Categories BB:FalsePositive: Windows Server False Positive Events
BB:NetworkDefinition: Broadcast Address Space	Network Definition	Common	Edit this BB to include the broadcast address space of your network. This is used to remove false positive events that may be caused by the use of broadcast messages.	
BB:NetworkDefinition: Client Networks	Network Definition	Common	Edit this BB to include all networks that include client hosts.	
BB:NetworkDefinition: Darknet Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Darket list.	
BB:NetworkDefinition: DLP Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Data Loss Prevention (DLP) list.	
BB:NetworkDefinition: DMZ Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Demilitarized Zone (DMZ) list.	
BB:NetworkDefinition: DMZ Addresses(DST)	Network Definition	Common	Edit this BB to include destination networks that you want to add to a Demilitarized Zone (DMZ) list.	
BB:NetworkDefinition: DMZ Addresses(SRC)	Network Definition	Common	Edit this BB to include source networks that you want to add to a Demilitarized Zone (DMZ) list.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:NetworkDefinition: Honeypot like Addresses	Network Definition	Common	Edit this BB by replacing other network with network objects defined in your network hierarchy that are currently not in use in your network or are used in a honeypot or tarpit installation. When these have been defined, you must enable the Anomaly: Potential Honeypot Access rule. You must also add a security or policy BB to these network objects to generate events based on attempted access.	
BB:NetworkDefinition: Inbound Communication from Internet to Local Host	Network Definition	Common	Edit this BB to include all traffic from the Internet to you local networks.	
BB:NetworkDefinition: Multicast Address Space	Network Definition	Common	Edit this BB to include networks that you want to add to a multicast address space list.	
BB:NetworkDefinition: NAT Address Range	Network Definition	Common	Edit this BB to define typical Network Address Translation (NAT) range you want to use in your deployment.	
BB:NetworkDefinition: Server Networks	Network Definition	Common	Edit this BB to include the networks where your servers are located.	
BB:NetworkDefinition: Trusted Network Segment	Network Definition	Common	Edit this BB to include event categories that are trusted local networks.	
BB:NetworkDefinition: Undefined IP Space	Network Definition	Common	Edit this BB to include areas of your network that does not contain any valid hosts.	
BB:NetworkDefinition: Untrusted Local Networks	Network Definition	Common	Edit this BB to include untrusted local networks.	
BB:NetworkDefinition: Untrusted Network Segment	Network Definition	Common	Edit this BB to include any untrusted networks.	BB:NetworkDefinition: Untrusted Local Network BB:NetworkDefinition: Inbound Communication from Internet to Local Host

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:NetworkDefinition: Watch List Addresses	Network Definition	Common	Edit this BB to include networks that should be added to a watch list.	
BB:Policy Violation: Application Policy Violation: NNTP to Internet	Policy	Flow	Edit this BB to include applications that are commonly associated with NNTP traffic to the Internet	
BB:Policy Violation: Application Policy Violation: Unknown Local Service	Policy	Flow	Edit this BB to include applications that are commonly associated with potentially unknown local services.	
BB:Policy Violation: Compliance Policy Violation: Clear Text Application Usage	Policy	Flow	Edit this BB to include applications that are commonly associated with unencrypted protocols like telnet and FTP.	
BB: Policy Violation: Connection to Social Networking website	Policy	Flow	Edit this BB to include applications that are commonly associated with social networking websites.	
BB:Policy Violation: IRC IM Policy Violation: IM Communications	Policy	Flow	Edit this BB to include applications that are commonly associated with Instant Messaging communications.	
BB:Policy Violation: IRC IM Policy Violation: IRC Connection to Internet	PolicyRecon	Flow	Edit this BB to include applications that are commonly associated with IRC connections to a remote host.	
BB:Policy Violation: Large Outbound Transfer	Policy	Flow	Edit this BB to include applications that are commonly associated with significant transfer of data to outside the local network. This may indicate suspicious activity.	
BB:Policy Violation: Mail Policy Violation: Outbound Mail Sender	Policy	Flow	Edit this BB to include applications that are commonly associated with a local host sending mail to remote hosts.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Policy Violation: Mail Policy Violation: Remote Connection to Internal Mail Server	Policy	Flow	Edit this BB to include applications that are commonly associated with potential unauthorized internal mail servers.	
BB:Policy Violation: P2P Policy Violation: Local P2P Client	Policy	Flow	Edit this BB to include applications that are commonly associated with local P2P clients. This BB detects flows coming from a local PSP server.	
BB:Policy Violation: P2P Policy Violation: Local P2P Server	Policy	Flow	Edit this BB to include applications that are commonly associated with local P2P clients. This BB detects flows coming from a local P2P client.	
BB:Policy Violation: Remote Access Policy Violation: Remote Access Shell	Policy	Flow	Edit this BB to include applications that are commonly associated with remote access. This BB detects a remote access attempt from a remote host.	
BB:Policy: Application Policy Violation Events	Policy	Event	Edit this BB to define policy application and violation events.	
BB:Policy: IRC/IM Connection Violations	Policy	Event	Edit this BB to define all policy IRC and IM connection violations.	
BB:Policy: Policy P2P	Policy	Event	Edit this BB to include all events that indicate P2P events.	
BB:PortDefinition: Authorized L2R Ports	Port\ Protocol Definition	Common	Edit this BB to include ports that are commonly detected in Local-to-Remote (L2R) traffic.	
BB:PortDefinition: Common Worm Ports	Port\ Protocol Definition	Common	Edit this BB to include all ports that are generally not seen in L2R traffic.	
BB:PortDefinition: Database Ports	Port\ Protocol Definition	Common	Edit this BB to include all common database ports.	
BB:PortDefinition: DHCP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common DHCP ports.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:PortDefinition: DNS Ports	Port\ Protocol Definition	Common	Edit this BB to include all common DNS ports.	
BB:PortDefinition: FTP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common FTP ports.	
BB:PortDefinition: Game Server Ports	Port\ Protocol Definition	Common	Edit this BB to include all common game server ports.	
BB:PortDefinition: IM Ports	Compliance	Common	Edit this BB to include all common IM ports.	
BB:PortDefinition: IRC Ports	Port\ Protocol Definition	Common	Edit this BB to include all common IRC ports.	
BB:PortDefinition: LDAP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by LDAP servers.	
BB:PortDefinition: Mail Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by mail servers.	
BB:PortDefinition: P2P Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by P2P servers.	
BB:PortDefinition: Proxy Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by proxy servers.	
BB:PortDefinition: RPC Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by RPC servers.	
BB:PortDefinition: SNMP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by SNMP servers.	
BB:PortDefinition: SSH Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by SSH servers.	
BB:PortDefinition: Syslog Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by the syslog servers.	
BB:PortDefinition: Web Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by Web servers.	
BB:PortDefinition: Windows Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by Windows servers.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:ProtocolDefinition: Windows Protocols	Port\ Protocol Definition	Common	Edit this BB to include all common protocols (not including TCP) used by Windows servers that will be ignored for false positive tuning rules.	
BB:Recon: Local: ICMP Scan (High)	Recon	Flow	Edit this BB to identify applications and protocols commonly associated with ICMP traffic. This BB detects when a host is scanning more than 100,000 hosts per minute using ICMP. This activity indicates a host performing reconnaissance activity at an extremely high rate. This is typical of a worm infection or a standard scanning application.	BB:Threats: Scanning: ICMP Scan High
BB:Recon: Local: ICMP Scan (Medium)	Recon	Flow	Edit this BB to identify applications and protocols commonly associated with ICMP traffic. This BB detects a host scanning more than 5,000 hosts per minute using ICMP. This indicates a host performing reconnaissance activity at an extremely high rate. This is typical of a worm infection or a host configured for network management purposes.	BB:Threats: Scanning: ICMP Scan Medium
BB:Recon: Local: ICMP Scan (Low)	Recon	Flow	Edit this BB to identify applications and protocols commonly associated with ICMP traffic. This BB detects a host scanning more than 500 hosts per minute using ICMP. This may indicate a host configured for network management or normal server behavior on a busy internal network. If this behavior continues for extended periods of time, this may indicate classic behavior of worm activity.	BB:Threats: Scanning: ICMP Scan Low

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Recon: Local: Potential Network Scan	Recon	Flow	This BB detects a host sending identical packets to a number of hosts that are not responding. This may indicate a host configured for network management or normal server behavior on a busy internal network. However, client hosts in your network should not be exhibiting this behavior for long periods of time.	BB:Threats: Scanning: Potential Scan
BB:Recon: Local: Scanning Activity (High)	Recon	Flow	This BB detects a host performing reconnaissance activity at an extremely high rate (more than 100,000 hosts per minute), which is typical of a worm infection of a scanning application.	BB:Threats: Scanning: Empty Responsive Flows High
BB:Recon: Local: Scanning Activity (Low)	Recon	Flow	This BB detects a host scanning more than 500 hosts per minute. This indicates a host performing reconnaissance activity at a high rate. This is typical of a worm infection or a host configured for network management purposes.	BB:Threats: Scanning: Empty Responsive Flows Low
BB:Recon: Local: Scanning Activity (Medium)	Recon	Flow	This BB detects a host scanning more than 5,000 hosts per minute. This indicates a host performing reconnaissance activity at a high rate. This is typical of a worm infection or a host configured for network management purposes.	BB:Threats: Scanning: Empty Responsive Flows Medium
BB:Recon: Remote: ICMP Scan (High)	Recon	Flow	This BB detects a host scanning more than 100,000 hosts per minute using ICMP. This indicates a host performing reconnaissance activity at an extremely high rate. This is typical of a worm infection or a standard scanning application.	BB:Threats: Scanning: ICMP Scan High

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Recon: Remote: ICMP Scan (Low)	Recon	Flow	This BB detects a host scanning more than 500 hosts per minute using ICMP. This may indicate a host configured for network management or normal server behavior on a busy internal network. If this behavior continues for extended periods of time, this may indicate classic behavior of worm activity. We recommend that you check the host of infection or malware installation.	BB:Threats: Scanning: ICMP Scan Low
BB:Recon: Remote: ICMP Scan (Medium)	Recon	Flow	This BB detects a host scanning more than 5,000 hosts per minute using ICMP. This indicates a host performing reconnaissance activity at an extremely high rate. This is typical of a worm infection or a host configured for network management purposes.	B:Threats: Scanning: ICMP Scan Medium
BB:Recon: Remote: Potential Network Scan	Recon	Flow	This BB detects a host sending identical packets to a number of hosts that are not responding. This may indicate a host configured for network management or normal server behavior on a busy internal network. However, client hosts in your network should not be exhibiting this behavior for long periods of time.	BB:Threats: Scanning: Potential Scan
BB:Recon: Remote: Scanning Activity (High)	Recon	Flow	This BB detects a host performing reconnaissance activity at an extremely high rate (more than 100,000 hosts per minute), which is typical of a worm infection of a scanning application.	BB:Threats: Scanning: Empty Responsive Flows High

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Recon: Remote: Scanning Activity (Low)	Recon	Flow	This BB detects a host scanning more than 500 hosts per minute. This indicates a host performing reconnaissance activity at a high rate. This is typical of a worm infection or a host configured for network management purposes.	BB:Threats: Scanning: Empty Responsive Flows Low
BB:Recon: Remote: Scanning Activity (Medium)	Recon	Flow	This BB detects a host scanning more than 5,000 hosts per minute. This indicates a host performing reconnaissance activity at a high rate. This is typical of a worm infection or a host configured for network management purposes.	BB:Threats: Scanning: Empty Responsive Flows Medium
BB:Recon Detected: All Recon Rules	Recon	Event	Edit this BB to define all IBM default reconnaissance tests. This BB is used to detect a host that has performed reconnaissance such that other follow on tests can be performed. For example, reconnaissance followed by firewall accept.	
BB:Recon Detected: Devices That Merge Recon into Single Events	Recon	Event	Edit this BB to include all devices that accumulate reconnaissance across multiple hosts or ports into a single event. This rule forces these events to become offenses.	
BB:Recon Detected: Host Port Scan	Recon	Event	Edit this BB to define reconnaissance scans on hosts in your deployment.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Recon Detected: Port Scan Detected Across Multiple Hosts	Recon	Event	Edit this BB to indicate port scanning activity across multiple hosts. By default, this BB applies when a source IP address is performing reconnaissance against more than five hosts within 10 minutes. If internal, this may indicate an exploited system or a worm scanning for destination IP addresses.	
BB:Suspicious: Local: Anomalous ICMP Flows	Suspicious	Flow	This BB detects an excessive number of ICMP flows from one source IP address, where the applied ICMP types and codes are considered abnormal when seen entering or leaving the network.	BB:Threats: Suspicious IP Protocol Usage: Suspicious ICMP Type Code
BB:Suspicious: Local: Inbound Unidirectional Flows Threshold	Suspicious	Flow	This BB detects an excessive rate (more than 1,000) of unidirectional flows within the last 5 minutes. This may indicate a scan is in progress, worms, DoS attack, or issues with your network configuration.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc Flows BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Local: Invalid TCP Flag Usage	Suspicious	Flow	This BB detects flows that appear to have improper flag combinations. This may indicate various behaviors, such as OS detection, DoS attacks, or even forms of reconnaissance.	BB:Threats: Suspicious IP Protocol Usage: Illegal TCP Flag Combination

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Suspicious: Local: Outbound Unidirectional Flows Threshold	Suspicious	Flow	This BB detects an excessive rate of outbound unidirectional flows (remote host not responding) within 5 minutes.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc Flows BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows B:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Local: Port 0 Flows Detected	Suspicious	Flow	This BB detects flows with Port 0 as the destination or source port. This may be considered suspicious.	BB:Threats: Suspicious IP Protocol Usage: TCP or UDP Port 0
BB:Suspicious: Local: Rejected Communication Attempts	Suspicious	Flow	This BB detects flows that indicate a host is attempting to establish connections to other hosts and is being refused by the hosts.	BB:Threats: Suspicious IP Protocol Usage: Zero Payload Bidirectional Flows
BB:Suspicious: Local: Suspicious IRC Traffic	Suspicious	Flow	This BB detects suspicious IRC traffic.	BB:Threats: Suspicious Activity: Suspicious IRC Ports BB:Threats: Suspicious Activity: Suspicious IRC Traffic
BB:Suspicious: Local: Unidirectional ICMP Detected	Suspicious	Flow	This BB detects excessive unidirectional ICMP traffic from a single source. This may indicate an attempt to enumerate hosts on the network or other serious network issues.	BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Local: Unidirectional ICMP Responses Detected	Suspicious	Flow	This BB detects excessive unidirectional ICMP responses from a single source. This may indicate an attempt to enumerate hosts on the network or other serious network issues.	BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Replies

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Suspicious: Local: Unidirectional TCP Flows	Suspicious	Flow	This BB detects flows that indicate a host is sending an excessive quantity (at least 15) of unidirectional flows. These types of flows may be considered normal, however, client workstations and other devices, should not be seen emitting large quantities of such flows. This activity should be considered suspicious.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows
BB:Suspicious: Local: Unidirectional UDP or Misc Flows	Suspicious	Flow	This BB detects an excessive number of unidirectional UDP and miscellaneous flows from a single source.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows
BB:Suspicious: Remote: Anomalous ICMP Flows	Suspicious	Flow	This BB detects an excessive number of ICMP flows from one source IP address and the applied ICMP types and codes are considered abnormal when seen entering or leaving the network.	BB:Threats: Suspicious IP Protocol Usage: Suspicious ICMP Type Code
BB:Suspicious: Remote: Inbound Unidirectional Flows Threshold	Suspicious	Flow	This BB detects an excessive rate (more than 1,000) of unidirectional flows within the last 5 minutes. This may indicate a scan is in progress, worms, DoS attack, or issues with your network configuration.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc Flows BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Remote: Invalid TCP Flag Usage	Suspicious	Flow	This BB detects flows that appear to have improper flag combinations. This may indicate various troubling behaviors, such as OS detection, DoS attacks, or reconnaissance.	BB:Threats: Suspicious IP Protocol Usage: Illegal TCP Flag Combination

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Suspicious: Remote: Outbound Unidirectional Flows Threshold	Suspicious	Flow	This BB detects an excessive rate of outbound unidirectional flows (remote host not responding) within 5 minutes.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc Flows BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Remote: Port 0 Flows Detected	Suspicious	Flow	This BB detects flows with Port 0 as the destination or source port. This may be considered suspicious.	BB:Threats: Suspicious IP Protocol Usage: TCP or UDP Port 0
BB:Suspicious: Remote: Rejected Communications Attempts	Suspicious	Flow	This BB detects flows that indicate a host is attempting to establish connections to other hosts and is being refused by the hosts.	BB:Threats: Suspicious IP Protocol Usage: Zero Payload Bidirectional Flows
BB:Suspicious: Remote: Suspicious IRC Traffic	Suspicious	Flow	This BB detects suspicious IRC traffic.	BB:Threats: Suspicious Activity: Suspicious IRC Ports BB:Threats: Suspicious Activity: Suspicious IRC Traffic
BB:Suspicious: Remote: Unidirectional ICMP Detected	Suspicious	Flow	This BB detects excessive unidirectional ICMP traffic from a single source. This may indicate an attempt to enumerate hosts on the network or other serious network issues.	BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows
BB:Suspicious: Remote: Unidirectional ICMP Responses Detected	Suspicious	Flow	This BB detects excessive unidirectional ICMP responses from a single source. This may indicate an attempt to enumerate hosts on the network or other serious network issues.	BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Replies

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Suspicious: Remote: Unidirectional TCP Flows	Suspicious	Flow	This BB detects flows that indicate a host is sending an excessive quantity (at least 15) of unidirectional flows. These types of flows may be considered normal, however, client workstations and other devices, should not be seen emitting large quantities of such flows. This activity should be considered suspicious.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows
BB:Suspicious: Remote: Unidirectional UDP or Misc Flows	Suspicious	Flow	This BB detects an excessive number of unidirectional UDP and miscellaneous flows from a single source.	BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows
BB:Threats: DoS: Inbound Flood with No Response High	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 6,000,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Inbound Flood with No Response Low	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 30,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Inbound Flood with No Response Medium	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 300,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Multi-Host Attack High	Threats	Flow	This BB detects a high number of hosts potentially performing a denial of service attack.	
BB:Threats: DoS: Multi-Host Attack Low	Threats	Flow	This BB detects a lower number of hosts potentially performing a denial of service attack.	
BB:Threats: DoS: Multi-Host Attack Medium	Threats	Flow	This BB detects a medium number of hosts potentially performing a denial of service attack.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Threats: DoS: Outbound Flood with No Response High	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 6,000,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Outbound Flood with No Response Low	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 30,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Outbound Flood with No Response Medium	Threats	Flow	This BB detects a denial of service condition where the source packet count is greater than 300,000 and there is no response from the hosts being targeted.	
BB:Threats: DoS: Potential ICMP DoS	Threats	Flow	This BB detects potential a potential ICMP DoS attacks.	
BB:Threats: DoS: Potential Multihost Attack	Threats	Flow	This BB detects multiple hosts potentially performing a denial of service attack.	
BB:Threats: DoS: Potential TCP DoS	Threats	Flow	This BB detects potential a potential TCP DoS attacks.	
BB:Threats: DoS: Potential UDP DoS	Threats	Flow	This BB detects potential a potential UDP DoS attacks.	
BB:Threats: Port Scans: Host Scans	Threats	Flow	This BB detects potential reconnaissance by flows.	
BB:Threats: Port Scans: UDP Port Scan	Threats	Flow	This BB detects UDP based port scans.	
BB:Threats: Remote Access Violations: Remote Desktop Access from Remote Hosts	Threats	Flow	This BB detects flows where a remote desktop application is being accessed from a remote host.	
BB:Threats: Remote Access Violations: VNC Activity from Remote Hosts	Threats	Flow	This BB detects flows where a VNC service is being accessed from a remote host.	
BB:Threats: Scanning: Empty Responsive Flows High	Threats	Flow	This BB detects potential reconnaissance activity where the source packet count is greater than 100,000.	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Threats: Scanning: Empty Responsive Flows Low	Threats	Flow	This BB detects potential reconnaissance activity where the source packet count is greater than 500.	
BB:Threats: Scanning: Empty Responsive Flows Medium	Threats	Flow	This BB detects potential reconnaissance activity where the source packet count is greater than 5,000.	
BB:Threats: Scanning: ICMP Scan High	Threats	Flow	This BB detects a high level of ICMP reconnaissance activity.	
BB:Threats: Scanning: ICMP Scan Low	Threats	Flow	This BB detects a low level of ICMP reconnaissance activity.	
BB:Threats: Scanning: ICMP Scan Medium	Threats	Flow	This BB detects a medium level of ICMP reconnaissance activity.	
BB:Threats: Scanning: Potential Scan	Threats	Flow	This BB detects potential reconnaissance activity.	
BB:Threats: Scanning: Scan High	Threats	Flow	This BB detects a high level of potential reconnaissance activity.	
BB:Threats: Scanning: Scan Low	Threats	Flow	This BB detects a low level of potential reconnaissance activity.	
BB:Threats: Scanning: Scan Medium	Threats	Flow	This BB detects a medium level of potential reconnaissance activity.	
BB:Threats: Suspicious Activity: Suspicious IRC Traffic	Threats	Flow	This BB detects suspicious IRC traffic.	
BB:Threats: Suspicious IP Protocol Usage: Illegal TCP Flag Combination	Threats	Flow	This BB detects flows that have an illegal TCP flag combination.	
BB:Threats: Suspicious IP Protocol Usage: Large DNS Packets	Threats	Flow	This BB detects abnormally large DNS traffic.	
BB:Threats: Suspicious IP Protocol Usage: Large ICMP Packets	Threats	Flow	This BB detects flows with abnormally large ICMP packets.	
BB:Threats: Suspicious IP Protocol Usage: Long Duration Outbound Flow	Threats	Flow	This BB detects flows that have been active for more than 48 hours	

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
BB:Threats: Suspicious IP Protocol Usage: Suspicious ICMP Type Code	Threats	Flow	This BB detects ICMP flows with suspicious ICMP type codes.	
BB:Threats: Suspicious IP Protocol Usage: TCP or UDP Port 0	Threats	Flow	This BB detects suspicious flows using port 0.	
BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Flows	Threats	Flow	This BB detects unidirectional ICMP flows.	
BB:Threats: Suspicious IP Protocol Usage: Unidirectional ICMP Replies	Threats	Flow	This BB detects traffic where ICMP replies are seen with no request.	
BB:Threats: Suspicious IP Protocol Usage: Zero Payload Bidirectional Flows	Threats	Flow	This BB detects bidirectional traffic that does not include payload.	
BB:Threats: Suspicious IP Protocol Usage:Unidirectional TCP Flows	Threats	Flow	This BB detects unidirectional TCP flows.	
BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc Flows	Threats	Flow	This BB detects unidirectional UDP and other miscellaneous flows.	
User-BB:FalsePositive: User Defined False Positives Tunings	User Tuning	Common	This BB contains any events that you have tuned using the False Positive tuning function. For more information, see the *IBM Security QRadar SIEM Users Guide*.	
User-BB:FalsePositive: Server Type 1 - User Defined False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User-BB:HostDefinition: Server Type 1 - User Defined
User-BB:FalsePositive: Server Type 1 - User Defined False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined in the associated BB.	User-BB:HostDefinition: Server Type 1 - User Defined

Table 15-2 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
User-BB:FalsePositive: User Defined Server Type 2 False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 2 - User Defined
User-BB:FalsePositive: User Defined Server Type 2 False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 2 - User Defined
User-BB:FalsePositive: User Defined Server Type 3 False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 3 - User Defined
User-BB:FalsePositive: User Defined Server Type 3 False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined the associated BB.	User:BB:HostDefinition: Server Type 3 - User Defined
User-BB:HostDefinition: Server Type 1 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the associated BBs.	User-BB:FalsePositives: Server Type 1 - User Defined False Positive Category User-BB:False Positives: Server Type 1 - User Defined False Positive Events
User-BB:HostDefinition: Server Type 2 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the associated BBs.	User-BB:FalsePositives: User Defined Server Type 2 False Positive Category User-BB:False Positives: User Defined Server Type 2 False Positive Events
User-BB:HostDefinition: Server Type 3 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the as defined in the associated BBs.	User-BB:FalsePositives: User Defined Server Type 3 False Positive Category User-BB:False Positives: User Defined Server Type 3 False Positive Events

B VIEWING AUDIT LOGS

Changes made by QRadar SIEM users are recorded in the audit logs. You can view the audit logs to monitor changes to QRadar SIEM and the users performing those changes.

This section includes the following topics:

Audit Log Overview

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches a size of 200 MB. The current log file is named **`audit.log`**. When the file reaches a size of 200 MB, the file is compressed and renamed as follows: **`audit.1.gz, audit.2.gz`**, with the file number incrementing each time a log file is archived. QRadar SIEM stores up to 50 archived log files.

Logged Actions

QRadar SIEM logs the following categories of actions in the audit log file:

NOTE You can view audit log events using the **Log Activity** tab. Table 16-1 provides a record of the logged actions.

Table 16-1 Logged Actions

Category	Action
Administrator Authentication	Log in to the QRadar SIEM Administration Console.
	Log out of the QRadar SIEM Administration Console.
Assets	Delete an asset.
	Delete all assets.
Audit Log Access	Perform a search that includes events with a high-level event category of Audit.

Table 16-1 Logged Actions (continued)

Category	Action
Backup and Recovery	Edit the configuration.
	Initiate the backup.
	Complete the backup.
	Fail the backup.
	Delete the backup.
	Synchronize the backup.
	Cancel the backup.
	Initiate the restore.
	Upload a backup.
	Upload an invalid backup.
	Initiate the restore.
	Purge the backup.
Custom Properties	Add a custom event property.
	Edit a custom event property.
	Delete a custom event property.
	Add a custom flow property.
	Edit a custom flow property.
	Delete a custom flow property.
Chart Configuration	Save flow or event chart configuration.
Custom Property Expressions	Add a custom event property expression.
	Edit a custom event property expression.
	Delete a custom event property expression.
	Add a custom flow property expression.
	Edit a custom flow property expression.
	Delete a custom flow property expression.
Event and Flow Retention Buckets	Add a bucket.
	Delete a bucket.
	Edit a bucket.
	Enable or disable a bucket.
Flow Sources	Add a flow source.
	Edit a flow source.
	Delete a flow source.
Groups	Add a group.
	Delete a group.
	Edit a group.

Table 16-1 Logged Actions (continued)

Category	Action
High Availability	Add an HA host.
	Remove an HA host.
	Set an HA system offline.
	Set an HA system online.
	Restore an HA system.
Index Management	Enable indexing on a property
	Disable indexing on a property
Installation	Install a .rpm package, such as a DSM update.
Log Sources	Add a log source.
	Edit a log source.
	Delete a log source.
	Add a log source group.
	Edit a log source group.
	Delete a log source group.
	Edit the DSM parsing order.
License	Add a license key.
	Edit a license key.
Log Source Extension	Add an log source extension.
	Edit the log source extension.
	Delete a log source extension.
	Upload a log source extension.
	Upload a log source extension successfully.
	Upload an invalid log source extension.
	Download a log source extension.
	Report a log source extension.
	Modify a log sources association to a device or device type.
Offenses	Hide an offense.
	Close an offense.
	Close all offenses.
	Add a destination note.
	Add a source note.
	Add a network note.
	Add an offense note.
	Add a reason for closing offenses.
	Edit a reason for closing offenses.

Table 16-1 Logged Actions (continued)

Category	Action
Protocol Configuration	Add a protocol configuration.
	Delete a protocol configuration.
	Edit a protocol configuration.
QIDmap	Add a QID map entry.
	Edit a QID map entry.
Reference Sets	Create a reference set.
	Edit a reference set.
	Purge elements in a reference set.
	Delete a reference set.
	Add reference set elements.
	Delete reference set elements.
	Delete all reference set elements.
	Import reference set elements.
	Export reference set elements.
Reports	Add a template.
	Delete a template.
	Edit a template.
	Generate a report.
	Delete a report.
	Delete generated content.
	View a generated report.
	Email a generated report.
Root Login	Log in to QRadar SIEM, as root.
	Log out of QRadar SIEM, as root.
Rules	Add a rule.
	Delete a rule.
	Edit a rule.
Scanner	Add a scanner.
	Delete a scanner.
	Edit a scanner.
Scanner Schedule	Add a schedule.
	Edit a schedule.
	Delete a schedule.

Table 16-1 Logged Actions (continued)

Category	Action
Session Authentication	Create a new administration session.
	Terminate an administration session.
	Deny an invalid authentication session.
	Expire a session authentication.
	Create an authentication session.
	Terminate an authentication session.
SIM	Clean a SIM model.
Store and Forward	Add a Store and Forward schedule.
	Edit a Store and Forward schedule.
	Delete a Store and Forward schedule.
Syslog Forwarding	Add a syslog forwarding.
	Delete a syslog forwarding.
	Edit a syslog forwarding.
System Management	Shutdown a system.
	Restart a system.
TNC Recommendations	Create a recommendation.
	Edit a recommendation.
	Delete a recommendation.
User Accounts	Add an account.
	Edit an account.
	Delete an account.
User Authentication	Log in to QRadar SIEM.
	Log out of QRadar SIEM.
User Authentication Ariel	Deny a login attempt.
	Add an Ariel property.
	Delete an Ariel property.
	Edit an Ariel property.
	Add an Ariel property extension.
	Delete an Ariel property extension.
	Edit an Ariel property extension.
User Roles	Add a role.
	Edit a role.
	Delete a role.

Table 16-1 Logged Actions (continued)

Category	Action
VIS	Discover a new host.
	Discover a new operating system.
	Discover a new port.
	Discover a new vulnerability.

Viewing the Log File

To view the audit logs:

Step 1 Using SSH, log in to QRadar SIEM as the root user:

- User Name: **root**
- Password: **<password>**

Step 2 Go to the following directory:

`/var/log/audit`

Step 3 Open the audit log file.

Each entry in the log file displays using the following format:

NOTE The maximum size of any audit message (not including date, time, and host name) is 1024 characters.

`<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>`

Where:

`<date_time>` is the date and time of the activity in the format: Month Date HH:MM:SS.

`<host name>` is the host name of the Console where this activity was logged.

`<user>` is the name of the user that performed the action.

`<IP address>` is the IP address of the user that performed the action.

`(thread ID)` is the identifier of the Java™ thread that logged this activity.

`<category>` is the high-level category of this activity.

`<sub-category>` is the low-level category of this activity.

`<action>` is the activity that occurred.

`<payload>` is the complete record that has changed, if any. This may include a user record or an event rule.

For example:

`Nov  6 12:22:31 localhost.localdomain admin@10.100.100.15 (Session) [Authentication] [User] [Login]`

```
Nov 6 12:22:31 localhost.localdomain jsam@10.100.100.15 (0)
[Configuration] [User Account] [Account Modified]
username=james, password=/oJDuXP7YXUYQ, networks=ALL,
email=sam@q1labs.com, userrole=Admin

Nov 13 10:14:44 localhost.localdomain admin@10.100.45.61 (0)
[Configuration] [FlowSource] [FlowSourceModified] Flowsource(
name="tim", enabled="true", deployed="false",
asymmetrical="false", targetQflow=DeployedComponent(id=3),
flowsourceType=FlowsourceType(id=6),
flowsourceConfig=FlowsourceConfig(id=1))
```

C EVENT CATEGORIES

This document provides information on the types of event categories and the processing of events.

This section includes the following topics:

NOTE The Risk high-level category is only displayed on the QRadar SIEM user interface when IBM Security QRadar Risk Manager is installed.

High-Level Event Categories

The high-level event categories include:

Table 17-1 High-Level Event Categories

Category	Description
Recon	Events relating to scanning and other techniques used to identify network resources, for example, network or host port scans.
DoS	Events relating to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.
Authentication	Events relating to authentication controls, group, or privilege change, for example, log in or log out.
Access	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
Exploit	Events relating to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
Malware	Events relating to viruses, trojans, back door attacks, or other forms of hostile software. This may include a virus, trojan, malicious software, or spyware.
Suspicious Activity	The nature of the threat is unknown but behavior is suspicious including protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known IDS evasion techniques.
System	Events related to system changes, software installation, or status messages.
Policy	Events regarding corporate policy violations or misuse.
CRE	Events generated from an offense or event rule. For more information on creating custom rules, see the *IBM Security QRadar SIEM Administration Guide*.
Potential Exploit	Events relating to potential application exploits and buffer overflow attempts.
SIM Audit	Events relating to user interaction with the Console and administrative functions.
VIS Host Discovery	Events relating to the host, ports, or vulnerabilities that the VIS component discovers.
Application	Events relating to application activity.
Audit	Events relating to audit activity in IBM Security QRadar Risk Manager.
Risk	Events relating to risk activity in IBM Security QRadar Risk Manager Risk Manager.

Recon

The Recon category indicates events relating to scanning and other techniques used to identify network resources. The associated low-level event categories include:

Table 17-2 Recon Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Form of Recon	Indicates an unknown form of reconnaissance.	2
Application Query	Indicates reconnaissance to applications on your system.	3
Host Query	Indicates reconnaissance to a host in your network.	3
Network Sweep	Indicates reconnaissance on your network.	4
Mail Reconnaissance	Indicates reconnaissance on your mail system.	3
Windows Reconnaissance	Indicates reconnaissance for windows.	3
Portmap / RPC Request	Indicates reconnaissance on your portmap or RPC request.	3
Host Port Scan	Indicates a scan occurred on the host ports.	4
RPC Dump	Indicates Remote Procedure Call (RPC) information is removed.	3
DNS Reconnaissance	Indicates reconnaissance on the DNS server.	3
Misc Reconnaissance Event	Indicates a miscellaneous reconnaissance event.	2
Web Reconnaissance	Indicates web reconnaissance on your network.	3
Database Reconnaissance	Indicates database reconnaissance on your network.	3
ICMP Reconnaissance	Indicates reconnaissance on ICMP traffic.	3
UDP Reconnaissance	Indicates reconnaissance on UDP traffic.	3
SNMP Reconnaissance	Indicates reconnaissance on SNMP traffic.	3
ICMP Host Query	Indicates an ICMP host query.	3
UDP Host Query	Indicates a UDP host query.	3
NMAP Reconnaissance	Indicates NMAP reconnaissance.	3
TCP Reconnaissance	Indicates TCP reconnaissance on your network.	3

Table 17-2 Recon Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Unix Reconnaissance	Indicates reconnaissance on your UNIX® network.	3
FTP Reconnaissance	Indicates FTP reconnaissance.	3

DoS

The DoS category indicates events relating to Denial Of Service (DoS) attacks against services or hosts. The associated low-level event categories include:

Table 17-3 DoS Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown DoS Attack	Indicates an unknown DoS attack.	8
ICMP DoS	Indicates an ICMP DoS attack.	9
TCP DoS	Indicates a TCP DoS attack.	9
UDP DoS	Indicates a UDP DoS attack.	9
DNS Service DoS	Indicates a DNS service DoS attack.	8
Web Service DoS	Indicates a web service DoS attack.	8
Mail Service DoS	Indicates a mail server DoS attack.	8
Distributed DoS	Indicates a distributed DoS attack.	9
Misc DoS	Indicates a miscellaneous DoS attack.	8
Unix DoS	Indicates a Unix DoS attack.	8
Windows DoS	Indicates a Windows DoS attack.	8
Database DoS	Indicates a database DoS attack.	8
FTP DoS	Indicates an FTP DoS attack.	8
Infrastructure DoS	Indicates a DoS attack on the infrastructure.	8
Telnet DoS	Indicates a Telnet DoS attack.	8
Brute Force Login	Indicates access to your system through unauthorized methods.	8
High Rate TCP DoS	Indicates a high rate TCP DoS attack.	8
High Rate UDP DoS	Indicates a high rate UDP DoS attack.	8
High Rate ICMP DoS	Indicates a high rate ICMP DoS attack.	8
High Rate DoS	Indicates a high rate DoS attack.	8
Medium Rate TCP DoS	Indicates a medium rate TCP attack.	8
Medium Rate UDP DoS	Indicates a medium rate UDP attack.	8
Medium Rate ICMP DoS	Indicates a medium rate ICMP attack.	8
Medium Rate DoS	Indicates a medium rate DoS attack.	8

Table 17-3 DoS Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Medium Rate DoS	Indicates a medium rate DoS attack.	8
Low Rate TCP DoS	Indicates a low rate TCP DoS attack.	8
Low Rate UDP DoS	Indicates a low rate UDP DoS attack.	8
Low Rate ICMP DoS	Indicates a low rate ICMP DoS attack.	8
Low Rate DoS	Indicates a low rate DoS attack.	8
Distributed High Rate TCP DoS	Indicates a distributed high rate TCP DoS attack.	8
Distributed High Rate UDP DoS	Indicates a distributed high rate UDP DoS attack.	8
Distributed High Rate ICMP DoS	Indicates a distributed high rate ICMP DoS attack.	8
Distributed High Rate DoS	Indicates a distributed high rate DoS attack.	8
Distributed Medium Rate TCP DoS	Indicates a distributed medium rate TCP DoS attack.	8
Distributed Medium Rate UDP DoS	Indicates a distributed medium rate UDP DoS attack.	8
Distributed Medium Rate ICMP DoS	Indicates a distributed medium rate ICMP DoS attack.	8
Distributed Medium Rate DoS	Indicates a distributed medium rate DoS attack.	8
Distributed Low Rate TCP DoS	Indicates a distributed low rate TCP DoS attack.	8
Distributed Low Rate UDP DoS	Indicates a distributed low rate UDP DoS attack.	8
Distributed Low Rate ICMP DoS	Indicates a distributed low rate ICMP DoS attack.	8
Distributed Low Rate DoS	Indicates a distributed low rate DoS attack.	8
High Rate TCP Scan	Indicates a high rate TCP scan.	8
High Rate UDP Scan	Indicates a high rate UDP scan.	8
High Rate ICMP Scan	Indicates a high rate ICMP scan.	8
High Rate Scan	Indicates a high rate scan.	8
Medium Rate TCP Scan	Indicates a medium rate TCP scan.	8
Medium Rate UDP Scan	Indicates a medium rate UDP scan.	8
Medium Rate ICMP Scan	Indicates a medium rate ICMP scan.	8
Medium Rate Scan	Indicates a medium rate scan.	8
Low Rate TCP Scan	Indicates a low rate TCP scan.	8
Low Rate UDP Scan	Indicates a low rate UDP scan.	8

Table 17-3 DoS Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Low Rate ICMP Scan	Indicates a low rate ICMP scan.	8
Low Rate Scan	Indicates a low rate scan.	8
VoIP DoS	Indicates a VoIP DoS attack.	8
Flood	Indicates a Flood attack.	8
TCP Flood	Indicates a TCP flood attack.	8
UDP Flood	Indicates a UDP flood attack.	8
ICMP Flood	Indicates a ICMP flood attack.	8
SYN Flood	Indicates a SYN flood attack.	8
URG Flood	Indicates a flood attack with the urgent (URG) flag on.	8
SYN URG Flood	Indicates a SYN flood attack with the urgent (URG) flag on.	8
SYN FIN Flood	Indicates a SYN FIN flood attack.	8
SYN ACK Flood	Indicates a SYN ACK flood attack.	8

Authentication

The authentication category indicates events relating to authentication, sessions and access controls to monitor users on the network. The associated low-level event categories include:

Table 17-4 Authentication Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Authentication	Indicates unknown authentication.	1
Host Login Succeeded	Indicates a successful host login.	1
Host Login Failed	Indicates the host login has failed.	3
Misc Login Succeeded	Indicates that the login sequence succeeded.	1
Misc Login Failed	Indicates that login sequence failed.	3
Privilege Escalation Failed	Indicates that the privileged escalation failed.	3
Privilege Escalation Succeeded	Indicates that the privilege escalation succeeded.	1
Mail Service Login Succeeded	Indicates that the mail service login succeeded.	1
Mail Service Login Failed	Indicates that the mail service login failed.	3
Auth Server Login Failed	Indicates that the authentication server login failed.	3

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Auth Server Login Succeeded	Indicates that the authentication server login succeeded.	1
Web Service Login Succeeded	Indicates that the web service login succeeded.	1
Web Service Login Failed	Indicates that the web service login failed.	3
Admin Login Successful	Indicates an administrative login has been successful.	1
Admin Login Failure	Indicates the administrative login failed.	3
Suspicious Username	Indicates that a user attempted to access the network using an incorrect user name.	4
Login with username/ password defaults successful	Indicates that a user accessed the network using the default user name and password.	4
Login with username/ password defaults failed	Indicates that a user has been unsuccessful accessing the network using the default user name and password.	4
FTP Login Succeeded	Indicates that the FTP login has been successful.	1
FTP Login Failed	Indicates that the FTP login failed.	3
SSH Login Succeeded	Indicates that the SSH login has been successful.	1
SSH Login Failed	Indicates that the SSH login failed.	2
User Right Assigned	Indicates that user access to network resources has been successfully granted.	1
User Right Removed	Indicates that user access to network resources has been successfully removed.	1
Trusted Domain Added	Indicates that a trusted domain has been successfully added to your deployment.	1
Trusted Domain Removed	Indicates that a trusted domain has been removed from your deployment.	1
System Security Access Granted	Indicates that system security access has been successfully granted.	1
System Security Access Removed	Indicates that system security access has been successfully removed.	1
Policy Added	Indicates that a policy has been successfully added.	1

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Policy Change	Indicates that a policy has been successfully changed.	1
User Account Added	Indicates that a user account has been successfully added.	1
User Account Changed	Indicates a change to an existing user account.	1
Password Change Failed	Indicates that an attempt to change an existing password failed.	3
Password Change Succeeded	Indicates that a password change has been successful.	1
User Account Removed	Indicates that a user account has been successfully removed.	1
Group Member Added	Indicates that a group member has been successfully added.	1
Group Member Removed	Indicates that a group member has been removed.	1
Group Added	Indicates that a group has been successfully added.	1
Group Changed	Indicates a change to an existing group.	1
Group Removed	Indicates a group has been removed.	1
Computer Account Added	Indicates a computer account has been successfully added.	1
Computer Account Changed	Indicates a change to an existing computer account.	1
Computer Account Removed	Indicates a computer account has been successfully removed.	1
Remote Access Login Succeeded	Indicates that access to the network using a remote login has been successful.	1
Remote Access Login Failed	Indicates that an attempt to access the network using a remote login failed.	3
General Authentication Successful	Indicates that the authentication processes has been successful.	1
General Authentication Failed	Indicates that the authentication process failed.	3
Telnet Login Succeeded	Indicates that the telnet login has been successful.	1
Telnet Login Failed	Indicates that the telnet login failed.	3
Suspicious Password	Indicates that a user attempted to login using a suspicious password.	4

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Samba Login Successful	Indicates a user successfully logged in using Samba.	1
Samba Login Failed	Indicates user login failed using Samba.	3
Auth Server Session Opened	Indicates that a communication session with the authentication server has been started.	1
Auth Server Session Closed	Indicates that a communication session with the authentication server has been closed.	1
Firewall Session Closed	Indicates that a firewall session has been closed.	1
Host Logout	Indicates that a host successfully logged out.	1
Misc Logout	Indicates that a user successfully logged out.	1
Auth Server Logout	Indicates that the process to log out of the authentication server has been successful.	1
Web Service Logout	Indicates that the process to log out of the web service has been successful.	1
Admin Logout	Indicates that the administrative user successfully logged out.	1
FTP Logout	Indicates that the process to log out of the FTP service has been successful.	1
SSH Logout	Indicates that the process to log out of the SSH session has been successful.	1
Remote Access Logout	Indicates that the process to log out using remote access has been successful.	1
Telnet Logout	Indicates that the process to log out of the Telnet session has been successful.	1
Samba Logout	Indicates that the process to log out of Samba has been successful.	1
SSH Session Started	Indicates that the SSH login session has been initiated on a host.	1
SSH Session Finished	Indicates the termination of an SSH login session on a host.	1
Admin Session Started	Indicates that a login session has been initiated on a host by an administrative or privileged user.	1

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Admin Session Finished	Indicates the termination of an administrator or privileged users login session on a host.	1
VoIP Login Succeeded	Indicates a successful VoIP service login	1
VoIP Login Failed	Indicates an unsuccessful attempt to access VoIP service.	1
VoIP Logout	Indicates a user logout,	1
VoIP Session Initiated	Indicates the beginning of a VoIP session.	1
VoIP Session Terminated	Indicates the end of a VoIP session.	1
Database Login Succeeded	Indicates a successful database login.	1
Database Login Failure	Indicates a database login attempt failed.	3
IKE Authentication Failed	Indicates a failed Internet Key Exchange (IKE) authentication has been detected.	3
IKE Authentication Succeeded	Indicates a successful IKE authentication has been detected.	1
IKE Session Started	Indicates an IKE session started.	1
IKE Session Ended	Indicates an IKE session ended.	1
IKE Error	Indicates an IKE error message.	1
IKE Status	Indicates IKE status message.	1
RADIUS Session Started	Indicates a RADIUS session started.	1
RADIUS Session Ended	Indicates a RADIUS session ended.	1
RADIUS Session Denied	Indicates a RADIUS session has been denied.	1
RADIUS Session Status	Indicates a RADIUS session status message.	1
RADIUS Authentication Failed	Indicates a RADIUS authentication failure.	3
RADIUS Authentication Successful	Indicates a RADIUS authentication succeeded.	1
TACACS Session Started	Indicates a TACACS session started.	1
TACACS Session Ended	Indicates a TACACS session ended.	1
TACACS Session Denied	Indicates a TACACS session has been denied.	1
TACACS Session Status	Indicates a TACACS session status message.	1

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
TACACS Authentication Successful	Indicates a TACACS authentication succeeded.	1
TACACS Authentication Failed	Indicates a TACACS authentication failure.	1
Deauthenticating Host Succeeded	Indicates that the deauthentication of a host has been successful.	1
Deauthenticating Host Failed	Indicates that the deauthentication of a host failed.	3
Station Authentication Succeeded	Indicates that the station authentication has been successful.	1
Station Authentication Failed	Indicates that the station authentication of a host failed.	3
Station Association Succeeded	Indicates that the station association has been successful.	1
Station Association Failed	Indicates that the station association failed.	3
Station Reassociation Succeeded	Indicates that the station reassociation has been successful.	1
Station Reassociation Failed	Indicates that the station association failed.	3
Disassociating Host Succeeded	Indicates that the disassociating a host has been successful.	1
Disassociating Host Failed	Indicates that the disassociating a host failed.	3
SA Error	Indicates a Security Association (SA) error message.	5
SA Creation Failure	Indicates a Security Association (SA) creation failure.	3
SA Established	Indicates that a Security Association (SA) connection established.	1
SA Rejected	Indicates that a Security Association (SA) connection rejected.	3
Deleting SA	Indicates the deletion of a Security Association (SA).	1
Creating SA	Indicates the creation of a Security Association (SA).	1
Certificate Mismatch	Indicates a certificate mismatch.	3
Credentials Mismatch	Indicates a credentials mismatch.	3
Admin Login Attempt	Indicates an admin login attempt.	2
User Login Attempt	Indicates a user login attempt.	2
User Login Successful	Indicates a successful user login.	1

Table 17-4 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
User Login Failure	Indicates a failed user login.	3

Access

The access category indicates authentication and access controls for monitoring network events. The associated low-level event categories include:

Table 17-5 Access Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Network Communication Event	Indicates an unknown network communication event.	3
Firewall Permit	Indicates access to the firewall has been permitted.	0
Firewall Deny	Indicates access to the firewall has been denied.	4
Flow Context Response	Indicates events from the Classification Engine in response to a SIM request.	5
Misc Network Communication Event	Indicates a miscellaneous communications event.	3
IPS Deny	Indicates Intrusion Prevention Systems (IPS) denied traffic.	4
Firewall Session Opened	Indicates the firewall session has been opened.	0
Firewall Session Closed	Indicates the firewall session has been closed.	0
Dynamic Address Translation Successful	Indicates that dynamic address translation has been successful.	0
No Translation Group Found	Indicates that no translation group has been found.	2
Misc Authorization	Indicates that access has been granted to a miscellaneous authentication server.	2
ACL Permit	Indicates that an Access Control List (ACL) permitted access.	0
ACL Deny	Indicates that an Access Control List (ACL) denied access.	4
Access Permitted	Indicates that access has been permitted.	0
Access Denied	Indicates that access has been denied.	4
Session Opened	Indicates that a session has been opened.	1

Table 17-5 Access Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Session Closed	Indicates that a session has been closed.	1
Session Reset	Indicates that a session has been reset.	3
Session Terminated	Indicates that a session has been terminated.	4
Session Denied	Indicates that a session has been denied.	5
Session in Progress	Indicates that a session is currently in progress.	1
Session Delayed	Indicates that a session has been delayed.	3
Session Queued	Indicates that a session has been queued.	1
Session Inbound	Indicates that a session is inbound.	1
Session Outbound	Indicates that a session is outbound.	1
Unauthorized Access Attempt	Indicates that an unauthorized access attempt has been detected.	6
Misc Application Action Allowed	Indicates that an application action has been permitted.	1
Misc Application Action Denied	Indicates that an application action has been denied.	3
Database Action Allowed	Indicates that a database action has been permitted.	1
Database Action Denied	Indicates that a database action has been denied.	3
FTP Action Allowed	Indicates that a FTP action has been permitted.	1
FTP Action Denied	Indicates that a FTP action has been denied.	3
Object Cached	Indicates an object cached.	1
Object Not Cached	Indicates an object not cached.	1
Rate Limiting	Indicates that the network is rate limiting traffic.	4
No Rate Limiting	Indicates that the network is not rate limiting traffic.	0

Exploit

The exploit category indicates events where a communication or access has occurred. The associated low-level event categories include:

Table 17-6 Exploit Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Exploit Attack	Indicates an unknown exploit attack.	9
Buffer Overflow	Indicates a buffer overflow.	9
DNS Exploit	Indicates a DNS exploit.	9
Telnet Exploit	Indicates a Telnet exploit.	9
Linux Exploit	Indicates a Linux® exploit.	9
Unix Exploit	Indicates a Unix® exploit.	9
Windows Exploit	Indicates a Microsoft® Windows exploit.	9
Mail Exploit	Indicates a mail server exploit.	9
Infrastructure Exploit	Indicates an infrastructure exploit.	9
Misc Exploit	Indicates a miscellaneous exploit.	9
Web Exploit	Indicates a web exploit.	9
Session Hijack	Indicates a session in your network has been interceded.	9
Worm Active	Indicates an active worm.	10
Password Guess/Retrieve	Indicates that a user has requested access to their password information from the database.	9
FTP Exploit	Indicates an FTP exploit.	9
RPC Exploit	Indicates an RPC exploit.	9
SNMP Exploit	Indicates an SNMP exploit.	9
NOOP Exploit	Indicates an NOOP exploit.	9
Samba Exploit	Indicates an Samba exploit.	9
Database Exploit	Indicates a database exploit.	9
SSH Exploit	Indicates an SSH exploit.	9
ICMP Exploit	Indicates an ICMP exploit.	9
UDP Exploit	Indicates a UDP exploit.	9
Browser Exploit	Indicates an exploit on your browser.	9
DHCP Exploit	Indicates a DHCP exploit	9
Remote Access Exploit	Indicates a remote access exploit	9
ActiveX Exploit	Indicates an exploit through an ActiveX application.	9
SQL Injection	Indicates that an SQL injection has occurred.	9

Table 17-6 Exploit Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Cross-Site Scripting	Indicates a cross-site scripting vulnerability.	9
Format String Vulnerability	Indicates a format string vulnerability.	9
Input Validation Exploit	Indicates that an input validation exploit attempt has been detected.	9
Remote Code Execution	Indicates that a remote code execution attempt has been detected.	9
Memory Corruption	Indicates that a memory corruption exploit has been detected.	9
Command Execution	Indicates that a remote command execution attempt has been detected.	9

Malware

The malicious software (malware) category indicates events relating to application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 17-7 Malware Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Malware	Indicates an unknown virus.	4
Backdoor Detected	Indicates that a backdoor to the system has been detected.	9
Hostile Mail Attachment	Indicates a hostile mail attachment.	6
Malicious Software	Indicates a virus.	6
Hostile Software Download	Indicates a hostile software download to your network.	6
Virus Detected	Indicates a virus has been detected.	8
Misc Malware	Indicates miscellaneous malicious software	4
Trojan Detected	Indicates a trojan has been detected.	7
Spyware Detected	Indicates spyware has been detected on your system.	6
Content Scan	Indicates that an attempted scan of your content has been detected.	3
Content Scan Failed	Indicates that a scan of your content has failed.	8
Content Scan Successful	Indicates that a scan of your content has been successful.	3
Content Scan in Progress	Indicates that a scan of your content is currently in progress.	3

Table 17-7 Malware Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Keylogger	Indicates that a key logger has been detected.	7
Adware Detected	Indicates that Ad-Ware has been detected.	4

Suspicious Activity

The suspicious activity category indicates events relating to viruses, trojans, back door attacks, and other forms of hostile software. The associated low-level event categories include:

Table 17-8 Suspicious Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Suspicious Event	Indicates an unknown suspicious event.	3
Suspicious Pattern Detected	Indicates a suspicious pattern has been detected.	3
Content Modified By Firewall	Indicates that content has been modified by the firewall.	3
Invalid Command or Data	Indicates an invalid command or data.	3
Suspicious Packet	Indicates a suspicious packet.	3
Suspicious Activity	Indicates suspicious activity.	3
Suspicious File Name	Indicates a suspicious file name.	3
Suspicious Port Activity	Indicates suspicious port activity.	3
Suspicious Routing	Indicates suspicious routing.	3
Potential Web Vulnerability	Indicates potential web vulnerability.	3
Unknown Evasion Event	Indicates an unknown evasion event.	5
IP Spoof	Indicates an IP spoof.	5
IP Fragmentation	Indicates IP fragmentation.	3
Overlapping IP Fragments	Indicates overlapping IP fragments.	5
IDS Evasion	Indicates an IDS evasion.	5
DNS Protocol Anomaly	Indicates a DNS protocol anomaly.	3
FTP Protocol Anomaly	Indicates an FTP protocol anomaly.	3
Mail Protocol Anomaly	Indicates a mail protocol anomaly.	3
Routing Protocol Anomaly	Indicates a routing protocol anomaly.	3
Web Protocol Anomaly	Indicates a web protocol anomaly.	3
SQL Protocol Anomaly	Indicates an SQL protocol anomaly.	3

Table 17-8 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Executable Code Detected	Indicates that an executable code has been detected.	5
Misc Suspicious Event	Indicates a miscellaneous suspicious event.	3
Information Leak	Indicates an information leak.	1
Potential Mail Vulnerability	Indicates a potential vulnerability in the mail server.	4
Potential Version Vulnerability	Indicates a potential vulnerability in the QRadar SIEM version.	4
Potential FTP Vulnerability	Indicates a potential FTP vulnerability.	4
Potential SSH Vulnerability	Indicates a potential SSH vulnerability.	4
Potential DNS Vulnerability	Indicates a potential vulnerability in the DNS server.	4
Potential SMB Vulnerability	Indicates a potential SMB (Samba) vulnerability.	4
Potential Database Vulnerability	Indicates a potential vulnerability in the database.	4
IP Protocol Anomaly	Indicates a potential IP protocol anomaly	3
Suspicious IP Address	Indicates a suspicious IP address has been detected.	2
Invalid IP Protocol Usage	Indicates an invalid IP protocol.	2
Invalid Protocol	Indicates an invalid protocol.	4
Suspicious Window Events	Indicates a suspicious event with a screen on your desktop.	2
Suspicious ICMP Activity	Indicates suspicious ICMP activity.	2
Potential NFS Vulnerability	Indicates a potential Network File System (NFS) vulnerability.	4
Potential NNTP Vulnerability	Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.	4
Potential RPC Vulnerability	Indicates a potential RPC vulnerability.	4
Potential Telnet Vulnerability	Indicates a potential Telnet vulnerability on your system.	4
Potential SNMP Vulnerability	Indicates a potential SNMP vulnerability.	4
Illegal TCP Flag Combination	Indicates an invalid TCP flag combination has been detected.	5
Suspicious TCP Flag Combination	Indicates a potentially invalid TCP flag combination has been detected.	4

Table 17-8 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Illegal ICMP Protocol Usage	Indicates an invalid use of the ICMP protocol has been detected.	5
Suspicious ICMP Protocol Usage	Indicates a potentially invalid use of the ICMP protocol has been detected.	4
Illegal ICMP Type	Indicates an invalid ICMP type has been detected.	5
Illegal ICMP Code	Indicates an invalid ICMP code has been detected.	5
Suspicious ICMP Type	Indicates a potentially invalid ICMP type has been detected.	4
Suspicious ICMP Code	Indicates a potentially invalid ICMP code has been detected.	4
TCP port 0	Indicates a TCP packet using a reserved port (0) for source or destination.	4
UDP port 0	Indicates a UDP packets using a reserved port (0) for source or destination.	4
Hostile IP	Indicates the use of a known hostile IP address.	4
Watch list IP	Indicates the use of an IP address from a watch list of IP addresses.	4
Known offender IP	Indicates the use of an IP address of a known offender.	4
RFC 1918 (private) IP	Indicates the use of an IP address from a private IP address range.	4
Potential VoIP Vulnerability	Indicates a potential VoIP vulnerability.	4
Blacklist Address	Indicates that an IP address is on the black list.	8
Watchlist Address	Indicates that the IP address is on the list of IP addresses being monitored.	7
Darknet Address	Indicates that the IP address is part of a darknet.	5
Botnet Address	Indicates that the address is part of a botnet.	7
Suspicious Address	Indicates that the IP address should be monitored.	5
Bad Content	Indicates bad content has been detected.	7
Invalid Cert	Indicates an invalid certificate has been detected.	7

Table 17-8 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
User Activity	Indicates that user activity has been detected.	7
Suspicious Protocol Usage	Indicates suspicious protocol usage has been detected.	5
Suspicious BGP Activity	Indicates that suspicious Border Gateway Protocol (BGP) usage has been detected.	5
Route Poisoning	Indicates that route corruption has been detected.	5
ARP Poisoning	Indicates that ARP-cache poisoning has been detected.	5
Rogue Device Detected	Indicates a rogue device has been detected.	5

System

The system category indicates events relating to system changes, software installation, or status messages. The associated low-level event categories include:

Table 17-9 System Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown System Event	Indicates an unknown system event.	1
System Boot	Indicates a system boot.	1
System Configuration	Indicates a change in the system configuration.	1
System Halt	Indicates the system has been halted.	1
System Failure	Indicates a system failure.	6
System Status	Indicates any information event.	1
System Error	Indicates a system error.	3
Misc System Event	Indicates a miscellaneous system event.	1
Service Started	Indicates system services have started.	1
Service Stopped	Indicates system services have stopped.	1
Service Failure	Indicates a system failure.	6
Successful Registry Modification	Indicates that a modification to the registry has been successful.	1
Successful Host-Policy Modification	Indicates that a modification to the host policy has been successful.	1

Table 17-9 System Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Successful File Modification	Indicates that a modification to a file has been successful.	1
Successful Stack Modification	Indicates that a modification to the stack has been successful.	1
Successful Application Modification	Indicates that a modification to the application has been successful.	1
Successful Configuration Modification	Indicates that a modification to the configuration has been successful.	1
Successful Service Modification	Indicates that a modification to a service has been successful.	1
Failed Registry Modification	Indicates that a modification to the registry has failed.	1
Failed Host-Policy Modification	Indicates that a modification to the host policy has failed.	1
Failed File Modification	Indicates that a modification to a file has failed.	1
Failed Stack Modification	Indicates that a modification to the stack has failed.	1
Failed Application Modification	Indicates that a modification to an application has failed.	1
Failed Configuration Modification	Indicates that a modification to the configuration has failed.	1
Failed Service Modification	Indicates that a modification to the service has failed.	1
Registry Addition	Indicates that an new item has been added to the registry.	1
Host-Policy Created	Indicates that a new entry has been added to the registry.	1
File Created	Indicates that a new has been created in the system.	1
Application Installed	Indicates that a new application has been installed on the system.	1
Service Installed	Indicates that a new service has been installed on the system.	1
Registry Deletion	Indicates that a registry entry has been deleted.	1
Host-Policy Deleted	Indicates that a host policy entry has been deleted.	1
File Deleted	Indicates that a file has been deleted.	1
Application Uninstalled	Indicates that an application has been uninstalled.	1

Table 17-9 System Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Service Uninstalled	Indicates that a service has been uninstalled.	1
System Informational	Indicates system information.	3
System Action Allow	Indicates that an attempted action on the system has been authorized.	3
System Action Deny	Indicates that an attempted action on the system has been denied.	4
Cron	Indicates a crontab message.	1
Cron Status	Indicates a crontab status message.	1
Cron Failed	Indicates a crontab failure message.	4
Cron Successful	Indicates a crontab success message.	1
Daemon	Indicates a daemon message.	1
Daemon Status	Indicates a daemon status message.	1
Daemon Failed	Indicates a daemon failure message.	4
Daemon Successful	Indicates a daemon success message.	1
Kernel	Indicates a kernel message.	1
Kernel Status	Indicates a kernel status message.	1
Kernel Failed	Indicates a kernel failure message.	
Kernel Successful	Indicates a kernel successful message.	1
Authentication	Indicates an authentication message.	1
Information	Indicates an informational message.	2
Notice	Indicates a notice message.	3
Warning	Indicates a warning message.	5
Error	Indicates an error message.	7
Critical	Indicates a critical message.	9
Debug	Indicates a debug message.	1
Messages	Indicates a generic message.	1
Privilege Access	Indicates that privilege access has been attempted.	3
Alert	Indicates an alert message.	9
Emergency	Indicates an emergency message.	9
SNMP Status	Indicates an SNMP status message.	1
FTP Status	Indicates an FTP status message.	1
NTP Status	Indicates an NTP status message.	1
Access Point Radio Failure	Indicates an access point radio failure.	3

Table 17-9 System Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Encryption Protocol Configuration Mismatch	Indicates an encryption protocol configuration mismatch.	3
Client Device or Authentication Server Misconfigured	Indicates a client device or authentication server has been not configured properly.	5
Hot Standby Enable Failed	Indicates a hot standby enable failure.	5
Hot Standby Disable Failed	Indicates a hot standby disable failure.	5
Hot Standby Enabled Successfully	Indicates hot standby has been enabled successfully.	1
Hot Standby Association Lost	Indicates a hot standby association has been lost.	5
MainMode Initiation Failure	Indicates MainMode initiation failure.	5
MainMode Initiation Succeeded	Indicates that the MainMode initiation has been successful.	1
MainMode Status	Indicates a MainMode status message has been reported.	1
QuickMode Initiation Failure	Indicates that the QuickMode initiation failed.	5
Quickmode Initiation Succeeded	Indicates that the QuickMode initiation has been successful.	1
Quickmode Status	Indicates a QuickMode status message has been reported.	1
Invalid License	Indicates an invalid license.	3
License Expired	Indicates an expired license.	3
New License Applied	Indicates a new license applied.	1
License Error	Indicates a license error.	5
License Status	Indicates a license status message.	1
Configuration Error	Indicates that a configuration error has been detected.	5
Service Disruption	Indicates that a service disruption has been detected.	5
License Exceeded	Indicates that the license capabilities have been exceeded.	3
Performance Status	Indicates that the performance status has been reported.	1
Performance Degradation	Indicates that the performance is being degraded.	4
Misconfiguration	Indicates that a incorrect configuration has been detected.	5

Policy

The policy category indicates events relating to administration of network policy and the monitoring network resources for policy violations. The associated low-level event categories include:

Table 17-10 Policy Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Policy Violation	Indicates an unknown policy violation.	2
Web Policy Violation	Indicates a web policy violation.	2
Remote Access Policy Violation	Indicates a remote access policy violation.	2
IRC/IM Policy Violation	Indicates an instant messenger policy violation.	2
P2P Policy Violation	Indicates a Peer-to-Peer (P2P) policy violation.	2
IP Access Policy Violation	Indicates an IP access policy violation.	2
Application Policy Violation	Indicates an application policy violation.	2
Database Policy Violation	Indicates a database policy violation.	2
Network Threshold Policy Violation	Indicates a network threshold policy violation.	2
Porn Policy Violation	Indicates a porn policy violation.	2
Games Policy Violation	Indicates a games policy violation.	2
Misc Policy Violation	Indicates a miscellaneous policy violation.	2
Compliance Policy Violation	Indicates a compliance policy violation.	2
Mail Policy Violation	Indicates a mail policy violation.	2
IRC Policy Violation	Indicates an IRC policy violation	2
IM Policy Violation	Indicates a policy violation related to instant messaging (IM) activities.	2
VoIP Policy Violation	Indicates a VoIP policy violation	2
Succeeded	Indicates a policy successful message.	1
Failed	Indicates a policy failure message.	4

CRE

The CRE category indicates events generated from a custom offense, flow or event rule. The associated low-level event categories include:

Table 17-11 CRE Category

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown CRE Event	Indicates an unknown custom rules engine event.	5

Table 17-11 CRE Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Single Event Rule Match	Indicates a single event rule match.	5
Event Sequence Rule Match	Indicates an event sequence rule match.	5
Cross-Offense Event Sequence Rule Match	Indicates a cross-offense event sequence rule match.	5
Offense Rule Match	Indicates an offense rule match.	5

Potential Exploit

The Potential Exploit category indicates events relating to potential application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 17-12 Potential Exploit Category

Low Level Event Category	Description	Severity Level (0 to 10)
Unknown Potential Exploit Attack	Indicates a potential exploitative attack has been detected.	7
Potential Buffer Overflow	Indicates a potential buffer overflow has been detected.	7
Potential DNS Exploit	Indicates a potentially exploitative attack through the DNS server has been detected.	7
Potential Telnet Exploit	Indicates a potentially exploitative attack through Telnet has been detected.	7
Potential Linux Exploit	Indicates a potentially exploitative attack through Linux has been detected.	7
Potential Unix Exploit	Indicates a potentially exploitative attack through Unix has been detected.	7
Potential Windows Exploit	Indicates a potentially exploitative attack through Windows has been detected.	7
Potential Mail Exploit	Indicates a potentially exploitative attack through mail has been detected.	7
Potential Infrastructure Exploit	Indicates a potential exploitative attack on the system infrastructure has been detected.	7
Potential Misc Exploit	Indicates a potentially exploitative attack has been detected.	7

Table 17-12 Potential Exploit Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Potential Web Exploit	Indicates a potentially exploitative attack through the web has been detected.	7
Potential Botnet connection	Indicates a potentially exploitative attack using Botnet has been detected.	6
Potential worm activity	Indicates a potentially exploitive attack using worm activity has been detected.	6

SIM Audit

The SIM Audit events category indicates events related to user interaction with the Console and administrative functionality. User login and configuration changes will generate events that are sent to the Event Collector, which correlates with other security events from the network. The associated low-level event categories include:

Table 17-13 SIM Audit Event Category

Low Level Event Category	Description	Severity Level (0 to 10)
SIM User Authentication	Indicates a user login or logout on the Console.	5
SIM Configuration Change	Indicates that a user has made a change to the SIM configuration or deployment.	3
SIM User Action	Indicates that a user has initiated a process in the SIM module. This may include starting a backup process or generated a report.	3
Session Created	Indicates a user session has been created.	3
Session Destroyed	Indicates a user session has been destroyed.	3
Admin Session Created	Indicates an admin session has been created.	
Admin Session Destroyed	Indicates an admin session has been destroyed.	3
Session Authentication Invalid	Indicates an invalid session authentication.	5
Session Authentication Expired	Indicates a session authentication expired.	3

VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities detected on the network, the VIS component generates events. These events are sent to the Event Collector to be correlated with other security events.

The associated low-level event categories include:

Table 17-14 VIS Host Discovery Category

Low Level Event Category	Description	Severity Level (0 to 10)
New Host Discovered	Indicates that the VIS component has detected a new host.	3
New Port Discovered	Indicates that the VIS component has detected a new open port.	3
New Vuln Discovered	Indicates that the VIS component has detected a new vulnerability.	3
New OS Discovered	Indicates that the VIS component has detected a new operating system on a host.	3
Bulk Host Discovered	Indicates that the VIS component has detected many new hosts in a short period of time.	3

Application

The Application category indicates events relating to application activity, such as email or FTP activity. The associated low-level event categories include:

Table 17-15 Application Category

Low Level Event Category	Description	Severity Level (0 to 10)
Mail Opened	Indicates that an email connection has been established.	1
Mail Closed	Indicates that an email connection has been closed.	1
Mail Reset	Indicates that an email connection has been reset.	3
Mail Terminated	Indicates that an email connection has been terminated.	4
Mail Denied	Indicates that an email connection has been denied.	4
Mail in Progress	Indicates that an email connection is being attempted.	1
Mail Delayed	Indicates that an email connection has been delayed.	4
Mail Queued	Indicates that an email connection has been queued.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Mail Redirected	Indicates that an email connection has been redirected.	1
FTP Opened	Indicates that an FTP connection has been opened.	1
FTP Closed	Indicates that an FTP connection has been closed.	1
FTP Reset	Indicates that an FTP connection has been reset.	3
FTP Terminated	Indicates that an FTP connection has been terminated.	4
FTP Denied	Indicates that an FTP connection has been denied.	4
FTP In Progress	Indicates that an FTP connection is currently in progress.	1
FTP Redirected	Indicates that an FTP connection has been redirected.	3
HTTP Opened	Indicates that an HTTP connection has been established.	1
HTTP Closed	Indicates that an HTTP connection has been closed.	1
HTTP Reset	Indicates that an HTTP connection has been reset.	3
HTTP Terminated	Indicates that an HTTP connection has been terminated.	4
HTTP Denied	Indicates that an HTTP connection has been denied.	4
HTTP In Progress	Indicates that an HTTP connection is currently in progress.	1
HTTP Delayed	Indicates that an HTTP connection has been delayed.	3
HTTP Queued	Indicates that an HTTP connection has been queued.	1
HTTP Redirected	Indicates that an HTTP connection has been redirected.	1
HTTP Proxy	Indicates that an HTTP connection is being proxied.	1
HTTPS Opened	Indicates that an HTTPS connection has been established.	1
HTTPS Closed	Indicates that an HTTPS connection has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
HTTPS Reset	Indicates that an HTTPS connection has been reset.	3
HTTPS Terminated	Indicates that an HTTPS connection has been terminated.	4
HTTPS Denied	Indicates that an HTTPS connection has been denied.	4
HTTPS In Progress	Indicates that an HTTPS connection is currently in progress.	1
HTTPS Delayed	Indicates that an HTTPS connection has been delayed.	3
HTTPS Queued	Indicates that an HTTPS connection has been queued.	3
HTTPS Redirected	Indicates that an HTTPS connection has been redirected.	3
HTTPS Proxy	Indicates that an HTTPS connection is proxied.	1
SSH Opened	Indicates than an SSH connection has been established.	1
SSH Closed	Indicates that an SSH connection has been closed.	1
SSH Reset	Indicates that an SSH connection has been reset.	3
SSH Terminated	Indicates that an SSH connection has been terminated.	4
SSH Denied	Indicates that an SSH session has been denied.	4
SSH In Progress	Indicates that an SSH session is currently in progress.	1
RemoteAccess Opened	Indicates that a remote access connection has been established.	1
RemoteAccess Closed	Indicates that a remote access connection has been closed.	1
RemoteAccess Reset	Indicates that a remote access connection has been reset.	3
RemoteAccess Terminated	Indicates that a remote access connection has been terminated.	4
RemoteAccess Denied	Indicates that a remote access connection has been denied.	4
RemoteAccess In Progress	Indicates that a remote access connection is currently in progress.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
RemoteAccess Delayed	Indicates that a remote access connection has been delayed.	3
RemoteAccess Redirected	Indicates that a remote access connection has been redirected.	3
VPN Opened	Indicates that a VPN connection has been opened.	1
VPN Closed	Indicates that a VPN connection has been closed.	1
VPN Reset	Indicates that a VPN connection has been reset.	3
VPN Terminated	Indicates that a VPN connection has been terminated.	4
VPN Denied	Indicates that a VPN connection has been denied.	4
VPN In Progress	Indicates that a VPN connection is currently in progress.	1
VPN Delayed	Indicates that a VPN connection has been delayed	3
VPN Queued	Indicates that a VPN connection has been queued.	3
VPN Redirected	Indicates that a VPN connection has been redirected.	3
RDP Opened	Indicates that an RDP connection has been established.	1
RDP Closed	Indicates that an RDP connection has been closed.	1
RDP Reset	Indicates that an RDP connection has been reset.	3
RDP Terminated	Indicates that an RDP connection has been terminated.	4
RDP Denied	Indicates that an RDP connection has been denied.	4
RDP In Progress	Indicates that an RDP connection is currently in progress.	1
RDP Redirected	Indicates that an RDP connection has been redirected.	3
FileTransfer Opened	Indicates that a file transfer connection has been established.	1
FileTransfer Closed	Indicates that a file transfer connection has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
FileTransfer Reset	Indicates that a file transfer connection has been reset.	3
FileTransfer Terminated	Indicates that a file transfer connection has been terminated.	4
FileTransfer Denied	Indicates that a file transfer connection has been denied.	4
FileTransfer In Progress	Indicates that a file transfer connection is currently in progress.	1
FileTransfer Delayed	Indicates that a file transfer connection has been delayed.	3
FileTransfer Queued	Indicates that a file transfer connection has been queued.	3
FileTransfer Redirected	Indicates that a file transfer connection has been redirected.	3
DNS Opened	Indicates that a DNS connection has been established.	1
DNS Closed	Indicates that a DNS connection has been closed.	1
DNS Reset	Indicates that a DNS connection has been reset.	5
DNS Terminated	Indicates that a DNS connection has been terminated.	5
DNS Denied	Indicates that a DNS connection has been denied.	5
DNS In Progress	Indicates that a DNS connection is currently in progress.	1
DNS Delayed	Indicates that a DNS connection has been delayed.	5
DNS Redirected	Indicates that a DNS connection has been redirected.	4
Chat Opened	Indicates that a chat connection has been opened.	1
Chat Closed	Indicates that a chat connection has been closed.	1
Chat Reset	Indicates that a chat connection has been reset.	3
Chat Terminated	Indicates that a chat connection has been terminated.	3
Chat Denied	Indicates that a chat connection has been denied.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Chat In Progress	Indicates that a chat connection is currently in progress.	1
Chat Redirected	Indicates that a chat connection has been redirected.	1
Database Opened	Indicates that a database connection has been established.	1
Database Closed	Indicates that a database connection has been closed.	1
Database Reset	Indicates that a database connection has been reset.	5
Database Terminated	Indicates that a database connection has been terminated.	5
Database Denied	Indicates that a database connection has been denied.	5
Database In Progress	Indicates that a database connection is currently in progress.	1
Database Redirected	Indicates that a database connection has been redirected.	3
SMTP Opened	Indicates that an SMTP connection has been established.	1
SMTP Closed	Indicates that an SMTP connection has been closed.	1
SMTP Reset	Indicates that an SMTP connection has been reset.	3
SMTP Terminated	Indicates that an SMTP connection has been terminated.	5
SMTP Denied	Indicates that an SMTP connection has been denied.	5
SMTP In Progress	Indicates that an SMTP connection is currently in progress.	1
SMTP Delayed	Indicates that an SMTP connection has been delayed.	3
SMTP Queued	Indicates that an SMTP connection has been queued.	3
SMTP Redirected	Indicates that an SMTP connection has been redirected.	3
Auth Opened	Indicates that an authorization server connection has been established.	1
Auth Closed	Indicates that an authorization server connection has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Auth Reset	Indicates that an authorization server connection has been reset.	3
Auth Terminated	Indicates that an authorization server connection has been terminated.	4
Auth Denied	Indicates that an authorization server connection has been denied.	4
Auth In Progress	Indicates that an authorization server connection is currently in progress.	1
Auth Delayed	Indicates that an authorization server connection has been delayed.	3
Auth Queued	Indicates that an authorization server connection has been queued.	3
Auth Redirected	Indicates that an authorization server connection has been redirected.	2
P2P Opened	Indicates that a Peer-to-Peer (P2P) connection has been established.	1
P2P Closed	Indicates that a P2P connection has been closed.	1
P2P Reset	Indicates that a P2P connection has been reset.	4
P2P Terminated	Indicates that a P2P connection has been terminated.	4
P2P Denied	Indicates that a P2P connection has been denied.	3
P2P In Progress	Indicates that a P2P connection is currently in progress.	1
Web Opened	Indicates that a web connection has been established.	1
Web Closed	Indicates that a web connection has been closed.	1
Web Reset	Indicates that a web connection has been reset.	4
Web Terminated	Indicates that a web connection has been terminated.	4
Web Denied	Indicates that a web connection has been denied.	4
Web In Progress	Indicates that a web connection is currently in progress.	1
Web Delayed	Indicates that a web connection has been delayed.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Web Queued	Indicates that a web connection has been queued.	1
Web Redirected	Indicates that a web connection has been redirected.	1
Web Proxy	Indicates that a web connection has been proxied.	1
VoIP Opened	Indicates that a Voice Over IP (VoIP) connection has been established.	1
VoIP Closed	Indicates that a VoIP connection has been closed.	1
VoIP Reset	Indicates that a VoIP connection has been reset.	3
VoIP Terminated	Indicates that a VoIP connection has been terminated.	3
VoIP Denied	Indicates that a VoIP connection has been denied.	3
VoIP In Progress	Indicates that a VoIP connection is currently in progress.	1
VoIP Delayed	Indicates that a VoIP connection has been delayed.	3
VoIP Redirected	Indicates that a VoIP connection has been redirected.	3
LDAP Session Started	Indicates a LDAP session has started.	1
LDAP Session Ended	Indicates a LDAP session has ended.	1
LDAP Session Denied	Indicates a LDAP session has been denied.	3
LDAP Session Status	Indicates a LDAP session status message has been reported.	1
LDAP Authentication Failed	Indicates a LDAP authentication has failed.	4
LDAP Authentication Succeeded	Indicates a LDAP authentication has been successful.	1
AAA Session Started	Indicates that an Authentication, Authorization and Accounting (AAA) session has started.	1
AAA Session Ended	Indicates that an AAA session has ended.	1
AAA Session Denied	Indicates that an AAA session has been denied.	3
AAA Session Status	Indicates that an AAA session status message has been reported.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
AAA Authentication Failed	Indicates that an AAA authentication has failed.	4
AAA Authentication Succeeded	Indicates that an AAA authentication has been successful.	1
IPSEC Authentication Failed	Indicates that an Internet Protocol Security (IPSEC) authentication has failed.	4
IPSEC Authentication Succeeded	Indicates that an IPSEC authentication has been successful.	1
IPSEC Session Started	Indicates that an IPSEC session has started.	1
IPSEC Session Ended	Indicates that an IPSEC session has ended.	1
IPSEC Error	Indicates that an IPSEC error message has been reported.	5
IPSEC Status	Indicates that an IPSEC session status message has been reported.	1
IM Session Opened	Indicates that an Instant Messenger (IM) session has been established.	1
IM Session Closed	Indicates that an IM session has been closed.	1
IM Session Reset	Indicates that an IM session has been reset.	3
IM Session Terminated	Indicates that an IM session has been terminated.	3
IM Session Denied	Indicates that an IM session has been denied.	3
IM Session In Progress	Indicates that an IM session is in progress.	1
IM Session Delayed	Indicates that an IM session has been delayed	3
IM Session Redirected	Indicates that an IM session has been redirected.	3
WHOIS Session Opened	Indicates that a WHOIS session has been established.	1
WHOIS Session Closed	Indicates that a WHOIS session has been closed.	1
WHOIS Session Reset	Indicates that a WHOIS session has been reset.	3
WHOIS Session Terminated	Indicates that a WHOIS session has been terminated.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
WHOIS Session Denied	Indicates that a WHOIS session has been denied.	3
WHOIS Session In Progress	Indicates that a WHOIS session is in progress.	1
WHOIS Session Redirected	Indicates that a WHOIS session has been redirected.	3
Traceroute Session Opened	Indicates that a Traceroute session has been established.	1
Traceroute Session Closed	Indicates that a Traceroute session has been closed.	1
Traceroute Session Denied	Indicates that a Traceroute session has been denied.	3
Traceroute Session In Progress	Indicates that a Traceroute session is in progress.	1
TN3270 Session Opened	TN3270 is a terminal emulation program, which is used to connect to an IBM 3270 terminal. This category indicates that a TN3270 session has been established.	1
TN3270 Session Closed	Indicates that a TN3270 session has been closed.	1
TN3270 Session Reset	Indicates that a TN3270 session has been reset.	3
TN3270 Session Terminated	Indicates that a TN3270 session has been terminated.	3
TN3270 Session Denied	Indicates that a TN3270 session has been denied.	3
TN3270 Session In Progress	Indicates that a TN3270 session is in progress.	1
TFTP Session Opened	Indicates that a TFTP session has been established.	1
TFTP Session Closed	Indicates that a TFTP session has been closed.	1
TFTP Session Reset	Indicates that a TFTP session has been reset.	3
TFTP Session Terminated	Indicates that a TFTP session has been terminated.	3
TFTP Session Denied	Indicates that a TFTP session has been denied.	3
TFTP Session In Progress	Indicates that a TFTP session is in progress.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Telnet Session Opened	Indicates that a Telnet session has been established.	1
Telnet Session Closed	Indicates that a Telnet session has been closed.	1
Telnet Session Reset	Indicates that a Telnet session has been reset.	3
Telnet Session Terminated	Indicates that a Telnet session has been terminated.	3
Telnet Session Denied	Indicates that a Telnet session has been denied.	3
Telnet Session In Progress	Indicates that a Telnet session is in progress.	1
Syslog Session Opened	Indicates that a syslog session has been established.	1
Syslog Session Closed	Indicates that a syslog session has been closed.	1
Syslog Session Denied	Indicates that a syslog session has been denied.	3
Syslog Session In Progress	Indicates that a syslog session is in progress.	1
SSL Session Opened	Indicates that a Secure Socket Layer (SSL) session has been established.	1
SSL Session Closed	Indicates that an SSL session has been closed.	1
SSL Session Reset	Indicates that an SSL session has been reset.	3
SSL Session Terminated	Indicates that an SSL session has been terminated.	3
SSL Session Denied	Indicates that an SSL session has been denied.	3
SSL Session In Progress	Indicates that an SSL session is in progress.	1
SNMP Session Opened	Indicates that a Simple Network Management Protocol (SNMP) session has been established.	1
SNMP Session Closed	Indicates that an SNMP session has been closed.	1
SNMP Session Denied	Indicates that an SNMP session has been denied.	3
SNMP Session In Progress	Indicates that an SNMP session is in progress.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
SMB Session Opened	Indicates that a Server Message Block (SMB) session has been established.	1
SMB Session Closed	Indicates that an SMB session has been closed.	1
SMB Session Reset	Indicates that an SMB session has been reset.	3
SMB Session Terminated	Indicates that an SMB session has been terminated.	3
SMB Session Denied	Indicates that an SMB session has been denied.	3
SMB Session In Progress	Indicates that an SMB session is in progress.	1
Streaming Media Session Opened	Indicates that a Streaming Media session has been established.	1
Streaming Media Session Closed	Indicates that a Streaming Media session has been closed.	1
Streaming Media Session Reset	Indicates that a Streaming Media session has been reset.	3
Streaming Media Session Terminated	Indicates that a Streaming Media session has been terminated.	3
Streaming Media Session Denied	Indicates that a Streaming Media session has been denied.	3
Streaming Media Session In Progress	Indicates that a Streaming Media session is in progress.	1
RUSERS Session Opened	Indicates that a (Remote Users) RUSERS session has been established.	1
RUSERS Session Closed	Indicates that a RUSERS session has been closed.	1
RUSERS Session Denied	Indicates that a RUSERS session has been denied.	3
RUSERS Session In Progress	Indicates that a RUSERS session is in progress.	1
RSH Session Opened	Indicates that a Remote Shell (RSH) session has been established.	1
RSH Session Closed	Indicates that an RSH session has been closed.	1
RSH Session Reset	Indicates that an RSH session has been reset.	3
RSH Session Terminated	Indicates that an RSH session has been terminated.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
RSH Session Denied	Indicates that an RSH session has been denied.	3
RSH Session In Progress	Indicates that an RSH session is in progress.	1
RLOGIN Session Opened	Indicates that a Remote Login (RLOGIN) session has been established.	1
RLOGIN Session Closed	Indicates that an RLOGIN session has been closed.	1
RLOGIN Session Reset	Indicates that an RLOGIN session has been reset.	3
RLOGIN Session Terminated	Indicates that an RLOGIN session has been terminated.	3
RLOGIN Session Denied	Indicates that an RLOGIN session has been denied.	3
RLOGIN Session In Progress	Indicates that an RLOGIN session is in progress.	1
REXEC Session Opened	Indicates that a (Remote Execution) REXEC session has been established.	1
REXEC Session Closed	Indicates that an REXEC session has been closed.	1
REXEC Session Reset	Indicates that an REXEC session has been reset.	3
REXEC Session Terminated	Indicates that an REXEC session has been terminated.	3
REXEC Session Denied	Indicates that an REXEC session has been denied.	3
REXEC Session In Progress	Indicates that an REXEC session is in progress.	1
RPC Session Opened	Indicates that a Remote Procedure Call (RPC) session has been established.	1
RPC Session Closed	Indicates that an RPC session has been closed.	1
RPC Session Reset	Indicates that an RPC session has been reset.	3
RPC Session Terminated	Indicates that an RPC session has been terminated.	3
RPC Session Denied	Indicates that an RPC session has been denied.	3
RPC Session In Progress	Indicates that an RPC session is in progress.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
NTP Session Opened	Indicates that a Network Time Protocol (NTP) session has been established.	1
NTP Session Closed	Indicates that an NTP session has been closed.	1
NTP Session Reset	Indicates that an NTP session has been reset.	3
NTP Session Terminated	Indicates that an NTP session has been terminated.	3
NTP Session Denied	Indicates that an NTP session has been denied.	3
NTP Session In Progress	Indicates that an NTP session is in progress.	1
NNTP Session Opened	Indicates that a Network News Transfer Protocol (NNTP) session has been established.	1
NNTP Session Closed	Indicates that an NNTP session has been closed.	1
NNTP Session Reset	Indicates that an NNTP session has been reset.	3
NNTP Session Terminated	Indicates that an NNTP session has been terminated.	3
NNTP Session Denied	Indicates that an NNTP session has been denied.	3
NNTP Session In Progress	Indicates that an NNTP session is in progress.	1
NFS Session Opened	Indicates that a Network File System (NFS) session has been established.	1
NFS Session Closed	Indicates that an NFS session has been closed.	1
NFS Session Reset	Indicates that an NFS session has been reset.	3
NFS Session Terminated	Indicates that an NFS session has been terminated.	3
NFS Session Denied	Indicates that an NFS session has been denied.	3
NFS Session In Progress	Indicates that an NFS session is in progress.	1
NCP Session Opened	Indicates that a Network Control Program (NCP) session has been established.	1
NCP Session Closed	Indicates that an NCP session has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
NCP Session Reset	Indicates that an NCP session has been reset.	3
NCP Session Terminated	Indicates that an NCP session has been terminated.	3
NCP Session Denied	Indicates that an NCP session has been denied.	3
NCP Session In Progress	Indicates that an NCP session is in progress.	1
NetBIOS Session Opened	Indicates that a NetBIOS session has been established.	1
NetBIOS Session Closed	Indicates that a NetBIOS session has been closed.	1
NetBIOS Session Reset	Indicates that a NetBIOS session has been reset.	3
NetBIOS Session Terminated	Indicates that a NetBIOS session has been terminated.	3
NetBIOS Session Denied	Indicates that a NetBIOS session has been denied.	3
NetBIOS Session In Progress	Indicates that a NetBIOS session is in progress.	1
MODBUS Session Opened	Indicates that a MODBUS session has been established.	1
MODBUS Session Closed	Indicates that a MODBUS session has been closed.	1
MODBUS Session Reset	Indicates that a MODBUS session has been reset.	3
MODBUS Session Terminated	Indicates that a MODBUS session has been terminated.	3
MODBUS Session Denied	Indicates that a MODBUS session has been denied.	3
MODBUS Session In Progress	Indicates that a MODBUS session is in progress.	1
LPD Session Opened	Indicates that a Line Printer Daemon (LPD) session has been established.	1
LPD Session Closed	Indicates that an LPD session has been closed.	1
LPD Session Reset	Indicates that an LPD session has been reset.	3
LPD Session Terminated	Indicates that an LPD session has been terminated.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
LPD Session Denied	Indicates that an LPD session has been denied.	3
LPD Session In Progress	Indicates that an LPD session is in progress.	1
Lotus Notes Session Opened	Indicates that a Lotus Notes session has been established.	1
Lotus Notes Session Closed	Indicates that a Lotus Notes session has been closed.	1
Lotus Notes Session Reset	Indicates that a Lotus Notes session has been reset.	3
Lotus Notes Session Terminated	Indicates that a Lotus Notes session has been terminated.	3
Lotus Notes Session Denied	Indicates that a Lotus Notes session has been denied.	3
Lotus Notes Session In Progress	Indicates that a Lotus Notes session is in progress.	1
Kerberos Session Opened	Indicates that a Kerberos session has been established.	1
Kerberos Session Closed	Indicates that a Kerberos session has been closed.	1
Kerberos Session Reset	Indicates that a Kerberos session has been reset.	3
Kerberos Session Terminated	Indicates that a Kerberos session has been terminated.	3
Kerberos Session Denied	Indicates that a Kerberos session has been denied.	3
Kerberos Session In Progress	Indicates that a Kerberos session is in progress.	1
IRC Session Opened	Indicates that an Internet Relay Chat (IRC) session has been established.	1
IRC Session Closed	Indicates that an IRC session has been closed.	1
IRC Session Reset	Indicates that an IRC session has been reset.	3
IRC Session Terminated	Indicates that an IRC session has been terminated.	3
IRC Session Denied	Indicates that an IRC session has been denied.	3
IRC Session In Progress	Indicates that an IRC session is in progress.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
IEC 104 Session Opened	Indicates that an IEC 104 session has been established.	1
IEC 104 Session Closed	Indicates that an IEC 104 session has been closed.	1
IEC 104 Session Reset	Indicates that an IEC 104 session has been reset.	3
IEC 104 Session Terminated	Indicates that an IEC 104 session has been terminated.	3
IEC 104 Session Denied	Indicates that an IEC 104 session has been denied.	3
IEC 104 Session In Progress	Indicates that an IEC 104 session is in progress.	1
Ident Session Opened	Indicates that a TCP Client Identity Protocol (Ident) session has been established.	1
Ident Session Closed	Indicates that an Ident session has been closed.	1
Ident Session Reset	Indicates that an Ident session has been reset.	3
Ident Session Terminated	Indicates that an Ident session has been terminated.	3
Ident Session Denied	Indicates that an Ident session has been denied.	3
Ident Session In Progress	Indicates that an Ident session is in progress.	1
ICCP Session Opened	Indicates that an Inter-Control Center Communications Protocol (ICCP) session has been established.	1
ICCP Session Closed	Indicates that an ICCP session has been closed.	1
ICCP Session Reset	Indicates that an ICCP session has been reset.	3
ICCP Session Terminated	Indicates that an ICCP session has been terminated.	3
ICCP Session Denied	Indicates that an ICCP session has been denied.	3
ICCP Session In Progress	Indicates that an ICCP session is in progress.	1
Groupwise Session Opened	Indicates that a Groupwise session has been established.	1
Groupwise Session Closed	Indicates that a Groupwise session has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Groupwise Session Reset	Indicates that a Groupwise session has been reset.	3
Groupwise Session Terminated	Indicates that a Groupwise session has been terminated.	3
Groupwise Session Denied	Indicates that a Groupwise session has been denied.	3
Groupwise Session In Progress	Indicates that a Groupwise session is in progress.	1
Gopher Session Opened	Indicates that a Gopher session has been established.	1
Gopher Session Closed	Indicates that a Gopher session has been closed.	1
Gopher Session Reset	Indicates that a Gopher session has been reset.	3
Gopher Session Terminated	Indicates that a Gopher session has been terminated.	3
Gopher Session Denied	Indicates that a Gopher session has been denied.	3
Gopher Session In Progress	Indicates that a Gopher session is in progress.	1
GIOP Session Opened	Indicates that a General Inter-ORB Protocol (GIOP) session has been established.	1
GIOP Session Closed	Indicates that a GIOP session has been closed.	1
GIOP Session Reset	Indicates that a GIOP session has been reset.	3
GIOP Session Terminated	Indicates that a GIOP session has been terminated.	3
GIOP Session Denied	Indicates that a GIOP session has been denied.	3
GIOP Session In Progress	Indicates that a GIOP session is in progress.	1
Finger Session Opened	Indicates that a Finger session has been established.	1
Finger Session Closed	Indicates that a Finger session has been closed.	1
Finger Session Reset	Indicates that a Finger session has been reset.	3
Finger Session Terminated	Indicates that a Finger session has been terminated.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Finger Session Denied	Indicates that a Finger session has been denied.	3
Finger Session In Progress	Indicates that a Finger session is in progress.	1
Echo Session Opened	Indicates that an Echo session has been established.	1
Echo Session Closed	Indicates that an Echo session has been closed.	1
Echo Session Denied	Indicates that an Echo session has been denied.	3
Echo Session In Progress	Indicates that an Echo session is in progress.	1
Remote .NET Session Opened	Indicates that a Remote .NET session has been established.	1
Remote .NET Session Closed	Indicates that a Remote .NET session has been closed.	1
Remote .NET Session Reset	Indicates that a Remote .NET session has been reset.	3
Remote .NET Session Terminated	Indicates that a Remote .NET session has been terminated.	3
Remote .NET Session Denied	Indicates that a Remote .NET session has been denied.	3
Remote .NET Session In Progress	Indicates that a Remote .NET session is in progress.	1
DNP3 Session Opened	Indicates that a Distributed Network Proctologic (DNP3) session has been established.	1
DNP3 Session Closed	Indicates that a DNP3 session has been closed.	1
DNP3 Session Reset	Indicates that a DNP3 session has been reset.	3
DNP3 Session Terminated	Indicates that a DNP3 session has been terminated.	3
DNP3 Session Denied	Indicates that a DNP3 session has been denied.	3
DNP3 Session In Progress	Indicates that a DNP3 session is in progress.	1
Discard Session Opened	Indicates that a Discard session has been established.	1
Discard Session Closed	Indicates that a Discard session has been closed.	1

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Discard Session Reset	Indicates that a Discard session has been reset.	3
Discard Session Terminated	Indicates that a Discard session has been terminated.	3
Discard Session Denied	Indicates that a Discard session has been denied.	3
Discard Session In Progress	Indicates that a Discard session is in progress.	1
DHCP Session Opened	Indicates that a Dynamic Host Configuration Protocol (DHCP) session has been established.	1
DHCP Session Closed	Indicates that a DHCP session has been closed.	1
DHCP Session Denied	Indicates that a DHCP session has been denied.	3
DHCP Session In Progress	Indicates that a DHCP session is in progress.	1
DHCP Success	Indicates that a DHCP lease has been successfully obtained	1
DHCP Failure	Indicates that a DHCP lease cannot be obtained.	3
CVS Session Opened	Indicates that a Concurrent Versions System (CVS) session has been established.	1
CVS Session Closed	Indicates that a CVS session has been closed.	1
CVS Session Reset	Indicates that a CVS session has been reset.	3
CVS Session Terminated	Indicates that a CVS session has been terminated.	3
CVS Session Denied	Indicates that a CVS session has been denied.	3
CVS Session In Progress	Indicates that a CVS session is in progress.	1
CUPS Session Opened	Indicates that a Common Unix Printing System (CUPS) session has been established.	1
CUPS Session Closed	Indicates that a CUPS session has been closed.	1
CUPS Session Reset	Indicates that a CUPS session has been reset.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
CUPS Session Terminated	Indicates that a CUPS session has been terminated.	3
CUPS Session Denied	Indicates that a CUPS session has been denied.	3
CUPS Session In Progress	Indicates that a CUPS session is in progress.	1
Chargen Session Started	Indicates that a Character Generator (Chargen) session has been started.	1
Chargen Session Closed	Indicates that a Chargen session has been closed.	1
Chargen Session Reset	Indicates that a Chargen session has been reset.	3
Chargen Session Terminated	Indicates that a Chargen session has been terminated.	3
Chargen Session Denied	Indicates that a Chargen session has been denied.	3
Chargen Session In Progress	Indicates that a Chargen session is in progress.	1
Misc VPN	Indicates that a miscellaneous VPN session has been detected	1
DAP Session Started	Indicates that a DAP session has been established.	1
DAP Session Ended	Indicates that a DAP session has ended.	1
DAP Session Denied	Indicates that a DAP session has been denied.	3
DAP Session Status	Indicates that a DAP session status request has been made.	1
DAP Session in Progress	Indicates that a DAP session is in progress.	1
DAP Authentication Failed	Indicates that a DAP authentication has failed.	4
DAP Authentication Succeeded	Indicates that DAP authentication has succeeded.	1
TOR Session Started	Indicates that a TOR session has been established.	1
TOR Session Closed	Indicates that a TOR session has been closed.	1
TOR Session Reset	Indicates that a TOR session has been reset.	3

Table 17-15 Application Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
TOR Session Terminated	Indicates that a TOR session has been terminated.	3
TOR Session Denied	Indicates that a TOR session has been denied.	3
TOR Session In Progress	Indicates that a TOR session is in progress.	1
Game Session Started	Indicates a game session has started.	1
Game Session Closed	Indicates a game session has been closed.	1
Game Session Reset	Indicates a game session has been reset.	3
Game Session Terminated	Indicates a game session has been terminated.	3
Game Session Denied	Indicates a game session has been denied.	3
Game Session In Progress	Indicates a game session is in progress.	1
Admin Login Attempt	Indicates that an attempt to log in as an administrative user has been detected.	2
User Login Attempt	Indicates that an attempt to log in as a non-administrative user has been detected.	2

Audit

The Audit category indicates audit related events. The associated low-level event categories include:

Table 17-16 Audit Categories

Low Level Event Category	Description	Severity Level (0 to 10)
General Audit Event	Indicates a general audit event has been started.	1
Built-in Execution	Indicates that a built-in audit task has been run.	1
Bulk Copy	Indicates that a bulk copy of data has been detected.	1
Data Dump	Indicates that a data dump has been detected.	1
Data Import	Indicates that a data import has been detected.	1
Data Selection	Indicates that a data selection process has been detected.	1

Table 17-16 Audit Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Data Truncation	Indicates that the data truncation process has been detected.	1
Data Update	Indicates that the data update process has been detected.	1
Procedure/Trigger Execution	Indicates that the database procedure or trigger execution has been detected.	1
Schema Change	Indicates that the schema for a procedure or trigger execution has been altered.	1

Risk

The Risk category indicates events related to IBM Security QRadar Risk Manager. The associated low-level event categories include:

Table 17-17 Risk Categories

Low Level Event Category	Description	Severity Level (0 to 10)
Compliance Violation	Indicates a compliance violation has been detected.	5
Data Loss Possible	Indicates that the possibility of data loss has been detected.	5
Exposed Vulnerability	Indicates that the network or device has an exposed vulnerability.	9
Fraud	Indicates a host or device is susceptible to fraud.	7
Local Access Vulnerability	Indicates that the network or device has local access vulnerability.	7
Loss of Confidentiality	Indicates that a loss of confidentially has been detected.	5
Mis-Configured Rule	Indicates a rule is not configured properly.	3
Mis-Configured Device	Indicates a device on the network is not configured properly.	3
Mis-Configured Host	Indicates a network host is not configured properly.	3
No Password	Indicates no password exists.	7
Open Wireless Access	Indicates that the network or device has open wireless access.	5
Policy Exposure	Indicates a policy exposure has been detected.	5
Possible DoS Target	Indicates a host or device is a possible DoS target.	3

Table 17-17 Risk Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)
Possible DoS Weakness	Indicates a host or device has a possible DoS weakness.	3
Remote Access Vulnerability	Indicates that the network or device has a remote access vulnerability.	9
Un-Encrypted Data Transfer	Indicates that a host or device is transmitting data that is not encrypted.	3
Un-Encrypted Data Store	Indicates that the data store is not encrypted.	3
Weak Authentication	Indicates a host or device is susceptible to fraud.	5
Weak Encryption	Indicates that the host or device has weak encryption.	5

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 *http:\\www.ibm.com/legal/copytrade.shtml*.

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

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

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

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

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

INDEX

F

G

H

I

J

L

M

N

T

U

V