

IBM Security QRadar
Version 7.3.1

Administration Guide



Note

Before you use this information and the product that it supports, read the information in [“Notices” on page 383](#).

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.1 and subsequent releases unless superseded by an updated version of this document.

© **Copyright International Business Machines Corporation 2012, 2017.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction.....	xi
Chapter 1. What's new for administrators.....	1
New features and enhancements in QRadar V7.3.1.....	1
New features and enhancements in QRadar V7.3.0.....	5
Chapter 2. QRadar administration.....	7
Capabilities in your IBM Security QRadar product.....	7
Supported web browsers	8
Chapter 3. User management.....	11
User roles.....	11
Creating a user role.....	11
Editing a user role.....	14
Deleting a user role.....	17
Security profiles.....	17
Permission precedence.....	18
Creating a security profile.....	18
Editing a security profile.....	19
Duplicating a security profile.....	20
Deleting a security profile.....	20
User accounts.....	21
Creating a user account.....	21
View information about the current user.....	22
Disabling a user account.....	22
Deleting a user account.....	22
Deleting saved searches of a deleted user.....	23
User authentication.....	23
Changing QRadar user passwords.....	24
External authentication guidelines for administrative users.....	25
Configuring system authentication.....	25
Configuring RADIUS authentication.....	26
Configuring TACACS authentication.....	27
Configuring Active Directory authentication.....	28
LDAP authentication.....	29
Configuring LDAP authentication.....	29
Synchronizing data with an LDAP server.....	33
Configuring SSL or TLS certificates.....	33
Displaying hover text for LDAP information	34
Multiple LDAP repositories.....	35
Example: Least privileged access configuration and set up.....	35
Chapter 4. License management.....	37
Event and flow processing capacity.....	37
Shared license pool.....	38
Capacity sizing.....	38
Internal events.....	39
Burst handling.....	39
Example: Incoming data spike.....	40
Uploading a license key.....	41

Allocating a license key to a host.....	42
Distributing event and flow capacity.....	42
Viewing license details.....	43
Deleting licenses.....	44
Exporting license information.....	44
Chapter 5. System management.....	45
View system health information.....	45
QRadar component types.....	45
Data nodes.....	47
Data rebalancing after a data node is added.....	47
Viewing the progress of data rebalancing.....	48
Saving all event data to a Data Node appliance.....	48
Archiving Data Node content.....	49
Network interface management.....	49
Configuring network interfaces.....	49
QRadar system time.....	51
Configuring system time.....	51
NAT-enabled networks	52
Configuring a NAT group.....	53
Changing the NAT status for a managed host.....	54
Managing off-site hosts.....	54
Configuring an off-site source.....	54
Configuring an off-site target.....	55
Generating public keys for QRadar products.....	56
Forwarding filtered flows.....	56
Example: Forwarding normalized events and flows.....	57
Managed hosts.....	58
Bandwidth considerations for managed hosts.....	59
Encryption.....	59
Adding a managed host.....	60
Adding an IPv4-only managed host in a dual-stack environment.....	61
Configuring a managed host.....	62
Removing a managed host.....	62
Configuring your local firewall.....	63
Configuring email.....	63
Making changes in your QRadar environment.....	64
Changes that impact event collection.....	64
Deploying changes.....	65
Restarting the event collection service.....	65
Shutting down a system.....	65
Restarting a system.....	65
Collecting log files.....	66
Changing the root password on your QRadar console.....	66
Resetting SIM.....	67
Chapter 6. Set up QRadar.....	69
Network hierarchy.....	69
Guidelines for defining your network hierarchy.....	69
Acceptable CIDR values.....	70
Defining your network hierarchy.....	72
Automatic updates.....	73
Viewing pending updates.....	74
Configuring automatic update settings.....	75
Configuring updates behind a proxy server that uses SSL or TLS interception.....	76
Scheduling an update.....	77
Clearing scheduled updates.....	77

Checking for new updates.....	77
Manually installing automatic updates.....	77
Viewing your update history.....	78
Restoring hidden updates.....	78
Viewing the autoupdate log.....	78
Manual updates.....	78
Configuring an update server.....	79
Configuring the QRadar Console as the update server.....	80
Download updates to the update server.....	80
Configuring system settings.....	81
Customizing the right-click menu.....	81
Enhancing the right-click menu for event and flow columns.....	82
Asset retention values overview.....	84
Adding or editing a QRadar login message.....	85
IF-MAP server certificates.....	86
Configuring IF-MAP Server Certificate for Basic Authentication.....	86
Configuring IF-MAP Server Certificate for Mutual Authentication.....	86
Replacing SSL certificates in QRadar products.....	87
Installing a new SSL Certificate on the QRadar Console.....	90
Troubleshooting.....	91
Creating an SSL certificate signing request with SAN names	92
IPv6 addressing in QRadar deployments.....	93
Advanced iptables rules examples.....	95
Configuring iptables rules.....	96
Data retention.....	97
Configuring retention buckets.....	98
Managing retention bucket sequence.....	99
Enabling and disabling a retention bucket.....	100
Deleting a Retention Bucket.....	100
System notifications.....	100
Configuring system notifications.....	101
Configuring custom email notifications.....	102
Custom offense close reasons.....	105
Adding a custom offense close reason.....	105
Editing custom offense close reason.....	106
Deleting a custom offense close reason.....	106
Configuring a custom asset property.....	106
Index management.....	107
Enabling indexes.....	107
Enabling payload indexing to optimize search times.....	108
Configuring the retention period for payload indexes.....	108
Set restrictions to prevent resource-intensive searches.....	109
Types of resource restrictions.....	109
Resource restrictions in distributed environments.....	110
Configuring resource restrictions.....	111
App nodes.....	112
Prerequisites for setting up an App Node.....	112
Setting up an App Node.....	114
Adding an App Node.....	117
Removing an App Node.....	117
Checking the integrity of event and flow logs.....	118
Adding custom actions.....	119
Testing your custom action.....	120
Passing parameters to a custom action script.....	121
Managing aggregated data views.....	123
Accessing a GLOBALVIEW database.....	124

Chapter 7. Processing event data in QRadar.....	125
DSM Editor overview.....	125
Properties in the DSM Editor.....	126
Property configuration in the DSM Editor.....	127
How to write a format string in the DSM Editor.....	127
How to write regex for well-structured logs.....	128
How to write regex for natural language logs.....	129
How to write an expression for structured data in JSON format.....	129
How to write a JSON keypath expression.....	129
Opening the DSM Editor.....	131
Configuring a log source type.....	132
Configuring Auto Property Discovery for Log Source types.....	132
Custom property definitions in the DSM Editor.....	133
Selectivity.....	133
Expressions.....	134
Creating a custom property.....	134
Event mapping.....	136
Identity properties for event mappings.....	136
Creating an event map and categorization.....	136
Exporting contents from the DSM Editor.....	137
Exporting contents as a package.....	137
Exporting content for single custom property.....	138
Chapter 8. Using reference data in QRadar.....	139
Types of reference data collections.....	139
Reference sets overview.....	140
Adding, editing, and deleting reference sets.....	141
Viewing the contents of a reference set.....	142
Adding elements to a reference set.....	143
Exporting elements from a reference set.....	144
Deleting elements from a reference set.....	144
Creating reference data collections by using the command line.....	145
Command reference for reference data utilities.....	146
Creating reference data collections with the APIs.....	148
Reference data collection examples.....	151
Tracking expired user accounts.....	151
Integrate dynamic data from external sources	152
Chapter 9. User information source configuration.....	153
User information source overview.....	153
User information sources.....	153
Reference data collections for user information.....	154
Integration workflow example.....	154
User information source configuration and management task overview.....	155
Configuring the Tivoli Directory Integrator Server.....	155
Creating and managing user information source.....	157
Creating a user information source.....	157
Retrieving user information sources.....	159
Editing a user information source.....	159
Deleting a user information source.....	159
Collecting user information.....	160
Chapter 10. IBM X-Force integration.....	161
X-Force Threat Intelligence feed	161
Enabling the X-Force Threat Intelligence feed.....	161
Updating X-Force data in a proxy server.....	161

Preventing X-Force data from downloading data locally.....	162
IBM Security Threat Content app.....	162
Installing the IBM Security Threat Content application.....	163
IBM X-Force Exchange plug-in for QRadar.....	164
Installing the IBM X-Force Exchange plug-in.....	164
Chapter 11. Managing authorized services.....	165
Viewing authorized services.....	165
Adding an authorized service.....	165
Revoking authorized services.....	166
Chapter 12. Backup and recovery.....	167
Backup QRadar configurations and data.....	168
Scheduling nightly backup.....	168
Creating an on-demand configuration backup archive.....	170
Creating an email notification for a failed backup.....	170
Manage existing backup archives.....	172
Importing a backup archive.....	172
Deleting a backup archive.....	173
Restore QRadar configurations and data.....	173
Restoring a backup archive.....	174
Restoring a backup archive created on a different QRadar system.....	175
Restoring data.....	177
Verifying restored data.....	178
WinCollect files are not restored during a configuration restore.....	179
Backup and restore applications.....	179
Backing up and restoring apps.....	180
Backing up and restoring app data.....	180
Chapter 13. Flow sources.....	183
Types of flow sources.....	184
NetFlow.....	184
IPFIX.....	185
sFlow.....	185
J-Flow.....	186
Packeteer.....	186
Flowlog file.....	186
Napatech interface.....	186
Adding or editing a flow source.....	186
Forwarding packets to QRadar Packet Capture.....	187
Enabling and disabling a flow source.....	189
Deleting a Flow Source.....	189
Flow source aliases.....	189
Adding a flow source alias.....	190
Deleting a flow source alias.....	190
Chapter 14. Remote networks and services configuration.....	191
Default remote network groups.....	191
Default remote service groups.....	192
Guidelines for network resources.....	193
Managing remote networks objects.....	193
Managing remote services objects.....	194
QID map overview.....	194
Creating a QID map entry.....	195
Modifying a QID map entry.....	196
Importing Qid map entries.....	196
Exporting QID map entries.....	197

Chapter 15. Server discovery.....	199
Discovering servers.....	199
Chapter 16. Domain segmentation.....	201
Overlapping IP addresses.....	201
Domain definition and tagging.....	201
Creating domains.....	203
Domain privileges that are derived from security profiles.....	204
Domain-specific rules and offenses.....	205
Example: Domain privilege assignments based on custom properties.....	207
Chapter 17. Multitenant management.....	209
User roles.....	209
Domains and log sources.....	210
Provisioning a new tenant.....	210
Monitoring license usage.....	211
Detecting dropped events and flows.....	213
Rules management in multitenant deployments.....	213
Restricting log activity capabilities for tenant users.....	214
Network hierarchy updates in a multitenant deployment.....	214
Retention policies for tenants.....	215
Chapter 18. Asset Management.....	217
Sources of asset data.....	217
Incoming asset data workflow.....	218
Updates to asset data.....	220
Asset reconciliation exclusion rules.....	220
Asset merging.....	221
Identification of asset growth deviations.....	222
System notifications that indicate asset growth deviations.....	222
Example: How configuration errors for log source extensions can cause asset growth deviations.....	223
Troubleshooting asset profiles that exceed the normal size threshold.....	223
New asset data is added to the asset blacklists.....	224
Prevention of asset growth deviations.....	224
Stale asset data.....	225
Asset blacklists and whitelists.....	225
Tuning the Asset Profiler retention settings.....	229
Tuning the number of IP addresses allowed for a single asset.....	230
Identity exclusion searches.....	230
Advanced tuning of asset reconciliation exclusion rules.....	232
Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist.....	233
Clean up asset data after growth deviations.....	234
Deleting invalid assets.....	234
Deleting blacklist entries.....	235
Chapter 19. Configuring QRadar systems to forward data to other systems.....	237
Adding forwarding destinations.....	237
Configuring forwarding profiles.....	238
Configuring routing rules to forward data.....	239
Configuring routing rules to use the QRadar Data Store.....	240
Using custom rules & rule responses to forward data.....	241
Viewing forwarding destinations.....	242
Viewing and managing forwarding destinations.....	242
Viewing and managing routing rules.....	242

Chapter 20. Event store and forward	245
Store and forward overview.....	245
Viewing the Store and Forward schedule list.....	245
Creating a new Store and Forward schedule.....	248
Editing a Store and Forward schedule.....	249
Deleting a Store and Forward schedule.....	249
Chapter 21. Security content.....	251
Types of security content.....	251
Methods of importing and exporting content.....	252
Exporting all custom content.....	252
Exporting all custom content of a specific type.....	253
Searching for specific content items to export.....	255
Exporting a single custom content item.....	256
Exporting custom content items of different types.....	258
Installing extensions by using Extensions Management.....	260
Importing content by using the content management script.....	261
Updating content by using the content management script.....	262
Manually installing content packs from IBM Fix Central.....	263
Content type identifiers for exporting custom content.....	263
Content management script parameters.....	264
Chapter 22. SNMP trap configuration.....	267
Customizing the SNMP trap information sent to another system.....	267
Customizing the SNMP trap output.....	268
Adding a custom SNMP trap to QRadar.....	270
Sending SNMP traps to a specific host.....	270
Chapter 23. Protect sensitive data.....	273
How does data obfuscation work?.....	273
Data obfuscation profiles.....	274
Data obfuscation expressions.....	274
Scenario: Obfuscating user names.....	275
Creating a data obfuscation profile.....	276
Creating data obfuscation expressions.....	276
Deobfuscating data so that it can be viewed in the console.....	277
Editing or disabling obfuscation expressions created in previous releases.....	278
Chapter 24. Log files.....	279
Audit logs.....	279
Viewing the audit log file.....	279
Creating reports from audit log searches in QRadar.....	280
Logged actions.....	281
Chapter 25. Event categories.....	287
High-level event categories.....	287
Recon.....	288
DoS.....	290
Authentication.....	293
Access.....	302
Exploit.....	304
Malware.....	306
Suspicious Activity.....	308
System.....	312
Policy.....	317

Unknown.....	319
CRE.....	320
Potential Exploit.....	320
Flow.....	322
User Defined.....	323
SIM Audit.....	326
VIS Host Discovery.....	327
Application.....	328
Audit.....	353
Risk.....	357
Risk Manager Audit.....	358
Control.....	359
Asset Profiler.....	361
Sense.....	366
Chapter 26. Common ports and servers used by QRadar.....	369
QRadar port usage	369
Viewing IMQ port associations.....	376
Searching for ports in use by QRadar.....	377
QRadar public servers.....	377
Docker containers and network interfaces.....	378
Chapter 27. RESTful API	381
Accessing the interactive API documentation page.....	381
Notices.....	383
Trademarks.....	384
Terms and conditions for product documentation.....	384
IBM Online Privacy Statement.....	385
General Data Protection Regulation.....	385
Glossary.....	387
A.....	387
B.....	387
C.....	388
D.....	388
E.....	389
F.....	389
G.....	389
H.....	390
I.....	390
K.....	391
L.....	391
M.....	391
N.....	392
O.....	392
P.....	392
Q.....	393
R.....	393
S.....	394
T.....	394
V.....	395
W.....	395
Index.....	397

Introduction to QRadar product administration

Administrators use IBM Security QRadar SIEM to manage dashboards, offenses, log activity, network activity, assets, and reports.

Intended audience

This guide is intended for all QRadar SIEM users responsible for investigating and managing network security. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>).

For information about how to access more technical documentation in the QRadar products library, see [Accessing IBM Security Documentation Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

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

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. What's new for administrators

Learn about the new features and capabilities that make it easier for you to configure and administer your IBM Security QRadar deployment.

New features and enhancements in QRadar V7.3.1

The following new features and enhancements make it easier for administrators to manage their IBM Security QRadar V7.3.1 deployment.

To view a list of all new features in this release, see the *What's New* document on the [IBM Knowledge Center \(www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_pdf_launch.html\)](http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_pdf_launch.html).

Reduced downtime for event collection services

In earlier versions, deploying changes to your QRadar system sometimes resulted in gaps in data collection while the `hostcontext` service restarted. To minimize these interruptions, the event collection service is now managed separately from other QRadar services. The new event collection service, `ecs-ec-ingress`, listens on port 7787.

With the new separation of services, the event collection service does not automatically restart each time that you deploy changes. The service restarts only when the deployed changes impact the event collection service directly.

This enhancement significantly reduces interruptions in collecting data, and makes it easier for you to comply with your organization's data collection targets.

 [Learn more about making changes in your QRadar deployment...](#)


Continuous collection of events during minor patch updates

You can expect fewer disruptions in event collection when you apply future patches to QRadar V7.3.1 or later. Minor patches that do not require the system to restart will not restart the event collection service.

Ability to restart only the event collection service

From the QRadar product interface, you can restart the event collection service on all managed hosts in your deployment.

This new capability is useful when you want to restart the event collection service without impacting other QRadar services. For example, after you restore a configuration backup, you can defer restarting the service to a time that is convenient for you.

 [Learn more about restarting the event collection service...](#)


Event collection continues when you install or update a protocol RPM

Before QRadar V7.3.1, installing or updating a protocol RPM required a full deployment, which caused event collection to stop for several minutes for all installed protocols.

Now, protocols are loaded dynamically when you deploy the changes. Only those protocols that were updated experience a brief outage (in seconds).

New slide-out navigation menu with favorite tabs

As the number of apps that are installed in your deployment grows, so does the number of visible tabs. The new slide-out navigation menu makes it easier for you to find the apps that you use the most by managing which tabs are visible in QRadar.


When you upgrade to QRadar V7.3.1, all QRadar tabs are available from the slide-out menu (). Each menu item is marked as a favorite, which also makes it available as a tab. You can control which tabs are visible by selecting or clearing the star next to the menu item.

To access the settings that were on the **Admin** tab in earlier QRadar versions, click **Admin** at the bottom of the slide-out navigation menu.

Browser-based system notifications

QRadar now uses your browser notification settings to display system notifications. With this enhancement, you can continue to monitor the status and health of your QRadar deployment even when QRadar is not the active browser window. To show system notifications on your screen, you must configure your browser to allow notifications from QRadar.

Browser notifications are supported for Mozilla Firefox, Google Chrome, and Microsoft Edge 10. Microsoft Internet Explorer does not support browser-based notifications. Notifications in Internet Explorer now appear in a restyled QRadar notification window.

 [Learn more about system notifications...](#)

More health metrics data

QRadar collects up to 60x more health metrics data than before, making it easier for administrators to monitor their deployment and diagnose issues when they occur. You can visualize the new health metrics by using the QRadar Deployment Intelligence app, which is available from the IBM Security App Exchange.

The QRadar Deployment Intelligence app replaces the **System Health** information that was previously available on the **Admin** tab.

The additional health metrics data increases the size of the QRadar log files and the disk storage requirements for the data. Administrators who require more control over the disk storage that is required for the accumulated health data can create a retention bucket that uses Log Source Type = Health Metrics as the criteria.

 [Learn more about using retention buckets to manage disk storage...](#)

 [Learn more about installing IBM Security QRadar apps](#)

IPv6 support

QRadar uses the network hierarchy objects and groups to view network activity and monitor groups or services in your network. The network hierarchy can be defined by a range of IP addresses in IPv6 as well as IPv4 format. In addition to Network Hierarchy, Offense Manager used to only support IPv6 indexing but it now updates and displays all the appropriate fields for an offense with IPv6 data.

 [Learn more about IPv6 addressing in QRadar deployments...](#)


Improved security with new password policy

When using local QRadar authentication, you can enforce minimum password length and complexity, and control password expiry and reuse. The rules that you set are enforced for administrative and non-administrative users.

 [Learn more about configuring system authentication...](#)


Create an alias for the User Base DN (distinguished name) that is used for LDAP authentication

When you enter your user name on the login page, the Repository ID acts as an alias for the User Base DN (distinguished name). This use of an alias omits the need for typing a long distinguished name that might be hard to remember.

 [Learn more about configuring LDAP authentication...](#)

Edit or create a login message that is displayed to users in QRadar

Provide users with important information before they log in to QRadar. If needed, you can force users to consent to the login message terms before they can log in.

 [Learn more about creating or editing a login message...](#)

Monitor successful login events by running reports in QRadar

Easily monitor successful login events for the time period that you configure by running the **Weekly Successful Login Events** report template on the QRadar **Reports** tab.

Two new preinstalled apps in QRadar V7.3.1

App Authorization Manager

The **App Authorization Manager** app provides improved security for app authorization tokens. Users who have the appropriate permissions can delete authorization tokens, or change the assigned user level authorization.

QRadar Assistant App

The **QRadar Assistant App** provides the following functionality on the **Dashboard** tab:

- Recommended apps and content extensions that are based on your configured preferences.
- QRadar Help Center dashboard widget to help you access helpful information about QRadar.
- Content update status is highlighted, and then users can download updates from within QRadar.
- IBM Security Support Twitter feed.

Log source auto-detection configuration

Before QRadar V7.3.1, log source auto-detection configuration was controlled by a configuration file that was edited manually on each event processor managed host.


As of QRadar V7.3.1, global configuration settings are now available. You can use the QRadar REST API or a command line script to enable and disable which log source types are auto-detected. If you use a smaller number of log source types, you can configure which log sources are auto-detected to improve the speed of detection. Log source auto-detection configuration also helps to improve the accuracy of detecting devices that share a common format, and can improve pipeline performance by avoiding the creation of incorrectly detected devices.

Note: You can still enable per-event processor auto-detection settings by using the configuration file method. You can manage the method that is used on each event processor in **Admin > System & License Management > Component Management**. Upgrades from previous versions do not enable global settings, and retain the use of the local configuration files. Fresh installations of QRadar V7.3.1 enable the global auto-detection settings option.

 [Learn more about configuring managed hosts...](#)

Configuring auto property discovery for log source types and a new Configuration tab in DSM Editor


You can configure the automatic discovery of new properties for a log source type. By default, the Auto Property Discovery option for a log source type is disabled. When you enable the option on the new **Configuration** tab of the DSM Editor, new properties are automatically generated. The new properties capture all the fields that are present in the events that are received by the selected log source type. The newly discovered properties become available in the **Properties** tab of the DSM Editor.

 [Learn more about property configuration in the DSM Editor....](#)

New IBM QRadar Data Store offering

A new offering, IBM QRadar Data Store, normalizes and stores both security and operational log data for future analysis and review. The offering supports the storage of an unlimited number of logs without counting against your organization's Events Per Second QRadar SIEM license, and enables your organization to build custom apps and reports based on this stored data to gain deeper insights into your environments.

Enhancements to the routing rules require entitlement for QRadar Data Store, but is not currently enforced. In the future, when entitlement is enforced, access to the collected event data will be restricted to properly licensed systems. When the license is applied and the routing rule enhancement is selected, events that match the routing rule will be stored to disk and will be available to view and for searches. The events bypass the custom rule engine and no real-time correlation or analytics occur. The events can't contribute to offenses and are ignored when historical correlation runs. Some apps will also ignore these events. <https://www.ibm.com/support/docview.wss?uid=swg22009471> (<https://www-ibm.com/support/docview.wss?uid=swg22009471>).

 [Learn more about configuring routing rules to forward data....](#)

Log Source Extensions can extract values events in JSON format by key reference

Log Source Extensions can now extract values by using the JsonKeypath.

For an event data in a nested JSON format, a valid JSON expression is in the form */"<name of top-level field>"/"<name of sub-level field_1>".../"<name of sub-level field_n>"*.

The following two examples show how to extract data from a JSON record:

- Simple case of an event for a flat JSON record: `{"action": "login", "user": "John Doe"}`
To extract the 'user' field, use this expression: `/"user"`.

- Complex case of an event for a JSON record with nested objects: { "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }

To extract just the 'last_name' value from the 'user' subobject, use this expression: /"user"/"last_name".

New features and enhancements in QRadar V7.3.0

IBM Security QRadar V7.3.0 introduces new capabilities for tenant users, improved security, more flexibility when managing licenses, and a dedicated App Node for sharing applications.

Protect your QRadar instance with strong passwords

QRadar V7.3.0.2 introduces a strong password policy. When you enable the policy, system authentication passwords must contain a minimum number of characters and optionally must also contain at least 3 of the following attributes: uppercase characters, lowercase characters, special characters, numbers. Users are prompted to change their password if they log in with a password that does not meet the requirements.

The password policy settings apply to administrative and non-administrative user passwords that are managed by QRadar (system authentication) and do not apply to passwords that are managed by another authentication provider (external authentication) or root passwords.

 [Learn more about configuring system authentication...](#)

Log source limits are removed

Improvements to the licensing model in QRadar V7.3.0 now make it easier for you to manage log sources. Log source limits are removed and you no longer need to purchase licenses for log sources.

When you upgrade to QRadar V7.3.0, the previous log source limits are removed.

Easily distribute event and flow capacity across your deployment

Adapt to workload changes by allocating events per second (EPS) and flows per minute (FPM) to any host in your deployment, regardless of which host the license is allocated to.

The EPS and FPM from individual licenses are now aggregated into a shared license pool. As an administrator, you can use the new **License Pool Management** window to quickly see the cumulative EPS and FPM capacity across the deployment, and to determine the best way to allocate the EPS and FPM to the managed hosts.

For example, you have a QRadar V7.2.8 distributed deployment that has two event processors, one with 7,500 EPS and the other with 15,000 EPS. When you upgrade to QRadar V7.3.0, each processor maintains the pre-upgrade EPS allocations, but the combined 22,500 EPS become part of the shared license pool. When the data volumes for the event processors change, or when you add a managed host, you can redistribute the EPS capacity.

 [Learn more about managing the shared license pool...](#)

Tenant users can create custom properties

Tenant users can create custom properties to extract or calculate important information from the event or flow payload without assistance from a Managed Security Service Provider (MSSP) administrator. With this capability, tenant users can view and search on data that QRadar does not typically normalize and display.


As an MSSP administrator, you have write permissions for all custom properties that are created by tenant users. To improve search performance, you can optimize a tenant's custom properties when the properties are used frequently in rules and reports. Tenant users cannot optimize properties that they create.

For information about working with custom event and flow properties, see the *IBM Security QRadar User Guide*.

Tenant users can create reference data collections

In QRadar V7.2.8, tenant users can view reference data that is created by their MSSP Administrator. Now, in V7.3.0, tenant users who have the **Delegated Administration > Manage Reference Data** user role can create and manage their own reference data collections, without assistance from an MSSP administrator.

With this capability, tenant users can track referential business data or data from external sources, which can then be used in QRadar searches, filters, rule test conditions, and rule responses. For example, a reference set that contains the user IDs of terminated employees can be used to prevent employees from logging in to the network.


 [Learn more about creating and managing reference data collections...](#)

Serve QRadar apps from a dedicated App Node

Before QRadar V7.3.0, all QRadar apps had to be installed on the QRadar Console. Systems with many apps, or systems with resource-intensive apps, might have performance issues because of memory, storage, and CPU resource limitations on the QRadar Console.

Now, in QRadar V7.3.0, you can install a dedicated App Node server that serves your apps and their data without the performance limitations of apps that are installed on the QRadar Console.

When you set up a Red Hat Enterprise Linux 7.2 or CentOS 7.2 server with the memory, storage, and CPU resources that you require, you can install the App Node from the QRadar **Admin** tab in minutes. The App Node installation process installs all necessary software and transfers any apps that are installed on the QRadar Console to your App Node.

 [Learn more about setting up App Nodes...](#)


Optimized back up and recovery process for applications

Application configurations can now be backed up and restored separate from the application data.

Application configurations are backed up as part of the nightly configuration backup. The configuration backup includes apps that are installed on the QRadar Console and on an App Node. You can restore the application configuration by selecting the **Installed Applications Configuration** option when you restore a backup.

Application data is backed up separate from the application configuration by using an easy-to-use script that runs nightly. You can also use the script to restore the app data, and to configure backup times and data retention periods.

 [Learn more about backing up and restoring apps...](#)

 [Learn more about backing up and restoring app data...](#)

Security updates

QRadar V7.3.0 uses TLS 1.2 (Transport Layer Security) for secure communications. The Secure Socket Layer (SSL) and TLS 1.1 protocols are not supported.

There's a small change to the steps for updating the default CA certificate when automatic updates go through a proxy server.

Chapter 2. QRadar administration

As an IBM Security QRadar administrator, you have a variety of tools available to help you configure and manage your QRadar deployment.

For example, using the tools on the **Admin** tab, you can perform the following tasks:

- Deploy and manage QRadar hosts and licenses.
- Configure user accounts and authentication.
- Build a network hierarchy.
- Configure domains and set up a multi-tenant environment.
- Define and manage log and flow data sources.
- Manage QRadar data retention.
- Manage assets and reference data.
- Schedule regular backups of QRadar configuration and data.
- Monitor the system health of managed hosts.

Capabilities in your IBM Security QRadar product

IBM Security QRadar product documentation describes functionality such as offenses, flows, assets, and historical correlation, that might not be available in all QRadar products. Depending on the product that you are using, some documented features might not be available in your deployment.

IBM QRadar Log Manager

QRadar Log Manager is a basic, high-performance, and scalable solution for collecting, analyzing, storing, and reporting on large volumes of network and security event logs.

IBM Security QRadar SIEM

QRadar SIEM is an advanced offering that includes the full range of security intelligence capabilities for on-premises deployments. It consolidates log source and network flow data from thousands of assets, devices, endpoints, and applications that are distributed throughout your network, and performs immediate normalization and correlation activities on the raw data to distinguish real threats from false positives.

IBM QRadar on Cloud

QRadar on Cloud provides IBM security professionals to manage the infrastructure, while your security analysts perform the threat detection and management tasks. You can protect your network, and meet compliance monitoring and reporting requirements, with reduced total cost of ownership.

QRadar product capabilities

IBM Security QRadar product documentation describes capabilities, such as offenses, flows, assets, and historical correlation, that might not be available in all QRadar products. Review the following table to compare the capabilities in each product.

Table 1. Comparison of QRadar capabilities			
Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Full administrative capabilities	Yes	No	Yes
Supports hosted deployments	No	Yes	No

<i>Table 1. Comparison of QRadar capabilities (continued)</i>			
Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand-alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
QRadar Vulnerability Manager integration	Yes	Yes	Yes
Network activity monitoring	Yes	Yes	No
Asset profiling	Yes	Yes	No ¹
Offenses management	Yes	Yes	No
Network flow capture and analysis	Yes	Yes	No
Historical correlation	Yes	Yes	No
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No
¹ QRadar Log Manager tracks asset data only if QRadar Vulnerability Manager is installed.			

Some documentation, such as the *Administration Guide* and the *User Guide*, is common across multiple products and might describe capabilities that are not available in your deployment. For example, IBM QRadar on Cloud users do not have full administrative capabilities as described in the *IBM Security QRadar Administration Guide*.

Supported web browsers

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

The following table lists the supported versions of web browsers.

<i>Table 2. Supported web browsers for QRadar products</i>	
Web browser	Supported versions
64-bit Mozilla Firefox	45.8 Extended Support Release and later

Table 2. Supported web browsers for QRadar products (continued)

Web browser	Supported versions
64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.	11.0, Edge 38.14393 and later
64-bit Google Chrome	Latest

Chapter 3. User management

You define user roles, security profiles, and user accounts to control who has access to IBM Security QRadar, which tasks they can perform, and which data they have access to.

When you initially configure QRadar, use the **User Management** feature on the **Admin** tab to configure and manage user accounts for all users that require access to QRadar.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

User roles

A user role defines the functions that a user can access in IBM Security QRadar.

During the installation, two default user roles are defined: **Admin** and **All**.

Before you add user accounts, you must create the user roles to meet the permission requirements of your users.

Creating a user role

Create user roles to manage the functions that a user can access in IBM Security QRadar.

About this task

By default, your system provides a default administrative user role, which provides access to all areas of QRadar. 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.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > User Roles**.
3. On the toolbar, click **New**.
4. In the **User Role Name** field, type a unique name for this user role.
5. Select the permissions that you want to assign to the user role.

Learn more about user role permissions:

The permissions that are visible on the **User Role Management** window are dependent on which QRadar components are installed.

Table 3. Description of User Role Management window permissions	
Permission	Description
Admin	Grants administrative access to the user interface. You can grant specific Admin permissions. Users with System Administrator permission can access all areas of the user interface. Users who have this access cannot edit other administrator accounts.

Table 3. Description of **User Role Management** window permissions (continued)

Permission	Description
Delegated Administration	Grant users permissions to perform limited administrative functions. In a multi-tenant environment, tenant users with Delegated Administration permissions can see only data for their own tenant environment. If you assign other administrative permissions that are not part of Delegated Administration , tenant users can see data for all tenants.
Offenses	Grants the access to all the functions on the Offenses tab. User roles must have the Maintain Custom Rules permission to create and edit custom rules.
Log Activity	Grants access to functions in the Log Activity tab. You can also grant specific permissions: Maintain Custom Rules Grants permission to create or edit rules that are displayed on the Log Activity tab. Manage Time Series Grants permission to configure and view time series data charts. User Defined Event Properties Grants permission to create custom event properties. View Custom Rules Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.
Assets	Note: This permission is displayed only if IBM Security QRadar Vulnerability Manager is installed on your system. Grants access to the function in the Assets tab. You can grant specific permissions: Perform VA Scans Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment Guide</i> . Remove Vulnerabilities Grants permission to remove vulnerabilities from assets. Server Discovery Grants permission to discover servers. View VA Data Grants permission to vulnerability assessment data. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i> .

Table 3. Description of **User Role Management** window permissions (continued)

Permission	Description
Network Activity	<p>Grants access to all the functions in the Network Activity tab. You can grant specific access to the following permissions:</p> <p>Maintain Custom Rules Grants permission to create or edit rules that are displayed on the Network Activity tab.</p> <p>Manage Time Series Grants permission to configure and view time series data charts.</p> <p>User Defined Flow Properties Grants permission to create custom flow properties.</p> <p>View Custom Rules Grants permission to view custom rules. If the user role does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</p> <p>View Flow Content Grants permission to access to flow data.</p>
Reports	<p>Grants permission to access all of the functions on the Reports tab.</p> <p>Distribute Reports via Email Grants permission to distribute reports through email.</p> <p>Maintain Templates Grants permission to edit report templates.</p>
Vulnerability Manager	<p>Grants permission to QRadar Vulnerability Manager function. QRadar Vulnerability Manager must be activated.</p> <p>For more information, see the <i>IBM Security QRadar Vulnerability Manager User Guide</i>.</p>
Forensics	<p>Grants permission to QRadar Incident Forensics capabilities.</p> <p>Create cases in Incident Forensics Grants permission to create cases for collections of imported document and pcap files.</p>
IP Right Click Menu Extensions	Grants permission to options added to the right-click menu.
Platform Configuration	<p>Grants permission to Platform Configuration services.</p> <p>Dismiss System Notifications Grants permission to hide system notifications from the Messages tab.</p> <p>View Reference Data Grants permission to view reference data when it is available in search results.</p> <p>View System Notifications Grants permission to view system notifications from the Messages tab.</p>

6. In the **Dashboards** area, select the dashboards you want the user role to access, and click **Add**.

Note: A dashboard displays no information if the user role does not have permission to view dashboard data. If a user modifies the displayed dashboards, the defined dashboards for the user role appear at the next login.

7. Click **Save** and close the **User Role Management** window.
8. On the **Admin** tab menu, click **Deploy Changes**.

Editing a user role

You can edit an existing role to change the permissions that are assigned to the role.

About this task

To quickly locate the user role you want to edit on the **User Role Management** window, you can type a role name in the **Type to filter** text box. This box is located above the left pane.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > User Roles**.
3. In the left pane of the **User Role Management** window, select the user role that you want to edit.
4. In the right pane, update the permissions, as necessary.

Learn more about user role permissions:

The permissions that are visible on the **User Role Management** window are dependent on which QRadar components are installed.

Table 4. Description of User Role Management window permissions	
Permission	Description
Admin	Grants administrative access to the user interface. You can grant specific Admin permissions. Users with System Administrator permission can access all areas of the user interface. Users who have this access cannot edit other administrator accounts.
Delegated Administration	Grant users permissions to perform limited administrative functions. In a multi-tenant environment, tenant users with Delegated Administration permissions can see only data for their own tenant environment. If you assign other administrative permissions that are not part of Delegated Administration , tenant users can see data for all tenants.
Offenses	Grants the access to all the functions on the Offenses tab. User roles must have the Maintain Custom Rules permission to create and edit custom rules.

Table 4. Description of **User Role Management** window permissions (continued)

Permission	Description
Log Activity	<p>Grants access to functions in the Log Activity tab. You can also grant specific permissions:</p> <p>Maintain Custom Rules Grants permission to create or edit rules that are displayed on the Log Activity tab.</p> <p>Manage Time Series Grants permission to configure and view time series data charts.</p> <p>User Defined Event Properties Grants permission to create custom event properties.</p> <p>View Custom Rules Grants permission to view custom rules. If granted to a user role that does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</p>
Assets	<p>Note: This permission is displayed only if IBM Security QRadar Vulnerability Manager is installed on your system.</p> <p>Grants access to the function in the Assets tab. You can grant specific permissions:</p> <p>Perform VA Scans Grants permission to complete vulnerability assessment scans. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment Guide</i>.</p> <p>Remove Vulnerabilities Grants permission to remove vulnerabilities from assets.</p> <p>Server Discovery Grants permission to discover servers.</p> <p>View VA Data Grants permission to vulnerability assessment data. For more information about vulnerability assessment, see the <i>Managing Vulnerability Assessment guide</i>.</p>

Table 4. Description of **User Role Management** window permissions (continued)

Permission	Description
Network Activity	<p>Grants access to all the functions in the Network Activity tab. You can grant specific access to the following permissions:</p> <p>Maintain Custom Rules Grants permission to create or edit rules that are displayed on the Network Activity tab.</p> <p>Manage Time Series Grants permission to configure and view time series data charts.</p> <p>User Defined Flow Properties Grants permission to create custom flow properties.</p> <p>View Custom Rules Grants permission to view custom rules. If the user role does not also have the Maintain Custom Rules permission, the user role cannot create or edit custom rules.</p> <p>View Flow Content Grants permission to access to flow data.</p>
Reports	<p>Grants permission to access all of the functions on the Reports tab.</p> <p>Distribute Reports via Email Grants permission to distribute reports through email.</p> <p>Maintain Templates Grants permission to edit report templates.</p>
Vulnerability Manager	<p>Grants permission to QRadar Vulnerability Manager function. QRadar Vulnerability Manager must be activated.</p> <p>For more information, see the <i>IBM Security QRadar Vulnerability Manager User Guide</i>.</p>
Forensics	<p>Grants permission to QRadar Incident Forensics capabilities.</p> <p>Create cases in Incident Forensics Grants permission to create cases for collections of imported document and pcap files.</p>
IP Right Click Menu Extensions	Grants permission to options added to the right-click menu.
Platform Configuration	<p>Grants permission to Platform Configuration services.</p> <p>Dismiss System Notifications Grants permission to hide system notifications from the Messages tab.</p> <p>View Reference Data Grants permission to view reference data when it is available in search results.</p> <p>View System Notifications Grants permission to view system notifications from the Messages tab.</p>

5. Modify the **Dashboards** options for the user role as required.
6. Click **Save**.
7. Close the **User Role Management** window.
8. On the **Admin** tab, click **Deploy Changes**.

Deleting a user role

If a user role is no longer required, you can delete the user role.

About this task

If user accounts are assigned to the user role you want to delete, you must reassign the user accounts to another user role. The system automatically detects this condition and prompts you to update the user accounts.

You can quickly locate the user role that you want to delete on the **User Role Management** window. Type a role name in the **Type to filter** text box, which is located above the left pane.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > User Roles**.
3. In the left pane of the **User Role Management** window, select the role that you want to delete.
4. On the toolbar, click **Delete**.
5. Click **OK**.
 - If user accounts are assigned to this user role, the **Users are Assigned to this User Role** window opens. Go to Step 7.
 - If no user accounts are assigned to this role, the user role is successfully deleted. Go to Step 8.
6. 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**.
7. Close the **User Role Management** window.
8. On the **Admin** tab, click **Deploy Changes**.

Security profiles

Security profiles define which networks, log sources, and domains that a user can access.

QRadar includes one default security profile for administrative users. The **Admin** security profile includes access to all networks, log sources, and domains.

Before you add user accounts, you must create more security profiles to meet the specific access requirements of your users.

Domains

Security profiles must be updated with an associated domain. You must define domains on the **Domain Management** window before the **Domains** tab is shown on the **Security Profile Management** window. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

Domain assignments take precedence over all settings on the **Permission Precedence**, **Networks**, and **Log Sources** tabs.

If the domain is assigned to a tenant, the tenant name appears in brackets beside the domain name in the **Assigned Domains** window.

Permission precedence

Permission precedence determines which security profile components to consider when the system displays events in the **Log Activity** tab and flows in the **Network Activity** tab.

Choose from the following restrictions when you create a security profile:

- **No Restrictions** - This option does not place restrictions on which events are displayed in the **Log Activity** tab, and which flows are displayed in the **Network Activity** tab.
- **Network Only** - This option restricts the user to view only events and flows that are associated with the networks that are specified in this security profile.
- **Log Sources Only** - This option restricts the user to view only events that are associated with the log sources that are specified in this security profile.
- **Networks AND Log Sources** - This option allows the user to view only events and flows that are associated with the log sources and networks that are specified in this security profile.

For example, if the security profile allows access to events from a log source 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** - This option allows the user to view events and flows that are associated with either the log sources or networks that are specified in this security profile.

For example, if a security profile allows access to events from a log source but the destination network is restricted, the event is displayed on the **Log Activity** tab if the permission precedence is set to **Networks OR Log Sources**. If the permission precedence is set to **Networks AND Log Sources**, the event is not displayed on the **Log Activity** tab.

Permission precedence for offense data

Security profiles automatically use the **Networks OR Log Sources** permission when offense data is shown. For example, if an offense has a destination IP address that your security profile permits you to see, but the security profile does not grant permissions to the source IP address, the **Offense Summary** window shows both the destination and source IP addresses.

Creating a security profile

To add user accounts, you must first create security profiles to meet the specific access requirements of your users.


About this task

IBM Security QRadar SIEM includes one default security profile for administrative users. The Admin security profile includes access to all networks, log sources, and domains.

To select multiple items on the **Security Profile Management** window, hold the Control key while you select each network or network group that you want to add.

If after you add networks, log sources or domains you want to remove one or more before you save the configuration, you can select the item and click the **Remove (<)** icon. To remove all items, click **Remove All**.

Procedure

1. On the navigation menu () , click **Admin**.
2. Click **System Configuration > User Management**.
3. Click the **Security Profiles** icon.
4. On the **Security Profile Management window** toolbar, click **New**.
5. Configure the following parameters:

- a) In the **Security Profile Name** field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.
 - b) OptionalType a description of the security profile. The maximum number of characters is 255.
 6. Click the **Permission Precedence** tab.
 7. In the Permission Precedence Setting pane, select a permission precedence option. See [“Permission precedence” on page 18](#).
 8. Configure the networks that you want to assign to the security profile:
 - a) Click the **Networks** tab.
 - b) From the navigation tree in the left pane of the **Networks** tab, select the network that you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the network to the Assigned Networks pane.
 - d) Repeat for each network you want to add.
 9. Configure the log sources that you want to assign to the security profile:
 - a) Click the **Log Sources** tab.
 - b) From the navigation tree in the left pane, select the log source group or log source you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the log source to the Assigned Log Sources pane.
 - d) Repeat for each log source you want to add.
 10. Configure the domains that you want to assign to the security profile:
 - a) Click the **Domains** tab.
 - b) From the navigation tree in the left pane, select the domain that you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the domain to the Assigned Domains pane.
 - d) Repeat for each domain that you want to add.
 11. Click **Save**.
- Note:** The log sources and domains that are assigned to the security profile must match. You cannot save the security profile if the log sources and domains do not match.
12. Close the **Security Profile Management** window.
 13. On the **Admin** tab, click **Deploy Changes**.


Editing a security profile

You can edit an existing security profile to update which networks and log sources a user can access and the permission precedence.

About this task

To quickly locate the security profile you want to edit on the **Security Profile Management** window, type the security profile name in the **Type to filter** text box. It is located above the left pane.

Procedure

1. On the navigation menu () , click **Admin**.
2. Click **System Configuration > User Management**.
3. Click the **Security Profiles** icon.
4. In the left pane, select the security profile you want to edit.
5. On the toolbar, click **Edit**.
6. Update the parameters as required.
7. Click **Save**.

8. If the **Security Profile Has Time Series Data** window opens, select one of the following options:

Option	Description
Keep Old Data and Save	Select this option to keep previously accumulated time series data. If you choose this option, users with this security profile might see previous data that they no longer have permission to see when they view time series charts.
Hide Old Data and Save	Select this option to hide the time-series data. If you choose this option, time series data accumulation restarts after you deploy your configuration changes.

9. Close the **Security Profile Management** window.
10. On the **Admin** tab, click **Deploy Changes**.


Duplicating a security profile

If you want to create a new security profile that closely matches an existing security profile, you can duplicate the existing security profile and then modify the parameters.

About this task

To quickly locate the security profile you want to duplicate on the Security Profile Management window, you can type the security profile name in the **Type to filter** text box, which is located above the left pane.

Procedure

1. On the navigation menu (), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Security Profiles**.
4. In the left pane, select the security profile you want to duplicate.
5. On the toolbar, click **Duplicate**.
6. In the **Confirmation** window, type a unique name for the duplicated security profile.
7. Click **OK**.
8. Update the parameters as required.
9. Close the **Security Profile Management** window.
10. On the **Admin** tab, click **Deploy Changes**.

Deleting a security profile


If a security profile is no longer required, you can delete the security profile.

About this task

If user accounts are assigned to the security profiles you want to delete, you must reassign the user accounts to another security profile. IBM Security QRadar SIEM automatically detects this condition and prompts you to update the user accounts.

To quickly locate the security profile you want to delete on the **Security Profile Management** window, you can type the security profile name in the **Type to filter** text box. It is located above the left pane.

Procedure

1. On the navigation menu (), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Security Profiles**.
4. In the left pane, select the security profile that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.

- If user accounts are assigned to this security profile, the **Users are Assigned to this Security Profile** window opens. Go to [“Deleting a user role” on page 17](#).
 - If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to [“Deleting a user role” on page 17](#).
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**.
 8. Close the **Security Profile Management** window.
 9. On the **Admin** tab, click **Deploy Changes**.

User accounts

The user account defines the unique username that is used to log in to IBM Security QRadar, and specifies which user role, security profile, and tenant assignments the user is assigned to.

When you initially configure your system, you must create user accounts for each user who requires access to QRadar.

Creating a user account

You can create new user accounts.

Before you begin


Before you can create a user account, you must ensure that the required user role and security profile are created.

About this task

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.

Procedure

1. On the navigation menu () , click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Users**.
4. On the **User Management** toolbar, click **New**.
5. Enter values for the following parameters:
 - a) In the **Username** field, type a unique user name for the new user. The user name must contain a maximum 30 characters.
 - b) In the **Password** field, type a password for the user to gain access. The password must meet the minimum length and complexity requirements that are enforced.
6. Click **Save**.
7. Close the **User Details** window.
8. Close the **User Management** window.
9. On the **Admin** tab, click **Deploy Changes**.

View information about the current user

You can view account information for the current user through the main product interface.

Procedure

1. In the top-right corner, click the arrow next to the user account name.
2. Click **User Preferences**.
3. Optional: Update the configurable user details.

Option	Description
Parameter	Description
Email	Type a new email address.
Password	Type a new password. The password must meet the minimum length and complexity requirements that are enforced.
Password (Confirm)	Type the new password again.
Enable Popup Notifications	Pop-up system notification messages are displayed at the lower right corner of the user interface. To disable pop-up notifications, clear this check box.

4. Click **Save**.

Disabling a user account

You can disable a user account to restrict a user from accessing QRadar. The option to disable a user account temporarily revokes a user's access without deleting the account.

About this task

If the user with the disabled account attempts to log in, a message is displayed to inform the user that the user name and password are no longer valid. Items that the user created, such as saved searches and reports, remain associated with the user.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Users**.
4. In the **Manage Users** pane, click the user account that you want to disable.
5. From the **User Details** window, select **Disabled** from the **User Role** list.
6. Click **Save**.
7. Close the **User Details** window.
8. Close the **User Management** window.
9. On the **Admin** tab, click **Deploy Changes**.

Deleting a user account


If a user account is no longer required, you can delete the user account.

About this task

After you delete a user, the user no longer has access to the user interface. If the user attempts to log in, a message is displayed to inform the user that the user name and password is no longer valid. Items that a deleted user created, such as saved searches and reports remain associated with the deleted user.

To quickly locate the user account you want to delete on the **User Management** window, you can type the user name in the **Search User** text box on the toolbar.

Procedure

1. On the navigation menu (), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Users**.
4. Select the user that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.
7. Close the **User Management** window.


Deleting saved searches of a deleted user

If a deleted user's saved searches are no longer required, you can delete the searches.

About this task

Saved searches that a deleted user created remain associated with the user until you delete the searches.

Procedure

1. On the navigation menu (), click **Log Activity** or **Network Activity**.
2. Click **Search > Manage Search Results**.
3. Click the **Status** column to sort the saved searches.
4. Select the saved searches with a status of "ERROR!" and click **Delete**.

User authentication

When authentication is configured and a user enters an invalid user name and password combination, a message is displayed to indicate that the login was invalid.

If the user attempts to access the system multiple times with invalid information, the user must wait the configured amount of time before making another attempt to access the system. You can configure console settings to determine the maximum number of failed logins and other related settings.

IBM Security QRadar supports the following authentication types:

- **System authentication** - Users are authenticated locally. System authentication 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 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 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 supports up to Cisco Secure ACS Express 4.3.
- **Microsoft Active Directory** - Users are authenticated by a Lightweight Directory Access Protocol (LDAP) server that uses Kerberos.
- **LDAP** - Users are authenticated by a Native LDAP server.

Prerequisite checklist for external authentication providers


Before you can configure RADIUS, TACACS, Active Directory, or LDAP as the authentication type, you must complete the following tasks:

- ___ • Configure the authentication server before you configure authentication in QRadar. For more information, see your server documentation.
- ___ • Ensure that the server has the appropriate user accounts and privilege levels to communicate with QRadar. For more information, see your server documentation.
- ___ • Ensure that the time of the authentication server is synchronized with the time of the QRadar server. For more information about setting time, see [“QRadar system time” on page 51](#).
- ___ • Ensure that all users have appropriate user accounts and roles to allow authentication with the vendor servers.



Changing QRadar user passwords

IBM Security QRadar occasionally changes the password policy to align with current security standards. When the password policy is updated, users who have local passwords are prompted to update their password the first time that they log in after the upgrade. In very few situations, some users may not be prompted to change their password after the upgrade, and you will have to change it for them.


To change SIEM user passwords, complete the following steps:

1. On the navigation menu () , click **Admin**.
2. Click **System Configuration > User Management > Users**.
3. Select a user from the list and click **Edit**.
4. In the **User Details** pane, enter the new password for the user, and click **Save**.
5. From the Admin tab, click **Deploy Changes** for the changes to take effect.

To change PCAP user passwords, complete the following steps:

1. On the navigation menu () , click **Admin**.
2. Click **System and License Management**.
3. Select **Systems View** from the **Display** list.
4. Highlight your QRadar Incident Forensics device.
5. On the **Deployment Actions** menu, click **Edit Host**.
6. Select the **Component Management**  icon .
7. In the PCAP Device Management window, reenter or change the login password for the user and click **Save**.
8. On the **Admin** tab, click **Advanced > Deploy Full Configuration** for the changes to take effect.

To change FTP user passwords, complete the following steps:

1. On the navigation menu () , click **Admin**.
2. In the **Forensics** section, click **Forensics User Permissions**.
3. Select a user from the **Users** list on the left side of the window.
4. In the **Edit User** pane, check the **Enable FTP access** box.
5. Reenter or change the password for the user.
6. Under **Assigned Cases**, click **Save User**.

External authentication guidelines for administrative users

Administrative users must be able to log into IBM Security QRadar when external authentication fails.

The QRadar administrative roles have both the external and local authentication methods available in case the external authentication fails. If the remote authentication fails, the administrative users can log in by using the local password. A local password must be set for administrative users when external authentication is configured.

The local password is not set when you create a non-administrative user because the local password is not synchronized with the remote authority. Non-administrative users are only able to authenticate their username and password to the remote authority. If the remote authority is disabled or the other user credentials are rejected, the user cannot log in.

Administrative users must update both the local and remote authentication passwords at the same time to avoid issues when the user logs in to QRadar and the remote authentication source is disabled. You cannot change the local administration password while the remote authority is active. To change the administration password, you must:

1. Temporarily disable external authentication.
2. Reset the password.
3. Reconfigure external password.

Configuring system authentication

You can configure local authentication on your IBM Security QRadar system. You can specify length, complexity, and expiry requirements for local passwords.

About this task

The local authentication password policy applies to local passwords for administrative users. The policy also applies to non-administrative users if no external authentication is configured.

When the local authentication password policy is updated, users are prompted to change their password if they log in with a password that does not meet the new requirements.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > Authentication**.
3. Optional: In the **General Authentication Settings** tab, from the **Authentication Module** list box, select **System Authentication**, and then click **Save Authentication Module**.

System authentication is the default authentication module. If you change from another authentication module, then you must deploy QRadar before you do the next steps.

4. In the **Local Password Policy Configuration** tab, select the password complexity settings for local authentication.

Learn more about password complexity settings:

Table 5. Description of Password Complexity settings	
Password complexity setting	Description
Minimum Password Length	<p>Specifies the minimum number of characters that must be in a password.</p> <p>Important: To provide adequate security, passwords should contain at least 8 characters.</p>

Table 5. Description of Password Complexity settings (continued)	
Password complexity setting	Description
Use Complexity Rules	Requires that passwords meet a number of complexity rules, such as containing uppercase characters, lowercase characters, special characters, or numbers.
Number of rules required	The number of complexity rules that individual passwords must meet. Must be between one and the number of enabled complexity rules. For example, if all four complexity rules are enabled and individual passwords must meet any three of them, then enter 3.
Contain an uppercase character	Requires that passwords contain at least one uppercase character.
Contain a lowercase character	Requires that passwords contain at least one lowercase character.
Contain a digit	Requires that passwords contain at least one number.
Contain a special character	Requires that passwords contain at least one space or other character that is not a letter or number (for example, "%&'()*,-./:;<=>?@[\\]_` ~).
Not contain repeating characters	Disallows more than two repeating characters. For example, abbc is allowed but abbbc is not allowed.
Password History	Prevents passwords from being reused for a number of days. The number of days is calculated by Unique password count multiplied by Days before password will expire .
Unique password count	The number of password changes before a previous password can be reused.
Days before password will expire	The number of days before a password must be changed.

5. Click **Update Password Policy**.

Configuring RADIUS authentication

You can configure RADIUS authentication on your IBM Security QRadar system.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > Authentication**.
3. From the **Authentication Module** list, select **RADIUS Authentication**.
4. Configure the parameters:
 - a) In the **RADIUS Server** field, type the host name or IP address of the RADIUS server.
 - b) In the **RADIUS Port** field, type the port of the RADIUS server.
 - c) From the **Authentication Type** list box, select the type of authentication you want to perform.

Choose from the following options:

Description of authentication types

Option	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows workstations.
ARAP	Apple Remote Access Protocol (ARAP) establishes authentication for AppleTalk network traffic.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server.

- d) In the **Shared Secret** field, type the shared secret that IBM Security QRadar SIEM uses to encrypt RADIUS passwords for transmission to the RADIUS server.

5. Click **Save Authentication Module**.

Configuring TACACS authentication

You can configure TACACS authentication on your IBM Security QRadar system.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > Authentication**.
3. From the **Authentication Module** list, select **TACACS Authentication**.
4. Configure the parameters:
 - a) In the **TACACS Server** field, type the host name or IP address of the TACACS server.
 - b) In the **TACACS Port** field, type the port of the TACACS server.
 - c) From the **Authentication Type** list box, select the type of authentication you want to perform.

Choose from the following options:

Option	Description
ASCII	American Standard Code for Information Interchange (ASCII) sends the user name and password in clear text.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server. PAP is the default authentication type.
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows workstations.
MSCHAP2	Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAP2) authenticates remote Windows workstations by using mutual authentication.
EAPMD5	Extensible Authentication Protocol using MD5 Protocol (EAPMD5) uses MD5 to establish a PPP connection.


- d) In the **Shared Secret** field, type the shared secret that QRadar uses to encrypt TACACS passwords for transmission to the TACACS server.

5. Click **Save Authentication Module**.

Configuring Active Directory authentication

You can configure Microsoft Active Directory authentication on your IBM Security QRadar system.

Procedure

1. On the navigation menu (), click **Admin**.
2. On the navigation menu, click **System Configuration** and then click the **Authentication** icon.
3. From the **Authentication Module** list box, select **Active Directory**.
4. Click **Add**, and configure parameters for the Active Directory Repository.

The following table describes the parameters to configure:

LDAP parameters

Parameter	Description
Repository ID	The Repository ID is an identifier or alias that uniquely represents the server entered in the Server URL field and the domain from the Domain field. Use the Repository ID when you enter your login details. For example, you might use AD_1 to represent server_A on Domain_A in one Active Directory Repository, and AD_2 to represent server_B on Domain_A in your second repository.
Server URL	The URL that is used to connect to the LDAP server. For example, type ldaps://host_name:port. Note: If you specify a secure LDAP connection, the password is secure but the username is passed in clear text.
Context	Context that you want to use; for example, DC=QRADAR, DC=INC.
Domain	Domain that you want to use, for example; qradar.inc.

5. Enter the user name and password that you use to authenticate with the repository.
6. To test connectivity to the repository, click **Test Connection**.
7. To edit or remove a repository, select the repository, and then click **Edit** or **Remove**.
8. Click **Save**.

Users can log in by using the Domain\user or Repository_ID\user login formats.

The login request that uses Repository_ID\user is attempted on a specific server that is linked to a specific domain. For example, Server A on Domain A, which is more specific than the Domain\user login request format.

The login request that uses the Domain\user format is attempted on servers that are linked to the specified domain until a successful login is achieved. For example, there might be more than one server on a specific domain.

Note: For Active Directory user authentication, you must create a local QRadar user account in Active Directory authentication mode that is the same as the Active Directory (AD) account on the authentication server.

9. On the **Admin** page, click **Deploy Changes**.

LDAP authentication

You can configure IBM Security QRadar to use supported Lightweight Directory Access Protocol (LDAP) providers for user authentication and authorization.

QRadar reads the user and role information from the LDAP server, based on the authorization criteria that you defined.

In geographically dispersed environments, performance can be negatively impacted if the LDAP server and the QRadar console are not geographically close to each other. For example, user attributes can take a long time to populate if the QRadar console is in North America and the LDAP server is in Europe.

You can use the LDAP plug-in for authentication against an Active Directory server. In QRadar V7.2.4 and earlier, you must configure the server to allow anonymous bind for authentication. However, in QRadar V7.2.5 and later versions, LDAP plug-in supports authenticated binds against an Active Directory server.

QRadar V7.2.4 and later versions, use local LDAP authentication passwords that are stored locally for administrative users. These passwords are used if the external authenticator is unavailable, or if a connection to the LDAP server is unavailable due to network issues.

In QRadar V7.2.4 and earlier, multiple LDAP server configurations are not supported. However, in QRadar V7.2.5 and later versions, multiple LDAP server configurations are fully supported and includes new authentication options.

Configuring LDAP authentication

You can configure LDAP authentication on your IBM Security QRadar system.

Before you begin

If you plan to use SSL encryption or use TLS authentication with your LDAP server, you must import the SSL or TLS certificate from the LDAP server to the `/opt/qradar/conf/trusted_certificates` directory on your QRadar console. For more information about configuring the certificates, see [“Configuring SSL or TLS certificates” on page 33](#).

If you are using group authorization, you must configure a QRadar user role or security profile on the QRadar console for each LDAP group that is used by QRadar. Every QRadar user role or security profile must have at least one **Accept** group. The mapping of group names to user roles and security profiles is case-sensitive.

About this task

Authentication establishes proof of identity for any user who attempts to log in to the QRadar server. When a user logs in, the user name and password are sent to the LDAP directory to verify whether the credentials are correct. To send this information securely, configure the LDAP server connection to use Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption.

Authorization is the process of determining what access permissions a user has. Users are authorized to perform tasks based on their role assignments. You must have a valid bind connection to the LDAP server before you can select authorization settings.

User attribute values are case-sensitive. The mapping of group names to user roles and security profiles is also case-sensitive.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > Authentication**.
3. From the **Authentication Module** list, select **LDAP**.
4. Click **Add** and complete the basic configuration parameters.

Learn more about LDAP basic configuration parameters:

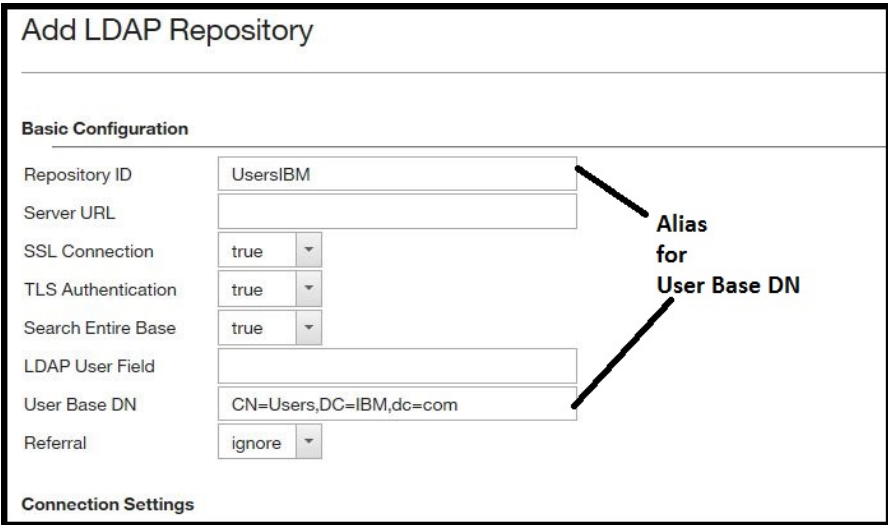
Parameter	Description
Repository ID	<p>The Repository ID is an alias for the User Base DN (distinguished name) that you use when you enter your login details, to avoid having to type a long string. When you have more than one repository in your network, you can place the User Base DN before the user name or you can use the shorter Repository ID.</p> <p>For example, the User Base DN is: CN=Users,DC=IBM,DC=com. You create a repository ID such as UsersIBM that is an alias for the user base DN.</p> <p>You can type the short repository ID UsersIBm instead of typing the following example of a complete User Base DN CN=Users,DC=IBM,DC=com</p> <p>Here's an example where you configure the repository ID to use as an alias for the User Base DN.</p> <div data-bbox="586 751 1468 1272">  </div> <p>Note: The Repository ID and User Base DN must be unique.</p>
Server URL	<p>The DNS name or IP address of the LDAP server. The URL must include a port value.</p> <p>For example, ldap://<host_name>:<port> or ldap://<ip_address>:<port>.</p>

Table 6. LDAP Basic Configuration parameters (continued)	
Parameter	Description
SSL connection	<p>Select True or False to specify whether Secure Sockets Layer (SSL) encryption is enabled.</p> <p>If SSL encryption is enabled, the value in the Server URL field must specify a secure connection. For example, <code>ldaps://secureldap.mydomain.com:636</code> uses a secure server URL.</p>
TLS authentication	<p>Select True or False to specify whether Transport Layer Security (TLS) authentication is enabled.</p> <p>Transport Layer Security (TLS) encryption to connect to the LDAP server is negotiated as part of the normal LDAP protocol and does not require a special protocol designation or port in the Server URL field.</p>
Search entire base	<p>Select True to search all subdirectories of the specified Directory Name (DN).</p> <p>Select False to search only the immediate contents of the Base DN. The subdirectories are not searched.</p>
LDAP user field	<p>The user field identifier that you want to search on.</p> <p>You can specify multiple user fields in a comma-separated list to allow users to authenticate against multiple fields. For example, if you specify uid,mailid, a user can be authenticated by providing either their user ID or their mail ID.</p>
User Base DN	<p>The Distinguished Name (DN) of the node where the search for a user would start. The User Base DN becomes the start location for loading users. For performance reasons, ensure that the User Base DN is as specific as possible.</p> <p>For example, if all of your user accounts are on the directory server in the Users folder, and your domain name is <code>ibm.com</code>, the User Base DN value would be <code>cn=Users,dc=ibm,dc=com</code>.</p>
Referral	Select Ignore or Follow to specify how referrals are handled.

5. Under **Connection Settings**, select the type of bind connection.

Learn more about bind connections:

Table 7. LDAP bind connections	
Bind connection type	Description
Anonymous bind	Use anonymous bind to create a session with the LDAP directory server that doesn't require that you provide authentication information.
Authenticated bind	<p>Use authenticated bind when you want the session to require a valid user name and password combination. A successful authenticated bind authorizes the authenticated user to read the list of users and roles from the LDAP directory during the session. For increased security, ensure that the user ID that is used for the bind connection does not have permissions to do anything other than reading the LDAP directory.</p> <p>Provide the Login DN and Password. For example, if the login name is <code>admin</code> and the domain is <code>ibm.com</code>, the Login DN would be <code>cn=admin,dc=ibm,dc=com</code>.</p>

- Click **Test connection** to test the connection information.

You must provide user information to authenticate against the user attributes that you specified in **LDAP User Field**. If you specified multiple values in **LDAP User Field**, you must provide user information to authenticate against the first attribute that is specified.

- Select the authorization method to use.

Learn more about authorization methods:

Table 8. LDAP authorization methods	
Authorization method parameter	Description
Local	The user name and password combination is verified for each user that logs in, but no authorization information is exchanged between the LDAP server and QRadar server. If you chose Local authorization, you must create each user on the QRadar console.
User attributes	Choose User Attributes when you want to specify which user role and security profile attributes can be used to determine authorization levels. You must specify both a user role attribute and a security profile attribute. The attributes that you can use are retrieved from the LDAP server, based on your connection settings. User attribute values are case-sensitive.
Group based	Choose Group Based when you want users to inherit role-based access permissions after they authenticate with the LDAP server. The mapping of group names to user roles and security profiles is case-sensitive.
Group base DN	Specifies the start node in the LDAP directory for loading groups. For example, if all of your groups are on the directory server in the Groups folder, and your domain name is <code>ibm.com</code> , the Group Base DN value would be <code>cn=Groups,dc=ibm,dc=com</code> .
Query limit enabled	Sets a limit on the number of groups that are returned.
Query result limit	The maximum number of groups that are returned by the query. By default, the query results are limited to show only the first 1000 query results.
By member	Select By Member to search for groups based on the group members. In the Group Member Field box, specify the LDAP attribute that is used to define the users group membership. For example, if the group uses the <code>memberUid</code> attribute to determine group membership, type <code>memberUid</code> in the Group Member Field box.
By query	Select By Query to search for groups by running a query. You provide the query information in the Group Member Field and Group Query Field text boxes. For example, to search for all groups that have at least one memberUid attribute and that have a cn value that starts with the letter 's', type <code>memberUid</code> in Group Member Field and type <code>cn=s*</code> in Group Query Field .

- If you specified Group Based authorization, click **Load Groups** and click the plus (+) or minus (-) icon to add or remove privilege groups.

The user role privilege options control which QRadar components the user has access to. The security profile privilege options control the QRadar data that each user has access to.

Note: Query limits can be set by selecting the **Query Limit Enabled** check box or the limits can be set on the LDAP server. If query limits are set on the LDAP server, you might receive a message that indicates that the query limit is enabled even if you did not select the **Query Limit Enabled** check box.

9. Click **Save**.
10. Click **Manage synchronization** to exchange authentication and authorization information between the LDAP server and the QRadar console.
 - a) If you are configuring the LDAP connection for the first time, click **Run Synchronization Now** to synchronize the data.
 - b) Specify the frequency for automatic synchronization.
 - c) Click **Close**.
11. Repeat the steps to add more LDAP servers, and click **Save Authentication Module** when complete.

Synchronizing data with an LDAP server

You can manually synchronize data between the IBM Security QRadar server and the LDAP authentication server.

About this task

If you use authorization that is based on user attributes or groups, user information is automatically imported from the LDAP server to the QRadar console.

Each group that is configured on the LDAP server must have a matching user role or security profile that is configured on the QRadar console. For each group that matches, the users are imported and assigned permissions that are based on that user role or security profile.

By default, synchronization happens every 24 hours. The timing for synchronization is based on the last run time. For example, if you manually run the synchronization at 11:45 pm, and set the synchronization interval to 8 hours, the next synchronization will happen at 7:45 am. If the access permissions change for a user that is logged in when the synchronization occurs, the session becomes invalid. The user is redirected back to the login screen with the next request.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management > Authentication**.
3. In the **Authentication Module** list, select **LDAP**.
4. Click **Manage Synchronization > Run Synchronization Now**.

Configuring SSL or TLS certificates

If you use an LDAP directory server for user authentication and you want to enable SSL encryption or TLS authentication, you must configure your SSL or TLS certificate.

Procedure

1. Using SSH, log in to your system as the root user.
 - a) User name: root
 - b) Password: <password>
2. Type the following command to create the /opt/qradar/conf/trusted_certificates/ directory:

```
mkdir -p /opt/qradar/conf/trusted_certificates
```
3. Copy the SSL or TLS certificate from the LDAP server to the /opt/qradar/conf/trusted_certificates directory on your system.
4. Verify that the certificate file name extension is .cert, which indicates that the certificate is trusted.

The QRadar system loads only .cert files.

Displaying hover text for LDAP information

You create an LDAP properties configuration file to display LDAP user information as hover text. This configuration file queries the LDAP database for LDAP user information that is associated with events, offenses, or assets (if available).

Before you begin

The web server must be restarted after the LDAP properties is created. Consider scheduling this task during a maintenance window when no active users are logged in to the system.

About this task

The following example lists properties that you can add to an ldap.properties configuration file.

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=user.name
ldap.password=your.encrypted.password
ldap.basedn=O=IBM,C=US
ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

Procedure

1. Use SSH to log in to IBM Security QRadar as a root user.
2. To obtain an encrypted LDAP user password, run the following **perl** script:

```
perl -I /opt/qradar/lib/Q1/ -e 'print "Password: ";my $password = <>;
$password =~ s/\n$//;use auCrypto; print Q1::auCrypto::encrypt ($password)'
```

3. Use a text editor to create the /opt/qradar/conf/ldap.properties configuration file.
4. Specify the location and authentication information to access the remote LDAP server.
 - a) Specify the URL of the LDAP server and the port number.

Use ldaps:// or ldap:// to connect to the remote server, for example, ldap.url=ldaps://LDAPserver.example.com:389.
 - b) Type the authentication method that is used to access the LDAP server.

Administrators can use the simple authentication method, for example, ldap.authentication=simple.
 - c) Type the user name that has permissions to access the LDAP server.

For example, ldap.userName=user.name.
 - d) To authenticate to the remote LDAP server, type the encrypted LDAP user password for the user.

For example, ldap.password=password.
 - e) Type the base DN used to search the LDAP server for users.

For example, ldap.basedn=BaseDN.
 - f) Type a value to use for the search parameter filter in LDAP.

For example, in QRadar, when you hover over ldap.filterString=(&(objectclass=user)(samaccountname=%USER%)), the %USER% value is replaced by the user name.
5. Type one or more attributes to display in the hover text.

You must include at least one LDAP attribute. Each value must use this format:

ldap.attributes.AttributeName=Descriptive text to show in UI.

6. Verify that there is read-level permission for the `ldap.properties` configuration file.
7. Log in to QRadar as an administrator.
8. On the navigation menu (☰), click **Admin**.
9. Click **Advanced** > **Restart Web Server**.

Results

Administrators can hover over the **Username** field on the **Log Activity** tab and **Offenses** tab, or hover over the **Last User** field on the **Assets** tab (if available) to display more information about the LDAP user.

Multiple LDAP repositories

You can configure IBM Security QRadar to map entries from multiple LDAP repositories into a single virtual repository.

If multiple repositories are configured, when a user logs in, they must specify which repository to use for authentication. They must specify the full path to the repository and the domain name in the user name field. For example, if Repository_1 is configured to use domain `ibm.com` and Repository_2 is configured to use domain `ibm.ca.com`, the login information might look like these examples:

- `OU=User Accounts,OU=PHX,DC=qcorpaa,DC=aa,DC=ibm.com\username`
- `OU=Office,OU=User Accounts,DC=qcorpaa,DC=aa,DC=ibm.ca.com\username`

User information is automatically imported from the LDAP server for repositories that use user attributes or group authorization. For repositories that use local authorization, you must create users directly on the QRadar system.

Example: Least privileged access configuration and set up

Grant users only the minimum amount of access that they require to do their day-to-day tasks.

You can assign different privileges for IBM Security QRadar data and QRadar capabilities. You can do this assignment by specifying different accept and deny groups for security profiles and user roles. Accept groups assign privileges and deny groups restrict privileges.

Let's look at an example. Your company hired a group of student interns. John is in his final year of a specialized cyber security program at the local university. He was asked to monitor and review known network vulnerabilities and prepare a remediation plan based on the findings. Information about the company's network vulnerabilities is confidential.

As the QRadar administrator, you must ensure that the student interns have limited access to data and systems. Most student interns must be denied access to IBM Security QRadar Vulnerability Manager, but John's special assignment requires that he has this access. Your organization's policy is that student interns never have access to the QRadar API.

The following table shows that John must be a member of the **company.interns** and **qvm.interns** groups to have access to IBM Security QRadar Risk Manager and QRadar Vulnerability Manager.

Table 9. User role privilege groups		
User Role	Accept	Deny
Admin	qradar.admin	company.firedemployees
QVM	qradar.qvm qvm.interns	company.firedemployees qradar.qrm company.interns
QRM	qradar.qrm company.interns	company.firedemployees

The following table shows that the security profile for **qvm.interns** restricts John from accessing the QRadar API.

<i>Table 10. Security profile privilege groups</i>		
Security profile	Accept	Deny
QVM	qradar.secprofile.qvm	company.firedemployees
API	qradar.secprofile.qvm.api	company.firedemployees qradar.secprofile.qvm.interns

Chapter 4. License management

License keys entitle you to specific IBM Security QRadar products, and control the event and flow capacity for your QRadar deployment. You can add licenses to your deployment to activate other QRadar products, such as QRadar Vulnerability Manager.

When you install QRadar, the default license key is temporary and gives you access to the system for 35 days from the installation date. The email that you received from IBM when you purchased QRadar contains your permanent license keys. These license keys extend the capabilities of your appliance, and you must apply them before the default license expires.

To apply a license key to the system, follow these steps:

1. Obtain the license key. For new or updated license keys, contact your local sales representative.
2. [Upload the license key.](#)
3. [Allocate the license to a system.](#)
4. [Deploy the full configuration.](#)

After you apply the license keys to QRadar, [redistribute the EPS and FPM rates](#) to ensure that each of the managed hosts is allocated enough capacity to handle the average volume of network traffic, and still have enough EPS and FPM available to efficiently handle a data spike. You do not need to deploy the changes after you redistribute the EPS and FPM capacity.

License expiry

The processing capacity of the system is measured by the volume of events and flows that QRadar can process in real time. The capacity can be limited by either the appliance hardware or the license keys. The temporary license key allows for 5,000 events per second (EPS) on the QRadar Console, and 10,000 EPS on each managed host. The FPM rate for the temporary license is 200,000 on both the QRadar Console and the managed hosts.

When a license expires, QRadar continues to process events and flows up to the licensed capacity limits. If the EPS and FPM capacity of the expired license was allocated to a host, the shared license pool might go into a deficit, and cause QRadar to block capabilities on the **Network Activity** and **Log Activity** tabs.

When QRadar is not licensed to handle the volume of incoming network data, you can add a license that has more event or flow capacity.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

[System management](#)

IBM Security QRadar has a modular architecture that supports deployments of varying sizes and topologies.

Event and flow processing capacity

The capacity of a deployment is measured by the number of events per second (EPS) and flows per minute (FPM) that IBM Security QRadar can collect, normalize, and correlate in real time. The event and flow capacity is set by the licenses that are uploaded to the system.

Each host in your QRadar deployment must have enough event and flow capacity to ensure that QRadar can handle incoming data spikes. Most incoming data spikes are temporary, but if you continually receive system notifications that indicate that the system exceeded the license capacity, you can replace an existing license with a license that has more EPS or FPM capacity.

Related concepts

[Burst handling](#)

IBM Security QRadar uses burst handling to ensure that no data is lost when the system exceeds the allocated events per second (EPS) or flows per minute (FPM) license limits.

Related tasks

[Distributing event and flow capacity](#)

Shared license pool

The EPS and FPM rate that is set by each license is combined into a shared license pool. From the shared license pool, you can distribute the processing capacity to any host within a specific deployment or that is managed by a single console, regardless of which host the original license is allocated to.

By adjusting the allocation of the shared license pool, you ensure that the event and flow capacity is distributed according to the network workload, and that each QRadar host has enough EPS and FPM to effectively manage periods of peak traffic.

In deployments that have separate event collector and event processor appliances, the event collector inherits the EPS rate from the event processor that it is attached to. To increase the capacity of the event collector, allocate more EPS from the shared license pool to the parent event processor.

Contributions to the license pool

A license that includes both event and flow capacity might not contribute both the EPS and FPM to the shared license pool. The license pool contributions depend on the type of appliance that the license is allocated to. For example, when you apply a license to a 16xx Event Processor, only the EPS is added to the license pool. The same license, when applied to a 17xx Flow Processor, contributes only the FPM to the license pool. Applying the license to an 18xx Event/Flow Processor contributes both EPS and FPM to the pool. With exception of software licenses for event or flow collectors, all software licenses contribute both the EPS and FPM to the shared license pool, regardless of which type of appliance the license is allocated to.

A license key that has a serial number can apply to only one host, and the EPS and FPM capacity of that license cannot be allocated to another host. As a result, a license key that has a serial number does not contribute to the shared license pool.

Exceeding your licensed processing capacity limits

The license pool becomes over-allocated when the combined EPS and FPM that is allocated to the managed hosts exceeds the EPS and FPM that is in the shared license pool. When the license pool is overallocated, the **License Pool Management** window shows a negative value for the EPS and FPM, and the allocation chart turns red. QRadar blocks functionality on the **Network Activity** and **Log Activity** tabs, including the ability to view events and flows from the **Messages** list on the main QRadar toolbar.

To enable the blocked functionality, reduce the EPS and FPM that you allocated to the managed hosts in your deployment. If the existing licenses do not have enough event and flow capacity to handle the volume of network data, upload a new license that includes enough EPS or FPM to resolve the deficit in the shared license pool.

Expired licenses

When a license expires, QRadar continues to process events and flows at the allocated rate.

If the EPS and FPM capacity of the expired license was allocated to a host, the shared resources in the license pool might go into a deficit, and cause QRadar to block functionality on the **Network Activity** and **Log Activity** tabs.

Capacity sizing

The best way to deal with spikes in data is to ensure that your deployment has enough events per second (EPS) and flows per minute (FPM) to balance peak periods of incoming data. The goal is to allocate EPS

and FPM so that the host has enough capacity to process data spikes efficiently, but does not have large amounts of idle EPS and FPM.

When the EPS or FPM that is allocated from the license pool is very close to the average EPS or FPM for the appliance, the system is likely to accumulate data in a temporary queue to be processed later. The more data that accumulates in the temporary queue, also known as the burst-handling queue, the longer it takes QRadar to process the backlog. For example, a QRadar host with an allocated rate of 10,000 EPS takes longer to empty the burst handling queue when the average EPS rate for the host is 9,500, compared to a system where the average EPS rate is 7,000.

Offenses are not generated until the data is processed by the appliance, so it is important to minimize how frequently QRadar adds data to the burst handling queue. By ensuring that each managed host has enough capacity to process short bursts of data, you minimize the time that it takes for QRadar to process the queue, ensuring that offenses are created when an event occurs.

When the system continuously exceeds the allocated processing capacity, you cannot resolve the problem by increasing the queue size. The excess data is added to the end of the burst handling queue where it must wait to be processed. The larger the queue, the longer it takes for the queued events to be processed by the appliance.

Related concepts

Example: Incoming data spike

Every morning, between 8am and 9am, a company's network experiences a data spike as employees log in and begin to use the network resources.

Internal events

IBM Security QRadar appliances generate a small number of internal events when they communicate with each other as they process data.

To ensure that the internal events are not counted against the allocated capacity, the system automatically returns all internal events to the license pool immediately after they are generated.

Burst handling

IBM Security QRadar uses burst handling to ensure that no data is lost when the system exceeds the allocated events per second (EPS) or flows per minute (FPM) license limits.

When QRadar receives a data spike that causes it to exceed the allocated EPS and FPM limits, the extra events and flows are moved to a temporary queue to be processed when the incoming data rate slows. When burst handling is triggered, a system notification alerts you that the appliance exceeded the EPS or FPM license limit.

The backlog in the temporary queue is processed in the order that the events or flows were received. The older data at the start of the queue is processed before the most recent data at the end of the queue. The rate at which the queue empties or fills is impacted by several factors, including the volume and duration of the data spike, the capacity of the appliance, and the payload size.

Hardware appliances normally can handle burst rates at least 50% greater than the appliance's stated EPS and FPM capability, and can store up to 5GB in the temporary queue. The actual burst rate capability depends upon the system load. VM appliances can achieve similar results if the VM is adequately sized and meets the performance requirements.

The burst recovery rate is the difference between the allocated rate and the incoming rate. When the volume of incoming data slows, the system processes the backlog of events or flows in the queue as fast as the recovery rate allows. The smaller the recovery rate, the longer it takes to empty the queue.

Related concepts

Event and flow processing capacity

Related tasks

Distributing event and flow capacity

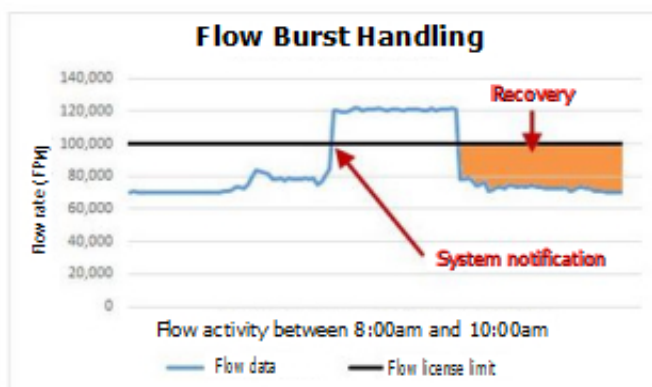
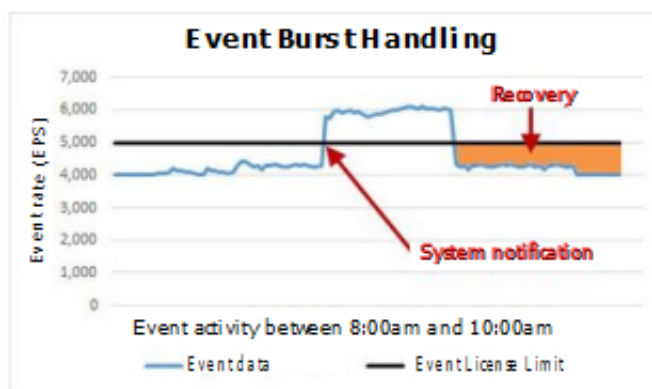
Example: Incoming data spike

Every morning, between 8am and 9am, a company's network experiences a data spike as employees log in and begin to use the network resources.

The company's deployment includes a QRadar 1828 Event/Flow Processor appliance that is allocated 5,000 events per second (EPS) and 100,000 flows per minute (FPM). The average capacity for this appliance is 4,000 EPS and 70,000 FPM.

During the data spike, which peaks around 9am, the appliance routinely receives up to 6,000 EPS and 120,000 FPM. QRadar automatically moves the extra events and flows (1,000 EPS and 20,000 FPM) to the burst handling queue, and generates a system notification to alert the administrator that the appliance exceeded the allocated capacity.

The following images show a two-hour window when the incoming event and flow data exceeds the licensed capacity, which triggers a system notification, and a recovery period after the data volume returns to normal.



The recovery rate is the difference between the allocated EPS or FPM amount and the current incoming data rate. In this example, when the event and flow rates return to normal, the recovery rate is 1,000 EPS and 30,000 FPM.

5,000 licensed events - 4,000 incoming events = 1,000 EPS recovery rate
100,000 licensed flows - 70,000 incoming flows = 30,000 FPM recovery rate

Offenses are not generated until the data is processed by the appliance, so it is important to allocate enough EPS and FPM to the appliance to ensure that it can recover from a data spike quickly.

Related concepts

Capacity sizing

The best way to deal with spikes in data is to ensure that your deployment has enough events per second (EPS) and flows per minute (FPM) to balance peak periods of incoming data. The goal is to allocate EPS and FPM so that the host has enough capacity to process data spikes efficiently, but does not have large amounts of idle EPS and FPM.

Related tasks

[Distributing event and flow capacity](#)

Uploading a license key

License keys determine your entitlement to IBM Security QRadar products and features, and the system capacity for handling events and flows.

Before you begin

If you need assistance to obtain a new or updated license key, contact your local sales representative.

About this task

You must upload a license key when you are doing these tasks:


- Updating an expired QRadar console license
- Increasing the events per minute (EPS) or flows per minute (FPM) limits
- Adding a QRadar product to your deployment, such as IBM Security QRadar Vulnerability Manager, to your deployment

In QRadar V7.3.0, you do not need to upload a new license when you add an Event Processor or Flow Processor to your deployment. Event and flow processors are automatically assigned a perpetual, or permanent, appliance license, and you can allocate EPS or FPM from the license pool to the appliance.

If the license key for your QRadar Console expires, you are automatically directed to the **System and License Management** window when you log on. You must upload a license key before you can continue.

If a managed host system has an expired license key, a message is displayed when you log in that indicates that a managed host requires a new license key. You use the **System and License Management** window to update the license key. If the license pool is not over allocated, delete the expired key and allocate EPS or FPM from the license pool to the managed host.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. On the toolbar, click **Upload License**.
4. In the dialog box, click **Select File**.
5. Select the license key, and click **Open**.
6. Click **Upload**, and then click **Confirm**.

Results

The license is uploaded to your QRadar Console and is displayed in the **System and License Management** window.

By default, most licenses are not immediately allocated to a QRadar host. However, the system automatically allocates all QRadar Vulnerability Manager, QRadar Risk Manager, and QRadar Incident Forensics keys to the QRadar console.

What to do next

Allocate the license to a system.

Allocating a license key to a host

Allocate a license key to an IBM Security QRadar host when you want to replace an existing license, add new QRadar products, or increase the event or flow capacity in the shared license pool.

Before you begin


You must upload a license key.

About this task

You can allocate multiple licenses to a QRadar console. For example, you can allocate license keys that add IBM Security QRadar Risk Manager and QRadar Vulnerability Manager to your QRadar console.

You cannot revert a license key after you add it to a QRadar host. If you mistakenly allocate a license to the wrong host, you must deploy the change, and then delete the license from the system. After the license is deleted, you can upload the license again, and then reallocate it. After the license is allocated to the correct host, you must deploy the changes again.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. From the **Display** list, select **Licenses**.
4. Select the license, and click **Allocate System to License**.

Tip: When you select **System** from the **Display** list, the label changes to **Allocate License to a System**.

5. To filter the list of licenses, type a keyword in the search box.
6. On the **Allocate a System to a License** window, select the host that you want to allocate the license to, and click **Allocate System to License**.

Distributing event and flow capacity

Use the **License Pool Management** window to ensure that the events per second (EPS) and flows per minute (FPM) that you are entitled to is fully used. Also, ensure that IBM Security QRadar is configured to handle periodic bursts of data without dropping events or flows, or having excessive unused EPS and FPM.


Before you begin

Ensure that the license pool has enough unallocated EPS or FPM. If the EPS or FPM in the license pool is fully allocated, redistribute the allocations.

About this task

Proper allocation of EPS and FPM capacity is important to ensure that QRadar processes all events and flows in a timely manner. The goal is to allocate EPS and FPM so that the host has enough capacity to process data spikes efficiently, without having excessive idle EPS and FPM capacity.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.

3. From the **Display** list, select **Licenses**.
4. Click **License Pool Management** and hover the mouse over the circle charts to see the total capacity for the deployment.
5. In the **License Allocations** table, review the data to determine whether the appliance has enough event and flow capacity to cover the average EPS and FPM, and still have enough left to cover the peak volumes.

Learn more about reviewing the event and flow capacity data:

- The **EPS Allocation** and **FPM Allocation** columns show the capacity that is assigned to each QRadar processor or QRadar console.
 - The **Average EPS** and **Average FPM** columns show the average number of events and flows that were processed by the QRadar host over the last 30 days.
 - Click the host name to view the details about the peak EPS and FPM rates for the past 30 days.
6. To change the allocated EPS or FPM rate for the QRadar host, click the edit icon.
 7. Update the **Allocated EPS** or **Allocated FPM** field, and click **Save**.
The revised EPS and FPM allocations are validated against these criteria:
 - The EPS allocation must be a multiple of 100, and the FPM allocation must be a multiple of 5,000.
 - The allocated EPS or FPM cannot cause the license pool to be over-allocated.
 - The allocated EPS or FPM cannot exceed the hardware limits for the appliance type.

Related concepts

[Example: Incoming data spike](#)

Every morning, between 8am and 9am, a company's network experiences a data spike as employees log in and begin to use the network resources.

[Burst handling](#)

IBM Security QRadar uses burst handling to ensure that no data is lost when the system exceeds the allocated events per second (EPS) or flows per minute (FPM) license limits.

[Event and flow processing capacity](#)

Viewing license details

View the license details to see information such as the status, expiration, and event and flow rate limits for each license that is uploaded to the system.

About this task

Licenses that are not yet allocated to a host appear at the top of the **License** table. Each host in the deployment has a summary row, which is shown in bold. The **Event Rate Limit** and the **Flow Rate Limit** fields on the summary row shows the EPS and FPM that is allocated to the host. If the host does not have any allocated EPS or FPM, **N/A** is shown in the **Event Rate Limit** and the **Flow Rate Limit** columns.

Licenses that are allocated to a QRadar host appear as a child row, nested beneath the QRadar host summary row. For the QRadar Console and Event and Flow Processor appliances, the child row shows the capacity and expiration dates for the EPS and FPM portion of the license. Before you manage the licenses, select the row that corresponds to the individual license.

Procedure


1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. From the **Display** list, select **Licenses**.
4. To view detailed information about a specific host or license, select the nested row, and then click **Actions > View License**.

Table 11. License	
State	Description
Unallocated	The license is uploaded but not allocated to a QRadar host. The EPS and FPM of the license don't contribute to the license pool.
Undeployed	The license is allocated to a QRadar host, but is not deployed. The license is not yet active in your deployment. The EPS and FPM are included in the license pool.
Deployed	The license is allocated and active in your deployment. The EPS and FPM are included in the license pool.

Deleting licenses

Delete a license if you mistakenly allocated it to the wrong QRadar host. Also, delete an expired license to stop IBM Security QRadar from generating daily system notifications about the expired license.

About this task

You cannot delete a license if it causes the license pool to be over-allocated. QRadar validates that the license pool has enough unallocated EPS and FPM capacity to cover the loss in capacity when the license is deleted. For example, if you want to delete a license that has 2,500 EPS associated with it, the license pool must have at least 2,500 EPS that has not been allocated to a QRadar host.

If the license pool does not have enough unallocated EPS and FPM to cover the deficit, you must adjust the EPS and FPM allocations to ensure that the pool is not over-allocated when you delete the license.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. From the **Display** list, select **Licenses**.
4. In the host table, select the nested child row that contains the license that you want to delete.
5. Click **Actions > Delete License**.

The **License Expiration Date** shows **Perpetual** with an **Event Rate Limit** and **Flow Rate Limit** of 0.

Exporting license information

For auditing, export information about the license keys that are installed on your system to an external .xml file.

You can't use the .xml file to move licenses to another system. Use it only for viewing detailed information about the individual license keys.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. From the **Display** list, select **Licenses**.
4. From the **Actions** menu, select **Export Licenses**.
5. Save the file locally and click **OK**.

Chapter 5. System management

IBM Security QRadar has a modular architecture that supports deployments of varying sizes and topologies.

In a single-host deployment, all the software components run on a single appliance, and the QRadar Console provides the user interface, the real-time event and flow views, reports, offenses, asset information, and administrative functions.

To scale QRadar, you can add non-console managed hosts to the deployment. You can configure a specific component type, such as collectors, processors, and data nodes, for each managed host, providing greater flexibility to manage data collection and processing in a distributed environment.

Related concepts

[License management](#)

License keys entitle you to specific IBM Security QRadar products, and control the event and flow capacity for your QRadar deployment. You can add licenses to your deployment to activate other QRadar products, such as QRadar Vulnerability Manager.

[Capabilities in your IBM Security QRadar product](#)

View system health information

The QRadar Deployment Intelligence app is a powerful monitoring application that consolidates historical health data for each managed host in your deployment. Use the app to monitor the health of your QRadar deployment.

The **Host status overview** on the QRadar Deployment Intelligence dashboard shows the state of each appliance (active, standby, offline, or unknown), and the number of notifications for each host, the host name and appliance type, disk usage, status, and time changed. From the **Host status overview**, you can drill down to see more visual information about the status of the managed host, including the event and flow rates, system notifications, and disk information.

To assist with troubleshooting issues in your deployment, use the **Get Logs** capability to collect log files from the QRadar Console and any other managed hosts in your deployment.

The QRadar Deployment Intelligence app is available on the IBM Security App Exchange. You must install the app and then create an authorized service token to allow the app to use the QRadar API to request data from the managed hosts.

The QRadar Deployment Intelligence app uses QRadar health metrics to monitor your deployment. Health metrics are essential, lightweight system events that do not count against your license.

QRadar component types

Each IBM Security QRadar appliance that is added to the deployment has configurable components that specify the way that the managed host behaves in QRadar.

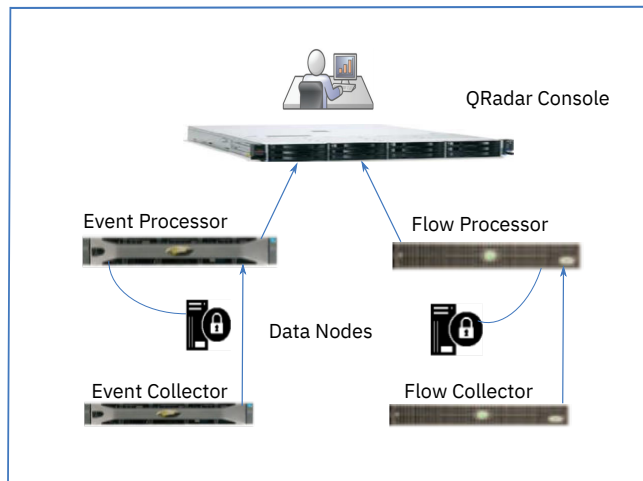


Figure 2. QRadar event and flow components

QRadar Console

The QRadar Console provides the QRadar product interface, real-time event and flow views, reports, offenses, asset information, and administrative functions. In distributed environments, the QRadar Console is used to manage the other components in the deployment.

Event Collector

The Event Collector collects events from local and remote log sources, and normalizes the raw event data so that it can be used by QRadar. To conserve system resources, the Event Collector bundles identical events together and sends the data to the Event Processor.

Event Processor

The Event Processor processes events that are collected from one or more Event Collector components. If events are matched to the custom rules that are defined on the Console, the Event Processor follows the action that is defined in the rule response.

Each Event Processor has local storage. Event data is stored on the processor, or it can be stored on a Data Node.

QRadar QFlow Collector

QRadar QFlow Collector collects network flows from devices on your network. Live and recorded feeds are included, such as network taps, span ports, NetFlow, and QRadar flow logs.

Restriction: QRadar Log Manager doesn't support flow collection.

Flow Processor

The Flow Processor processes flows from one or more QRadar QFlow Collector appliances. The Flow Processor appliance can also collect external network flows such as NetFlow, J-Flow, and sFlow directly from routers in your network.

Flow Processors include an on-board processor and internal storage for flow data.

Data Node

The Data Node receives security events and flows from event and flow processors, and stores the data to disk.

The Data Node is always connected to either an Event Processor or a Flow Processor.

Off-site source and target appliances

An off-site appliance is a QRadar appliance that is not part of the deployment that is monitored by the QRadar Console.

An off-site source appliance forwards normalized data to an Event Collector. You can configure an off-site source to encrypt the data before forwarding.

An off-site target appliance receives normalized event or flow data from any Event Collector, or any processor in your deployment.

Later versions of QRadar systems can receive data from earlier versions of QRadar systems, but earlier versions can't receive data from later versions. To avoid problems, upgrade all receivers before you upgrade senders.

Data nodes

A data node is an appliance that you can add to your event and flow processors to increase storage capacity and improve search performance. You can add an unlimited number of data nodes to your IBM Security QRadar deployment, and they can be added at any time. Each data node can be connected to only one processor, but a processor can support multiple data nodes.

For more information about planning your deployment, see the *IBM Security QRadar Architecture and Deployment Guide*.

Data rebalancing after a data node is added

When you add a data node, IBM Security QRadar rebalances the data to improve search and overall system performance.

Data rebalancing includes decompressing older data, and moving data that was on the original storage device to evenly distribute it across all connected devices.

For example, your deployment has an event processor that receives 20,000 events per second (EPS). When you add data nodes, QRadar automatically distributes the events across the event processor and all data nodes that are available to it. If you add three data nodes, the event processor stores 5,000 EPS and sends 5,000 EPS to each of the attached data nodes. The event processor is still processing all of the events, but the data nodes provide more storage, indexing, and search capabilities to improve the overall performance.

Data that is collected in QRadar V7.2.6 and earlier

By default, data that is collected with QRadar V7.2.6 and earlier versions is not compressed. Data compression occurs only when QRadar detects that the available storage on a device is less than the available storage threshold. The disk maintenance process compresses the data into gzip format, and applies the data deletion policies until the volume of data is back within the threshold amount.

When you add a data node, QRadar rebalances the data, and when enough storage space is available, data that is in `gzip` format is decompressed. The search performance on the older data immediately improves, and performance continues to improve because most searches use more recent data that is uncompressed.

Because the pre-V7.2.7 data is now decompressed, the disk volumes might quickly exceed the threshold for free storage space. When the available disk space falls beneath the threshold settings, the disk maintenance process compresses any data that is eligible for compression, according to the retention policies, until the free storage threshold is reached.

Data that is collected in QRadar V7.2.7 and later

In QRadar V7.2.7, all new data is written to disk in compressed format. The disk maintenance processes do not compress new data.

The data deletion policy is not affected by the data format. When QRadar exceeds the available storage threshold, the disk maintenance processes delete data in both the old and new format according to the data retention settings.

Viewing the progress of data rebalancing

When you add a data node, IBM Security QRadar automatically redistributes the data to balance it across the storage volumes in your deployment.

Search performance improvements are realized only after the data rebalancing is complete. You can view the progress of the data rebalancing, and also see data such as the percentage of disk space that is used.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. In the host table, select the managed host that you want to view more information about.
 - To view information about the cluster of managed hosts, select the top-level host.
 - To view information about a specific data node, select the data node.
5. On the **Actions** menu, click **View and manage system**.
6. Click the **Security Data Distribution** tab to view the progress of data rebalancing and the capacity of the Data Node appliance.

Note: You can also view information about the progress of data node rebalancing in the deployment status bar on the **Admin** tab.


Saving all event data to a Data Node appliance

To improve the performance of an event processor, configure IBM Security QRadar to save all event data on a Data Node appliance. With this configuration, the event processor only processes events; it doesn't store event data locally.

An event processor that is configured to only process events still saves event data locally when no active Data Node appliances are available. When a Data Node appliance becomes available, QRadar transfers as much data as possible from the event processor to the Data Node.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the Event Processor from the host table, and on the **Deployment Actions** menu, click **Edit Host**.



5. Click the **Component Management** settings icon ()
6. Under **Event Processor**, in the **Event Processor Mode** field, select **Processing-Only**.
7. Click **Save**, and then click **Save** again.
8. On the **Admin** tab, click **Deploy Changes**.

Archiving Data Node content

Configure a Data Node appliance to use **Archive** mode when you want the Data Node to provide online access to historical data without impacting storage for incoming data.

In **Archive** mode, the appliance does not receive new data, but existing data is saved.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the Data Node appliance in the host table, and on the **Deployment Actions** menu, click **Edit Host**.
5. Click the **Component Management** settings icon ()
6. In the **Data Node Mode** field, select **Archive**, and then click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

What to do next

To resume storing data on the Data Node appliance, set the mode back to **Active**.

Network interface management

In addition to the default management interface, you can add extra network interfaces to your IBM Security QRadar appliances to provide alternative network connectivity.

Use extra network interfaces for the following purposes:

- Provide a dedicated crossover connection between high-availability (HA) peers. You configure a crossover connection during HA setup.
- Provide a dedicated data collection interface for inbound events or external flow sources. TCP-based data sources must be in the same subnet as the data collection interface.
- Connect to backup and network storage systems (iSCSI).
- Increase bandwidth and add fault tolerance by bonding interfaces.

Note: WinCollect configurations that are connected to a non-managed port are not supported.

Configuring network interfaces

Use bonding to increase the available bandwidth or the fault tolerance of your IBM Security QRadar appliances by combining 2 or more network interfaces into a single channel.


Before you begin

Note: The QRadar appliance network management interface, including bonding options, is configured only at the UNIX shell prompt during setup.

Configure the management interface on a QRadar Console before you add a managed host. See "Configuring bonded management interfaces" in *IBM Security QRadar Installation Guide* for more information about configuring the management interface.

You can't bond an existing slave interface. You can bond management interfaces only at the shell prompt. You can bond crossovers from the **High Availability** (HA) configuration screen.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. From the **Display** menu, click **Systems**.
4. Select the host for which you want to configure network interfaces.
5. Click **Actions > View and Manage System**, and click the **Network Interfaces** tab.
6. To edit a network interface, follow these steps:
 - a) Select the device that you want to edit, and click **Edit**.
 - b) In the **Role** list, select the role for the device:
 - Choose **Regular** when the device is used for data collection.
This interface must have an IP address. The subnet of the interface cannot be the same subnet used by the management interface.
 - Choose **Monitor** when the device is a IBM Security QRadar QFlow Collector that is used for packet collection. This interface does not require an IP address.
 - Choose **Disabled** to prevent the device from being used for any network connectivity.
 - c) To apply the configuration to the active HA node, click **Apply this interface configuration and IP address to the active HA node**.
 - d) Click **Save**.
7. To create a bonded network interface, follow these steps:

You can bond two or more interfaces that have either a regular or monitor role that is assigned to them. You can bond only interfaces that are assigned the same roles.

 - a) Select the device and click **Bond**.
 - b) Type the IP address and netmask.
 - c) To apply the configuration to the active HA node, click **Apply this interface configuration and IP address to the active HA node**.

Note: By selecting this option, you keep the interface active on whichever of the two high-availability (HA) nodes is active. You can use this option on an interface that is used to receive inbound data, such as syslog messages or netflow data records. This option migrates data between the primary and secondary nodes, to whichever one is active.

 - d) Enter a bonding option. The default bonding option that is configured on this interface is mode=4.

Note:

Bonded interfaces support various modes of operation, depending on the capabilities of the switch that they are connected to. The following table describes the supported bonding modes that you might use.

Table 12. Bonding modes		
Bonding modes	Bonding name	Description
mode=1	Active backup	Only one slave is active. Another slave becomes active when the active slave fails.
mode=4	802.3ad	Uses Link Aggregation Control Protocol (LACP) to create aggregation groups that share duplex settings and speed.

For more information about configuring specific bonding options, see your vendor-specific operating system documentation.

- e) Click **Add** and select the interface that you want to add as a slave, and then click **OK**.
 - f) Click **Save** to create your bonded interface.
8. To break a bonded interface back into single interfaces, select the bonded device, and then click **Unbond**.

What to do next

If the connection doesn't work when you configure your bonded interface settings, use SSH to log in to the host, and look in the `/var/log/message` log file for any network interface errors.

You can also try changing the setting to `mode=1`, or you can physically disconnect all but one of the Ethernet connections in the bonded interface group. If this workaround works, verify that your switch infrastructure supports the mode that you are trying to use. Switches don't always support `mode=4`.

QRadar system time

When your deployment spans multiple time zones, configure all appliances to use the same time zone as the IBM Security QRadar Console. Alternatively, you can configure all appliances to use Greenwich Mean Time (GMT).

Configure the IBM Security QRadar system time from the QRadar user interface. You can configure the time manually, or by configuring Network Time Protocol (NTP) servers to maintain the system time.

The time is automatically synchronized between the QRadar Console and the managed hosts.

Problems that are caused by mismatched time zones

To ensure that searches and data-related functions work properly, all appliances must synchronize time settings with the QRadar Console appliance. When the time zone settings are mismatched, you might see inconsistent results between QRadar searches and report data.


The Accumulator service runs on all appliances with local storage to create minute by minute accumulations, and hourly and daily roll ups. QRadar uses the accumulated data in reports and time series graphs. When the time zones are mismatched in a distributed deployment, report and time series graphs might show inconsistent results when compared to AQL query results due to the way that the accumulated data is aggregated.

QRadar searches run against data that is stored in the Ariel databases, which use a date structure (YYYY/MM/DD/HH/MM) to store files to disk. Changing the time zone after the data is written to disk disrupts the file naming sequence in the Ariel databases and might cause data integrity problems.

Configuring system time

Configure system time on your QRadar Console by setting the time manually, or by using NTP servers to maintain the time. QRadar synchronizes the QRadar Console time with the managed hosts in your deployment.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the host for which you want to configure the system time settings.
5. From the **Actions** menu, click **View and Manage System**.
6. Click the **System Time** tab.
7. To configure time on the QRadar Console, follow these steps:

- a) In the **Time Zone** list, select the time zone that applies to the QRadar Console.
- b) To manually configure the time, click **Set time manually:**, and then set the date and time for the console.
Note: If you set the system time to a future date that is affected by Daylight Saving Time (DST) changes, the time you set is adjusted by 1 hour. For example, on 4 July 2016 in the U.S.A, you set the date to December 16, 2016 and the time to 8:00 PM. The time that you set ignores the DST change and is adjusted to 7:00 PM.
- c) To manage time by using NTP servers, follow these steps:
 - 1) Click **Specify NTP Servers**, and click **Add More**.
 - 2) In the **Server 1 Address** field, type an IP address or a host name for the NTP server. Host names are resolved by a DNS server.
8. To configure time on a managed host, in the **Time Zone** list, select the time zone that applies to the host.
On a managed host, you can configure only the time zone. The system time is synchronized with the QRadar Console but if the managed host is in a different time zone, then you can change to that time zone.
9. Click **Save**.
10. Click **OK** to accept that services are restarted, or **Cancel** to cancel the changes.
Data collection for events and flows stops until the hostcontext and tomcat services are restarted.

What to do next

When you set the system time on VMware systems and then restart the system, the changes might be lost. To prevent the time changes from being lost, you can disable time synchronization on the virtual device by editing the virtual machine's configuration file and adding these lines to the synchronization properties:

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

The .vmx file is typically located in the directory where you created the virtual machine. For more information, see the vendor-specific documentation for your operating system.

NAT-enabled networks

Network address translation (NAT) converts an IP address in one network to a different IP address in another network. NAT provides increased security for your IBM Security QRadar deployment because requests are managed through the conversion process and internal IP addresses are hidden. With NAT, computers that are located on a private, internal network are converted through a network device, typically a firewall, and can communicate to the public internet through that network. Use NAT to map individual internal IP addresses to individual external IP addresses.

QRadar NAT configuration requires static NAT and allows only one public IP address per managed host.

Any QRadar host that is not in the same NAT group with its peer, or is in a different NAT group, is configured to use the public IP address of that host to reach it. For example, when you configure a public IP address on the QRadar Console, any host that is located in the same NAT group uses the private IP address of the QRadar Console to communicate. Any managed host that is located in a different NAT group uses the public IP address of the QRadar Console to communicate.

If you have a host in one of these NAT group locations that does not require external conversion, enter the private IP address in both the **Private IP** and **Public IP** fields. Systems in remote locations with a different NAT group than the console still require an external IP address and NAT, because they need to be able to establish connections to the console. Only hosts that are located in the same NAT group as the console can use the same public and private IP addresses.

Configuring a NAT group

Configure a Network Address Translation (NAT) group to limit the number of public IP addresses that are required for your IBM Security QRadar managed hosts to communicate with the internet.

Before you begin


Ensure that the NAT-enabled network is using static NAT translation.

About this task

It is important to complete the NAT configuration for each managed host in your deployment before you deploy the changes. After deployment, managed hosts that aren't NAT-enabled might not be able to communicate with the QRadar Console.

QRadar can support multiple NAT networks when the public IP address for the QRadar Console is the same in each network.

Procedure

1. On the navigation menu (☰), click **Admin**.
 2. In the **System Configuration** section, click **System and License Management**.
 3. In the **Display** list, select **Systems**.
 4. To configure a NAT group for the QRadar Console, follow these steps:
 - a) Select the QRadar Console appliance in the host table.
 - b) On the **Deployment Actions** menu, click **Edit Host**.
 - c) Select the **Network Address Translation** check box.
 - d) In the **NAT Group** list, select the NAT group that the console belongs to, or click the settings icon  to create a new NAT group.
 - e) In the **Public IP** field, type the public IP address for the console, and then click **Save**.
 5. Configure each managed host in the same network to use the same NAT group as the QRadar Console.
 - a) Select the managed host appliance in the host table.
 - b) On the **Deployment Actions** menu, click **Edit Host**.
 - c) Select the **Network Address Translation** check box.
 - d) In the **NAT Group** list, select the NAT group that the QRadar Console belongs to.
 - e) In the **Public IP** field, type the public IP address for the managed host.
- Note:** Unless an event collector is connecting to a managed host that uses NAT, configure the managed host to use the same the public IP address and the private IP address.
- f) Click **Save**.
6. On the **Admin** tab, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

What to do next

To fix communication issues between the QRadar Console and hosts that are not NAT-enabled after deployment, edit the iptables rules for the managed host to configure the local firewall to allow the QRadar Console to access the managed host.

Changing the NAT status for a managed host

Configure a managed host to use network address translation (NAT) to ensure that it can communicate with the QRadar Console and other managed hosts in the same network.

Before you begin

Ensure that the NAT-enabled network is using static NAT translation.

The QRadar Console and all managed hosts in the same network must be members of the same NAT group.

To change the NAT status for a managed host, make sure that you update the managed host configuration within IBM Security QRadar before you update the device. Updating the configuration first prevents the host from becoming unreachable, and ensures that you can continue to deploy changes to that host.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click the **System and License Management** icon.
3. In the **Display** list, select **Systems**.
4. Select the host in the host table, and on the **Deployment Actions** menu, click **Edit Host**.
5. To disable NAT, clear the **Network Address Translation** check box.
6. To enable NAT, follow these steps:
 - a) Select the **Network Address Translation** check box.
 - b) From the **NAT Group** list, select the group that the managed host belongs to.
 - c) In the **Public IP** field, type the public IP address that the managed host uses to communicate with other hosts in a different NAT group.
7. Click **Save**.
8. On the **Admin** tab, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

What to do next

If you enabled NAT, you might have to update the firewall configuration for the managed host that you want to communicate with. For more information, see [“Configuring your local firewall” on page 63](#).

Managing off-site hosts

An off-site host is a QRadar appliance that can't be accessed through the QRadar Console in your current deployment. You can configure an off-site host to transfer data to or to receive data from your QRadar deployment.

Configuring an off-site source

To forward event and flow data to an Event Collector in another deployment, configure the target deployment to include an off-site source so that it knows which computer is sending the data.

About this task

To prevent connection errors, when you configure off-site source and target components, deploy the IBM Security QRadar Console with the off-site source first. Then, deploy the QRadar Console with the off-site target.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. On the **Deployment Actions** menu, click **Manage Off-site Sources**.
5. Click **Add** and configure the parameters.

The name can be up to 20 characters in length and can include underscores or hyphens.

6. Click **Save**.
7. Click **Manage Connections** to specify which QRadar hosts you want to receive the data.
The host must have an Event Collector to receive the data.
8. Repeat the steps to configure all off-site sources that you want to configure.
9. Deploy the changes and restart the event collection service.

Configuring an off-site target

To forward event and flow data to an Event Collector in another deployment, configure the source deployment to include an off-site target so that it knows which computer to send the data to.

Before you begin

You must know the listening ports for the off-site target appliance. By default, the listening port for events is 32004, and 32000 for flows.

To find the listening port on the target appliance, follow these steps:

1. In the target deployment, click the **System and License Management** icon.
2. Select the host and click **Deployment Actions > Edit Host**.
3. Click the **Component Management** settings icon (⚙️), and find the ports in the **Event Forwarding Listening Port** and **Flow Forwarding Listening Port** fields.

About this task

To prevent connection errors, when you configure off-site source and target components, deploy the IBM Security QRadar Console with the off-site source first. Then, deploy the QRadar Console with the off-site target.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. On the **Deployment Actions** menu, click **Manage Off-site Targets**.
5. Click **Add** and configure the parameters.

The name can be up to 20 characters in length and can include underscores or hyphens. The default port to listen for events is 32004, and 32000 for flows.

Note: If the off-site target is a managed host with encrypted host connections to its console, port 22 for SSH opens no matter which port is selected in the user interface.

6. Click **Save**.
7. Click **Manage Connections** to specify which QRadar hosts you want to receive the data.
Only hosts that have an Event Collector are shown in the list.
8. Repeat the steps to configure all off-site targets that you want to configure.
9. On the **Admin** tab, click **Deploy changes**.

Generating public keys for QRadar products

To forward normalized events in IBM Security QRadar, you must copy the public key file, `/root/.ssh/id_rsa.pub`, from the off-site source to the off-site target.

If the off-site source and off-site target are on separate systems, the public key is automatically generated. If the off-site source and target are both on an all-in-one system, the public key is not automatically generated. You must manually generate the public key.

Procedure

To manually generate the public key, follow these steps:

1. Use SSH to log in to your system as the root user.
2. To generate the public key, type the following command:

```
opt/qradar/bin/ssh-key-generating
```


3. Press Enter.

The public and private key pair is generated and saved in the `/root/.ssh/id_rsa` folder.

Forwarding filtered flows

You can set up forwarding of filtered flows. You can use filtered flows to split flow forwarding across multiple boxes, and to forward specific flows for specific investigations.

Procedure

1. On the target system, set up the source system as an off-site source.
 - a) On the navigation menu () , click **Admin**.
 - b) Click **System and License Management > Deployment Actions > Manage Off-Site Sources**.
 - c) Add the source system IP address, and select **Receive Events** and/or **Receive Flows**.
 - d) Select **Manage Connections** and select which host is expecting to receive the off-site connection.
 - e) Click **Save**.
 - f) Select **Deploy Full Configuration** from the **Advanced** menu for the changes to take effect.
2. On the source system, set up the forwarding destination, IP address, and port number.
 - a) Click **Main menu > Admin**.
 - b) Click **Forwarding Destinations > Add**.
 - c) Set the IP address of the target system and the destination port.
 - d) Enter 32000 for the port number on the source system. Port 32000 is used for flow forwarding.
 - e) Select **Normalized** from the **Event Format** list.
3. Set up routing rules.
 - a) Click **Main menu > Admin**.
 - b) Click **Routing Rules > Add**.
 - c) Select the rules that you want to add.

Note: Rules forward flows that are based on offenses, or based on CRE information when **Offline Forwarding** is selected on the Routing Rules page.

The flows that are filtered on the **Routing Rules** screen are forwarded.

Example: Forwarding normalized events and flows

To forward normalized events and flows, configure the target deployment to include an off-site source so that it knows which computer is sending the data. Configure the source deployment to include an off-site target so that it knows which computer to send the data to.

About this task

The following diagram shows forwarding event and flow data between deployments.

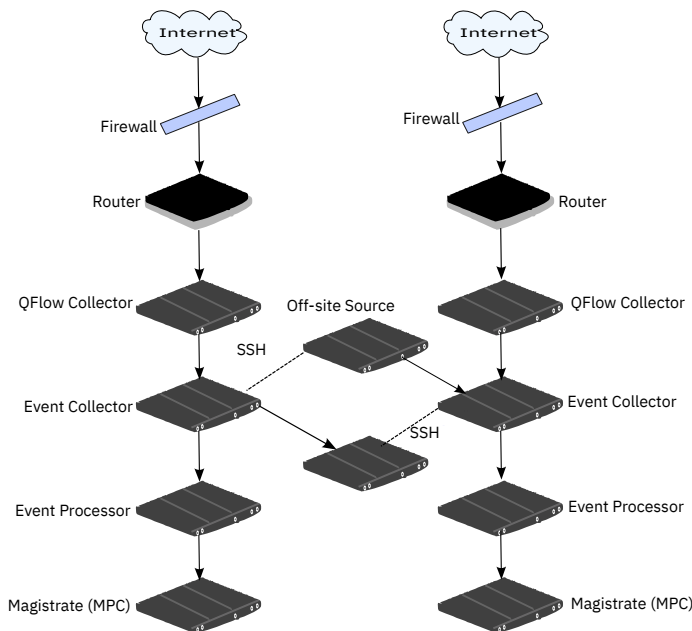


Figure 3. Forwarding data between deployments by using SSH

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, see [“Generating public keys for QRadar products” on page 56](#).

Procedure

To forward normalized events and flows from Deployment A to Deployment B:

1. Configure an off-site target in Deployment A.

The off-site target configuration includes the IP address of the Event Collector in Deployment B that receives the data.

2. Configure an off-site source in Deployment B.

The off-site source configuration includes the IP address and the port number of the Event Collector in Deployment A that is sending the data.

3. To transfer encrypted data, you must enable encryption on both the off-site source and the off-site target.

To ensure appropriate access, the SSH public key for the source system (Deployment A) must be available to the target system (Deployment B). For example, to enable encryption between Deployment A and Deployment B, follow these steps:

4. Create ssh keys by using the **ssh-keygen -l -t rsa** command, and press enter when prompted about the directory and passphrase.

By default, the `id_rsa.pub` file is stored in the `/root/.ssh` directory.

5. Copy the `id_rsa.pub` file to the `/root/.ssh` directory on the Event Collector and on the QRadar Console in the source system (Deployment A).
6. Rename the file to `authorized_keys`.

Ensure that the source system is configured with the appropriate permissions to send event and flow data to the target system.

7. If you didn't use the `chmod 600 authorized_keys` command to assign `rw` owner privileges to the file and the parent directory, use the `ssh-copy-id` command with the `-i` parameter to specify that the identity file `/root/.ssh/id_rsa.pub` be used.

For example, type the following command to append entries or create a new `authorized_keys` file on the target console with the right privileges. This command does not check for duplicate entries.

```
ssh-copy-id -i root@10.100.133.80
```

8. Configure the source system to ensure that forwarding of events and flows is not interrupted by other configuration activities, such as adding a managed host to one of the consoles.

For example, if a managed host is added to a console that is forwarding events, then an `authorized_keys` file must exist in the `/root/.ssh` directory on the managed host. If not, adding a managed host fails. This file is required regardless of whether encryption is used between the managed host and the console.

9. On the QRadar Console in the source system (Deployment A), create a `ssh_keys_created` file under `/opt/qradar/conf`.
10. Change the owner and group to **nobody** and the permission to **775** to make sure that the file can be backed up and restored properly.

```
chown nobody:nobody /opt/qradar/conf/ssh_keys_created
chmod 775 /opt/qradar/conf/ssh_keys_created
```

11. To prevent connection errors, deploy the changes in the target system (Deployment B) before you deploy the changes in the source system (Deployment A).

What to do next

If you update the Event Collector configuration or the monitoring ports, you must manually update the configuration for the off-site source and off-site target to maintain the connection between the two deployments.

If you want to disconnect the source system (Deployment A), you must remove the connections from both deployments. Remove the off-site target from the source system (Deployment A), and then remove the off-site source from the target system (Deployment B).

Managed hosts

For greater flexibility over data collection and event and flow processing, build a distributed IBM Security QRadar deployment by adding non-console managed hosts, such as collectors, processors, and data nodes.

For more information about planning and building your QRadar environment, see the *IBM Security QRadar Architecture and Deployment Guide*.

Software compatibility requirements

Software versions for all IBM Security QRadar appliances in the deployment must be at the same version and fix pack level. Deployments that use different versions of software are not supported because mixed software environments can cause rules not to fire, offenses not to be created or updated, and errors in search results.

When a managed host uses a software version that is different than the QRadar console, you might be able to view components that were already assigned to the host, but you cannot configure the component or add or assign new components.

Internet Protocol (IP) requirements

Various combinations of IP protocols are supported when adding non-console managed hosts, as described in the following table:

Table 13. Supported combinations of IP protocols when adding non-console managed hosts				
Managed hosts	QRadar Console (IPv6, single)	QRadar Console (IPv6, HA)	QRadar Console (dual stack, single)	QRadar Console (dual stack, HA)
IPv4, single	x	x	✓	x
IPv4, HA	x	x	x	x
IPv6, single	✓	✓	✓	x
IPv6, HA	✓	✓	✓	x

Restriction: By default, you cannot add an IPv4-only managed host to an IPv6 and IPv4 dual-stack console. You must run a script to enable an IPv4-only managed host. For more information, see [Adding an IPv4-only managed host in a dual-stack environment](#).

Bandwidth considerations for managed hosts

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the IBM Security QRadar console and all managed hosts. Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS).

An Event Collector that is configured to store and forward data to an Event Processor forwards the data according to the schedule that you set. Ensure that you have sufficient bandwidth to cover the amount of data that is collected, otherwise the forwarding appliance cannot maintain the scheduled pace.

Use the following methods to mitigate bandwidth limitations between data centers:

Process and send data to hosts at the primary data center

Design your deployment to process and send data as it's collected to hosts at the primary data center where the console resides. In this design, all user-based searches query the data from the local data center rather than waiting for remote sites to send back data.

You can deploy a store and forward event collector, such as a QRadar 15XX physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

Don't run data-intensive searches over limited bandwidth connections

Ensure that users don't run data-intensive searches over links that have limited bandwidth. Specifying precise filters on the search limits the amount of data that is retrieved from the remote locations, and reduces the bandwidth that is required to send the query result back.

Encryption

To provide secure data transfer between each of the appliances in your environment, IBM Security QRadar has integrated encryption support that uses OpenSSH. Encryption occurs between managed hosts; therefore, you must have at least one managed host before you can enable encryption.

When encryption is enabled, a secure tunnel is created on the client that initiates the connection, by using an SSH protocol connection. When you enable encryption on a managed host, an SSH tunnel is created for all client applications on the managed host. When you enable encryption on a non-Console managed host,

encryption tunnels are automatically created for databases and other support service connections to the Console.

For example, with encryption enabled on an Event Processor, the connection between the Event Processor and Event Collector is encrypted, and the connection between the Event Processor and Magistrate is encrypted.

Adding a managed host

Add managed hosts, such as event and flow collectors, event and flow processors, and data nodes, to distribute data collection and processing activities across your IBM Security QRadar deployment.

Before you begin

Ensure that the managed host has the same IBM Security QRadar version and fix pack level as the QRadar Console that you are using to manage it.

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see [“NAT-enabled networks ” on page 52.](#)

About this task

The following table describes the components that you can connect:

Table 14. Supported component connections		
Source connection	Target connection	Description
QRadar QFlow Collector	Event Collector	You can connect a IBM Security QRadar QFlow Collector only to an Event Collector. The number of connections is not restricted. You can't connect a QRadar QFlow Collector to the Event Collector on a 15xx appliance.
Event Collector	Event Processor	You can connect an Event Collector to only one Event Processor. You can connect a non-console Event Collector to an Event Processor on the same system. A console Event Collector can be connected only to a console Event Processor. You can't remove this connection.
Event Processor	Event Processor	You can't connect a console Event Processor to a non-console Event Processor. You can connect a non-console Event Processor to another console or non-console Event Processor, but not both at the same time. When a non-console managed host is added, the non-console Event Processor is connected to the console Event Processor.
Data Node	Event Processor	You can connect a data node to an event or flow processor only. You can connect multiple Data Nodes to the same processor to create a storage cluster.
Event Collector	Off-site target	The number of connections is not restricted.

Table 14. Supported component connections (continued)

Source connection	Target connection	Description
Off-site source	Event Collector	<p>The number of connections is not restricted.</p> <p>An Event Collector that is connected to an event-only appliance can't receive an off-site connection from system hardware that has the Receive Flows feature enabled.</p> <p>An Event Collector that is connected to a QFlow-only appliance can't receive an off-site connection from a remote system that has the Receive Flows feature enabled.</p>

If you configured IBM Security QRadar Incident Forensics in your deployment, you can add a QRadar Incident Forensics managed host. For more information, see the *IBM Security QRadar Incident Forensics Installation Guide*.

If you configured IBM Security QRadar Vulnerability Manager in your deployment, you can add vulnerability scanners and a vulnerability processor. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.

If you configured IBM Security QRadar Risk Manager in your deployment, you can add a managed host. For more information, see the *IBM Security QRadar Risk Manager Installation Guide*.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. On the **Deployment Actions** menu, click **Add Host**.
5. Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.
6. Click **Add**.
7. Optional: Use the **Deployment actions > View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.
8. On the **Admin** tab, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

Adding an IPv4-only managed host in a dual-stack environment

By default, in IBM Security QRadar products, you can't add an IPv4-only managed host to an IPv6 and IPv4 dual-stack console. You must run a script to enable an IPv4-only managed host.

About this task

You cannot add an IPv4-only managed host to a QRadar High Availability (HA) deployment.

Procedure

1. On a QRadar Console with IPv6 addressing, type the following command:
`/opt/qradar/bin/setup_v6v4_console.sh`
2. To add an IPv4 managed host, type the following command:

```
/opt/qradar/bin/add_v6v4_host.sh
```

3. Add the IPv4-only managed host.

Related tasks

[Adding a managed host](#)

Configuring a managed host

Configure a managed host to specify which role the managed host fulfills in your deployment. For example, you can configure the managed host as a collector, processor, or a data node. You can also change the encryption settings, and assign the host to a network address translation (NAT) group.



To make network configuration changes, such as an IP address change to your QRadar Console and managed host systems after you install your QRadar deployment, use the `qchange_netsetup` utility. For more information about network settings, see the *Installation Guide* for your product.

Before you begin

Ensure that the managed host has the same IBM Security QRadar version and fix pack level as the QRadar Console that is used to manage it. You can't edit or remove a managed host that uses a different version of QRadar.

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see [“NAT-enabled networks”](#) on page 52.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the host in the host table, and on the **Deployment Actions** menu, click **Edit Host**.
 - a) To create an SSH encryption tunnel on port 22 for the managed host, select the **Encrypt Host Connections** check box.
 - b) To configure the managed host to use a NAT-enabled network, select the **Network Address Translation** check box, and then configure the **NAT Group** and **Public IP address**.
 - c) To configure the components on the managed host, click the **Component Management** settings icon () and configure the options.
 - d) Click **Save**.
5. On the **Admin** tab, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.


Removing a managed host

You can remove non-Console managed hosts from your deployment. You can't remove a managed host that hosts the IBM Security QRadar Console.

Before you begin

Ensure that the managed host has the same IBM Security QRadar version and fix pack level as the QRadar Console that is used to manage it. You can't remove a host that is running a different version of QRadar.

Procedure

1. On the navigation menu () , click **Admin**.

2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. On the **Deployment Actions** menu, click **Remove host** and click **OK**.

You can't remove a QRadar Console host.

5. On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

Configuring your local firewall

Use the local firewall to manage access to the IBM Security QRadar managed host from specific devices that are outside the network. When the firewall list is empty, access to the managed host is disabled, except through the ports that are opened by default.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the host for which you want to configure firewall access settings.
5. From the **Actions** menu, click **View and Manage System**.
6. Click the **Firewall** tab and type the information for the device that needs to connect to the host.
 - a) Configure access for devices that are outside of your deployment and need to connect to this host.
 - b) Add this access rule.
7. Click **Save**.

If you change the **External Flow Source Monitoring Port** parameter in the QFlow configuration, you must also update your firewall access configuration.

Configuring email

Configure an email server to distribute alerts, reports, notifications, and event messages in IBM Security QRadar.

About this task

When you're setting up QRadar, it looks for a mail relay server to use to send out email messages.

If you configure the mail server setting as `localhost`, then the mail messages don't leave the QRadar box. You can only configure one email server for QRadar.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the host for which you want to configure email settings.
5. From the **Actions** menu, click **View and Manage System**.
6. Click the **Email Server** tab and type the host name or IP address of the email server that you want to use.

If you want to use the email server that QRadar provides, type `localhost` to use local email processing.

7. Click **Save**.

Making changes in your QRadar environment

When you make configuration changes to IBM Security QRadar, the changes are saved to a staging area, and the deployment banner on the **Admin** tab is updated indicating that changes need to be deployed. Deploying the changes might require QRadar services to restart.

QRadar has two methods of deploying changes: standard and full configuration. The type of deployment that is required depends on the type of changes that were made.

Standard deployment

This deployment method restarts only those services that are directly affected by the changes that were made. You begin a standard deployment by clicking **Deploy changes** on the banner on the **Admin** tab.

The following list shows examples of changes that require a standard deployment:

- Adding or editing a new user or user role.
- Setting a password for another user.
- Changing a users' role or security profile.

Full configuration deployment

Changes that affect the entire QRadar deployment must be deployed by using the full configuration deployment method. You begin a full configuration deployment by clicking **Deploy full configuration** from the **Advanced** menu on the **Admin** tab.

This method rebuilds all configuration files on each of the managed hosts. To ensure that the new configuration is loaded properly, all services on the managed hosts are automatically restarted, except for the event collection service. While the other services restart, QRadar continues collecting events and stores them in a buffer until the managed hosts come back online.

The following list shows examples of changes that require a full configuration deployment:

- Adding a managed host.
- Changing the configuration for a managed host.
- Configuring offsite hosts for sending or receiving data from the QRadar Console.
- Restoring a configuration backup.

Changes that impact event collection

Events come into QRadar through the `ecs-ec-ingress` event collection service. Starting in QRadar V7.3.1, the service is managed separately from other QRadar services. To minimize interruptions in collecting event data, the service does not automatically restart when the `hostcontext` service restarts.

The following situations can cause an interruption in event collection:

- Rebooting an appliance that collects events.
- Adding an HA managed host.
- During HA failover.
- Restoring a configuration backup.
- Adding or removing an off-site source connection
- Whenever a partition's disk usage exceeds the maximum threshold.

When you deploy changes after you restore a configuration backup, you can restart the event collection service now or later. When you choose to restart the service later, QRadar deploys all changes that don't depend on the event collection service, and continues to collect events while the other services restart. The deployment banner continues to show undeployed changes, and the `Event collection service must be restarted` message is shown when you view the details.

Deploying changes

Changes that are made to the IBM Security QRadar deployment must be pushed from the staging area to the production area.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Check the deployment banner to determine whether changes must be deployed.
3. Click **View Details** to view information about the undeployed configuration changes.
4. Choose the deployment method:
 - a) To deploy changes and restart only the affected services, click **Deploy Changes** on the deployment banner.
 - b) To rebuild the configuration files and restart all services on each managed host, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

Restarting the event collection service

There might be situations when you want to restart only the event collection service across all managed hosts in your IBM Security QRadar environment. For example, when a new version of the **ecs-ec-ingress** service is available for upgrade, or when you deferred restarting the service during an earlier deployment.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. On the **Advanced** menu, click **Restart Event Collection Services**.

Note: Event collection is briefly interrupted while the service restarts.

Shutting down a system

When you shut down a system, the appliance is powered off. The IBM Security QRadar interface is unavailable and data collection stops while the system is shut down.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the system that you want to shut down.
5. From the **Actions** menu, select **Shutdown System**.

Restarting a system

When you restart a system, the IBM Security QRadar interface is unavailable and data collection stops while the system restarts.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.

3. In the **Display** list, select **Systems**.
4. Select the system that you want to restart.
5. From the **Actions** menu, select **Restart System**.

Collecting log files

IBM Security QRadar log files contain detailed information about your deployment, such as host names, IP addresses, and email addresses. If you need help with troubleshooting, you can collect the log files and send them to IBM Support.

About this task

You can collect the log files for one or more host systems at the same time. Depending on the size of your deployment and the number of managed hosts, this might take awhile. The QRadar console log files are automatically included in each log file collection.

You can continue to use the QRadar console while the log file collection is running. If the system is actively collecting log files, you can't begin a new collection request. Cancel the active collection process and start another collection.

When the log file collection process completes, a system notification appears on the **System Monitoring** dashboard.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the hosts in the host table.
5. Click **Actions > Collect Log Files**.
6. Click **Advanced Options** and choose the options for the log file collection.

Encrypted log file collections can be decrypted only by IBM Support. If you want access to the log file collection, don't encrypt the file.

7. Click **Collect Log Files**.

Under **System Support Activities Messages**, a message indicates the status of the collection process.

8. To download the log file collection, wait for the **Log file collection completed successfully** notification, and click **Click here to download files**.

Changing the root password on your QRadar Console

As a good security practice, change the root password on your QRadar Console at regular intervals.

Procedure

1. Use SSH to log in to your QRadar Console as the root user.
2. Type the user name and password for the root user.
The user name and password are case-sensitive.
3. Use the **passwd** command to change your password.

Resetting SIM

After you tune your deployment, avoid receiving any additional false positive information by resetting SIM to remove all offense, and source and destination IP addresses from the database and the disk.

About this task

The SIM reset process can take several minutes, depending on the amount of data in your system. If you attempt to move to other areas of the IBM Security QRadar user interface during the SIM reset process, an error message is displayed.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. From the **Advanced** menu, select **Clean SIM Model**.
3. Read the information on the **Reset SIM Data Model** window.
4. Select one of the following options.

Option	Description
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 from the database, including protected offenses, source IP addresses, and destination IP addresses.

5. If you want to continue, select the **Are you sure you want to reset the data model?** check box.
6. Click **Proceed**.
7. When the SIM reset process is complete, click **Close**.
8. Refresh your web browser.

Chapter 6. Set up QRadar

Use the settings on the Admin tab to configure your IBM Security QRadar deployment, including your network hierarchy, automatic updates, system settings, event retention buckets, system notifications, console settings, and index management.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

Network hierarchy

IBM Security QRadar uses the network hierarchy objects and groups to view network activity and monitor groups or services in your network.

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

Related concepts

[Network hierarchy updates in a multitenant deployment](#)

Guidelines for defining your network hierarchy

Building a network hierarchy in IBM Security QRadar is an essential first step in configuring your deployment. Without a well configured network hierarchy, QRadar cannot determine flow directions, build a reliable asset database, or benefit from useful building blocks in rules.

Consider the following guidelines when you define your network hierarchy:

- Organize your systems and networks by role or similar traffic patterns.

For example, you might organize your network to include groups for mail servers, departmental users, labs, or development teams. Using this organization, you can differentiate network behavior and enforce behaviour-based network management security policies. However, 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, and makes it easier to create specific security policies for the server.

- Place servers with high volumes of traffic, such as mail servers, at the top of the group. This hierarchy provides you with a visual representation when a discrepancy occurs.
- Do not configure a network group with more than 15 objects.

Large network groups can cause difficulty when you view detailed information for each object. If your deployment processes more than 600,000 flows, consider creating multiple top-level groups.

- Conserve disk space by combining multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network group.

For example, add key servers as individual objects, and group other major but related servers into multi-CIDR objects.

Table 15. Example of multiple CIDRs and subnets in a single network group		
Group	Description	IP addresses
1	Marketing	10.10.5.0/24
2	Sales	10.10.8.0/21

Table 15. Example of multiple CIDRs and subnets in a single network group (continued)

Group	Description	IP addresses
3	Database Cluster	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

- Define an all-encompassing group so that when you define new networks, the appropriate policies and behavior monitors are applied.

In the following example, if you add an HR department network, such as 10.10.50.0/24, to the Cleveland group, the traffic displays as Cleveland-based and any rules you apply to the Cleveland group are applied by default.

Table 16. Example of an all-encompassing group

Group	Subgroup	IP address
Cleveland	Cleveland miscellaneous	10.10.0.0/16
Cleveland	Cleveland Sales	10.10.8.0/21
Cleveland	Cleveland Marketing	10.10.1.0/24

- In a domain-enabled environment, ensure that each IP address is assigned to the appropriate domain.

Acceptable CIDR values

IBM Security QRadar accepts specific CIDR values.

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

Table 17. 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
/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

Table 17. Acceptable CIDR values (continued)			
CIDR Length	Mask	Number of Networks	Hosts
/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

Related tasks

Defining your network hierarchy

A default network hierarchy that contains pre-defined network groups is included in IBM QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Defining your network hierarchy

A default network hierarchy that contains pre-defined network groups is included in IBM QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

About this task

Network objects are containers for Classless Inter-Domain Routing (CIDR) addresses. Any IP address that is defined in a CIDR range in the network hierarchy is considered to be a local address. Any IP address that is not defined in a CIDR range in the network hierarchy is considered to be a remote address. A CIDR can belong only to one network object, but subsets of a CIDR range can belong to another network object. Network traffic matches the most exact CIDR. A network object can have multiple CIDR ranges assigned to it.

Some of the default building blocks and rules in QRadar use the default network hierarchy objects. Before you change a default network hierarchy object, search the rules and building blocks to understand how the object is used and which rules and building blocks might need adjustments after you modify the object. It is important to keep the network hierarchy, rules, and building blocks up-to-date to prevent false offenses.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Network Hierarchy**.
3. From the menu tree on the **Network Views** window, select the area of the network in which you want to work.
4. To add network objects, click **Add** and complete the following fields:

Option	Description
Name	The unique name of the network object. Tip: You can use periods in network object names to define network object hierarchies. For example, if you enter the object name D.E.F, you create a three-tier hierarchy with E as a subnode of D, and F as a subnode of E.
Group	The network group in which to add the network object. Select from the Group list, or click Add a New Group . Tip: When you add a network group, you can use periods in network group names to define network group hierarchies. For example, if you enter the group name

Option	Description
	A . B . C, you create a three-tier hierarchy with B as a subnode of A, and C as a subnode of B.
IP/CIDR(s)	Type an IP address or CIDR range for the network object, and click Add . You can add multiple IP addresses and CIDR ranges.
Description	A description of the network object. This field is optional.
Country/Region	The country or region in which the network object is located. This field is optional.
Longitude and Latitude	The geographic location (longitude and latitude) of the network object. These fields are co-dependent and optional.

5. Click **Create**.

6. Repeat the steps to add more network objects, or click **Edit** or **Delete** to work with existing network objects.

Related concepts

[Acceptable CIDR values](#)

IBM Security QRadar accepts specific CIDR values.

Automatic updates

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

Updated configuration files help to eliminate false positives and to protect your system from the latest malicious sites, botnets, and other suspicious Internet activity.

Automatic update requirements

The IBM Security QRadar 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.

Update files are available for manual download from the [IBM Fix Central](http://www.ibm.com/support/fixcentral) (<http://www.ibm.com/support/fixcentral>).

To maintain the integrity of your current configuration and information, either replace your existing configuration files or integrate the updated files with your existing files.

After you install updates on your Console and deploy your changes, the Console updates its managed hosts.

Description of updates

Update files can include the following updates:

- Configuration updates that are based on content, including configuration file changes, vulnerabilities, QID maps, supportability scripts, and security threat information updates.
- DSM, scanner, and protocol updates that include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, such as updated JAR files or large patches, that require restarting the user interface service.
- Minor updates, such as daily automatic update logs or QID map scripts, that do not restart the user interface service.

Automatic updates for high availability deployments

When you update your configuration files on a primary host and deploy your changes, the updates are automatically made on the secondary host. If you do not deploy your changes, the updates are made on the secondary host through an automated process that runs hourly.

Frequency of automatic updates for new installations and upgrades

The default frequency of the automatic update is determined by the installation type and the QRadar version.

- If you upgrade from QRadar versions earlier than V7.2, the value to which the update frequency is set remains the same after the upgrade. By default, the update is set to weekly, but you can manually change the frequency.
- If you install a new installation of QRadar V7.2 or later, the default frequency of the update is daily. You can manually change the frequency.

Related concepts

Manual updates

If your deployment includes a IBM Security QRadar Console that is unable to access the Internet, or you want to manually manage updates to your system, you can manage the update process manually by setting up a IBM Security QRadar update server.

Viewing pending updates

Your system is preconfigured for weekly automatic updates. You can view the pending updates in the **Updates** window.

About this task

Your system needs to be operational long enough to retrieve the weekly 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](#).

The **Check for Updates** toolbar provides the following functions:

Table 18. Check for Updates 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” on page 78 .
Install	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” on page 77 .
Schedule	You can configure a specific date and time to manually install selected updates on your Console. Scheduling is useful when you want to schedule the update installation during off-peak hours. For more information, see “Scheduling an update” on page 77 .

Table 18. **Check for Updates** toolbar functions (continued)

Function	Description
Unschedule	You can remove preconfigured schedules for manually installing updates on your Console. For more information, see “Scheduling an update” on page 77.
Search By Name	You can 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	Pauses the automatic refresh process. To resume automatic refresh, click Play .
Refresh	Refreshes the list of updates.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. To view details on an update, select the update.

Configuring automatic update settings

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

About this task

You can select the **Auto Deploy** to automatically deploy updates. If **Auto Deploy** is not selected, then you must manually deploy changes, from the **Dashboard** tab, after updates are installed.

Restriction: In high-availability (HA) environment, automatic updates aren't installed when a secondary host is active. The updates are installed only after the primary host become the active node.

You can select **Auto Restart Service** to allow automatic updates that require the user interface to restart. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the updated from the **Check for Updates** window.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Change Settings**.
4. On the **Basic** tab, select the schedule for updates.
 - a) In the **Configuration Updates** section, select the method that you want to use for updating your configuration files.
 - To merge your existing configuration files with the server updates without affecting your custom signatures, custom entries, and remote network configurations, select **Auto Integrate**.
 - To override your customizations with server settings, select **Auto Update**.
 - b) In the **DSM, Scanner, Protocol Updates** section, select an option to install updates.
 - c) In the **Major Updates** section, select an option for receiving major updates for new releases.

- d) In the **Minor Updates** section, select an option for receiving patches for minor system issues.
 - e) If you want to deploy update changes automatically after updates are installed, select the **Auto Deploy** check box.
 - f) If you want to restart the user interface service automatically after updates are installed, select the **Auto Restart Service** check box.
5. Click the **Advanced** tab to configure the update server and backup settings.
- a) In **Web Server** field, type the web server from which you want to obtain the updates.
The default web server is `https://qmmunity.q1labs.com/`.
 - b) In the **Directory field**, type the directory location on which the web server stores the updates.
The default directory is `autoupdates/`.
 - c) Optional: Configure the settings for proxy server.
If the application server uses a proxy server to connect to the Internet, you must configure the proxy server. If you are using an authenticated proxy, you must provide the username and password for the proxy server.
 - d) Optional: In the **Proxy password** field, type the password for the proxy server.
Note: The password cannot contain the "#" or "?" characters.
 - e) In the **Backup Retention Period** list, type or select the number of days that you want to store files that are replaced during the update process.
The files are stored in the location that is specified in the **Backup Location**. The minimum is one day and the maximum is 65535 years.
 - f) In the **Backup Location** field, type the location where you want to store backup files.
 - g) In the **Download Path** field, 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`.
6. Click **Save**.

Configuring updates behind a proxy server that uses SSL or TLS interception

To configure IBM Security QRadar updates behind a proxy server, add your proxy server's CA certificate to the `ca-bundle.crt` file.

Procedure

1. Create a backup copy of the `ca-bundle.crt` file in QRadar.
For example, use the copy command to create a `.bak` file: `cp /etc/ssl/certs/ca-bundle.crt{,bak}`.
2. Get the root CA certificate from your proxy server. For more information, see the proxy server documentation.

Note: You must use only the root CA certificate from your proxy server.

3. Add the CA certificate to the `ca-bundle.crt` file by typing the following command:

```
cp proxycert.pem /etc/pki/ca-trust/source/anchors
```

4. Extract the certificate by typing the following command:

```
update-ca-trust extract
```

5. Type the following command to run the auto update:


```
/opt/qradar/bin/UpdateConfs.pl -ds runnow 1
```

6. Verify that auto updates work by tailing the log in `/var/log/autoupdates/`.

Scheduling an update

Automatic updates occur on a recurring schedule according to the settings on the **Update Configuration** page. To reduce performance impacts on your system, you can schedule a large update or a set of updates to run during off-peak hours.

Procedure


1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Optional: If you want to schedule specific updates, select the updates that you want to schedule.
4. From the **Schedule** list, select the type of update you want to schedule.
5. Using the calendar, select the start date and time of when you want to start your scheduled updates.

Clearing scheduled updates

Scheduled updates display a status of **Scheduled** in the **Status** field. You can cancel any scheduled update.

After the schedule is cleared, the status of the update displays as **New**.


Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Check for Updates**.
4. Optional: If you want to clear specific scheduled updates, select the updates that you want to clear.
5. From the **Unschedule** list, select the type of scheduled update that you want to clear.

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.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Check for Updates**.
4. Click **Get new updates**.


Manually installing automatic updates

IBM provides updates regularly. By default, updates are automatically downloaded and installed on your system. However, you can install an update at a time other than the preconfigured schedule.

About this task

The system retrieves the new updates from IBM [Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/). This might take an extended period. When complete, new updates are listed on the **Updates** window.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Check for Updates**.

4. Optional: If you want to install specific updates, select the updates that you want to schedule.
5. From the **Install** list, select the type of update you want to install.

Viewing your update history

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

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **View Update History**.
4. Optional: Using the **Search by Name** field, you can type a keyword and then press Enter to locate a specific update by name.
5. To investigate a specific update, select the update.

A description of the update and any installation error messages are displayed in the right pane of the **View Update History** page.

Restoring hidden updates

You can remove updates from the **Check for Updates** page. You can view and restore the hidden updates on the **Restore Hidden Updates** page.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Restore Hidden Updates**.
4. Optional: To locate an update by name, type a keyword in the **Search by Name** field and press Enter.
5. Select the hidden update that you want to restore.
6. Click **Restore**.

Viewing the autoupdate log

The autoupdate log contains the most recent automatic update that was run on your system.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. On the navigation menu, click **View Log**.

Manual updates

If your deployment includes a IBM Security QRadar Console that is unable to access the Internet, or you want to manually manage updates to your system, you can manage the update process manually by setting up a IBM Security QRadar update server.

The autoupdate package includes all files necessary to manually set up an update server in addition to the necessary system configuration files for each update. After the initial setup, you only need to download and uncompress the most current autoupdate package to manually update your configuration.

You can subscribe to notifications in [IBM Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/) to receive notification of new updates.

Related concepts

Automatic updates

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

Configuring an update server

Configure an Apache server as the update server for your IBM Security QRadar deployment.

Before you begin

Download the autoupdate package from [Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/). You can find QRadar products in the Security Systems **Product Group**.


Procedure

1. Access your Apache server and create an update directory named autoupdates/.

By default, the update directory is in the web root directory of the Apache server. You can place the directory in another location if you configure IBM Security QRadar accordingly.

2. Optional: Create an Apache user account and password to be used by the update process.
3. Save the autoupdate package file on your Apache server in the autoupdates/ directory that you created.
4. On the Apache server, type the following command to uncompress the autoupdate package.

```
tar -zxvf updatepackage-[timestamp].tgz
```

5. On the navigation menu () , click **Admin**.
6. In the **System Configuration** section, click **Auto Update**.
7. Click **Change Settings**, and click the **Advanced** tab.
8. In the **Server Config** pane, configure the settings for the Apache server.
 - a) In the **Web Server** field, type the address or directory path of your Apache server.

If the Apache server runs on non-standard ports, add the port number to the end of the address. For example, type `https://qmmunity.q1labs.com:8080/`.
 - b) In the **Directory** field, type the directory location where the web server stores the updates.

The default directory is `autoupdates/`.
 - c) Optional: If the application server uses a proxy server to connect to the internet, type the URL in the **Proxy Server** field.
 - d) Optional: If you are using an authenticated proxy, type the credentials in the **Proxy Username** and **Proxy Password** fields.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy changes**.
11. Using SSH, log in to QRadar as the root user.
12. Type the following command to configure the user name that you set for your Apache server:

```
/opt/qradar/bin/UpdateConfs.pl -change_username <username>
```

13. Type the following command to configure the password that you set for your Apache server:

```
/opt/qradar/bin/UpdateConfs.pl -change_password <password>
```

14. To test the update server, type the following command as a single line of text in the command line interface.

```
wget -q -O- --no-check-certificate  
https://<your update server>/<directory path to updates>/manifest_list
```

15. Type the user name and password.

Configuring the QRadar Console as the update server

To streamline your maintenance process, you can configure your QRadar Console to be your update server so that QRadar updates are automatically downloaded to the Console.

Procedure

1. Download the auto update package from Fix Central (www.ibm.com/support/fixcentral/).
You can find QRadar products in the Security Systems **Product Group** list on Fix Central.
2. Save the auto update package file in the `/tmp/` directory on your QRadar Console.

Note: The size of the auto update file is approximately 2 - 3 GB.

3. Log in to QRadar as the root user.
4. Type the following command to create the auto update directory:

```
mkdir -p /opt/qradar/www/autoupdates/
```

5. To verify that the Console has enough space for the auto update file, type the following command:

```
df -h /opt/qradar/
```

If you do not have enough space in the current directory, you can create another directory structure in the `/store` directory, such as `/store/downloads`.

6. Create a symbolic link to `/opt/qradar/www/autoupdates` by typing the following command:

```
ln -s /store/downloads /opt/qradar/www/autoupdates
```

7. To verify that the symbolic link was created properly, type the following command:


```
touch /store/downloads/testfile
```

8. Confirm that the test file value is created in the `/opt/qradar/www/autoupdates` directory by typing the following command:

```
ls /opt/qradar/www/autoupdates
```

9. Copy the `autoupdates-<version>.tgz` file from the `/tmp/` directory to the QRadar Console, and place it in the `/opt/qradar/www/autoupdates/` directory or the symbolic link directory that you created in Step 6.
10. On the QRadar Console, type the following commands to extract the auto update package:

```
cd /opt/qradar/www/autoupdates/  
tar -zxf /tmp/<name_of_autoupdate_file>
```

11. Log in to QRadar.
12. On the navigation menu () , click **Admin**.
13. In the **System Configuration** section, click **Auto Update**.
14. Click **Change Settings**, and select the **Advanced** tab.
15. In the **Directory** field, type `autoupdates/`.
16. In the **Web Server** field, type `https://localhost/`.
17. Click **Save**.

Download updates to the update server

You can download updates from Fix Central to your update server.

Before you begin

You must configure your update server and set up IBM Security QRadar to receive updates from the update server.

Procedure

1. Download the autoupdate package from [IBM Fix Central](http://www.ibm.com/support/fixcentral/) (<http://www.ibm.com/support/fixcentral/>).
You can find QRadar products in the Security Systems **Product Group** list on Fix Central.
2. Save the autoupdate package file on your update server in the autoupdates/ directory that you created.
3. Type the following command to uncompress the autoupdate package:

```
tar -xzf autoupdate-[timestamp].tgz
```

4. Log in to QRadar as the root user.
5. Type the following command to test your update server:


```
lynx https://<your update server>/<directory path to updates>/manifest_list
```

6. Type the user name and password of your update server.

Configuring system settings

System settings specify how your IBM Security QRadar system components are configured for normal operation.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Configure the system settings. Click the **Help** button to see setting descriptions.
4. Click **Save**.
5. On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

Customizing the right-click menu

To provide quick access to functions related to IP addresses, customize the Plugin options in the IP address right-click menu. For example, you can add more menu items, such as an option to lookup the IP address in a threat intelligence database.

About this task

The `ip_context_menu.xml` file controls the available options in the right-click menu and accepts `menuEntry` XML elements. To add more options, add a `menuEntry` element for each right-click option that you want to add. The syntax for the `menuEntry` element is:

```
<menuEntry name="{Name}" description="{Description}" url="{URL}"
requiredCapabilities="{Required Capabilities}"/>
<menuEntry name="{Name}" description="{Description}"
exec="{Command}" requiredCapabilities="{Required Capabilities}"/>
```

The following list describes the attributes in the `menuEntry` element:

Name

The text that is displayed in the right-click menu.

Description

The description of the entry. The description text is displayed in the tooltip for your menu option. The description is optional.

URL

Specifies the web address that opens in a new window.

You can use the placeholder %IP% to represent the IP address. The ampersand character (&), the left angle bracket (<), and the right angle bracket (>) must be escaped using the strings &, <, and >; respectively.

For example, to pass a URL with multiple parameters that includes a placeholder for the IP address, you can use this syntax: `url="/lookup?&ip=%IP%;force=true"`

Command

A command that you want to run on the IBMQRadar Console. The output of the command is displayed in a new window. Use the placeholder, %IP%, to represent the IP address that is selected.

Required Capabilities

Any capabilities, for example, "ADMIN", that the user must have before they select this option, comma-delimited. If the user does not have all capabilities that are listed, the entries are not displayed. Required capabilities is an optional field. For more information about required capabilities, see the *IBM Security QRadar Application Framework Developer Quick Start Guide*.

The edited file must look similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This is a configuration file to add custom actions into
the IP address right-click menu. Entries must be of one of the
following formats: -->
<contextMenu>
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

Important: Calling shell scripts or programs from the right-click menu or any other web interface can introduce security vulnerabilities such as OS command injection or path traversal attacks. Consider more secure methods, such as implementing a QRadar app extension.

Procedure

1. Using SSH, log in to the QRadar Console as the root user.
2. On the QRadar Console, if the `ip_context_menu.xml` file does not exist under the `/opt/qradar/conf` directory, copy the `ip_context_menu.xml` file from the `/opt/qradar/conf/templates` directory to the `/opt/qradar/conf` directory.
3. Open the `/opt/qradar/conf/ip_context_menu.xml` file for editing.
4. Edit the file to add, modify, or remove `menuEntry` XML elements.
5. Save and close the file.
6. To apply these changes, restart the QRadar GUI by typing the following command:
`systemctl restart tomcat`

Enhancing the right-click menu for event and flow columns

You can add more actions to the right-click options that are available on the columns in the **Log Activity** table or the **Network Activity** table. For example, you can add an option to view more information about the source IP or destination IP.

You can pass any data that is in the event or flow to the URL or script.

Procedure

1. Using SSH, log in to the QRadar Console appliance as the root user.

- Go to the `/opt/qradar/conf` directory and create a file that is named `arielRightClick.properties`.
- Edit the `/opt/qradar/conf/arielRightClick.properties` file. Use the following table to specify the parameters that determine the options for the right-click menu.

Table 19. Description of the <code>arielRightClick.properties</code> file parameters			
Parameter	Requirement	Description	Example
pluginActions	Required	Indicates either a URL or script action.	
arielProperty	Required	Specifies the column, or Ariel field name, for which the right-click menu is enabled.	sourceIP sourcePort destinationIP qid
text	Required	Specifies the text that is displayed on the right-click menu.	Google search
useFormattedValue	Optional	Specifies whether formatted values are passed to the script. Set to true to ensure that the formatted value for attributes, such as username and payload, are passed. Formatted values are easier for administrators to read than unformatted values.	If the parameter is set to true for the event name (QID) property, the event name of the QID is passed to the script. If the parameter is set to false, the raw, unformatted QID value is passed to the script.
url	Required to access a URL	Specifies the URL, which opens in a new window, and the parameters to pass to the URL. Use the format: <code>\$Ariel_Field Name\$</code>	<code>sourceIPwebUrlAction.url=http://www.mywebsite.com?q=\$sourceIP\$</code>
command	Required if the action is a command	Specifies the absolute path of the command or script file.	<code>destinationPortScriptAction.command=/bin/echo</code>
arguments	Required if the action is a command	Specifies the data to pass to the script. Use the following format: <code>\$Ariel_Field Name\$</code>	<code>destinationPortScriptAction.arguments=\$qid\$</code>

For each of the key names that are specified in the `pluginActions` list, define the action by using a key with the format *key name, property*.

- Save and close the file.
- Log in to the QRadar user interface.
- On the navigation menu (☰), click **Admin**.
- Click **Advanced > Restart Web Server**.

Example

The following example shows how to add *Test URL* as a right-click option for source IP addresses.

```
pluginActions=sourceIPwebUrlAction
sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

The following example shows how to enable script action for destination ports.

```
pluginActions=destinationPortScriptAction

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

The following example shows adding several parameters to a URL or a scripting action.

```
pluginActions=qidwebUrlAction,sourcePortScriptAction

qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Search on Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$-$CONTEXT$
```

Asset retention values overview

Additional information for the period, in days, that you want to store the asset profile information.

- Assets are tested against the retention thresholds at regular intervals. By default, the cleanup interval is 12 hours
- All specified retention periods are relative to the last seen date of the information, regardless of whether the information was last seen by a scanner or passively observed by the system.
- Asset information is deleted as it expires, meaning that following a cleanup interval, all asset information within its retention threshold remains.
- By default, assets that are associated with un-remediated vulnerabilities (as detected by IBM Security QRadar Vulnerability Manager or other scanner) are retained.
- Assets can always be deleted manually through the user interface.

Table 20. Asset components		
Asset component	Default retention (in days)	Notes
IP Address	120 days	By default, user-supplied IP Addresses are retained until they are deleted manually.
MAC Addresses (Interfaces)	120 days	By default, user-supplied interfaces are retained until they are deleted manually.
DNS and NetBIOS Hostnames	120 days	by default, user-supplied hostnames are retained until they are deleted manually.

Table 20. Asset components (continued)

Asset component	Default retention (in days)	Notes
Asset Properties	120 days	By default, user-supplied IP Addresses are retained until they are deleted manually. The asset properties this value can affect are Given Name, Unified Name, Weight, Description, Business Owner, Business Contact, Technical Owner, Technical Contact, Location, Detection Confidence, Wireless AP, Wireless SSID, Switch ID, Switch Port ID, CVSS Confidentiality Requirement, CVSS Integrity Requirement, CVSS Availability Requirement, CVSS Collateral Damage Potential, Technical User, User Supplied OS, OS Override Type, OS Override Id, Extended, Legacy (Pre-7.2) Cvss Risk, VLAN, and Asset Type.
Asset Products	120 days	By default, user-supplied products are retained until they are deleted manually. Asset products include Asset OS, Asset Installed Applications, and products that are associated with open asset ports
Asset "Open" Ports	120 days	
Asset netBIOS Groups	120 days	NetBIOS groups are seldom used, and more customers may not be aware of their existence. In the case where they are used, they are deleted after 120 days.
Asset Client Application	120 days	Client Applications are not yet leveraged in the user interface. This value can be ignored.
Asset Users	30 days	

Adding or editing a QRadar login message

Create a new login message or edit an existing login message on your IBM Security QRadar Console.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Click **Authentication Settings**.
4. To edit the login message, click **Edit** in the **Login Message** field.

- a) Type your message in the **Edit Login Message** window.
- b) To force users to consent to the login message before they can log in, select the check box.
- c) Click **Save**.

The login message is saved in the `opt/qradar/conf/LoginMessage.txt` file.

Note: You can also upload the `LoginMessage.txt` file to the `opt/qradar/conf/` directory.

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

6. To see your changes, log out of QRadar.

IF-MAP server certificates

The Interface For Metadata Access Points (IF-MAP) rule response enables the IBM Security QRadar console to publish alert and offense data that is derived from events, flows, and offenses to an IF-MAP server.

Before you can configure IF-MAP authentication on the **System Settings** window, you must configure your IF-MAP server certificate.

Configuring IF-MAP Server Certificate for Basic Authentication

This task provides instruction for how to configure your IF-MAP certificate for basic authentication.

Before you begin

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.

Procedure

1. Using SSH, log in to IBM Security QRadar as the root user.
2. 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 IBM Security QRadar console and on your IF-MAP server.

This task provides steps to configure the certificate on your QRadar console. For assistance configuring the certificate on your IF-MAP server, contact your IF-MAP server administrator.

Before you begin

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.

Procedure

1. Using SSH, log in to IBM Security QRadar as the root user.
2. Access the certificate to the `/opt/qradar/conf/trusted_certificates` directory
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.
4. Type the following command to create the Public-Key Cryptography Standards file with the `.pkcs12` file extension:

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

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
```

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.
7. Type the following command to change the permissions of the directory:

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

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

```
systemctl restart tomcat
```

Replacing SSL certificates in QRadar products

By default, IBM Security QRadar is configured with a self-signed Security Sockets Layer certificate. When you use a self-signed certificate to access the web, you're prompted with a warning message that the certificate is unrecognized. You can replace this SSL certificate with either an updated self-signed certificate, an internal certificate authority (CA) signed, or a public CA signed certificate.

SSL certificates overview

SSL is a security protocol that provides communication privacy so that client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

SSL is an industry standard that is used by websites to protect online transactions. To generate an SSL link, a web server requires an SSL certificate. SSL certificates are issued by internal or trusted third-party certifying authorities.

Trusted Root

Browsers and operating systems include a preinstalled list of trusted certificates, which are installed in the Trusted Root Certification authorities store.

Table 21. QRadar Supported Certificates	
Certificate	Description
Self-signed	A self-signed certificate provides basic security, enabling data encryption between the user and the application. Because self-signed certificates cannot be authenticated by any existing known root certificate authorities, users are warned about this unknown certificate and must accept it to proceed.
Internal CA signed	Organizations that have their own internal root CA can create a certificate by using that internal CA. This certificate is supported by QRadar, and the internal root CA is also imported into the QRadar environment.

Table 21. QRadar Supported Certificates (continued)

Certificate	Description
Public CA / Intermediate CA signed	<p>Certificates that are signed by known public CAs and intermediate certificates are supported by QRadar. Public signed certificates can be used directly in QRadar, and certificates that are signed with Intermediate CA are installed by using both the signed certificate and the intermediate certificate to provide valid certificate functions.</p> <p>Note: An intermediate certificate is commonly used by organizations that create multiple SSL keys in their environment, and want to have them signed by a known/commercial certificate vendor. When they use the intermediate key, they can then create sub-keys from this intermediate key. When this configuration is used, QRadar must be configured with both the intermediate certificate and the host SSL certificate so that connections to the host can verify the full certificate path.</p>

SSL connections between QRadar components

To establish all internal SSL connections between components, QRadar uses the web server certificate that is preinstalled on the QRadar Console. When the preinstalled certificate is replaced, the certificate installation process copies the certificate to all managed hosts in the deployment, except for QRadar Incident Forensics appliances.

All trusted certificates for QRadar must meet the following requirements:

- The certificate must be an X.509 certificate and have PEM base64 encoding.
- The certificate must have a .cert, .crt, .pem, or .der file extension.
- Keystore files that contain certificates must have the .truststore file extension.
- The certificate file must be stored in the /opt/qradar/conf/trusted_certificates directory.

Important: If you are an IBM Security QRadar Incident Forensics customer, contact [Customer Support](#) (www.ibm.com/support/) for assistance with installing or updating your custom SSL certificate in the QRadar Incident Forensics keystore.

If the SSL key is configured with a password, it must be manually entered each time that the service is restarted. With this configuration, the web UI service is unavailable until the password is entered, such as during a QRadar patch installation, HA failover, or system restart. In this instance, users can't log in and QRadar managed hosts can't retrieve configuration updates or report log source, rule and data storage status messages until the web service is available.

Replacing an SSL certificate is not supported by QRadar Packet Capture and QRadar Network Packet Capture.

Creating an SSL certificate signing request with 2048-bit RSA keys

1. Use SSH to log in to the QRadar Console.
2. Generate a private key file by using the following command:

```
openssl genrsa -out qradar.key 2048
```

Note: Do not use the private encryption options, because they can cause compatibility issues.

The qradar.key file is created in the current directory. Keep this file to use when you install the certificate.

3. Generate the certificate signing request (CSR) file. The `qradar.csr` file is used to create the SSL Certificate, with an internal CA or commercial certificate authorities. Run the following command, and provide necessary information as prompted:

```
openssl req -new -key qradar.key -out qradar.csr
```

Example output:

```
Provide the following information prompted in the command-line:
[root@qradar ~]# openssl genrsa -out qradar.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@bluecar ~]# openssl req -new -key qradar.key -out qradar.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:MyState
Locality Name (eg, city) [Default City]:MyCity
Organization Name (eg, company) [Default Company Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyCompanyOrg
Common Name (eg, your name or your server's hostname) []:qradar.mycompany.com
Email Address []:username@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@bluecar ~]#
```

4. If you want to verify the information in the CSR before you send it, you can type the following command:

```
openssl req -noout -text -in qradar.csr
```

If incorrect information was entered, run the OpenSSL command again to re-create the CSR file.

5. Use the Secure File Transfer Protocol or another program to securely copy the CSR file to your computer.
6. Submit the CSR to your internal or commercial certificate authority for signing according to their instructions.

Note: The CSR is identified as a certificate in Apache format.

Creating a multi-domain (SAN) SSL certificate signing request

1. Use SSH to log in to the QRadar Console.
2. Create and save a `sancert.conf` configuration file containing the following information:

```
[ req ]
default_bits          = 2048 # RSA key size
encrypt_key           = no   # Protect private key
default_md             = sha256 # MD to use
utf8                  = yes   # Input is UTF-8
string_mask            = utf8only # Emit UTF-8 strings
prompt               = no    # Prompt for DN
distinguished_name     = server_dn # DN template
req_extensions         = server_reqext # Desired extensions

[ server_dn ]
countryName            = <country_or_region_code> # ISO 3166
stateOrProvinceName    = <state_or_province>
localityName           = <city_or_locality>
organizationName       = <organization_name>
organizationalUnitName = <organizational_unit_name>
```

```

commonName          = <common_name> # Should match a SAN under alt_names

[ server_reqext ]
basicConstraints     = CA:FALSE
keyUsage             = critical,digitalSignature,keyEncipherment
extendedKeyUsage     = serverAuth
subjectKeyIdentifier = hash
subjectAltName       = @alt_names

[alt_names]
DNS.1                = qradar.example.com #Example
DNS.2                = console.example.com #Example
IP.3                 = 192.0.2.0 #Example

```

3. Generate a private key and public certificate signing request (CSR) pair by using the following command:

```

openssl req -new -nodes -sha256 -out <csr_filename>.csr -config sancert.conf
-keyout <privatekey_filename>.key

```

The key file is created in the current directory. Keep this file to use when you install the certificate.

The CSR file is used to create the SSL Certificate, with an internal CA or commercial certificate authorities.

4. If you want to verify the information in the CSR before you send it, you can type the following command:

```

openssl req -noout -text -in <csr_filename>.csr

```

If incorrect information was entered, update the `sancert.conf` configuration file and repeat the previous step.

5. Use the Secure File Transfer Protocol or another program to securely copy the CSR file to your computer.
6. Submit the CSR to your internal or commercial certificate authority for signing, according to their instructions.

Note: The CSR is identified as a certificate in Apache format.

Certificates signed by an internal certificate authority

If the certificate is issued by an internal certificate authority and not a commercial certificate provider, QRadar must be updated to include the internal root certificate into the local certificate store for proper certificate validation. Root verification certificates are automatically included with the operating system.

To update the trust anchors root certificate store in RedHat:

1. Copy the CA's root certificate to `/etc/pki/ca-trust/source/anchors/`.
2. Run the following command at the SSH command line:

```

update-ca-trust

```

Installing a new SSL Certificate on the QRadar Console

Before you begin

You must have the following:

- The newly signed certificate from either your internal CA, or a public one.
- The `qradar.key` private key to generate the CSR file.
- An intermediate certificate, if used by your certificate provider.

Note: If an intermediate certificate is used, run the `"install-ssl-cert.sh"` command with the `-i` flag to install both the new certificate and the intermediate certificate. When used, it prompts for 3 file paths:

- SSLCertificateFile
- SSLIntermediateCertificateFile
- SSLCertificateKeyFile

Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Install the certificate by entering the following command:


```
[root@qavm215 ~]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/new.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/new.certs/cert.key
```

Example output:

```
You have specified the following:

    SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? y
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
- Restarting httpd service ... (OK)
Restarting services:
- Stopping hostcontext ... (OK)
- Restarting Tomcat ... (OK)
- Starting hostcontext ... (OK)
Tue Sep 19 14:45:57 ADT 2017 [install-ssl-cert.sh] OK: Install SSL Cert Completed
[root@qavm215 ~]#
```

3. On the navigation menu () , click **Admin**.
4. Click **Advanced** > **Deploy Full Configuration**

Note: When you deploy the full configuration, QRadar restarts all services. Data collection for events and flows stops until the deployment completes.

Troubleshooting

If you have issues with your certificate, such as an incorrect name or IP address, or if the expiration date passes, or you have a change of IP or host name on your console, you can choose to revert to a self-signed certificate.

To generate a self-signed certificate, follow these steps on the QRadar Console:

1. Back up the certificates that were installed previously that are not working. Existing certificates are detected and reported when you run certificate generation, causing the generation process to stop.

```
mkdir /root/backup.certs/
mv /etc/httpd/conf/certs/cert.* /root/backup.certs/
```

2. Run the **/opt/qradar/bin/install-ssl-cert.sh --generate** command to generate new certificates. This process is also used during QRadar installation to generate the initial SSL certificate.

```
[root@qavm215 certs]# /opt/qradar/bin/install-ssl-cert.sh --generate
Generating self-signed SSL certificate ... (OK)
Installing generated SSL certificate ... (OK)
Tue Sep 19 14:00:42 ADT 2017 [install-ssl-cert.sh] OK:
Generated SSL certificate installed successfully
[root@qavm215 certs]#
```

3. Move the newly generated certificates to a new directory. Use the `install-ssl-certs.sh` script in Install mode to install and distribute the new SSL certificates.

```
[root@qavm215 ~]# mkdir /root/updated.certs/
[root@qavm215 ~]# mv /etc/httpd/conf/certs/cert.* /root/updated.certs/
[root@qavm215 ~]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/updated.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/updated.certs/cert.key

You have specified the following:

    SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? y
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
- Restarting httpd service ... (OK)
Restarting services:
- Stopping hostcontext ... (OK)
- Restarting Tomcat ... (OK)
- Starting hostcontext ... (OK)
Tue Sep 19 14:45:57 ADT 2017 [install-ssl-cert.sh] OK:
Install SSL Cert Completed
[root@qavm215 ~]#
```

Creating an SSL certificate signing request with SAN names

Generate SSL certificates with a Subject Alternative Name (SAN) when you want to browse through non-direct connections. SAN properties allow an SSL certificate to provide protection by authenticating a single host against multiple host names.

About this task

Creating SSL certificates with SAN properties are optional. and are not needed unless you want the certificate to secure multiple host names.

Procedure

1. Use SSH to log in to the QRadar Console.
2. Make a backup copy of the `/etc/pki/tls/openssl.cnf` file and edit it.

Note: Do not edit the original `openssl.cnf` file.

3. Add the following information under the respective section:

```
[ req ]
req_extensions = v3_req

[v3_req]
subjectAltName = @alt_names

[alt_names]
DNS.1           = qradar.example.com  #Example
DNS.2           = console.example.com #Example
IP.1            = 1.2.3.4             #Example
```

4. Type the following command to generate a private key file.

```
openssl genrsa -out qradar.key 2048
```

Note: Do not use the private encryption options because they can cause compatibility issues.

The `qradar.key` file is created in the current directory. Keep this file to use when you install the certificate.

5. Generate the certificate signing request (CSR) file.

The `qradar.csr` file is used to create the SSL certificate, with an internal CA or commercial certificate authorities.

- a) Type the following command, and provide the necessary information when prompted:

```
openssl req -new -key qradar.key -out qradar.csr -config /etc/pki/tls/openssl.cnf
```

Example output:

```
Provide the following information prompted in the command-line:
[root@qradar ~]# openssl genrsa -out qradar.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@bluecar ~]# openssl req -new -key qradar.key -out qradar.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:MyState
Locality Name (eg, city) [Default City]:MyCity
Organization Name (eg, company) [Default Company Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyCompanyOrg
Common Name (eg, your name or your server's hostname) []:qradar.mycompany.com
Email Address []:gdpreusername@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@bluecar ~]#
```

6. To verify the information in the CSR before you send it, type the following command:

```
openssl req -noout -text -in qradar.csr
```

If incorrect information was entered, run the `openssl` command again to re-create the CSR file.

7. Use the Secure File Transfer Protocol or another program to securely copy the CSR file to your computer.

If you chose to add SAN properties, they appear as follows:

```
X509v3 Subject Alternative Name:
      DNS:server1.example.com, DNS:mail.example.com, IP Address:1.2.3.4
```

8. Submit the CSR to your internal or commercial certificate authority for signing according to their instructions.

Note: The CSR is identified as a certificate in Apache format.

IPv6 addressing in QRadar deployments

IPv4 and IPv6 addressing is supported for network connectivity and management of IBM Security QRadar software and appliances. When you install QRadar, you are prompted to specify whether your Internet Protocol is IPv4 or IPv6.

QRadar components that support IPv6 addressing

The following QRadar components support IPv6 addressing.

Network Activity tab

Because **IPv6 Source Address** and **IPv6 Destination Address** are not default columns, they are not automatically displayed. To display these columns, you must select them when you configure your search parameters (column definition).

To save space and indexing in an IPv4 or IPv6 source environment, extra IP address fields are not stored or displayed. In a mixed IPv4 and IPv6 environment, a flow record contains both IPv4 and IPv6 addresses.

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow might not support IPv6.

Log Activity tab

Because **IPv6 Source Address** and **IPv6 Destination Address** are not default columns, they are not automatically displayed. To display these columns, you must select them when you configure your search parameters (column definition).

DSMs can parse IPv6 addresses from the event payload. If any DSM cannot parse IPv6 addresses, a log source extension can parse the addresses. For more information about log source extensions, see the *DSM Configuration Guide*.

Searching, grouping, and reporting on IPv6 fields

You can search events and flows by using IPv6 parameters in the search criteria.

You can also group and sort event and flow records that are based on IPv6 parameters.

You can create reports that are based on data from IPv6-based searches.

Custom rules

In custom rules and building blocks, IP parameters support IPv4 and IPv6 addresses unless the parameters are labeled as one or the other (for example, **SRC IPv6** supports only IPv6 addresses).

Device support modules (DSMs)

DSMs can parse IPv6 source and destination address from event payloads.

Deploying QRadar in IPv6 or mixed environments

To log in to QRadar in an IPv6 or mixed environment, wrap the IP address in square brackets. For example, `https://[<IP Address>]`

Both IPv4 and IPv6 environments can use a hosts file for address translation. In an IPv6 or mixed environment, the client resolves the Console address by its host name. You must add the IP address of the IPv6 console to the `/etc/hosts` file on the client.

Flow sources, such as NetFlow and sFlow, are accepted from IPv4 and IPv6 addresses. Event sources, such as syslog and SNMP, are accepted from IPv4 and IPv6 addresses. You can disable superflows and flow bundling in an IPv6 environment.

Restriction: By default, you cannot add an IPv4-only managed host to an IPv6 and IPv4 dual-stack console. You must run a script to enable an IPv4-only managed host. For more information, see [Adding an IPv4-only managed host in a dual-stack environment](#).

IPv6 addressing limitations

When QRadar is deployed in an IPv6 environment, the following limitations are known:

- Some parts of the QRadar deployment do not take advantage of the IPv6-enabled network hierarchy, including surveillance, searching, and analysis.
- No host profile test in custom rules for IPv6 addresses.

- No specialized indexing or optimization of IPv6 addresses.

Related tasks

Adding an IPv4-only managed host in a dual-stack environment

By default, in IBM Security QRadar products, you can't add an IPv4-only managed host to an IPv6 and IPv4 dual-stack console. You must run a script to enable an IPv4-only managed host.

Advanced iptables rules examples

You can configure your iptables rules to better control access to QRadar, restrict inbound data sources, and redirect traffic. The following examples can help you to gain better insight to your network, by manually adjusting your iptables.

Blocking iptables access to SSH

Consoles and unmanaged hosts allow SSH from any inbound request. When a host is added to the deployment, the consoles allow SSH access from the QRadar Console, and the console keeps port 22 open for inbound connections. You can limit the inbound connections on port 22 by modifying a host's iptables rules.

You can block SSH access from other managed hosts on your console, which can break encrypted connections.

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.41 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.59 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -j DROP
```

Enabling ICMP to QRadar systems

You can enable ping responses from your QRadar system by adding the following rule to the `/opt/qradar/conf/iptables.pre` file.

```
-A INPUT -p icmp -j ACCEPT
```

Run the following script to create an entry in the `/etc/sysconfig/iptables` file.

`/opt/qradar/conf/iptables_update.pl`

Important: You can limit this rule to a specific host by adding the `-s source.ip.address` field.

Blocking unwanted data sources

You can block out a data source such as a log source or a netflow data source, for a short time, rather than disabling the original device. To block a particular host, you can add an entry similar to the following to `/opt/qradar/conf/iptables.pre`.

Block a netflow from the router:

```
-A INPUT -p udp -s <IP Address> --dport 2055 -j REJECT
```

Block a syslog from another source:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Block a syslog from a specific subnet:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Redirecting iptables to syslog ports

You can redirect syslog traffic on non-standard ports into port 514 on a QRadar Event Collector. You can use the following steps to enable an iptables rule to redirect the alternative port back into 514 on the Event Collector.

1. Enable the NAT option in the Linux kernel by adding or updating the following line in the `/etc/sysctl.conf` file.

```
net.ipv4.ip_forward = 1
```

Note: For changes to take effect to the NAT rule, you might need to restart your service.

2. Enable ipforwarding in the current active kernel.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

3. Add the following lines to the `/opt/qradar/conf/iptables-nat.post`. Enter the port number that you want to redirect as the `<portnumber>`.

```
-A PREROUTING -p udp --dport <portnumber> -j REDIRECT --to-ports 514
-A PREROUTING -p tcp --dport <portnumber> -j REDIRECT --to-ports 514
```

4. Enter the following command to rebuild your iptables.

```
/opt/qradar/bin/iptables_update.pl
```

5. Verify the redirection by typing the following command.

```
iptables -nvL -t nat
```

The following code is an example of what the output might look like.

```
Chain PREROUTING (policy ACCEPT 140 packets, 8794 bytes) pkts bytes target
prot opt in out source destination 0 0 REDIRECT udp -- * * 0.0.0.0/0
0.0.0.0/0 udp dpt:10529 redir ports 514 0 0 REDIRECT tcp -- * * 0.0.0.0/0
0.0.0.0/0 tcp dpt:10529 redir ports 514 Chain POSTROUTING (policy ACCEPT 207
packets, 25772 bytes) pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 207 packets, 25772 bytes) pkts bytes target prot
opt in out source destination
```

Redirecting inbound syslog traffic

You can use your QRadar Console as a syslog message gateway to redirect inbound events, by configuring rules in iptables.

1. Enable the forwarding rule for a log source on your Event Collector.
2. Set the forwarding destination for the TCP syslog to be the console IP address on port 7780.
3. From the command line of the console, add the following iptables rule to redirect to another host.

```
iptables -I OUTPUT --src 0/0 --dst 153.2.200.80 -p
tcp --dport 7780 -j REDIRECT --to-ports 514
```

Configuring iptables rules

Access to the QRadar network services is controlled first on hosts with iptables. The iptables rules are adjusted and configured based on the requirements of the deployment. Ports for Ariel searching, streaming, and times when you are using encryption (tunneling) can update various iptables rules.

About this task

You can configure and check iptables rules for IPv4 and IPv6. The following procedure indicates how you can tune your iptables manually.

Procedure

1. Log in to QRadar as the root user by using SSH.

Login: <root>

Password: <password>

2. Type the following command to edit the pre rules iptables file:

IPv4:

```
vi /opt/qradar/conf/iptables.pre
```

IPv6:

```
vi /opt/qradar/conf/ip6tables.pre
```

The iptables.pre configuration file is displayed.

3. Type the following command to edit the post rules iptables file:

IPv4:

```
vi /opt/qradar/conf/iptables.post
```

IPv6:

```
vi /opt/qradar/conf/ip6tables.post
```

The iptables.post configuration file is displayed.

4. Add the following rule for QRadar to access a specific port number, where *portnumber* is the port number:

To accept UDP traffic for a specific port input:

```
-A INPUT -m udp -p udp --dport <portnumber> -j ACCEPT
```

To accept TCP traffic for a specific port input:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport <portnumber> -j ACCEPT
```

5. Save your iptables configuration.
6. Run the following script to propagate the changes:

```
/opt/qradar/bin/iptables_update.pl
```

7. Type the following commands to check for existing iptables:

IPv4:

```
iptables -L -n -v
```

IPv6:

```
ip6tables -L -n -v
```

Data retention

Retention buckets define how long event and flow data is retained in IBM Security QRadar.

As QRadar receives events and flows, each one is compared against the retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the deletion policy time period is reached. The default retention period is 30 days; then, the data is immediately deleted.

Retention buckets are sequenced in priority order from the top row to the bottom row. 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.

Tenant data

You can configure up to 10 retention buckets for shared data, and up to 10 retention buckets for each tenant.

When data comes into the system, the data is assessed to determine whether it is shared data or whether the data belongs to a tenant. Tenant-specific data is compared to the retention bucket filters that are defined for that tenant. When the data matches a retention bucket filter, the data is stored in that retention bucket until the retention policy time period is reached.

If you don't configure retention buckets for the tenant, the data is automatically placed in the default retention bucket for the tenant. The default retention period is 30 days, unless you configure a tenant-specific retention bucket.

For more information about tenant data retention, see [“Retention policies for tenants”](#) on page 215.

Configuring retention buckets

Configure retention policies to define how long IBM Security QRadar is required to keep event and flow data, and what to do when that data reaches a certain age.

About this task

Changes to the retention bucket filters are applied immediately to incoming data only. For example, if you configured a retention bucket to retain all data from source IP address 10.0.0.0/8 for 1 day, and you later edit the filter to retain data from source IP 192.168.0.1, the change is not retroactive. Immediately upon changing the filter, the retention bucket has 24 hours of 10.0.0.0/8 data, and all data that is collected after the filter change is 192.168.0.1 data.

The retention policy on the bucket is applied to all data in the bucket, regardless of the filters criteria. Using the previous example, if you changed the retention policy from 1 day to 7 days, both the 10.0.0.0/8 data and the 192.168.0.1 data in the bucket is retained for 7 days.

The **Distribution** of a retention bucket indicates the retention bucket usage as a percentage of total data retention in all your retention buckets. The distribution is calculated on a per-tenant basis.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant that you want the retention bucket to apply to.

Note: To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.

4. To configure a new retention bucket, follow these steps:
 - a) Double-click the first empty row in the table to open the **Retention Properties** window.
 - b) Configure the retention bucket parameters.

Learn more about retention bucket parameters:

Properties	Description
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	The retention period that specifies how long the data is to be kept. When the retention period is reached, data is deleted according to the Delete data in this bucket parameter. QRadar does not delete data within the retention period.

Properties	Description
Delete data in this bucket	<p>Select Immediately after the retention period has expired to delete data immediately on matching the Keep data placed in this bucket for parameter. The data is deleted at the next scheduled disk maintenance process, regardless of disk storage requirements.</p> <p>Select When storage space is required to keep data that matches the Keep data placed in this bucket for parameter in storage until the disk monitoring system detects that storage is required.</p> <p>Deletions that are based on storage space begin when the free disk space drops to 15% or less, and the deletions continue until the free disk space is 18% or the policy time frame that is set in the Keep data placed in this bucket for field runs out. For example, if the used disk space reaches 85% for records, data is deleted until the used percentage drops to 82%. When storage is required, only data that matches the Keep data placed in this bucket for field is deleted.</p> <p>If the bucket is set to Delete data in this bucket: immediately after the retention period has expired, no disk space checks are done and the deletion task immediately removes any data that is past the retention.</p>
Description	Type a description for the retention bucket.
Current Filters	Configure the filter criteria that each piece of data is to be compared against.

- c) Click **Add Filter** after you specify each set of filter criteria.
- d) Click **Save**.
- 5. To edit an existing retention bucket, select the row from the table and click **Edit**.
- 6. To delete a retention bucket, select the row from the table and click **Delete**.
- 7. Click **Save**.

Incoming data that matches the retention policy properties is immediately stored in the retention bucket.

Managing retention bucket sequence


You can change the order of the retention buckets to ensure that data is being matched against the retention buckets in the order that matches your requirements.

About this task

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

Procedure

- On the navigation menu () , click **Admin**.
- In the **Data sources** section, click **Event Retention** or **Flow Retention**.
- If you configured tenants, in the **Tenant** list, select the tenant for the retention buckets that you want to reorder.

Note: To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.
- Select the row that corresponds to the retention bucket that you want to move, and click **Up** or **Down** to move it to the correct location.

5. Click **Save**.


Enabling and disabling a retention bucket

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

About this task

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.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant for the retention bucket that you want to change.

Note: To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.

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


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.

About this task

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

Procedure



1. On the navigation menu () , click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant for the retention bucket that you want to delete.

Note: To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.

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

System notifications

IBM Security QRadar continuously monitors all appliances and delivers information, warning, and error notifications to the QRadar Console, making it easier for you to monitor the status and health of your deployment.

To show system notifications on your screen, you must configure your browser to allow pop-up windows and ensure that the **Enable Popup Notifications** check box is selected in your user preferences (). If you disable desktop notifications for QRadar, you can still view the system notifications under the notifications () menu.

Note: Browser notifications are supported for Mozilla Firefox, Google Chrome, and Microsoft Edge 10. Microsoft Internet Explorer does not support browser-based notifications. Notifications in Internet

Explorer appear in a QRadar notification box. The way that the notifications appear and how long the messages stay on the screen might vary between browsers.

Configuring system notifications

You can configure thresholds for system performance alerts.

About this task


The following table describes the Global System Notifications window parameters

Table 22. Global System Notifications window parameters	
Parameter	Description
System load over 1 minute	Type the threshold system load average over the last minute.
System load over 5 minutes	Type the threshold system load average over the last 5 minutes.
System load over 15 minutes	Type the threshold system load average over the last 15 minutes.
Average time in ms for I/O requests for device	Type the threshold time in ms for I/O requests
Percentage of swap used	Type the threshold percentage of used swap space.
Received packets per second	Type the threshold number of packets received per second.
Transmitted packets per second	Type the threshold number of packets transmitted per second.
Received bytes per second	Type the threshold number of bytes received per second.
Transmitted bytes per second	Type the threshold number of bytes transmitted per second.
Receive errors	Type the threshold number of corrupted packets received per second.
Transmit errors	Type the threshold number of corrupted packets transmitted per second.
Packet collisions	Type the threshold number of collisions that occur per second while transmitting packets.
Dropped receive packets	Type the threshold number of received packets that are dropped per second due to a lack of space in the buffers.
Dropped transmit packets	Type the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers.
Transmit carrier errors	Type the threshold number of carrier errors that occur per second while transmitting packets.
Receive frame errors	Type the threshold number of frame alignment errors that occur per second on received packets.
Receive fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets.

Table 22. Global System Notifications window parameters (continued)

Parameter	Description
Transmit fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **Global System Notifications**.
3. Enter values for each parameter that you want to configure.
4. For each parameter, select **Enabled** and **Response Criteria** and then select one of the following options:

Option	Description
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.

5. Type a description of the preferred resolution to the alert.
6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

Configuring custom email notifications

When you configure rules in IBM Security QRadar, specify that each time the rule generates a response, an email notification is sent to recipients. The email notification provides useful information, such as event or flow properties.

About this task

You can customize the content that is included in the email notification for rule response by editing the `alert-config.xml` file.

Note: References to flows do not apply to IBM QRadar Log Manager.

You must create a temporary directory where you can safely edit your copy of the files, without the risk of overwriting the default files. After you edit and save the `alert-config.xml` file, you must run a script that validates your changes. The validation script automatically applies your changes to a staging area, from where you can deploy by using the QRadar deployment editor.

Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Create a new temporary directory to use to safely edit copies of the default files.
3. To copy the files that are stored in the `custom_alerts` directory to the temporary directory, type the following command:

```
cp /store/configservices/staging/globalconfig/templates/
custom_alerts/*.xml <directory_name>
```

The `<directory_name>` option is the name of the temporary directory that you created.

4. Confirm that the files were copied successfully:
 - a) To list the files in the directory, type `ls -lah`.
 - b) Verify that the `alert-config.xml` file is listed.
5. Open the `alert-config.xml` file for editing.
6. Edit the contents of the `<template>` element.

- a) Required: Specify the type of template to use. Valid options are event or flow.

```
<templatetype>event</templatetype>
```

```
<templatetype>flow</templatetype>
```

- b) Type a name for the email template:

```
<templatename>Default flow template</templatename>
```

- c) Set the <active> element to true:

```
<active>true</active>
```

- d) Edit the parameters in the <body> or <subject> elements to include the information that you want to see.

Important: The <active></active> property must be set to `True` for each event and flow template type that you want to appear as an option in QRadar. You must also ensure that the <filename></filename> property is left empty.

Notification parameters that you can use in the template:

Table 23. Accepted Notification Parameters		
Common Parameters	Event Parameters	Flow Parameters
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Port
Credibility	SrcPostNATIPAddress	SourceBytes
Relevance	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocol		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex

Table 23. Accepted Notification Parameters (continued)

Common Parameters	Event Parameters	Flow Parameters
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomProperty		SourcePayload
CustomPropertiesList		
CalculatedProperty		
CalculatedPropertiesList		
AQLCustomProperty		
AqlCustomPropertiesList		

Note: If you do not want to retrieve the entire list when you use the CustomProperties, CalculatedProperties, or AqlCustomProperties parameter, you can select a specific property by using the following tags:

- Custom Property: `${body.CustomProperty("<custom_property_name>")}`
- Calculated Property: `${body.CalculatedProperty("<calculated_property_name>")}`
- AQL Custom Property: `${body.AqlCustomProperty("<AQL_custom_property_name>")}`

- To create multiple email templates, copy and paste the following sample email template in the `<template>` element in the `alert-config.xml` file. Repeat Step 6 for each template that you add.

Sample email template:

```
<template>
  <templatename>Default Flow</templatename>
  <templatetype>flow</templatetype>
  <active>true</active>
  <filename></filename>
  <subject>${RuleName} Fired </subject>
  <body>
    The ${AppName} event custom rule engine sent an automated response:

    ${StartTime}

    Rule Name:                ${RuleName}
    Rule Description:         ${RuleDescription}

    Source IP:                ${SourceIP}
    Source Port:              ${SourcePort}
    Source Username (from event): ${UserName}
    Source Network:           ${SourceNetwork}

    Destination IP:           ${DestinationIP}
    Destination Port:         ${DestinationPort}
    Destination Username (from Asset Identity): ${DestinationUserName}
    Destination Network:      ${DestinationNetwork}

    Protocol:                 ${Protocol}
    QID:                      ${Qid}
  </body>
</template>
```

```

Event Name:                ${EventName}
Event Description:          ${EventDescription}
Category:                  ${Category}

Log Source ID:             ${LogSourceId}
Log Source Name:           ${LogSourceName}

Payload:                   ${Payload}

CustomPropertiesList:       ${CustomPropertiesList}

AQL Custom Property, CEP_aql_1:  ${body.AqlCustomProperty("CEP_aql_1")}
Calculated Property, CEP_calc_2:  ${body.CalculatedProperty("CEP_calc_2")}
Regex Property, CEP_reg_3:       ${body.CustomProperty("CEP_reg_3")}

</body>
<from></from>
<to></to>
<cc></cc>
<bcc></bcc>
</template>


```

8. Save and close the alert-config.xml file.
9. Validate the changes by typing the following command.

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

The `<directory_name>` parameter is the name of the temporary directory that you created.

If the script validates the changes successfully, the following message is displayed: File alert-config.xml was deployed successfully to staging!

10. Deploy the changes in QRadar.
 - a) Log in to QRadar.
 - b) On the navigation menu () , click **Admin**.
 - c) Click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

Custom offense close reasons

You can manage the options listed in the **Reason for Closing** list box on the **Offenses** tab.

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.

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.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.

3. Click **Add**.
4. Type a unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
5. 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 that 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.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.
3. Select the offense close reason that you want to edit.
4. Click **Edit**.
5. Type a new unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
6. Click **OK**.

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.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.
3. Select the offense close reason that you want to delete.
4. Click **Delete**.
5. Click **OK**.

Configuring a custom asset property

Custom asset properties provide more query options when you run queries on the assets that you have in IBM Security QRadar.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Custom Asset Properties**.
3. In the **Name** field, enter a descriptor for the custom asset property.
4. In the **Type** list, select **Numeric** or **Text** to define the information type for the custom asset property.
5. Click **OK**.
6. Click the **Assets** tab.
7. Click **Edit Asset > Custom Asset Properties**.
8. Enter the required information in the value field.
9. Click **OK**.

Index management

Use Index Management to control database indexing on event and flow properties. To improve the speed of searches in IBM Security QRadar, narrow the overall data by adding an indexed field in your search query.

An *index* is a set of items that specify information about data in a file and its location in the file system. Data indexes are built in real-time as data is streamed or are built upon request after data is collected. Searching is more efficient because systems that use indexes don't have to read through every piece of data to locate matches. The index contains references to unique terms in the data and their locations. Because indexes use disk space, storage space might be used to decrease search time.

Use indexing event and flow properties first 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. When a search starts in QRadar, the search engine first filters the data set by indexed properties. The indexed filter eliminates portions of the data set and reduces the overall data volume and number of event or flow logs that must be searched. Without any filters, QRadar takes more time to return the results for large data sets.

For example, you might want to find all the logs in the past six months that match the text: The operation is not allowed. By default, QRadar stores full text indexing for the past 30 days. Therefore, to complete a search from the last 6 months, the system must reread every payload value from every event or flow in that time frame to find matches. Your results display faster when you search with an indexed value filter such as a **Log Source Type**, **Event Name**, or **Source IP**.

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

To enable payload indexing, you must enable indexing on the Quick Filter property.

Enabling indexes

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.

About this task

Modifying database indexing might decrease system performance. Ensure that you monitor the statistics after you enable indexing on multiple properties.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Index Management**.
3. Select one or more properties from the **Index Management** list.
4. Choose one of the following options:

Situation	Time frame	Action	Reason
The index is disabled and % of Searches Using Property is above 30% and % of Searches Missing Index is above 30%.	24 hours, 7 days, or 30 days	Click Enable Index .	This search property is used often. Enabling an index can improve performance.

Situation	Time frame	Action	Reason
The index is enabled and % of Searches Using Property is zero.	30 days	Click Disable Index .	The enabled index is not used in the searches. Disable the indexed property to preserve disk space.

5. Click **Save**.

6. Click **OK**.

Results

In lists that include event and 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.

Enabling payload indexing to optimize search times

You use the **Quick Filter** feature on the **Log Activity** and **Network Activity** tab to search event and flow payloads by using a text string. To optimize event and flow search times, enable payload indexing on the **Quick Filter** property.

Restriction: Payload indexing increases disk storage requirements and might affect system performance. Enable payload indexing if your deployment meets the following conditions:

- The event and flow processors are at less than 70% disk usage.
- The event and flow processors are less than 70% of the maximum events per second (EPS) or flows per interface (FPI) rating.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Index Management**.
3. In the **Quick Search** field, type **Quick Filter**.

The **Quick Filter** property is displayed.

4. Select the **Quick Filter** property that you want to index.

In the results table, use the value in the **Database** column to identify the events or flows **Quick Filter** property.

5. On the toolbar, click **Enable Index**. A green dot indicates that the payload index is enabled.

If a list includes event or flow properties that are indexed, the property names are appended with the following text: [Indexed].

6. Click **Save**.

What to do next

To manage payload indexes, see [“Configuring the retention period for payload indexes”](#) on page 108.

Configuring the retention period for payload indexes

By default, IBM Security QRadar sets 30 days for the data retention period of the payload index. You can search for specific values in quick filter indexes beyond 30 days by changing the default retention in QRadar.

Before you begin

Your virtual and physical appliances require a minimum of 24 GB of RAM to enable full payload indexing. However, 48 GB of RAM is suggested.


The minimum and suggested RAM values applies to all QRadar systems, such as 16xx, 17xx, or 18xx appliances, that are processing events or flows.

About this task

The retention values reflect the time spans that you are typically searching. The minimum retention period is 1 day and the maximum is 2 years.

Note: Quick Filter searches that use a time frame outside of the Payload Index Retention setting can trigger slow and resource-intensive system responses. For example, if the payload index retention is set for 1 day, and you use a time frame for the last 30 hours in the search.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. In the **Database Settings** section, select a retention time period from the **Payload Index Retention** list.
4. Click **Save**.
5. Close the **System Settings** window.
6. On the **Admin** tab, click **Deploy Changes**.

What to do next

If you retain payload indexes longer than the default value, extra disk space is used. After you select a greater value in the **Payload Index Retention** field, monitor system notifications to ensure that you do not fill disk space.

Set restrictions to prevent resource-intensive searches

You can balance the usage of your QRadar infrastructure by setting resource restrictions on IBM Security QRadar event and flow searches.

Before you set resource restrictions, carefully consider the normal operational procedures in your environment. Try to set restrictions that ensure that all users have access to the data that they require, yet prevent them from inadvertently running large queries that negatively impact the system availability and performance for other users.

Types of resource restrictions

You can set limitations on searches by configuring either time or data set restrictions based on user, role, or tenant.

Resource restrictions are applied in the following order: user, user role, and tenant. For example, restrictions that are set for a user take precedence over restrictions that are set for the user role or tenant that the user is assigned to.

You can set the following types of restrictions on event and flow searches:

- The length of time that a search runs before data is returned.
- The time span of the data to be searched.
- The number of records that are processed by the Ariel query server.

Note: Ariel search stops when the record limit is reached, but all in-progress search results are returned to the search manager and are not truncated. Therefore, the search result set is often larger than the specified record limit.

User-based restrictions

User-based restrictions define limits for an individual user, and they take precedence over role and tenant restrictions.

For example, your organization hires university students to work with the junior analysts in your SOC. The students have the same user role as the other junior analysts, but you apply more restrictive user-based restrictions until the students are properly trained in building QRadar queries.

Role-based restrictions

Role-based restrictions allow you to define groups of users who require different levels of access to your QRadar deployment. By setting role-based restrictions, you can balance the needs of different types of users.

For example, a junior security analyst might focus on security incidents that happened recently, while a senior security analyst might be more involved in forensic investigations that review data over a longer period of time. By setting role-based restrictions, you can limit a junior analyst to accessing only the last 7 days of data, while a senior analyst has access to a much larger time span of data.

Tenant-based restrictions

In a Managed Security Service Provider (MSSP) or a multi-divisional organization, tenant-based restrictions can help you ensure quality of service by preventing resource contention and degradation of services. You can prevent a tenant from querying terabytes of data that can negatively impact the system performance for all other tenants.

As an MSSP, you might define standard resource restrictions based on a set of criteria that each tenant is compared to. For example, the standard configuration for a medium-sized tenant might include resource restrictions that limit searches to accessing only the last 14 days of data and a maximum of 10,000 records returned.

Resource restrictions in distributed environments

In a distributed environment, the timing of the data transfer between the IBM Security QRadar console and managed hosts can impact the search results.

When you run a search in IBM Security QRadar, the search runs on all nodes at the same time. Each managed host runs the search, and sends the aggregated results to the QRadar console when the search is complete or when it reaches the predefined number of rows.

It is important to understand how the resource restrictions that you set might impact the search results that are returned to a user:

Canceled searches

Each managed host periodically checks the state of the resource restriction limit. If a limit is reached, the search is automatically canceled to prevent the incomplete results from being cached and reused.

Results that were collected before the search was canceled by the system can be viewed by clicking **Search > Manage Search Results** on the **Log Activity** or **Network Activity** tab.

Empty search results

When you set time-limit or record-limit restrictions, the remote aggregation might cause the QRadar console to reach the resource restriction limit before the managed host sends the partial aggregate to the console. In this situation, the search results might appear to be empty even though some data was collected.

Inconsistent search results

QRadar monitors the load on each managed host, and manages the search to ensure optimized performance throughout the entire deployment. Depending on the system load, searches that are run repeatedly might show slightly different results due to the managed hosts that return the data in a different order.

For example, in a deployment that has six event processors, EP1, EP3, and EP5 might be the first processors to return data on the initial run. In subsequent runs, EP2, EP4, and EP6 might return data first, which accounts for the inconsistent search results.

Limited search results

You can set a limit restriction on search results for QRadar that limits the number of records that are read from the disk in a search query. A limit ensures that the query stops after any managed host that is participating in the search reads the restricted number of entries from the disk. The query does not retrieve all the data and gives you only the restricted number of rows. Setting this restriction can prevent a system crash in the instance of a large amount of data.

For example, if you set the restriction at 10,000 rows, the query stops running after the managed host processes 10,000 records.

Depending on the frequency that users reach the resource restrictions, you can tune the limits to avoid restricting users from running reasonable searches to meet their job requirements. Users who consistently run searches that strain the system might benefit from more training in building QRadar queries. For more information, see the *IBM Security QRadar Ariel Query Language Guide*.


Configuring resource restrictions

Set resource restrictions to apply time or data limitations to event and flow searches.

About this task


You can set the following types of resource restrictions:

- **Execution time** restrictions specify the maximum amount of time that a query runs before data is returned.
- **Time span** restrictions specify the time span of the data to be searched.
- **Record limit** restrictions specify the number of data records that are returned by a search query.

Users who run searches that are limited by resource restrictions see the resource restriction icon () next to the search criteria.

Note: The search result set is often larger than the specified record limit. When the record limit is reached, the search manager signals all search participants to stop (there are multiple search participants even on a single system), but results continue to accumulate until the search fully stops on all participants. All search results are added to the result set.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Resource Restrictions**.
3. If your deployment has tenants that are configured, click **Role** or **Tenant** to specify the type of restrictions to set.
4. Double-click the role or tenant that you want to set restrictions for.
5. To set restrictions for all users who are assigned to the user role or tenant, follow these steps:
 - a) Click the summary row at the top to open the **Edit Restriction** dialog box.
 - b) Click **Enabled** for the type of restriction that you want to set, and specify the restriction values.
 - c) Click **Save**.
6. To set restrictions for a specific user, follow these steps:
 - a) Double-click the user that you want to set the restrictions for.
To search for a user, type the user name in the filter field.
 - b) Click **Enabled** for the type of restriction that you want to set, and specify the restriction values.

c) Click **Save**.

App Nodes

An App Node is an unmanaged host that is dedicated to running apps. Provision an App Node to provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. Apps such as User Behavior Analytics require more resources than are currently available on the Console.

You can use any server for an App Node that meets the requirements that are outlined in [“Prerequisites for setting up an App Node” on page 112](#). Place your App Node server and QRadar Console in the same data center for the best performance.

The node setup process installs and configures all of the necessary software. When you add the App Node, apps that are installed on the QRadar Console are transferred to the App Node.

Note: QRadar managed hosts cannot be used as App Nodes. You must use an external host for your App Node. You can use only one App Node in a QRadar deployment.

Related concepts

[Backup and restore applications](#)

IBM Security QRadar provides a way to backup and restore application configurations separate from the application data.

Prerequisites for setting up an App Node

To set up an App Node server that is separate from your QRadar Console, your server must adhere to the minimum system requirements, such as software, open ports, and operating system versions.

To set up a physical server or VM as an App Node, use the following requirements.

Note: You must not make configuration changes on the App Node changes that are not specified in this document, including the following changes.

- SSH configuration changes
- Firewall configuration changes
- Permission changes of any file, directory, or mount that contains QRadar executable scripts
- Configuring multiple NICs

These and other configuration changes cause the App Node installation to fail.

The following table shows the minimum specifications for an App Node.

Note: If you are using some larger apps, such as Pulse and User Behavior Analytics with Machine Learning, the minimum requirements might be insufficient.

Table 24. App Node minimum specifications	
Requirement	Description
Memory (RAM)	12 GB
Processors (CPU cores)	4
Storage	256 GB of free disk space Create a /store partition that uses approximately 80% of the available storage capacity.

The following table shows the operating system settings that are necessary for an App Node.

Table 25. App Node operating system settings	
Requirement	Description
Operating system	<p>The operating system must be Red Hat Enterprise Linux (RHEL) 7.3 or CentOS 7.3, unless you are using QRadar V7.3.1 p6 or later. If you are using QRadar V7.3.1 p6 or later, use RHEL 7.5 or Cent OS 7.5.</p> <p>The App Node requires access to repositories for dependencies, which are downloaded from external sources, so it's acceptable to install the minimal ISO for the operating system. This requirement contrasts with the managed host where all dependencies are included in the product installation media and software fixes.</p>
Operating system repositories	<p>Your App Node server must maintain access to the repositories specific to its operating system (RHEL or CentOS). Installations and updates fail without repository access. Use the yum command to install OS package dependencies. Verify yum access by running the following command:</p> <pre>yum repolist</pre> <p>Note: The protobuf package is not included in the default RHEL repositories. If you are installing your App Node on RHEL, you must enable the optional repositories to install the protobuf package, by typing the following command:</p> <pre>subscription-manager repos --enable=rhel-7-server-optional-rpms</pre> <p>To list the repositories that you're subscribed to, type the following command:</p> <pre>subscription-manager repos --list</pre>
Time zone synchronization	The App Node server must be configured with the same time and time zone as your Console.

The following table shows the network specifications for an App Node.

Table 26. App Node network specifications	
Requirement	Description
Network connection	The App Node must have an internet connection.
Ports to open on the QRadar Console and the App Node	<p>Ports 22, 1443 and 5443 must be open on any external firewalls from your Console to the App Node.</p> <p>Ports 22, 5443 and 5444 must be open on any external firewalls from your App Node back to the QRadar Console.</p>
Network Address Translation (NAT)	If you have an environment that uses Network Address Translation (NAT), both the Console and the App Node must exist within the same NAT Group.
IPv6 (Internet Protocol version 6)	IPv6 is a Docker requirement. If you're using IPv4 addressing, you can automatically assign IPv6 to interfaces to satisfy this requirement. An easy way to verify that IPv6 is running is to check for IPv6 addresses on your App Node interfaces.

Table 26. App Node network specifications (continued)	
Requirement	Description
Firewalld	<p>Ensure that Firewalld is running on the App Node so that the Console can connect to your apps on the App Node. To verify that Firewalld is running, type the following command:</p> <pre>systemctl status firewalld</pre>
Unencrypted tunnels between QRadar Console and the App Node	You can't configure encrypted tunnels between the App Node server and the Console.
TCP forwarding	<p>Verify that the AllowTcpForwarding parameter in the <code>/etc/ssh/sshd_config</code> file is configured as yes, which is the default setting.</p> <p>Either of the following entries in the <code>/etc/ssh/sshd_config</code> file are acceptable:</p> <pre>AllowTcpForwarding yes</pre> <pre>#AllowTcpForwarding yes</pre> <p>Note: The App Node installation fails when the AllowTcpForwarding parameter is configured as no.</p>
App Nodes and web proxy configuration	<p>When your App Node is configured to use a web proxy, you must add a <code>NO_PROXY</code> configuration to the <code>/etc/environment</code> file to prevent the localhost and services, such as consul.service.consul and vault.service.consul, from making calls to the web proxy.</p> <p>Add the following lines (continuous) to the <code>/etc/environment</code> file:</p> <pre>NO_PROXY="<app_node_IP_address>,localhost,127.0.0.1,zookeeper.service.consul,vault.service.consul,docker-registry.service.consul,marathon.service.consul,consul.service.consul,framework_app_proxy.service.consul,service-launcher.service.consul"</pre> <pre>no_proxy="<app_node_IP_address>,localhost,127.0.0.1,zookeeper.service.consul,vault.service.consul,docker-registry.service.consul,marathon.service.consul,consul.service.consul,framework_app_proxy.service.consul,service-launcher.service.consul"</pre>

Related tasks

[Adding an App Node](#)

To offset the processing capacity that is done by the QRadar Console for apps, add an App Node to your deployment. The App Node is an unmanaged host that is dedicated to running apps.

Setting up an App Node

Several steps are necessary to set up the App Node server and to transfer the apps from the Console to the App Node.

Procedure

1. Install Centos or RHEL on a host that meets the App Node requirements.

Notes:

- The operating system must be the minimal version of Red Hat Enterprise Linux (RHEL) 7.3 or CentOS 7.3, unless you are using QRadar V7.3.1 p6 or later. If you are using QRadar V7.3.1 p6 or later, use the minimal version of RHEL 7.5 or Cent OS 7.5.
 - Ensure that you allow 80% of disk space for the `/store` partition.
2. Configure a packages repository for yum installation. If you do not have network access on the App Node server, make the local DVD drive a packages repository for yum installations, and then create a directory for the mount point. For more information about setting up repositories, see the [RHEL documentation](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/) (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/).
Verify that your repository works by typing the **yum repolist** command.
 3. Verify that the date and time are synchronized between the App Node and the QRadar Console.
You can use the **timedatectl** command to reset the time or configure **NTP**.
 4. Log in to the QRadar Console and list your docker containers by typing the following command:

```
ls /store/docker/containers/
```

5. List your apps by typing the following command on the QRadar Console:

```
/opt/qradar/support/qapp_utils_730.py ps
```

These apps are transferred to the App Node when you run the App Node setup. Run the command on the Console again to verify that the apps are transferred.

6. Create an App Node user and password on the App Node and then configure password-less **sudo** access for this user.

Note: The home directory of the App Node user cannot have group writable permissions set to it, because this permission can cause SSH connections to be rejected.

- a) Create an App Node user by typing the following commands:

```
useradd <app_node_user>
```

```
passwd <app_node_user>
```

- b) Type `visudo` to edit the `/etc/sudoers` file, and add the following line at the end of the file:

```
<app_node_user> <tab> ALL=(ALL) <tab> NOPASSWD: ALL
```

- c) Save and close the file.
 - d) Test the user name and password and then test **sudo** access.
7. Verify that **AllowTcpForwarding** is configured as yes in the `/etc/ssh/sshd_config` file on the App Node.

What to do next

Follow the instructions for [“Adding an App Node”](#) on page 117.

App Node setup tips

During the setup you can use various commands to list and verify the status of Docker and your apps on both the QRadar Console and the App Node when the setup is finished.

The following list shows helpful commands that you can use to help you with the App Node setup and to verify the app status:

Verify that sudo works without a password on the App Node

To test **sudo** access, log in as `<app_node_user>` and type the following command:

```
sudo ls /root
```

Connect to the App Node from the QRadar Console

Use an SSH client to connect to the App Node from the QRadar Console.

```
ssh <app_node_user>@<app_node_IP_address>
```

The following prompt for the App Node is shown: [*<app_node_user>*@control-01 ~]\$ or [*root*@control-01 ~]\$ if you log in as the root user.

List your apps

Type the following command to list the installed apps:

```
/opt/qradar/support/qapp_utils_730.py ps
```

Here's an example of the output:

```
Collecting app data..... Complete!
Id   Name      Container      Container Image      Container ip:port  Host ip:port      ABCDEFGHI
1053 QRadar App Editor 5dca41d9e5e1 qregi...1053:2.0-release 192.0.2.0:5000 203.0.113.86:25568 ++++++++
1054 Hello World - 345555f3070 qregi.../qapp/1054:1.0.2 192.0.2.2:5000 203.0.113.86:7072 ++++++++
1055 QRadar Vuln app b79118c4cb0 qregi...44/qapp/1055:1.0 192.0.2.6:5000 203.0.113.86:25600 ++++++++
```

Note: When the apps are transferred to the App Node, the Host `ip:port` reference changes from the QRadar Console to the App Node.

Verify that Docker containers are created on the App Node

On the App Node, type the following command:

```
ls /store/docker/containers/
```

Here's an example of the output:

```
345555f30703c7641e042e1ddba9c3294174c2d4ed7a0108ef5d9282fcc1d49
364ee70aaee7237676a36ccf007d3664786b6192c545ca328c5512810606fe06
447142c433f59e2937ae4bae2395e23f90db0335deb8287fe6743ca0a864e14b
```

Note: You can also run this command on your QRadar Console before you set up the App Node to list your docker containers.

Verify that docker services are running

```
systemctl status docker
```

Accessing your app's command line

Access an installed app on the command line by using the container ID for the app.

To display a list of running app containers, type the following command:

```
/opt/qradar/support/qapp_utils_730.py ps
```

The following output example shows an app that is installed and is running.

```
Id   Name      Container      Container Image      Container ip:port  Host ip:port      ABCDEFGHI
1053 QRadar App Editor 5dca41d9e5e1 qregi...1053:2.0-release 192.0.2.0:5000 203.0.113.86:25568 ++++++++
```

Type the following command to connect to an app:

```
/opt/qradar/support/qapp_utils_730.py connect <app_ID>
```

Here's an example of the output:

```
Collecting app data..... Complete!
```

```
bash-4.1#
```


Go to the `/store/log` directory to view the app logs.

```
bash-4.1# cd /store/log
bash-4.1# ls
app.log  celery.log  startup.log  supervisord.log
bash-4.1#
```

Adding an App Node

To offset the processing capacity that is done by the QRadar Console for apps, add an App Node to your deployment. The App Node is an unmanaged host that is dedicated to running apps.

Before you begin

Before you can add an App Node:

- Follow the instructions in [“Setting up an App Node” on page 114](#).
- You must provide the IP address of the host and a user account with **sudo** access.

For more information about setting up a server to act as an App Node, see [“Prerequisites for setting up an App Node” on page 112](#).

About this task

Procedure

1. On the **Admin** tab, click **Node Management**.
2. To add an App Node, click **Add** on the **Node Management** window and add the App Node IP address, and the App Node user and password information.

Confirm the host **ssh** key information for the node you are creating. The installation process takes up to 30 minutes to complete. For more information about the installation process as it is happening, click **Details**.

Results

The App Node setup process moves any apps that you installed on the QRadar Console to the App Node. The App Node host name changes to `control-01`.

Note: The App Node changes the status of all apps that were running or stopped on the QRadar Console to a running state when they are moved.

What to do next

You use the **Extensions Management** window to install apps on the App Node that you set up. Any apps that you install in future are installed on the App Node, not on the QRadar Console.

Removing an App Node

If you are doing maintenance, or are consolidating servers, you can remove an App Node from your deployment.

Procedure

In the **Node Management** window on the Admin tab, select the node that you want to remove in the **Node Management** table and click **Remove**.

- To move apps from the App Node back to the QRadar Console, select the **Revert to Console** removal type.

The product attempts to move apps onto the Console if there is disk space available for them. The order in which apps are moved is determined by their size (including any associated data). The smallest apps are moved first. Because the available space for apps on the Console is likely to be less than on the App Node, you might not be able to transfer all your apps. Use the **Extension Management**

window to delete any apps that you no longer require from the App Node before you select the **Revert to Console** removal option.

By default, up to 10% of the available memory on the Console, and up to 90% of the /store partition on the Console is available for apps.

- To retain your apps on the App Node, select the **Maintenance Mode** removal type.

Maintenance Mode removes the App Node entry from the **Node Management** table and stops the apps on the App Node. The apps are restarted when you add the App Node again.

- To force apps to revert to the Console, select the **Forced Revert** removal type.

Forced Revert moves apps to the Console even if the Console doesn't have sufficient resources to run the apps. Any app that can run on the Console start after they are reverted. Any app that can't run on the Console is moved to the Console in an error state.

Note: The **Forced Revert** removal type is intended to be used if your App Node is down and you need to restore apps to the Console while you fix the App Node. **Forced Revert** recreates applications with no data volume on the Console. Any app that has been forced to revert will be like a newly installed app.

For more information about the removal process as it is progressing, click **Details**.

Checking the integrity of event and flow logs

When log hashing is enabled, any system that writes event and flow data creates hash files. Use these hash files to verify that the event and flow logs were not modified since they were originally written to disk.

The hash files are generated in memory before the files are written to disk, so the event and flow logs cannot be tampered with before the hash files are generated.

Before you begin

Ensure that log hashing is enabled for your IBM Security QRadar system. For information about enabling the flow log hashing or event log hashing parameters, see [Configuring system settings](#).

About this task

You must log in to the system that has the data storage for events and flows, and run a utility to check the logs. You cannot check the log integrity in the event and flow viewer interface.

This table describes the parameters that are used with the **check_ariel_integrity.sh** utility.

Table 27. Parameters for the check_ariel_integrity.sh utility	
Parameter	Description
-d	Duration of time, in minutes, of the log file data to scan. The time period immediately precedes the end time that is specified using the -t parameter. For example, if -d 5 is entered, all log data that was collected five minutes before the -t end time is scanned.
-n	The QRadar database to scan. Valid options are events and flows.
-t	The end time for the scan. The format for the end time is "yyyy/mm/dd hh:mm" where hh is specified in 24-hour format. If no end time is entered, the current time is used.
-a	Hashing algorithm to use. This algorithm must be the same one that was used to create the hash keys. If no algorithm is entered, SHA-1 is used.
-r	The location of the log hashing. This argument is required only when the log hashing is not in the location that is specified in the configuration file, /opt/qradar/conf/arielConfig.xml.

Table 27. Parameters for the **check_ariel_integrity.sh** utility (continued)

Parameter	Description
-k	The key that is used for Hash-based Message Authentication Code (HMAC) encryption. If you do not specify an HMAC key and your system is enabled for HMAC encryption, the check_ariel_integrity.sh script defaults to the key specified in the system settings.
-h	Shows the help message for the check_ariel_integrity.sh utility.

Procedure

1. Use SSH to log in to QRadar as the root user.
2. To run the utility, type the following command:

```
/opt/qradar/bin/check_ariel_integrity.sh -d <duration> -n <database name>
[-t <endtime>] [-a <hash algorithm>] [-i <hash root directory>] [-k <hmac key>]
```

For example, to validate the last 10 minutes of event data, type the following command:

```
/opt/qradar/bin/check_ariel_integrity.sh -n events -d 10
```

Results

If an ERROR or FAILED message is returned, the hash key that is generated from the current data on the disk does not match the hash key that was created when the data was written to the disk. Either the key or the data was modified.

Adding custom actions

Attach scripts to custom rules to do specific actions in response to network events. Use the **Custom Action** window to manage custom action scripts.

Use custom actions to select or define the value that is passed to the script and the resulting action.

For example, you can write a script to create a firewall rule that blocks a source IP address from your network in response to a rule that is triggered by a defined number of failed login attempts.

The following examples are custom actions that are the outcomes of passing values to a script:

- Block users and domains.
- Initiate work flows and updates in external systems.
- Update TAXI servers with a STIX representation of a threat.

Custom actions work best with low volume custom rule events and with custom rules that have a low response limiter value.

1. On the navigation menu (☰), click **Admin**.
2. In the **Custom Actions** section, click **Define Actions**.
3. To upload your scripts, click **Add**. Programming language versions that the product supports are listed in the **Interpreter** list.

For the security of your deployment, QRadar does not support the full range of scripting functionality that is provided by the Python, Perl, or Bash languages.

4. Specify the parameters that you want to pass to the script that you uploaded.

Table 28. Custom action parameters	
Parameter	Description
Fixed property	<p>Values that are passed to the custom action script.</p> <p>These properties are not based on the events or flow themselves, but cover other defined values that you can use the script to act on. For example, pass the fixed properties username and password for a third-party system to a script to send an SMS alert.</p> <p>Encrypt fixed properties by selecting the Encrypt value check box.</p>
Network event property	<p>Dynamic Ariel properties that are generated by events. Select from the Property list.</p> <p>For example, the network event property sourceip provides a parameter that matches the source IP address of the triggered event.</p> <p>For more information about Ariel properties, see the <i>IBM Security QRadar Ariel Query Language Guide</i>.</p>

Parameters are passed into your script in the order in which you added them in the **Custom Actions** window.

When custom action scripts are run, a `chroot jail` is set up in the `/opt/qradar/bin/ca_jail/` directory. Any content in the `/opt/qradar/bin/ca_jail/` directory can be modified and written to by scripts. The custom action user's home directory (`/home/customactionuser`) can also be modified.

A script can run only from inside the jail environment so that it does not interfere with the QRadar run environment. All file access during custom action execution is relative to the `/opt/qradar/bin/ca_jail/` directory.

The custom action user account might not have permission to run follow-up commands, such as logging into a firewall and blocking an IP address. Test whether your script runs successfully before you associate it with a rule.

Note: The type of custom action that you implement depends on your network infrastructure and its components. For example, you can configure REST APIs on Cisco devices to block suspect IP addresses. Other third-party vendors might not provide a REST interface, so you might need to develop your own web services solution to run custom actions.

You must run the `dos2unix` utility on scripts that originate from a Windows or DOS system. Windows or DOS systems typically add control characters. To successfully test custom action scripts by using the script **Test Execution** function in QRadar, you must remove the control characters.

Testing your custom action

Test whether your script runs successfully and has the intended result before you associate it with a rule.

About this task

Custom action scripts run inside a testing environment that is isolated from your production environment. Custom action scripts typically run on the managed host that runs the event processor. However, if you have an All-In-One appliance, custom actions run on the QRadar Console.

Test Execution is supported only on the QRadar Console and is not supported on managed hosts.

If you must write to disk from a custom action script, you must use the following directory: `/home/customactionuser`.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Custom actions** section, click **Define actions**.
3. Select a custom action from the list and click **Test Execution > Execute** to test your script. The result of the test and any output that is produced by the script is returned.
4. After you configure and test your custom action, use the **Rule Wizard** to create a new event rule and associate the custom action with it.

For more information about event rules, see the *IBM Security QRadar User Guide*.

Passing parameters to a custom action script

Sample scripts in Bash, Python, and Perl show how to pass parameters to custom action scripts.

The following simple sample scripts show how to query the asset model API for an asset with the supplied offense source IP address. For the sake of this example, the scripts output the JSON that is returned by the endpoint.

The scripts require three parameters:

- Console IP address
- API token
- Offense source IP address

These parameters are configured in the Define Custom Action window **Script Parameters** area:

Define Custom Action

Script File:

File will upload on save.

Script Parameters

Parameter Name:

☐ Fixed Property

☒ Network Event Property

Property:

Name	Type	Value
console_ip	Fixed Property	
api_token	Fixed Property	4e176ca6-a46e-3471-8211-45f3d7f2893e
offense_source_ip	Network Event Property	sourceip

Figure 4. Custom action script parameters

Each parameter is passed to the script in the order in which it was added in the Define Custom Action window. In this case:

1. console_ip
2. api_token
3. offense_source_ip

The variables that are defined at the beginning of each of the sample scripts use the sample parameter names that were added in the Define Custom Action window.

```
#!/bin/bash
console_ip=$1
api_token=$2
offense_source_ip=$3

auth_header="SEC:$api_token"

output=$(curl -k -H $auth_header https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29)

# Basic print out of the output of the command
echo $output
```

Figure 5. *call_asset_model.sh*

```
#!/usr/bin/python
import sys
import requests
console_ip = sys.argv[1]
api_token = sys.argv[2]
offense_source_ip = sys.argv[3]

auth_header = {'SEC' : api_token }

endpoint = "https://{0}/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22{1}%22%29%29"
.format(console_ip, offense_source_ip)

response = requests.get(endpoint, headers=auth_header, verify=False)

# Basic print out of the output of the command
print(response.json())
```

Figure 6. *call_asset_model.py*

```
#!/usr/bin/perl
use strict;
use warnings;
use LWP::UserAgent;

my $console_ip = $ARGV[0];
my $api_token = $ARGV[1];
my $offense_source_ip = $ARGV[2];

my $endpoint = "https://$console_ip/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29";

my $client = LWP::UserAgent -> new(ssl_opts => { verify_hostname => 0 });

my $response = $client -> get($endpoint, "SEC" => $api_token);

# Basic print out of the output of the command
print $response -> decoded_content;
```

Figure 7. *call_asset_model.pl*

For more information on how to authenticate the API using authorized services, see the *IBM Security QRadar API Guide*.

Related concepts

[“Managing authorized services” on page 165](#)

You can configure authorized services on the **Admin** tab to authenticate an API call for your IBM Security QRadar deployment.

Managing aggregated data views

A large volume of data aggregation can decrease your system performance. The Ariel function uses a separate database for aggregated data in order to improve system performance and to make the data more readily available. You can disable, enable, or delete aggregated data views. Time series charts, report charts, and anomaly rules use aggregated data views.

About this task

The items that appear in the **Display** list sort the data.

The Aggregated Data View is required to generate data for ADE rules, time series graphs, and reports.

Disable or delete views if the maximum number of views is reached.

Duplicate views can appear in the **Aggregated Data ID** column because an aggregated data view can include multiple searches.

Procedure


1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Aggregated Data Management**.
3. To filter the list of aggregated data views, perform one the following options:
 - Select an option from the **View**, **Database**, **Show**, or **Display** list.
 - Type an aggregated data ID, report name, chart name, or saved search name in the search field.
4. To manage an aggregated data view, select the view, and then click the appropriate action on the toolbar:
 - If you select **Disable View** or **Delete View**, content dependencies are displayed for the aggregated data view. After you disable or delete the view, the dependent components no longer use aggregated data.
 - Enable a previously disabled aggregated data view to restore the view.

Table 29. Aggregated Data Management View column descriptions	
Column	Description
Aggregated Data ID	Identifier for the aggregated data
Saved Search Name	Defined name for the saved search
Column Name	Column identifier
Times Searches	Search count
Data Written	The size of the written data
Database Name	Database where the file was written
Last Modified Time	Timestamp of the last data modification
Unique Count Enabled	True or False: Search the results to display unique event and flowcounts instead of average counts over time.

Accessing a GLOBALVIEW database

Use the QRadar REST API documentation interface to get the GLOBALVIEW database results for a given saved search name and time range. The type of data contained in the database results corresponds to the type of saved search queried.

Procedure

1. Find a saved search.
 - a) On the navigation menu () , click **Admin**.
 - b) In the **System Configuration** section, click **Aggregated Data Management**.
 - c) Under the **Saved Search Name** column, record a saved search name from the list.
2. Query the QRadar REST API to find a search ID.
 - a) Log in to the QRadar API, `https://<Console IP>/api_doc`, as an administrator.
 - b) Click the most recent version of the QRadar API.
 - c) Click the `/ariel/searches` endpoint.
 - d) Click **POST**.
 - e) In the **query_expression** parameter field, type the following command: `select * from GLOBALVIEW('savedsearch', 'timerange')`

Use one of the following values for the *timerange* variable:

```
NORMAL  
HOURLY  
DAILY
```

The following example shows query for Top Log Sources with a time range of the last two days:

```
select * from GLOBALVIEW('Top Log Sources', 'DAILY') last 2 days
```

- f) Click **Try It Out!**
 - g) Copy the search ID from the response body.
3. Get the search results.
 - a) From the `/ariel/searches/search{id}/results` endpoint, click **GET**.
 - b) In the **search_id** parameter field, enter the search ID.
 - c) Click **Try It Out!**.
 - d) Ensure that the search successfully completes.
 - e) Get the database results from the response body.

Chapter 7. Processing event data in QRadar

In IBM Security QRadar, use the DSM Editor to solve parsing problems and to add custom parsing.

The DSM Editor provides real-time feedback so that you know whether your customization works the way that you expect it to.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

DSM Editor overview

Instead of manually creating a log source extension to fix parsing issues or extend support for new log source types, use the DSM Editor. The DSM Editor provides different views of your data. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definition.

The DSM Editor provides the following views:

Workspace

The **Workspace** shows you raw event data. Use sample event payloads to test the behavior of the log source type, and then the **Workspace** area shows you the data that you capture in real time.

All sample events are sent from the workspace to the DSM simulator, where properties are parsed and QID maps are looked up. The results are displayed in the **Log Activity Preview** section. Click the edit icon to open in edit mode.

In the edit mode, you paste up to 100,000 characters of event data into the workspace or edit data directly. When you edit properties on the **Properties** tab, matches in the payload are highlighted in the workspace. Custom properties and overridden system properties are also highlighted in the **Workspace**.

Log activity preview

The **Log activity preview** section simulates how the payloads in the **Workspace** appear in the **Log Activity** viewer. If nothing is displayed in the **Workspace**, then the **Log Activity** viewer is empty.

Click the configure icon to select which columns to show or hide in the **Log Activity Preview** window, and to reorder the columns. Every standard property that is supported displays in the preview. You can choose the columns that display in the preview from the **Configure Preview Columns** window. Available columns in the list that are marked with an asterisk (*), such as **Event name**, **Severity**, **Low-level category**, and **QID**, are populated from the QID map.

Fields that are populated from the QID map cannot be parsed verbatim from the raw events data in the workspace and for this reason, they cannot be defined or edited. However, you can adjust their values by selecting the corresponding Event ID/Event Category combination from the **Event Mappings** tab.

Properties

The **Properties** tab contains the combined set of system and custom properties that constitute a DSM configuration. Configuring a system property differs from configuring a custom property. You can override a property, by selecting the **Override system behaviour** check box and defining the regex or JSON expression.

Matches in the payload are highlighted in the event data in the workspace. The highlighting color is two-toned, depending on what you capture. For example, the orange highlighting represents the capture group value while the bright yellow highlighting represents the rest of the regex that you specified. The feedback in the workspace shows whether you have the correct regex. If an expression is in focus, the highlighting in the workspace reflects only what that expression can match. If the overall property is in focus, then the

highlighting turns green and shows what the aggregate set of expressions can match, taking into account the order of precedence.

In the **Format String** field, capture groups are represented by using the `$<number>` notation. For example, `$1` represents the first capture group from the regex, `$2` is the second capture group, and so on.

You can add multiple expressions to the same property, and you can assign precedence by dragging and dropping the expressions to the top of the list.

A warning icon beside any of the properties indicates that no expression was added.

Event mappings tab

The **Event Mappings** tab displays all the event ID and category combinations that exist in the system for a selected log source type. If a new event mapping is created, it is added to the list of event ID and category combination that is displayed in the **Event Mappings** tab. In general, the **Event Mappings** tab displays all event ID and category combinations and the QID records that they are mapped to.

Configuration tab

You can configure Auto Property Discovery for structured data that are in JSON format. By default, log source types have Auto Property Discovery turned off.

When you enable **Auto Property Discovery** on the **Configuration** tab, the property discovery engine automatically generates new properties to capture all fields that are present in the events that are received by a log source type. You can configure the number of consecutive events to be inspected for new properties in the **Discovery Completion Threshold** field. Newly discovered properties appear in the **Properties** tab, and are made available for use in the rules and search indexes. However, if no new properties are discovered before the threshold, the discovery process is considered complete and **Auto Property Discovery** for that log source type is disabled. You can manually enable the Auto Property Discovery on the Configuration tab at any time.

Note: To continuously inspect events for a log source type, you must make sure that you set the **Discovery Completion Threshold** value to 0.

Related concepts

Properties in the DSM Editor

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

Properties in the DSM Editor

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

A DSM cannot have multiple properties with the same name.

The configuration of a system property differs from a custom property.

System properties

System properties cannot be deleted but you can override the default behavior. There are two types of system properties:

Predefined system property

Displays the default QRadar behavior that is used for the DSM.

Override system property

System properties with override configured (log source extension) show **Override** in the status line. When a system property has an override, a log source extension for that DSM uses the regular expressions that you entered for the configuration.

Custom properties

Custom properties show **Custom** in the status line.

Custom properties differ from system properties in these ways:

- Custom properties display **Custom** below their name.
- Custom properties have no **Override system behavior** check box.
- To make a custom property available for rules and search indexing, select the **Enable this Property for use in Rules and Search Indexing** check box when you create a custom property.

Note: When you select this option, QRadar attempts to extract the property from events as soon as they enter the pipeline. Extracted property information and the remainder of the event record are persisted. The property does not need to be extracted again when it is used in a search, or report. The process enhances performance when the property is retrieved, but the process can have a negative impact on performance during event collection and storage.

- Custom properties must have one or more expressions to be valid.

Related concepts

[DSM Editor overview](#)

Instead of manually creating a log source extension to fix parsing issues or extend support for new log source types, use the DSM Editor. The DSM Editor provides different views of your data. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definition.

[Custom property definitions in the DSM Editor](#)

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

Property configuration in the DSM Editor

Configure properties in the DSM Editor to change the behavior of an overridden system property or the custom property of a DSM.

When you override the behavior of a system property, you must provide a valid JSON or regex on the **Properties** tab. The **Format String** field is a combination of regex capture groups and literal characters. The string is used to populate system properties by one or more values that are captured from events, and with more formatting characters or injected information. For example, you might want to parse an IP address and a port to combine them both into a string. If your regular expression (regex) has two capture groups, you can combine them by using this format string: **\$1:\$2**.



Attention: The DSM Editor allows capture group references of 1 through 9 in any specific match. If you reference any capture group above 9, the log source extension might not work correctly.

You must configure each custom property that you create. You must provide a valid JSON or regex and capture group for a custom property on the **Properties** tab. You can also define selectivity and enable or disable your expression.

Related concepts

[“Custom property definitions in the DSM Editor” on page 133](#)

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

How to write a format string in the DSM Editor

Use the **Format String** field on the **Property Configuration** tab to reference capture groups that you defined in the regex. Capture groups are referenced in their order of precedence.

A capture group is any regex that is enclosed within parenthesis. A capture group is referenced with an **\$n** notation, where **n** is a group number that contains a regular expression (regex). You can define multiple capture groups.

For example, you have a payload with company and host name variables.

```
"company":"ibm", "hostname":"localhost.com"
"company":"ibm", "hostname":"johndoe.com"
```

You can customize the host name from the payload to display *ibm.hostname.com* by using capture groups:

1. In the **regex** field, enter the following regular expression:

```
"company": "(.*)".* "hostname": "(.*)"
```

2. In the **Format String** field, enter the capture group \$1.\$2 where \$1 is the value for the company variable (in this case ibm) and \$2 is the value for the host name in the payload.

The following output is given:

```
ibm.localhost.com
```

```
ibm.johndoe.com
```

How to write regex for well-structured logs

Well-structured logs are a style of event formatting that is composed of a set of properties and are presented in this way:

```
<name_of_property_1><assignment_character>
<value_of_property_1><delimiter_character>
<name_of_property_2><assignment_character>
<value_of_property_2><delimiter_character>
<name_of_property_3><assignment_character>
<value_of_property_3><delimiter_character>...
```

Use the following general guidelines:

- The **<assignment_character>** either '=' or ':' or a multi-character sequence such as '->'.
- The **<delimiter_character>** either a white space character (space or tab) or a list delimiter, such as a comma or semi-colon.
- The **<value_of_property>** and sometimes **<name_of_property>** are encapsulated in quotation marks or other wrapping characters.

For example, consider a simple login event that is generated by a device or an application. The device might report on the account of a user who logged in, the time the login occurred, and the IP address of the computer from which the user logged in. A name/value pair-style event might look like this snippet:

```
<13>Sep 09 22:40:40 192.0.2.12 action=login accountname=JohnDoe clientIP=192.0.2.24
timestamp=01/09/2016 22:40:39 UTC
```

Note: The string "<13>Sep 09 22:40:40 192.0.2.12" is a syslog header. The string is not part of the event body.

The following table shows how the properties of the well-structured log example above, can be captured:

Table 30. Regex for capturing properties of a well-structured log	
Property	Regex
action	action=(.*)\t
accountname	accountname=(.*)\t
clientIP	clientIP=(.*)\t
timestamp	timestamp=(.*)\t

The patterns that are enclosed within the brackets denote the capture group. Each regex in the table captures everything after the equal sign (=) and before the next tab character.

How to write regex for natural language logs

Natural language logs are presented in a sentence-like form and each event type might look different.

For example, a simple login event can be presented in the following form:

```
<13>Sep 09 22:40:40 192.0.2.12 Account JohnDoe initiated a login action
from 192.0.2.24 at 01/09/2016 22:40:39 UTC
```

The following table shows how the properties of the natural language log in the example above, can be captured:

Table 31. Regex for capturing properties of a natural language log	
Property	Regex
action	initiated a (.*?) action
accountname	Account (.*?) initiated
clientIP	from (.*?) at
timestamp	at (.*?)

Note: Writing regex for natural language logs requires you to look at the static information that surrounds the value you want to capture before you create the capture group.

How to write an expression for structured data in JSON format

Structured data in JSON format contains one or more properties, which are represented as a key-value pair.

You can extract properties from an event data presented in JSON format by writing a JSON expression that matches the property. The JSON expression must be a path in the format of `/"<name of top-level field>"`.

For example, you have an event data formatted in JSON:

```
{ "action": "login", "user": "John Doe" }
```

To extract the 'user' property, type the expression `/ "user"` in the **Expression** field.

However, for an event data with a nested JSON format such as the following example:

```
{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }
```

you can extract the 'last_name' of the user by typing the expression `/ "user" / "last_name"` in the **Expression** field.

How to write a JSON keypath expression

To uniquely identify the fields that you want to extract from a JSON object, your JSON expression must follow specific JSON keypath conventions.

Use the following guidelines for your JSON keypath expressions:

- A forward slash (/) must be at the start of all JSON keypaths. All paths must start at the beginning of the root JSON object. Subsequent slashes in the keypath indicate access to fields that are nested in the JSON object.
- Field names must be enclosed in double quotation marks.

A valid path might look like the following example:

```
/"object"/"nestedObject"/"furtherNestedObject"/"desiredPropertyName"
```

- Square brackets indicate the handling of JSON arrays.

If you do not supply an index in the square brackets, the entire body of the array is extracted. If you supply an index in the square bracket, that index in the array is extracted or nested. Arrays begin at a zero index, where 0 is the first index in the array, 1 is the second index in the array, and so on.

In the following keypath example, the JSON parser looks into the second index of the "object" JSON array, and then within that array index, looks for a field called "desiredPropertyName".

```
/"object"[1]/"desiredPropertyName"
```

- Within log source extensions, you can supply and combine together multiple JSON keypaths to give a single result; this convention excludes custom properties. You can also choose to include literal text. Each of the JSON keypaths must be enclosed in curly braces.

Consider the following example:

```
{/"object"/"nestedObject"/"desiredPropertyName1"} {/"object"/"nestedObject"/"desiredPropertyName2"}
```

You get a parsed value from the first JSON keypath, a literal text space, and then a parsed value from the second JSON keypath.

Example: The following two examples show how to extract data from a JSON object:

- Simple case of a JSON object:

```
[{"name":"object1","field1":"value1"}, {"name":"object2","field2":"value2"}, {"name":"object3","field3":"value3"}]
```

The following table shows the values that are extractable from the keypaths in that sample object:

Table 32. Keypaths from the simple JSON object		
Keypaths	Description	Value
/[]	Extracts the entire JSON array from the root of the JSON object.	[{"name":"object1","field1":"value1"}, {"name":"object2","field2":"value2"}, {"name":"object3","field3":"value3"}]
/[1]/"name"	Extracts the value for the attribute called "name" from the JSON object at index 1 in the root JSON array.	object2

- Complex case of a JSON object:

```
<13>May 22 10:15:41 log.test.com {"module":"CPHalo","version":"1.0","user_name":"user123",
"event_type":"File integrity scan request created",
"event_category":"File Integrity Scanning Management","srcName":"domain-lab-123",
"timestamp":"2018-12-02T15:36:17.486","user":{
"email":"user123@example.com","first_name":"fname",
"last_name":"lname","alias":["alias name","alias1","name"]},"client_ip":"12.12.12.12",
"server_id":"12317412471421274","server_reported_fqdn":"None","actor_country":"USA",
"server_group_name":"Example Server","server_platform":"Linux",
"message":"A file integrity monitoring scan was requested for Linux server domain-lab-123
(13.13.13.13) by Halo user user123@example.com from IP address 12.12.12.12 (USA).",
"type":"fim_scan_request_created","id":"c2e8bf72-b74f-11e2-9055-870a490fcfb6"}
```

The following table shows the values that are extractable from the keypaths in that sample object:


Table 33. Keypaths from the complex JSON object		
Keypaths	Description	Value
/"user_name"	Extracts value of the "user_name" attribute from the root of the JSON object.	user123
/"user"/"alias"[]	Extracts the entire JSON array called "alias" that is nested under the "user" JSON object.	["alias name","alias1","name"]
/"user"/"alias"[0]	Extracts the value at index 0 within the "alias" JSON array that is nested under the "user" JSON Object.	alias name
/"user"/"first_name"	Extracts the value of the property called "first_name" that is nested under the "user" JSON Object.	fname
{/"user"/"first_name"}. {/ "user"/"last_name"}	Extracts the value of the property called "first_name" that is nested under the "user" JSON object, then inserts a literal '.' character, and then extracts the value of the property called "second_name" that is nested under the "user" JSON object. Pertains only to log source extensions and non-custom properties within the DSM Editor. This operation is not possible in custom properties.	fname.lname
{/"user"/"alias"[1]}@{/ "client_ip"}	Extracts the value at index 1 of the "alias" JSON array that is nested under the "user" JSON object, inserts a literal '@' character, and then extracts the value of the property called "client_ip" under the root JSON object. Pertains only to log source extensions and non-custom properties within the DSM Editor. This operation is not possible in custom properties.	alias1@12.12.12.12

Opening the DSM Editor

You can open the DSM Editor from the **Log activity** tab, or if you are an administrator, you can open it from the **Admin** tab. For example, if events that are sent to the system are not handled properly, you can select the event data from the **Log Activity** tab and send it to the DSM Editor. For events that are not yet sent to the system, you must be an administrator and access the DSM Editor from the **Admin** tab.

Procedure

1. To open the DSM Editor from the **Admin** tab, follow these steps:

- a) On the navigation menu () , click **Admin**.
 - b) In the **Data Sources** section, click **DSM Editor**.
2. To open the DSM Editor from the **Log Activity** tab, follow these steps:
- a) Click the **Log Activity** tab.
 - b) Pause the incoming results and then highlight one or more events.

Important: If more than one event from two or more log sources are selected, you are prompted to select which log source type you want to operate on. You can select only a single log source type, and only the events from log activity that match the selected log source type are automatically added to the workspace.
 - c) On the navigation menu, select **Actions > DSM Editor**

Configuring a log source type

With the DSM Editor, you can configure a new log source type or use an existing one in IBM Security QRadar.

About this task

You can configure log sources for custom applications and systems that don't have a supported DSM. Rather than using a universal DSM (uDSM), you can create a new log source type by using the DSM Editor. Then, you can associate the incoming events and extra content (custom properties, searches, rules, and so on) with just that log source type. When a uDSM is used for event feeds that have no supported DSM, any associated content is run against all of these events. Running the uDSM in this scenario is not good for system performance.

Note:

- The DSM Editor works on only 1 log source type at a time.
- You can delete custom log source types. Deleted log source types are not presented as an option when you create a new log source, and are not available for editing in the DSM Editor, but any existing log sources of this type remain active.

Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Data Sources** section, click **DSM Editor**.
3. Create a log source type or select an existing log source type:
 - To create a new log source type, click **Create New** and follow the prompts.
 - To locate an existing log source type, use the **Filter** field and then click **Select**.

Configuring Auto Property Discovery for Log Source types


You can configure auto discovery of new properties for a log source type.

About this task

By default, Auto Property Discovery for a log source type is disabled. Auto Property Discovery can be enabled on the **Configuration** tab. When enabled, new properties are automatically generated to capture all fields that are present in the events that the selected log source type receives. The newly discovered properties appear in the **Properties** tab of the DSM Editor.

Note: Auto Property Discovery works only for structured data that is in JSON format.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **Data Sources** section, click **DSM Editor**.
3. Select a log source type or create a new one from the **Select Log Source Type** window.
4. Click the **Configuration** tab.
5. Click **Enable Auto Property Discovery**.
6. Select the structured data format for the log source type from the **Property Discovery Format** list. The default is **JSON**.
7. To enable new properties to be use in rules and searches, turn on the **Enable Properties for use in Rules and Search Indexing**.
8. In the **Discovery Completion Threshold** field, set the number of consecutive events to inspect for new properties.
Note: If no new properties are discovered when the number of consecutive events are inspected, the discovery process is considered complete and Auto Property Discovery is disabled. You can manually re-enable Auto Property Discovery at any time. A threshold value of 0 means that the discovery process perpetually inspects events for the selected log source type.
9. Click **Save**.

Custom property definitions in the DSM Editor

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

Where relevant, each custom property has a set of configuration options that includes selectivity and data parsing. Each custom property definition within a DSM configuration is an ordered group of expressions that consists of an expression type, an expression, a capture group, an optional selectivity configuration, and an enabled or disabled toggle button. You can't modify the **Name**, **Field type**, **Description**, **optimize** fields, or any advanced options for a custom property on the **Properties** tab in the DSM Editor.

A custom property is shared across all DSMs, while specific implementations for reading values from payloads are at the DSM level.

Selectivity is specified when you configure an expression to run only when certain conditions are met.

Note: The **Capture Group** field of a custom property cannot be assigned a value greater than the number of capture groups in the regex.

Related concepts

[Properties in the DSM Editor](#)

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

Selectivity

In the DSM Editor, you can restrict running a custom property to certain criteria for better performance.

The following are the types of restrictions:

By high-level category and low-level category

A property is evaluated only when the high-level and low-level categories match a specific combination. For example, a property is evaluated only when the event is known to have a high-level category of **Authentication** and a low-level category of **Admin Logout**.

By specific QID

A property is evaluated only when the event that is seen maps to a specific QID. For example, when the event maps to a QID of **Login Failed**, the property is evaluated.

Expressions

You can define expressions for custom properties in the DSM Editor. Expressions are the mechanism that defines the behavior of a property. The main component of an expression is a valid regex or json. The data that makes up an expression depends on the property type.

For a custom property, you can choose only one capture group from the regex.

Creating a custom property

In the DSM Editor, you can define a custom property for one or more log source types whose events do not fit into the IBM Security QRadar normalized event model. For example, the set of system properties might not capture all relevant data from some applications, operating systems, databases, and other systems.

About this task

You can create custom property for data that does not fit into QRadar system properties. Use the custom properties in searches and test against them in rules.

Table 34. Custom property parameters	
Parameter	Description
Name	A descriptive name for the custom property that you create.
Field Type	The default is Text . Note: When you select Number or Date from the Field Type list, extra fields are displayed.
Enable this Property for use in Rules and Search Indexing	When enabled, QRadar attempts to extract the property from events immediately as they enter the system. Property information is persisted along with the rest of the event record and doesn't need to be extracted again when it is retrieved as part of a search or report. This enhances performance when the property is retrieved, but can have a negative impact on performance during the event collection process, as well as an impact to storage. Note: For Custom Properties to be used in rule tests or for search indexing, this option must be checked, because indexing and rule evaluation occurs before events are written to disk.
Use number format from a Locale	This field displays when you select Number from the Field Type list. If you select the Use number format from a Locale check box, you must select an Extracted Number Format from the list that displays.
Extracted Date/Time Format	This field displays when you select Date from the Field Type list. You must provide a datetime pattern that matches how the datetime appears in the original event. For example, 'MMM dd YYYY HH:mm:ss' is a valid datetime pattern for a timestamp like 'Apr 17 2017 11:29:00'.

Table 34. Custom property parameters (continued)

Parameter	Description
Locale	<p>This field displays when you select Date from the Field Type list. You must select the locale of the event.</p> <p>For example, if the locale is English, it will recognize 'Apr' as a short form of the month 'April'. But if the event is presented in French and the month token is 'Avr' (for Avril), then set the locale to a French one, or the code won't recognize it as a valid date.</p>

Procedure

- To add a custom property, click Add (+) on the **Properties** tab in the DSM Editor.
- To create a new custom property definition, use the following steps:
 - Select **Create New** on the **Choose a Custom Property Definition to Express** page.
 - On the **Create a new Custom Property Definition** page, enter values for the **Name**, **Field type**, and **Description** fields.

Note: When you select **Number** or **Date** from the **Field Type** list, extra fields display.
 - If you want to extract the property from events as they enter the system, select the **Enable this property for use in Rules and Search indexing** check box.
 - Click **Save**.
- To use an existing custom property, use the following steps:
 - On the **Choose a Custom Property Definition to Express** page, search for an existing custom property from the **Filter Definitions** field.
 - Click **Select** to add the custom property.
- To configure a custom property, use the following steps:
 - Locate and select the custom property on the **Properties** tab. Custom properties display the word **Custom** next to them, to differentiate them from system properties.
 - Select an expression type (Regex or JSON) from the **Expression Type** list.
 - Define a valid expression for the custom property based on the expression type selected in step b.

Note:

 - For Regex, the expression must be a valid java-compatible regular expression. Case-insensitive matching is supported only by using the (?i) token at the beginning of the expression. The (?i) token is saved in the log source extension .xml file. To use other expressions, such as (?s), manually edit the log source extension .xml file.
 - For JSON, the expression must be a path in the format of /"<name of top-level field>" with additional /"<name of sub-field>" to capture sub-fields if any.
 - If the expression type is Regex, select a capture group.
 - Optional: To limit an expression to run against a specific category, click **Edit** to add selectivity to the custom property, and select a **High Level Category** and a **Low Level Category**.
 - Optional: To limit an expression to run against a specific event or QID, click **Choose Event** to search for a specific QID.
 - From the **Expression** window, click **Ok**.
- To add multiple expressions and reorder them, follow these steps:
 - Click Add (+) at the top of the expressions list.

- b) Drag and drop expressions in the order that you want them to run.

Related information

[Guidance on defining a datetime pattern](#)

Event mapping

In the DSM Editor, the event mapping shows all the event ID and category combinations that are in the system.

An event mapping represents an association between an event ID and category combination and a QID record (referred to as event categorization). Event ID and category values are extracted by DSMs from events and are then used to look up the mapped event categorization or QID. Event categorizations store extra metadata for the event that might not exist verbatim in the raw event data, such as a human-readable name and description, a severity value, or a low level category assignment. Low-level categorization and severity are useful for search and rule definitions.



Warning: For multi-tenant environments, any user-defined mapping or event categorization information that is defined in the DSM Editor becomes visible across all tenants. You must ensure that no tenant-specific data is put in any event categorization names or descriptions.

Identity properties for event mappings

Identity data is a special set of system properties that includes **Identity Username**, **Identity IP**, **Identity NetBIOS Name**, **Identity Extended Field**, **Identity Host Name**, **Identity MAC**, **Identity Group Name**.

When identity properties are populated by a DSM, the identity data is forwarded to the asset profiler service that runs on the IBM Security QRadar console. The asset profiler is used to update the asset model, either by adding new assets or by updating the information on existing assets, including the **Last User** and **User Last Seen** asset fields when an **Identity Username** is provided.

IBM Security QRadar DSMs can populate identity data for certain events, such as those that establish an association or disassociation between identity properties. This association or disassociation is for performance and also for certain events that provide new or useful information that is needed for asset updates. For example, a login event establishes a new association between a user name and an asset (an IP address, a MAC address, or a host name, or a combination of them). The DSM generates identity data for any login events that it parses, but subsequent events of different types that involve the same user, provide no new association information. Therefore, the DSM does not generate identity for other event types.

Also, the DSMs for DHCP services can generate identity data for DHCP assigned events because these events establish an association between an IP address and a MAC address. DSMs for DNS services generate identity information for events that represents DNS lookups because these events establish an association between an IP address and a host name or DNS name.

You can configure the DSM Editor to override the behavior of the identity properties. However, unlike other system properties, overridden identity property has no effect unless it is linked to specific Event ID or Event Category combinations (event mappings). When identity property overrides are configured, you can go to the **Event Mappings** tab and select an event mapping to configure specific identity properties for that event. Only identity properties that are available and captured by the configured property regex or json are populated for an event.

Note: The **Identity Username** property is unique and cannot be independently configured. If any identity properties are enabled for a particular event mapping, then the **Identity Username** property is automatically populated for the event from the available **Username** property value.

Creating an event map and categorization

An event mapping is an event ID and category combination you use to map an event to a QID. With the DSM Editor, you can create a new event mapping to map all unknown events to an entry in the QID map.

Also, you can remap existing ones to either a newly created event categorization (QIDs) or to an existing one in the system.

Procedure

1. To add an event mapping, click the Add (+) icon on the **Event Mapping** tab of DSM Editor.
2. Enter values for the **event ID**, a **category** fields.
3. To create a new event categorization, use the following steps:
 - a) From the **Create a new Event Mapping** window, click **Choose Event**.
 - b) On the **Event Categorizations** page, click **Create New QID Record**.
 - c) Enter value for the **Name**, **Description** fields, and select a **Log Source Type**, a **High Level Category**, a **Low Level Category**, and a **Severity**.
 - d) Click **Save** to create the new event categorization.
4. To use an existing event categorization, use the following steps:
 - a) From the **Create a new Event Mapping** window, click **Choose Event**.
 - b) Search for an existing event categorization on the **Event Categorizations** window.
 - c) Select a **High Level category**, **Low Level category**, **Log Source Type** or **QID**. Results are shown in the **Search Results** pane.
 - d) Click **Ok** to add the event category.

Exporting contents from the DSM Editor

You can use a content management tool script to export custom content that is created in the DSM Editor. Contents can be exported from one IBM Security QRadar deployment and imported into another QRadar deployment. You can also export custom content to external media.

The DSM Editor produces the following content types:

Table 35. DSM Editor content types		
Custom content type	String	ID
Custom properties	customproperty	6
Log source type	sensordevicetype	24
Log source extensions	deviceextension	16
Custom QidMap entries	qidmap	27

The contentManagement.pl script is in the /opt/qradar/bin directory

Exporting contents as a package

You can use the content management tool script to search for specific content that is created in the DSM Editor. These contents are exported as a package.

Procedure

1. Use SSH to log in to QRadar as the root user.
2. To search for specific content items to export, type the following command:

```
./contentManagement.pl -a search -c [content_type] -r [regex]
```

For example, to search for the content items of a log source type, type the following command:

```
/opt/qradar/bin/contentManagement.pl -a search -c 24 -i  
"<search_name>"
```

3. Create a text file that lists the content that you want to export.

Each line must include the custom content type followed by a comma-separated list of unique IDs for that type.

For example, to export three log source types with ID 24, ID 26, and ID 95, all custom properties, create a text file with the following entries:

```
sensordevicetype, 24,26,95
```

4. Export the content items as a package by using the following command:

```
/opt/qradar/bin/contentManagement.pl -a export -c package -f <source_file>
```

Exporting content for single custom property

You can use the content management tool script to export content for each custom property that is created from the **Properties** tab in the DSM Editor.

About this task

When you use the DSM Editor to create custom properties, a **customproperty** entity is produced for each custom property that is created.

Procedure

1. Use SSH to log in to QRadar as the root user.
2. To search for specific content to export, type the following command:

```
./contentManagement.pl -a search -c [content_type] -i [regex]
```

For example, to search for the content of a custom property, type the following command:

```
/opt/qradar/bin/contentManagement.pl -a search -c 6 -i  
"<name_of_custom_property>"
```

3. To export a custom property content, type the following command:

```
/opt/qradar/bin/contentManagement.pl -a export -c [content_type]  
-i [content_identifier]
```

Chapter 8. Using reference data in QRadar

Use reference data collections to store and manage business data that you want to correlate against the events and flows in your IBM Security QRadar environment. You can add business data or data from external sources into a reference data collection, and then use the data in QRadar searches, filters, rule test conditions, and rule responses.

Reference data collections are stored on the QRadar console, but the collections are regularly copied to each managed host. For best performance on data lookups, the managed host caches the most frequently referenced data values.

External threat intelligence data

You can use reference data collections to integrate indicator of compromise (IOC) data from third-party vendors into QRadar. QRadar uses IOC data to detect suspicious behavior faster, which helps security analysts investigate threats and respond to incidents more quickly.

For example, you can import IOC data, such as IP addresses, DNS names, URLs, and MD5s, from open source or subscription-based threat data providers, and correlate it with events and incidents on your network.

Business data

Reference data collections can contain business data that is specific to your organization, such as a list of users with privileged system access. Use the business data to create blacklists and whitelists.

For example, use a reference set that contains the user IDs of terminated employees to prevent them from logging in to the network. Or, you can use business data to build a whitelist that allows only a limited set of IP addresses to do specific functions.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

Types of reference data collections

There are different types of reference data collections, and each type can handle different levels of data complexity. The most common types are reference sets and reference maps.

Table 36. Types of reference data collections		
Type of collection	Description	Usage
Reference set	A collection of unique values, in no particular order. Create a reference set by using QRadar, the command line, or the RESTful API.	Use a reference set to compare a property value against a list, such as IP addresses or user names. For example, you can verify whether the LoginID that was used to log in is assigned to a user.

Table 36. Types of reference data collections (continued)

Type of collection	Description	Usage
Reference map	<p>A collection of data that maps a unique key to a value.</p> <p>Create a reference map by using the command line, or the RESTful API.</p>	<p>Use a reference map to verify a unique combination of two property values.</p> <p>For example, to correlate user activity on your network, you can create a reference map that uses the LoginID parameter as a key, and the Username as a value.</p>
Reference map of sets	<p>A collection of data that maps a key to multiple values. Every key is unique and maps to one reference set.</p> <p>Create a reference map of sets by using the command line, or the RESTful API.</p>	<p>Use a reference map of sets to verify a combination of two property values against a list.</p> <p>For example, to test for authorized access to a patent, you can create a map of sets that uses a custom event property for Patent ID as the key, and the Username parameter as the value. Use the map of sets to populate a list of authorized users.</p>
Reference map of maps	<p>A collection of data that maps one key to another key, which is then mapped to a single value. Every key is unique and maps to one reference map.</p> <p>Create a reference map of maps by using the command line, or the RESTful API.</p>	<p>Use a reference map of maps to verify a combination of three property values.</p> <p>For example, to test for network bandwidth violations, you can create a map of maps that uses the Source IP parameter as the first key, the Application parameter as the second key, and the Total Bytes parameter as the value.</p>
Reference table	<p>Similar to a map of maps, but the second key is assigned a data type.</p> <p>Create a reference table by using the command line, or the RESTful API.</p>	<p>Use a reference table to verify a combination of three property values, when one of the properties is a specific data type.</p> <p>For example, you can create a reference table that stores Username as the first key, Source IP as the second key with an assigned cidr data type, and Source Port as the value.</p>

If you want to use the same reference data in both QRadar SIEM and QRadar Risk Manager, use a reference set. You can't use other types of reference data collections with QRadar Risk Manager.

Reference sets overview

Use reference sets in IBM Security QRadar to store data in a simple list format.

You can populate the reference set with external data, such as indicators of compromise (IOCs), or you can use it to store business data, such as IP addresses and user names, that is collected from events and flows that occur on your network.

A reference set contains unique values that you can use in searches, filters, rule test conditions, and rule responses. Use rules to test whether a reference set contains a data element, or configure the rule response to add data to a reference set. For example, you can create a rule that detects when an

employee accesses a prohibited website, and configure the rule response to add the employee's IP address or user name to a reference set.

For more information about configuring rule responses to add data to a reference set, see the *IBM Security QRadar User Guide*.

Reference sets are the only type of reference data collection that you can manage in QRadar. You can also use the [command-line](#) and the [Restful API documentation interface](#) to manage reference sets.

Related tasks

[Creating reference data collections by using the command line](#)

Use the command line to manage reference data collections that cannot be managed in IBM Security QRadar, such as reference maps, map of sets, map of maps, and tables. Although it's easier to manage reference sets using QRadar, use the command line when you want to schedule management tasks.

[Creating reference data collections with the APIs](#)

You can use the application program interface (API) to manage IBM Security QRadar reference data collections.

Adding, editing, and deleting reference sets

Use a reference set to compare a property value, such as an IP address or user name, against a list. You can use reference sets with rules to keep watch lists. For example, you can create a rule to detect when an employee accesses a prohibited website and then add that employee's IP address to a reference set.

About this task

After you add data to the reference set, the **Number of Elements** and **Associated Rules** parameters are automatically updated.

When you edit a reference set, you can change the data values, but you cannot change the type of data that the reference set contains.

Before a reference set is deleted, QRadar runs a dependency check to see whether the reference set has rules that are associated with it.

Note: If you use techniques to obscure data on the event properties that you want to compare to the reference set data, use an alphanumeric reference set and add the obscured data values.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. To add a reference set:
 - a) Click **Add** and configure the parameters.

Learn more about reference set parameters:

The following table describes each of the parameters that are used to configure a reference set.

Table 37. Reference Set parameters	
Parameter	Description
Name	The maximum length of the reference set name is 255 characters.

Table 37. Reference Set parameters (continued)	
Parameter	Description
Type	<p>Select the data types for the reference elements. You can't edit the Type parameter after you create a reference set.</p> <p>The IP type stores IPv4 addresses. Alphanumeric (Ignore Case) automatically changes any alphanumeric value to lowercase.</p> <p>To compare obfuscated event and flow properties to the reference data, you must use an alphanumeric reference set.</p>
Time to Live of elements	<p>Specifies when QRadar automatically deletes elements from the reference set. Lives Forever is the default setting.</p> <p>If you specify an amount of time, indicate whether the time-to-live interval is based on when the data was first seen, or was last seen.</p> <p>When a reference set element expires, a Reference Data Expiry event is triggered. The event contains the reference set name and the element value.</p>

b) Click **Create**.

4. Click **Edit** or **Delete** to work with existing reference sets.

Tip: To delete multiple reference sets, use the **Quick Search** text box to search for the reference sets that you want to delete, and then click **Delete Listed**.

Related tasks

[Viewing the contents of a reference set](#)

[Tracking expired user accounts](#)

Use reference data collections to identify stale data, such as expired user accounts, in your IBM Security QRadar environment.

Viewing the contents of a reference set

View information about the data elements in the reference set, such as the domain assignment, the expiry on the data, and when the element was last seen in your network.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select a reference set and click **View Contents**.
4. Click the **Content** tab to view information about each data element.

Tip: Use the search field to filter for all elements that match a keyword. You can't search for data in the **Time To Live** column.

Learn more about the data elements:

The following table describes the information that is shown for each data element in the reference set.

Table 38. Information about the reference set data elements	
Parameter	Description
Domain	Domain-specific reference data can be viewed by tenant users who have access to the domain, MSSP Administrators, and users who do not have a tenant assignment. Users in all tenants can view shared reference data.

Table 38. Information about the reference set data elements (continued)	
Parameter	Description
Value	The data element that is stored in the reference set. For example, the value might show user names or IP addresses.
Origin	Shows the user name when the data element is added manually, and the file name when the data was added by importing it from an external file. Shows the rule name when the data element is added in response to a rule.
Time to Live	The time that is remaining until this element is removed from the reference set.
Date Last Seen	The date and time that this element was last detected on your network.

- Click the **References** tab to view the rules that use the reference set in a rule test or in a rule response.

Table 39. Content tab parameters	
Parameter	Description
Rule Name	Name of the rule that is configured to use the reference set.
Group	The group that the rule belongs to.
Category	Shows if the rule is a custom rule or an anomaly detection rule.
Type	Shows event , flow , common , or offense to indicate the type of data that the rule is tested against.
Enabled	A rule must be enabled for the custom rule engine to evaluate it.
Response	The responses that are configured for this rule.
Origin	System indicates a default rule. Modified indicates that a default rule was customized. User indicates a user-created rule.

- To view or edit an associated rule, double-click the rule in the **References** list and complete the rule wizard.

Adding elements to a reference set

Add elements to a reference set when you want IBM Security QRadar to compare a property to the element value. Use QRadar to manually add elements to a reference set, or to import elements from a .csv file.

Before you begin

To import elements, make sure that the .csv file is stored locally.

About this task

You can assign reference data to a specific domain. Domain-specific reference data can be viewed by tenant users who have access to the domain, MSSP Administrators, and users who do not have a tenant assignment. Users in all tenants can view shared reference data. For example, MSSP users who are not administrators can view reference data that is assigned to a domain.

Procedure

- On the navigation menu (☰), click **Admin**.

2. In the **System Configuration** section, click **Reference Set Management**.
3. Select the reference set that you want to add the elements to, and click **View Contents**.
4. Click the **Content** tab.
5. To add data elements manually, follow these steps:
 - a) Click **Add** and configure the parameters.

Valid port values are 0 - 65535. Valid IP addresses are between 0 and 255.255.255.255.

Note: If you use data obfuscation techniques on the event properties that you want to compare to the reference set data, you must use an alphanumeric reference set that contains the obfuscated data values.
 - b) Click **Add**.
6. To add elements from a .csv file, follow these steps:
 - a) Click **Import**.
 - b) Click **Select File** and browse to select the .csv file that you want to import.

The .csv file must be formatted with all items comma-separated on a single line, or with each item on a separate line. A delimiter is not required when each item is on a separate line.
 - c) Select the **Domain** that you want to add the reference set data to.
 - d) Click **Import**.

The import adds the content of the text file to the reference set.

Exporting elements from a reference set

Export reference set elements to a .csv file when you want to include the information in reports, or share the information with people who don't use IBM Security QRadar.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select the reference set that you want to export, and click **View Contents**.
4. Click the **Content** tab, and click **Export**.
5. Choose whether to open the file immediately, or save the file, and then click **OK**.

Deleting elements from a reference set

You might need to delete elements from a reference set when an element is added to the reference set in error, or when you no longer need to compare the element with other IBM Security QRadar properties. For example, you might need to remove an asset that was mistakenly added to an asset exclusion blacklist.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select the reference set that contains the elements that you want to delete, and click **View Contents**.
4. Click the **Content** tab and choose one of the following options:
 - To delete a single element, select the element from the list, and click **Delete**.
 - To delete multiple elements, use the search box to filter the list to show only the elements that you want to delete, and then click **Delete Listed**.

Creating reference data collections by using the command line

Use the command line to manage reference data collections that cannot be managed in IBM Security QRadar, such as reference maps, map of sets, map of maps, and tables. Although it's easier to manage reference sets using QRadar, use the command line when you want to schedule management tasks.

About this task

Use the `ReferenceDataUtil.sh` script to manage reference sets and other types of reference data collections.

When you use an external file to populate the reference data collection, the first non-comment line in the file identifies the column names in the reference data collection. Each line after that is a data record that gets added to the collection. While the data type for the reference collection values is specified when the collection is created, each key is an alphanumeric string.

The following table shows examples of how to format data in an external file that is to be used for populating reference maps.

Table 40. Formatting data in an external file to be used for populating reference data collections	
Type of reference collection	Data formatting examples
Reference map	key1,data key1,value1 key2,value2
Reference map of sets	key1,data key1,value1 key1,value2
Reference map of maps	key1,key2,data map1,key1,value1 map1,key2,value2

You can also create reference data collections by using the `/reference_data` endpoint in the QRadar RESTful API.

Procedure

1. Using SSH, log in to IBM Security QRadar as the root user.
2. Go to the `/opt/qradar/bin` directory.
3. To create the reference data collection, type the following command:

```
./ReferenceDataUtil.sh create name  
[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]  
[ALN | NUM | IP | PORT | ALNIC | DATE]  
[-timeoutType=[FIRST_SEEN | LAST_SEEN]] [-timeToLive=]
```

4. To populate the map with data from an external file, type the following command:

```
./ReferenceDataUtil.sh load name filename  
[-encoding=...] [-sdf=" ... "]
```

Example

Here are some examples of how to use the command line to create different types of reference data collections:

- Create an alphanumeric map:

```
./ReferenceDataUtil.sh create testALN MAP ALN
```

- Create a map of sets that contains port values that will age out 3 hours after they were last seen:

```
./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT  
-timeoutType=LAST_SEEN -timeToLive='3 hours'
```

- Create a map of maps that contains numeric values that will age out 3 hours 15 minutes after they were first seen:

```
./ReferenceDataUtil.sh create testNUM MAPOFMAPS  
NUM -timeoutType=FIRST_SEEN -timeToLive='3 hours 15 minutes'
```

- Create a reference table where the default format is alphanumeric:

```
./ReferenceDataUtil.sh create testTable REFTABLE  
ALN -keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

What to do next

Log in to QRadar to create rules that add data to your reference data collections. You can also create rule tests that detect activity from elements that are in your reference data collection.

Related concepts

[Reference sets overview](#)

Command reference for reference data utilities

You can manage your reference data collections by using the `ReferenceDataUtil.sh` utility on the command line. The following commands are available to use with the script.

Create

Creates a reference data collection.

name

The name of the reference data collection.

[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]

The type of reference data collection.

[ALN | ALNIC | NUM | IP | PORT | DATE]

The type of data in the reference set.

- **ALN** specifies alphanumeric values. This data type supports IPv4 and IPv6 addresses.
- **ALNIC** specifies alphanumeric values, but rule tests ignore the case. This data type supports IPv4 and IPv6 addresses.
- **NUM** specifies numeric values.
- **IP** specifies IP addresses. This data type supports only IPv4 address.
- **PORT** specifies port addresses.
- **DATE** specifies date values.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]

Specifies whether the amount of time the data elements remain in the reference data collection is from the time the element was first seen or last seen.

[-TimeToLive=""]

The amount of time the data elements remain in the reference data collection.

[-keyType=name:elementType,name:elementType,...]

A mandatory **REFTABLE** parameter of consisting of key name to **ELEMENTTYPE** pairs.

[-key1Label=""]

An optional label for key1, or the primary key. A key is a type of information, such as an IP address.

[-valueLabel=""]

An optional label for the values of the collection.

Update

Updates a reference data collection.

name

The name of the reference data collection.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]

Specifies whether the amount of time the data elements remain in the reference data collection is from the time the element was first seen or last seen.

[-timeToLive=""]

The amount of time the data elements remain in the reference data collection.

[-keyType=name:elementType,name:elementType,...]

A mandatory **REFTABLE** parameter of consisting of key name to **elementType** pairs.

[-key1Label=""]

An optional label for key1.

[-valueLabel=""]

An optional label for the values of the collection.

Add

Adds a data element to a reference data collection

name

The name of the reference data collection.

<value> <key1> [key2]

The key value pair that you want to add. The keys are alphanumeric strings.

- MAP and MAPOFSETS require Key 1.
- MAPOFMAPS and REFTABLE require Key 1, and the second-level Key 2.

[-sdf=" ... "]

The Simple Date Format string that is used to parse the date data.

Delete

Deletes an element from a reference data collection.

name

The name of the reference data collection.

<value> <key1> [key2]

The key value pair that you want to delete. The keys are alphanumeric strings.

- MAP and MAPOFSETS require Key 1.
- MAPOFMAPS and REFTABLE require Key 1, and the second-level Key 2.

[-sdf=" ... "]

The Simple Date Format string that is used to parse the date data.

Remove

Removes a reference data collection.

name

The name of the reference data collection.

Purge

Purges all elements from a reference data collection.

name

The name of the reference data collection.

List

Lists elements in a reference data collection.

name

The name of the reference data collection.

[displayContents]

Lists all elements in the specified reference data collection.

Listall

Lists all elements in all reference data collection.

[displayContents]

Lists all elements in all reference data collections.

Load

Populates a reference data collection with data from an external .csv file.

name

The name of the reference data collection.

filename

The fully qualified file name to be loaded. Each line in the file represents a record to be added to the reference data collection.

[-encoding=...]

Encoding that is used to read the file.

[-sdf=" ... "]

The Simple Date Format string that is used to parse the date data.

Creating reference data collections with the APIs

You can use the application program interface (API) to manage IBM Security QRadar reference data collections.

Procedure

1. Use a web browser to access `https://<Console IP>/api_doc` and log in as the administrator.
2. Select the latest iteration of the IBM Security QRadar API.
3. Select the `/reference_data` directory.
4. To create a new reference set, follow these steps:
 - a) Select `/sets`.
 - b) Click **POST** and enter the relevant information in the **Value** fields.

Learn more about the parameters to create a reference set:

The following table provides information about the parameters that are required to create a reference set:

Table 41. Parameters - Reference Set					
Parameter	Type	Value	Data Type	MIME Type	Sample
element_type	query	(required)	String	text/plain	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	query	(required)	String	text/plain	String
fields	query	(optional)	String	text/plain	field_one (field_two, field_three), field_four
time_to_live	query	(optional)	String	text/plain	String
timeout_type	query	(optional)	String	text/plain	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
5. To create a new reference map, follow these steps:
- Click /maps.
 - Click **POST** and enter the relevant information in the **Value** fields.

Learn more about the parameters to create a reference map:

The following table provides information about the parameters that are required to create a reference map:

Table 42. Parameters - Reference Map					
Parameter	Type	Value	Data Type	MIME Type	Sample
element_type	query	(required)	String	text/plain	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	query	(required)	String	text/plain	String
fields	query	(optional)	String	text/plain	field_one (field_two, field_three), field_four
key_label	query	(optional)	String	text/plain	String
time_to_live	query	(optional)	String	text/plain	String
timeout_type	query	(optional)	String	text/plain	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	query	(optional)	String	text/plain	String

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
6. To create a new reference map of sets, follow these steps:

- a) Select `/map_of_sets`.
- b) Click **POST** and enter the relevant information in the **Value** fields.

Learn more about the parameters to create a reference map of sets:

The following table provides information about the parameters that are required to create a reference map of sets:

<i>Table 43. Parameters - Reference Map of Sets</i>					
Parameter	Type	Value	Data Type	MIME Type	Sample
element_type	query	(required)	String	text/plain	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	query	(required)	String	text/plain	String
fields	query	(optional)	String	text/plain	field_one (field_two, field_three), field_four
key_label	query	(optional)	String	text/plain	String
time_to_live	query	(optional)	String	text/plain	String
timeout_type	query	(optional)	String	text/plain	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	query	(optional)	String	text/plain	String

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
7. To create a new reference table or map of maps, follow these steps:

- a) Click `/tables`.
- b) Click **POST** and enter the relevant information in the **Value** fields.

Learn more about the parameters to create a reference table or a map of maps:

The following table provides information about the parameters that are required to create a reference table or a map of maps:

<i>Table 44. Parameters - Reference Table</i>					
Parameter	Type	Value	Data Type	MIME Type	Sample
element_type	query	(required)	String	text/plain	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	query	(required)	String	text/plain	String
fields	query	(optional)	String	text/plain	field_one (field_two, field_three), field_four

Table 44. Parameters - Reference Table (continued)					
Parameter	Type	Value	Data Type	MIME Type	Sample
key_name_types	query	(optional)	Array	application/json	[{ "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>", "key_name": "String" }]
outer_key_label	query	(optional)	String	text/plain	String
time_to_live	query	(optional)	String	text/plain	String
timeout_type	query	(optional)	String	text/plain	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

c) Click **Try It Out!** to finish creating the reference data collection and to view the results.

Related concepts

[Reference sets overview](#)

Examples for using reference data collections

These examples show how you can use reference data collections to track and store data that you want to use in QRadar searches, filters, rule test conditions, and rule responses.

Tracking expired user accounts

Use reference data collections to identify stale data, such as expired user accounts, in your IBM Security QRadar environment.

About this task

By default, reference data remains in QRadar until it is removed. However, when you create a reference data collection, you can configure QRadar to remove the data after a specified period of time.

When the data element expires, QRadar automatically deletes the value from the reference data collection and triggers an event to track the expiry.

Procedure

1. Create a reference set to keep track of the time since a user last logged in.
 - a) Set the **Time to Live of elements** to represent the period of time after which an unused user account is considered expired.
 - b) Select the **Since last seen** button.
2. Create a custom event rule to add login data, such as the **username**, to the reference set.

Note: QRadar tracks the **Date Last Seen** for each data element. If no data is added for a particular user within the time-to-live period, the reference set element expires, and a **Reference Data Expiry** event is triggered. The event contains the reference set name and the username that is expired.

3. Use the **Log Activity** tab to track the **Reference Data Expiry** events.

What to do next

Use the reference set data in searches, filters, rule test conditions, and rule responses.

Related tasks

[Adding, editing, and deleting reference sets](#)

Integrate dynamic data from external sources

Large enterprise organizations can use reference data collections to share information about their IT assets with the security teams that manage the IBM Security QRadar deployment.

For example, the Information Technology (IT) team maintains an asset management database that includes information about all the network assets. Some of the information, such as the IP addresses for the web servers, changes frequently.

Once a week, the IT team exports the list of IP addresses for all of the web servers that are deployed in the network and provides the list to the security team. The security team imports the list into a reference set, which can then be used in rules, searches, and reports to provide more context to the events and flows that are processed by QRadar.

Chapter 9. User information source configuration

Configure your IBM Security QRadar system to collect user and group information from Identity and Access Management endpoints.

QRadar uses the information that is collected from the endpoints to enrich the user information that is associated with the traffic and events that occur on your network.

Related concepts

[Capabilities in your IBM Security QRadar product](#)

User information source overview

You can configure a user information source to enable user information collection from an Identity and Access Management endpoint.

An Identity and Access Management endpoint is a product that collects and manages electronic user identities, group memberships, and access permissions. These endpoints are called user information sources.

Use the following utilities to configure and manage user information sources:

- **Tivoli Directory Integrator**- You must install and configure a Tivoli® Directory Integrator on a non-IBM Security QRadar host.
- **UISConfigUtil.sh** - Use this utility to create, retrieve, update, or delete user information sources. You can use user information sources to integrate IBM Security QRadar SIEM using a Tivoli Directory Integrator server.
- **GetUserInfo.sh** - Use this utility to collect user information from a user information source and store the information in a reference data collection. You can use this utility to collect user information on demand or on a schedule.

User information sources

A user information source is a configurable component that enables communication with an endpoint to retrieve user and group information.

IBM Security QRadar systems support the following user information sources:

Table 45. Supported information sources	
Information Source	Information that is collected
Microsoft Windows Active Directory (AD), version 2008 - Microsoft Windows AD is a directory service that authenticates and authorizes all users and computers that use your Windows network.	<ul style="list-style-type: none">• full_name• user_name• user_principal_name• family_name• given_name• account_is_disabled• account_is_locked• password_is_expired• password_can_not_be_changed• no_password_expired• password_does_not_expire

Table 45. Supported information sources (continued)

Information Source	Information that is collected
IBM Security Access Manager (ISAM), version 7.0 - ISAM is an authentication and authorization solution for corporate web, client/server, and existing applications. For more information, see your IBM Security Access Manager (ISAM) documentation.	<ul style="list-style-type: none"> • name_in_rgy • first-name • last-name • account_valid • password_valid
IBM Security Identity Manager (ISIM), version 6.0 - ISIM provides the software and services to deploy policy-based provisioning solutions. This product automates the process of provisioning employees, contractors, and IBM Business Partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise. For more information, see your IBM Security Integration Manager (ISIM) documentation.	<ul style="list-style-type: none"> • Full name • DN

Reference data collections for user information

This topic provides information about how reference data collections store data collected from user information sources.

When IBM Security QRadar SIEM collects information from a user information source, it automatically creates a reference data collection to store the information. The name of the reference data collection is derived from the user information source group name. For example, a reference data collection that is collected from Microsoft Windows AD might be named Domain Admins.

The reference data collection type is a Map of Maps. In a Reference Map of Maps, data is stored in records that map one key to another key, which is then mapped to a single value.

For example:

- #
- # Domain Admins
- # key1, key2, data
- smith_j, Full Name, John Smith
- smith_j, account_is_disabled, 0
- smith_j, account_is_locked, 0
- smith_j, account_is_locked, 1
- smith_j, password_does_not_expire, 1

For more information about reference data collections, see the *Reference Data Collections Technical Note*.

Integration workflow example

After user and group information is collected and stored in a reference data collection, there are many ways in which you can use the data in IBM Security QRadar SIEM.

You can create meaningful reports and alerts that characterize user adherence to your company's security policies.

Consider the following example:

To ensure activities that are performed by privileged ISIM users comply with your security policies, you can complete the following tasks:

Create a log source to collect and parse audit data for each ISIM server from which the logs are collected. For more information about how to create a log source, see the *Managing Log Sources Guide*.

1. Create a user information source for the ISIM server and collect ISIM Administrators user group information. This step creates a reference data collection that is called ISIM Administrators. See [“Creating a user information source”](#) on page 157.
2. Configure a building block to test for events in which the source IP address is the ISIM server and the user name is listed in the ISIM administrator reference data collection. For more information about building blocks, see the *User Guide* for your product.
3. Create an event search that uses the custom building block as a filter. For more information about event searches, see the *IBM Security QRadar User Guide* for your product.
4. Create a custom report that uses the custom event search to generate daily reports on the audit activity of the privileged ISIM users. These generated reports indicate whether any ISIM administrator activity breaches your security policy. For more information about reports, see the *IBM Security QRadar User Guide* for your product.

Note: If you want to collect application security logs, you must create a Device Support Module (DSM). For more information, see the *IBM Security QRadar DSM Configuration Guide*.

User information source configuration and management task overview

To initially integrate user information sources, you must perform the following tasks:

1. Configure a Tivoli Directory Integrator server. See [“Configuring the Tivoli Directory Integrator Server”](#) on page 155.
2. Create and manage user information sources. See [“Creating and managing user information source”](#) on page 157.
3. Collect user information. See [“Collecting user information”](#) on page 160.

Configuring the Tivoli Directory Integrator Server

For IBM Security QRadar to integrate with user information sources, you must install and configure a Tivoli Directory Integrator on a non-QRadar host.

About this task

No configuration is required on your QRadar system; however, you must access your Console to obtain the QRadarIAM_TDI.zip file. Then, install and configure a Tivoli Directory Integrator server on a separate host. Create and import a self-signed certificate.

When you extract the QRadarIAM_TDI.zip file on the Tivoli Directory Integrator server, the TDI directory is automatically created. The TDI directory includes the following files:

- QRadarIAM.sh, which is the TDI start up script for Linux
- QRadarIAM.bat, which is the TDI start up script for Microsoft Windows
- QRadarIAM.xml, which is the TDI xml script and must be stored in the same location as the QRadarIAM.properties file
- QRadarIAM.properties, which is the properties file for TDI xml script

When you install Tivoli Directory Integrator, you must configure a name for the Solutions directory. This task requires you to access the Solutions directory. Therefore, in the task steps, *<solution_directory>* refers to the name that you gave to the directory.

The following parameters are used to create and import certificates:

Table 46. Certification configuration parameters

Parameter	Description
<server_ip_address>	Defines the IP address of the Tivoli Directory Integrator server.
<days_valid>	Defines the number of days that the certificate is valid.
<keystore_file>	Defines the name of the keystore file.
-storepass <password>	Defines the password for keystore.
-keypass <password>	Defines the password for the private/public key pair.
<alias>	Defines the alias for an exported certificate.
<certificate_file>	Defines the file name of the certificate.

Procedure

1. Install Tivoli Directory Integrator on a non-QRadar host. For more information on how to install and configure Tivoli Directory Integrator, see your Tivoli Directory Integrator (TDI) documentation.
2. Using SSH, log in to your IBM Security QRadar Console as the root user.
 - a) User name: root
 - b) Password: <password>
3. Copy the QRadarIAM_TDI.zip file to the Tivoli Directory Integrator server.
4. On the Tivoli Directory Integrator server, extract the QRadarIAM_TDI.zip file in the Solutions directory.
5. Configure your Tivoli Directory Integrator server to integrate with QRadar.
 - a) Open the Tivoli Directory Integrator <solution_directory>/solution.properties file.
 - b) Uncomment the com.ibm.di.server.autoload property. If this property is already uncommented, note the value of the property.
 - c) Choose one of the following options:
 - Change directories to the autoload.tdi directory, which contains the com.ibm.di.server.autoload property by default.
 - Create an autoload.tdi directory in the <solution_directory> to store the com.ibm.di.server.autoload property.
 - d) Move the TDI/QRadarIAM.xml and TDI/QRadarIAM.property files from the Tivoli Directory Integrator directory to <solution_directory>/autoload.tdi directory or the directory you created in the previous step.
 - e) Move the QradarIAM.bat and QradarIAM.sh scripts from the Tivoli Directory Integrator directory to the location from which you want to start the Tivoli Directory Integrator.
6. Create and import the self-signed certificate into the Tivoli Directory Integrator truststore.
 - a) To generate a keystore and a private/public key pair, type the following command:
 - keytool -genkey -dname cn=<server_ip_address> -validity <days_valid> -keystore <keystore_file> -storepass <password> -keypass <password>
 - For example, keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret
 - b) To export the certificate from the keystore, type the following command:
 - keytool -export -alias <alias> -file <certificate_file> -keystore <keystore_file> -storepass <password>

- For example, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`
- c) To import the primary certificate back into the keystore as the self-signed CA certificate, type the following command:
- `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>`
 - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
- d) Copy the certificate file to the `/opt/qradar/conf/trusted_certificates` on the QRadar Console.
7. Import the CA certificate into the Tivoli Directory Integrator truststore.
- a) To import the CA certificate into the keystore as the self-signed CA certificate, type the following command:
- `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>`
 - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
- b) Copy the CA certificate file to the `/opt/qradar/conf/trusted_certificates` on the QRadar Console.
8. Edit the `<solution_directory>/solution.properties` file to uncomment and configure the following properties:
- `javax.net.ssl.trustStore=<keystore_file>`
 - `{protect}-javax.net.ssl.trustStorePassword=<password>`
 - `javax.net.ssl.keyStore=<keystore_file>`
 - `{protect}-javax.net.ssl.keyStorePassword=<password>`
- Note:** The default unmodified password might be displayed in the following format: `{enc1}EyHbak`. Enter the password as plain text. The password encrypts the first time that you start Tivoli Directory Integrator.
9. Start Tivoli Directory Integrator.

Creating and managing user information source

Use the `UISConfigUtil` utility to create, retrieve, update, or delete user information sources.

Creating a user information source

Use the `UISConfigUtil` utility to create a user information source.

Before you begin

Before you create a user information source, you must install and configure your Tivoli Directory Integrator server. For more information, see [“Configuring the Tivoli Directory Integrator Server” on page 155](#).

About this task

When you create a user information source, you must identify the property values required to configure the user information source. The following table describes the supported property values:

Table 47. Supported user interface property values

Property	Description
tdiserver	Defines the host name of the Tivoli Directory Integrator server.
tdiport	Defines the listening port for the HTTP connector on the Tivoli Directory Integrator server.
hostname	Defines the host name of the user information source host.
port	Defines the listening port for the Identity and Access Management registry on the user information host.
username	Defines the user name that IBM Security QRadar SIEM and use to authenticate to the Identity and Access Management registry.
password	Defines the password that is required to authenticate to the Identity and Access Management registry.
searchbase	Defines the base DN. Note: All users that are referenced in all groups must be found in a search from the searchbase.
search filter	Defines the search filter that is required to filter the groups that are retrieved from the Identity and Access Management registry.

Procedure

- Using SSH, log in to your IBM Security QRadar Console as the root user.
 - User name: root
 - Password: <password>
- To add a user information source, type the following command: `UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2...,proprn=valuen]`

Where:

- <name> Is the name of the user information source you want to add.
- <AD|ISAM|ISIM|ISFIM> Indicates the user information source type.
- [-d description] Is a description of the user information source. This parameter is optional.
- [-p prop1=value1,prop2=value2,...,proprn=valuen] Identifies the property values required for the user information source. For more information about the supported parameters, see [“Creating a user information source” on page 157](#).

For example:

- ```
/UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p
"tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,
hostname=vmibm7094.ottawa.ibm.com,port=389,
username=cn=root,password=password,\"searchbase=ou=org,DC=COM\",\\
\"searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem)
(objectClass=erSystemUser))\""
```

## Retrieving user information sources

Use the UISConfigUtil utility to retrieve user information sources.

### Procedure

1. Using SSH, log in to your IBM Security QRadar Console as the root user.
  - a) User name: root
  - b) Password: <password>
2. Choose one of the following options:
  - a) Type the following command to retrieve all user information sources: `UISConfigUtil.sh get <name>`
  - b) Type the following command to retrieve a specific user information source: `UISConfigUtil.sh get <name>`

Where <name> is the name of the user information source you want to retrieve.

For example:

```
[root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"
```

## Editing a user information source

Use the UISConfigUtil utility to edit a user information source.

### Procedure

1. Using SSH, log in to your IBM Security QRadar Console as the root user.
  - a) User name: root
  - b) Password: <password>
2. Type the following command to edit a user information source: `UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2,...,propn=valuen]`

Where:

- <name> Is the name of the user information source you want to edit.
- <AD|ISAM|ISIM|ISFIM> Indicates the user information source type. To update this parameter, type a new value.
- [-d description] Is a description of the user information source. This parameter is optional. To update this parameter, type a new description.
- [-p prop1=value1,prop2=value2,...,propn=valuen] Identifies the property values required for the user information source. To update this parameter, type new properties. For more information about the supported parameters, see [“Creating a user information source” on page 157](#).

For example:

```
./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p "searchbase=DC=local"
```

## Deleting a user information source

Use the UISConfigUtil utility to delete a user information source.

### Procedure

1. Using SSH, log in to your IBM Security QRadar Console as the root user.
  - a) User name: root

- b) Password: <password>
- 2. Type the following command to delete a user information source:

```
UISConfigUtil.sh delete <name>
```

Where <name> is the name of the user information source you want to delete.

#### **What to do next**

The collected user information is stored in a reference data collection in the IBM Security QRadar database. If no reference data collection exists, a new reference data collection is created. If a reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see [Reference data collections](#).

## **Collecting user information**

---

Use the GetUserInfo utility to collect user information from the user information sources and store the data in a reference data collection.

#### **About this task**

Use this task to collect user information on demand. If you want to create automatic user information collection on a schedule, create a cron job entry. For more information about cron jobs, see your Linux documentation.

#### **Procedure**

1. Using SSH, log in to your IBM Security QRadar Console as the root user.
  - a) User name: root
  - b) <password>
2. Type the following command to collect user information on demand:

```
GetUserInfo.sh <UISName>
```

Where <UISName> is the name of the user information source you want to collect information from.

#### **What to do next**

The collected user information is stored in a reference data collection on the database. If no reference data collection exists, a new reference data collection is created. If a reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see [“Reference data collections for user information” on page 154](#).

---

## Chapter 10. IBM X-Force integration

IBM X-Force security experts use a series of international data centers to collect tens of thousands of malware samples, analyze web pages and URLs, and run analysis to categorize potentially malicious IP addresses and URLs. IBM X-Force Exchange is the platform for sharing this data, which can be used in IBM Security QRadar.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

### X-Force Threat Intelligence feed

You can integrate IBM X-Force Exchange data into IBM Security QRadar to help your organization stay ahead of emerging threats by identifying and remediating undesirable activity in your environment before it threatens the stability of your network.

For example, you can identify and prioritize these types of incidents:

- A series of attempted logins for a dynamic range of IP addresses
- An anonymous proxy connection to a Business Partner portal
- A connection between an internal endpoint and a known botnet command and control
- Communication between an endpoint and a known malware distribution site

**Note:** IBM X-Force integration allows you to use the X-Force Threat Intelligence data in QRadar correlation rules and AQL queries. Access to the IBM X-Force Exchange REST API is not included.

### Enabling the X-Force Threat Intelligence feed

You must enable the X-Force Threat Intelligence feed before you can use the enhanced content that is installed with the IBM Security Threat Content application.

#### About this task

QRadar downloads approximately 30 MB of IP reputation data per day when you enable the X-Force Threat Intelligence feed.

#### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Select **Yes** in the **Enable X-Force Threat Intelligence Feed** field.

#### What to do next

Deploy the system setting changes to receive the data from the X-Force servers. For more information, see [Deploying changes](#).

### Updating X-Force data in a proxy server

IBM Security QRadar uses a reverse proxy lookup through an Apache server to collect data directly from IBM Security X-Force Threat Intelligence servers on the Internet.

#### About this task

All QRadar appliances in a deployment contact the Apache server to send cached requests. After the data is received by the IBM Security QRadar Console, the result is cached and replayed for all other managed hosts that make a request for new IP reputation data.

If a proxy is configured in your network, you must update the configuration to receive the X-Force data.

**Restriction:** NTLM authentication is not supported.

### Procedure

1. Use SSH to log in to the QRadar Console.
2. Open the `/etc/httpd/conf.d/ssl.conf` file in a text editor.
3. Add the following lines before `</VirtualHost>`:  

```
ProxyRemote https://license.xforce-security.com/ http://PROXY_IP:PROXY_PORT
ProxyRemote https://update.xforce-security.com/ http://PROXY_IP:PROXY_PORT
```
4. Update the IP address and port of the corporate proxy server to allow an anonymous connection to the X-Force security servers.
5. Save the changes to the `ssl.conf` file.
6. Restart the Apache server by typing the following command:

```
apachectl restart
```

Restarting the Apache server on the QRadar Console logs out all users and the managed hosts might produce error messages. Restart the Apache server during scheduled maintenance windows.

## Preventing X-Force data from downloading data locally

QRadar downloads approximately 30 MB of IP reputation data per day. To stop QRadar from downloading the X-Force data to your local system, disable the X-Force Threat Intelligence feed.


### Before you begin

Before you disable the X-Force feed, ensure that the X-Force rules are disabled, and that you are not using X-Force functions in saved searches.

### About this task

After the X-Force Threat Intelligence feed is disabled, the X-Force content is still visible in QRadar, but you cannot use the X-Force rules or add X-Force functions to AQL searches.

### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Select **No** in the **Enable X-Force Threat Intelligence Feed** field.

### What to do next

Deploy the system setting changes to receive the data from the X-Force servers. For more information, see [Deploying changes](#).

## IBM Security Threat Content app

The **IBM Security Threat Content** app on the IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub>) contains rules, building blocks, and custom properties that are intended for use with X-Force feed data.

The X-Force data includes a list of potentially malicious IP addresses and URLs with a corresponding threat score. You use the X-Force rules to automatically flag any security event or network activity data that involves the addresses, and to prioritize the incidents before you begin to investigate them.

The following list shows examples of the types of incidents that you can identify using the X-Force rules:

- when the *[source IP/destinationIP/anyIP]* is part of any of the following *[remote network locations]*
- when *[this host property]* is categorized by X-Force as *[Anonymization Servers/Botnet C&C/DynamicIPs/Malware/ScanningIPs/Spam]* with confidence value *[equal to] [this amount]*
- when *[this URL property]* is categorized by X-Force as *[Gambling/Auctions/Job Search/Alcohol/Social Networking/Dating]*

QRadar downloads approximately 30 MB of IP reputation data per day when you enable the X-Force Threat Intelligence feed for use with the **IBM Security Threat Content** application.

## Installing the IBM Security Threat Content application

The IBM Security Threat Content application contains IBM Security QRadar content, such as rules, building blocks, and custom properties, that are designed specifically for use with X-Force data. The enhanced content can help you to identify and to remediate undesirable activity in your environment before it threatens the stability of your network.

### Before you begin

Download the IBM Security Threat Content application from the IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub>).

### About this task

To use X-Force data in QRadar rules, offenses, and events, you must configure IBM Security QRadar to automatically load data from the X-Force servers to your QRadar appliance.

To load X-Force data locally, enable the X-Force Threat Intelligence feed in the system settings. If new information is available when X-Force starts, the IP address reputation or URL database is updated. These updates are merged into their own databases and the content is replicated from the QRadar Console to all managed hosts in the deployment.

The X-Force rules are visible in the product even if the **IBM Security Threat Content** application is later uninstalled.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Extensions Management**.
3. Upload the **IBM Security Threat Content** application to the QRadar console by following these steps:
  - a) Click **Add**.
  - b) Click **Browse** to find the extension.
  - c) Click **Install immediately** to install the extension without viewing the contents.
  - d) Click **Add**.
4. To view the contents of the extension, select it from the extensions list and click **More Details**.
5. To install the extension, follow these steps:
  - a) Select the extension from the list and click **Install**.
  - b) If the extension does not include a digital signature, or it is signed but the signature is not associated with the IBM Security certificate authority (CA), you must confirm that you still want to install it. Click **Install** to proceed with the installation.
  - c) Review the changes that the installation makes to the system.
  - d) Select **Overwrite** or **Keep existing data** to specify how to handle existing content items.
  - e) Click **Install**.
  - f) Review the installation summary and click **OK**.

The rules appear under the **Threats** group in the **Rules List** window. They must be enabled before they are used.

## What to do next

Enable the X-Force Threat Intelligence feed so that you can use the X-Force rules or add X-Force functions to AQL searches. For more information, see [“Enabling the X-Force Threat Intelligence feed” on page 161](#).

## IBM X-Force Exchange plug-in for QRadar

---

IBM X-Force Exchange is a sharing platform for threat intelligence that is used by security analysts, network security specialists, and security operations center teams.

The IBM X-Force Exchange (XFE) plug-in provides the option to search the information on the IBM X-Force Exchange website for IP addresses, URLs, CVEs, and web applications that are found in QRadar. For example, you can right-click a URL from a QRadar event to see what data the X-Force Exchange contains about the URL.

You can also use the right-click lookup option to submit IP addresses or URL data from QRadar searches, offenses, and rules to a public or private collection. The collection stores the information in one place as you use the data for more research.

Collections also contain a section that serves as a wiki-style notepad, where you can add comments or any free text that is relevant. You can use the collection to save X-Force reports, text comments, or any other content. An X-Force report has both a version of the report from the time that it was saved and a link to the current version of the report.

## Installing the IBM X-Force Exchange plug-in

Install the IBM X-Force Exchange plug-in on your QRadar Console so that you have right-click functionality to access data in IBM X-Force Exchange.

### Before you begin

This procedure requires a web server restart from the **Admin** tab to load the plug-in after the RPM is installed. Restarting the web server logs out all QRadar users, so it is advised that you install this plug-in during scheduled maintenance.


### About this task

If your QRadar system is version 7.2.3 or later, the plug-in is already installed. Administrators can verify that the plug-in is installed by right-clicking on any IP address in QRadar, and selecting **More Options > Plugin options**. If the IBM X-Force Exchange lookup is displayed, then the plug-in is installed.

### Procedure

1. Download the X-Force Exchange right-click plug-in from [IBM Fix Central](https://ibm.biz/BdX4BW) (<https://ibm.biz/BdX4BW>).
  - a) Copy the RPM file to the QRadar Console.
  - b) Type the following command to install the plug-in: `rpm -Uvh RightClick-XFE-7.2.<version>.x86_64.rpm`

2. Log in to the QRadar Console as an admin user.

3. On the navigation menu () , click **Admin**.

4. Select **Advanced > Restart Web Server**.

After the web server restarts, the X-Force right-click plug-in is enabled for IP addresses in QRadar for URL fields in the **Log Activity** tab.

5. Log in to the pop-up window for the X-Force Exchange website by using your IBMid, or continue as a guest.

Guest users are not able to use all features on the X-Force Exchange website.

6. Close the browser window after the initial login to the IBM X-Force Exchange website.



---

## Chapter 11. Managing authorized services

You can configure authorized services on the **Admin** tab to authenticate an API call for your IBM Security QRadar deployment.

The QRadar RESTful API uses authorized services to authenticate API calls to the QRadar Console. You can add or revoke an authorized service at any time. For more information about the RESTful API, see the *IBM Security QRadar API Guide*.

The **Manage Authorized Services** window provides the following information:

| Table 48. Parameters for authorized services |                                                                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Parameter                                    | Description                                                                                                     |
| <b>Service Name</b>                          | The name of the authorized service.                                                                             |
| <b>Authorized By</b>                         | The name of the user or administrator that authorized the addition of the service.                              |
| <b>Authentication Token</b>                  | The token that is associated with this authorized service.                                                      |
| <b>User Role</b>                             | The user role that is associated with this authorized service.                                                  |
| <b>Security Profile</b>                      | The security profile that is associated with this authorized service.                                           |
| <b>Created</b>                               | The date that this authorized service was created.                                                              |
| <b>Expires</b>                               | The date and time that the authorized service expires. By default, the authorized service is valid for 30 days. |

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

## Viewing authorized services

The **Authorized Services** window displays a list of authorized services, from which you can copy the token for the service.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Authorized Services**.
3. From the **Manage Authorized Services** window, select the appropriate authorized service.


The token is displayed in the **Selected Token** field in the top bar. You can copy the token into your vendor software to authenticate with IBM Security QRadar.

---

## Adding an authorized service

Use the **Add Authorized Service** window to add a new authorized service.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Authorized Services**.
3. Click **Add Authorized Service**.
4. In the **Service Name** field, type a name for this authorized service. The name can be up to 255 characters in length.
5. From the **User Role** list, select the user role that you want to assign to this authorized service. The user roles that are assigned to an authorized service determine the functions that this service can access on the IBM Security QRadar user interface.
6. From the **Security Profile** list, select the security profile that you want to assign to this authorized service. The security profile determines the networks and log sources that this service can access on the QRadar user interface.
7. In the **Expiry Date** list, type or select a date that you want this service to expire. If an expiry date is not required, select **No Expiry**.
8. Click **Create Service**.


The confirmation message contains a token field that you must copy into your vendor software to authenticate with QRadar.

## Revoking authorized services

---

Use the **Add Authorized Service** window to revoke an authorized service.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Authorized Services**.
3. From the **Manage Authorized Services** window, select the service that you want to revoke.
4. Click **Revoke Authorization**.

---

## Chapter 12. Backup and recovery

You can back up and recover IBM Security QRadar configuration information and data by using the backup and recovery feature to back up your event and flow data. However, you must restore event and flow data manually.

There are two types of backups: configuration backups and data backups. For more information, see [“Restoring data” on page 177](#).

By default, QRadar creates a backup archive of your configuration information each day at midnight. Configuration backups are stored only on the QRadar Console and include the following information:

- Application configuration
- Assets
- Certificates
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Flow sources
- Flow and event searches
- Groups
- Index management information
- License key information
- Log sources
- Offenses
- Reference set elements
- Store and Forward schedules
- User and user roles information
- Vulnerability data (if IBM Security QRadar Vulnerability Manager is installed)

Data backups include the following information:

- Audit log information
- Event data
- Flow data
- Report data
- Indexes

Each managed host in your deployment, including the QRadar Console, creates and stores the daily data backup files locally. A data backup archive is created for each day and includes the event and flow data from the previous day. The size of the daily data backup depends on the amount of event data received from the previous day.

The default location of the backup files is the `/store/backup/` directory. Your system might include a `/store/backup` mount from an external SAN or NAS service. External services provide long term, offline retention of data, which is commonly required for compliancy regulations, such as PCI.

The data backup does not include application data. To configure and manage backups for application data, see [“Backing up and restoring app data” on page 180](#).

### **Related concepts**

[Capabilities in your IBM Security QRadar product](#)

## Related tasks

[Restoring data](#)

## Backup QRadar configurations and data

By default, IBM Security QRadar 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. You can customize this nightly backup and create an on-demand configuration backup, as required.

### Scheduling nightly backup

Use the **Backup Recovery Configuration** window to configure a night scheduled backup process.

#### About this task

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

**Note:** The nightly backup starts running at midnight in the timezone where the QRadar Console is installed. If QRadar automatic updates are scheduled to run at the same time, the performance of QRadar might be impacted.


The **Backup Recovery Configuration** window provides the following parameters:

| Table 49. Backup Recovery Configuration parameters |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| General Backup Configuration                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Backup Repository Path                             | <p>Type the location where you want to store your backup file. The default location is <code>/store/backup</code>. This path must exist before the backup process is initiated. If this path does not exist, the backup process stops.</p> <p>If you modify this path, make sure that the new path is valid on every system in your deployment.</p> <ul style="list-style-type: none"><li>Active data is stored on the <code>/store</code> directory. If you have both active data and backup archives that are stored in the same directory, data storage capacity might easily be reached and your scheduled backups might fail. Specify a storage location on another system or copy your backup archives to another system after the backup process is complete for added security. You can use a Network File System (NFS) storage solution in your QRadar deployment. For more information about using NFS, see the <i>Offboard Storage Guide</i>.</li></ul> |

Table 49. Backup Recovery Configuration parameters (continued)

| Parameter                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Retention Period (days)                               | <p>Type or select the length of time, in days, that you want to store backup files. The default is 2 days.</p> <p>This period affects only backup files that are generated as a result of a scheduled process. On-demand backups or imported backup files are not affected by this value.</p>                                                                                                                                                                                                                                                                                                                                                              |
| Nightly Backup Schedule                                      | Select a backup option.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Select the managed hosts you would like to run data backups: | <p>This option is only displayed if you select the <b>Configuration and Data Backups</b> option.</p> <p>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 any managed hosts in your deployment, the managed hosts are listed below the Console and each managed host includes a check box.</p> <p>Select the check box for the managed hosts you want to run data backups on.</p> <p>For each host (Console or managed hosts), you can optionally clear the data items that you want to exclude from the backup archive.</p> |
| 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                                              | <p>From this list box, select the level of importance that you want the system to place on the configuration backup process, which is compared to other processes.</p> <p>A priority of medium or high have a greater impact on system performance.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |
| 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                                              | <p>From the list, select the level of importance you want the system to place on the data backup process, which is compared to other processes.</p> <p>A priority of medium or high have a greater impact on system performance.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. On the toolbar, click **Configure**.
4. On the **Backup Recovery Configuration** window, customize your nightly backup.
5. Click **Save**.
6. Close the **Backup Archives** window.
7. On the **Admin** tab, click **Deploy Changes**.


## Creating an on-demand configuration backup archive

If you must back up 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.

### About this task

You initiate an on-demand backup archive during a period when IBM Security QRadar has low processing load, such as after normal office hours. During the backup process, system performance is affected.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. From the toolbar, click **On Demand Backup**.
4. Enter values for the following parameters:

| Option             | Description                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | Type a unique name that you want to assign to this backup archive. The name can be up to 100 alphanumeric characters in length. The name can contain following characters: underscore (_), dash (-), or period (.). |
| <b>Description</b> | Type a description for this configuration backup archive. The description can be up to 255 characters in length.                                                                                                    |

5. Click **Run Backup**.

You can start a new backup or restore processes only after the on-demand backup is complete. You can monitor the backup archive process in the **Backup Archives** window.

## Creating an email notification for a failed backup

To receive a notification by email about a backup failure on the IBM Security QRadar Console or a QRadar Event Processor, create a rule that is based on the system notification message.

### Before you begin

You must configure an email server to distribute system notifications in QRadar. For more information, see [“Configuring your local firewall” on page 63](#).

### About this task

If a backup fails, you see one of the following backup failure system notifications:

- Backup: requires more disk space
- Backup: last Backup exceeded execution threshold
- Backup: unable to execute request

## Procedure

1. Click the **Offenses** tab.
2. In the **Offenses** pane, click **Rules**.
3. Click **Actions > New Event Rule**.
4. In the **Rule Wizard**, check the **Skip this page when running this rules wizard** box and click **Next**.
5. In the filter box, type the following search query:  
when the event QID is one of the following QIDs

### Learn more about tests:

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All Export as Building Block

when the event QID

+ when the event QID is one of the following QIDs

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply on events which are detected by the Local system

and when the event QID is one of the following QIDs

Please select any groups you would like this rule to be a member of:

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

<< Back Next >> Finish Cancel

Figure 8. Rule Wizard event test

6. Click the green add (+) icon.
7. In the **Rule** pane, click the **QIDs** link.
8. In the **QID/Name** field, type Backup :
9. Select the following QIDs and click **Add +**:
  - **Backup requires more disk space**
  - **Backup: last backup exceeded execution threshold**
  - **Backup unable to execute request**

## Learn more about QIDs:

Browse or Search for QIDs below. Select the desired QIDs and click 'Add'

High-Level Category: Any

Low-Level Category: Any

Log Source Type: Any

QID/Name: Backup:

Search

Matching QIDs

| QID      | Name ▲                                   | Description           | Severity |
|----------|------------------------------------------|-----------------------|----------|
| 38750033 | Backup requires more disk space          | Backup: Not enou...   | 7        |
| 38750032 | Backup unable to clean up bad backup     | Backup: Unable to ... | 6        |
| 38750031 | Backup unable to clean up db             | Backup: Unable to ... | 6        |
| 38750035 | Backup unable to execute request         | Backup: Unable to ... | 6        |
| 38750030 | Backup unable to init recovery engine    | Backup: Unable to ... | 6        |
| 38750034 | Backup unable to release running lock    | Backup: Unable To...  | 3        |
| 38750059 | Backup: last backup exceeded executio... | Backup: The last s... | 6        |
| 38750036 | File Location Incorrect                  | Backup: File Locat... | 5        |

Add +

Selected Items

(38750033) Backup requires more disk space  
(38750035) Backup unable to execute request  
(38750059) Backup: last backup exceeded execution threshold

Remove -

Submit Cancel

Figure 9. Rule Wizard QIDs

- Click **Submit**.
- In the **Rule** pane, type the following name for your rule test and click **Next**:  
Backup Failure
- In the **Rule Response** section, check the **Email** box and type the email addresses you want to notify.

## Manage existing backup archives

Use the **Backup and Recovery** icon on the **Admin** tab to view and manage all successful backup archives.

### Importing a backup archive


Importing a backup archive is useful if you want to restore a backup archive that was created on another IBM Security QRadar host.

#### About this task

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



## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. In the **Upload Archive** field, click **Browse**.
4. Locate and select the archive file that you want to upload. The archive file must include a .tgz extension.
5. Click **Open**.
6. Click **Upload**.


## Deleting a backup archive

To delete a backup archive file, the backup archive file and the Host Context component must be located on the same system. The system must also be in communication with the IBM Security QRadar Console and no other backup can be in progress.

### About this task

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.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. In the **Existing Backups** section, select the archive that you want to delete.
4. Click **Delete**.

## Restore QRadar configurations and data

---

Restoring a backup archive is useful if you want to restore previously archived configuration files, offense data, and asset data on your IBM Security QRadar system.

Before you restore a backup archive, note the following considerations:

- You can restore only a backup archive that is created within the same release of software and its software update level. For example, if you are running QRadar V7.3.1 p1, make sure that the backup archive is created on the QRadar V7.3.1 p1 Console.
- The restore process restores only your configuration information, offense data, and asset data. For more information, see [“Restoring data” on page 177](#).
- If the backup archive originated on a NATed Console system, you can restore only that backup archive on a NATed system.

To complete the restore process, perform the following steps on the Console:

1. Back up existing files and database tables.
2. Shut down Tomcat.
3. Shut down all system processes.
4. Extract all files from the backup archive and restore them to disk.
5. Restore the database tables.
6. Restart all system processes.
7. Restart Tomcat.

**Important:** If you are restoring WinCollect data, you must install the WinCollect SFS that matches the version of WinCollect in your backup before you restore the configuration. For more information, see [WinCollect files are not restored during configuration restore](#).

### Related tasks

[Restoring data](#)

## Restoring a backup archive

You can restore a backup archive. Restoring a backup archive is useful if you have a system hardware failure or you want to store a backup archive on a replacement appliance.

### About this task

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

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

The following parameters are available in the **Restore a Backup** window:

| Table 50. <b>Restore a Backup</b> parameters |                                                                                                                                                                                                                                  |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                    | Description                                                                                                                                                                                                                      |
| <b>Name</b>                                  | The name of the backup archive.                                                                                                                                                                                                  |
| <b>Description</b>                           | The description, if any, of the backup archive.                                                                                                                                                                                  |
| <b>Type</b>                                  | The type of backup. Only configuration backups can be restored, therefore, this parameter displays <b>config</b> .                                                                                                               |
| <b>Select All Configuration Items</b>        | When selected, this option indicates that all configuration items are included in the restoration of the backup archive.                                                                                                         |
| <b>Restore Configuration</b>                 | Lists the configuration items to include in the restoration of the backup archive. To remove items, you can clear the check boxes for each item you want to remove or clear the <b>Select All Configuration Items</b> check box. |
| <b>Select All Data Items</b>                 | When selected, this option indicates that all data items are included in the restoration of the backup archive.                                                                                                                  |
| <b>Restore Data</b>                          | 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.                    |

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. Select the archive that you want to restore.

4. Click **Restore**.
5. On the **Restore a Backup** window, configure the parameters.  
**Note:** By selecting the **Installed Applications Configuration** check box, you restore the install app configurations only. Extension configurations are not restored. Select the **Deployment Configuration** check box if you want to restore extension configurations.
6. Click **Restore**.
7. Click **OK**.
8. Click **OK**.
9. Choose one of the following options:
  - If the user interface was closed during the restore process, open a web browser and log in to IBM Security QRadar.
  - If the user interface was not closed, the login window is displayed. Log in to QRadar.
10. Follow the instructions on the status window.

### What to do next

After you verify that your data is restored to your system, ensure that your DSMs, vulnerability assessment (VA) scanners, and log source protocols are also restored.

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 a backup, the secondary host displays a failed status on the **System and License Management** window.

## Restoring a backup archive created on a different QRadar system

Each backup archive includes the IP address information of the system from which the backup archive was created. When you restore a backup archive from a different IBM Security QRadar system, the IP address of the backup archive and the system that you are restoring are mismatched. You can correct the mismatched IP addresses.

### About this task

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

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

You must stop the iptables service on each managed host in your deployment. The Iptables service is a Linux based firewall.

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


| Table 51. Restore a Backup (Managed Host Accessibility) parameters |                                        |
|--------------------------------------------------------------------|----------------------------------------|
| Parameter                                                          | Description                            |
| Host Name                                                          | The managed host name.                 |
| IP Address                                                         | The IP address of the managed host.    |
| Access Status                                                      | The access status to the managed host. |

The Restore a Backup window provides the following parameters:

Table 52. **Restore a Backup** parameters

| Parameter                             | Description                                                                                                                                                                                                                                                         |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                           | The name of the backup archive.                                                                                                                                                                                                                                     |
| <b>Description</b>                    | The description, if any, of the backup archive.                                                                                                                                                                                                                     |
| <b>Type</b>                           | The type of backup. Only configuration backups can be restored, therefore, this parameter displays <b>config</b> .                                                                                                                                                  |
| <b>Select All Configuration Items</b> | 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.                                              |
| <b>Restore Configuration</b>          | 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 <b>Select All Configuration Items</b> check box. |
| <b>Select All Data Items</b>          | 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.                                                               |
| <b>Restore Data</b>                   | 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.                                                       |

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. Select the archive that you want to restore, and click **Restore**.
4. On the **Restore a Backup** window, configure the parameters and then click **Restore**.
5. Stop the IP tables:
  - a) Using SSH, log in to the managed host as the root user.
  - b) Type the command, **service iptables stop**.
  - c) Repeat for all managed hosts in your deployment.
6. On the **Restore a Backup** window, click **Test Hosts Access**.
7. After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**.
8. If the **Access Status** column indicates a status of **No Access** for a host, stop iptables again, and then click **Test Host Access** again to attempt a connection.
9. On the **Restore a Backup** window, configure the parameters.

**Note:** By selecting the **Installed Applications Configuration** check box, you restore the install app configurations only. Extension configurations are not restored. Select the **Deployment Configuration** check box if you want to restore extension configurations.

10. Click **Restore**.
11. Click **OK**.
12. Click **OK** to log in.
13. Choose one of the following options:
  - If the user interface was closed during the restore process, open a web browser and log in to QRadar.
  - If the user interface was not closed, the login window is displayed. Log in to QRadar.
14. View the results of the restore process and follow the instructions to resolve any errors.
15. Refresh your web browser window.
16. From the **Admin** tab, select **Advanced > Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

### What to do next

After you verify that your data is restored to your system, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

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 a backup, the secondary host displays a failed status on the **System and License Management** window.

## Restoring data

You can restore the data on your IBM Security QRadar Console and managed hosts from backup files. The data portion of the backup files includes information such as source and destination IP address information, asset data, event category information, vulnerability data, flow data, and event data.

Each managed host in your deployment, including the QRadar Console, creates all backup files in the `/store/backup/` directory. Your system might include a `/store/backup` mount from an external SAN or NAS service. External services provide long term, offline retention of data, which is commonly required for compliance regulations, such as PCI.

**Restriction:** You must restore the configuration backup before you restore the data backup.

### Before you begin

Ensure that the following conditions are met:

- If you are restoring data on a new QRadar Console, the configuration backup is restored.
- You know the location of the managed host where the data is backed up.
- If your deployment includes a separate mount point for that volume, the `/store` or `/store/ariel` directory has sufficient space for the data that you want to recover.
- You know the date and time for the data that you want to recover.

### Procedure

1. Use SSH to log in to IBM Security QRadar as the root user.
2. Go to the `/store/backup` directory.
3. To list the backup files, type the following command:

```
ls -l
```
4. If backup files are listed, go to the root directory by typing the following command:

```
cd /
```

**Important:** The restored files must be in the /store directory. If you type cd instead of cd /, the files are restored to the /root/store directory.

5. To extract the backup files to their original directory, type the following command:

```
tar -zxpvPf /store/backup/backup.name.hostname_hostID .target date.backup
type.timestamp.tgz
```

| Table 53. Description of file name variables |                                                                                                            |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------|
| File name variable                           | Description                                                                                                |
| <i>name</i>                                  | The name of the backup.                                                                                    |
| <i>hostname_hostID</i>                       | The name of the QRadar system that hosts the backup file followed by the identifier for the QRadar system. |
| <i>target date</i>                           | The date that the backup file was created. The format of the target date is <i>day_month_year</i> .        |
| <i>backup type</i>                           | The options are data or config.                                                                            |
| <i>timestamp</i>                             | The time that the backup file was created.                                                                 |

## Results

Daily backup of data captures all data on each host. If you want to restore data on a managed host that contains only event or flow data, only that data is restored to that host. If you want to maintain the restored data, increase your data retention settings to prevent the nightly disk maintenance routines from deleting your restored data.

## Related concepts

### Backup and recovery

You can back up and recover IBM Security QRadar configuration information and data by using the backup and recovery feature to back up your event and flow data. However, you must restore event and flow data manually.

### Restore QRadar configurations and data

Restoring a backup archive is useful if you want to restore previously archived configuration files, offense data, and asset data on your IBM Security QRadar system.

## Verifying restored data

Verify that your data is restored correctly in IBM Security QRadar.

## Procedure

1. To verify that the files are restored, review the contents of one of the restored directories by typing the following command:

```
cd /store/ariel/flows/payloads/<yyyy/mm/dd>
```

```
cd /store/ariel/events/payloads/<yyyy/mm/dd>
```

You can view the restored directories that are created for each hour of the day. If directories are missing, data might not be captured for that time period.

2. Verify that the restored data is available.
  - a) Log in to the QRadar interface.
  - b) Click the **Log Activity** or **Network Activity** tab.
  - c) Select **Edit Search** from the **Search** list on the toolbar.

- d) In the **Time Range** pane of the **Search** window, select **Specific Interval**.
- e) Select the time range of the data you restored and then click **Filter**.
- f) View the results to verify the restored data.
- g) If your restored data is not available in the QRadar interface, verify that data is restored in the correct location and file permissions are correctly configured.

Restored files must be in the `/store` directory. If you typed `cd` instead of `cd /` when you extracted the restored files, check the `/root/store` directory for the restored files. If you did not change directories before you extracted the restored files, check the `/store/backup/store` directory for the restored files.

Typically, files are restored with the original permissions. However, if the files are owned by the root user account, issues might occur. If the files are owned by the root user account, change the permissions by using the **chown** and **chmod** commands.

### What to do next

After you verified that your data is restored, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, and log source protocols.

### WinCollect files are not restored during a configuration restore.

When you complete a configuration restore and some WinCollect files are not restored, it might be because the installation ISO contains a previous version of WinCollect.

The QRadar ISO contains a built-in version of WinCollect. When you restore by using that ISO, it deploys the WinCollect files that are stored in that ISO, rather than the files from your backup.

To remedy this issue, you must install the WinCollect SFS that matches the version of WinCollect in your backup before you restore the configuration. Perform the following tasks in this order:

1. Perform QRadar backup.
2. Bring new hardware online and deploy the ISO.
3. Install the WinCollect SFS that matches the version of WinCollect in your backup on the Console.
4. Restore the configuration backup.

The appropriate WinCollect files are deployed with the configuration restore.

## Backup and restore applications

---

IBM Security QRadar provides a way to backup and restore application configurations separate from the application data.

Application configurations are backed up as part of the nightly configuration backup. The configuration backup includes apps that are installed on the QRadar Console and on an App node. You can restore the application configuration by selecting the **Installed Applications Configuration** option when you restore a backup.

Application data is backed up separate from the application configuration by using an easy-to-use script that runs nightly. You can also use the script to restore the app data, and to configure backup times and data retention periods for app data.

### Related concepts

[App Nodes](#)

## Backing up and restoring apps

Use the IBM Security QRadar **Backup and Recovery** window on the **Admin** tab to back up and restore apps.

### About this task

You can back up your apps by creating a configuration backup. A configuration backup does not backup your app's data.

If an App Node is attached to your QRadar Console, the App Node's configuration is backed up as part of the console's Deployment Configuration. You cannot restore an App Node on a QRadar Console with a different IP address than the App Node was initially configured with.

By default, apps are restored to console unless an App Node is present. If QRadar cannot restore apps to your App Node, it attempts to back restore them to the QRadar Console. The number of App Node apps that can be restored onto the console is constrained by the amount of memory that is available on the QRadar Console. Apps that are defined as **node\_only** in their application manifest file cannot be restored to the QRadar Console.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Backup and Recovery**.
3. Select an existing backup in the **Backup and Recovery** window and click **Restore**.
4. Ensure that the **Installed Applications Configuration** check box is selected, and click **Restore**.

**Note:** By selecting the **Installed Applications Configuration** check box, you restore the install app configurations only. Extension configurations are not restored. Select the **Deployment Configuration** check box if you want to restore extension configurations.

## Backing up and restoring app data

Use the `marathon-volume-backup.py` script to back up and recover app data.

### About this task

A configuration backup that you do on the **Backup and Recovery** window does not back up your apps' data. The `/usr/local/bin/marathon-volume-backup.py` script runs nightly at 2:30 AM, and backs up each installed application's `/store` mounted volume. By default, data is retained for 7 days.

Use the script to do the following tasks:

- Back up data manually for installed apps.
- List all installed app data backups on the system.
- Restore data for installed apps.
- Run the retention process and set the retention period for backups.

This script is on both the QRadar Console and App Node if one is installed. After an App Node is added, data backups, data restores, and retentions are no longer carried out on the QRadar Console. You must use the script on the App Node.

### Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Go to the `/usr/local/bin/` directory.
  - Use the following commands to back up app data:
    - To back up data manually for all apps, enter the command:  
`./marathon-volume-backup.py backup -p /qapp`



- To back up data manually for a specific app, enter the command:  
`./marathon-volume-backup.py backup -p /qapp-<app_id>`  
 Where **<app\_id>** is the ID of the app whose data you want to back up.  
 The `marathon-volume-backup.py` script runs nightly at 2:30 AM local time to back up all installed apps. Backup archives are stored in the `/store/backup/marathon` folder.
- To view all data backups for installed apps, enter the following command:  
`./marathon-volume-backup.py ls`  
 This command outputs all backup archives that are stored in the `/store/backup/marathon` folder.
- To restore a backup archive, enter the following command:  
`./marathon-volume-backup.py restore -i <backup name>`  
 Use the **ls** command to find the name of a backup archive
- By default, all backup archives are retained for one week. The retention process runs nightly at 2:30 AM local time with the backup.
  - To perform retention manually, and use the default retention period, enter the following command:  
`./marathon-volume-backup.py retention`
  - You can also set the retention period manually by adding **-t** (time - defaults to 1) and **-p** (period - defaults to 0) switches.  
 The **-p** switch accepts three values: 0 for a week, 1 for a day, and 2 for an hour.  
 For example, to set the retention period for a back up to 3 weeks, enter the following command:  
`./marathon-volume-backup.py retention -t 3 -p 0`
- If you want to change the retention time that is used by the nightly timer, add flags to the retention command found in the following systemd service file:  
`/etc/systemd/system/framework-apps-data-backup.service`  
 For example, to change the retention period that is used by the nightly retention process to 5 days, locate the following line:  
`ExecStart=/usr/local/bin/marathon-volume-backup.py retention`  
 Replace it with:  
`ExecStart=/usr/local/bin/marathon-volume-backup.py retention -t 5 -p 1`  
 Save your changes, and run the `systemctl daemon-reload` command for systemd to apply the changes.



---

## Chapter 13. Flow sources

For IBM Security QRadar appliances, QRadar automatically adds default flow sources for the physical ports on the appliance, and includes a default NetFlow flow source.

If QRadar is installed on your own hardware, QRadar attempts to automatically detect and add default flow sources for any physical devices, such as a network interface card (NIC). When you assign a IBM Security QRadar QFlow Collector, QRadar includes a default NetFlow flow source.

Flow sources are classed as either internal or external:

### Internal flow sources

Includes any additional hardware that is 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 might include the following sources:

- Network 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. When external flow data is received by the same QRadar QFlow Collector, a distinct name helps to distinguish external flow source data from each other.

External flow sources might include the following sources:

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Flowlog file

QRadar SIEM can forward external flows source data by using the spoofing or non-spoofing method:

### Spoofing

Resends the inbound data that is received from flow sources to a secondary destination. To ensure that flow source data is sent to a secondary destination, configure the **Monitoring Interface** parameter in the flow source configuration to the port on which data is 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. As a result, QRadar QFlow Collector can 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 as Any. The QRadar QFlow Collector opens the listening port, which is the port that is 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.

## Types of flow sources

---

IBM Security QRadar QFlow Collector can process flows from multiple sources, which are categorized as either internal or external sources.

### Internal flow sources

Sources that include packet data by connecting to a SPAN port or a network TAP are considered internal sources. These sources provide raw packet data to a monitoring port on the Flow Collector, which converts the packet details into flow records.

QRadar does not keep the entire packet payload. Instead, it captures a snapshot of the flow, referred to as the *payload* or *content capture*, which includes packets from the beginning of the communication.

Flow collection from internal sources normally requires a dedicated Flow Collector.

### External flow sources

QRadar also supports external flow sources, such as routers that send NetFlow, sFlow, J-Flow, and Packeteer data.

External sources do not require as much CPU utilization to process so you can send them directly to a Flow Processor. In this configuration, you may have a dedicated flow collector and a flow processor, both receiving and creating flow data.

## NetFlow

NetFlow is a proprietary accounting technology that is developed by Cisco Systems. NetFlow monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is 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 IBM Security QRadar to accept NDEs and thus become a NetFlow collector. QRadar supports NetFlow versions 1, 5, 7, and 9. For more information on NetFlow, see the [Cisco web site](http://www.cisco.com) (<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. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for NetFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the IBM Security QRadar QFlow Collector configuration, you must also update your firewall access configuration.
- Make sure that the appropriate ports are configured for your QRadar QFlow Collector.

If you are using NetFlow version 9, make sure that 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. IPFIX monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is 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 intrusion protection system (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 IBM Security QRadar to accept NDEs and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After an NDE is sent from the IPFIX forwarding device, the IPFIX record might be purged.

To configure QRadar to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows by using the same process.

Your QRadar system might include a default NetFlow flow source; therefore, you might not be required to configure a NetFlow flow source. To confirm that your system includes a default NetFlow flow source, on the **Admin** tab, select **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 do the following tasks:

- Ensure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the IBM Security QRadar QFlow Collector configuration, you must also update your firewall access configuration.
- Ensure that the appropriate ports are configured for your QRadar QFlow Collector.
- Ensure that the IPFIX template from the IPFIX source includes the following IANA-listed Information Elements:
  - protocolIdentifier (4)
  - sourceIPv4Address (8)
  - destinationIPv4Address (12)
  - sourceTransportPort (7)
  - destinationTransportPort (11)
  - octetDeltaCount (1) or postOctetDeltaCount (23)
  - packetDeltaCount (2) or postPacketDeltaCount (24)
  - tcpControlBits (6) (TCP flows only)
  - flowStartSeconds (150) or flowStartMilliseconds (152) or flowStartDeltaMicroseconds (158)
  - flowEndSeconds (151) or flowEndMilliseconds (153) or flowEndDeltaMicroseconds (159)

## sFlow

sFlow is a multi-vendor and user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously.

A sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. IBM Security QRadar supports sFlow versions 2, 4, and 5. sFlow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information, see the [sFlow website](http://www.sflow.org) (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. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for sFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that the appropriate ports are configured for your QRadar VFlow 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, might not represent all network traffic. For more information on J-Flow, see the [Juniper Networks website](http://www.juniper.net) (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 IBM Security 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 IBM Security QRadar.

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. Inaccurate presentations of both traffic volumes and bidirectional flows might occur.

To configure Packeteer as an external flow source, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that you configure Packeteer devices to export flow detail records and configure the IBM Security QRadar QFlow Collector as the destination for the data export.
- Make sure that 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 more information, see the *Mapping Packeteer Applications into QRadar Technical Note*.

## Flowlog file

A Flowlog file is generated from the IBM Security QRadar flow logs.

## Napatech interface


If you installed a Napatech Network Adapter on your IBM Security QRadar system, the **Napatech Interface** option is displayed as a configurable packet-based flow source on the QRadar user interface. The Napatech Network Adapter provides next-generation programmable and intelligent network adapter for your network. For more information, see the Napatech documentation.

## Adding or editing a flow source

---

Use the **Flow Source** window to add a flow source.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Do one of the following actions:
  - To add a flow source, click **Add**.
  - To edit a flow source, select the flow source and click **Edit**.
4. To create this flow source from an existing flow source, select the **Build from existing flow source** check box, and select a flow source from the **Use as Template** list.
5. Enter the name for the **Flow Source Name**.

**Tip:** If the external flow source is also a physical device, use the device name as the flow source name. If the flow source is not a physical device, use a recognizable name.

For example, if you want to use IPFIX traffic, enter **ipf1**. If you want to use NetFlow traffic, enter **nf1**.
6. Select a flow source from the **Flow Source Type** list and configure the properties.
  - If you select the **Flowlog File** option, ensure that you configure the location of the Flowlog file for the **Source File Path** parameter.
  - If you select the **JFlow**, **Netflow**, **Packeteer FDR**, or **sFlow** options in the **Flow Source Type** parameter, ensure that you configure an available port for the **Monitoring Port** parameter.

The default port for the first NetFlow flow source that is configured in your network 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.
  - If you select the **Napatech Interface** option, enter the **Flow Interface** that you want to assign to the flow source.

**Restriction:** The **Napatech Interface** option is displayed only if you installed the Napatech Network Adapter on your system.
  - If you select the **Network Interface** option, for the **Flow Interface**, configure only one log source for each Ethernet interface.

**Restriction:** You cannot send different flow types to the same port.
7. If traffic on your network is configured to take alternate paths for inbound and outbound traffic, select the **Enable Asymmetric Flows** check box.
8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.

## Forwarding packets to QRadar Packet Capture

---

You can monitor network traffic by sending raw data packets to a IBM Security QRadar QFlow Collector 1310 appliance. The QRadar QFlow Collector uses a dedicated Napatech monitoring card to copy incoming packets from one port on the card to a second port that connects to a IBM Security QRadar Packet Capture appliance.

If you already have a QRadar QFlow Collector 1310 with a 10G Napatech network card, you can mirror the traffic to QRadar Packet Capture.

As shown in the following diagram, if you already have a QRadar QFlow Collector 1310 with a 10G Napatech network card, you can mirror the traffic to QRadar Packet Capture.

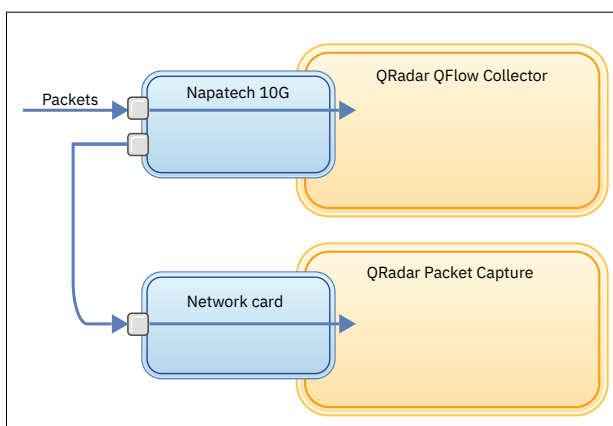


Figure 10. Packet data forwarding from a QRadar QFlow Collector to QRadar Packet Capture by using the Napatech card

## Before you begin

Ensure that the following hardware is set up in your environment:

- You attached the cable to port 1 of the Napatech card on the QRadar QFlow Collector 1310 appliance.
- You attached the cable that is connected to port 2 of the Napatech card, which is the forwarding port, to the QRadar Packet Capture appliance.
- Verify layer 2 connectivity by checking for link lights on both appliances.

## Procedure

1. Using SSH from your IBM Security QRadar Console, log in to QRadar QFlow Collector as the root user. On the QRadar QFlow Collector appliance, edit the following file.

`/opt/qradar/init/apply_tunings`

- a) Locate the following line, which is around line 137.

```

apply_multithread_qflow_changes()
{
 APPLIANCEID=`$NVABIN/myver -a`
 if ["$APPLIANCEID" == "1310"]; then
 MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -
d'-' -f2)
 if ["$MODELNUM" == "9220"]; then..

```

- b) In the AppendToConf lines that follow the code in the preceding step, add these lines:

```

AppendToConf SV_NAPATECH_FORWARD YES
AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDEST "0:1"

```

These statements enable packet forwarding, and forward packets from port 0 to port 1.

- c) Ensure that *multithreading* is enabled, by verifying that the following line is in the `/opt/qradar/conf/nva.conf` file.

```
MULTI_THREAD_ON=YES
```

2. Run the `apply_tunings` script to update the configuration files on the QRadar QFlow Collector, by typing the following command:
 

```
./apply_tunings restart
```
3. Restart IBM Security QRadar services by typing the following command:
 

```
systemctl restart hostcontext
```
4. Optional: Verify that your Napatech card is receiving and transmitting data.



- a) To verify that the Napatech card is receiving data, type the following command:  

```
/opt/napatech/bin/Statistics -dec -interactive
```

The "RX" packet and byte statistics increment if the card is receiving data.
  - b) To verify that the Napatech card is transmitting data, type the following command:  

```
/opt/napatech/bin/Statistics -dec -interactive
```

The "TX" statistics increment if the card is transmitting data.
  5. Optional: Verify that your QRadar Packet Capture is receiving packets from your QRadar QFlow Collector appliance.
    - a) Using SSH from your QRadar Console, log in to your QRadar Packet Capture appliance as root on port 4477.
    - b) Verify that the QRadar Packet Capture appliance is receiving packets by typing the following command:  

```
watch -d cat /var/www/html/statisdata/int0.txt
```


The `int0.txt` file updates as data flows into your QRadar Packet Capture appliance.
- For more information about packet capture, see the *IBM Security QRadar Packet Capture Quick Reference Guide*.

## Enabling and disabling a flow source

---

Using the **Flow Source** window, you can enable or disable a flow source.

### Procedure


1. On the navigation menu () , click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Select the flow source that you want to enable or disable, and click **Enable/Disable**.
4. On the **Admin** tab, click **Deploy Changes**.

## Deleting a Flow Source

---

Use the **Flow Source** window to delete a flow source.

### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Select the flow source that you want to delete, and click **Delete**.
4. On the **Admin** tab, click **Deploy Changes**.

## Flow source aliases

---

A flow source alias uses a virtual name to identify external flows that are sent to the same port on a flow collector. For example, the IBM Security QRadar QFlow Collector can have a single NetFlow flow source that is listening on port 2055, and can have multiple NetFlow sources sending to the same QRadar QFlow Collector. By using flow source aliases, you can identify the different NetFlow sources based by their IP addresses.

When QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, the QRadar QFlow Collector attempts a reverse DNS lookup. The lookup is used to determine the host name of the device.

You can configure the QRadar QFlow Collector to automatically create flow source aliases. When the QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, it does 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 the information to all QRadar QFlow Collector components in your deployment. If the lookup fails, QRadar creates a default alias for the flow source based on the flow source name and the source IP address. For example, the default alias might appear as **default\_NetFlow\_172.16.10.139**.

## Adding a flow source alias

Use the **Flow Source Alias** window to add a flow source alias.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Source Aliases**.
3. Do one of the following actions:
  - To add a flow source alias, click **Add** and enter the values for the parameters.
  - To edit an existing flow source alias, select the flow source alias, click **Edit**, and update the parameters.
4. Click **Save**.
5. On the **Admin** tab, click **Deploy Changes**.

**Note:** If you rename a flow source alias, you must use the original name to perform a historical search.

## Deleting a flow source alias

Use the **Flow Source Alias** window to delete a flow source alias.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Source Aliases**.
3. Select the flow source alias that you want to delete, and then click **Delete**.
4. On the **Admin** tab menu, click **Deploy Changes**.

## Chapter 14. Remote networks and services configuration

Use remote network and service groups to represent traffic activity on your network for a specific profile. Remote networks groups display user traffic that originates from named remote networks.

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 preexisting properties to suit your environment.

If you move an existing object to another group, the object name moves from the existing group to the newly selected group. However, when the configuration changes are deployed, the object data that is stored in the database is lost and the object ceases to function. To resolve this issue, create a new view and re-create the object that exists with another group.

You can group remote networks and services for use in the custom rules engine, flow, and event searches. You can also group networks and services in IBM Security QRadar Risk Manager, if it is available.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

## Default remote network groups

IBM Security QRadar includes default remote network groups.

The following table describes the default remote network groups.

| Table 54. Default remote network groups |                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group                                   | Description                                                                                                                                                                                                                                                                                                                                          |
| BOT                                     | <p>Specifies traffic that originates from BOT applications.</p> <p>For more information, see <a href="http://rules.emergingthreats.net/blockrules/emerging-botcc.rules">Botnet Command and Control drop rules on the Emerging Threats website (http://rules.emergingthreats.net/blockrules/emerging-botcc.rules)</a></p>                             |
| Bogon                                   | <p>Specifies traffic that originates from unassigned IP addresses.</p> <p>For more information, see <a href="http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt">bogon reference on the Team CYMRU website (http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt)</a>.</p>                                                       |
| HostileNets                             | <p>Specifies traffic that originates from known hostile networks.</p> <p>HostileNets has a set of 20 (rank 1 - 20 inclusive) configurable CIDR ranges.</p> <p>For more information, see <a href="http://www.dshield.org/ipsascii.html?limit=20">HostileNets reference on the DShield website (http://www.dshield.org/ipsascii.html?limit=20)</a></p> |

| Table 54. Default remote network groups (continued) |                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group                                               | Description                                                                                                                                                                                                                                                                     |
| Neighbours                                          | Specifies traffic that originates from nearby networks that your organization has network peering agreements with.<br><br>This group is blank by default. You must configure this group to classify traffic that originates from neighboring networks.                          |
| Smurfs                                              | Specifies traffic that originates from smurf attacks.<br><br>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.<br><br>A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.                                                                                                                       |
| TrustedNetworks                                     | Specifies traffic from trusted networks, including business partners that have remote access to your critical applications and services.<br><br>This group is blank by default.<br><br>You must configure this group to classify traffic that originates from trusted networks. |
| Watchlists                                          | Classifies traffic that originates from networks that you want to monitor.<br><br>This group is blank by default.                                                                                                                                                               |

Groups and objects that include superflows are only for informational purposes and cannot be edited. Groups and objects that include bogons are configured by the automatic update function.

**Note:** You can use reference sets instead of remote networks to provide some of this functionality. Although you can assign a confidence level to an IP value in a reference table, reference sets are used only with single IPs and cannot be used with CIDR ranges. You can use a CIDR value after a remote network update, but not with weight or confidence levels.

#### Related concepts

“Types of reference data collections” on page 139

There are different types of reference data collections, and each type can handle different levels of data complexity. The most common types are reference sets and reference maps.

## Default remote service groups

IBM Security QRadar includes the default remote service groups.

The following table describes the default remote service groups.

Table 55. Default remote network groups

| Parameter          | Description                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------|
| IRC_Servers        | Specifies traffic that originates from addresses commonly known as chat servers.                              |
| Online_Services    | Specifies traffic that originates from addresses commonly known online services that might involve data loss. |
| Porn               | Specifies traffic that originates from addresses commonly known to contain explicit pornographic material.    |
| Proxies            | Specifies traffic that originates from commonly known open proxy servers.                                     |
| Reserved_IP_Ranges | Specifies traffic that originates from reserved IP address ranges.                                            |
| Spam               | Specifies traffic that originates from addresses commonly known to produce SPAM or unwanted email.            |
| Spy_Adware         | Specifies traffic that originates from addresses commonly known to contain spyware or adware.                 |
| Superflows         | Specifies traffic that originates from addresses commonly known to produce superflows.                        |
| Warez              | Specifies traffic that originates from addresses commonly known to contain pirated software.                  |

## Guidelines for network resources

Given the complexities and network resources that are required for IBM Security QRadar SIEM in large structured networks, follow the suggested guidelines.

The following list describes some of the suggested practices that you can follow:


- 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, for standard system requirements, do not exceed more than 200 objects per group.  
More objects might impact your processing power when you investigate your traffic.

## Managing remote networks objects

After you create remote network groups, you can aggregate flow and event search results on remote network groups. You can also create rules that test for activity on remote network groups.

Use the **Remote Networks** window, you can add or edit a remote networks object.

### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Remote Networks and Services Configuration** section, click **Remote Networks and Services**.
3. To add a remote networks object, click **Add** and enter values for the parameters.
4. To edit a remote networks object, follow these steps:

- a) Double-click the group name.
- b) Select the profile and click the edit icon (✎) to edit the remote profile.
5. Click **Save**.
6. Click the previous icon (◀) to go back to the **Remote Networks and Services** window.
7. On the **Admin** tab, click **Deploy Changes**.

## Managing remote services objects

Remote services groups organize traffic that originates 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.

Use the **Remote Services** window to add or edit a remote services object.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Remote Networks and Services Configuration** section, click **Remote Networks and Services**.
3. To add a remote services object, click **Add** and enter the parameter values.
4. To edit a remote services object, click the group that you want displayed, click the **Edit** icon and change the values.
5. Click **Save**.
6. Click **Return**.
7. Close the **Remote Services** window.
8. On the **Admin** tab menu, click **Deploy Changes**.

## QID map overview

Use the IBM Security QRadar Identifier (QID) map utility to create, export, import, or modify user-defined QID map entries.

The QID map associates an event on an external device to a (QID).

See the following tasks for QID management:

- [“Creating a QID map entry” on page 195](#)
- [“Modifying a QID map entry” on page 196](#)
- [“Importing Qid map entries” on page 196](#)
- [“Exporting QID map entries” on page 197](#)

To run the utility, use the following syntax:

```
qidmap_cli.sh [-l|-c|-m|-i[-f <filename>]]-e[-f <filename>]]-d]
```

The following table describes the command-line options for the QID map utility.

| Table 56. QID map utility options |                                                  |
|-----------------------------------|--------------------------------------------------|
| Options                           | Description                                      |
| -l                                | Lists the low-level category.                    |
| -c                                | Creates a QID map entry                          |
| -m                                | Modifies an existing user-defined QID map entry. |

| Table 56. QID map utility options (continued) |                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Options                                       | Description                                                                                                      |
| -i                                            | Imports QID map entries.                                                                                         |
| -e                                            | Exports existing user-defined QID map entries.                                                                   |
| -f <filename>                                 | If you include the -i or -e option, specifies a file name to import or export QID map entries.                   |
| -d                                            | If you include the -i or -e option, specifies a delimiter for the import or export file. The default is a comma. |
| -h                                            | Displays the help options.                                                                                       |

## Creating a QID map entry

Create a IBM Security QRadar Identifier (QID) Map Entry to map an event of an external device to QID.

### Procedure

1. Using SSH, log in to QRadar as the root user.
2. To locate the low-level category for the QID map entry that you want to create, type the following command:

```
/opt/qradar/bin/qidmap_cli.sh -l
```

If you want to search for a particular low-level category, you can use the `grep` command to filter the results:

```
/opt/qradar/bin/qidmap_cli.sh -l | grep <text>
```

3. Type the following command:

```
qidmap_cli.sh -c --qname <name> --qdescription <description>
--severity <severity> --lowlevelcategoryid <ID>
```

The following table describes the command-line options for the QID map utility:

| Options                                   | Description                                                                                                                                                                                               |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-c</b>                                 | Creates a QID map entry.                                                                                                                                                                                  |
| <b>--qname &lt;name&gt;</b>               | The name that you want to associate with this QID map entry. The name can be up to 255 characters in length.<br><br>If you include spaces in the name, enclose the name value in double quotation marks.  |
| <b>--qdescription &lt;description&gt;</b> | The description for this QID map entry. The description can be up to 2048 characters in length.<br><br>If you include spaces in the description, enclose the description value in double quotation marks. |
| <b>--severity &lt;severity&gt;</b>        | The severity level that you want to assign to this QID map entry. The valid range is 1 - 10.                                                                                                              |
| <b>--lowlevelcategoryid &lt;ID&gt;</b>    | The low-level category ID you want to assign to this QID map entry.                                                                                                                                       |

## Modifying a QID map entry

Modify an existing user-defined IBM Security QRadar Identifier (QID) map entry.

### Procedure

1. Using SSH, log in to QRadar as the root user.
2. Type the following command:

```
qidmap_cli.sh -m --qid<QID> --qname <name> --qdescription <description>
--severity <severity>
```

The following table describes the command-line options for the QID map utility:

| Options                                   | Description                                                                                                                 |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>-m</b>                                 | Modifies an existing user-defined QID map entry.                                                                            |
| <b>--qid &lt;QID&gt;</b>                  | The QID that you want to modify.                                                                                            |
| <b>--qname &lt;name&gt;</b>               | The name that you want to associate with this QID map entry. The name can be up to 255 characters in length with no spaces. |
| <b>--qdescription &lt;description&gt;</b> | The description for this QID map entry. The description can be up to 2048 characters in length with no spaces.              |
| <b>--severity &lt;severity&gt;</b>        | The severity level that you want to assign to this QID map entry. The valid range is 0 - 10.                                |

## Importing Qid map entries

Using the IBM Security QRadar Identifier (QID) map utility, you can import QID map entries from a .txt file.

### Procedure

1. Create a .txt file that includes the user-defined QID map entries that you want to import. Ensure that each entry in the file is separated with a comma. Choose one of the following options:

- If you want to import a new list of user-defined QID map entries, create the file with the following format for each entry:

,<name>,<description>,<severity>,<category>

#### Example:

,buffer,buffer\_QID,7,18401 ,malware,malware\_misc,8,18403

- If you want to import an existing list of user-defined QID map entries, create the file with the following format for each entry:

<qid>,<name>,<description>,<severity>

**Example:** 2000002,buffer,buffer\_QID,7 2000001,malware,malware\_misc

The following table describes the command-line options of the QID utility.

| Options            | Description                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;qid&gt;</b> | The existing QID for the entry. This option is required if you want to import an existing exported list of QID entries. |



| Options                                   | Description                                                                                                                                                    |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | To import new QID entries, do not use this option. The QID map utility assigns an identifier (QID) for each entry in the file.                                 |
| <b>--qname &lt;name&gt;</b>               | The name that you want to associate with this QID map entry. The name can be up to 255 characters in length with no spaces.                                    |
| <b>--qdescription &lt;description&gt;</b> | The description for this QID map entry. The description can be up to 2048 characters in length with no spaces.                                                 |
| <b>--severity &lt;severity&gt;</b>        | The severity level that you want to assign to this QID map entry. The valid range is 0 - 10.                                                                   |
| <b>--lowlevelcategoryid &lt;ID&gt;</b>    | The low-level category ID that you want to assign to this QID map entry.<br><br>This option is only necessary if you want to import a new list of QID entries. |

2. Save and close the file.
3. Using SSH, log in to QRadar as the root user:
4. To import the QID map file, type the following command:

```
/opt/qradar/bin/qidmap_cli.sh -i -f <filename.txt>
```

The *<filename.txt>* option is the directory path and name of the file that contains the QID map entries. If any of the entries in the file cause an error, no entries in the file are enforced.

## Exporting QID map entries

View the mappings between the events of external devices and their unique identifiers by exporting your QID entries.

### About this task

For QID map entries that you created, use the QID map utility to export the entries to a .txt file.

For an entire QID map that includes the default system QID entries, use the **idlist.sh** command.

### Procedure

1. Using SSH, log in to IBM Security QRadar as the root user.
2. To export the QID map file of user-defined entries, type the following command:

```
/opt/qradar/bin/qidmap_cli.sh -e -f <filename.txt>
```

The *<filename.txt>* option is the directory path and name of the file that you want to contain your QID map entries.

3. To export the entire QID map, type the following command:

```
/opt/qradar/bin/idlist.sh -e qid > <filename.txt>
```

4. To determine the last modified date of your QID map, run an SQL query.  
For example, if a QID has the identification number 64250088, type the following SQL query to retrieve its last modified date:

```
psql -U qradar -c "select qid,to_timestamp(serial/1000) as date from qidmap_serial where qid = 64250088;"
```



## Chapter 15. Server discovery

The **Server Discovery** function uses the Asset Profile database to discover different server types that are based on port definitions. Then, you can select the servers to add to a server-type building block for rules.

The **Server Discovery** function is based on server-type building blocks. Ports are used to define the server type. Thus, the server-type building block works as a port-based filter when you search the Asset Profile database.

For more information about building blocks, see the *IBM Security QRadar User Guide*.

Use the **Server Discovery** function with IBM Security QRadar Vulnerability Manager to create exception rules for benign vulnerabilities. Reduce the number of vulnerabilities that you see for the following **Server Types**:

| Table 57. Server type vulnerabilities |                        |
|---------------------------------------|------------------------|
| Server Type                           | Vulnerability          |
| FTP Servers                           | FTP Server Present     |
| DNS Servers                           | DNS Server is Running  |
| Mail Servers                          | SMTP Server Detected   |
| Web Servers                           | Web Service is Running |

For more information about false positive vulnerabilities, see the *IBM Security QRadar Vulnerability Manager User Guide*.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

## Discovering servers

Use the **Assets** tab to discover servers on your network.

### Procedure

1. On the navigation menu (☰), click **Assets** to open the **Assets** tab.
2. On the **Assets** navigation menu, click **Server Discovery**.
3. From the **Server Type** list, select the server type that you want to discover.
4. Select one of the following options to determine the servers you want to discover:
  - To use the currently selected **Server Type** to search all servers in your deployment, select **All**.
  - To search servers in your deployment that were assigned to the currently selected **Server Type**, select **Assigned**.
  - To search servers in your deployment that are not assigned, select **Unassigned**.
5. To edit the standard server port list, click **Edit ports**.
6. From the **Network** list, select the network that you want to search.
7. Click **Discover Servers**.
8. In the **Matching Servers** table, select the check boxes of all servers you want to assign to the server role.
9. Click **Approve Selected Servers**.



---

## Chapter 16. Domain segmentation

Segmenting your network into different domains helps to ensure that relevant information is available only to those users that need it.

You can create security profiles to limit the information that is available to a group of users within that domain. Security profiles provide authorized users access to only the information that is required to complete their daily tasks. You modify only the security profile of the affected users, and not each user individually.

You can also use domains to manage overlapping IP address ranges. This method is helpful when you are using a shared IBM Security QRadar infrastructure to collect data from multiple networks. By creating domains that represent a particular address space on the network, multiple devices that are in separate domains can have the same IP address and still be treated as separate devices.

### **Related concepts**

[Capabilities in your IBM Security QRadar product](#)

---

## Overlapping IP addresses

An overlapping IP address is an IP address that is assigned to more than one device or logical unit, such as an event source type, on a network. Overlapping IP address ranges can cause significant problems for companies that merge networks after corporate acquisitions, or for Managed Security Service Providers (MSSPs) who are bringing on new clients.

IBM Security QRadar must be able to differentiate events and flows that come from different devices and that have the same IP address. If the same IP address is assigned to more than one event source, you can create domains to distinguish them.

For example, let's look at a situation where Company A acquires Company B and wants to use a shared instance of QRadar to monitor the new company's assets. The acquisition has a similar network structure that results in the same IP address being used for different log sources in each company. Log sources that have the same IP address cause problems with correlation, reporting, searching, and asset profiling.

To distinguish the origin of the events and flows that come in to QRadar from the log source, you can create two domains and assign each log source to a different domain. If required, you can also assign each event collector and flow collector to the same domain as the log source that sends events to them.

To view the incoming events by domain, create a search and include the domain information in the search results.

---

## Domain definition and tagging

Domains are defined based on IBM Security QRadar input sources. When events and flows come into QRadar, the domain definitions are evaluated and the events and flows are tagged with the domain information.

### **Specifying domains for events**

These are the ways to specify domains for events:

#### **Event collectors**

If an event collector is dedicated to a specific network segment or IP address range, you can flag that entire event collector as part of that domain.

All log sources that arrive at that event collector belong to the domain; therefore, any new auto-detected log sources are automatically added to the domain.

### **Log sources**

You can configure specific log sources to belong to a domain.

This method of tagging domains is an option for deployments in which an event collector can receive events from multiple domains.

### **Log source groups**

You can assign log source groups to a specific domain. This option allows broader control over the log source configuration.

Any new log sources that are added to the log source group automatically get the domain tagging that is associated with the log source group.

### **Custom properties**

You can apply custom properties to the log messages that come from a log source.

To determine which domain that specific log messages belong to, the value of the custom property is looked up against a mapping defined in the Domain Management editor.

This option is used for multi-address-range or multi-tenant log sources, such as file servers and document repositories.

### **Specifying domains for flows**

These are the ways to specify domains for flows:

#### **Flow collectors**

You can assign specific QFlow collectors to a domain.

All flow sources that arrive at that flow collector belong to the domain; therefore, any new auto-detected flow sources are automatically added to the domain.

#### **Flow sources**

You can designate specific flow sources to a domain.

This option is useful when a single QFlow collector is collecting flows from multiple network segments or routers that contain overlapping IP address ranges.

### **Specifying domains for scan results**

You can also assign vulnerability scanners to a specific domain so that scan results are properly flagged as belonging to that domain. A domain definition can consist of all QRadar input sources.

For information about assigning your network to preconfigured domains, see [“Network hierarchy” on page 69](#).

### **Precedence order for evaluating domain criteria**

When events and flows come into the QRadar system, the domain criteria is evaluated based on the granularity of the domain definition.

If the domain definition is based on an event, the incoming event is first checked for any custom properties that are mapped to the domain definition. If the result of a regular expression that is defined in a custom property does not match a domain mapping, the event is automatically assigned to the default domain.

If the event does not match the domain definition for custom properties, the following order of precedence is applied:

1. Log source
2. Log source group
3. Event Collector

If the domain is defined based on a flow, the following order of precedence is applied:

1. Flow source
2. Flow Collector

If a scanner has an associated domain, all assets that are discovered by the scanner are automatically assigned to the same domain as the scanner.

### Forwarding data to another QRadar system

Domain information is removed when data is forwarded to another QRadar system. Events and flows that contain domain information are automatically assigned to the default domain on the receiving QRadar system. To identify which events and flows are assigned to the default domain, you can create a custom search on the receiving system. You might want to reassign these events and flows to a user-defined domain.

## Creating domains

---

Use the **Domain Management** window to create domains based on IBM Security QRadar input sources.

### About this task

Use the following guidelines when you create domains:

- Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. Users who have limited domain access should not have administrative privileges because this privilege grants unlimited access to all domains.
- You can map the same custom property to two different domains, however the capture result must be different for each one.
- You cannot assign a log source, log source group, or event collector to two different domains. When a log source group is assigned to a domain, each of the mapped attributes is visible in the **Domain Management** window.

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes deployed.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Domain Management**.
3. To add a domain, click **Add** and type a unique name and description for the domain.  
**Tip:** You can check for unique names by typing the name in the **Input domain name** search box.
4. Depending on the domain criteria to be defined, click the appropriate tab.
  - To define the domain based on a custom property, log source group, log source, or event collector, click the **Events** tab.
  - To define the domain based on a flow source or flow collector, click the **Flows** tab.
  - To define the domain based on a scanner, including IBM Security QRadar Vulnerability Manager scanners, click the **Scanners** tab.
5. To assign a custom property to a domain, in the **Capture Result** box, type the text that matches the result of the regular expression (regex) filter.  
**Important:** You must select the **Optimize parsing for rules, reports, and searches** check box in the **Custom Event Properties** window to parse and store the custom event property. Domain segmentation will not occur if this option is not checked.
6. From the list, select the domain criteria and click **Add**.
7. After you add the source items to the domain, click **Create**.

### What to do next

Create security profiles to define which users have access to the domains. After you create the first domain in your environment, you must update the security profiles for all non-administrative users to specify the domain assignment. In domain-aware environments, non-administrative users whose security profile does not specify a domain assignment will not see any log activity or network activity.

Review the hierarchy configuration for your network, and assign existing IP addresses to the proper domains. For more information, see [“Network hierarchy”](#) on page 69.

## Domain privileges that are derived from security profiles

---

You can use security profiles to grant domain privileges and ensure that domain restrictions are respected throughout the entire IBM Security QRadar system. Security profiles also make it easier to manage privileges for a large group of users when your business requirements suddenly change.

Users can see only data within the domain boundaries that are set up for the security profiles that are assigned to them. Security profiles include domains as one of the first criteria that is evaluated to restrict access to the system. When a domain is assigned to a security profile, it takes priority over other security permissions. After domain restrictions are evaluated, individual security profiles are assessed to determine network and log permissions for that particular profile.

For example, a user is given privileges to Domain\_2 and access to network 10.0.0.0/8. That user can see only events, offenses, assets, and flows that come from Domain\_2 and contain an address from the 10.0.0.0/8 network.

As a QRadar administrator, you can see all domains and you can assign domains to non-administrative users. Do not assign administrative privileges to users whom you want to limit to a particular domain.

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

When you assign domains to a security profile, you can grant access to the following types of domains:

### User-defined domains

You can create domains that are based on input sources by using the Domain Management tool. For more information, see [Creating domains](#).

### Default domain

Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. The default domain contains system-wide events.

**Note:** Users who have access to the default domain can see system-wide events without restriction. Ensure that this access is acceptable before you assign default domain access to users. All administrators have access to the default domain.

Any log source that gets auto-discovered on a shared event collector (one that is not explicitly assigned to a domain), is auto-discovered on the default domain. These log sources require manual intervention. To identify these log sources, you must periodically run a search in the default domain that is grouped by log source.

### All domains

Users who are assigned to a security profile that has access to **All Domains** can see all active domains within the system, the default domain, and any domains that were previously deleted across the entire system. They can also see all domains that are created in the future.

If you delete a domain, it cannot be assigned to a security profile. If the user has the **All domains** assignment, or if the domain was assigned to the user before it was deleted, the deleted domain is returned in historical search results for events, flows, assets, and offenses. You can't filter by deleted domains when you run a search.

Administrative users can see which domains are assigned to the security profiles on the **Summary** tab in the **Domain Management** window.



## Rule modifications in domain-aware environments

Rules can be viewed, modified, or disabled by any user who has both the **Maintain Custom Rules** and **View Custom Rules** permissions, regardless of which domain that user belongs to.

**Important:** When you add the **Log Activity** capability to a user role, the **Maintain Custom Rules** and **View Custom Rules** permissions are automatically granted. Users who have these permissions have access to all log data for all domains, and they can edit rules in all domains, even if their security profile settings have domain-level restrictions. To prevent domain users from being able to access log data and modify rules in other domains, edit the user role and remove the **Maintain Custom Rules** and **View Custom Rules** permissions.

## Domain-aware searches

You can use domains as search criteria in custom searches. Your security profile controls which domains you can search against.

System-wide events and events that are not assigned to a user-defined domain are automatically assigned to the default domain. Administrators, or users who have a security profile that provides access to the default domain, can create a custom search to see all events that are not assigned to a user-defined domain.

The default domain administrator can share a saved search with other domain users. When the domain user runs that saved search, the results are limited to their domain.

## Domain-specific rules and offenses

---

A rule can work in the context of a single domain or in the context of all domains. Domain-aware rules provide the option of including the **And Domain Is** test.

You can restrict a rule so that it is applied only to events that are happening within a specified domain. An event that has a domain tag that is different from the domain that is set on the rule does not trigger an event response.

In an IBM Security QRadar system that does not have user-defined domains, a rule creates an offense and keeps contributing to it each time the rule fires. In a domain-aware environment, a rule creates a new offense each time the rule is triggered in the context of a different domain.

Rules that work in the context of all domains are referred to as system-wide rules. To create a system-wide rule that tests conditions across the entire system, select **Any Domain** in the domain list for the **And Domain Is** test. An **Any Domain** rule creates an **Any Domain** offense.

### Single-domain rule

If the rule is a stateful rule, the states are maintained separately for each domain. The rule is triggered separately for each domain. When the rule is triggered, offenses are created separately for each domain that is involved and the offenses are tagged with those domains.

### Single-domain offense

The offense is tagged with the corresponding domain name. It can contain only events that are tagged with that domain.

### System-wide rule

If the rule is a stateful rule, a single state is maintained for the whole system and domain tags are ignored. When the rule runs, it creates or contributes to a single system-wide offense.

### System-wide offense

The offense is tagged with **Any Domain**. It contains only events that are tagged with all domains.

The following table provides examples of domain-aware rules. The examples use a system that has three domains that are defined: Domain\_A, Domain\_B, and Domain\_C.

The rule examples in the following table may not be applicable in your QRadar environment. For example, rules that use flows and offenses are not applicable in IBM QRadar Log Manager.

Table 58. Domain-aware rules

| Domain text                                                                                                                                   | Explanation                                                                                                                                                                                                                                                                        | Rule response                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain is one of: Domain_A</b>                                                                                                             | Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.                                                                                                                                                                           | Creates or contributes to an offense that is tagged with Domain_A.                                                                                                                                                                                                                                                       |
| <b>domain is one of: Domain_A</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b>           | Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.                                                                                                                                                                           | Creates or contributes to an offense that is tagged with Domain_A. A single state, an HTTP flow counter, gets maintained for Domain_A.                                                                                                                                                                                   |
| <b>domain is one of: Domain_A, Domain_B</b>                                                                                                   | Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C.<br><br>This rule behaves as two independent instances of a single domain rule, and creates separate offenses for different domains.                              | For data that is tagged with Domain_A, it creates or contributes to a single domain offense that is tagged with Domain_A.<br><br>For data that is tagged with Domain_B, it creates or contributes to a single domain offense that is tagged with Domain_B.                                                               |
| <b>domain is one of: Domain_A, Domain_B</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> | Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C.<br><br>This rule behaves as two independent instances of a single domain rule, and maintains two separate states (HTTP flow counters) for two different domains. | When the rule detects 10 HTTP flows that are tagged with Domain_A within a minute, it creates or contributes to an offense that is tagged with Domain_A.<br><br>When the rule detects 10 HTTP flows that are tagged with Domain_B within a minute, it creates or contributes to an offense that is tagged with Domain_B. |
| No domain test defined                                                                                                                        | Looks at events that are tagged with all domains and creates or contributes to offenses on a per-domain basis.                                                                                                                                                                     | Each independent domain has offenses that are generated for it, but offenses do not contain contributions from other domains.                                                                                                                                                                                            |
| A rule has a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> and no domain test is defined        | Looks at events that are tagged with Domain_A, Domain_B, or Domain_C.                                                                                                                                                                                                              | Maintains separate states and creates separate offenses for each domain.                                                                                                                                                                                                                                                 |
| <b>domain is one of: Any Domain</b>                                                                                                           | Looks at all events, regardless of which domain it is tagged with.                                                                                                                                                                                                                 | Creates or contributes to a single system-wide offense that is tagged with Any Domain.                                                                                                                                                                                                                                   |

Table 58. Domain-aware rules (continued)

| Domain text                                                                                                                           | Explanation                                                                                                         | Rule response                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain is one of: Any Domain</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> | Looks at all events, regardless of which domain it is tagged with, and it maintains a single state for all domains. | Creates or contributes to a single system-wide offense that is tagged with Any Domain.<br><br>For example, if it detects 3 events that are tagged with Domain_A, 3 events that are tagged with Domain_B, and 4 events that are tagged with Domain_C within 1 minute, it creates an offense because it detected 10 events in total. |
| <b>domain is one of: Any Domain, Domain_A</b>                                                                                         | Works the same as a rule that has <b>domain is one of: Any Domain</b> .                                             | When the domain test includes Any Domain, any single domains that are listed are ignored.                                                                                                                                                                                                                                          |

When you view the offense table, you can sort the offenses by clicking the **Domain** column. The **Default Domain** is not included in the sort function so it does not appear in alphabetical order. However, it appears at the top or bottom of the **Domain** list, depending on whether the column is sorted in ascending or descending order. **Any Domain** does not appear in the list of offenses.

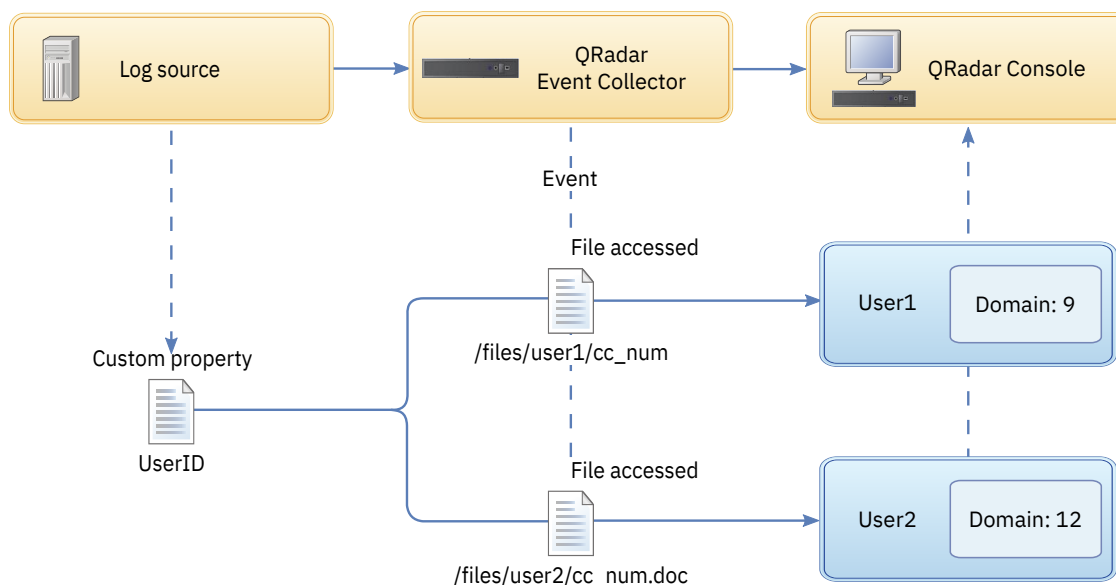
## Example: Domain privilege assignments based on custom properties

If your log files contain information that you want to use in a domain definition, you can expose the information as a custom event property.

You assign a custom property to a domain based on the capture result. You can assign the same custom property to multiple domains, but the capture results must be different.

For example, a custom event property, such as `userID`, might evaluate to a single user or a list of users. Each user can belong to only one domain.

In the following diagram, the log sources contain user identification information that is exposed as a custom property, `userID`. The event collector returns two user files, and each user is assigned to only one domain. In this case, one user is assigned to Domain: 9 and the other user is assigned to Domain: 12.



*Figure 11. Assigning domains by using custom event property*

If the capture results return a user that is not assigned to a specific user-defined domain, that user is automatically assigned to the default domain. Default domain assignments require manual intervention. Perform periodic searches to ensure that all entities in the default domain are correctly assigned.

**Important:** Before you use a custom property in a domain definition, ensure that **Optimize parsing for rules, reports, and searches** is checked on the **Custom Event Properties** window. This option ensures that the custom event property is parsed and stored when IBM Security QRadar receives the event for the first time. Domain segmentation doesn't occur if this option is not checked.

---

## Chapter 17. Multitenant management

Multitenant environments allow Managed Security Service Providers (MSSPs) and multi-divisional organizations to provide security services to multiple client organizations from a single, shared IBM Security QRadar deployment. You don't have to deploy a unique QRadar instance for each customer.

In a multitenant deployment, you ensure that customers see only their data by creating domains that are based on their QRadar input sources. Then, use security profiles and user roles to manage privileges for large groups of users within the domain. Security profiles and user roles ensure that users have access to only the information that they are authorized to see.

### **Related concepts**

[Capabilities in your IBM Security QRadar product](#)

---

### User roles in a multitenant environment

Multitenant environments include a service provider and multiple tenants. Each role has distinct responsibilities and associated activities.

#### **Service provider**

The service provider owns the system and manages its use by multiple tenants. The service provider can see data across all tenants. The Managed Security Service Provider (MSSP) administrator is typically responsible for the following activities:

- Administers and monitors the system health of the IBM Security QRadar deployment.
- Provisions new tenants.
- Creates roles and security profiles for tenant administrators and users.
- Secures the system against unauthorized access.
- Creates domains to isolate tenant data.
- Deploys changes that the tenant administrator made in the tenant environment.
- Monitors QRadar licenses.
- Collaborates with the tenant administrator.

#### **Tenants**

Each tenancy includes a tenant administrator and tenant users. The tenant administrator can be an employee of the tenant organization, or the service provider can administer the tenant on behalf of the customer.

The tenant administrator is responsible for the following activities:

- Configures [network hierarchy](#) definitions within their own tenancy.
- Configures and manages tenant data.
- Views log sources. Can edit the log source to coalesce data and can disable log sources.
- Collaborates with the MSSP administrator.

The tenant administrator can configure tenant-specific deployments, but they can't access or change the configuration for another tenant. They must contact the MSSP administrator to deploy changes in the QRadar environment, including network hierarchy changes within their own tenant.

Tenant users have no administrative privileges and can see only the data that they have access to. For example, a user can have privileges to view data from only 1 log source within a domain that has multiple log sources.

## Domains and log sources in multitenant environments

---

Use domains to separate overlapping IP addresses, and to assign sources of data, such as events and flows, into tenant-specific data sets.

When events or flows come into IBM Security QRadar, QRadar evaluates the domain definitions that are configured, and the events and flows are assigned to a domain. A tenant can have more than one domain. If no domains are configured, the events and flows are assigned to the default domain.

### Domain segmentation

Domains are virtual buckets that you use to segregate data based on the source of the data. They are the building blocks for multitenant environments. You configure domains from the following input sources:

- Event and flow collectors
- Flow sources
- Log sources and log source groups
- Custom properties
- Scanners

A multitenant deployment might consist of a basic hardware configuration that includes one QRadar Console, one centralized event processor, and then one event collector for each customer. In this configuration, you define domains at the collector level, which then automatically assigns the data that is received by QRadar to a domain.

To consolidate the hardware configuration even further, you can use one collector for multiple customers. If log or flow sources are aggregated by the same collector but belong to different tenants, you can assign the sources to different domains. When you use domain definitions at the log source level, each log source name must be unique across the entire QRadar deployment.

If you need to separate data from a single log source and assign it to different domains, you can configure domains from custom properties. QRadar looks for the custom property in the payload, and assigns it to the correct domain. For example, if you configured QRadar to integrate with a Check Point Provider-1 device, you can use custom properties to assign the data from that log source to different domains.

### Automatic log source detection

When domains are defined at the collector level and the dedicated event collector is assigned to a single domain, new log sources that are automatically detected are assigned to that domain. For example, all log sources that are detected on `Event_Collector_1` are assigned to `Domain_A`. All log sources that are automatically collected on `Event_Collector_2` are assigned to `Domain_B`.

When domains are defined at the log source or custom property level, log sources that are automatically detected and are not already assigned to a domain are automatically assigned to the default domain. The MSSP administrator must review the log sources in the default domain and allocate them to the correct client domains. In a multitenant environment, assigning log sources to a specific domain prevents data leakage and enforces data separation across domains.

## Provisioning a new tenant

---

As a Managed Security Services Provider (MSSP) administrator, you are using a single instance of IBM Security QRadar to provide multiple customers with a unified architecture for threat detection and prioritization.

In this scenario, you are onboarding a new client. You provision a new tenant and create a tenant administrator account that does limited administrative duties within their own tenant. You limit the access of the tenant administrator so that they can't see or edit information in other tenants.

Before you provision a new tenant, you must create the data sources, such as log sources or flow collectors, for the customer and assign them to a domain.

Complete the following tasks by using the tools on the **Admin** tab to provision the new tenant in QRadar:

1. To create the tenant, click **Tenant Management**.

For information about setting events per second (EPS) and flows per minute (FPM) limits for each tenant, see [“Monitoring license usage in multitenant deployments” on page 211](#).

2. To assign domains to the tenant, click **Domain Management**.

3. To create the tenant administrator role and grant the **Delegated Administration** permissions, click **User Roles**.

In a multitenant environment, tenant users with **Delegated administration** permissions can see only data for their own tenant environment. If you assign other administrative permissions that are not part of **Delegated Administration**, access is no longer restricted to that domain.

4. To create the tenant security profiles and restrict data access by specifying the tenant domains, click **Security Profiles**.

5. To create the tenant users and assign the user role, security profile, and tenant, click **Users**.

## Monitoring license usage in multitenant deployments

---

As the Managed Security Service Provider (MSSP) administrator, you monitor the event and flow rates across the entire IBM Security QRadar deployment.

When you create a tenant, you can set limits for both events per second (EPS) and flows per minute (FPM). By setting EPS and FPM limits for each tenant, you can better manage license capacities across multiple clients. If you have a processor that is collecting events or flows for a single customer, you do not need to assign tenant EPS and FPM limits. If you have a single processor that collects events or flows for multiple customers, you can set EPS and FPM limits for each tenant.

If you set the EPS and FPM limits to values that exceed the limits of either your software licenses or the appliance hardware, the system automatically throttles the events and flows for that tenant to ensure that the limits are not exceeded. If you do not set EPS and FPM limits for tenants, each tenant receives events and flows until either the license limits or the appliance limits are reached. The licensing limits are applied to the managed host. If you regularly exceed the license limitations, you can get a different license that is more suitable for your deployment.

### Viewing the cumulative license limits in your deployment

The EPS and FPM rates that you set for each tenant are not automatically validated against your license entitlements. To see the cumulative limits for the software licenses that are applied to the system as compared to the appliance hardware limits, do these steps:

1. On the navigation menu (☰), click **Admin** to open the admin tab.
2. In the **System Configuration** section, click **System and License Management**.
3. Expand **Deployment Details** and hover your mouse pointer over **Event Limit** or **Flow Limit**.

### Viewing EPS rates per log source

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rates for log sources.

1. On the **Log Activity** tab, select **Advanced Search** from the list on the **Search** toolbar.
2. To view the EPS per log source, type the following AQL query in the **Advanced Search** field:

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by logsourceid
```

```
order by EPS desc
last 24 hours
```

### Viewing EPS rates per domain

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rates for domains.

1. On the **Log Activity** tab, select **Advanced Search** from the drop-down list box on the **Search** toolbar.
2. To view the EPS per domain, type the following AQL query in the **Advanced Search** field:

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by domainid
order by EPS desc
last 24 hours
```

If you want to view average EPS rates for log sources only, click **Log Sources** in the **Data Sources** pane on the **Admin** tab. You can use this to quickly identify configuration issues with log sources that are failing to report.

### Viewing individual license limits in your deployment

The EPS and FPM rates that you set for each tenant are not automatically validated against your license entitlements. To see the individual limits for the software licenses that are applied to the system as compared to the appliance hardware limits, do these steps:

1. On the navigation menu (☰), click **Admin** to open the admin tab.
2. In the **System Configuration** section, click **System and License Management**.
3. Expand **Deployment Details** and hover your mouse over **Event Limit** or **Flow Limit**.

### Viewing the EPS rate for an individual log source

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rate for an individual log source.

1. Use a PSQL query to get a log source ID.
  - a. Use SSH to log in to QRadar as an administrator.
  - b. Access PSQL by using the following command:

```
psql -U qradar
```

- c. Get a list of log source names and IDs by using the following command:

```
select id,devicename from sensordevice;
```

- d. Select a log source ID from the list.
2. On the **Log Activity** tab, select **Advanced Search** from the list on the **Search** toolbar.
  3. To view the EPS rate for your selected log source, type the following AQL query in the **Advanced Search** field:

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from
events
where logsourceid=logsourceid
group by logsourceid
order by EPS desc
last 24 hours
```

### Viewing the EPS rate for an individual domain

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rate for an individual domain.



1. Use a PSQL query to get a domain ID.
  - a. Use SSH to log in to QRadar as an administrator.
  - b. Access PSQL by using the following command:

```
psql -U qradar
```

- c. Get a list of domain names and IDs by using the following command:

```
select id, name from domains;
```

- d. Select a domain ID from the list.
2. On the **Log Activity** tab, select **Advanced Search** from the list on the **Search** toolbar.
3. To view the EPS rate for your selected domain, type the following AQL query in the **Advanced Search** field:

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
where domainid=domainid
group by domainid
order by EPS desc
last 24 hours
```

## Detecting dropped events and flows

Events and flows are dropped when the IBM Security QRadar processing pipeline can't handle the volume of incoming events and flows, or when the number of events and flows exceeds the license limits for your deployment. You can look at the QRadar log file messages when these situations occur.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. View the `/var/log/qradar.error` log file and look for these messages:

These messages indicate that events or flows were dropped:

```
[Tenant:[tenantID]:[tenantName]
Event dropped while attempting to add to Tenant Event Throttle queue.
The Tenant Event Throttle queue is full.
```

```
[Tenant:[tenantID]:[tenantName]
Flow dropped while attempting to add to Tenant Flow Throttle queue.
The Tenant Flow Throttle queue is full.
```

These messages indicate that the processing pipeline was near capacity:

```
Throttle processor cannot keep up with events.
TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC is probably too short.
```

```
Throttle processor cannot keep up with flows.
TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC is probably too short.
```

If this warning persists, QRadar might drop events or flows.

### What to do next

If your system is dropping events and flows, you can expand your license to handle more data or you can set more restrictive EPS and FPM limits for each tenant.

## Rules management in multitenant deployments

In a multitenant environment, you must customize rules to make them tenant-aware. Tenant-aware rules use the **when the domain is one of the following** rule test, but the domain modifier determines the scope of the rule.

The following table shows how you can use the domain modifier to change the scope of rules in a multitenant deployment.

Table 59. Scope of rules in a multitenant environment

| Rule scope          | Description                                                                                                                                                      | Rule test example                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Single domain rules | These rules include only 1 domain modifier.                                                                                                                      | <b>and when the domain is one of the following:</b> <i>manufacturing</i>                 |
| Single tenant rules | These rules include all the domains that are assigned to the tenant. Use single tenant rules to correlate events across multiple domains within a single tenant. | <b>and when the domain is one of the following:</b> <i>manufacturing, finance, legal</i> |
| Global rules        | These rules use the <b>Any domain</b> modifier and run across all tenants.                                                                                       | <b>and when the domain is one of the following:</b> <i>Any domain</i>                    |

By being domain-aware, the custom rules engine (CRE) automatically isolates event correlations from different tenants by using their respective domains. For more information about working with rules in a domain-segmented network, see [Chapter 16, “Domain segmentation,”](#) on page 201.

## Restricting log activity capabilities for tenant users

To ensure that the tenant administrator and users can view the log data for only their tenant, you must restrict the permissions for the **Log Activity** capability.

### About this task

When you add the **Log Activity** capability to a user role, the **Maintain Custom Rules** and **View Custom Rules** permissions are automatically granted. Users who have these permissions have access to all log data for all domains. They can edit rules in all domains, even if their security profile settings have domain-level restrictions.

To prevent users from being able to access log data and modify rules in other domains or tenants, edit the user role and remove the **Maintain Custom Rules** and **View Custom Rules** permissions. Without these permissions, the tenant administrator and users cannot change rules, including those rules in their own domain.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **User Roles** and select the user role that you want to edit.
3. Under **Log Activity**, clear the **Maintain Custom Rules** and **View Custom Rules** check boxes.
4. Click **Save**.

## Network hierarchy updates in a multitenant deployment

IBM Security QRadar uses the network hierarchy to understand and analyze the network traffic in your environment. Tenant administrators who have the **Define network hierarchy** permission can change the network hierarchy within their own tenant.

Network hierarchy changes require a full configuration deployment to apply the updates in the QRadar environment. Full configuration deployments restart all QRadar services, and data collection for events and flows stops until the deployment completes. Tenant administrators must contact the Managed Security Service Provider (MSSP) administrator to deploy the changes. MSSP administrators can plan the deployment during a scheduled outage, and notify all tenant administrators in advance.

In a multitenant environment, the network object name must be unique across the entire deployment. You cannot use network objects that have the same name, even if they are assigned to different domains.

**Related concepts**

[Network hierarchy](#)

IBM Security QRadar uses the network hierarchy objects and groups to view network activity and monitor groups or services in your network.

## Retention policies for tenants

---

You can configure up to 10 retention buckets for shared data, and up to 10 retention buckets for each tenant. The default retention period is 30 days; then, the tenant data is automatically deleted. To keep tenant data for longer than 30 days, you must configure a retention bucket. Until you configure a retention bucket, all events or flows are stored in the default retention bucket for each tenant.

If your QRadar deployment has more than 10 tenants, you can configure a shared data retention policy and use the domain filter to create a domain-based retention policy for each of the domains within the tenant. Adding the domains specifies that the policy applies only to the data for that tenant.

**Related concepts**

[Data retention](#)



---

## Chapter 18. Asset Management

Assets and asset profiles that are created for servers and hosts in your network provide important information to assist you in resolving security issues. Using the asset data, you can connect offenses that are triggered in your system to physical or virtual assets to provide a starting point in a security investigation.

The **Assets** tab in IBM Security QRadar provides a unified view of the known information about the assets in your network. As QRadar discovers more information, the system updates the asset profile and incrementally builds a complete picture about the asset.

Asset profiles are built dynamically from identity information that is passively absorbed from event or flow data, or from data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually. For more information, see the topics *Importing Asset Profiles* and *Adding or editing an asset profile* in the *IBM Security QRadar User Guide*.

**Restriction:** IBM QRadar Log Manager tracks only asset data if IBM Security QRadar Vulnerability Manager is installed. For more information about the differences between QRadar SIEM and QRadar Log Manager, see [“Capabilities in your IBM Security QRadar product” on page 7](#).

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

## Sources of asset data

Asset data is received from several different sources in your IBM Security QRadar deployment.

Asset data is written to the asset database incrementally, usually 2 or 3 pieces of data at a time. With exception of updates from network vulnerability scanners, each asset update contains information about only one asset at a time.

Asset data usually comes from one of the following asset data sources:

### Events

Event payloads, such as those created by DHCP or authentication servers, often contain user logins, IP addresses, host names, MAC addresses, and other asset information. This data is immediately provided to the asset database to help determine which asset the asset update applies to.

Events are the primary cause for asset growth deviations.

### Flows

Flow payloads contain communication information such as IP address, port, and protocol that is collected over regular, configurable intervals. At the end of each interval, the data is provided to the asset database, one IP address at a time.

Because asset data from flows is paired with an asset based on a single identifier, the IP address, flow data is never the cause of asset growth deviations.

### Vulnerability scanners

QRadar integrates with both IBM and third-party vulnerability scanners that can provide asset data such as operating system, installed software, and patch information. The type of data varies from scanner to scanner and can vary from scan to scan. As new assets, port information, and vulnerabilities are discovered, data is brought into the asset profile based on the CIDR ranges that are defined in the scan.

It is possible for scanners to introduce asset growth deviations but it is rare.

### User interface

Users who have the Assets role can import or provide asset information directly to the asset database. Asset updates that are provided directly by a user are for a specific asset. Therefore the asset reconciliation stage is bypassed.

Asset updates that are provided by users do not introduce asset growth deviations.

### **Domain-aware asset data**

When an asset data source is configured with domain information, all asset data that comes from that data source is automatically tagged with the same domain. Because the data in the asset model is domain-aware, the domain information is applied to all QRadar components, including identities, offenses, asset profiles, and server discovery.

When you view the asset profile, some fields might be blank. Blank fields exist when the system did not receive this information in an asset update, or the information exceeded the asset retention period. The default retention period is 120 days. An IP address that appears as 0.0.0.0 indicates that the asset does not contain IP address information.

## **Incoming asset data workflow**

---

IBM Security QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

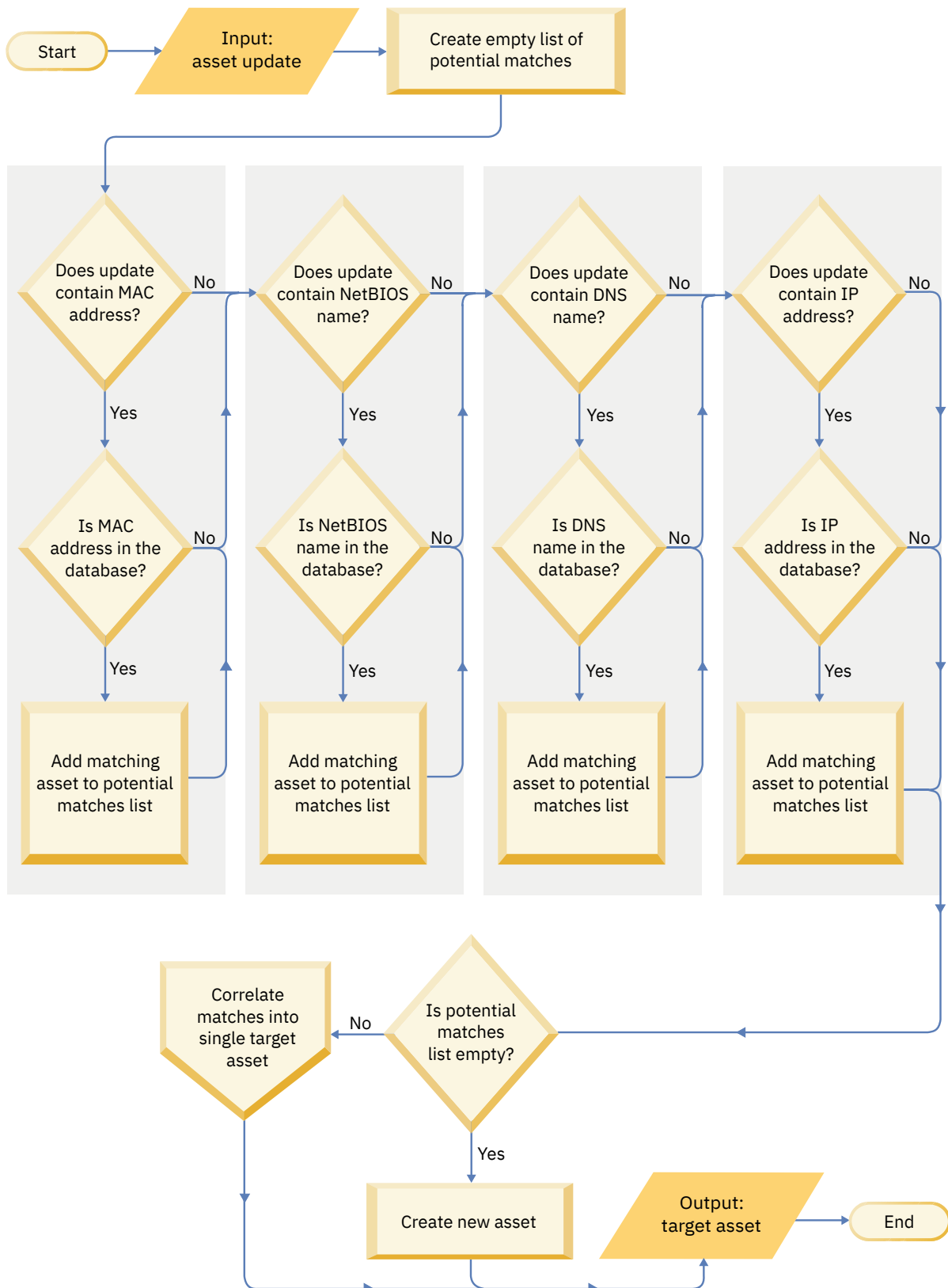


Figure 12. Asset data workflow diagram

1. QRadar receives the event. The asset profiler examines the event payload for identity information.

2. If the identity information includes a MAC address, a NetBIOS host name, or a DNS host name that are already associated with an asset in the asset database, then that asset is updated with any new information.
3. If the only available identity information is an IP address, the system reconciles the update to the existing asset that has the same IP address.
4. If an asset update has an IP address that matches an existing asset but the other identity information does not match, the system uses other information to rule out a false-positive match before the existing asset is updated.
5. If the identity information does not match an existing asset in the database, then a new asset is created based on the information in the event payload.

## Updates to asset data

---

IBM Security QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Each asset update must contain trusted information about a single asset. When QRadar receives an asset update, the system determines which asset to which the update applies.

*Asset reconciliation* is the process of determining the relationship between asset updates and the related asset in the asset database. Asset reconciliation occurs after QRadar receives the update but before the information is written to the asset database.

### Identity information

Every asset must contain at least one piece of identity data. Subsequent updates that contain one or more pieces of that same identity data are reconciled with the asset that owns that data. Updates that are based on IP addresses are handled carefully to avoid false-positive asset matches. False positive asset matches occur when one physical asset is assigned ownership of an IP address that was previously owned by another asset in the system.

When multiple pieces of identity data are provided, the asset profiler prioritizes the information from the most deterministic to the least in the following order:

- MAC address
- NetBIOS host name
- DNS host name
- IP address

MAC addresses, NetBIOS host names, and DNS host names are unique and therefore are considered as definitive identity data. Incoming updates that match an existing asset only by the IP address are handled differently than updates that match more definitive identity data.

### Asset reconciliation exclusion rules

With each asset update that enters IBM Security QRadar, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

By default, each piece of asset data is tracked over a two-hour period. If any one piece of identity data in the asset update exhibits suspicious behavior two or more times within 2 hours, that piece of data is added to the asset blacklists. Each type of identity asset data that is tested results in a new blacklist.

In domain-aware environments, the asset reconciliation exclusion rules track the behavior of asset data separately for each domain.

The asset reconciliation exclusion rules test the following scenarios:



| Table 60. Rule tests and responses                                                                  |                                                                                |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Scenario                                                                                            | Rule response                                                                  |
| When a MAC address is associated to three or more different IP addresses in 2 hours or less         | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |
| When a DNS host name is associated to three or more different IP addresses in 2 hours or less       | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less   | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less      | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less  | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When a DNS host name is associated to three or more different MAC addresses in 2 hours or less      | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When an IPv4 address is associated to three or more different DNS host names in 2 hours or less     | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When a MAC address is associated to three or more different DNS host names in 2 hours or less       | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |
| When an IPv4 address is associated to three or more different NetBIOS host names in 2 hours or less | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a DNS host name is associated to three or more different NetBIOS host names in 2 hours or less | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When a MAC address is associated to three or more different NetBIOS host names in 2 hours or less   | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |

You can view these rules on the **Offenses** tab by clicking **Rules** and then selecting the **asset reconciliation exclusion** group in the drop-down list.

## Asset merging

*Asset merging* is the process where the information for one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Asset merging occurs when an asset update contains identity data that matches two different asset profiles. For example, a single update that contains a NetBIOS host name that matches one asset profile and a MAC address that matches a different asset profile might trigger an asset merge.

Some systems can cause high volumes of asset merging because they have asset data sources that inadvertently combine identity information from two different physical assets into a single asset update. Some examples of these systems include the following environments:

- Central syslog servers that act as an event proxy
- Virtual machines
- Automated installation environments
- Non-unique host names, common with assets like iPads and iPhones.

- Virtual private networks that have shared MAC addresses
- Log source extensions where the identity field is `OverrideAndAlwaysSend=true`

Assets that have many IP addresses, MAC addresses, or host names show deviations in asset growth and can trigger system notifications.

## Identification of asset growth deviations

---

Sometimes, asset data sources produce updates that IBM Security QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

*Asset growth deviations* occur when the number of asset updates for a single device grows beyond the limit that is set by the retention threshold for a specific type of the identity information. Proper handling of asset growth deviations is critical to maintaining an accurate asset model.

At the root of every asset growth deviation is an asset data source whose data is untrustworthy for updating the asset model. When a potential asset growth deviation is identified, you must look at the source of the information to determine whether there is a reasonable explanation for the asset to accumulate large amounts of identity data. The cause of an asset growth deviation is specific to an environment.

### DHCP server example of unnatural asset growth in an asset profile

Consider a virtual private network (VPN) server in a Dynamic Host Configuration Protocol (DHCP) network. The VPN server is configured to assign IP addresses to incoming VPN clients by proxying DHCP requests on behalf of the client to the network's DHCP server.

From the perspective of the DHCP server, the same MAC address repeatedly requests many IP address assignments. In the context of network operations, the VPN server is delegating the IP addresses to the clients, but the DHCP server can't distinguish when a request is made by one asset on behalf of another.

The DHCP server log, which is configured as a QRadar log source, generates a DHCP acknowledgment (DHCP ACK) event that associates the MAC address of the VPN server with the IP address that it assigned to the VPN client. When asset reconciliation occurs, the system reconciles this event by MAC address, which results in a single existing asset that grows by one IP address for every DHCP ACK event that is parsed.

Eventually, one asset profile contains every IP address that was allocated to the VPN server. This asset growth deviation is caused by asset updates that contain information about more than one asset.

### Threshold settings

When an asset in the database reaches a specific number of properties, such as multiple IP addresses or MAC addresses, QRadar blocks that asset from receiving more updates.

The Asset Profiler threshold settings specify the conditions under which an asset is blocked from updates. The asset is updated normally up to the threshold value. When the system collects enough data to exceed the threshold, the asset shows an asset growth deviation. Future updates to the asset are blocked until the growth deviation is rectified.

## System notifications that indicate asset growth deviations

IBM Security QRadar generates system notifications to help you identify and manage the asset growth deviations in your environment.

The following system messages indicate that QRadar identified potential asset growth deviations:

- The system detected asset profiles that exceed the normal size threshold
- The asset blacklist rules have added new asset data to the asset blacklists

The system notification messages include links to reports to help you identify the assets that have growth deviations.

### Asset data that changes frequently

Asset growth can be caused by large volumes of asset data that changes legitimately, such as in these situations:

- A mobile device that travels from office-to-office frequently and is assigned a new IP address whenever it logs in.
- A device that connects to a public wifi with short IP addresses leases, such as at a university campus, might collect large volumes of asset data over a semester.

### Example: How configuration errors for log source extensions can cause asset growth deviations

Customized log source extensions that are improperly configured can cause asset growth deviations.

You configure a customized log source extension to provide asset updates to IBM Security QRadar by parsing user names from the event payload that is on a central log server. You configure the log source extension to override the event host name property so that the asset updates that are generated by the custom log source always specify the DNS host name of the central log server.

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

### Troubleshooting asset profiles that exceed the normal size threshold

IBM Security QRadar generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

```
The system detected asset profiles that exceed the normal size threshold
```

#### Explanation

The payload of the notification shows a list of the top five most frequently deviating assets and why the system marked each asset as a growth deviation. As shown in the following example, the payload also shows the number of times that the asset attempted to grow beyond the asset size threshold.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

When the asset data exceeds the configured threshold, QRadar blocks the asset from future updates. This intervention prevents the system from receiving more corrupted data and mitigates the performance impacts that might occur if the system attempts to reconcile incoming updates against an abnormally large asset profile.

#### Required user action

Use the information in the notification payload to identify the assets that are contributing to the asset growth deviation and determine what is causing the abnormal growth. The notification provides a link to a report of all assets that experienced deviating asset growth over the past 24 hours.

After you resolve the asset growth deviation in your environment, you can run the report again.

1. Click the **Log Activity** tab and click **Search > New Search**.
2. Select the **Deviating Asset Growth: Asset Report** saved search.
3. Use the report to identify and repair inaccurate asset data that was created during the deviation.

If the asset data is valid, QRadar administrators can increase the threshold limits for IP addresses, MAC addresses, NetBIOS host names, and DNS host names in the **Asset Profiler Configuration** on the QRadar **Admin** tab.

### Related concepts

#### Stale asset data

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.

## New asset data is added to the asset blacklists

IBM Security QRadar generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

```
The asset blacklist rules have added new asset data to the asset blacklists
```

### Explanation

Asset exclusion rules monitor asset data for consistency and integrity. The rules track specific pieces of asset data over time to ensure that they are consistently being observed with the same subset of data within a reasonable time.

For example, if an asset update includes both a MAC address and a DNS host name, the MAC address is associated with that DNS host name for a sustained period. Subsequent asset updates that contain that MAC address also contain that same DNS host name when one is included in the asset update. If the MAC address suddenly is associated with a different DNS host name for a short period, the change is monitored. If the MAC address changes again within a short period, the MAC address is flagged as contributing to an instance of deviating or abnormal asset growth.

### Required user action

Use the information in the notification payload to identify the rules that are used to monitor asset data. Click the **Asset deviations by log source** link in the notification to see the asset deviations that occurred in the last 24 hours.

If the asset data is valid, QRadar administrators can configure QRadar to resolve the problem.

- If your blacklists are populating too aggressively, you can tune the asset reconciliation exclusion rules that populate them.
- If you want to add the data to the asset database, you can remove the asset data from the blacklist and add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.

### Related concepts

#### Advanced tuning of asset reconciliation exclusion rules

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

## Prevention of asset growth deviations

After you confirm that the reported asset growth is legitimate, there are several ways to prevent IBM Security QRadar from triggering growth deviation messages for that asset.

Use the following list to help you decide how to prevent asset growth deviations:

- [Understand how QRadar handles stale asset data.](#)
- [Tune the asset profiler retention settings to limit the length of time that asset data is retained.](#)
- [Tune the number of IP addresses allowed for a single asset.](#)
- [Create identity exclusion searches to exclude certain events from providing asset updates.](#)
- [Tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth.](#)
- Create asset whitelists to prevent data from reappearing on the asset blacklists.
- Modify the entries on the asset blacklists and asset whitelists.
- Ensure that your DSMs are up to date. QRadar provides a weekly automatic update that might contain DSM updates and corrections to parsing issues.

## Stale asset data

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.

*Stale asset data* is historical asset data that is not actively or passively observed within a specific time. Stale asset data is deleted when it exceeds the configured retention period.

The historical records become active again if they are observed by IBM Security QRadar passively, through events and flows, or actively, through port and vulnerability scanners.

Preventing asset growth deviations requires finding the right balance between the number of IP addresses allowed for a single asset and the length of time that QRadar retains the asset data. You must consider the performance and manageability trade-offs before you configure QRadar to accommodate high levels of asset data retention. While longer retention periods and higher per-asset thresholds might appear desirable all the time, a better approach is to determine a baseline configuration that is acceptable for your environment and test that configuration. Then, you can increase the retention thresholds in small increments until the right balance is achieved.

### Related tasks

[Tuning the Asset Profiler retention settings](#)

[Tuning the number of IP addresses allowed for a single asset](#)

## Asset blacklists and whitelists

IBM Security QRadar uses a group of asset reconciliation rules to determine if asset data is trustworthy. When asset data is questionable, QRadar uses asset blacklists and whitelists to determine whether to update the asset profiles with the asset data.

An *asset blacklist* is a collection of data that QRadar considers untrustworthy. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

The asset blacklists and whitelists are reference sets. You can view and modify the asset blacklist and whitelist data using the **Reference Set Management** tool in the QRadar Console. For more information about working with reference sets, see [“Reference sets overview” on page 140](#).

Alternatively, you can use the command line interface (CLI) or the RestFUL API endpoint to update the content of the asset blacklists and whitelists.

## Asset blacklists

An *asset blacklist* is a collection of data that IBM Security QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

Every asset update in QRadar is compared to the asset blacklists. Blacklisted asset data is applied globally for all domains. If the asset update contains identity information (MAC address, NetBIOS host name, DNS host name, or IP address) that is found on a blacklist, the incoming update is discarded and the asset database is not updated.

The following table shows the reference collection name and type for each type of identity asset data.

| Table 61. Reference collection names for asset blacklist data                               |                                        |                                  |
|---------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|
| Type of identity data                                                                       | Reference collection name              | Reference collection type        |
| IP addresses (v4)                                                                           | Asset Reconciliation IPv4 Blacklist    | Reference Set [Set Type: IP]     |
| DNS host names                                                                              | Asset Reconciliation DNS Blacklist     | Reference Set [Set Type: ALNIC*] |
| NetBIOS host names                                                                          | Asset Reconciliation NetBIOS Blacklist | Reference Set [Set Type: ALNIC*] |
| MAC Addresses                                                                               | Asset Reconciliation MAC Blacklist     | Reference Set [Set Type: ALNIC*] |
| * ALNIC is an alphanumeric type that can accommodate both host name and MAC address values. |                                        |                                  |

You can use the **Reference Set Management** tool to edit the blacklist entries. For information about working with reference sets, see [Reference sets management](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html) ([http://www.ibm.com/support/knowledgecenter/SS42VS\\_7.2.7/com.ibm.qradar.doc/c\\_qradar\\_adm\\_mge\\_ref\\_set.html](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html)).

## Related concepts

### [Asset whitelists](#)

## Asset whitelists

You can use asset whitelists to keep IBM Security QRadar asset data from inadvertently reappearing in the asset blacklists.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

You can use the **Reference Set Management** tool to edit the whitelist entries. For information about working with reference sets, see [Reference sets management](#).

## Example of a whitelist use case

The whitelist is helpful if you have asset data that continues to show up in the blacklists when it is a valid asset update. For example, you might have a round robin DNS load balancer that is configured to rotate across a set of five IP addresses. The Asset Reconciliation Exclusion rules might determine that the multiple IP addresses associated with the same DNS host name are indicative of an asset growth deviation, and the system might add the DNS load balancer to the blacklist. To resolve this problem, you can add the DNS host name to the Asset Reconciliation DNS Whitelist.

## Mass entries to the asset whitelist

An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network. Ignoring asset deviations by adding mass entries to the asset whitelist is not helpful in building an accurate asset database. Instead of adding mass whitelist entries, review the asset blacklist to determine what is contributing to the deviating asset growth and then determine how to fix it.

## Types of asset whitelists

Each type of identity data is kept in a separate whitelist. The following table shows the reference collection name and type for each type of identity asset data.

| Table 62. Reference collection name for asset whitelist data                           |                                        |                                  |
|----------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|
| Type of data                                                                           | Reference collection name              | Reference collection type        |
| IP addresses                                                                           | Asset Reconciliation IPv4 Whitelist    | Reference Set [Set Type: IP]     |
| DNS host names                                                                         | Asset Reconciliation DNS Whitelist     | Reference Set [Set Type: ALNIC*] |
| NetBIOS host names                                                                     | Asset Reconciliation NetBIOS Whitelist | Reference Set [Set Type: ALNIC*] |
| MAC addresses                                                                          | Asset Reconciliation MAC Whitelist     | Reference Set [Set Type: ALNIC*] |
| * ALNIC is an alphanumeric type that can accommodate host name and MAC address values. |                                        |                                  |

## Related concepts

### Asset blacklists

An *asset blacklist* is a collection of data that IBM Security QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

### Updating the asset blacklists and whitelists by using reference set utility

You can use the IBM Security QRadar reference set utility to add or modify the entries that are on the asset blacklists or whitelists.

To manage your reference sets, run the `ReferenceDataUtil.sh` utility from `/opt/qradar/bin` on the QRadar Console.

The commands to add new values to each list are described in the following table. The parameter values must exactly match the asset update values that are provided by the originating asset data source.

| Table 63. Command syntax to modify asset blacklist and whitelist data |                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                                  | Command syntax                                                                                                                                                                                                                                                                                              |
| Asset Reconciliation IPv4 Blacklist                                   | <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" IP</pre> <p>For example, this command adds IP address 192.168.3.56 to the blacklist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56</pre>                                                         |
| Asset Reconciliation DNS Blacklist                                    | <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" DNS</pre> <p>For example, this command adds domain name 'misbehaving.asset.company.com' to the blacklist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"</pre>                   |
| Asset Reconciliation NetBIOS Blacklist                                | <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Blacklist" NETBIOS</pre> <p>For example, this command removes NetBIOS host name 'deviantGrowthAsset-156384' from the blacklist:</p> <pre>ReferenceDataUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"</pre> |

Table 63. Command syntax to modify asset blacklist and whitelist data (continued)

| Name                                   | Command syntax                                                                                                                                                                                                                                                                  |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Asset Reconciliation MAC Blacklist     | <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR</pre> <p>For example, this command adds MAC address '00:a0:1a:2b:3c:4d' to the blacklist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:1a:2b:3c:4d"</pre>           |
| Asset Reconciliation IPv4 Whitelist    | <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP</pre> <p>For example, this command deletes IP address 10.1.95.142 from the whitelist:</p> <pre>ReferenceDataUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142</pre>                       |
| Asset Reconciliation DNS Whitelist     | <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" DNS</pre> <p>For example, this command adds domain name 'loadbalancer.company.com' to the whitelist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"</pre> |
| Asset Reconciliation NetBIOS Whitelist | <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" NETBIOS</pre> <p>For example, this command adds NetBIOS name 'assetName-156384' to the whitelist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"</pre>    |
| Asset Reconciliation MAC Whitelist     | <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" MACADDR</pre> <p>For example, this command adds MAC address '00:a0:1a:2b:3c:4d' to the whitelist:</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" "00:a0:1a:2b:3c:4d"</pre>           |

## Related tasks

[Updating the blacklists and whitelists using the RESTful API](#)

## Updating the blacklists and whitelists using the RESTful API

You can use the IBM Security QRadar RESTful API to customize the content of the asset blacklists and whitelists.

## About this task

You must specify the exact name of the reference set that you want to view or update.

- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation MAC Blacklist
- Asset Reconciliation IPv4 Whitelist
- Asset Reconciliation DNS Whitelist
- Asset Reconciliation NetBIOS Whitelist
- Asset Reconciliation MAC Whitelist



## Procedure

1. Type the following URL in your web browser to access the RESTful API interface:

```
https://ConsoleIPAddress/api_doc
```

2. In the navigation pane on the left, find 4.0>/reference\_data >/sets > /{name}.
3. To view the contents of an asset blacklist or whitelist, follow these steps:
  - a) Click the **GET** tab and scroll down to the **Parameters** section.
  - b) In the **Value** field for the **Name** parameter, type the name of the asset blacklist or whitelist that you want to view.
  - c) Click **Try It Out** and view the results at the bottom of the screen.
4. To add a value to an asset blacklist or whitelist, follow these steps:
  - a) Click the **POST** tab and scroll down to the **Parameters** section.
  - b) Type in the values for the following parameters:

| Table 64. Parameters that are required to add new asset data |                                                                                                                                                                                       |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter name                                               | Parameter description                                                                                                                                                                 |
| name                                                         | Represents the name of the reference collection that you want to update.                                                                                                              |
| value                                                        | Represents the data item that you want to add to the asset blacklist or whitelist. Must exactly match the asset update values that are provided by the originating asset data source. |

- c) Click **Try It Out** to add the new value to the asset whitelist or asset blacklist.

### What to do next

For more information about using the RESTful API to change the reference sets, see the *IBM Security QRadar API Guide*.

### Related concepts

[Updating the asset blacklists and whitelists by using reference set utility](#)

You can use the IBM Security QRadar reference set utility to add or modify the entries that are on the asset blacklists or whitelists.

## Tuning the Asset Profiler retention settings

IBM Security QRadar uses the asset retention settings to manage the size of the asset profiles.

The default retention period for most asset data is 120 days after the last time it was either passively or actively observed in QRadar. User names are retained for 30 days.

Asset data that is added manually by QRadar users does not usually contribute to asset growth deviations. By default, this data is retained forever. For all other types of asset data, the **Retain Forever** flag is suggested only for static environments.

### About this task


You can adjust the retention time based on the type of asset identity data that is in the event. For example, if multiple IP addresses are merging under one asset, you can change the Asset IP Retention period from 120 days to a lower value.

When you change the asset retention period for a specific type of asset data, the new retention period is applied to all asset data in QRadar. Existing asset data that already exceeds the new threshold is removed when the deployment is complete. To ensure that you can always identify named hosts even when the asset data is beyond the retention period, the asset retention cleanup process does not remove the last known host name value for an asset.

Before you determine how many days that you want to retain the asset data, understand the following characteristics about longer retention periods:

- provides a better historical view of your assets.
- creates larger data volumes per asset in the asset database.
- increases the probability that stale data will contribute to asset growth deviation messages.

#### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Asset Profiler Configuration**.
3. Click **Asset Profiler Retention Configuration**.
4. Adjust the retention values and click **Save**.
5. Deploy the changes into your environment for the updates to take effect.

#### Related tasks

[Tuning the number of IP addresses allowed for a single asset](#)

### Tuning the number of IP addresses allowed for a single asset

IBM Security QRadar monitors the number of IP addresses that a single asset accumulates over time.

By default, QRadar generates a system message when a single asset accumulates more than 75 IP addresses. If you expect assets to accumulate more than 75 IP addresses, you can tune the **Number of IPs Allowed for a Single Asset** value to avoid future system messages.

#### About this task

Setting the limit for the number of IP addresses too high prevents QRadar from detecting asset growth deviations before they have a negative impact on the rest of the deployment. Setting the limit too low increases the number of asset growth deviations that are reported.


You can use the following guideline when you tune the **Number of IPs Allowed for a Single Asset** setting for the first time.

Number of IP addresses that are allowed for a single asset = (*<retention time (days)>* x *<estimated IP addresses per day>*) + *<buffer number of IP addresses>*

Where

- *<estimated IP addresses per day>* is the number of IP addresses that a single asset might accumulate in one day under normal conditions
- *<retention time (days)>* is the preferred amount of time to retain the asset IP addresses

#### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Asset Profiler Configuration**.
3. Click **Asset Profiler Configuration**.
4. Adjust the configuration values and click **Save**.
5. Deploy the changes into your environment for the updates to take effect.

#### Related tasks

[Tuning the Asset Profiler retention settings](#)

### Identity exclusion searches

Identity exclusion searches can be used to manage single assets that accumulate large volumes of similar identity information for known, valid reasons.

For example, log sources can provide large volumes of asset identity information to the asset database. They provide IBM Security QRadar with near real-time changes to asset information and they can keep

your asset database current. But log sources are most often the source of asset growth deviations and other asset-related anomalies.

When a log source sends incorrect asset data to QRadar, try to fix the log source so that the data it sends is usable by the asset database. If the log source cannot be fixed, you can build an identity exclusion search that blocks the asset information from entering the asset database.

You can also use an identity exclusion search where `Identity_Username+Is Any Of + Anonymous Logon` to ensure that you are not updating assets that are related to service accounts or automated services.

### Differences between identity exclusion searches and blacklists

While identity exclusion searches appear to have similar functionality to asset blacklists, there are significant differences.

Blacklists can specify only raw asset data, such as MAC addresses and host names, that is to be excluded. Identity exclusion searches filter out asset data based on search fields like log source, category, and event name.

Blacklists do not account for the type of data source that is providing the data, whereas identity exclusion searches can be applied to events only. Identity exclusion searches can block asset updates based on common event search fields, such as event type, event name, category, and log source.

### Creating identity exclusion searches

To exclude certain events from providing asset data to the asset database, you can create an IBM Security QRadar identity exclusion search.

#### About this task


The filters that you create for the search must match events that you want to exclude, not the events that you want to keep.

You might find it helpful to run the search against events that are already in the system. However, when you save the search, you must select **Real Time (streaming)** in the **Timespan** options. If you do not choose this setting, the search does not match any results when it runs against the live stream of events that are coming into QRadar.

When you update the saved identity exclusion search without changing the name, the identity exclusion list that is used by the Asset Profiler is updated. For example, you might edit the search to add more filtering of the asset data that you want to exclude. The new values are included and the asset exclusion starts immediately after the search is saved.

#### Procedure

1. Create a search to identify the events that do not provide asset data to the asset database.
  - a) On the **Log Activity** tab, click **Search > New Search**.
  - b) Create the search by adding search criteria and filters to match the events that you want to exclude from asset updates.
  - c) In the **Time Range** box, select **Real Time (streaming)** and then click **Filter** to run the search.
  - d) On the search results screen, click **Save Criteria** and provide the information for the saved search.

**Note:** You can assign the saved search to a search group. An Identity Exclusion search group exists in the **Authentication, Identity and User Activity** folder.
  - e) Click **OK** to save the search.
2. Identify the search that you created as an identity exclusion search.
  - a) On the navigation menu () , click **Admin**.
  - b) In the **System Configuration** section, click **Asset Profiler Configuration**.
  - c) Click **Manage Identity Exclusion** at the bottom of the screen.

- d) Select the identity exclusion search that you created from the list of searches on the left and click the add icon (>).

**Tip:** If you can't find the search, type the first few letters into the filter at the top of the list.

- e) Click **Save**.

3. On the **Admin** tab, click **Deploy changes** for the updates to take effect.

## Advanced tuning of asset reconciliation exclusion rules

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

For example, consider this normalized template from an Asset Reconciliation Exclusion rule.

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
by the Local system and NOT when any of
Identity Host Name are contained in any of
Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
and when at least N1 events are seen with the same
Identity Host Name and different Identity IP in N2
```

This table lists the variables in the rule template that can be tuned and the result of the change. Avoid changing other variables in the template.

| Table 65. Options for tuning the asset reconciliation rules |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variable                                                    | Default value | Tuning result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| N1                                                          | 3             | <p>Tuning this variable to a lower value results in more data being added to the blacklist because fewer events with conflicting data are needed for the rule to fire.</p> <p>Tuning this variable to a higher value results in less data being added to the blacklist because more events with conflicting data are needed for the rule to fire.</p>                                                                                                                                                                                                                                                  |
| N2                                                          | 2 hours       | <p>Tuning this variable to a lower value reduces the window of time in which N1 events must be seen for the rule to fire. The time required to observe matching data is decreased, which results in less data being added to the blacklist.</p> <p>Tuning this variable to a higher value increases the time in which N1 events must be seen for the rule to fire. The time to observe matching data is increased, which results in more data being added to the blacklist.</p> <p>Increasing the time period might impact system memory resources as data is tracked over longer periods of time.</p> |

The Asset Reconciliation Exclusion rules are system-wide rules. Changes to the rules affect the way that the rule behaves throughout the entire system.

### Applying different tuning for rules

It might be necessary to apply different tuning for rules in different parts of the system. To apply different tuning for rules, you must duplicate the Asset Reconciliation Exclusion rules that you want to tune and add one or more tests to constrain the rules so that you test only certain parts of the system. For example, you might want to create rules that test only networks, log sources, or event types.

### About this task

Always be cautious when you are adding new rules to the system because as some tasks and CRE rules might impact system performance. It might be beneficial to add the new rules to the top of each test

stack to allow the system to bypass the remainder of the test logic whenever an asset update matches the criteria for the new rule.

## Procedure

1. Duplicate the rule.

a) On the **Offenses** tab, click **Rules** and select the rule that you want to copy.

b) Click **Actions > Duplicate**.

It can be helpful if the name of the new rule is indicative of the reason for duplicating it.

2. Add a test to the rule.

Determine a filter that you want to use to apply the rule only to a subset of system data. For example, you can add a test that matches only events from a specific log source.

3. Tune the variables of the rule to achieve the wanted behavior.

4. Update the original rule.

a) Add the same test that you added to the duplicate rule to the original rule, but this time invert the rules AND and AND NOT operators.

Inverting the operators prevents events from being triggered in both rules.

## Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

As the Network security administrator, you manage a corporate network that includes a public wifi network segment where IP address leases are typically short and frequent. The assets on this segment of the network tend to be transient, primarily notebooks and hand-held devices that log in and out of the public wifi frequently. Commonly, a single IP address is used multiple times by different devices over a short time.

In the rest of your deployment, you have a carefully managed network that consists only of inventoried, well-named company devices. IP address leases are much longer in this part of the network, and IP addresses are accessed by authentication only. On this network segment, you want to know immediately when there are any asset growth deviations and you want to keep the default settings for the asset reconciliation exclusion rules.

### Blacklisting IP addresses

In this environment, the default asset reconciliation exclusion rules inadvertently blacklist the entire network in a short time.

Your security team finds the asset-related notifications that are generated by the wifi segment are a nuisance. You want to prevent the wifi from triggering any more deviating asset growth notifications.

### Tuning asset reconciliation rules to ignore some asset updates

You review the **Asset deviation by log source** report in the last system notification. You determine that the blacklisted data is coming from the DHCP server on your wifi.

The values in the **Event Count** column, **Flow Count** column and the **Offenses** column for the row corresponding to the **AssetExclusion: Exclude IP By MAC Address** rule indicate that your wifi DHCP server is triggering this rule.

You add a test to the existing asset reconciliation exclusion rules to stop rules from adding wifi data to the blacklist.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
```

and when at least 3 events are seen with the same Identity IP and different Identity MAC in 2 hours.

The updated rule tests only the events from the log sources that are not on your wifi DHCP server. To prevent wifi DHCP events from undergoing more expensive reference set and behavior analysis tests, you also moved this test to the top of the test stack.

## Clean up asset data after growth deviations

---

IBM Security QRadar uses the asset model to connect offenses in your deployment to physical or virtual assets in your network. The ability to collect and view relevant data on how assets are used is an important step in resolving security issues. It is important to maintain the asset database to ensure that the data is current and accurate.

Whether you fix the source of the problem or block the asset updates, you must clean up the asset database by removing the invalid asset data and removing the asset blacklist entries.

### Deleting invalid assets

After you fix the assets that contributed to the asset growth deviation, clean up your asset artifacts by using selective clean up or rebuilding the asset database.

#### About this task

##### Selective clean up

This method is for asset growth deviations of limited scope. Selectively removing the affected assets is the least invasive way to clean up asset artifacts, but if many assets were affected, it can also be the most tedious.

##### Rebuild the asset database

Rebuilding the asset database from scratch is the most efficient and precise method of deleting assets when asset growth deviations are pervasive.

This method passively regenerates assets in your database based on the new tuning that you configured to resolve the asset growth issues. With this approach, all scan results and residual asset data are lost, but the data can be reclaimed by rerunning a scan or re-importing scan results.

### Procedure

1. To selectively remove invalid artifacts in the asset database, perform these steps:
  - a) On the **Log Activity** tab, run the **Deviating Asset Growth: Asset Report** event search.  
This search returns a report of assets that are affected by deviating asset growth and must be deleted.
  - b) On the **Assets** tab, click **Actions > Delete Asset**  
There might be a delay before the asset no longer appears in IBM Security QRadar.
2. To rebuild the asset database from scratch, perform these steps:
  - a) Use SSH to log in to the QRadar Console as an administrator.
  - b) Run the `/opt/qradar/support/cleanAssetModel.sh` script from the console command line and select **Option 1** when prompted.

Rebuilding the asset database restarts the asset reconciliation engine.


### Results

Purging a blacklist removes all blacklist entries, including those entries that were added manually. Blacklist entries that were manually added must be added again.

## Deleting blacklist entries

After you fixed the cause of the blacklist entries, you must clean up the remnant entries. You can remove the individual blacklist entries, however it is better to purge all blacklist entries and allow the blacklist values that are unrelated to the asset growth deviation to regenerate.

### Procedure

1. To purge a blacklist by using the IBM Security QRadar Console:
  - a) On the navigation menu () , click **Admin**.
  - b) In the **System Configuration** section, click **Reference Set Management**.
  - c) Select a reference set and then click **Delete**.
  - d) Use the quick search text box to search for the reference sets that you want to delete, and then click **Delete Listed**.
2. To purge a blacklist by using the QRadar Console command-line interface:
  - a) Change directory to `/opt/qradar/bin`.
  - b) Run the following command.

```
./ReferenceDataUtil.sh purge "Reference Collection Name"
```

where *Reference Collection Name* is one of the following lists:

- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation MAC Blacklist

### Results

Purging a blacklist removes all blacklist entries, including those entries that were added manually. Blacklist entries that were manually added must be added again.





## Chapter 19. Configuring QRadar systems to forward data to other systems

You can configure IBM Security QRadar systems to forward data to one or more vendor systems, such as ticketing or alerting systems. You can also forward normalized data to other QRadar systems. The target system that receives the data from QRadar is known as a *forwarding destination*.

With exception of domain tagging, QRadar systems ensure that all forwarded data is unaltered. Domain information is removed from forwarded data. Events and flows that contain domain information are automatically assigned to the default domain on the receiving system.

To avoid compatibility problems when sending event and flow data, ensure that the deployment receiving the data is the same version or higher than the deployment that is sending the data.

1. Configure one or more forwarding destinations.
2. To determine what data you want to forward, configure routing rules, custom rules, or both.
3. Configure the routing options to apply to the data.

For example, you can configure all data from a specific event collector to forward to a specific ticketing system. You can also bypass correlation by removing the data that matches a routing rule.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

## Adding forwarding destinations

Before you can configure routing rules or custom rules to forward data, you must add forwarding destinations. Normalized events that you forward can be interpreted only by other QRadar systems.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Forwarding Destinations**.
3. On the toolbar, click **Add**.
4. In the **Forwarding Destinations** window, enter values for the parameters.

The following table describes some of the **Forwarding Destinations** parameters.

| Table 66. <i>Forwarding Destinations</i> parameters |                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                           | Description                                                                                                                                                                                                                                                                                                                              |
| <b>Destination Address</b>                          | The IP address or host name of the vendor system that you want to forward data to.                                                                                                                                                                                                                                                       |
| <b>Event Format</b>                                 | <ul style="list-style-type: none"><li>• <b>Payload</b> is the data in the format that the log source or flow source sent.</li><li>• <b>Normalized</b> is raw data that is parsed and prepared as readable information for the user interface.</li><li>• <b>JSON</b> (Javascript Object Notation) is a data-interchange format.</li></ul> |

| Table 66. <b>Forwarding Destinations</b> parameters (continued) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Protocol</b>                                                 | Use the <b>TCP</b> protocol to send normalized data by using the TCP protocol. You must create an off-site source at the destination address on port 32004.<br><br><b>Restriction:</b> You cannot transmit normalized and JSON data by using the UDP protocol. If you select the <b>Normalized</b> or <b>JSON</b> options, the <b>UDP</b> option in the <b>Protocol</b> list is disabled.                                                                                                   |
| <b>Prefix a syslog header if it is missing or invalid</b>       | Applicable only when the event format is <b>Payload</b> .<br><br>When QRadar forwards syslog messages, the outbound message is verified to ensure that it has a valid syslog header.<br><br>If a valid syslog header is not detected and this check box is selected, the prefixed syslog header includes the originating IP address from the packet that QRadar received in the <b>Hostname</b> field of the syslog header. If this check box is not selected, the data is sent unmodified. |

5. Click **Save**.

### What to do next

Setting up a forwarding destination does not automatically send data to that destination. You must configure either a routing rule or a custom rule to forward data to the destination.

## Configuring forwarding profiles

If you want to specify which properties to forward to the forwarding destination, configure a forwarding profile.

You must re-create JSON forwarding profiles that you created in IBM Security QRadar V7.2.3 or earlier.

### About this task

You can use forwarding profiles only when the event data is sent in JSON format.

You can select specific event or flow properties, including custom properties, to forward to an external destination. You can enhance the readability of the event data by specifying an alias name and default value for the attribute. Alias names and default values are specific to the profile they are defined in. If the attributes are used in other profiles, the alias names and default values must be redefined.

You can use a single profile that has multiple forwarding destinations. When you edit a profile, ensure that the changes are appropriate for all forwarding destinations that the profile is associated with.

When you delete a profile, all forwarding destinations that used the profile automatically revert to using the default profile.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Forwarding Destinations**.
3. On the toolbar, click **Profile Manager**.
4. To create a new profile, click **New**.
5. Type a name for the profile and select the check box beside the attributes that you want to include in the event data set.
6. To change an existing profile, select the profile and click **Edit** or **Delete**.
7. Click **Save**.

## Configuring routing rules to forward data

---

Forward data by configuring filter-based routing rules.

### About this task

You can configure routing rules to forward data in either online or offline mode:

- In **Online** mode, your data remains current because forwarding is done in real time. If the forwarding destination becomes unreachable, any data sent to that destination is not delivered, resulting in missing data on that remote system. To ensure that delivery is successful, use offline mode.
- In **Offline** mode, all data is first stored in the database and then sent to the forwarding destination. This mode ensures that no data is lost; however, delays in data forwarding can occur.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Routing Rules**.
3. On the toolbar, click **Add**.
4. In the **Routing Rule** window, type a name and description for your routing rule.
5. In the **Mode** field, select one of the following options: **Online** or **Offline**.
6. In the **Forwarding Event Collector** or **Forwarding Event Processor** list, select the event collector from which you want to forward data.

#### Learn more about the forwarding appliance:

##### Forwarding Event Collector

Specifies the Event Collector that you want this routing rule to process data from. This option displays when you select the **Online** option.

**Note:** Online/Realtime forwarding is not impacted by any Rate Limit or Scheduling configurations that might be configured on a Store and Forward (15xx) event collectors.

##### Forwarding Event Processor

Specifies the Event Processor that you want this routing rule to process data from. This option is displayed when you select the **Offline** option.

**Restriction:** This option is not available if **Drop** is selected from the **Routing Options** pane.

7. In the **Data Source** field, select which data source you want to route: **Events** or **Flows**.

The labels for the next section change based on which data source you select.

8. Specify which events or flows to forward by applying filters:
  - a) To forward all incoming data, select the **Match All Incoming Events** or **Match All Incoming Flows** check box.

**Restriction:** If you select this check box, you cannot add a filter.

  - b) To forward only some events or flows, specify the filter criteria, and then click **Add Filter**.
9. Specify the routing options to apply to the forwarded data:
  - a) If you want to edit, add, or delete a forwarding destination, click the **Manage Destinations** link.
  - b) To forward log data that matches the specified filters, select the **Forward** check box and then select the check box for each forwarding destination.

**Restriction:** If you select the **Forward** check box, you can select only one of these check boxes: **Drop**, **Bypass Correlation**, or **Log Only**.

#### Learn more about routing options:

- The **Forward** option specifies that data is forwarded to the specified forwarding destination. Data is also stored in the database and processed by the Custom Rules Engine (CRE).

- The **Drop** option specifies that data is dropped. The data is not stored in the database and is not processed by the CRE. This option is not available if you select the **Offline** option. Any events that are dropped are credited back 100% to the license.
- The **Bypass Correlation** option specifies that data bypasses CRE, but it is stored in the database. This option is not available if you select the **Offline** option.
- The **Log Only (Exclude Analytics)** option specifies that events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available for flows.

**Note:** The **Log Only** option requires entitlement for QRadar Data Store, but is not currently enforced. In the future, when entitlement is enforced, access to the collected event data will be restricted to properly licensed systems. When the license is applied, and the **Log Only** option is selected, events that match the routing rule will be stored to disk and will be available to view and for searches. The events bypass the custom rule engine and no real-time correlation or analytics occur. The events can't contribute to offenses and are ignored when historical correlation runs. Some apps will also ignore Log Only events (<https://www.ibm.com/support/docview.wss?uid=swg22009471>).

You can combine three options:

- **Forward and Drop**

Data is forwarded to the specified forwarding destination. Data is not stored in the database and is not processed by the CRE.

- **Forward and Bypass Correlation**

Data is forwarded to the specified forwarding destination. Data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the data.

- **Forward and Log Only (Exclude Analytics)**

Events are forwarded to the specified forwarding destination in online mode. Events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available in offline mode.

If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database.

10. Click **Save**.


## Configuring routing rules to use the QRadar Data Store

A new offering, IBM QRadar Data Store, normalizes and stores both security and operational log data for future analysis and review. The offering supports the storage of an unlimited number of logs without counting against your organization's Events Per Second QRadar SIEM license, and enables your organization to build custom apps and reports based on this stored data to gain deeper insights into your environments.

### About this task

Using the **Log Only (Exclude Analytics)** option requires entitlement for QRadar Data Store, but is not currently enforced. In the future, when entitlement is enforced, access to the collected event data will be restricted to properly licensed systems. When the license is applied and the **Log Only (Exclude Analytics)** option is selected, events that match the routing rule will be stored to disk and will be available to view and for searches. The events bypass the custom rule engine and no real-time correlation or analytics occur. The events can't contribute to offenses and are ignored when historical correlation runs. Some apps will also ignore Log Only events (<https://www.ibm.com/support/docview.wss?uid=swg22009471>).

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Routing Rules**.
3. On the toolbar, click **Add**.
4. In the **Routing Rule** window, type a name and description for your routing rule.
5. In the **Mode** field, select **Online**.
6. In the **Forwarding Event Collector** list, select the event collector on which you want to apply the **Log Only (Exclude Analytics)** option.
7. In the **Data Source** field, select **Events**.
8. Specify which events to apply the **Log Only (Exclude Analytics)** option to by applying filters:
  - a) To apply the **Log Only (Exclude Analytics)** option to all incoming data, select the **Match All Incoming Events** check box.  
**Restriction:** If you select this check box, you cannot add a filter.
  - b) To apply the **Log Only (Exclude Analytics)** option to only some events, specify the filter criteria, and then click **Add Filter**.
9. To apply the **Log Only (Exclude Analytics)** option to log data that matches the specified filters, select **Log Only (Exclude Analytics)**.

**Note:** The **Log Only (Exclude Analytics)** option specifies that events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available for flows.

You can combine the **Forward** and **Log Only (Exclude Analytics)** options. Events are forwarded to the specified forwarding destination in online mode. Events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available in offline mode.

If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database.

10. Click **Save**.

## Using custom rules & rule responses to forward data

---

Use the **Custom Rule** wizard to configure forwarding of event data that matches rules in your system. Configure the rule response to forward event data to one or more forwarding destinations.

### About this task

The criteria that determines the event data that is sent to a forwarding destination is based on the tests and building blocks that are included in the rule.

When the rule is configured and enabled, all event data that matches the rule tests are automatically sent to the specified forwarding destinations. For more information about how to edit or add a rule, see the *IBM Security QRadar User Guide* for your product.

## Procedure

1. Click the **Offenses** or **Log Activity** tab.
2. On the **Rules** menu, select **Rules**.
3. In the **Rules List** window, select the rule to edit, or click **Actions** to create a new rule.
4. On the **Rule Response** page in the **Rule** wizard, ensure that you select the **Send to Forwarding Destinations** option.

# Viewing forwarding destinations

The **Forwarding Destinations** window provides valuable information about your forwarding destinations. Statistics for the data sent to each forwarding destination is displayed.

For example, you can see the following information:

- The total number events and flows that were seen for this forwarding destination.
- The number of events or flows that were sent to this forwarding destination.
- The number of events or flows that were dropped before the forwarding destination was reached.

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Forwarding Destinations**.
3. View the statistics for your forwarding destinations.

# Viewing and managing forwarding destinations

Use the **Forwarding Destination** window to view, edit, and delete forwarding destinations.

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Forwarding Destinations**.

Statistics for the data sent to each forwarding destination is displayed. For example, you can see the following information:

- The total number events and flows that were seen for this forwarding destination.
  - The number of events or flows that were sent to this forwarding destination.
  - The number of events or flows that were dropped before the forwarding destination was reached.
3. On the toolbar, click an action, as described in the following table.

| Table 67. Description of the <b>Forwarding Destination</b> toolbar actions |                                                                    |
|----------------------------------------------------------------------------|--------------------------------------------------------------------|
| Action                                                                     | Description                                                        |
|                                                                            |                                                                    |
|                                                                            | Changes the configured name, format, IP address, port, or protocol |
|                                                                            |                                                                    |

# Viewing and managing routing rules

Use the **Event Routing Rules** window to enable or disable the rules, or to edit a rule to change the configured name, Event Collector, filters, or routing options.

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Routing Rules**.
3. Select the routing rule you want to manage.
4. To edit the routing rule, on the toolbar, click **Edit** and update the parameters.

5. To remove the routing rule, on the toolbar, click **Delete**.
  6. To enable or disable the routing rule, on the toolbar, click **Enable/Disable**.
- If you enable a routing rule that is configured to drop events, a confirmation message is displayed.





---

## Chapter 20. Event store and forward

Use the Store and Forward feature to manage schedules for forwarding events from your dedicated Event Collector appliances to Event Processor components in your deployment.

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590. For more information about 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 by using the **Deployment Editor**. Use the Store and Forward feature to schedule a time range for when you want the Event Collector to forward events. During the time when events are not forwarding, the events are stored locally on the appliance. The events are not accessible in the IBM Security QRadar Console user interface.

Use the scheduling feature to store events during your business hours. Forward the events to an Event Processor when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to forward events to an Event Processor during non-business hours.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

### 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

Use the **Store and Forward** window to see a list of schedules. The schedules include statistics that help you evaluate the status, performance, and progress of your schedules.

#### Before you begin

You must create a schedule. By default, the first time that you access the **Store and Forward** window, no schedules are listed.

#### About this task

You can use options on the toolbar and the **Display** list box to change your view of the schedule list. Change your view of the list 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. The list then groups by the **Event Collector** column and makes it easier for you to locate the Event Collector that you want to investigate.

By default, the Store and Forward list is configured to display the list that is organized by the schedule (**Display > Schedules**).

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Store and Forward**.
3. In the **Store and Forward** window, view the parameters for each schedule.

The following table describes some of the parameters for the schedule.

| Table 68. <i>Store and Forward</i> window parameters |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Display                                              | <p>The <b>Schedules</b> option shows a hierarchy of the parent-child relationship between the schedules, event processors, and the associated event collectors.</p> <p>The <b>Event Collectors</b> option shows the lowest level in the hierarchy, which is a list of event collectors.</p> <p><b>Event Processors</b> option shows a hierarchy of the parent-child relationship between the event processors and the associated event collectors.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Name                                                 | <p>For the <b>Schedules</b> option, the <b>Name</b> column is displayed the following format.</p> <ul style="list-style-type: none"> <li>• <b>First Level</b> represents the name of the schedule.</li> <li>• <b>Second Level</b> represents the name of the event processor.</li> <li>• <b>Third Level</b> represents the name of the event collector.</li> </ul> <p>For the <b>Event Processors</b> option, the column is displayed in the following format</p> <ul style="list-style-type: none"> <li>• <b>First Level</b> represents the name of the event processor.</li> <li>• <b>Second Level</b> represents the name of the event collector.</li> </ul> <p><b>Tip:</b> 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 by using options on the toolbar.</p> |

Table 68. **Store and Forward** window parameters (continued)

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schedule Name    | <p>Displays the name of the schedule for the <b>Event Collectors</b> or <b>Event Processors</b> options.</p> <p>If an event processor is associated with more than one schedule, the <b>Schedule Name</b> shows <b>Multiplen</b>, where <i>n</i> is the number of schedules.</p> <p><b>Tip:</b> Click the plus symbol (+) to view the associated schedules.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Last Status      | <p>Displays the status of the Store and Forward process:</p> <ul style="list-style-type: none"> <li>• <b>Forwarding</b> indicates that event forwarding is in progress.</li> <li>• <b>Forward Complete</b> indicates that event forwarding is successfully completed and events are stored locally on the event collector. The stored events are forwarded when the schedule indicates that forwarding can start again.</li> <li>• <b>Warn</b> indicates that the percentage of events that are remaining in storage exceeds the percentage of time that is remaining in the Store and Forward schedule.</li> <li>• <b>Error</b> indicates that event forwarding was stopped before all stored events were forwarded.</li> <li>• <b>Inactive</b> indicates that no event collectors are assigned to the schedule, or the assigned event collectors are not receiving any events.</li> </ul> <p><b>Tip:</b> Move your mouse pointer over the <b>Last Status</b> column to view a summary of the status.</p> |
| Forwarded Events | <p>Displays the number of events (in K, M, or G) forwarded in the current session.</p> <p><b>Tip:</b> Move your mouse pointer over the value in the <b>Forwarded Events</b> column to view the number of events.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Remaining Events | <p>Displays the number of events (in K, M, or G) remaining to be forwarded in the current session.</p> <p><b>Tip:</b> Move your mouse pointer over the value in the <b>Remaining Events</b> column to view the number of events.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Table 68. <b>Store and Forward</b> window parameters (continued) |                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                        | Description                                                                                                                                                                                                                                              |
| Average Event Rate                                               | Displays the average rate at which events are forwarding from the event collector to the event processor.<br><br><b>Tip:</b> Move your mouse pointer over the value in the <b>Average Event Rate</b> column to view the average events per second (EPS). |
| Current® Event Rate                                              | Displays the rate at which events are forwarding from the event collector to the event processor.<br><br><b>Tip:</b> Move your mouse pointer over the value in the <b>Current Event Rate</b> column to view the current events per second (EPS)          |
| Transfer Rate Limit                                              | The transfer rate limit is configurable.<br><br>The transfer rate limit can be configured to display in kilobytes per second (KBs), megabytes per second (MBs), or gigabytes per second (GBs).                                                           |

## Creating a new Store and Forward schedule

Use the Store and Forward Schedule wizard to create a schedule that controls when your event collector starts and stops forwarding data to an event processor.

You can create and manage multiple schedules to control event forwarding from multiple IBM Security QRadar event collectors in a geographically distributed deployment.

### Before you begin

Ensure that your dedicated event collector is added to your deployment and connected to an event processor. The connection between an event collector and an event processor is configured in the **Deployment Editor**.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Store and Forward**.
3. Click **Actions > Create**.
  - a) Click **Next** to move to the **Select Collectors** page.
  - b) On the **Select Collectors** page, configure the parameters.  
  
If the event collector that you want to configure is not listed, you must add it before you can proceed. For more information about adding an event collector, see [“Adding a managed host” on page 60](#).
  - c) On the **Schedule Options** page, configure the parameters.  
  
**Note:** 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.
  - d) Finish the configuration.  
  
You can now view the schedule in the **Store and Forward** window. After you create a new schedule, it might take up to 10 minutes for statistics to start displaying in the **Store and Forward** window.

## Editing a Store and Forward schedule

---

You can edit a **Store and Forward** schedule to add or remove IBM Security QRadar event collectors and change the schedule parameters. After you edit a **Store and Forward** schedule, the statistics that are displayed in the **Store and Forward** list are reset.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Store and Forward**.
3. Select the schedule that you want to edit.
4. Click **Actions > Edit**.

You can also double-click a schedule for editing.

5. Click **Next** to move to the **Select Collectors** page.
6. On the **Select Collectors** page, edit the parameters.
7. Click **Next** to move to the **Schedule Options** page.
8. On the **Schedule Options** page, edit the scheduling parameters.
9. Click **Next** to move to the **Summary** page.
10. On the **Summary** page, confirm the options that you edited for this schedule.

After you edit a schedule, it might take up to 10 minutes for statistics to update in the **Store and Forward** window.

## Deleting a Store and Forward schedule

---

You can delete a **Store and Forward** schedule.

### Procedure

1. On the navigation menu, click **System Configuration**.
2. Click the **Store and Forward** icon.
3. Select the schedule that you want to delete.
4. Click **Actions > Delete**.

After the schedule is deleted, the associated IBM Security QRadar event collectors resume continuous forwarding of events to their assigned event processor.



---

## Chapter 21. Security content

You use the content management tools in IBM Security QRadar to import security content such as rules, reports, dashboards and applications into QRadar. Security content can come from other QRadar systems, or it can be developed independently to extend existing QRadar capabilities.

### **Related concepts**

Capabilities in your IBM Security QRadar product

---

### Types of security content

IBM Security QRadar content is bundled into two types: content packs and extensions.

#### **Content packs**

Security *content packs* contain enhancements to specific types of security content. Often, they include content for third-party integrations or operating systems. For example, a security content pack for a third-party integration might contain new custom event properties that make information in the event payload searchable for the log source and available for reporting.

Security content packs are available from IBM Fix Central (<http://www.ibm.com/support/fixcentral>). Content packs are not available as part of an auto-update.

#### **Extensions**

IBM and other vendors write security *extensions* that enhance or extend QRadar capabilities. An extension can contain apps, content items, such as custom rules, report templates, saved searches, or contain updates to existing content items. For example, an extension might include an app to add a tab in QRadar that provides visualizations for an offense.

On IBM Security App Exchange, extensions are known as apps. You can download QRadar apps from IBM Security App Exchange and use the **Extensions Management** tool to install them. Apps are not available as part of an auto-update.

#### **Sources of security content**

QRadar content is available from the following sources:

##### **IBM Security App Exchange**

IBM Security App Exchange (<https://apps.xforce.ibmcloud.com>) is an app store and portal where you can browse and download QRadar extensions. It is a new way to share code, visualizations, reports, rules, and applications.

##### **IBM Fix Central**

IBM Fix Central ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)) provides fixes and updates to your system software, hardware, and operating system. You can download security content packs and extensions from IBM Fix Central.

##### **QRadar deployments**

You export custom content from a QRadar deployment as an extension and then import it into another system when you want to reuse the content. For example, you can export content from your development environment to your production environment. You can use the content management script to export all content, or you can choose to export only some custom content.

## Methods of importing and exporting content

---

You can use the following tools to import and export content in your IBM Security QRadar deployment.

### Extensions Management tool

Use the **Extensions Management** tool to add extensions to your QRadar deployment. When you import content using the **Extensions Management** tool, you can view the content before it is installed. If the content items exist in your system, you can specify whether to replace the content item or skip the update.

You cannot use the **Extensions Management** tool to export content.

### Content management script

Use the content management script to export custom content from your QRadar deployment into an external, portable format. You can then use the script to import the custom content into another QRadar deployment. The script is useful when you want to automate moving content between your QRadar deployments.

The `contentManagement.pl` script is in the `/opt/qradar/bin` directory.

You must use the content management script to export content from the QRadar source deployment. You can use either the content management script or the **Extensions Management** tool to import the content to the target deployment.

**Note:** You can export content from an earlier version of QRadar and import into a later version. However, you cannot import content from a later version into an earlier version.

**Note:** If you migrate override rules from one QRadar deployment to another, use the **Replace Existing Content Items** option to ensure that the rules are imported correctly.

## Exporting all custom content

You use the `contentManagement.pl` script to export all custom content in your IBM Security QRadar deployment.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to `/opt/qradar/bin` directory, and type the command to export all of the custom content:

```
./contentManagement.pl -a export -c all
```

### Examples:

- To include accumulated data in the export, type the following command:

```
./contentManagement.pl --action export --content-type all -g
```

- To specify the directory for the exported file and change the compression format, type the following command:

```
./contentManagement.pl -a export -c all -o [filepath] -t [compression_type]
```

### Results

The content is exported to a compressed file, for example, `all-ContentExport-20151022101803.zip`. You can manually change the file name to a name that is more descriptive. The exported file might contain more content items than expected because all dependencies are exported with the specified content items. For example, if you export a report, the saved search that the report uses is also exported.



## Exporting all custom content of a specific type

You can export all custom content of a specific type in one action.

### About this task

The content management script uses text identifiers or numeric identifiers to specify the type of content that you want to export.

| Table 69. Content type identifiers for exporting custom content                                                     |                              |                    |
|---------------------------------------------------------------------------------------------------------------------|------------------------------|--------------------|
| Custom content type                                                                                                 | Text identifier              | Numeric identifier |
| Dashboards                                                                                                          | <b>dashboard</b>             | 4                  |
| Reports                                                                                                             | <b>report</b>                | 10                 |
| Saved searches                                                                                                      | <b>search</b>                | 1                  |
| FGroups <sup>1</sup>                                                                                                | <b>fgroup</b>                | 12                 |
| FGroup types                                                                                                        | <b>fgrouptype</b>            | 13                 |
| Custom rules                                                                                                        | <b>customrule</b>            | 3                  |
| Custom properties                                                                                                   | <b>customproperty</b>        | 6                  |
| Log sources                                                                                                         | <b>sensordevice</b>          | 17                 |
| Log source types                                                                                                    | <b>sensordevicetype</b>      | 24                 |
| Log source categories                                                                                               | <b>sensordevicecategory</b>  | 18                 |
| Log source extensions                                                                                               | <b>deviceextension</b>       | 16                 |
| Reference data collections                                                                                          | <b>referencedata</b>         | 28                 |
| Custom QID map entries                                                                                              | <b>qidmap</b>                | 27                 |
| Historical correlation profiles                                                                                     | <b>historicalsearch</b>      | 25                 |
| Custom functions                                                                                                    | <b>custom_function</b>       | 77                 |
| Custom actions                                                                                                      | <b>custom_action</b>         | 78                 |
| Applications                                                                                                        | <b>installed_application</b> | 100                |
| DSM event mapping                                                                                                   | <b>dsmevent</b>              | 41                 |
| <sup>1</sup> An FGroup represents a group of content, such as a log source group, reporting group, or search group. |                              |                    |

### Procedure

1. Use SSH to log in to IBM Security QRadar as the root user.
2. Go to the `/opt/qradar/bin` directory and type the command to export all content of the specified type:

```
./contentManagement.pl -a export --content-type [content_type] --id all
```

### Parameters:

| Table 70. <i>contentManagement.pl</i> script parameters for exporting custom content of a specific type |                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                                               | Description                                                                                                                                                                                                                                                                                                             |
| <b>-c</b> <i>[content_type]</i><br>or<br><b>--content-type</b> <i>[content_type]</i>                    | Specifies the type of content.<br><br>You can type the corresponding text or numeric identifier to specify the content type.                                                                                                                                                                                            |
| <b>-e</b><br>or<br><b>--include-reference-data-elements</b>                                             | Set this flag to include reference data keys and elements in the export.<br><br>Reference data keys and reference data elements are applicable to the <code>referencedata</code> content type. This parameter is applicable only when you export reference data, or content items that are dependent on reference data. |
| <b>-g</b><br>or<br><b>--global-view</b>                                                                 | Includes accumulated data in the export.                                                                                                                                                                                                                                                                                |
| <b>-i</b> <i>[content_identifier]</i><br>or<br><b>--id</b> <i>[content_identifier]</i>                  | Specifies the identifier of a specific instance of custom content such as a single report or a single reference set.<br><br>You can specify <i>all</i> to export all content of the specified type.                                                                                                                     |
| <b>-o</b> <i>[filepath]</i><br>or<br><b>--output-directory</b> <i>[filepath]</i>                        | Specifies the full path to the directory where the export file is written.<br><br>If no output directory is specified, the content is exported to the current directory. If the specified output directory does not exist, it is created.                                                                               |
| <b>-t</b> <i>[compression_type]</i><br>or<br><b>--compression-type</b> <i>[compression_type]</i>        | Specifies the compression type of the export file.<br><br>Valid options are ZIP and TARGZ (case sensitive). If you do not specify a compression type, the default compression type is ZIP.                                                                                                                              |

#### Examples:

- To export all custom searches, type the following command:

```
./contentManagement.pl --action export --content-type search --id all
```

- To export all reports and include accumulated data, type the following command:

```
./contentManagement.pl -a export -c 10 --id all --global-view
```

#### Results

The content is exported to a compressed file, for example, `reports-ContentExport-20151022101803.zip`. You can manually change the file name to a name that is more descriptive. The exported file might contain more content items than expected because all dependencies are exported with the specified content items. For example, if you export a report, the saved search that the report uses is also exported.

## Searching for specific content items to export

You use the content management script to search for specific content in your IBM Security QRadar deployment. After you find the content, you can use the unique identifier to export the content item.

### About this task

The following table lists the identifiers to use when you want to search for specific types of content.

| Table 71. Content type identifiers for searching custom content                                                     |                              |                    |
|---------------------------------------------------------------------------------------------------------------------|------------------------------|--------------------|
| Custom content type                                                                                                 | Text identifier              | Numeric identifier |
| Dashboards                                                                                                          | <b>dashboard</b>             | 4                  |
| Reports                                                                                                             | <b>report</b>                | 10                 |
| Saved searches                                                                                                      | <b>search</b>                | 1                  |
| FGroups <sup>1</sup>                                                                                                | <b>fgroup</b>                | 12                 |
| FGroup types                                                                                                        | <b>fgrouptype</b>            | 13                 |
| Custom rules                                                                                                        | <b>customrule</b>            | 3                  |
| Custom properties                                                                                                   | <b>customproperty</b>        | 6                  |
| Log sources                                                                                                         | <b>sensordevice</b>          | 17                 |
| Log source types                                                                                                    | <b>sensordevicetype</b>      | 24                 |
| Log source categories                                                                                               | <b>sensordevicecategory</b>  | 18                 |
| Log source extensions                                                                                               | <b>deviceextension</b>       | 16                 |
| Reference data collections                                                                                          | <b>referencedata</b>         | 28                 |
| Custom QID map entries                                                                                              | <b>qidmap</b>                | 27                 |
| Historical correlation profiles                                                                                     | <b>historicalsearch</b>      | 25                 |
| Custom functions                                                                                                    | <b>custom_function</b>       | 77                 |
| Custom actions                                                                                                      | <b>custom_action</b>         | 78                 |
| Applications                                                                                                        | <b>installed_application</b> | 100                |
| <sup>1</sup> An FGroup represents a group of content, such as a log source group, reporting group, or search group. |                              |                    |

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to the `/opt/qradar/bin` directory and type the following command to search for custom content that matches a regular expression:

```
./contentManagement.pl -a search -c [content_type] -r [regex]
```

#### Parameters:

| Table 72. contentManagement.pl script parameters for searching content items |                                                                                                                                                                                               |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                    | Description                                                                                                                                                                                   |
| <b>-c</b> [content_type]<br>or<br><b>--content-type</b> [content_type]       | Specifies the type of content to search for.<br><br>You must specify the type of content to search for. You cannot use <code>-c package</code> or <code>-c all</code> with the search action. |

| Table 72. <i>contentManagement.pl</i> script parameters for searching content items (continued) |                                                                                               |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Parameter                                                                                       | Description                                                                                   |
| <b>-r</b> <i>[regex]</i><br>or<br><b>--regex</b> <i>[regex]</i>                                 | Specifies the content to search for.<br>All content that matches the expression is displayed. |

#### Examples:

- To search for all reports that includes Overview in the description, type the following command:

```
/opt/qradar/bin/contentManagement.pl --action search
--content-type report --regex "Overview"
```

- To list all log sources, type the following command:

```
/opt/qradar/bin/contentManagement.pl -a search -c 17 -r "\w"
```

The search results list details, including the unique ID, for the content items that are found.

```
[INFO] Search results:
[INFO] - [ID] - [Name] - [Description]
[INFO] - [67] - [Asset Profiler-2 :: hostname] - [Asset Profiler]
[INFO] - [62] - [SIM Generic Log DSM-7 :: hostname] - [SIM Generic Log DSM]
[INFO] - [63] - [Custom Rule Engine-8 :: hostname] - [Custom Rule Engine]
[INFO] - [71] - [Pix @ apophis] - [Pix device]
[INFO] - [70] - [Snort @ wolverine] - [Snort device]
[INFO] - [64] - [SIM Audit-2 :: hostname] - [SIM Audit]
[INFO] - [69] - [Health Metrics-2 :: hostname] - [Health Metrics]
```

#### What to do next

Use the unique identifier to export specific content items from QRadar. For more information, see [“Exporting custom content items of different types” on page 258](#) and [“Exporting a single custom content item” on page 256](#).

## Exporting a single custom content item

Export a single custom content item, such as a custom rule or a saved search, from IBM Security QRadar.

#### Before you begin

You must know the unique identifier for the custom content item that you want to export. For information about finding the unique identifiers for content items, see [“Searching for specific content items to export” on page 255](#).

#### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to the `/opt/qradar/bin` directory and type the command to export the content:

```
./contentManagement.pl -a export -c [content_type] -i [content_identifier]
```

#### Parameters:

| Table 73. <i>contentManagement.pl</i> script parameters for exporting a single content item      |                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                                        | Description                                                                                                                                                                                                                                                                                                       |
| <b>-c</b> <i>[content_type]</i><br>or<br><b>--content-type</b> <i>[content_type]</i>             | Specifies the type of content to export.<br><br>Type the <u>corresponding text identifier or numeric identifier for specific content types</u> .                                                                                                                                                                  |
| <b>-e</b><br>or<br><b>--include-reference-data-elements</b>                                      | Set this flag to include reference data keys and elements in the export.<br><br>Reference data keys and reference data elements are applicable to the <u>referencedata</u> content type. This parameter is applicable only when you export reference data, or content items that are dependent on reference data. |
| <b>-g</b><br>or<br><b>--global-view</b>                                                          | Includes accumulated data in the export.                                                                                                                                                                                                                                                                          |
| <b>-i</b> <i>[content_identifier]</i><br>or<br><b>--id</b> <i>[content_identifier]</i>           | Specifies the <u>identifier of a specific instance of custom content</u> such as a single report or a single reference set.                                                                                                                                                                                       |
| <b>-o</b> <i>[filepath]</i><br>or<br><b>--output-directory</b> <i>[filepath]</i>                 | Specifies the full path to the directory where the export file is written.<br><br>If no output directory is specified, the content is exported to the current directory. If the specified output directory does not exist, it is created.                                                                         |
| <b>-t</b> <i>[compression_type]</i><br>or<br><b>--compression-type</b> <i>[compression_type]</i> | Used with the export action.<br><br>Specifies the compression type of the export file. Valid options are ZIP and TARGZ (case sensitive). If you do not specify a compression type, the default compression type is ZIP.                                                                                           |

### Examples:

- To export the dashboard that has ID 7 into the current directory, type the following command:

```
./contentManagement.pl -a export -c dashboard -i 7
```

- To export the log source that has ID 70, including accumulated data, into the `/store/cmt/exports` directory, type the following command:

```
./contentManagement.pl -a export -c sensordevice -i 70 -o /store/cmt/exports -g
```

### Results

The content is exported to a compressed `.zip` file. The exported file might contain more content items than expected because all dependencies are exported with the specified content items. For example, if you export a report, the saved search that the report uses is also exported. You can manually change the file name to a name that is more descriptive.

## Exporting custom content items of different types

Export multiple custom content items from IBM Security QRadar, such as custom rules, or dashboards and reports, by using the content management script.

### Before you begin

You must know the unique identifiers for each custom content item that you want to export. For information about finding the unique identifiers for content items, see [“Searching for specific content items to export”](#) on page 255.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Create a text file that lists the content that you want to export.

Each line must include the custom content type followed by a comma-separated list of unique IDs for that type.

**Example:** To export two dashboards that have ID 5 and ID 7, all custom rules, and a group, create a text file that has the following entries:

```
dashboard, 5,7
customrule, all
fgroup, 77
```

3. Go to `/opt/qradar/bin` and type the command to export the content:

```
./contentManagement.pl -a export -c package -f [source_file]
```

### Parameters:

| Table 74. <i>contentManagement.pl</i> script parameters for exporting different types of content item |                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                |
| <b>-c</b> [content_type]<br>or<br><b>--content-type</b> [content_type]                                | Specifies the type of content.<br><br>You can specify <code>-c package</code> , or you can type the <a href="#">corresponding text or numeric identifier for specific content types</a> . When you use <code>-c package</code> , you must specify the <code>--file</code> or <code>--name</code> parameters.                                               |
| <b>-e</b><br>or<br><b>--include-reference-data-elements</b>                                           | Set this flag to include reference data keys and elements in the export.<br><br>Reference data keys and reference data elements are applicable to the <code>referencedata</code> content type. This parameter is applicable only when you export reference data, or content items that are dependent on reference data.                                    |
| <b>-f</b> [source_file]<br>or<br><b>--file</b> [source_file]                                          | Specifies the path and file name of the text file that contains the list of custom content items that you want to export.<br><br>The first time you use the <code>--file</code> parameter, a package template file is written to the <code>/store/cmt/packages</code> directory so that you can reuse it.<br><br>The filename and path are case-sensitive. |

| Table 74. <i>contentManagement.pl</i> script parameters for exporting different types of content item (continued) |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>-g</b><br>or<br><b>--global-view</b>                                                                           | Includes accumulated data in the export.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>-n</b> <i>[name]</i><br>or<br><b>--name</b> <i>[name]</i>                                                      | Specifies the name of the package template file that contains the list of custom content to export.<br><br>The package template file is created the first time that you use the <b>--file</b> parameter. By default, the <b>--name</b> parameter assumes that the text file is in the <code>/store/cmt/packages</code> directory.<br><br>You must specify the <b>--file</b> or <b>--name</b> parameter when <b>--content-type package</b> is used. |
| <b>-o</b> <i>[filepath]</i><br>or<br><b>--output-directory</b> <i>[filepath]</i>                                  | Specifies the full path to the directory where the export file is written.<br><br>If no output directory is specified, the content is exported to the current directory. If the specified output directory does not exist, it is created.                                                                                                                                                                                                          |
| <b>-t</b> <i>[compression_type]</i><br>or<br><b>--compression-type</b> <i>[compression_type]</i>                  | Specifies the compression type of the export file.<br><br>Valid compression types are ZIP and TARGZ (case sensitive). If you do not specify a compression type, the default compression type is ZIP.                                                                                                                                                                                                                                               |

### Examples:

- To export all items in the `exportlist.txt` file in the `qradar` directory, and save the exported file in the current directory, type the following command:

```
./contentManagement.pl -a export -c package -f /qradar/exportlist.txt
```

- To export all items in the `exportlist.txt` file in the `qradar` directory, including accumulated data, and save the output in the `/store/cmt/exports` directory, type the following command:

```
./contentManagement.pl -a export -c package
```

```
--file /qradar/exportlist.txt -o /store/cmt/exports -g
```

When you use the **--file** parameter, a package template file is automatically generated in `/store/cmt/packages`. To use the package template file, specify the filename as the value for the **--name** parameter.

### Results

The content is exported to a compressed `.zip` file. The exported file might contain more content items than expected because all dependencies are exported with the specified content items. For example, if you export a report, the saved search that the report uses is also exported. You can manually change the file name to a name that is more descriptive.

## Installing extensions by using Extensions Management

Use the **Extensions Management** tool to add security extensions to IBM Security QRadar. The **Extensions Management** tool lets you view the content items in the extension and specify the method of handling content updates before you install the extension.

### Before you begin

Extensions must be on your local computer before you install them in QRadar.

You can download QRadar extensions from the IBM Security App Exchange (<https://apps.xforce.ibmcloud.com/>) and from IBM Fix Central ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)).

### About this task

An extension is a bundle of QRadar functionality. An extension can include content such as rules, reports, searches, reference sets, and dashboards. It can also include applications that enhance QRadar functionality.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Extensions Management**.
3. To upload a new extension to the QRadar console, follow these steps:
  - a) Click **Add**.
  - b) Click **Browse** and navigate to find the extension.
  - c) Click **Install immediately** to install the extension without viewing the contents.
  - d) Click **Add**.
4. To view the contents of the extension, select it from the extensions list and click **More Details**.
5. To install the extension, follow these steps:
  - a) Select the extension from the list and click **Install**.
  - b) To assign a user to the app, select the **User Selection** menu, and then select a user. For example, you might want to associate the app with a specified user that is listed in the User Selection menu who has the defined permissions.

#### Note:

This screen appears only if any of the apps in the extension that you are installing are configured to request authentication for background processes.

- c) If the extension does not include a digital signature, or it is signed but the signature is not associated with the IBM Security Certificate Authority (CA), you must confirm that you still want to install it. Click **Install** to proceed with the installation.
- d) Review the changes that the installation makes to the system.
- e) Select **Preserve Existing Items** or **Replace Existing Items** to specify how to handle existing content items.

**Note:** If the extension contains overridden system rules, select **Replace Existing Items** to ensure that the rules are imported correctly.
- f) Click **Install**.
- g) Review the installation summary and click **OK**.



# Importing content by using the content management script

You can import custom content that you exported from another IBM Security QRadar system.

## Before you begin

If you want to import content from another QRadar system, you must first export the content and copy it to the target system. For more information about exporting content, see [“Content type identifiers for exporting custom content”](#) on page 263.

When you import content that has log sources, confirm that DSM and protocol RPMs are installed and current on the target system.

**Note:** If the content contains overridden system rules, use the update action instead of import to ensure that the rules are imported correctly.

You can export content from an earlier version of QRadar and import into a later version. However, you cannot import content from a later version into an earlier version.

You do not have to export content in a specific order. However, do not start multiple imports on the same system at the same time. The imports will fail due to conflicts with shared resources.

## Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to the directory where the export content file is located.
3. Type this command to import the content:

```
/opt/qradar/bin/contentManagement.pl -a import -f [source_file] -u [user]
```

### Parameters:

| Table 75. contentManagement.pl script parameters for importing custom content |                                                                                                                                                                 |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                     | Description                                                                                                                                                     |
| <b>-f</b> [source_file]<br>or<br><b>--file</b> [source_file]                  | Specifies the file that contains the content items to import.<br><br>Valid file types are zip, targz, and xml.<br><br>The filename and path are case-sensitive. |
| <b>-u</b> [user]<br>or<br><b>--user</b> [user]                                | Specifies the user that replaces the current owner when you import user-specific data. The user must exist on the target system before you import the content.  |

### Examples:

- To import content from the fgroup-ContentExport-20120418163707.tar.gz file in the current directory, type the following command:

```
/opt/qradar/bin/contentManagement.pl --action import
-f fgroup-ContentExport-20120418163707.tar.gz
```

- To import content from the fgroup-ContentExport-20120418163707.tar.gz file in the current directory and make the admin user the owner of all sensitive data in the import, type the following command:

```
/opt/qradar/bin/contentManagement.pl --action import
--file fgroup-ContentExport-20120418163707.tar.gz --user admin
```

The import script displays the following message when reference data is actively collected while it is being exported: Foreign key constraint violation. To avoid this issue, run the export process when no reference data is being collected.

### Related tasks

[“Updating content by using the content management script” on page 262](#)

Use the update action to update existing IBM Security QRadar content or add new content to the system.

## Updating content by using the content management script

Use the update action to update existing IBM Security QRadar content or add new content to the system.

### Before you begin

If you want to update content with content that was exported from another QRadar system, ensure that the exported file is on the target system. For more information about exporting content, see [“Content type identifiers for exporting custom content” on page 263](#).

When you import content that has log sources, confirm that DSM and protocol RPMs are installed and current on the target system.

You can export content from an earlier version of QRadar and import into a later version. However, you cannot import content from a later version into an earlier version.

You do not have to export content in a specific order. However, do not start multiple imports on the same system at the same time. The imports will fail due to conflicts with shared resources.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. To update content, type the following command:

```
/opt/qradar/bin/contentManagement.pl -a update -f [source_file]
```

### Parameters:

| Table 76. contentManagement.pl script parameters for updating custom content |                                                                                                                                                                       |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                                    | Description                                                                                                                                                           |
| <b>-f</b> [source_file]<br>or<br><b>--file</b> [source_file]                 | Specifies the file that contains the content items to update.<br><br>Valid file types are zip, targz, and xml.<br><br>The filename and path are case-sensitive.       |
| <b>-u</b> [user]<br>or<br><b>--user</b> [user]                               | Specifies the user that replaces the current owner when you import user-specific data.<br><br>The user must exist on the target system before you import the content. |

### Example:

- To update based on the content in the fgroup-ContentExport-20120418163707.zip file, type the following command:

```
/opt/qradar/bin/contentManagement.pl --action update
-f fgroup-ContentExport-20120418163707.zip
```

## Manually installing content packs from IBM Fix Central

Install the content pack by using the command line.

### Procedure

1. Download the content pack (RPM file) from [IBM Fix Central](http://www.ibm.com/support/fixcentral) ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)).
2. Copy the RPM file to QRadar Console.
3. Use SSH to log in to QRadar as the root user.
4. From the directory that includes the downloaded file, type the following command:  

```
rpm -Uvh filename
```
5. Log in to the QRadar as an administrator.
6. On the navigation menu (☰), click **Admin**.
7. Select **Advanced** > **Restart Web Server**.

## Content type identifiers for exporting custom content

When you export a specific type of custom content from IBM Security QRadar, you must specify the content type. You must use either the text identifier or the numeric identifier for the content type.

When you export content from a QRadar appliance, the content management script checks content dependencies, and then includes associated content in the export.

For example, when the content management script detects that a saved search is associated with a report that you want to export, the saved search is also exported. You can't export offense, asset, or vulnerability saved searches.

You use the content type identifier when you want to export all custom content of a specific type. If you want to export a specific content item from your QRadar deployment, you must know the unique identifier for that specific content item. For more information, see [“Searching for specific content items to export”](#) on page 255.

The following table describes the content type identifiers that are passed into the `contentManagement.pl` script for the `-c` parameter.

| Table 77. Content type identifiers for exporting custom content |                             |                    |
|-----------------------------------------------------------------|-----------------------------|--------------------|
| Custom content type                                             | Text identifier             | Numeric identifier |
| All custom content                                              | <b>all</b>                  | Not applicable     |
| Custom list of content                                          | <b>package</b>              | Not applicable     |
| Dashboards                                                      | <b>dashboard</b>            | 4                  |
| Reports                                                         | <b>report</b>               | 10                 |
| Saved searches                                                  | <b>search</b>               | 1                  |
| FGroups <sup>1</sup>                                            | <b>fgroup</b>               | 12                 |
| FGroup types                                                    | <b>fgrouptype</b>           | 13                 |
| Custom rules                                                    | <b>customrule</b>           | 3                  |
| Custom properties                                               | <b>customproperty</b>       | 6                  |
| Log sources                                                     | <b>sensordevice</b>         | 17                 |
| Log source types                                                | <b>sensordevicetype</b>     | 24                 |
| Log source categories                                           | <b>sensordevicecategory</b> | 18                 |

| Table 77. Content type identifiers for exporting custom content (continued)                                |                              |                    |
|------------------------------------------------------------------------------------------------------------|------------------------------|--------------------|
| Custom content type                                                                                        | Text identifier              | Numeric identifier |
| Log source extensions                                                                                      | <b>deviceextension</b>       | 16                 |
| Reference data collections                                                                                 | <b>referencedata</b>         | 28                 |
| Custom QID map entries                                                                                     | <b>qidmap</b>                | 27                 |
| Historical correlation profiles                                                                            | <b>historicalsearch</b>      | 25                 |
| Custom functions                                                                                           | <b>custom_function</b>       | 77                 |
| Custom actions                                                                                             | <b>custom_action</b>         | 78                 |
| Applications                                                                                               | <b>installed_application</b> | 100                |
| <sup>1</sup> An FGroup is a group of content such as a log source group, reporting group, or search group. |                              |                    |

## Content management script parameters

Use the `contentManagement.pl` script to export content from one IBM Security QRadar deployment and import it to another deployment.

The following table describes the parameters for the `contentManagement.pl` script and the actions to which each parameter applies.

```
/opt/qradar/bin/contentManagement.pl --action [action_type] [script_parameters]
```

| Table 78. <code>contentManagement.pl</code> script parameters          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>-a</b> [action_type]<br>or<br><b>--action</b> [action_type]         | Required. Specifies the action.<br><br>Valid action types are <code>export</code> , <code>search</code> , <code>import</code> , and <code>update</code> .<br><br>The <code>import</code> action adds only content that does not exist in the deployment.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>-c</b> [content_type]<br>or<br><b>--content-type</b> [content_type] | Used with the <code>export</code> and <code>search</code> actions. Specifies the type of content.<br><br>When used with the <code>export</code> action, you can specify <code>-c all</code> or <code>-c package</code> , or you can type the corresponding text or numeric identifier for specific content types. When you use <code>-c package</code> , you must specify the <code>--file</code> or <code>--name</code> parameters.<br><br>When used with the <code>search</code> action, you must specify the type of content to search for. You cannot use <code>-c package</code> or <code>-c all</code> with the <code>search</code> action. |
| <b>-d</b><br>or<br><b>--debug</b>                                      | Used with all actions.<br><br>Use debug level logging when you run the <code>contentManagement.pl</code> script to see more detailed information, such as logs for customer support.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 78. *contentManagement.pl* script parameters (continued)

| Parameter                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-e</b><br>or<br><b>--include-reference-data-elements</b>                            | <p>Used with the <code>export</code> action.</p> <p>Set this flag to include reference data keys and elements in the export.</p> <p>Reference data keys and reference data elements are applicable to the <code>referencedata</code> content type. This parameter is applicable only when you export reference data, or content items that are dependent on reference data.</p>                                                                                                                                                                                                                                                                                                                                                   |
| <b>-f</b> <i>[file_path]</i><br>or<br><b>--file</b> <i>[file_path]</i>                 | <p>Used with <code>export</code>, <code>import</code>, and <code>update</code> actions.</p> <p>When used with the <code>export</code> action, specifies the path and file name of the text file that contains the list of custom content items that you want to export. The first time you use the <code>--file</code> parameter, a package template file is written to the <code>/store/cmt/packages</code> directory so that you can reuse it.</p> <p>When used with the <code>import</code> or <code>update</code> action, specifies the file that contains the content items to import. Valid file types are <code>zip</code>, <code>targz</code>, and <code>xml</code>.</p> <p>The filename and path are case-sensitive.</p> |
| <b>-g</b><br>or<br><b>--global-view</b>                                                | <p>Used with the <code>export</code> action.</p> <p>Includes accumulated data in the export.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>-h</b> <i>[action_type]</i><br>or<br><b>--help</b> <i>[action_type]</i>             | <p>Used with all actions.</p> <p>Displays help that is specific to the <code>action_type</code>. When no <code>action_type</code> is specified, displays a general help message.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>-i</b> <i>[content_identifier]</i><br>or<br><b>--id</b> <i>[content_identifier]</i> | <p>Used with the <code>export</code> action.</p> <p>Specifies the identifier of a specific instance of custom content such as a single report or a single reference set. You can specify <i>all</i> to export all content of the specified type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>-n</b> <i>[name]</i><br>or<br><b>--name</b> <i>[name]</i>                           | <p>Used with the <code>export</code> action.</p> <p>Specifies the name of the package template file that contains the list of custom content to export.</p> <p>The package template file is created the first time that you use the <code>--file</code> parameter. The <code>--name</code> parameter assumes that the package template file is in the <code>/store/cmt/packages</code> directory.</p> <p>You must specify the <code>--file</code> or <code>--name</code> parameter when <code>--content-type package</code> is used.</p>                                                                                                                                                                                          |

Table 78. *contentManagement.pl* script parameters (continued)

| Parameter                                                                                        | Description                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-o</b> <i>[filepath]</i><br>or<br><b>--output-directory</b> <i>[filepath]</i>                 | <p>Used with the <code>export</code> action.</p> <p>Specifies the full path to the directory where the export file is written.</p> <p>If no output directory is specified, the content is exported to the current directory. If the specified output directory does not exist, it is created.</p> |
| <b>-q</b><br>or<br><b>--quiet</b>                                                                | <p>Used with all actions. No output appears on the screen.</p>                                                                                                                                                                                                                                    |
| <b>-r</b> <i>[regex]</i><br>or<br><b>--regex</b> <i>[regex]</i>                                  | <p>Used with the <code>search</code> action.</p> <p>When searching, you must use the <code>--regex</code> parameter to specify the content to search for. All content that matches the expression is displayed.</p>                                                                               |
| <b>-t</b> <i>[compression_type]</i><br>or<br><b>--compression-type</b> <i>[compression_type]</i> | <p>Used with the <code>export</code> action.</p> <p>Specifies the compression type of the export file. Valid compression types are ZIP and TARGZ (case sensitive). If you do not specify a compression type, the default compression type is ZIP.</p>                                             |
| <b>-u</b> <i>[user]</i><br>or<br><b>--user</b> <i>[user]</i>                                     | <p>Used with the <code>import</code> action.</p> <p>Specifies the user that replaces the current owner when you import user-specific data. The user must exist on the target system before you import the content.</p>                                                                            |
| <b>-v</b><br>or<br><b>--verbose</b>                                                              | <p>Used with all actions.</p> <p>Use when you log in to view default-level information for the content management tool.</p>                                                                                                                                                                       |

---

## Chapter 22. SNMP trap configuration

IBM Security QRadar uses the Net-SNMP agent, which supports various system resource monitoring MIBs. They can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information about Net-SNMP, see Net-SNMP documentation.

In IBM Security QRadar, you can configure a rule to generate a rule response that sends an SNMP trap when configured conditions are met. QRadar acts as an agent to send the SNMP traps to another system.

A Simple Network Management Protocol (SNMP) trap is an event or offense notification that QRadar sends to a configured SNMP host for additional processing.

Customize the SNMP configuration parameters in the custom rules wizard and modify the SNMP traps that the custom rule engine sends to other software for management. QRadar provides two default traps. However, you can add custom traps or modify the existing traps to use new parameters.

For more information on SNMP, go to the [The Internet Engineering Task Force](http://www.ietf.org/) (<http://www.ietf.org/>) website and type RFC 1157 in the search field.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

## Customizing the SNMP trap information sent to another system

In IBM Security QRadar, you can edit the SNMP trap parameters to customize the information that is sent to another SNMP managing system when a rule condition is met.

**Restriction:** The SNMP trap parameters are displayed in the custom rules wizard only if SNMP is enabled in the QRadar system settings.

### Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to the `/opt/qradar/conf` directory and make backup copies of the following files:
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
3. Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the `eventCRE.snmp.xml` file.
  - To edit the SNMP parameters for offense rules, open the `offenseCRE.snmp.xml` file.
4. Inside the `<snmp>` element and before the `<creSNMPTrap>` element, insert the following section, updating the labels as needed:

```
<creSNMPResponse name="snmp_response_1">
 <custom name="MyColor">
 <string label="What is your favorite color?"/>
 </custom>
 <custom name="MyCategory">
 <list label="Select a category">
 <option label="Label1" value="Category1"/>
 <option label="Label2" value="Category2"/>
 </list>
 </custom>
</creSNMPResponse>
```

5. Save and close the file.
6. Copy the file from the `/opt/qradar/conf` directory to the `/store/configservices/staging/globalconfig` directory.
7. Log in to the QRadar interface.

- On the **Admin** tab, select **Advanced > Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

### What to do next

[Customize the SNMP trap output..](#)

## Customizing the SNMP trap output

IBM Security QRadar uses SNMP to send traps that provide information when rule conditions are met.

By default, QRadar uses the QRadar management information base (MIB) to manage the devices in the communications network. However, you can customize the output of the SNMP traps to adhere to another MIB.

### Procedure

- Use SSH to log in to QRadar as the root user.
- Go to the `/opt/qradar/conf` directory and make backup copies of the following files:
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
- Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the `eventCRE.snmp.xml` file.
  - To edit the SNMP parameters for offense rules, open the `offenseCRE.snmp.xml` file.
- To change the trap that is used for SNMP trap notification, update the following text with the appropriate trap object identifier (OID):

```
-<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
name="eventCRENotification">
```

- Use the following table to help you update the variable binding information:

Each variable binding associates a particular MIB object instance with its current value.


Table 79. Value types for variable binding		
Value type	Description	Example
string	Alphanumeric characters You can configure multiple values.	
integer32	A numerical value	<code>name="ATTACKER_PORT" type="integer32"&gt;%ATTACKER_PORT%</code>
oid	Each SNMP trap carries an identifier that is assigned to an object within the MIB	<code>OID="1.3.6.1.4.1.20212.2.46"</code>



Table 79. Value types for variable binding (continued)		
Value type	Description	Example
gauge32	A numerical value range	
counter64	A numerical value that increments within a defined minimum and maximum range	

6. For each of the value types, include any of the following fields:

Table 80. Fields for the variable bindings		
Field	Description	Example
Native	For more information about these fields, see the /opt/qradar/conf/snmp.help file.	<b>Example:</b> <sup>1</sup> If the value type is ipAddress, you must use a variable that is an IP address. The string value type accepts any format.
Custom	Custom SNMP trap information that you configured for the custom rules wizard	<b>Example:</b> <sup>1</sup> If you used the default file information and want to include this information in the SNMP trap, include the following code: <pre>&lt;variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"&gt; My favorite color is %MyColor%&lt;/variableBinding&gt;</pre>
<sup>1</sup> Surround the field name with percentage (%) signs. Within the percentage signs, fields must match the value type.		

7. Save and close the file.
8. Copy the file from the /opt/qradar/conf directory to the /store/configservices/staging/globalconfig directory.
9. Log in to the QRadar as an administrator.
10. On the navigation menu () , click **Admin**.
11. Select **Advanced > Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

### Related information

[Adding a custom SNMP trap to QRadar](#)

# Adding a custom SNMP trap to QRadar

In IBM Security QRadar products, you can create a new option for the SNMP trap selection in the custom rules wizard. The trap names that are specified in the list box are configured in the `snmp-master.xml` configuration file.

## Procedure

1. Use SSH to log in to QRadar as the root user.
2. Go to the `/opt/qradar/conf` directory.
3. Create an SNMP settings file for the new trap.  
**Tip:** Copy, rename, and modify one of the existing SNMP settings files.
4. Make a backup copy of the `snmp-master.xml` file.
5. Open the `snmp-master.xml` file for editing.
6. Add a new `<include>` element.

The `<include>` element has the following attributes:

Table 81. Attributes for the <code>&lt;include&gt;</code> element	
Attribute	Description
name	Displayed in the list box
uri	The name of the custom SNMP settings file

For Example:

```
<include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
```

The traps are displayed in the menu in the same order in which they are listed in the `snmp-master.xml` file.

7. Save and close the file.
8. Copy the `snmp-master.xml` file and the `customSNMPdef01.xml` file from the `/opt/qradar/conf` directory to the `/store/configservices/staging/globalconfig` directory.
9. Log in to the QRadar interface.
10. Log in to the QRadar as an administrator.
11. On the navigation menu (☰), click **Admin**.
12. Select **Advanced > Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.

## Related information

[Customizing the SNMP trap output](#)

# Sending SNMP traps to a specific host

By default, in IBM Security QRadar products, SNMP traps are sent to the host that is identified in your `host.conf` file. You can customize the `snmp.xml` file to send SNMP traps to a different host.

## Procedure


1. Use SSH to log in to QRadar as the root user.

2. Go to the /opt/qradar/conf directory and make backup copies of the following files:
  - eventCRE.snmp.xml
  - offenseCRE.snmp.xml
3. Open the configuration file for editing.
  - To edit the SNMP parameters for event rules, open the eventCRE.snmp.xml file.
  - To edit the SNMP parameters for offense rules, open the offenseCRE.snmp.xml file.
4. Add no more than one <trapConfig> element inside the <snmp> element inside the <creSNMPTrap> element and before any other child elements.

```
<trapConfig>
 <!-- All attribute values are default -->
 <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST
 </snmpHost>
 <!-- Community String for Version 2 -->
 <communityString>COMMUNITY_STRING</communityString>
 <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
 or NOAUTH_PRIV) -->
 <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
 AUTH_PASSWORD
 </authentication>
 <!-- decryptionProtocol (DES, AES128, AES192 or AES256) -->
 <decryption decryptionProtocol="AES256">
 DECRYPTIONPASSWORD
 </decryption>
 <!-- SNMP USER-->
 <user> SNMP_USER </user>
</trapConfig>
```

5. Use the following table to help you update the attributes.

Table 82. Attribute values to update in the <trapConfig> element	
Element	Description
</snmpHost>	The new host to which you want to send SNMP traps.  The value for the snmpVersion attribute for <snmpHost> element must be 2 or 3.
<communityString>	The community string for the host
<authentication>	An authentication protocol, security level, and password for the host.
<decryption>	The decryption protocol and password for the host.
<user>	SNMP user

6. Save and close the file.
7. Copy the file from the /opt/qradar/conf directory to the /store/configservices/staging/globalconfig directory.
8. Log in to the QRadar as an administrator.
9. On the navigation menu () , click **Admin**.
10. Select **Advanced** > **Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays with the option to cancel the deployment and restart the service at a more convenient time.



---

## Chapter 23. Protect sensitive data

Configure a data obfuscation profile to prevent unauthorized access to sensitive or personal identifiable information in IBM Security QRadar.

*Data obfuscation* is the process of strategically hiding data from QRadar users. You can hide custom properties, normalized properties, such as user names, or you can hide the content of a payload, such as credit card or social security numbers.

The expressions in the data obfuscation profile are evaluated against the payload and normalized properties. If the data matches the obfuscation expression, the data is hidden in QRadar. Users who try to query the database directly cannot see the sensitive data. The data must be reverted back to its original form, or *deobfuscated*, by uploading the private key that was generated when the data obfuscation profile was created.

To ensure that QRadar can still correlate on the hidden data values, the obfuscation process is deterministic. It displays the same set of characters each time the data value is found.

### **Related concepts**

[Capabilities in your IBM Security QRadar product](#)

---

## How does data obfuscation work?

Before you configure data obfuscation in your IBM Security QRadar deployment, you must understand how it works for new and existing offenses, assets, rules, and log source extensions.

### **Existing event data**

When a data obfuscation profile is enabled, the system masks the data for each event as it is received by QRadar. Events that are received by the appliance before data obfuscation is configured remain in the original unobfuscated state. The older event data is not masked and users can see the information.

### **Assets**

When data obfuscation is configured, the asset model accumulates data that is masked while the pre-existing asset model data remains unmasked.

To prevent someone from using unmasked data to trace the obfuscated information, purge the asset model data to remove the unmasked data. QRadar will repopulate the asset database with obfuscated values.

### **Offenses**

To ensure that offenses do not display data that was previously unmasked, close all existing offenses by resetting the SIM model. For more information, see [“Resetting SIM” on page 67](#).

### **Rules**

You must update rules that depend on data that was previously unmasked. For example, rules that are based on a specific user name do not fire when the user name is obfuscated.

### **Log source extensions**

Log source extensions that change the format of the event payload can cause issues with data obfuscation.

## Data obfuscation profiles

The data obfuscation profile contains information about which data to mask. It also tracks the keystore that is required to decrypt the data.

### Enabled profiles

Enable a profile only when you are sure that the expressions correctly target the data that you want to obfuscate. If you want to test the regular expression before you enable the data obfuscation profile, you can create a regex-based custom property.

A profile that is enabled immediately begins obfuscating data as defined by the enabled expressions in the profile. The enabled profile is automatically locked. Only the user who has the private key can disable or change the profile after it is enabled.

To ensure that obfuscated data can be traced back to an obfuscation profile, you cannot delete a profile that was enabled, even after you disable it.

### Locked profiles

A profile is automatically locked when you enable it, or you can lock it manually.

A locked profile has the following restrictions:

- You cannot edit it.
- You cannot enable or disable it. You must provide the keystore and unlock the profile before you can change it.
- You cannot delete it, even after it is unlocked.
- If a keystore is used with a profile that is locked, all other profiles that use that keystore are automatically locked.

The following table shows examples of profiles that are locked or unlocked:

Table 83. Locked profile examples	
Scenario	Result
Profile A is locked. It was created by using keystore A. Profile B is also created by using keystore A.	Profile B is automatically locked.
Profile A is created and enabled.	Profile A is automatically locked.
Profile A, Profile B, and Profile C are currently locked. All were created by using keystore A. Profile B is selected and <b>Lock/Unlock</b> is clicked.	Profile A, Profile B, and Profile C are all unlocked.

## Data obfuscation expressions

Data obfuscation expressions identify the data to hide. You can create data obfuscation expressions that are based on field-based properties or you can use regular expressions.

### Field-based properties

Use a field-based property to hide user names, group names, host names, and NetBIOS names. Expressions that use field-based properties obfuscate all instances of the data string. The data is hidden regardless of its log source, log source type, event name, or event category.

If the same data value exists in more than one of the fields, the data is obfuscated in all fields that contain the data even if you configured the profile to obfuscate only one of the four fields. For example, if you have a host name that is called `IBMHost` and a group name that is called `IBMHost`, the value `IBMHost` is

obfuscated in both the host name field and the group name field even if the data obfuscation profile is configured to obfuscate only host names.

## Regular expressions

Use a regular expression to obfuscate one data string in the payload. The data is hidden only if it matches the log source, log source type, event name, or category that is defined in the expression.

You can use high-level and low-level categories to create a regular expression that is more specific than a field-based property. For example, you can use the following regex patterns to parse user names:

Table 84. Regex user name parsing	
Example regex patterns	Matches
<code>userName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*(@[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])?.)+[a-zA-Z]{2,20})\$</code>	john_smith@EXAMPLE.com, jon@example.com, jon@us.example.com
<code>userName=(^[[\\w]+[^\W])((^[\\W]\.?)([\\w]+[^\W]\$))</code>	john.smith, John.Smith, john, jon_smith
<code>userName=^([a-zA-Z][a-zA-Z-]*[\\w_-]*[\\S]\$ ^[a-zA-Z-][0-9_-]*[\\S]\$ ^[a-zA-Z]*[\\S]\$)</code>	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
<code>userName=(/S+)</code>	Matches any non-white space after the equal, =, sign. This regular expression is non-specific and can lead to system performance issues.
<code>msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*)@b((([01]?d?d 2[0-4]d 25[0-5])\.){3}([01]?d?d 2[0-4]d 25[0-5])b</code>	Matches users with IP address. For example, john.smith@192.0.2.0
<code>src=b((([01]?d?d 2[0-4]d 25[0-5])\.){3}([01]?d?d 2[0-4]d 25[0-5])b</code>	Matches IP address formats.
<code>host=^((([a-zA-Z0-9] [a-zA-Z0-9][a-zA-Z0-9-]*[a-zA-Z0-9])\.)*([A-Za-z0-9] [A-Za-z0-9][A-Za-z0-9-]*[A-Za-z0-9]))\$</code>	hostname.example.com, hostname.co.uk

## Scenario: Obfuscating user names

You are an IBM Security QRadar administrator. Your organization has an agreement with the workers union that all personal identifiable information must be hidden from QRadar users. You want to configure QRadar to hide all user names.

Use the **Data Obfuscation Management** feature on the **Admin** tab to configure QRadar to hide the data:

1. Create a data obfuscation profile and download the system-generated private key. Save the key in a secure location.
2. Create the data obfuscation expressions to target the data that you want to hide.
3. Enable the profile so that the system begins to obfuscate the data.
4. To read the data in QRadar, upload the private key to deobfuscate the data.

## Creating a data obfuscation profile

IBM Security QRadar uses data obfuscation profiles to determine which data to mask, and to ensure that the correct keystore is used to unmask the data.

### About this task

You can create a profile that creates a new keystore or you can use an existing keystore. If you create a keystore, it must be downloaded and stored in a secure location. Remove the keystore from the local system and store it in a location that can be accessed only by users who are authorized to view the unmasked data.

Configuring profiles that use different keystores is useful when you want to limit data access to different groups of users. For example, create two profiles that use different keystores when you want one group of users to see user names and another group of users to see host names.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, click **Data Obfuscation Management**.
3. To create a new profile, click **Add** and type a unique name and description for the profile.
4. To create a new keystore for the profile, complete these steps:
  - a) Click **System generate keystore**.
  - b) In the **Provider** list box, select **IBMJCE**.
  - c) In the **Algorithm** list box, select **JCE** and select whether to generate 512-bit or 1024-bit encryption keys.  
In the **Keystore Certificate CN** box, the fully qualified domain name for the QRadar server is auto-populated.
  - d) In the **Keystore password** box, enter the keystore password.  
The keystore password is required to protect the integrity of the keystore. The password must be at least 8 characters in length.
  - e) In the **Verify keystore password**, retype the password.
5. To use an existing keystore with the profile, complete these steps:
  - a) Click **Upload keystore**.
  - b) Click **Browse** and select the keystore file.
  - c) In the **Keystore password** box, type the password for the keystore.
6. Click **Submit**.
7. Download the keystore.  
Remove the keystore from your system and store it in a secure location.

### What to do next

[Create the data obfuscation expressions](#) that target the data that you want to hide.

## Creating data obfuscation expressions

The data obfuscation profile uses expressions to specify which data to hide. The expressions can use either field-based properties or regular expressions.

### About this task

After an expression is created, you cannot change the type. For example, you cannot create a property-based expression and then later change it to a regular expression.

You cannot obfuscate a normalized numeric field, such as port number or an IP address.



Multiple expressions that obfuscate the same data cause data to be obfuscated twice. To decrypt data that is obfuscated multiple times, each keystore that is used in the obfuscation process must be applied in the order that the obfuscation occurred.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, click **Data Obfuscation Management**.
3. Click the profile that you want to configure, and click **View Contents**.  
You cannot configure profiles that are locked.
4. To create a new data obfuscation expression, click **Add** and type a unique name and description for the profile.
5. Select the **Enabled** check box to enable the profile.
6. To create a field-based expression, click **Field Based** and select the field type to obfuscate.
7. To create a regular expression, click **Regex** and configure the regex properties.
8. Click **Save**.

## Deobfuscating data so that it can be viewed in the console

When data obfuscation is configured on an IBM Security QRadar system, the masked version of the data is shown throughout the application. You must have both the corresponding keystore and the password to deobfuscate the data so that it can be viewed.

### Before you begin

You must be an administrator and have the private key and the password for the key before you can deobfuscate data. The private key must be on your local computer.

### About this task

Before you can see the obfuscated data, you must upload the private key. After the key is uploaded, it remains available on the system for the duration of the current session. The session ends when you log out of QRadar, when the cache is cleared on the QRadar Console, or when there is an extended period of inactivity. When the session ends, the private keys that were uploaded in the previous session are no longer visible.

QRadar can use the keys available in the current session to automatically deobfuscate data. With auto-deobfuscation enabled, you do not have to repeatedly select the private key on the **Obfuscation Session Key** window each time that you want to view the data. Auto-deobfuscate is automatically disabled when the current session ends.

### Procedure

1. On the **Event Details** page, find the data that you want to deobfuscate.
2. To deobfuscate identity-based data:
  - a) Click the lock icon next to the data that you want to deobfuscate.
  - b) In the **Upload Key** section, click **Select File** and select the keystore to upload.
  - c) In the **Password** box, type the password that matches the keystore.
  - d) Click **Upload**.

The **Deobfuscation** window shows the event payload, the profile names that are associated with the keystore, the obfuscated text, and the deobfuscated text.

- e) Optional: Click **Toggle Auto Deobfuscate** to enable auto-deobfuscation.

After you toggle the auto-deobfuscation setting, you must refresh the browser window and reload the event details page for the changes to appear.

3. To deobfuscate payload data that is not identity-based:
  - a) On the toolbar on the **Event Details** page, click **Obfuscation > Deobfuscation keys**.
  - b) In the **Upload Key** section, click **Select File** and select the private key to upload.
  - c) In the **Password** box, type the password that matches the private key and click **Upload**.
  - d) In the **Payload information** box, select and copy the obfuscated text to the clipboard.
  - e) On the toolbar on the **Event Details** page, click **Obfuscation > Deobfuscation**.
  - f) Paste the obfuscated text in to dialog box.
  - g) Select the obfuscation profile from the drop-down list and click **Deobfuscate**.

## Editing or disabling obfuscation expressions created in previous releases

When you upgrade to IBM Security QRadar V7.2.6, data obfuscation expressions that were created in previous releases are automatically carried forward and continue to obfuscate data. These expressions appear in a single data obfuscation profile, named **AutoGeneratedProperty**.

Although you can see the expressions, you cannot edit or disable data obfuscation expressions that were created in earlier versions. You must manually disable them and create a data obfuscation profile that contains the revised expressions.

### About this task

To disable an old expression, you must edit the `xml` configuration file that defines the attributes for the expression. You can then run the `obfuscation_updater.sh` script to disable it.

Ensure that you disable old expressions before you create new expressions that obfuscate the same data. Multiple expressions that obfuscate the same data cause the data to be obfuscated twice. To decrypt data that is obfuscated multiple times, each keystore that is used in the obfuscation process must be applied in the order that the obfuscation occurred.

### Procedure

1. Use SSH to log in to your QRadar Console as the root user.
2. Edit the obfuscation expressions `.xml` configuration file that you created when you configured the expressions.
3. For each expression that you want to disable, change the **Enabled** attribute to `false`.
4. To disable the expressions, run the `obfuscation_updater.sh` script by typing the following command:

```
obfuscation_updater.sh [-p <path_to_private_key>] [-e
<path_to_obfuscation_xml_config_file>]
```

The `obfuscation_updater.sh` script is in the `/opt/qradar/bin` directory, but you can run the script from any directory on your QRadar Console.

### What to do next

Create a [data obfuscation profile](#) to obfuscate data and manage obfuscation expressions directly in QRadar.

# Chapter 24. Log files

Operations performed in IBM Security QRadar are recorded in log files for tracking purposes. Log files can help you troubleshoot problems by recording the activities that take place when you work with a product.

The following log files can help you identify and resolve problems when they occur:

- /var/log/qradar.log
- /var/log/qradar.error
- /var/log/qradar-sql.log
- /opt/tomcat6/logs/catalina.out
- /var/log/qflow.debug

If you want to collect the QRadar log files and review them later, see [“Collecting log files” on page 66](#).

## Related concepts

[Capabilities in your IBM Security QRadar product](#)

## Audit logs

Changes that are made by IBM Security QRadar users are recorded in the audit logs.

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches 200 MB. The current log file is named `audit.log`. When the file reaches 200 MB, the file is compressed and renamed to `audit.1.gz`. The file number increments each time that a log file is archived. QRadar stores up to 50 archived log files.

## Viewing the audit log file

Use Secure Shell (SSH) to log in to your IBM Security QRadar system and monitor changes to your system.

### About this task

You can use **Log Activity** tab to view normalized audit log events.

The maximum size of any audit message, excluding date, time, and host name, is 1024 characters.

Each entry in the log file displays by using the following format:

`<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>`

The following table describes the log file format options.

Table 85. Description of the parts of the log file format	
File format part	Description
<i>date_time</i>	The date and time of the activity in the format: Month Date HH:MM:SS
<i>host name</i>	The host name of the Console where this activity was logged.
<i>user</i>	The name of the user who changed the settings.
<i>IP address</i>	The IP address of the user who changed the settings.

Table 85. Description of the parts of the log file format (continued)	
File format part	Description
<i>thread ID</i> )	The identifier of the Java™ thread that logged this activity.
<i>category</i>	The high-level category of this activity.
<i>sub-categor</i>	The low-level category of this activity.
<i>action</i>	The activity that occurred.
<i>payload</i>	The complete record, which might include the user record or event rule, that changed.

### Procedure

1. Using SSH, log in to QRadar as the root user:
2. **User Name:** root
3. **Password:** *password*
4. Go to the following directory:  
    /var/log/audit
5. Open and view the audit log file.

### Related tasks

[“Creating reports from audit log searches in QRadar” on page 280](#)

To help you track how users interact with IBM Security QRadar, create reports that are based on your search results.


## Creating reports from audit log searches in QRadar

To help you track how users interact with IBM Security QRadar, create reports that are based on your search results.

### Procedure

1. Click **Log Activity > Add Filter**.
2. In the **Add Filter** window, configure the following settings:

Table 86. Settings to configure	
Settings to configure	Value
<b>Parameter</b>	Log Source [Indexed]
<b>Operator</b>	Equals
<b>Log Source</b>	SIM Audit-2

3. Click **Add Filter**.
4. If events are streaming into the **Log Activity** tab, click **Pause** (.
5. From the **View** list, select a time interval.
6. To save the search, click **Save Criteria**, provide a name for the search, and then click **OK**.
7. To generate a report from your search result, follow these steps:

- a) From the **Reports** tab, click **Actions > Create**.
- b) Follow the report wizard.
- c) In the **Saved Searches** field, type the name of the search that you created for the SIM audit log source.
- d) Click **Save Container Details**.
- e) Finish the report wizard pages.

## Logged actions

The IBM Security QRadar audit logs are in the `/var/log/audit` directory.

The following list describes the categories of actions that are in the audit log file:

### Administrator Authentication

- Log in to the Administration Console.
- Log out of the Administration Console.

### Assets

- Delete an asset.
- Delete all assets.

### Audit Log Access

A search that includes events that have a high-level event category of Audit.

### Backup and Recovery

- Edit the configuration.
- Initiate the backup.
- Complete the backup.
- Fail the backup.
- Delete the backup.
- Synchronize the backup.
- Cancel the backup.
- Upload a backup.
- Upload an invalid backup.
- Initiate the restore.
- Purge the backup.

### Chart Configuration

Save flow or event chart configuration.

### Content Management

- Content export initiated.
- Content export complete.
- Content import initiated.
- Content import complete.
- Content update initiated.
- Content update complete.
- Content search initiated.
- Applications added.
- Applications modified.
- Custom actions added.

- Custom actions modified.
- Ariel property added.
- Ariel property modified.
- Ariel property expression added.
- Ariel property expression modified.
- CRE rule added.
- CRE rule modified.
- Dashboard added.
- Dashboard modified.
- Device extension added.
- Device extension modified.
- Device extension association modified.
- Grouping added.
- Grouping modified.
- Historical correlation profile added.
- Historical correlation profile modified.
- QID map entry added.
- QID map entry modified.
- Reference data created.
- Reference data updated.
- Security profile added.
- Security profile modified.
- Sensor device added.
- Sensor device modified.

### **Custom Properties**

- Add a custom event property.
- Edit a custom event property.
- Delete a custom event property.
- Edit a custom flow property.
- Delete a custom flow property.

### **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.

### **Flow Sources**

- Add a flow source.
- Edit a flow source.
- Delete a flow source.

## **Groups**

- Add a group.
- Delete a group.
- Edit a group.

## **Historical Correlation**

- Add a historical correlation profile.
- Delete a historical correlation profile.
- Modify a historical correlation profile.
- Enable a historical correlation profile.
- Disable a historical correlation profile.
- Historical correlation profile is running.
- Historical correlation profile is canceled.

## **Licensing**

- Add a license key.
- Delete a license key.
- Delete license pool allocation.
- Update license pool allocation.

## **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.

## **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.

## **IBM Security QRadar Vulnerability Manager**

- Create a scanner schedule.
- Update a scanner schedule.
- Delete a scanner schedule.
- Start a scanner schedule.
- Pause a scanner schedule.
- Resume a scanner schedule.

## **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.

## **Retention Buckets**

- Add a bucket.
- Delete a bucket.
- Edit a bucket.
- Enable or disable a bucket.

## **Root Login**

- Log in to QRadar, as root user.
- Log out of QRadar, as root user.

## **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.

## **Session Authentication**

- Create an 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**

- Shut down a system.
- Restart a system.

## **User Accounts**

- Add an account.
- Edit an account.
- Delete an account.

## **User Authentication**

- Log in to the user interface.
- Log out of the user interface.

## **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.

**VIS**

- Discover a new host.
- Discover a new operating system.
- Discover a new port.
- Discover a new vulnerability.

## Chapter 25. Event categories

Event categories are used to group incoming events for processing by IBM Security QRadar. The event categories are searchable and help you monitor your network.

Events that occur on your network are aggregated into high-level and low-level categories. Each high-level category contains low-level categories and an associated severity level and ID number.

You can review the severity levels that are assigned to events and adjust them to suit your corporate policy needs.

You can run an AQL query by using high-level and low-level event category IDs. The category IDs for the associated category names can be retrieved from the event category tables.

For example, if you are developing applications on QRadar, you can run an AQL search similar to the following query from the command line, to gather data from Ariel:

```
select qidname(qid) as 'Event', username as 'Username', devicetime as 'Time'
from events where '<high-level category ID>' and '<Low-level category ID>' and
LOGSOURCENAME(logsourceid) like "%Low-level category name%" last 3 days
```

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

## High-level event categories

Events in IBM Security QRadar log sources are grouped into high-level categories. Each event is assigned to a specific high-level category.

Categorizing the incoming events ensures that you can easily search the data.

The following table describes the high-level event categories.

Table 87. High-level event categories		
Category	Category ID	Description
<a href="#">“Recon” on page 288</a>	1000	Events that are related to scanning and other techniques that are used to identify network resources, for example, network or host port scans.
<a href="#">“DoS” on page 290</a>	2000	Events that are related to denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.
<a href="#">“Authentication” on page 293</a>	3000	Events that are related to authentication controls, group, or privilege change, for example, log in or log out.
<a href="#">“Access” on page 302</a>	4000	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
<a href="#">“Exploit” on page 304</a>	5000	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
<a href="#">“Malware” on page 306</a>	6000	Events that are related to viruses, trojans, back door attacks, or other forms of hostile software. Malware events might include a virus, trojan, malicious software, or spyware.

Table 87. High-level event categories (continued)

Category	Category ID	Description
<a href="#">“Suspicious Activity” on page 308</a>	7000	The nature of the threat is unknown but behavior is suspicious. The threat might include protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known intrusion detection system (IDS) evasion techniques.
<a href="#">“System” on page 312</a>	8000	Events that are related to system changes, software installation, or status messages.
<a href="#">“Policy” on page 317</a>	9000	Events regarding corporate policy violations or misuse.
<a href="#">“Unknown” on page 319</a>	10000	Events that are related to unknown activity on your system.
<a href="#">“CRE” on page 320</a>	12000	Events that are generated from an offense or event rule.
<a href="#">“Potential Exploit” on page 320</a>	13000	Events relate to potential application exploits and buffer overflow attempts.
<a href="#">Flow</a>	14000	Events that are related to flow actions.
<a href="#">“User Defined” on page 323</a>	15000	Events that are related to user-defined objects.
<a href="#">“SIM Audit” on page 326</a>	16000	Events that are related to user interaction with the Console and administrative functions.
<a href="#">“VIS Host Discovery” on page 327</a>	17000	Events that are related to the host, ports, or vulnerabilities that the VIS component discovers.
<a href="#">“Application” on page 328</a>	18000	Events that are related to application activity.
<a href="#">“Audit” on page 353</a>	19000	Events that are related to audit activity.
<a href="#">“Risk” on page 357</a>	20000	Events that are related to risk activity in IBM Security QRadar Risk Manager.
<a href="#">“Risk Manager Audit” on page 358</a>	21000	Events that are related to audit activity in QRadar Risk Manager.
<a href="#">“Control” on page 359</a>	22000	Events that are related to your hardware system.
<a href="#">“Asset Profiler” on page 361</a>	23000	Events that are related to asset profiles.
<a href="#">Sense</a>	24000	Events that are related to UBA.

## Recon

The Recon category contains events that are related to scanning and other techniques that are used to identify network resources.

The following table describes the low-level event categories and associated severity levels for the Recon category.

*Table 88. Low-level categories and severity levels for the Recon events category*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Form of Recon	1001	An unknown form of reconnaissance.	2
Application Query	1002	Reconnaissance to applications on your system.	3
Host Query	1003	Reconnaissance to a host in your network.	3
Network Sweep	1004	Reconnaissance on your network.	4
Mail Reconnaissance	1005	Reconnaissance on your mail system.	3
Windows Reconnaissance	1006	Reconnaissance for Windows operating system.	3
Portmap / RPC r \Request	1007	Reconnaissance on your portmap or RPC request.	3
Host Port Scan	1008	Indicates that a scan occurred on the host ports.	4
RPC Dump	1009	Indicates that Remote Procedure Call (RPC) information is removed.	3
DNS Reconnaissance	1010	Reconnaissance on the DNS server.	3
Misc Reconnaissance Event	1011	Miscellaneous reconnaissance event.	2
Web Reconnaissance	1012	Web reconnaissance on your network.	3
Database Reconnaissance	1013	Database reconnaissance on your network.	3
ICMP Reconnaissance	1014	Reconnaissance on ICMP traffic.	3
UDP Reconnaissance	1015	Reconnaissance on UDP traffic.	3
SNMP Reconnaissance	1016	Reconnaissance on SNMP traffic.	3
ICMP Host Query	1017	Indicates an ICMP host query.	3
UDP Host Query	1018	Indicates a UDP host query.	3

*Table 88. Low-level categories and severity levels for the Recon events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
NMAP Reconnaissance	1019	Indicates NMAP reconnaissance.	3
TCP Reconnaissance	1020	Indicates TCP reconnaissance on your network.	3
UNIX Reconnaissance	1021	Reconnaissance on your UNIX network.	3
FTP Reconnaissance	1022	Indicates FTP reconnaissance.	3

## DoS

The DoS category contains events that are related to denial-of-service (DoS) attacks against services or hosts.

The following table describes the low-level event categories and associated severity levels for the DoS category.

*Table 89. Low-level categories and severity levels for the DoS events category*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown DoS Attack	2001	Indicates an unknown DoS attack.	8
ICMP DoS	2002	Indicates an ICMP DoS attack.	9
TCP DoS	2003	Indicates a TCP DoS attack.	9
UDP DoS	2004	Indicates a UDP DoS attack.	9
DNS Service DoS	2005	Indicates a DNS service DoS attack.	8
Web Service DoS	2006	Indicates a web service DoS attack.	8
Mail Service DoS	2007	Indicates a mail server DoS attack.	8
Distributed DoS	2008	Indicates a distributed DoS attack.	9
Misc DoS	2009	Indicates a miscellaneous DoS attack.	8
UNIX DoS	2010	Indicates a UNIX DoS attack.	8
Windows DoS	2011	Indicates a Windows DoS attack.	8

Table 89. Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Database DoS	2012	Indicates a database DoS attack.	8
FTP DoS	2013	Indicates an FTP DoS attack.	8
Infrastructure DoS	2014	Indicates a DoS attack on the infrastructure.	8
Telnet DoS	2015	Indicates a Telnet DoS attack.	8
Brute Force Login	2016	Indicates access to your system through unauthorized methods.	8
High Rate TCP DoS	2017	Indicates a high rate TCP DoS attack.	8
High Rate UDP DoS	2018	Indicates a high rate UDP DoS attack.	8
High Rate ICMP DoS	2019	Indicates a high rate ICMP DoS attack.	8
High Rate DoS	2020	Indicates a high rate DoS attack.	8
Medium Rate TCP DoS	2021	Indicates a medium rate TCP attack.	8
Medium Rate UDP DoS	2022	Indicates a medium rate UDP attack.	8
Medium Rate ICMP DoS	2023	Indicates a medium rate ICMP attack.	8
Medium Rate DoS	2024	Indicates a medium rate DoS attack.	8
Low Rate TCP DoS	2025	Indicates a low rate TCP DoS attack.	8
Low Rate UDP DoS	2026	Indicates a low rate UDP DoS attack.	8
Low Rate ICMP DoS	2027	Indicates a low rate ICMP DoS attack.	8
Low Rate DoS	2028	Indicates a low rate DoS attack.	8
Distributed High Rate TCP DoS	2029	Indicates a distributed high rate TCP DoS attack.	8
Distributed High Rate UDP DoS	2030	Indicates a distributed high rate UDP DoS attack.	8

Table 89. Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Distributed High Rate ICMP DoS	2031	Indicates a distributed high rate ICMP DoS attack.	8
Distributed High Rate DoS	2032	Indicates a distributed high rate DoS attack.	8
Distributed Medium Rate TCP DoS	2033	Indicates a distributed medium rate TCP DoS attack.	8
Distributed Medium Rate UDP DoS	2034	Indicates a distributed medium rate UDP DoS attack.	8
Distributed Medium Rate ICMP DoS	2035	Indicates a distributed medium rate ICMP DoS attack.	8
Distributed Medium Rate DoS	2036	Indicates a distributed medium rate DoS attack.	8
Distributed Low Rate TCP DoS	2037	Indicates a distributed low rate TCP DoS attack.	8
Distributed Low Rate UDP DoS	2038	Indicates a distributed low rate UDP DoS attack.	8
Distributed Low Rate ICMP DoS	2039	Indicates a distributed low rate ICMP DoS attack.	8
Distributed Low Rate DoS	2040	Indicates a distributed low rate DoS attack.	8
High Rate TCP Scan	2041	Indicates a high rate TCP scan.	8
High Rate UDP Scan	2042	Indicates a high rate UDP scan.	8
High Rate ICMP Scan	2043	Indicates a high rate ICMP scan.	8
High Rate Scan	2044	Indicates a high rate scan.	8
Medium Rate TCP Scan	2045	Indicates a medium rate TCP scan.	8
Medium Rate UDP Scan	2046	Indicates a medium rate UDP scan.	8
Medium Rate ICMP Scan	2047	Indicates a medium rate ICMP scan.	8
Medium Rate Scan	2048	Indicates a medium rate scan.	8



<i>Table 89. Low-level categories and severity levels for the DoS events category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Low Rate TCP Scan	2049	Indicates a low rate TCP scan.	8
Low Rate UDP Scan	2050	Indicates a low rate UDP scan.	8
Low Rate ICMP Scan	2051	Indicates a low rate ICMP scan.	8
Low Rate Scan	2052	Indicates a low rate scan.	8
VoIP DoS	2053	Indicates a VoIP DoS attack.	8
Flood	2054	Indicates a Flood attack.	8
TCP Flood	2055	Indicates a TCP flood attack.	8
UDP Flood	2056	Indicates a UDP flood attack.	8
ICMP Flood	2057	Indicates an ICMP flood attack.	8
SYN Flood	2058	Indicates a SYN flood attack.	8
URG Flood	2059	Indicates a flood attack with the urgent (URG) flag on.	8
SYN URG Flood	2060	Indicates a SYN flood attack with the urgent (URG) flag on.	8
SYN FIN Flood	2061	Indicates a SYN FIN flood attack.	8
SYN ACK Flood	2062	Indicates a SYN ACK flood attack.	8

## Authentication

The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

The following table describes the low-level event categories and associated severity levels for the authentication category.

<i>Table 90. Low-level categories and severity levels for the authentication events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Authentication	3001	Indicates unknown authentication.	1

*Table 90. Low-level categories and severity levels for the authentication events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Host Login Succeeded	3002	Indicates a successful host login.	1
Host Login Failed	3003	Indicates that the host login failed.	3
Misc Login Succeeded	3004	Indicates that the login sequence succeeded.	1
Misc Login Failed	3005	Indicates that login sequence failed.	3
Privilege Escalation Failed	3006	Indicates that the privileged escalation failed.	3
Privilege Escalation Succeeded	3007	Indicates that the privilege escalation succeeded.	1
Mail Service Login Succeeded	3008	Indicates that the mail service login succeeded.	1
Mail Service Login Failed	3009	Indicates that the mail service login failed.	3
Auth Server Login Failed	3010	Indicates that the authentication server login failed.	3
Auth Server Login Succeeded	3011	Indicates that the authentication server login succeeded.	1
Web Service Login Succeeded	3012	Indicates that the web service login succeeded.	1
Web Service Login Failed	3013	Indicates that the web service login failed.	3
Admin Login Successful	3014	Indicates that an administrative login was successful.	1
Admin Login Failure	3015	Indicates the administrative login failed.	3
Suspicious Username	3016	Indicates that a user attempted to access the network by using an incorrect user name.	4
Login with username/ password defaults successful	3017	Indicates that a user accessed the network by using the default user name and password.	4

Table 90. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Login with username/ password defaults failed	3018	Indicates that a user was unsuccessful accessing the network by using the default user name and password.	4
FTP Login Succeeded	3019	Indicates that the FTP login was successful.	1
FTP Login Failed	3020	Indicates that the FTP login failed.	3
SSH Login Succeeded	3021	Indicates that the SSH login was successful.	1
SSH Login Failed	3022	Indicates that the SSH login failed.	2
User Right Assigned	3023	Indicates that user access to network resources was successfully granted.	1
User Right Removed	3024	Indicates that user access to network resources was successfully removed.	1
Trusted Domain Added	3025	Indicates that a trusted domain was successfully added to your deployment.	1
Trusted Domain Removed	3026	Indicates that a trusted domain was removed from your deployment.	1
System Security Access Granted	3027	Indicates that system security access was successfully granted.	1
System Security Access Removed	3028	Indicates that system security access was successfully removed.	1
Policy Added	3029	Indicates that a policy was successfully added.	1
Policy Change	3030	Indicates that a policy was successfully changed.	1
User Account Added	3031	Indicates that a user account was successfully added.	1
User Account Changed	3032	Indicates a change to an existing user account.	1

*Table 90. Low-level categories and severity levels for the authentication events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Password Change Failed	3033	Indicates that an attempt to change an existing password failed.	3
Password Change Succeeded	3034	Indicates that a password change was successful.	1
User Account Removed	3035	Indicates that a user account was successfully removed.	1
Group Member Added	3036	Indicates that a group member was successfully added.	1
Group Member Removed	3037	Indicates that a group member was removed.	1
Group Added	3038	Indicates that a group was successfully added.	1
Group Changed	3039	Indicates a change to an existing group.	1
Group Removed	3040	Indicates that a group was removed.	1
Computer Account Added	3041	Indicates that a computer account was successfully added.	1
Computer Account Changed	3042	Indicates a change to an existing computer account.	1
Computer Account Removed	3043	Indicates that a computer account was successfully removed.	1
Remote Access Login Succeeded	3044	Indicates that access to the network by using a remote login was successful.	1
Remote Access Login Failed	3045	Indicates that an attempt to access the network by using a remote login failed.	3
General Authentication Successful	3046	Indicates that the authentication processes was successful.	1
General Authentication Failed	3047	Indicates that the authentication process failed.	3

*Table 90. Low-level categories and severity levels for the authentication events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Telnet Login Succeeded	3048	Indicates that the telnet login was successful.	1
Telnet Login Failed	3049	Indicates that the telnet login failed.	3
Suspicious Password	3050	Indicates that a user attempted to log in by using a suspicious password.	4
Samba Login Successful	3051	Indicates that a user successfully logged in by using Samba.	1
Samba Login Failed	3052	Indicates a user failed to log in by using Samba.	3
Auth Server Session Opened	3053	Indicates that a communication session with the authentication server was started.	1
Auth Server Session Closed	3054	Indicates that a communication session with the authentication server was closed.	1
Firewall Session Closed	3055	Indicates that a firewall session was closed.	1
Host Logout	3056	Indicates that a host successfully logged out.	1
Misc Logout	3057	Indicates that a user successfully logged out.	1
Auth Server Logout	3058	Indicates that the process to log out of the authentication server was successful.	1
Web Service Logout	3059	Indicates that the process to log out of the web service was successful.	1
Admin Logout	3060	Indicates that the administrative user successfully logged out.	1
FTP Logout	3061	Indicates that the process to log out of the FTP service was successful.	1

Table 90. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
SSH Logout	3062	Indicates that the process to log out of the SSH session was successful.	1
Remote Access Logout	3063	Indicates that the process to log out using remote access was successful.	1
Telnet Logout	3064	Indicates that the process to log out of the Telnet session was successful.	1
Samba Logout	3065	Indicates that the process to log out of Samba was successful.	1
SSH Session Started	3066	Indicates that the SSH login session was initiated on a host.	1
SSH Session Finished	3067	Indicates the termination of an SSH login session on a host.	1
Admin Session Started	3068	Indicates that a login session was initiated on a host by an administrative or privileged user.	1
Admin Session Finished	3069	Indicates the termination of an administrator or privileged users login session on a host.	1
VoIP Login Succeeded	3070	Indicates a successful VoIP service login	1
VoIP Login Failed	3071	Indicates an unsuccessful attempt to access VoIP service.	1
VoIP Logout	3072	Indicates a user logout,	1
VoIP Session Initiated	3073	Indicates the beginning of a VoIP session.	1
VoIP Session Terminated	3074	Indicates the end of a VoIP session.	1
Database Login Succeeded	3075	Indicates a successful database login.	1
Database Login Failure	3076	Indicates a database login attempt failed.	3

Table 90. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
IKE Authentication Failed	3077	Indicates a failed Internet Key Exchange (IKE) authentication was detected.	3
IKE Authentication Succeeded	3078	Indicates that a successful IKE authentication was detected.	1
IKE Session Started	3079	Indicates that an IKE session started.	1
IKE Session Ended	3080	Indicates that an IKE session ended.	1
IKE Error	3081	Indicates an IKE error message.	1
IKE Status	3082	Indicates IKE status message.	1
RADIUS Session Started	3083	Indicates that a RADIUS session started.	1
RADIUS Session Ended	3084	Indicates a RADIUS session ended.	1
RADIUS Session Denied	3085	Indicates that a RADIUS session was denied.	1
RADIUS Session Status	3086	Indicates a RADIUS session status message.	1
RADIUS Authentication Failed	3087	Indicates a RADIUS authentication failure.	3
RADIUS Authentication Successful	3088	Indicates a RADIUS authentication succeeded.	1
TACACS Session Started	3089	Indicates a TACACS session started.	1
TACACS Session Ended	3090	Indicates a TACACS session ended.	1
TACACS Session Denied	3091	Indicates that a TACACS session was denied.	1
TACACS Session Status	3092	Indicates a TACACS session status message.	1
TACACS Authentication Successful	3093	Indicates a TACACS authentication succeeded.	1
TACACS Authentication Failed	3094	Indicates a TACACS authentication failure.	1

*Table 90. Low-level categories and severity levels for the authentication events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Deauthenticating Host Succeeded	3095	Indicates that the deauthentication of a host was successful.	1
Deauthenticating Host Failed	3096	Indicates that the deauthentication of a host failed.	3
Station Authentication Succeeded	3097	Indicates that the station authentication was successful.	1
Station Authentication Failed	3098	Indicates that the station authentication of a host failed.	3
Station Association Succeeded	3099	Indicates that the station association was successful.	1
Station Association Failed	3100	Indicates that the station association failed.	3
Station Reassociation Succeeded	3101	Indicates that the station reassociation was successful.	1
Station Reassociation Failed	3102	Indicates that the station association failed.	3
Disassociating Host Succeeded	3103	Indicates that the disassociating a host was successful.	1
Disassociating Host Failed	3104	Indicates that the disassociating a host failed.	3
SA Error	3105	Indicates a Security Association (SA) error message.	5
SA Creation Failure	3106	Indicates a Security Association (SA) creation failure.	3
SA Established	3107	Indicates that a Security Association (SA) connection established.	1
SA Rejected	3108	Indicates that a Security Association (SA) connection rejected.	3
Deleting SA	3109	Indicates the deletion of a Security Association (SA).	1



*Table 90. Low-level categories and severity levels for the authentication events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Creating SA	3110	Indicates the creation of a Security Association (SA).	1
Certificate Mismatch	3111	Indicates a certificate mismatch.	3
Credentials Mismatch	3112	Indicates a credentials mismatch.	3
Admin Login Attempt	3113	Indicates an admin login attempt.	2
User Login Attempt	3114	Indicates a user login attempt.	2
User Login Successful	3115	Indicates a successful user login.	1
User Login Failure	3116	Indicates a failed user login.	3
SFTP Login Succeeded	3117	Indicates a successful SSH File Transfer Protocol (SFTP) login.	1
SFTP Login Failed	3118	Indicates a failed SSH File Transfer Protocol (SFTP) login.	3
SFTP Logout	3119	Indicates an SSH File Transfer Protocol (SFTP) logout.	1
Identity Granted	3120	Indicates that an identity was granted.	1
Identity Removed	3121	Indicates that an identity was removed.	1
Identity Revoked	3122	Indicates that an identity was revoked.	1
Policy Removed	3123	Indicates that a policy was removed.	1
User Account Lock	3124	Indicates that a user account was locked.	1
User Account Unlock	3125	Indicates that a user account was unlocked	1
User Account Expired	3126	Indicates that a user account is expired	1

## Access

The access category contains authentication and access controls that are used for monitoring network events.

The following table describes the low-level event categories and associated severity levels for the access category.

<i>Table 91. Low-level categories and severity levels for the access events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Network Communication Event	4001	Indicates an unknown network communication event.	3
Firewall Permit	4002	Indicates that access to the firewall was allowed.	0
Firewall Deny	4003	Indicates that access to the firewall was denied.	4
Flow Context Response (QRadar SIEM only)	4004	Indicates events from the Classification Engine in response to a SIM request.	5
Misc Network Communication Event	4005	Indicates a miscellaneous communications event.	3
IPS Deny	4006	Indicates Intrusion Prevention Systems (IPS) denied traffic.	4
Firewall Session Opened	4007	Indicates that the firewall session was opened.	0
Firewall Session Closed	4008	Indicates that the firewall session was closed.	0
Dynamic Address Translation Successful	4009	Indicates that dynamic address translation was successful.	0
No Translation Group Found	4010	Indicates that no translation group was found.	2
Misc Authorization	4011	Indicates that access was granted to a miscellaneous authentication server.	2
ACL Permit	4012	Indicates that an Access Control List (ACL) allowed access.	0

*Table 91. Low-level categories and severity levels for the access events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
ACL Deny	4013	Indicates that an Access Control List (ACL) denied access.	4
Access Permitted	4014	Indicates that access was allowed.	0
Access Denied	4015	Indicates that access was denied.	4
Session Opened	4016	Indicates that a session was opened.	1
Session Closed	4017	Indicates that a session was closed.	1
Session Reset	4018	Indicates that a session was reset.	3
Session Terminated	4019	Indicates that a session was allowed.	4
Session Denied	4020	Indicates that a session was denied.	5
Session in Progress	4021	Indicates that a session is in progress.	1
Session Delayed	4022	Indicates that a session was delayed.	3
Session Queued	4023	Indicates that a session was queued.	1
Session Inbound	4024	Indicates that a session is inbound.	1
Session Outbound	4025	Indicates that a session is outbound.	1
Unauthorized Access Attempt	4026	Indicates that an unauthorized access attempt was detected.	6
Misc Application Action Allowed	4027	Indicates that an application action was allowed.	1
Misc Application Action Denied	4028	Indicates that an application action was denied.	3
Database Action Allowed	4029	Indicates that a database action was allowed.	1
Database Action Denied	4030	Indicates that a database action was denied.	3

<i>Table 91. Low-level categories and severity levels for the access events category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
FTP Action Allowed	4031	Indicates that an FTP action was allowed.	1
FTP Action Denied	4032	Indicates that an FTP action was denied.	3
Object Cached	4033	Indicates that an object was cached.	1
Object Not Cached	4034	Indicates that an object was not cached.	1
Rate Limiting	4035	Indicates that the network rate-limits traffic.	4
No Rate Limiting	4036	Indicates that the network does not rate-limit traffic.	0
P11 Access Permitted	4037	Indicates that P11 access is permitted.	8
P11 Access Denied	4038	Indicates that P11 access was attempted and denied.	8
IPS Permit	4039	Indicates an IPS permit.	0

## Exploit

The exploit category contains events where a communication or an access exploit occurred.

The following table describes the low-level event categories and associated severity levels for the exploit category.

<i>Table 92. Low-level categories and severity levels for the exploit events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Exploit Attack	5001	Indicates an unknown exploit attack.	9
Buffer Overflow	5002	Indicates a buffer overflow.	9
DNS Exploit	5003	Indicates a DNS exploit.	9
Telnet Exploit	5004	Indicates a Telnet exploit.	9
Linux Exploit	5005	Indicates a Linux exploit.	9
UNIX Exploit	5006	Indicates a UNIX exploit.	9

Table 92. Low-level categories and severity levels for the exploit events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Windows Exploit	5007	Indicates a Microsoft Windows exploit.	9
Mail Exploit	5008	Indicates a mail server exploit.	9
Infrastructure Exploit	5009	Indicates an infrastructure exploit.	9
Misc Exploit	5010	Indicates a miscellaneous exploit.	9
Web Exploit	5011	Indicates a web exploit.	9
Session Hijack	5012	Indicates that a session in your network was interceded.	9
Worm Active	5013	Indicates an active worm.	10
Password Guess/Retrieve	5014	Indicates that a user requested access to their password information from the database.	9
FTP Exploit	5015	Indicates an FTP exploit.	9
RPC Exploit	5016	Indicates an RPC exploit.	9
SNMP Exploit	5017	Indicates an SNMP exploit.	9
NOOP Exploit	5018	Indicates an NOOP exploit.	9
Samba Exploit	5019	Indicates a Samba exploit.	9
SSH Exploit	5020	Indicates an SSH exploit.	9
Database Exploit	5021	Indicates a database exploit.	9
ICMP Exploit	5022	Indicates an ICMP exploit.	9
UDP Exploit	5023	Indicates a UDP exploit.	9
Browser Exploit	5024	Indicates an exploit on your browser.	9
DHCP Exploit	5025	Indicates a DHCP exploit	9
Remote Access Exploit	5026	Indicates a remote access exploit	9

<i>Table 92. Low-level categories and severity levels for the exploit events category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
ActiveX Exploit	5027	Indicates an exploit through an ActiveX application.	9
SQL Injection	5028	Indicates that an SQL injection occurred.	9
Cross-Site Scripting	5029	Indicates a cross-site scripting vulnerability.	9
Format String Vulnerability	5030	Indicates a format string vulnerability.	9
Input Validation Exploit	5031	Indicates that an input validation exploit attempt was detected.	9
Remote Code Execution	5032	Indicates that a remote code execution attempt was detected.	9
Memory Corruption	5033	Indicates that a memory corruption exploit was detected.	9
Command Execution	5034	Indicates that a remote command execution attempt was detected.	9
Code Injection	5035	Indicates that a code injection was detected.	9
Replay Attack	5036	Indicates that a replay attack was detected.	9

## Malware

The malicious software (malware) category contains events that are related to application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the malware category.

<i>Table 93. Low-level categories and severity levels for the malware events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Malware	6001	Indicates an unknown virus.	4
Backdoor Detected	6002	Indicates that a back door to the system was detected.	9
Hostile Mail Attachment	6003	Indicates a hostile mail attachment.	6

*Table 93. Low-level categories and severity levels for the malware events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Malicious Software	6004	Indicates a virus.	6
Hostile Software Download	6005	Indicates a hostile software download to your network.	6
Virus Detected	6006	Indicates that a virus was detected.	8
Misc Malware	6007	Indicates miscellaneous malicious software	4
Trojan Detected	6008	Indicates that a trojan was detected.	7
Spyware Detected	6009	Indicates that spyware was detected on your system.	6
Content Scan	6010	Indicates that an attempted scan of your content was detected.	3
Content Scan Failed	6011	Indicates that a scan of your content failed.	8
Content Scan Successful	6012	Indicates that a scan of your content was successful.	3
Content Scan in Progress	6013	Indicates that a scan of your content is in progress.	3
Keylogger	6014	Indicates that a key logger was detected.	7
Adware Detected	6015	Indicates that Ad-Ware was detected.	4
Quarantine Successful	6016	Indicates that a quarantine action successfully completed.	3
Quarantine Failed	6017	Indicates that a quarantine action failed.	8
Malware Infection	6018	Indicates that a malware infection was detected.	10
Remove Successful	6019	Indicates that the removal was successful.	3
Remove Failed	6020	Indicates that the removal failed.	8

## Suspicious Activity

The suspicious category contains events that are related to viruses, trojans, back door attacks, and other forms of hostile software.

The following table describes the low-level event categories and associated severity levels for the suspicious activity category.

<i>Table 94. Low-level categories and severity levels for the suspicious activity events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Suspicious Event	7001	Indicates an unknown suspicious event.	3
Suspicious Pattern Detected	7002	Indicates that a suspicious pattern was detected.	3
Content Modified By Firewall	7003	Indicates that content was modified by the firewall.	3
Invalid Command or Data	7004	Indicates an invalid command or data.	3
Suspicious Packet	7005	Indicates a suspicious packet.	3
Suspicious Activity	7006	Indicates suspicious activity.	3
Suspicious File Name	7007	Indicates a suspicious file name.	3
Suspicious Port Activity	7008	Indicates suspicious port activity.	3
Suspicious Routing	7009	Indicates suspicious routing.	3
Potential Web Vulnerability	7010	Indicates potential web vulnerability.	3
Unknown Evasion Event	7011	Indicates an unknown evasion event.	5
IP Spoof	7012	Indicates an IP spoof.	5
IP Fragmentation	7013	Indicates IP fragmentation.	3
Overlapping IP Fragments	7014	Indicates overlapping IP fragments.	5
IDS Evasion	7015	Indicates an IDS evasion.	5
DNS Protocol Anomaly	7016	Indicates a DNS protocol anomaly.	3
FTP Protocol Anomaly	7017	Indicates an FTP protocol anomaly.	3



*Table 94. Low-level categories and severity levels for the suspicious activity events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Mail Protocol Anomaly	7018	Indicates a mail protocol anomaly.	3
Routing Protocol Anomaly	7019	Indicates a routing protocol anomaly.	3
Web Protocol Anomaly	7020	Indicates a web protocol anomaly.	3
SQL Protocol Anomaly	7021	Indicates an SQL protocol anomaly.	3
Executable Code Detected	7022	Indicates that an executable code was detected.	5
Misc Suspicious Event	7023	Indicates a miscellaneous suspicious event.	3
Information Leak	7024	Indicates an information leak.	1
Potential Mail Vulnerability	7025	Indicates a potential vulnerability in the mail server.	4
Potential Version Vulnerability	7026	Indicates a potential vulnerability in the IBM Security QRadar version.	4
Potential FTP Vulnerability	7027	Indicates a potential FTP vulnerability.	4
Potential SSH Vulnerability	7028	Indicates a potential SSH vulnerability.	4
Potential DNS Vulnerability	7029	Indicates a potential vulnerability in the DNS server.	4
Potential SMB Vulnerability	7030	Indicates a potential SMB (Samba) vulnerability.	4
Potential Database Vulnerability	7031	Indicates a potential vulnerability in the database.	4
IP Protocol Anomaly	7032	Indicates a potential IP protocol anomaly	3
Suspicious IP Address	7033	Indicates that a suspicious IP address was detected.	2
Invalid IP Protocol Usage	7034	Indicates an invalid IP protocol.	2

*Table 94. Low-level categories and severity levels for the suspicious activity events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Invalid Protocol	7035	Indicates an invalid protocol.	4
Suspicious Window Events	7036	Indicates a suspicious event with a screen on your desktop.	2
Suspicious ICMP Activity	7037	Indicates suspicious ICMP activity.	2
Potential NFS Vulnerability	7038	Indicates a potential network file system (NFS) vulnerability.	4
Potential NNTP Vulnerability	7039	Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.	4
Potential RPC Vulnerability	7040	Indicates a potential RPC vulnerability.	4
Potential Telnet Vulnerability	7041	Indicates a potential Telnet vulnerability on your system.	4
Potential SNMP Vulnerability	7042	Indicates a potential SNMP vulnerability.	4
Illegal TCP Flag Combination	7043	Indicates that an invalid TCP flag combination was detected.	5
Suspicious TCP Flag Combination	7044	Indicates that a potentially invalid TCP flag combination was detected.	4
Illegal ICMP Protocol Usage	7045	Indicates that an invalid use of the ICMP protocol was detected.	5
Suspicious ICMP Protocol Usage	7046	Indicates that a potentially invalid use of the ICMP protocol was detected.	4
Illegal ICMP Type	7047	Indicates that an invalid ICMP type was detected.	5
Illegal ICMP Code	7048	Indicates that an invalid ICMP code was detected.	5
Suspicious ICMP Type	7049	Indicates that a potentially invalid ICMP type was detected.	4

*Table 94. Low-level categories and severity levels for the suspicious activity events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Suspicious ICMP Code	7050	Indicates that a potentially invalid ICMP code was detected.	4
TCP port 0	7051	Indicates a TCP packet uses a reserved port (0) for source or destination.	4
UDP port 0	7052	Indicates a UDP packet uses a reserved port (0) for source or destination.	4
Hostile IP	7053	Indicates the use of a known hostile IP address.	4
Watch list IP	7054	Indicates the use of an IP address from a watch list of IP addresses.	4
Known offender IP	7055	Indicates the use of an IP address of a known offender.	4
RFC 1918 (private) IP	7056	Indicates the use of an IP address from a private IP address range.	4
Potential VoIP Vulnerability	7057	Indicates a potential VoIP vulnerability.	4
Blacklist Address	7058	Indicates that an IP address is on the black list.	8
Watchlist Address	7059	Indicates that the IP address is on the list of IP addresses being monitored.	7
Darknet Address	7060	Indicates that the IP address is part of a darknet.	5
Botnet Address	7061	Indicates that the address is part of a botnet.	7
Suspicious Address	7062	Indicates that the IP address must be monitored.	5
Bad Content	7063	Indicates that bad content was detected.	7

<i>Table 94. Low-level categories and severity levels for the suspicious activity events category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Invalid Cert	7064	Indicates that an invalid certificate was detected.	7
User Activity	7065	Indicates that user activity was detected.	7
Suspicious Protocol Usage	7066	Indicates that suspicious protocol usage was detected.	5
Suspicious BGP Activity	7067	Indicates that suspicious Border Gateway Protocol (BGP) usage was detected.	5
Route Poisoning	7068	Indicates that route corruption was detected.	5
ARP Poisoning	7069	Indicates that ARP-cache poisoning was detected.	5
Rogue Device Detected	7070	Indicates that a rogue device was detected.	5
Government Agency Address	7071	Indicates that a government agency address was detected.	3

## System

The system category contains events that are related to system changes, software installation, or status messages.

The following table describes the low-level event categories and associated severity levels for the system category.

<i>Table 95. Low-level categories and severity levels for the system events category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown System Event	8001	Indicates an unknown system event.	1
System Boot	8002	Indicates a system restart.	1
System Configuration	8003	Indicates a change in the system configuration.	1
System Halt	8004	Indicates that the system was halted.	1
System Failure	8005	Indicates a system failure.	6

Table 95. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
System Status	8006	Indicates any information event.	1
System Error	8007	Indicates a system error.	3
Misc System Event	8008	Indicates a miscellaneous system event.	1
Service Started	8009	Indicates that system services started.	1
Service Stopped	8010	Indicates that system services stopped.	1
Service Failure	8011	Indicates a system failure.	6
Successful Registry Modification	8012	Indicates that a modification to the registry was successful.	1
Successful Host-Policy Modification	8013	Indicates that a modification to the host policy was successful.	1
Successful File Modification	8014	Indicates that a modification to a file was successful.	1
Successful Stack Modification	8015	Indicates that a modification to the stack was successful.	1
Successful Application Modification	8016	Indicates that a modification to the application was successful.	1
Successful Configuration Modification	8017	Indicates that a modification to the configuration was successful.	1
Successful Service Modification	8018	Indicates that a modification to a service was successful.	1
Failed Registry Modification	8019	Indicates that a modification to the registry failed.	1
Failed Host-Policy Modification	8020	Indicates that a modification to the host policy failed.	1
Failed File Modification	8021	Indicates that a modification to a file failed.	1

*Table 95. Low-level categories and severity levels for the system events category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Failed Stack Modification	8022	Indicates that a modification to the stack failed.	1
Failed Application Modification	8023	Indicates that a modification to an application failed.	1
Failed Configuration Modification	8024	Indicates that a modification to the configuration failed.	1
Failed Service Modification	8025	Indicates that a modification to the service failed.	1
Registry Addition	8026	Indicates that a new item was added to the registry.	1
Host-Policy Created	8027	Indicates that a new entry was added to the registry.	1
File Created	8028	Indicates that a new was created in the system.	1
Application Installed	8029	Indicates that a new application was installed on the system.	1
Service Installed	8030	Indicates that a new service was installed on the system.	1
Registry Deletion	8031	Indicates that a registry entry was deleted.	1
Host-Policy Deleted	8032	Indicates that a host policy entry was deleted.	1
File Deleted	8033	Indicates that a file was deleted.	1
Application Uninstalled	8034	Indicates that an application was uninstalled.	1
Service Uninstalled	8035	Indicates that a service was uninstalled.	1
System Informational	8036	Indicates system information.	3
System Action Allow	8037	Indicates that an attempted action on the system was authorized.	3

Table 95. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
System Action Deny	8038	Indicates that an attempted action on the system was denied.	4
Cron	8039	Indicates a crontab message.	1
Cron Status	8040	Indicates a crontab status message.	1
Cron Failed	8041	Indicates a crontab failure message.	4
Cron Successful	8042	Indicates a crontab success message.	1
Daemon	8043	Indicates a daemon message.	1
Daemon Status	8044	Indicates a daemon status message.	1
Daemon Failed	8045	Indicates a daemon failure message.	4
Daemon Successful	8046	Indicates a daemon success message.	1
Kernel	8047	Indicates a kernel message.	1
Kernel Status	8048	Indicates a kernel status message.	1
Kernel Failed	8049	Indicates a kernel failure message.	
Kernel Successful	8050	Indicates a kernel successful message.	1
Authentication	8051	Indicates an authentication message.	1
Information	8052	Indicates an informational message.	2
Notice	8053	Indicates a notice message.	3
Warning	8054	Indicates a warning message.	5
Error	8055	Indicates an error message.	7
Critical	8056	Indicates a critical message.	9
Debug	8057	Indicates a debug message.	1

Table 95. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Messages	8058	Indicates a generic message.	1
Privilege Access	8059	Indicates that privilege access was attempted.	3
Alert	8060	Indicates an alert message.	9
Emergency	8061	Indicates an emergency message.	9
SNMP Status	8062	Indicates an SNMP status message.	1
FTP Status	8063	Indicates an FTP status message.	1
NTP Status	8064	Indicates an NTP status message.	1
Access Point Radio Failure	8065	Indicates an access point radio failure.	3
Encryption Protocol Configuration Mismatch	8066	Indicates an encryption protocol configuration mismatch.	3
Client Device or Authentication Server Misconfigured	8067	Indicates that a client device or authentication server was not configured properly.	5
Hot Standby Enable Failed	8068	Indicates a hot standby enable failure.	5
Hot Standby Disable Failed	8069	Indicates a hot standby disable failure.	5
Hot Standby Enabled Successfully	8070	Indicates that hot standby was enabled successfully.	1
Hot Standby Association Lost	8071	Indicates that a hot standby association was lost.	5
MainMode Initiation Failure	8072	Indicates MainMode initiation failure.	5
MainMode Initiation Succeeded	8073	Indicates that the MainMode initiation was successful.	1
MainMode Status	8074	Indicates a MainMode status message was reported.	1



<i>Table 95. Low-level categories and severity levels for the system events category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
QuickMode Initiation Failure	8075	Indicates that the QuickMode initiation failed.	5
Quickmode Initiation Succeeded	8076	Indicates that the QuickMode initiation was successful.	1
Quickmode Status	8077	Indicates a QuickMode status message was reported.	1
Invalid License	8078	Indicates an invalid license.	3
License Expired	8079	Indicates an expired license.	3
New License Applied	8080	Indicates a new license applied.	1
License Error	8081	Indicates a license error.	5
License Status	8082	Indicates a license status message.	1
Configuration Error	8083	Indicates that a configuration error was detected.	5
Service Disruption	8084	Indicates that a service disruption was detected.	5
EPS or FPM allocation exceeded	8085	Indicates that the license pool allocations for EPS or FPM were exceeded.	3
Performance Status	8086	Indicates that the performance status was reported.	1
Performance Degradation	8087	Indicates that the performance is being degraded.	4
Misconfiguration	8088	Indicates that an incorrect configuration was detected.	5

## Policy

The policy category contains events that are related to administration of network policy and the monitoring network resources for policy violations.

The following table describes the low-level event categories and associated severity levels for the policy category.

*Table 96. Low-level categories and severity levels for the policy category*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Policy Violation	9001	Indicates an unknown policy violation.	2
Web Policy Violation	9002	Indicates a web policy violation.	2
Remote Access Policy Violation	9003	Indicates a remote access policy violation.	2
IRC/IM Policy Violation	9004	Indicates an instant messenger policy violation.	2
P2P Policy Violation	9005	Indicates a Peer-to-Peer (P2P) policy violation.	2
IP Access Policy Violation	9006	Indicates an IP access policy violation.	2
Application Policy Violation	9007	Indicates an application policy violation.	2
Database Policy Violation	9008	Indicates a database policy violation.	2
Network Threshold Policy Violation	9009	Indicates a network threshold policy violation.	2
Porn Policy Violation	9010	Indicates a porn policy violation.	2
Games Policy Violation	9011	Indicates a games policy violation.	2
Misc Policy Violation	9012	Indicates a miscellaneous policy violation.	2
Compliance Policy Violation	9013	Indicates a compliance policy violation.	2
Mail Policy Violation	9014	Indicates a mail policy violation.	2
IRC Policy Violation	9015	Indicates an IRC policy violation	2
IM Policy Violation	9016	Indicates a policy violation that is related to instant message (IM) activities.	2
VoIP Policy Violation	9017	Indicates a VoIP policy violation	2
Succeeded	9018	Indicates a policy successful message.	1

*Table 96. Low-level categories and severity levels for the policy category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Failed	9019	Indicates a policy failure message.	4
Data Loss Prevention Policy Violation	9020	Indicates a data loss prevention policy violation.	2
Watchlist Object	9021	Indicates a watchlist object.	2
Web Policy Allow	9022	Indicates a new web policy allowance.	1

## Unknown

The Unknown category contains events that are not parsed and therefore cannot be categorized.

The following table describes the low-level event categories and associated severity levels for the Unknown category.

*Table 97. Low-level categories and severity levels for the Unknown category*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown	10001	Indicates an unknown event.	3
Unknown Snort Event	10002	Indicates an unknown Snort event.	3
Unknown Dragon Event	10003	Indicates an unknown Dragon event.	3
Unknown Pix Firewall Event	10004	Indicates an unknown Cisco Private Internet Exchange (PIX) Firewall event.	3
Unknown Tipping Point Event	10005	Indicates an unknown HP TippingPoint event.	3
Unknown Windows Auth Server Event	10006	Indicates an unknown Windows Auth Server event.	3
Unknown Nortel Event	10007	Indicates an unknown Nortel event.	3
Stored	10009	Indicates an unknown stored event.	3
Behavioral	11001	Indicates an unknown behavioral event.	3
Threshold	11002	Indicates an unknown threshold event.	3

<i>Table 97. Low-level categories and severity levels for the Unknown category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Anomaly	11003	Indicates an unknown anomaly event.	3

## CRE

The custom rule event (CRE) category contains events that are generated from a custom offense, flow, or event rule.

The following table describes the low-level event categories and associated severity levels for the CRE category.

<i>Table 98. Low-level categories and severity levels for the CRE category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown CRE Event	12001	Indicates an unknown custom rules engine event.	5
Single Event Rule Match	12002	Indicates a single event rule match.	5
Event Sequence Rule Match	12003	Indicates an event sequence rule match.	5
Cross-Offense Event Sequence Rule Match	12004	Indicates a cross-offense event sequence rule match.	5
Offense Rule Match	12005	Indicates an offense rule match.	5

## Potential Exploit

The potential exploit category contains events that are related to potential application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the potential exploit category.

<i>Table 99. Low-level categories and severity levels for the potential exploit category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unknown Potential Exploit Attack	13001	Indicates that a potential exploitative attack was detected.	7
Potential Buffer Overflow	13002	Indicates that a potential buffer overflow was detected.	7

*Table 99. Low-level categories and severity levels for the potential exploit category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Potential DNS Exploit	13003	Indicates that a potentially exploitative attack through the DNS server was detected.	7
Potential Telnet Exploit	13004	Indicates that a potentially exploitative attack through Telnet was detected.	7
Potential Linux Exploit	13005	Indicates that a potentially exploitative attack through Linux wasLinux detected.	7
Potential UNIX Exploit	13006	Indicates that a potentially exploitative attack through UNIX was detected.	7
Potential Windows Exploit	13007	Indicates that a potentially exploitative attack through Windows wasWindows detected.	7
Potential Mail Exploit	13008	Indicates that a potentially exploitative attack through mail was detected.	7
Potential Infrastructure Exploit	13009	Indicates that a potential exploitative attack on the system infrastructure was detected.	7
Potential Misc Exploit	13010	Indicates that a potentially exploitative attack was detected.	7
Potential Web Exploit	13011	Indicates that a potentially exploitative attack through the web was detected.	7
Potential Botnet Connection	13012	Indicates a potentially exploitative attack that uses botnet was detected.	6
Potential Worm Activity	13013	Indicates a potential attack that uses worm activity was detected.	6

## Flow

The flow category includes events that are related to flow actions.

The following table describes the low-level event categories and associated severity levels for the flow category.

<i>Table 100. Low-level categories and severity levels for the flow category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Unidirectional Flow	14001	Indicates a unidirectional flow of events.	5
Low number of Unidirectional Flows	14002	Indicates a low number of unidirectional flows of events.	5
Medium number of Unidirectional Flows	14003	Indicates a medium number of unidirectional flows of events.	5
High number of Unidirectional Flows	14004	Indicates a high number of unidirectional flows of events.	5
Unidirectional TCP Flow	14005	Indicates a unidirectional TCP flow.	5
Low number of Unidirectional TCP Flows	14006	Indicates a low number of unidirectional TCP flows.	5
Medium number of Unidirectional TCP Flows	14007	Indicates a medium number of unidirectional TCP flows.	5
High number of Unidirectional TCP Flows	14008	Indicates a high number of unidirectional TCP flows.	5
Unidirectional ICMP Flow	14009	Indicates a unidirectional ICMP flow.	5
Low number of Unidirectional ICMP Flows	14010	Indicates a low number of unidirectional ICMP flows.	5
Medium number of Unidirectional ICMP Flows	14011	Indicates a medium number of unidirectional ICMP flows.	5
High number if Unidirectional ICMP Flows	14012	Indicates a high number of unidirectional ICMP flows.	5
Suspicious ICMP Flow	14013	Indicates a suspicious ICMP flow.	5
Suspicious UDP Flow	14014	Indicates a suspicious UDP flow.	5
Suspicious TCP Flow	14015	Indicates a suspicious TCP flow.	5
Suspicious Flow	14016	Indicates a suspicious flow.	5
Empty Packet Flows	14017	Indicates empty packet flows.	5

Table 100. Low-level categories and severity levels for the flow category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Low number of Empty Packet Flows	14018	Indicates a low number of empty packet flows.	5
Medium number of Empty Packet Flows	14019	Indicates a medium number of empty packet flows.	5
High number of Empty Packet Flows	14020	Indicates a high number of empty packet flows.	5
Large Payload Flows	14021	Indicates a large payload of flows.	5
Low number of Large Payload Flows	14022	Indicates a low number of large payload flows.	5
Medium number of Large Payload Flows	14023	Indicates a medium number of large payload flows.	5
High number of Large Payload Flows	14024	Indicates a high number of large payload flows.	5
One Attacker to Many Target Flows	14025	Indicates that one attacker is targeting many flows.	5
Many Attacker to one Target Flow	14026	Indicates that many attackers are targeting one flow.	5
Unknown Flow	14027	Indicates an unknown flow.	5
Netflow Record	14028	Indicates a Netflow record.	5
QFlow Record	14029	Indicates a QFlow record.	5
SFlow Record	14030	Indicates an SFlow record.	5
Packeteer Record	14031	Indicates a Packeteer record.	5
Misc Flow	14032	Indicates a misc flow.	5
Large Data Transfer	14033	Indicates a large transfer of data.	5
Large Data Transfer Outbound	14034	Indicates a large transfer of outbound data.	5
VoIP Flows	14035	Indicates VoIP Flows.	5

## User Defined

The User Defined category contains events that are related to user-defined objects

The following table describes the low-level event categories and associated severity levels for the User Defined category.

*Table 101. Low-level categories and severity levels for the User Defined category*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Custom Sentry Low	15001	Indicates a low severity custom anomaly event.	3
Custom Sentry Medium	15002	Indicates a medium severity custom anomaly event.	5
Custom Sentry High	15003	Indicates a high severity custom anomaly event.	7
Custom Sentry 1	15004	Indicates a custom anomaly event with a severity level of 1.	1
Custom Sentry 2	15005	Indicates a custom anomaly event with a severity level of 2.	2
Custom Sentry 3	15006	Indicates a custom anomaly event with a severity level of 3.	3
Custom Sentry 4	15007	Indicates a custom anomaly event with a severity level of 4.	4
Custom Sentry 5	15008	Indicates a custom anomaly event with a severity level of 5.	5
Custom Sentry 6	15009	Indicates a custom anomaly event with a severity level of 6.	6
Custom Sentry 7	15010	Indicates a custom anomaly event with a severity level of 7.	7
Custom Sentry 8	15011	Indicates a custom anomaly event with a severity level of 8.	8
Custom Sentry 9	15012	Indicates a custom anomaly event with a severity level of 9.	9
Custom Policy Low	15013	Indicates a custom policy event with a low severity level.	3
Custom Policy Medium	15014	Indicates a custom policy event with a medium severity level.	5
Custom Policy High	15015	Indicates a custom policy event with a high severity level.	7



*Table 101. Low-level categories and severity levels for the User Defined category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Custom Policy 1	15016	Indicates a custom policy event with a severity level of 1.	1
Custom Policy 2	15017	Indicates a custom policy event with a severity level of 2.	2
Custom Policy 3	15018	Indicates a custom policy event with a severity level of 3.	3
Custom Policy 4	15019	Indicates a custom policy event with a severity level of 4.	4
Custom Policy 5	15020	Indicates a custom policy event with a severity level of 5.	5
Custom Policy 6	15021	Indicates a custom policy event with a severity level of 6.	6
Custom Policy 7	15022	Indicates a custom policy event with a severity level of 7.	7
Custom Policy 8	15023	Indicates a custom policy event with a severity level of 8.	8
Custom Policy 9	15024	Indicates a custom policy event with a severity level of 9.	9
Custom User Low	15025	Indicates a custom user event with a low severity level.	3
Custom User Medium	15026	Indicates a custom user event with a medium severity level.	5
Custom User High	15027	Indicates a custom user event with a high severity level.	7
Custom User 1	15028	Indicates a custom user event with a severity level of 1.	1
Custom User 2	15029	Indicates a custom user event with a severity level of 2.	2
Custom User 3	15030	Indicates a custom user event with a severity level of 3.	3

<i>Table 101. Low-level categories and severity levels for the User Defined category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Custom User 4	15031	Indicates a custom user event with a severity level of 4.	4
Custom User 5	15032	Indicates a custom user event with a severity level of 5.	5
Custom User 6	15033	Indicates a custom user event with a severity level of 6.	6
Custom User 7	15034	Indicates a custom user event with a severity level of 7.	7
Custom User 8	15035	Indicates a custom user event with a severity level of 8.	8
Custom User 9	15036	Indicates a custom user event with a severity level of 9.	9

## SIM Audit

The SIM Audit category contains events that are related to user interaction with the IBM Security QRadar Console and administrative features.

The following table describes the low-level event categories and associated severity levels for the SIM Audit category.

<i>Table 102. Low-level categories and severity levels for the SIM Audit category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
SIM User Authentication	16001	Indicates a user login or logout on the Console.	5
SIM Configuration Change	16002	Indicates that a user changed the SIM configuration or deployment.	3
SIM User Action	16003	Indicates that a user initiated a process, such as starting a backup or generating a report, in the SIM module.	3
Session Created	16004	Indicates that a user session was created.	3
Session Destroyed	16005	Indicates that a user session was destroyed.	3

<i>Table 102. Low-level categories and severity levels for the SIM Audit category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Admin Session Created	16006	Indicates that an admin session was created.	
Admin Session Destroyed	16007	Indicates that an admin session was destroyed.	3
Session Authentication Invalid	16008	Indicates an invalid session authentication.	5
Session Authentication Expired	16009	Indicates that a session authentication expired.	3
Risk Manager Configuration	16010	Indicates that a user changed the IBM Security QRadar Risk Manager configuration.	3

## VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities that are 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 following table describes the low-level event categories and associated severity levels for the VIS host discovery category.

<i>Table 103. Low-level categories and severity levels for the VIS host discovery category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
New Host Discovered	17001	Indicates that the VIS component detected a new host.	3
New Port Discovered	17002	Indicates that the VIS component detected a new open port.	3
New Vuln Discovered	17003	Indicates that the VIS component detected a new vulnerability.	3
New OS Discovered	17004	Indicates that the VIS component detected a new operating system on a host.	3
Bulk Host Discovered	17005	Indicates that the VIS component detected many new hosts in a short period.	3

## Application

The application category contains events that are related to application activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the application category.

<i>Table 104. Low-level categories and severity levels for the application category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Mail Opened	18001	Indicates that an email connection was established.	1
Mail Closed	18002	Indicates that an email connection was closed.	1
Mail Reset	18003	Indicates that an email connection was reset.	3
Mail Terminated	18004	Indicates that an email connection was terminated.	4
Mail Denied	18005	Indicates that an email connection was denied.	4
Mail in Progress	18006	Indicates that an email connection is being attempted.	1
Mail Delayed	18007	Indicates that an email connection was delayed.	4
Mail Queued	18008	Indicates that an email connection was queued.	3
Mail Redirected	18009	Indicates that an email connection was redirected.	1
FTP Opened	18010	Indicates that an FTP connection was opened.	1
FTP Closed	18011	Indicates that an FTP connection was closed.	1
FTP Reset	18012	Indicates that an FTP connection was reset.	3
FTP Terminated	18013	Indicates that an FTP connection was terminated.	4
FTP Denied	18014	Indicates that an FTP connection was denied.	4
FTP In Progress	18015	Indicates that an FTP connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
FTP Redirected	18016	Indicates that an FTP connection was redirected.	3
HTTP Opened	18017	Indicates that an HTTP connection was established.	1
HTTP Closed	18018	Indicates that an HTTP connection was closed.	1
HTTP Reset	18019	Indicates that an HTTP connection was reset.	3
HTTP Terminated	18020	Indicates that an HTTP connection was terminated.	4
HTTP Denied	18021	Indicates that an HTTP connection was denied.	4
HTTP In Progress	18022	Indicates that an HTTP connection is in progress.	1
HTTP Delayed	18023	Indicates that an HTTP connection was delayed.	3
HTTP Queued	18024	Indicates that an HTTP connection was queued.	1
HTTP Redirected	18025	Indicates that an HTTP connection was redirected.	1
HTTP Proxy	18026	Indicates that an HTTP connection is being proxied.	1
HTTPS Opened	18027	Indicates that an HTTPS connection was established.	1
HTTPS Closed	18028	Indicates that an HTTPS connection was closed.	1
HTTPS Reset	18029	Indicates that an HTTPS connection was reset.	3
HTTPS Terminated	18030	Indicates that an HTTPS connection was terminated.	4
HTTPS Denied	18031	Indicates that an HTTPS connection was denied.	4
HTTPS In Progress	18032	Indicates that an HTTPS connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
HTTPS Delayed	18033	Indicates that an HTTPS connection was delayed.	3
HTTPS Queued	18034	Indicates that an HTTPS connection was queued.	3
HTTPS Redirected	18035	Indicates that an HTTPS connection was redirected.	3
HTTPS Proxy	18036	Indicates that an HTTPS connection is proxied.	1
SSH Opened	18037	Indicates that an SSH connection was established.	1
SSH Closed	18038	Indicates that an SSH connection was closed.	1
SSH Reset	18039	Indicates that an SSH connection was reset.	3
SSH Terminated	18040	Indicates that an SSH connection was terminated.	4
SSH Denied	18041	Indicates that an SSH session was denied.	4
SSH In Progress	18042	Indicates that an SSH session is in progress.	1
RemoteAccess Opened	18043	Indicates that a remote access connection was established.	1
RemoteAccess Closed	18044	Indicates that a remote access connection was closed.	1
RemoteAccess Reset	18045	Indicates that a remote access connection was reset.	3
RemoteAccess Terminated	18046	Indicates that a remote access connection was terminated.	4
RemoteAccess Denied	18047	Indicates that a remote access connection was denied.	4
RemoteAccess In Progress	18048	Indicates that a remote access connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
RemoteAccess Delayed	18049	Indicates that a remote access connection was delayed.	3
RemoteAccess Redirected	18050	Indicates that a remote access connection was redirected.	3
VPN Opened	18051	Indicates that a VPN connection was opened.	1
VPN Closed	18052	Indicates that a VPN connection was closed.	1
VPN Reset	18053	Indicates that a VPN connection was reset.	3
VPN Terminated	18054	Indicates that a VPN connection was terminated.	4
VPN Denied	18055	Indicates that a VPN connection was denied.	4
VPN In Progress	18056	Indicates that a VPN connection is in progress.	1
VPN Delayed	18057	Indicates that a VPN connection was delayed	3
VPN Queued	18058	Indicates that a VPN connection was queued.	3
VPN Redirected	18059	Indicates that a VPN connection was redirected.	3
RDP Opened	18060	Indicates that an RDP connection was established.	1
RDP Closed	18061	Indicates that an RDP connection was closed.	1
RDP Reset	18062	Indicates that an RDP connection was reset.	3
RDP Terminated	18063	Indicates that an RDP connection was terminated.	4
RDP Denied	18064	Indicates that an RDP connection was denied.	4
RDP In Progress	18065	Indicates that an RDP connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
RDP Redirected	18066	Indicates that an RDP connection was redirected.	3
FileTransfer Opened	18067	Indicates that a file transfer connection was established.	1
FileTransfer Closed	18068	Indicates that a file transfer connection was closed.	1
FileTransfer Reset	18069	Indicates that a file transfer connection was reset.	3
FileTransfer Terminated	18070	Indicates that a file transfer connection was terminated.	4
FileTransfer Denied	18071	Indicates that a file transfer connection was denied.	4
FileTransfer In Progress	18072	Indicates that a file transfer connection is in progress.	1
FileTransfer Delayed	18073	Indicates that a file transfer connection was delayed.	3
FileTransfer Queued	18074	Indicates that a file transfer connection was queued.	3
FileTransfer Redirected	18075	Indicates that a file transfer connection was redirected.	3
DNS Opened	18076	Indicates that a DNS connection was established.	1
DNS Closed	18077	Indicates that a DNS connection was closed.	1
DNS Reset	18078	Indicates that a DNS connection was reset.	5
DNS Terminated	18079	Indicates that a DNS connection was terminated.	5
DNS Denied	18080	Indicates that a DNS connection was denied.	5



Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
DNS In Progress	18081	Indicates that a DNS connection is in progress.	1
DNS Delayed	18082	Indicates that a DNS connection was delayed.	5
DNS Redirected	18083	Indicates that a DNS connection was redirected.	4
Chat Opened	18084	Indicates that a chat connection was opened.	1
Chat Closed	18085	Indicates that a chat connection was closed.	1
Chat Reset	18086	Indicates that a chat connection was reset.	3
Chat Terminated	18087	Indicates that a chat connection was terminated.	3
Chat Denied	18088	Indicates that a chat connection was denied.	3
Chat In Progress	18089	Indicates that a chat connection is in progress.	1
Chat Redirected	18090	Indicates that a chat connection was redirected.	1
Database Opened	18091	Indicates that a database connection was established.	1
Database Closed	18092	Indicates that a database connection was closed.	1
Database Reset	18093	Indicates that a database connection was reset.	5
Database Terminated	18094	Indicates that a database connection was terminated.	5
Database Denied	18095	Indicates that a database connection was denied.	5
Database In Progress	18096	Indicates that a database connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Database Redirected	18097	Indicates that a database connection was redirected.	3
SMTP Opened	18098	Indicates that an SMTP connection was established.	1
SMTP Closed	18099	Indicates that an SMTP connection was closed.	1
SMTP Reset	18100	Indicates that an SMTP connection was reset.	3
SMTP Terminated	18101	Indicates that an SMTP connection was terminated.	5
SMTP Denied	18102	Indicates that an SMTP connection was denied.	5
SMTP In Progress	18103	Indicates that an SMTP connection is in progress.	1
SMTP Delayed	18104	Indicates that an SMTP connection was delayed.	3
SMTP Queued	18105	Indicates that an SMTP connection was queued.	3
SMTP Redirected	18106	Indicates that an SMTP connection was redirected.	3
Auth Opened	18107	Indicates that an authorization server connection was established.	1
Auth Closed	18108	Indicates that an authorization server connection was closed.	1
Auth Reset	18109	Indicates that an authorization server connection was reset.	3
Auth Terminated	18110	Indicates that an authorization server connection was terminated.	4
Auth Denied	18111	Indicates that an authorization server connection was denied.	4

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Auth In Progress	18112	Indicates that an authorization server connection is in progress.	1
Auth Delayed	18113	Indicates that an authorization server connection was delayed.	3
Auth Queued	18114	Indicates that an authorization server connection was queued.	3
Auth Redirected	18115	Indicates that an authorization server connection was redirected.	2
P2P Opened	18116	Indicates that a Peer-to-Peer (P2P) connection was established.	1
P2P Closed	18117	Indicates that a P2P connection was closed.	1
P2P Reset	18118	Indicates that a P2P connection was reset.	4
P2P Terminated	18119	Indicates that a P2P connection was terminated.	4
P2P Denied	18120	Indicates that a P2P connection was denied.	3
P2P In Progress	18121	Indicates that a P2P connection is in progress.	1
Web Opened	18122	Indicates that a web connection was established.	1
Web Closed	18123	Indicates that a web connection was closed.	1
Web Reset	18124	Indicates that a web connection was reset.	4
Web Terminated	18125	Indicates that a web connection was terminated.	4
Web Denied	18126	Indicates that a web connection was denied.	4
Web In Progress	18127	Indicates that a web connection is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Web Delayed	18128	Indicates that a web connection was delayed.	3
Web Queued	18129	Indicates that a web connection was queued.	1
Web Redirected	18130	Indicates that a web connection was redirected.	1
Web Proxy	18131	Indicates that a web connection was proxied.	1
VoIP Opened	18132	Indicates that a Voice Over IP (VoIP) connection was established.	1
VoIP Closed	18133	Indicates that a VoIP connection was closed.	1
VoIP Reset	18134	Indicates that a VoIP connection was reset.	3
VoIP Terminated	18135	Indicates that a VoIP connection was terminated.	3
VoIP Denied	18136	Indicates that a VoIP connection was denied.	3
VoIP In Progress	18137	Indicates that a VoIP connection is in progress.	1
VoIP Delayed	18138	Indicates that a VoIP connection was delayed.	3
VoIP Redirected	18139	Indicates that a VoIP connection was redirected.	3
LDAP Session Started	18140	Indicates an LDAP session started.	1
LDAP Session Ended	18141	Indicates an LDAP session ended.	1
LDAP Session Denied	18142	Indicates that an LDAP session was denied.	3
LDAP Session Status	18143	Indicates that an LDAP session status message was reported.	1
LDAP Authentication Failed	18144	Indicates that an LDAP authentication failed.	4

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
LDAP Authentication Succeeded	18145	Indicates that an LDAP authentication was successful.	1
AAA Session Started	18146	Indicates that an Authentication, Authorization, and Accounting (AAA) session started.	1
AAA Session Ended	18147	Indicates that an AAA session ended.	1
AAA Session Denied	18148	Indicates that an AAA session was denied.	3
AAA Session Status	18149	Indicates that an AAA session status message was reported.	1
AAA Authentication Failed	18150	Indicates that an AAA authentication failed.	4
AAA Authentication Succeeded	18151	Indicates that an AAA authentication was successful.	1
IPSEC Authentication Failed	18152	Indicates that an Internet Protocol Security (IPSEC) authentication failed.	4
IPSEC Authentication Succeeded	18153	Indicates that an IPSEC authentication was successful.	1
IPSEC Session Started	18154	Indicates that an IPSEC session started.	1
IPSEC Session Ended	18155	Indicates that an IPSEC session ended.	1
IPSEC Error	18156	Indicates that an IPSEC error message was reported.	5
IPSEC Status	18157	Indicates that an IPSEC session status message was reported.	1
IM Session Opened	18158	Indicates that an Instant Messenger (IM) session was established.	1
IM Session Closed	18159	Indicates that an IM session was closed.	1
IM Session Reset	18160	Indicates that an IM session was reset.	3

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
IM Session Terminated	18161	Indicates that an IM session was terminated.	3
IM Session Denied	18162	Indicates that an IM session was denied.	3
IM Session In Progress	18163	Indicates that an IM session is in progress.	1
IM Session Delayed	18164	Indicates that an IM session was delayed	3
IM Session Redirected	18165	Indicates that an IM session was redirected.	3
WHOIS Session Opened	18166	Indicates that a WHOIS session was established.	1
WHOIS Session Closed	18167	Indicates that a WHOIS session was closed.	1
WHOIS Session Reset	18168	Indicates that a WHOIS session was reset.	3
WHOIS Session Terminated	18169	Indicates that a WHOIS session was terminated.	3
WHOIS Session Denied	18170	Indicates that a WHOIS session was denied.	3
WHOIS Session In Progress	18171	Indicates that a WHOIS session is in progress.	1
WHOIS Session Redirected	18172	Indicates that a WHOIS session was redirected.	3
Traceroute Session Opened	18173	Indicates that a Traceroute session was established.	1
Traceroute Session Closed	18174	Indicates that a Traceroute session was closed.	1
Traceroute Session Denied	18175	Indicates that a Traceroute session was denied.	3
Traceroute Session In Progress	18176	Indicates that a Traceroute session is in progress.	1
TN3270 Session Opened	18177	TN3270 is a terminal emulation program, which is used to connect to an IBM 3270 terminal. This category indicates that a TN3270 session was established.	1

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
TN3270 Session Closed	18178	Indicates that a TN3270 session was closed.	1
TN3270 Session Reset	18179	Indicates that a TN3270 session was reset.	3
TN3270 Session Terminated	18180	Indicates that a TN3270 session was terminated.	3
TN3270 Session Denied	18181	Indicates that a TN3270 session was denied.	3
TN3270 Session In Progress	18182	Indicates that a TN3270 session is in progress.	1
TFTP Session Opened	18183	Indicates that a TFTP session was established.	1
TFTP Session Closed	18184	Indicates that a TFTP session was closed.	1
TFTP Session Reset	18185	Indicates that a TFTP session was reset.	3
TFTP Session Terminated	18186	Indicates that a TFTP session was terminated.	3
TFTP Session Denied	18187	Indicates that a TFTP session was denied.	3
TFTP Session In Progress	18188	Indicates that a TFTP session is in progress.	1
Telnet Session Opened	18189	Indicates that a Telnet session was established.	1
Telnet Session Closed	18190	Indicates that a Telnet session was closed.	1
Telnet Session Reset	18191	Indicates that a Telnet session was reset.	3
Telnet Session Terminated	18192	Indicates that a Telnet session was terminated.	3
Telnet Session Denied	18193	Indicates that a Telnet session was denied.	3
Telnet Session In Progress	18194	Indicates that a Telnet session is in progress.	1
Syslog Session Opened	18201	Indicates that a syslog session was established.	1
Syslog Session Closed	18202	Indicates that a syslog session was closed.	1
Syslog Session Denied	18203	Indicates that a syslog session was denied.	3

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Syslog Session In Progress	18204	Indicates that a syslog session is in progress.	1
SSL Session Opened	18205	Indicates that a Secure Socket Layer (SSL) session was established.	1
SSL Session Closed	18206	Indicates that an SSL session was closed.	1
SSL Session Reset	18207	Indicates that an SSL session was reset.	3
SSL Session Terminated	18208	Indicates that an SSL session was terminated.	3
SSL Session Denied	18209	Indicates that an SSL session was denied.	3
SSL Session In Progress	18210	Indicates that an SSL session is in progress.	1
SNMP Session Opened	18211	Indicates that a Simple Network Management Protocol (SNMP) session was established.	1
SNMP Session Closed	18212	Indicates that an SNMP session was closed.	1
SNMP Session Denied	18213	Indicates that an SNMP session was denied.	3
SNMP Session In Progress	18214	Indicates that an SNMP session is in progress.	1
SMB Session Opened	18215	Indicates that a Server Message Block (SMB) session was established.	1
SMB Session Closed	18216	Indicates that an SMB session was closed.	1
SMB Session Reset	18217	Indicates that an SMB session was reset.	3
SMB Session Terminated	18218	Indicates that an SMB session was terminated.	3
SMB Session Denied	18219	Indicates that an SMB session was denied.	3
SMB Session In Progress	18220	Indicates that an SMB session is in progress.	1
Streaming Media Session Opened	18221	Indicates that a Streaming Media session was established.	1



Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Streaming Media Session Closed	18222	Indicates that a Streaming Media session was closed.	1
Streaming Media Session Reset	18223	Indicates that a Streaming Media session was reset.	3
Streaming Media Session Terminated	18224	Indicates that a Streaming Media session was terminated.	3
Streaming Media Session Denied	18225	Indicates that a Streaming Media session was denied.	3
Streaming Media Session In Progress	18226	Indicates that a Streaming Media session is in progress.	1
RUSERS Session Opened	18227	Indicates that a (Remote Users) RUSERS session was established.	1
RUSERS Session Closed	18228	Indicates that a RUSERS session was closed.	1
RUSERS Session Denied	18229	Indicates that a RUSERS session was denied.	3
RUSERS Session In Progress	18230	Indicates that a RUSERS session is in progress.	1
Rsh Session Opened	18231	Indicates that a remote shell (rsh) session was established.	1
Rsh Session Closed	18232	Indicates that an rsh session was closed.	1
Rsh Session Reset	18233	Indicates that an rsh session was reset.	3
Rsh Session Terminated	18234	Indicates that an rsh session was terminated.	3
Rsh Session Denied	18235	Indicates that an rsh session was denied.	3
Rsh Session In Progress	18236	Indicates that an rsh session is in progress.	1
RLOGIN Session Opened	18237	Indicates that a Remote Login (RLOGIN) session was established.	1
RLOGIN Session Closed	18238	Indicates that an RLOGIN session was closed.	1

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
RLOGIN Session Reset	18239	Indicates that an RLOGIN session was reset.	3
RLOGIN Session Terminated	18240	Indicates that an RLOGIN session was terminated.	3
RLOGIN Session Denied	18241	Indicates that an RLOGIN session was denied.	3
RLOGIN Session In Progress	18242	Indicates that an RLOGIN session is in progress.	1
REXEC Session Opened	18243	Indicates that a (Remote Execution) REXEC session was established.	1
REXEC Session Closed	18244	Indicates that an REXEC session was closed.	1
REXEC Session Reset	18245	Indicates that an REXEC session was reset.	3
REXEC Session Terminated	18246	Indicates that an REXEC session was terminated.	3
REXEC Session Denied	18247	Indicates that an REXEC session was denied.	3
REXEC Session In Progress	18248	Indicates that an REXEC session is in progress.	1
RPC Session Opened	18249	Indicates that a Remote Procedure Call (RPC) session was established.	1
RPC Session Closed	18250	Indicates that an RPC session was closed.	1
RPC Session Reset	18251	Indicates that an RPC session was reset.	3
RPC Session Terminated	18252	Indicates that an RPC session was terminated.	3
RPC Session Denied	18253	Indicates that an RPC session was denied.	3
RPC Session In Progress	18254	Indicates that an RPC session is in progress.	1
NTP Session Opened	18255	Indicates that a Network Time Protocol (NTP) session was established.	1
NTP Session Closed	18256	Indicates that an NTP session was closed.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
NTP Session Reset	18257	Indicates that an NTP session was reset.	3
NTP Session Terminated	18258	Indicates that an NTP session was terminated.	3
NTP Session Denied	18259	Indicates that an NTP session was denied.	3
NTP Session In Progress	18260	Indicates that an NTP session is in progress.	1
NNTP Session Opened	18261	Indicates that a Network News Transfer Protocol (NNTP) session was established.	1
NNTP Session Closed	18262	Indicates that an NNTP session was closed.	1
NNTP Session Reset	18263	Indicates that an NNTP session was reset.	3
NNTP Session Terminated	18264	Indicates that an NNTP session was terminated.	3
NNTP Session Denied	18265	Indicates that an NNTP session was denied.	3
NNTP Session In Progress	18266	Indicates that an NNTP session is in progress.	1
NFS Session Opened	18267	Indicates that a Network File System (NFS) session was established.	1
NFS Session Closed	18268	Indicates that an NFS session was closed.	1
NFS Session Reset	18269	Indicates that an NFS session was reset.	3
NFS Session Terminated	18270	Indicates that an NFS session was terminated.	3
NFS Session Denied	18271	Indicates that an NFS session was denied.	3
NFS Session In Progress	18272	Indicates that an NFS session is in progress.	1
NCP Session Opened	18273	Indicates that a Network Control Program (NCP) session was established.	1
NCP Session Closed	18274	Indicates that an NCP session was closed.	1
NCP Session Reset	18275	Indicates that an NCP session was reset.	3

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
NCP Session Terminated	18276	Indicates that an NCP session was terminated.	3
NCP Session Denied	18277	Indicates that an NCP session was denied.	3
NCP Session In Progress	18278	Indicates that an NCP session is in progress.	1
NetBIOS Session Opened	18279	Indicates that a NetBIOS session was established.	1
NetBIOS Session Closed	18280	Indicates that a NetBIOS session was closed.	1
NetBIOS Session Reset	18281	Indicates that a NetBIOS session was reset.	3
NetBIOS Session Terminated	18282	Indicates that a NetBIOS session was terminated.	3
NetBIOS Session Denied	18283	Indicates that a NetBIOS session was denied.	3
NetBIOS Session In Progress	18284	Indicates that a NetBIOS session is in progress.	1
MODBUS Session Opened	18285	Indicates that a MODBUS session was established.	1
MODBUS Session Closed	18286	Indicates that a MODBUS session was closed.	1
MODBUS Session Reset	18287	Indicates that a MODBUS session was reset.	3
MODBUS Session Terminated	18288	Indicates that a MODBUS session was terminated.	3
MODBUS Session Denied	18289	Indicates that a MODBUS session was denied.	3
MODBUS Session In Progress	18290	Indicates that a MODBUS session is in progress.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
LPD Session Opened	18291	Indicates that a Line Printer Daemon (LPD) session was established.	1
LPD Session Closed	18292	Indicates that an LPD session was closed.	1
LPD Session Reset	18293	Indicates that an LPD session was reset.	3
LPD Session Terminated	18294	Indicates that an LPD session was terminated.	3
LPD Session Denied	18295	Indicates that an LPD session was denied.	3
LPD Session In Progress	18296	Indicates that an LPD session is in progress.	1
Lotus Notes® Session Opened	18297	Indicates that a Lotus Notes session was established.	1
Lotus Notes Session Closed	18298	Indicates that a Lotus Notes session was closed.	1
Lotus Notes Session Reset	18299	Indicates that a Lotus Notes session was reset.	3
Lotus Notes Session Terminated	18300	Indicates that a Lotus Notes session was terminated.	3
Lotus Notes Session Denied	18301	Indicates that a Lotus Notes session was denied.	3
Lotus Notes Session In Progress	18302	Indicates that a Lotus Notes session is in progress.	1
Kerberos Session Opened	18303	Indicates that a Kerberos session was established.	1
Kerberos Session Closed	18304	Indicates that a Kerberos session was closed.	1
Kerberos Session Reset	18305	Indicates that a Kerberos session was reset.	3
Kerberos Session Terminated	18306	Indicates that a Kerberos session was terminated.	3

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Kerberos Session Denied	18307	Indicates that a Kerberos session was denied.	3
Kerberos Session In Progress	18308	Indicates that a Kerberos session is in progress.	1
IRC Session Opened	18309	Indicates that an Internet Relay Chat (IRC) session was established.	1
IRC Session Closed	18310	Indicates that an IRC session was closed.	1
IRC Session Reset	18311	Indicates that an IRC session was reset.	3
IRC Session Terminated	18312	Indicates that an IRC session was terminated.	3
IRC Session Denied	18313	Indicates that an IRC session was denied.	3
IRC Session In Progress	18314	Indicates that an IRC session is in progress.	1
IEC 104 Session Opened	18315	Indicates that an IEC 104 session was established.	1
IEC 104 Session Closed	18316	Indicates that an IEC 104 session was closed.	1
IEC 104 Session Reset	18317	Indicates that an IEC 104 session was reset.	3
IEC 104 Session Terminated	18318	Indicates that an IEC 104 session was terminated.	3
IEC 104 Session Denied	18319	Indicates that an IEC 104 session was denied.	3
IEC 104 Session In Progress	18320	Indicates that an IEC 104 session is in progress.	1
Ident Session Opened	18321	Indicates that a TCP Client Identity Protocol (Ident) session was established.	1
Ident Session Closed	18322	Indicates that an Ident session was closed.	1
Ident Session Reset	18323	Indicates that an Ident session was reset.	3

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Ident Session Terminated	18324	Indicates that an Ident session was terminated.	3
Ident Session Denied	18325	Indicates that an Ident session was denied.	3
Ident Session In Progress	18326	Indicates that an Ident session is in progress.	1
ICCP Session Opened	18327	Indicates that an Inter-Control Center Communications Protocol (ICCP) session was established.	1
ICCP Session Closed	18328	Indicates that an ICCP session was closed.	1
ICCP Session Reset	18329	Indicates that an ICCP session was reset.	3
ICCP Session Terminated	18330	Indicates that an ICCP session was terminated.	3
ICCP Session Denied	18331	Indicates that an ICCP session was denied.	3
ICCP Session In Progress	18332	Indicates that an ICCP session is in progress.	1
GroupWiseSession Opened	18333	Indicates that a GroupWisesession was established.	1
GroupWiseSession Closed	18334	Indicates that a GroupWise session was closed.	1
GroupWiseSession Reset	18335	Indicates that a GroupWisesession was reset.	3
GroupWiseSession Terminated	18336	Indicates that a GroupWisesession was terminated.	3
GroupWiseSession Denied	18337	Indicates that a GroupWise session was denied.	3
GroupWiseSession In Progress	18338	Indicates that a GroupWise session is in progress.	1
Gopher Session Opened	183398	Indicates that a Gopher session was established.	1
Gopher Session Closed	18340	Indicates that a Gopher session was closed.	1

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Gopher Session Reset	18341	Indicates that a Gopher session was reset.	3
Gopher Session Terminated	18342	Indicates that a Gopher session was terminated.	3
Gopher Session Denied	18343	Indicates that a Gopher session was denied.	3
Gopher Session In Progress	18344	Indicates that a Gopher session is in progress.	1
GIOP Session Opened	18345	Indicates that a General Inter-ORB Protocol (GIOP) session was established.	1
GIOP Session Closed	18346	Indicates that a GIOP session was closed.	1
GIOP Session Reset	18347	Indicates that a GIOP session was reset.	3
GIOP Session Terminated	18348	Indicates that a GIOP session was terminated.	3
GIOP Session Denied	18349	Indicates that a GIOP session was denied.	3
GIOP Session In Progress	18350	Indicates that a GIOP session is in progress.	1
Finger Session Opened	18351	Indicates that a Finger session was established.	1
Finger Session Closed	18352	Indicates that a Finger session was closed.	1
Finger Session Reset	18353	Indicates that a Finger session was reset.	3
Finger Session Terminated	18354	Indicates that a Finger session was terminated.	3
Finger Session Denied	18355	Indicates that a Finger session was denied.	3
Finger Session In Progress	18356	Indicates that a Finger session is in progress.	1
Echo Session Opened	18357	Indicates that an Echo session was established.	1
Echo Session Closed	18358	Indicates that an Echo session was closed.	1
Echo Session Denied	18359	Indicates that an Echo session was denied.	3
Echo Session In Progress	18360	Indicates that an Echo session is in progress.	1



*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Remote .NET Session Opened	18361	Indicates that a Remote .NET session was established.	1
Remote .NET Session Closed	18362	Indicates that a Remote .NET session was closed.	1
Remote .NET Session Reset	18363	Indicates that a Remote .NET session was reset.	3
Remote .NET Session Terminated	18364	Indicates that a Remote .NET session was terminated.	3
Remote .NET Session Denied	18365	Indicates that a Remote .NET session was denied.	3
Remote .NET Session In Progress	18366	Indicates that a Remote .NET session is in progress.	1
DNP3 Session Opened	18367	Indicates that a Distributed Network Proctologic (DNP3) session was established.	1
DNP3 Session Closed	18368	Indicates that a DNP3 session was closed.	1
DNP3 Session Reset	18369	Indicates that a DNP3 session was reset.	3
DNP3 Session Terminated	18370	Indicates that a DNP3 session was terminated.	3
DNP3 Session Denied	18371	Indicates that a DNP3 session was denied.	3
DNP3 Session In Progress	18372	Indicates that a DNP3 session is in progress.	1
Discard Session Opened	18373	Indicates that a Discard session was established.	1
Discard Session Closed	18374	Indicates that a Discard session was closed.	1
Discard Session Reset	18375	Indicates that a Discard session was reset.	3
Discard Session Terminated	18376	Indicates that a Discard session was terminated.	3
Discard Session Denied	18377	Indicates that a Discard session was denied.	3

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Discard Session In Progress	18378	Indicates that a Discard session is in progress.	1
DHCP Session Opened	18379	Indicates that a Dynamic Host Configuration Protocol (DHCP) session was established.	1
DHCP Session Closed	18380	Indicates that a DHCP session was closed.	1
DHCP Session Denied	18381	Indicates that a DHCP session was denied.	3
DHCP Session In Progress	18382	Indicates that a DHCP session is in progress.	1
DHCP Success	18383	Indicates that a DHCP lease was successfully obtained	1
DHCP Failure	18384	Indicates that a DHCP lease cannot be obtained.	3
CVS Session Opened	18385	Indicates that a Concurrent Versions System (CVS) session was established.	1
CVS Session Closed	18386	Indicates that a CVS session was closed.	1
CVS Session Reset	18387	Indicates that a CVS session was reset.	3
CVS Session Terminated	18388	Indicates that a CVS session was terminated.	3
CVS Session Denied	18389	Indicates that a CVS session was denied.	3
CVS Session In Progress	18390	Indicates that a CVS session is in progress.	1
CUPS Session Opened	18391	Indicates that a Common UNIX Printing System (CUPS) session was established.	1
CUPS Session Closed	18392	Indicates that a CUPS session was closed.	1
CUPS Session Reset	18393	Indicates that a CUPS session was reset.	3
CUPS Session Terminated	18394	Indicates that a CUPS session was terminated.	3

*Table 104. Low-level categories and severity levels for the application category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
CUPS Session Denied	18395	Indicates that a CUPS session was denied.	3
CUPS Session In Progress	18396	Indicates that a CUPS session is in progress.	1
Chargen Session Started	18397	Indicates that a Character Generator (Chargen) session was started.	1
Chargen Session Closed	18398	Indicates that a Chargen session was closed.	1
Chargen Session Reset	18399	Indicates that a Chargen session was reset.	3
Chargen Session Terminated	18400	Indicates that a Chargen session was terminated.	3
Chargen Session Denied	18401	Indicates that a Chargen session was denied.	3
Chargen Session In Progress	18402	Indicates that a Chargen session is in progress.	1
Misc VPN	18403	Indicates that a miscellaneous VPN session was detected	1
DAP Session Started	18404	Indicates that a DAP session was established.	1
DAP Session Ended	18405	Indicates that a DAP session ended.	1
DAP Session Denied	18406	Indicates that a DAP session was denied.	3
DAP Session Status	18407	Indicates that a DAP session status request was made.	1
DAP Session in Progress	18408	Indicates that a DAP session is in progress.	1
DAP Authentication Failed	18409	Indicates that a DAP authentication failed.	4
DAP Authentication Succeeded	18410	Indicates that DAP authentication succeeded.	1
TOR Session Started	18411	Indicates that a TOR session was established.	1
TOR Session Closed	18412	Indicates that a TOR session was closed.	1

Table 104. Low-level categories and severity levels for the application category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
TOR Session Reset	18413	Indicates that a TOR session was reset.	3
TOR Session Terminated	18414	Indicates that a TOR session was terminated.	3
TOR Session Denied	18415	Indicates that a TOR session was denied.	3
TOR Session In Progress	18416	Indicates that a TOR session is in progress.	1
Game Session Started	18417	Indicates that a game session was started.	1
Game Session Closed	18418	Indicates that a game session was closed.	1
Game Session Reset	18419	Indicates that a game session was reset.	3
Game Session Terminated	18420	Indicates that a game session was terminated.	3
Game Session Denied	18421	Indicates that a game session was denied.	3
Game Session In Progress	18422	Indicates that a game session is in progress.	1
Admin Login Attempt	18423	Indicates that an attempt to log in as an administrative user was detected.	2
User Login Attempt	18424	Indicates that an attempt to log in as a non-administrative user was detected.	2
Client Server	18425	Indicates client/server activity.	1
Content Delivery	18426	Indicates content delivery activity.	1
Data Transfer	18427	Indicates a data transfer.	3
Data Warehousing	18428	Indicates data warehousing activity.	3
Directory Services	18429	Indicates directory service activity.	2
File Print	18430	Indicates file print activity.	1
File Transfer	18431	Indicates file transfer.	2
Games	18432	Indicates game activity.	4

<i>Table 104. Low-level categories and severity levels for the application category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Healthcare	18433	Indicates healthcare activity.	1
Inner System	18434	Indicates inner system activity.	1
Internet Protocol	18435	Indicates Internet Protocol activity.	1
Legacy	18436	Indicates legacy activity.	1
Mail	18437	Indicates mail activity.	1
Misc	18438	Indicates miscellaneous activity.	2
Multimedia	18439	Indicates multimedia activity.	2
Network Management	18440	Indicates network management activity.	
P2P	18441	Indicates Peer-to-Peer (P2P) activity.	4
Remote Access	18442	Indicates Remote Access activity.	3
Routing Protocols	18443	Indicates routing protocol activity.	1
Security Protocols	18444	Indicates security protocol activity.	2
Streaming	18445	Indicates streaming activity.	2
Uncommon Protocol	18446	Indicates uncommon protocol activity.	3
VoIP	18447	Indicates VoIP activity.	1
Web	18448	Indicates web activity.	1
ICMP	18449	Indicates ICMP activity	1

## Audit

The audit category contains events that are related to audit activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the audit category.

<i>Table 105. Low-level categories and severity levels for the audit category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
General Audit Event	19001	Indicates that a general audit event was started.	1

*Table 105. Low-level categories and severity levels for the audit category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Built-in Execution	19002	Indicates that a built-in audit task was run.	1
Bulk Copy	19003	Indicates that a bulk copy of data was detected.	1
Data Dump	19004	Indicates that a data dump was detected.	1
Data Import	19005	Indicates that a data import was detected.	1
Data Selection	19006	Indicates that a data selection process was detected.	1
Data Truncation	19007	Indicates that the data truncation process was detected.	1
Data Update	19008	Indicates that the data update process was detected.	1
Procedure/Trigger Execution	19009	Indicates that the database procedure or trigger execution was detected.	1
Schema Change	19010	Indicates that the schema for a procedure or trigger execution was altered.	1
Create Activity Attempted	19011	Indicates that creating activity was attempted.	1
Create Activity Succeeded	19012	Indicates that creating activity was successful.	1
Create Activity Failed	19013	Indicates that creating activity failed.	3
Read Activity Attempted	19014	Indicates that a reading activity was attempted.	1
Read Activity Succeeded	19015	Indicates that a reading activity was successful.	1
Read Activity Failed	19016	Indicates that reading activity failed.	3
Update Activity Attempted	19017	Indicates that updating activity was attempted.	1
Update Activity Succeeded	19018	Indicates that updating activity was successful.	1

*Table 105. Low-level categories and severity levels for the audit category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Update Activity Failed	19019	Indicates that updating activity failed.	3
Delete Activity Attempted	19020	Indicates that deleting activity was attempted.	1
Delete Activity Succeeded	19021	Indicates that deleting activity was successful.	1
Delete Activity Failed	19022	Indicates that deleting activity failed.	3
Backup Activity Attempted	19023	Indicates that backup activity was attempted.	1
Backup Activity Succeeded	19024	Indicates that backup activity was successful.	1
Backup Activity Failed	19025	Indicates that backup activity failed.	3
Capture Activity Attempted	19026	Indicates that capturing activity was attempted.	1
Capture Activity Succeeded	19027	Indicates that capturing activity was successful.	1
Capture Activity Failed	19028	Indicates that capturing activity failed.	3
Configure Activity Attempted	19029	Indicates that configuration activity was attempted.	1
Configure Activity Succeeded	19030	Indicates that configuration activity was successful.	1
Configure Activity Failed	19031	Indicates that configuration activity failed.	3
Deploy Activity Attempted	19032	Indicates that deployment activity was attempted.	1
Deploy Activity Succeeded	19033	Indicates that deployment activity was successful.	1
Deploy Activity Failed	19034	Indicates that deployment activity failed.	3
Disable Activity Attempted	19035	Indicates that disabling activity was attempted.	1
Disable Activity Succeeded	19036	Indicates that disabling activity was successful.	1

*Table 105. Low-level categories and severity levels for the audit category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Disable Activity Failed	19037	Indicates that disabling activity failed.	3
Enable Activity Attempted	19038	Indicates that enabling activity was attempted.	1
Enable Activity Succeeded	19039	Indicates that enabling activity was successful.	1
Enable Activity Failed	19040	Indicates that enabling activity failed.	3
Monitor Activity Attempted	19041	Indicates that monitoring activity was attempted.	1
Monitor Activity Succeeded	19042	Indicates that monitoring activity was successful.	1
Monitor Activity Failed	19043	Indicates that monitoring activity failed.	3
Restore Activity Attempted	19044	Indicates that restoring activity was attempted.	1
Restore Activity Succeeded	19045	Indicates that restoring activity was successful.	1
Restore Activity Failed	19046	Indicates that restoring activity failed.	3
Start Activity Attempted	19047	Indicates that starting activity was attempted.	1
Start Activity Succeeded	19048	Indicates that starting activity was successful.	1
Start Activity Failed	19049	Indicates that starting activity failed.	3
Stop Activity Attempted	19050	Indicates that stopping activity was attempted.	1
Stop Activity Succeeded	19051	Indicates that stopping activity was successful.	1
Stop Activity Failed	19052	Indicates that stopping activity failed.	3
Undeploy Activity Attempted	19053	Indicates that undeploy activity was attempted.	1
Undeploy Activity Succeeded	19054	Indicates that undeploy activity was successful.	1
Undeploy Activity Failed	19055	Indicates that undeploy activity failed.	3



<i>Table 105. Low-level categories and severity levels for the audit category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Receive Activity Attempted	19056	Indicates that receiving activity was attempted.	1
Receive Activity Succeeded	19057	Indicates that receiving activity was successful.	1
Receive Activity Failed	19058	Indicates that receiving activity failed	3
Send Activity Attempted	19059	Indicates that sending activity was attempted.	1
Send Activity Succeeded	19060	Indicates that sending activity was successful.	1
Send Activity Failed	19061	Indicates that sending activity failed.	3

## Risk

The risk category contains events that are related to IBM Security QRadar Risk Manager.

The following table describes the low-level event categories and associated severity levels for the risk category.

<i>Table 106. Low-level categories and severity levels for the risk category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Policy Exposure	20001	Indicates that a policy exposure was detected.	5
Compliance Violation	20002	Indicates that a compliance violation was detected.	5
Exposed Vulnerability	20003	Indicates that the network or device has an exposed vulnerability.	9
Remote Access Vulnerability	20004	Indicates that the network or device has a remote access vulnerability.	9
Local Access Vulnerability	20005	Indicates that the network or device has local access vulnerability.	7
Open Wireless Access	20006	Indicates that the network or device has open wireless access.	5
Weak Encryption	20007	Indicates that the host or device has weak encryption.	5

*Table 106. Low-level categories and severity levels for the risk category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Un-Encrypted Data Transfer	20008	Indicates that a host or device is transmitting data that is not encrypted.	3
Un-Encrypted Data Store	20009	Indicates that the data store is not encrypted.	3
Mis-Configured Rule	20010	Indicates that a rule is not configured properly.	3
Mis-Configured Device	20011	Indicates that a device on the network is not configured properly.	3
Mis-Configured Host	20012	Indicates that a network host is not configured properly.	3
Data Loss Possible	20013	Indicates that the possibility of data loss was detected.	5
Weak Authentication	20014	Indicates that a host or device is susceptible to fraud.	5
No Password	20015	Indicates that no password exists.	7
Fraud	20016	Indicates that a host or device is susceptible to fraud.	7
Possible DoS Target	20017	Indicates a host or device is a possible DoS target.	3
Possible DoS Weakness	20018	Indicates a host or device has a possible DoS weakness.	3
Loss of Confidentiality	20019	Indicates that a loss of confidentiality was detected.	5
Policy Monitor Risk Score Accumulation	20020	Indicates that a policy monitor risk score accumulation was detected.	1

## Risk Manager Audit

The risk category contains events that are related to IBM Security QRadar Risk Manager audit events.

The following table describes the low-level event categories and associated severity levels for the Risk Manager audit category.

<i>Table 107. Low-level categories and severity levels for the Risk Manager audit category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Policy Monitor	21001	Indicates that a policy monitor was modified.	3
Topology	21002	Indicates that a topology was modified.	3
Simulations	21003	Indicates that a simulation was modified.	3
Administration	21004	Indicates that administrative changes were made.	3

## Control

The control category contains events that are related to your hardware system.

The following table describes the low-level event categories and associated severity levels for the control category.

<i>Table 108. Low-level categories and severity levels for the control category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Device Read	22001	Indicates that a device was read.	1
Device Communication	22002	Indicates communication with a device.	1
Device Audit	22003	Indicates that a device audit occurred.	1
Device Event	22004	Indicates that a device event occurred.	1
Device Ping	22005	Indicates that a ping action to a device occurred.	1
Device Configuration	22006	Indicates that a device was configured.	1
Device Registration	22007	Indicates that a device was registered.	1
Device Route	22008	Indicates that a device route action occurred.	1
Device Import	22009	Indicates that a device import occurred.	1
Device Information	22010	Indicates that a device information action occurred.	1

Table 108. Low-level categories and severity levels for the control category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Device Warning	22011	Indicates that a warning was generated on a device.	1
Device Error	22012	Indicates that an error was generated on a device.	1
Relay Event	22013	Indicates a relay event.	1
NIC Event	22014	Indicates a Network Interface Card (NIC) event.	1
UIQ Event	22015	Indicates an event on a mobile device.	1
IMU Event	22016	Indicates an event on an Integrated Management Unit (IMU).	1
Billing Event	22017	Indicates a billing event.	1
DBMS Event	22018	Indicates an event on the Database Management System (DBMS).	1
Import Event	22019	Indicates that an import occurred.	1
Location Import	22020	Indicates that a location import occurred.	1
Route Import	22021	Indicates that a route import occurred.	1
Export Event	22022	Indicates that an export occurred.	1
Remote Signaling	22023	Indicates remote signaling.	1
Gateway Status	22024	Indicates gateway status.	1
Job Event	22025	Indicates that a job occurred.	1
Security Event	22026	Indicates that a security event occurred.	1
Device Tamper Detection	22027	Indicates that the system detected a tamper action.	1
Time Event	22028	Indicates that a time event occurred.	1

<i>Table 108. Low-level categories and severity levels for the control category (continued)</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Suspicious Behavior	22029	Indicates that suspicious behavior occurred.	1
Power Outage	22030	Indicates that a power outage occurred.	1
Power Restoration	22031	Indicates that power was restored.	1
Heartbeat	22032	Indicates that a heartbeat ping occurred.	1
Remote Connection Event	22033	Indicates a remote connection to the system.	1

## Asset Profiler

The asset profiler category contains events that are related to asset profiles.

The following table describes the low-level event categories and associated severity levels for the asset profiler category.

<i>Table 109. Low-level categories and severity levels for the asset profiler category</i>			
<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Asset Created	23001	Indicates that an asset was created.	1
Asset Updated	23002	Indicates that an asset was updated.	1
Asset Observed	23003	Indicates that an asset was observed.	1
Asset Moved	23004	Indicates that an asset was moved.	1
Asset Deleted	23005	Indicates that an asset was deleted.	1
Asset Hostname Cleaned	23006	Indicates that a host name was cleaned.	1
Asset Hostname Created	23007	Indicates that a host name was created.	1
Asset Hostname Updated	23008	Indicates that a host name was updated.	1
Asset Hostname Observed	23009	Indicates that a host name was observed.	1
Asset Hostname Moved	23010	Indicates that a host name was moved.	1

Table 109. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Asset Hostname Deleted	23011	Indicates that a host name was deleted.	1
Asset Port Cleaned	23012	Indicates that a port was cleaned.	1
Asset Port Created	23013	Indicates that a port was created.	1
Asset Port Updated	23014	Indicates that a port was updated.	1
Asset Port Observed	23015	Indicates that a port was observed.	1
Asset Port Moved	23016	Indicates that a port was moved.	1
Asset Port Deleted	23017	Indicates that a port was deleted.	1
Asset Vuln Instance Cleaned	23018	Indicates that a vulnerability instance was cleaned.	1
Asset Vuln Instance Created	23019	Indicates that a vulnerability instance was created.	1
Asset Vuln Instance Updated	23020	Indicates that a vulnerability instance was updated.	1
Asset Vuln Instance Observed	23021	Indicates that a vulnerability instance was observed.	1
Asset Vuln Instance Moved	23022	Indicates that a vulnerability instance was moved.	1
Asset Vuln Instance Deleted	23023	Indicates that a vulnerability instance was deleted.	1
Asset OS Cleaned	23024	Indicates that an operating system was cleaned.	1
Asset OS Created	23025	Indicates that an operating system was created.	1
Asset OS Updated	23026	Indicates that an operating system was updated.	1

*Table 109. Low-level categories and severity levels for the asset profiler category (continued)*

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
Asset OS Observed	23027	Indicates that an operating system was observed.	1
Asset OS Moved	23028	Indicates that an operating system was moved.	1
Asset OS Deleted	23029	Indicates that an operating system was deleted.	1
Asset Property Cleaned	23030	Indicates that a property was cleaned.	1
Asset Property Created	23031	Indicates that a property was created.	1
Asset Property Updated	23032	Indicates that a property was updated.	1
Asset Property Observed	23033	Indicates that a property was observed.	1
Asset Property Moved	23034	Indicates that a property was moved.	1
Asset Property Deleted	23035	Indicates that a property was moved.	1
Asset IP Address Cleaned	23036	Indicates that an IP address was cleaned.	1
Asset IP Address Created	23037	Indicates that an IP address was created.	1
Asset IP Address Updated	23038	Indicates that an IP address was updated.	1
Asset IP Address Observed	23039	Indicates that an IP address was observed.	1
Asset IP Address Moved	23040	Indicates that an IP address was moved.	1
Asset IP Address Deleted	23041	Indicates that an IP address was deleted.	1
Asset Interface Cleaned	23042	Indicates that an interface was cleaned.	1
Asset Interface Created	23043	Indicates that an interface was created.	1
Asset Interface Updated	23044	Indicates that an interface was updated.	1
Asset Interface Observed	23045	Indicates that an interface was observed.	1

Table 109. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Asset Interface Moved	23046	Indicates that an interface was moved.	1
Asset Interface Merged	23047	Indicates that an interface was merged.	1
Asset Interface Deleted	23048	Indicates that an interface was deleted.	1
Asset User Cleaned	23049	Indicates that a user was cleaned.	1
Asset User Observed	23050	Indicates that a user was observed.	1
Asset User Moved	23051	Indicates that a user was moved.	1
Asset User Deleted	23052	Indicates that a user was deleted.	1
Asset Scanned Policy Cleaned	23053	Indicates that a scanned policy was cleaned.	1
Asset Scanned Policy Observed	23054	Indicates that a scanned policy was observed.	1
Asset Scanned Policy Moved	23055	Indicates that a scanned policy was moved.	1
Asset Scanned Policy Deleted	23056	Indicates that a scanned policy was deleted.	1
Asset Windows Application Cleaned	23057	Indicates that a Windows application was cleaned.	1
Asset Windows Application Observed	23058	Indicates that a Windows application was observed.	1
Asset Windows Application Moved	23059	Indicates that a Windows application was moved.	1
Asset Windows Application Deleted	23060	Indicates that a Windows application was deleted.	1
Asset Scanned Service Cleaned	23061	Indicates that a scanned service was cleaned.	1
Asset Scanned Service Observed	23062	Indicates that a scanned service was observed.	1
Asset Scanned Service Moved	23063	Indicates that a scanned service was moved.	1
Asset Scanned Service Deleted	23064	Indicates that a scanned service was deleted.	1



Table 109. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Asset Windows Patch Cleaned	23065	Indicates that a Windows patch was cleaned.	1
Asset Windows Patch Observed	23066	Indicates that a Windows patch was observed.	1
Asset Windows Patch Moved	23067	Indicates that a Windows patch was moved.	1
Asset Windows Patch Deleted	23068	Indicates that a Windows patch was deleted.	1
Asset UNIX Patch Cleaned	23069	Indicates that a UNIX patch was cleaned.	1
Asset UNIX Patch Observed	23070	Indicates that a UNIX patch was observed.	1
Asset UNIX Patch Moved	23071	Indicates that a UNIX patch was moved.	1
Asset UNIX Patch Deleted	23072	Indicates that a UNIX patch was deleted.	1
Asset Patch Scan Cleaned	23073	Indicates that a patch scan was cleaned.	1
Asset Patch Scan Created	23074	Indicates that a patch scan was created.	1
Asset Patch Scan Moved	23075	Indicates that a patch scan was moved.	1
Asset Patch Scan Deleted	23076	Indicates that a patch scan was deleted.	1
Asset Port Scan Cleaned	23077	Indicates that a port scan was cleaned.	1
Asset Port Scan Created	23078	Indicates that a port scan was cleaned.	1
Asset Port Scan Moved	23079	Indicates that a patch scan was moved.	1
Asset Port Scan Deleted	23080	Indicates that a patch scan was deleted.	1
Asset Client Application Cleaned	23081	Indicates that a client application was cleaned.	1
Asset Client Application Observed	23082	Indicates that a client application was observed.	1

Table 109. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Category ID	Description	Severity level (0 - 10)
Asset Client Application Moved	23083	Indicates that a client application was moved.	1
Asset Client Application Deleted	23084	Indicates that a client application was deleted.	1
Asset Patch Scan Observed	23085	Indicates that a patch scan was observed.	1
Asset Port Scan Observed	23086	Indicates that a port scan was observed.	1
NetBIOS Group Created	23087	Indicates that a NetBIOS group was created.	1
NetBIOS Group Updated	23088	Indicates that a NetBIOS group was updated.	1
NetBIOS Group Observed	23089	Indicates that a NetBIOS group was observed.	1
NetBIOS Group Deleted	23090	Indicates that a NetBIOS group was deleted.	1
NetBIOS Group Cleaned	23091	Indicates that a NetBIOS group was cleaned.	1
NetBIOS Group Moved	23092	Indicates that a NetBIOS group was moved.	1

## Sense

The sense category contains events that are related to sense user behavior analytics.

The following table describes the low-level event categories and associated severity levels for the sense category.

Table 110.

Low-level event category	Category ID	Description	Severity level (0 - 10)
User Behavior	24001	Indicates the user's behavior.	5
User Geography	24002	Indicates the user's geography.	5
User Time	24003	Indicates the user's time.	5

Table 110. (continued)

<b>Low-level event category</b>	<b>Category ID</b>	<b>Description</b>	<b>Severity level (0 - 10)</b>
User Access	24004	Indicates the user's access.	5
User Privilege	24005	Indicates the user's privilege.	5
User Risk	24006	Indicates the user's risk.	5
Sense Offense	24007	Indicates that a sense offense occurred.	5
Resource Risk	24008	Indicates the resources that are at risk.	5



---

## Chapter 26. Common ports and servers used by QRadar

IBM Security QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

### SSH communication on port 22

All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. IBM Security QRadar QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

### Open ports that are not required by QRadar

You might find additional open ports in the following situations:

- When you install QRadar on your own hardware, you may see open ports that are used by services, daemons, and programs included in Red Hat Enterprise Linux.
- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as `rpc.mountd` and `rpc.rquotad`.

### Related concepts

[Capabilities in your IBM Security QRadar product](#)

---

## QRadar port usage

Review the list of common ports that IBM Security QRadar services and components use to communicate across the network. You can use the port list to determine which ports must be open in your network. For example, you can determine which ports must be open for the QRadar Console to communicate with remote event processors.

### WinCollect remote polling

WinCollect agents that remotely poll other Microsoft Windows operating systems might require additional port assignments.

For more information, see the IBM Security QRadar WinCollect *User Guide*.

### QRadar listening ports

The following table shows the QRadar ports that are open in a LISTEN state. The LISTEN ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all QRadar products.

Table 111. Listening ports that are used by QRadar services and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the QRadar Console to all other components.	<p>Remote management access.</p> <p>Adding a remote system as a managed host.</p> <p>Log source protocols to retrieve files from external devices, for example the log file protocol.</p> <p>Users who use the command-line interface to communicate from desktops to the Console.</p> <p>High-availability (HA).</p>
25	SMTP	TCP	From all managed hosts to the SMTP gateway.	<p>Emails from QRadar to an SMTP gateway.</p> <p>Delivery of error and warning email messages to an administrative email contact.</p>
111	Port mapper	TCP/UDP	<p>Managed hosts that communicate with the QRadar Console.</p> <p>Users that connect to the QRadar Console.</p>	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
123	Network Time Protocol (NTP)	TCP/UDP	QRadar Console to the NTP server. HA primary to secondary, and vice versa.	Time synchronization between QRadar HA pairs, and between the QRadar Console and the NTP server.
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or IBM Security QRadar event collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	<p>This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.</p> <p><b>Note:</b> DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.</p>
137	Windows NetBIOS name service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
138	Windows NetBIOS datagram service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows NetBIOS session service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
162	NetSNMP	UDP	<p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>	UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
199	NetSNMP	TCP	<p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
427	Service Location Protocol (SLP)	UDP/TCP		The Integrated Management Module uses the port to find services on a LAN.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console.	<p>Configuration downloads to managed hosts from the QRadar Console.</p> <p>QRadar managed hosts that connect to the QRadar Console.</p> <p>Users to have log in access to QRadar.</p> <p>QRadar Console that manage and provide configuration updates for WinCollect agents.</p>

Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
445	Microsoft Directory Service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	<p>External network appliances that provide TCP syslog events use bidirectional traffic.</p> <p>External network appliances that provide UDP syslog events use unidirectional traffic.</p> <p>Internal syslog traffic from QRadar hosts to the QRadar Console.</p>	<p>External log sources to send event data to QRadar components.</p> <p>Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar.</p>
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.	Internal logging port for syslog-ng.
2049	NFS	TCP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) protocol to share files or data between components.
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the IBM Security QRadar QFlow Collector.	NetFlow datagram from components, such as routers.
2375	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage QRadar application framework resources.
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Microsoft Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.
3900	Integrated Management Module remote presence port	TCP/UDP		Use this port to interact with the QRadar console through the Integrated Management Module.



Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution.
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Required for provisioning managed hosts from the <b>Admin</b> tab.
6514	Syslog	TCP	External network appliances that provide encrypted TCP syslog events use bidirectional traffic.	External log sources to send encrypted event data to QRadar components.
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure.
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	<p>Message queue broker for communications between components on a managed host.</p> <p><b>Note:</b> You must permit access to these ports from the QRadar console to unencrypted hosts.</p> <p>Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports. For more information about finding randomly bound ports, see <a href="#">“Viewing IMQ port associations”</a> on page 376.</p>
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	JMX server ports	TCP	Internal communications. These ports are not available externally.	<p>JMX server (Java Management Beans) monitoring for all internal QRadar processes to expose supportability metrics.</p> <p>These ports are used by QRadar support.</p>
7789	HA Distributed Replicated Block Device	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations.
7800	Apache Tomcat	TCP	From the Event Collector to the QRadar Console.	Real-time (streaming) for events.
7801	Apache Tomcat	TCP	From the Event Collector to the QRadar Console.	Real-time (streaming) for flows.
7803	Apache Tomcat	TCP	From the Event Collector to the QRadar Console.	Anomaly detection engine port.
7804	QRM Arc builder	TCP	Internal control communications between QRadar processes and ARC builder.	This port is used for QRadar Risk Manager only. It is not available externally.
8000	Event Collection service (ECS)	TCP	From the Event Collector to the QRadar Console.	Listening port for specific Event Collection Service (ECS).

Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
8001	SNMP daemon port	UDP	External SNMP systems that request SNMP trap information from the QRadar Console.	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat.  This port is bound and only accepts connections from the local host.
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and QRadar Console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.
8844	Apache Tomcat	TCP	Unidirectional from the QRadar Console to the appliance that is running the QRadar Vulnerability Manager processor.	Used by Apache Tomcat to read RSS feeds from the host that is running the QRadar Vulnerability Manager processor.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between QRadar processes and the XForce Reputation IP database.
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QRadar QFlow Collector.	NetFlow datagram from components, such as routers.
9999	IBM Security QRadar Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the QRadar Vulnerability Manager processor	Used for QRadar Vulnerability Manager (QVM) command information. The QRadar Console connects to this port on the host that is running the QRadar Vulnerability Manager processor. This port is only used when QVM is enabled.
10000	QRadar web-based, system administration interface	TCP/UDP	User desktop systems to all QRadar hosts.	In QRadar V7.2.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access.  Port 10000 is disabled in V7.2.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.

Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for QRadar Vulnerability Manager (QVM) configuration and storage. This port is only used when QVM is enabled.
20000-23000	SSH Tunnel	TCP	Bidirectional from the QRadar Console to all other encrypted managed hosts.	Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to QRadar appliances with a Fibre Channel card.	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt).
32000	Normalized flow forwarding	TCP	Bidirectional between QRadar components.	Normalized event data that is communicated from an off-site source or between QRadar QFlow Collectors.
32004	Normalized event forwarding	TCP	Bidirectional between QRadar components.	Normalized event data that is communicated from an off-site source or between QRadar Event Collectors.
32005	Data flow	TCP	Bidirectional between QRadar components.	Data flow communication port between QRadar Event Collectors when on separate managed hosts.
32006	Ariel queries	TCP	Bidirectional between QRadar components.	Communication port between the Ariel proxy server and the Ariel query server.
32007	Offense data	TCP	Bidirectional between QRadar components.	Events and flows contributing to an offense or involved in global correlation.
32009	Identity data	TCP	Bidirectional between QRadar components.	Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).
32010	Flow listening source port	TCP	Bidirectional between QRadar components.	Flow listening port to collect data from QRadar QFlow Collectors.
32011	Ariel listening port	TCP	Bidirectional between QRadar components.	Ariel listening port for database searches, progress information, and other associated commands.
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components.	Data flows, such as events, flows, flow context, and event search queries.

Table 111. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
40799	PCAP data	UDP	From Juniper Networks SRX Series appliances to QRadar.	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances.  <b>Note:</b> The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation.
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster.	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).

## Viewing IMQ port associations

Several ports that are used by IBM Security QRadar allocate extra random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ by using telnet to connect to the local host and doing a lookup on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports that are generated for the service are reallocated and the service is provided with a new set of port numbers.

### Procedure

1. Using SSH, log in to the QRadar Console as the root user.
2. To display a list of associated ports for the IMQ messaging connection, type the following command:

```
telnet localhost 7676
```

The results from the telnet command might look similar to this output:

```
[root@domain ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
[imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
cluster_discovery tcp CLUSTER_DISCOVERY 44913
jmximi imi JMX 0 [url=service:jmx:imi://domain.ibm.com/stub/<urlpath>]
admin tcp ADMIN 43691
jms tcp NORMAL 7677
cluster tcp CLUSTER 36615
```

The telnet output shows 3 of the 4 random high-numbered TCP ports for IMQ. The fourth port, which is not shown, is a JMX Remote Method Invocation (RMI) port that is available over the JMX URL that is shown in the output.

If the telnet connection is refused, it means that IMQ is not currently running. It is probable that the system is either starting up or shutting down, or that services were shut down manually.

## Searching for ports in use by QRadar

Use the **netstat** command to determine which ports are in use on the IBM Security QRadar Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

### Procedure

1. Using SSH, log in to your QRadar Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

```
netstat -nap
```

3. To search for specific information from the netstat port list, type the following command:

```
netstat -nap | grep port
```

### Examples:

- To display all ports that match 199, type the following command:

```
netstat -nap | grep 199
```

- To display information on all listening ports, type the following command:

```
netstat -nap | grep LISTEN
```

## QRadar public servers

To provide you with the most current security information, IBM Security QRadar requires access to a number of public servers and RSS feeds.

### Public servers

Table 112. Public servers that QRadar must access. This table lists descriptions for the IP addresses or host names that QRadar accesses.	
IP address or hostname	Description
194.153.113.31	IBM Security QRadar Vulnerability Manager DMZ scanner
194.153.113.32	QRadar Vulnerability Manager DMZ scanner
qmmunity.q1labs.com	QRadar auto-update servers. For more information about auto-update servers, see <a href="http://www.ibm.com/support/docview.wss?uid=swg21958881">www.ibm.com/support</a> (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).
qmmunity-eu.q1labs.com	QRadar auto-update servers. For more information about auto-update servers, see <a href="http://www.ibm.com/support/docview.wss?uid=swg21958881">www.ibm.com/support</a> (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).
update.xforce-security.com	X-Force Threat Feed update server

*Table 112. Public servers that QRadar must access.* This table lists descriptions for the IP addresses or host names that QRadar accesses. (continued)

IP address or hostname	Description
license.xforce-security.com	X-Force Threat Feed licensing server

## RSS feeds for QRadar products

*Table 113. RSS feeds .* The following list describes the requirements for RSS feeds that QRadar uses. Copy URLs into a text editor and remove page breaks before pasting into a browser.

Title	URL	Requirements
Security Intelligence	<a href="http://feeds.feedburner.com/SecurityIntelligence">http://feeds.feedburner.com/SecurityIntelligence</a>	QRadar and an Internet connection
Security Intelligence Vulns / Threats	<a href="http://securityintelligence.com/topics/vulnerabilities-threats/feed">http://securityintelligence.com/topics/vulnerabilities-threats/feed</a>	QRadar and an Internet connection
IBM My Notifications	<a href="http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.reqid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgoth&amp;feeder.maxfeed=25">http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.reqid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgoth&amp;feeder.maxfeed=25</a>	QRadar and an Internet connection
Security News	<a href="http://IP_address_of_QVM_processor:8844/rss/research/news.rss">http://IP_address_of_QVM_processor:8844/rss/research/news.rss</a>	IBM Security QRadar Vulnerability Manager processor is deployed
Security Advisories	<a href="http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss">http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss</a>	QRadar Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	<a href="http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss">http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss</a>	QRadar Vulnerability Manager processor deployed
Scans Completed	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss</a>	QRadar Vulnerability Manager processor is deployed
Scans In Progress	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss</a>	QRadar Vulnerability Manager processor is deployed

## Docker containers and network interfaces

A Docker network defines a communication trust zone where communication is unrestricted between containers in that network.

Each network is associated with a bridge interface on the host, and firewall rules are defined to filter traffic between these interfaces. Typically, containers within a zone that share the same Docker network and host bridge interface can communicate with each other. An exception to this general rule is that apps run on the same docker network, but are isolated from each other by the firewall.

### Docker interfaces

To view a list of Docker interfaces, type the following command:

```
docker network ls
```

Here's an example of the output:

```
[root@q1dk00 ~]# docker network ls
NETWORK ID NAME DRIVER SCOPE
943dd35a4747 appProxy bridge local
9e2ba36111d1 dockerApps bridge local
514471d98b42 dockerInfra bridge local
```

The `dockerApps` interface is used to apply rules for communication between apps.

The `appProxy` interface displays the `nginx_framework_apps_proxy` container.

The `dockerInfra` interface is used to host `service_launcher` and `qoauth`. Apps are isolated from most infrastructure components but they must be able to connect to `service_launcher` and `qoauth` to manage secrets and authorization.

### Information about Docker interfaces

Type the following command to get information about Docker interfaces:

```
docker inspect <docker_container_ID> | grep NetworkMode
```

Here's an example of the output:

```
"NetworkMode": "appProxy"
```

This example shows how you use the **`docker inspect <docker_container_ID>`** command and pipe it to **`less`** to view more network details:

```
docker inspect d9b3e58649de | less
```

Here's an example of the output:

```
"Networks": {
 "dockerApps": {
 "IPAMConfig": null,
 "Links": null,
 "Aliases": [
 "d9b3e58649de"
], "NetworkID":
 "79bc4716da5139a89cfa5360a3b72824e67701523768822d11b53caeea5e349e",
 "EndpointID":
 "9dba9d9a174b037f72333945b72cdf60c3719fdb9a3a10a14a8ee3cc0e92a856",
 "Gateway": "172.18.0.1",
 "IPAddress": "172.18.0.2",
 "IPPrefixLen": 16,
 "IPv6Gateway": "2003:db8:1::1",
 "GlobalIPv6Address": "2003:db8:1::2",
 "GlobalIPv6PrefixLen": 64,
 "MacAddress": "02:42:ac:12:00:02"
 }
}
```

The output in this example shows the configuration of the network that is used by the specified container (`d9b3e58649de`), and shows the Docker network interface name (`dockerApps`) and the IP address of the network that is assigned to the Docker container.





---

## Chapter 27. RESTful API

The representational state transfer (REST) application programming interface (API) is useful when you want to integrate IBM Security QRadar with other solutions. You can perform actions on the QRadar Console by sending HTTPS requests to specific endpoints (URLs) on the QRadar Console.

Each endpoint contains the URL of the resource that you want to access and the action that you want to complete on that resource. The action is indicated by the HTTP method of the request: GET, POST, PUT, or DELETE. For more information about the parameters and responses for each endpoint, see the *IBM Security QRadar API Guide*.

### QRadar API forum and code samples

The API forum provides more information about the REST API, including the answers to frequently asked questions and annotated code samples that you can use in a test environment. For more information, see the [API forum](https://ibm.biz/qradarforums) (<https://ibm.biz/qradarforums>).

---

## Accessing the interactive API documentation page

Use the interactive API documentation page to access technical details for the RESTful APIs and experiment with making API requests to your server.

### About this task

The API documentation user interface provides descriptions and the ability to use the following REST API interfaces:

Table 114. REST API interfaces	
REST API	Description
/api/analytics	Create, update, and remove custom actions for rules.
/api/ariel	View event and flow properties, create event and flow searches, and manage searches.
/api/asset_model	Returns a list of all assets in the model. You can also list all available asset property types and saved searches, and update an asset.
/api/auth	Log out and invalidate the current session.
/api/config	View and manage tenants, domains, and QRadar extensions.
/api/data_classification	View all high and low level categories, QRadar Identifier (QID) records, and event mappings. You can also create or edit QID records and mappings.
/api/forensics	Manage capture recoveries and cases.
/api/gui_app_framework	Install and manage applications that are created by using the GUI Application Framework Software Development Kit.
/api/help	Returns a list of API capabilities.

Table 114. REST API interfaces (continued)

REST API	Description
/api/qrm	Manage QRM saved search groups, question groups, simulation groups, topology saved search groups, and model groups.
/api/qvm	Retrieves assets, vulnerabilities, networks, open services, networks, and filters. You can also create or update remediation tickets.
/api/reference_data	View and manage reference data collections.
/api/scanner	View, create, or start a remote scan that is related to a scan profile.
/api/services	Perform tasks such as WHOIS lookups, port scan lookups, DNS lookups, and DIG lookups. You can also retrieve geolocation data for an IP or set of IPs.
/api/siem	View, update, and close offenses. You can also add notes and manage offense closing reasons.
/api/staged_config	Retrieve staged configuration for users, hosts, notifications, remote networks, and remote services. You can also initiate or see the state of a deploy action, and update and delete Yara rules.
/api/system	Manage server hosts, network interfaces, and firewall rules.

#### Procedure

1. To access the interactive API documentation interface, enter the following URL in your web browser:  
[https://ConsoleIPAddress/api\\_doc/](https://ConsoleIPAddress/api_doc/).
2. Click the arrow icon beside the API version you want to use.  
9.0 is the latest version for QRadar V7.3.1.
3. Go to the endpoint that you want to access.
4. Read the endpoint documentation and complete the request parameters.
5. Click **Try it out** to send the API request to your console and receive a properly formatted HTTPS response.

**Note:** When you click **Try it out**, the action is performed on the QRadar system. Not all actions can be reversed, for example, you cannot reopen an offense after you close it.

6. Review and gather the information that you need to integrate with QRadar.

## 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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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 actual people or business enterprises is entirely coincidental.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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

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

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



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

## Terms and conditions for product documentation

---

Permissions for the use of these publications are granted subject to the following terms and conditions.

### **Applicability**

These terms and conditions are in addition to any terms of use for the IBM website.

### **Personal use**

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

## Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

## Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## IBM Online Privacy Statement

---

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

## General Data Protection Regulation

---

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: <https://ibm.com/gdpr>

# Glossary

---

This glossary provides terms and definitions for the IBM Security QRadar SIEM software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the [IBM Terminology website](#) (opens in new window).

## A

---

### **accumulator**

A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

### **active system**

In a high-availability (HA) cluster, the system that has all of its services running.

### **Address Resolution Protocol (ARP)**

A protocol that dynamically maps an IP address to a network adapter address in a local area network.

### **administrative share**

A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

### **anomaly**

A deviation from the expected behavior of the network.

### **application signature**

A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

### **ARP**

See [Address Resolution Protocol](#).

### **ARP Redirect**

An ARP method for notifying the host if a problem exists on a network.

### **ASN**

See [autonomous system number](#).

### **asset**

A manageable object that is either deployed or intended to be deployed in an operational environment.

### **autonomous system number (ASN)**

In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

## B

---

### **behavior**

The observable effects of an operation or event, including its results.

### **bonded interface**

See [link aggregation](#).

**burst**

A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

---

**C****CIDR**

See [Classless Inter-Domain Routing](#).

**Classless Inter-Domain Routing (CIDR)**

A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

**client**

A software program or computer that requests services from a server.

**cluster virtual IP address**

An IP address that is shared between the primary or secondary host and the HA cluster.

**coalescing interval**

The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

**Common Vulnerability Scoring System (CVSS)**

A scoring system by which the severity of a vulnerability is measured.

**console**

A display station from which an operator can control and observe the system operation.

**content capture**

A process that captures a configurable amount of payload and then stores the data in a flow log.

**credential**

A set of information that grants a user or process certain access rights.

**credibility**

A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

**CVSS**

See [Common Vulnerability Scoring System](#).

---

**D****database leaf object**

A terminal object or node in a database hierarchy.

**datapoint**

A calculated value of a metric at a point in time.

**Device Support Module (DSM)**

A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

**DHCP**

See [Dynamic Host Configuration Protocol](#).

**DNS**

See [Domain Name System](#).

**Domain Name System (DNS)**

The distributed database system that maps domain names to IP addresses.



**DSM**

See [Device Support Module](#).

**duplicate flow**

Multiple instances of the same data transmission received from different flow sources.

**Dynamic Host Configuration Protocol (DHCP)**

A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

---

**E****encryption**

In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

**endpoint**

The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

**external scanning appliance**

A machine that is connected to the network to gather vulnerability information about assets in the network.

---

**F****false positive**

An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

**flow**

A single transmission of data passing over a link during a conversation.

**flow log**

A collection of flow records.

**flow sources**

The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

**forwarding destination**

One or more vendor systems that receive raw and normalized data from log sources and flow sources.

**FQDN**

See [fully qualified domain name](#).

**FQNN**

See [fully qualified network name](#).

**fully qualified domain name (FQDN)**

In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is `rchland.vnet.ibm.com`.

**fully qualified network name (FQNN)**

In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is `CompanyA.Department.Marketing`.

---

**G****gateway**

A device or program used to connect networks or systems with different network architectures.

## H

---

### **HA**

See [high availability](#).

### **HA cluster**

A high-availability configuration consisting of a primary server and one secondary server.

### **Hash-Based Message Authentication Code (HMAC)**

A cryptographic code that uses a cryptic hash function and a secret key.

### **high availability (HA)**

Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

### **HMAC**

See [Hash-Based Message Authentication Code](#).

### **host context**

A service that monitors components to ensure that each component is operating as expected.

## I

---

### **ICMP**

See [Internet Control Message Protocol](#).

### **identity**

A collection of attributes from a data source that represent a person, organization, place, or item.

### **IDS**

See [intrusion detection system](#).

### **Internet Control Message Protocol (ICMP)**

An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

### **Internet Protocol (IP)**

A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also [Transmission Control Protocol](#).

### **Internet service provider (ISP)**

An organization that provides access to the Internet.

### **intrusion detection system (IDS)**

Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

### **intrusion prevention system (IPS)**

A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

### **IP**

See [Internet Protocol](#).

### **IP multicast**

Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

### **IPS**

See [intrusion prevention system](#).

### **ISP**

See [Internet service provider](#).

## K

---

### **key file**

In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

## L

---

### **L2L**

See [Local To Local](#).

### **L2R**

See [Local To Remote](#).

### **LAN**

See [local area network](#).

### **LDAP**

See [Lightweight Directory Access Protocol](#).

### **leaf**

In a tree, an entry or node that has no children.

### **Lightweight Directory Access Protocol (LDAP)**

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

### **link aggregation**

The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

### **live scan**

A vulnerability scan that generates report data from the scan results based on the session name.

### **local area network (LAN)**

A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

### **Local To Local (L2L)**

Pertaining to the internal traffic from one local network to another local network.

### **Local To Remote (L2R)**

Pertaining to the internal traffic from one local network to another remote network.

### **log source**

Either the security equipment or the network equipment from which an event log originates.

### **log source extension**

An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

## M

---

### **Magistrate**

An internal component that analyzes network traffic and security events against defined custom rules.

### **magnitude**

A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

## N

---

### **NAT**

See [network address translation](#).

### **NetFlow**

A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

### **network address translation (NAT)**

In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

### **network hierarchy**

A type of container that is a hierarchical collection of network objects.

### **network layer**

In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

### **network object**

A component of a network hierarchy.

## O

---

### **offense**

A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

### **offsite source**

A device that is away from the primary site that forwards normalized data to an event collector.

### **offsite target**

A device that is away from the primary site that receives event or data flow from an event collector.

### **Open Source Vulnerability Database (OSVDB)**

Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

### **open systems interconnection (OSI)**

The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

### **OSI**

See [open systems interconnection](#).

### **OSVDB**

See [Open Source Vulnerability Database](#).

## P

---

### **parsing order**

A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

### **payload data**

Application data contained in an IP flow, excluding header and administrative information.

### **primary HA host**

The main computer that is connected to the HA cluster.

**protocol**

A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

---

**Q****QID Map**

A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

---

**R****R2L**

See [Remote To Local](#).

**R2R**

See [Remote To Remote](#).

**recon**

See [reconnaissance](#).

**reconnaissance (recon)**

A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

**reference map**

A data record of direct mapping of a key to a value, for example, a user name to a global ID.

**reference map of maps**

A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

**reference map of sets**

A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

**reference set**

A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

**reference table**

A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

**refresh timer**

An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

**relevance**

A measure of relative impact of an event, category, or offense on the network.

**Remote To Local (R2L)**

The external traffic from a remote network to a local network.

**Remote To Remote (R2R)**

The external traffic from a remote network to another remote network.

**report**

In query management, the formatted data that results from running a query and applying a form to it.

**report interval**

A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

**routing rule**

A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

**rule**

A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

## S

---

**scanner**

An automated security program that searches for software vulnerabilities within web applications.

**secondary HA host**

The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

**severity**

A measure of the relative threat that a source poses on a destination.

**Simple Network Management Protocol (SNMP)**

A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

**SNMP**

See [Simple Network Management Protocol](#).

**SOAP**

A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

**standby system**

A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

**subnet**

See [subnetwork](#).

**subnet mask**

For internet subnetting, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

**subnetwork (subnet)**

A network that is divided into smaller independent subgroups, which still are interconnected.

**sub-search**

A function that allows a search query to be performed within a set of completed search results.

**superflow**

A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

**system view**

A visual representation of both primary and managed hosts that compose a system.

## T

---

**TCP**

See [Transmission Control Protocol](#).

**Transmission Control Protocol (TCP)**

A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-

host protocol in packet-switched communication networks and in interconnected systems of such networks. See also [Internet Protocol](#).

**truststore file**

A key database file that contains the public keys for a trusted entity.

## V

---

**violation**

An act that bypasses or contravenes corporate policy.

**vulnerability**

A security exposure in an operating system, system software, or application software component.

## W

---

**whois server**

A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.





---

# Index

## A

- about [11](#)
- access category
  - description [302](#)
- Admin tab [7](#)
- aggregated data views
  - deleting [123](#)
  - disabling [123](#)
  - enabling [123](#)
  - managing [123](#)
- application category
  - description [328](#)
- Ariel database
  - right-click actions [82](#)
- Asset retention values, overview [84](#)
- audit category
  - description [353](#)
- audit log
  - viewing [279](#)
- audit log file
  - logged actions [281](#)
- audit logs
  - description [279](#)
- authentication
  - Active Directory [25](#)
  - LDAP [25](#), [29](#)
  - overview [23](#)
  - RADIUS [25](#)
  - supported authentication providers [23](#)
  - system [25](#)
  - TACACS [25](#)
- authentication category
  - description [293](#)
- authorized services
  - about [165](#)
  - adding [165](#)
  - revoking [166](#)
  - token [165](#)
  - viewing [165](#)
- automatic update
  - scheduling [77](#)
- autoupdate log [78](#)

## B

- backing up your information [168](#)
- backup and recovery
  - deleting backup archives [173](#)
  - importing backup archives [172](#)
  - initiating backup [170](#)
  - scheduling backups [168](#)
- bonding [49](#)

## C

- changes

- changes (*continued*)
  - deploying [65](#)
- collecting log files [66](#)
- commands
  - description [146](#)
- configuration [63](#), [153](#)
- configuring
  - forwarding profiles [238](#)
  - system authentication [25](#)
- configuring Microsoft Active Directory [28](#)
- content
  - importing [260](#)
- content management tool
  - custom content item, exporting [256](#)
  - custom content items, exporting multiple [258](#)
  - custom content, exporting all of a specific type [253](#)
  - custom content, importing [261](#)
  - existing content, updating [262](#)
  - exporting a single custom content item [256](#)
  - exporting all custom content of a specific type [253](#)
  - exporting multiple custom content items [258](#)
  - importing custom content [261](#)
  - searching for custom content [132](#), [134](#), [136](#), [255](#)
  - update [262](#)
- CRE category
  - custom rule event, *See* CRE
  - description [320](#)
- create [18](#)
- create user information source [157](#)
- creating [11](#), [157](#)
- creating a new store and forward schedule [248](#)
- creating account [21](#)
- custom rules wizard
  - adding SNMP traps [270](#)
  - configuring SNMP traps [267](#)

## D

- data
  - obfuscation
    - decrypting [277](#)
- data node
  - archiving data [49](#)
  - save event processor data [48](#)
- Data Node
  - rebalance progress, viewing [48](#)
- data obfuscation
  - creating a profile [276](#)
  - creating expressions [276](#)
  - overview [273](#)
- deleting [17](#), [159](#)
- deleting a security profile [20](#)
- deleting a store and forward schedule [249](#)
- deleting backup archives [173](#)
- deploying changes [65](#)
- disabling account [22](#), [23](#)
- domains

- domains (*continued*)
  - creating [203](#)
  - default domain [204](#)
  - domain-aware searches [204](#)
  - overlapping IP addresses [201](#)
  - rules and offenses [205](#)
  - segmenting your network [201](#)
  - tagging events and flows [201](#)
  - user-defined domains [204](#)
  - using security profiles [204](#)
- DoS category
  - description [290](#)
- duplicating a security profile [20](#)

## E

- edit [19](#)
- editing [14](#), [159](#)
- editing a store and forward schedule [249](#)
- email, custom notifications [102](#)
- encryption [59](#)
- event categories
  - description [287](#)
- event category correlation
  - access category [302](#)
  - application category [328](#)
  - audit category [353](#)
  - authentication category [293](#)
  - CRE category [320](#)
  - DoS category [290](#)
  - exploit category
    - description [304](#)
  - high-level categories [287](#)
  - malware category [306](#)
  - policy category [317](#)
  - potential exploit category [320](#)
  - recon category [288](#)
  - risk category [357](#)
  - Risk Manager audit category [358](#)
  - SIM Audit events category [326](#)
  - suspicious category [308](#)
  - system category [312](#)
  - unknown category [319](#)
  - User Defined category [323](#)
  - VIS host discovery category [327](#)
- Event Collector
  - about [45](#)
- event forwarding
  - configuring [239](#), [240](#)
- Event Processor
  - about [45](#)
- event retention
  - configuring [98](#)
  - deleting [100](#)
  - enabling and disabling [100](#)
  - managing [99](#)
  - sequencing [99](#)
- event view
  - building [45](#)
- events
  - domain creation [203](#)
  - domain tagging [201](#)
  - storing and forwarding [245](#)
  - storing and forwarding events [245](#)

- exploit category [304](#)
- exporting [44](#)
- extensions
  - importing [260](#)
- external flow sources [183](#)

## F

- flow configuration [186](#)
- flow retention
  - configuring [98](#)
  - deleting [100](#)
  - enabling and disabling [100](#)
  - managing [99](#)
  - sequencing [99](#)
- flow source
  - about [183](#)
  - adding aliases [190](#)
  - adding flow source [186](#)
  - deleting aliases [190](#)
  - deleting flow source [189](#)
  - domain tagging [201](#)
  - editing aliases [190](#)
  - enabling or disabling [189](#)
  - external [183](#)
  - internal [183](#)
  - managing aliases [189](#)
  - virtual name [189](#)
- flow sources
  - domain creation [203](#)
- flowlog file [186](#)
- forwarding destinations
  - in domain-aware environments [201](#)
  - managing [242](#)
  - specifying properties [238](#)
  - viewing [242](#)
- forwarding normalized events and flows [57](#)
- forwarding profiles
  - configuring [238](#)

## G

- glossary [387](#)

## H

- hidden updates [78](#)
- hiding data, *See* data obfuscation
- high-level categories
  - description [287](#)
- host
  - adding [60](#)

## I

- importing backup archives [172](#)
- importing content [260](#)
- initiating a backup [170](#)
- internal flow sources [183](#)
- introduction [xi](#)
- IPv6
  - support and limitations [93](#)

## J

J-Flow [186](#)

## L

LDAP

authentication [29](#)

displaying user information [34](#)

license

license status [42](#)

license details

viewing [43](#)

license key [41](#), [44](#)

logged actions

audit log file [281](#)

## M

malware category

description [306](#)

managed host

adding [60](#)

editing [62](#)

removing [62](#)

managed hosts

IPv6 support [93](#)

management task overview [155](#)

managing [11](#), [21](#), [157](#)

masking data, *See* data obfuscation

## N

NAT

enabling [62](#)

using with QRadar [52](#)

NetFlow [184](#)

network

domains [201](#)

Network Address Translation. [52](#)

network administrator [xi](#)

network hierarchy

creating [69](#)

network resources

suggested guidelines [193](#)

new features

Version 7.3.0 [5](#)

Version 7.3.1 [1](#)

## O

obfuscation

data

decrypting [277](#)

off-site source [57](#)

off-site target [57](#)

offense close reason [105](#)

offenses

domain-aware [205](#)

overlapping IP addresses

domain segmentation [201](#)

overview [153](#)

## P

Packeteer [186](#)

parameters

description [146](#)

password [66](#)

passwords

complexity [25](#)

expiry [25](#)

payload indexing

enabling [108](#)

payload searches

enabling indexes [108](#)

policy category

description [317](#)

potential exploit category

description [320](#)

public key

generating [56](#)

## Q

QID map entry, modifying [196](#)

QID map overview [194](#)

Qid map, importing entries [196](#)

QRadar identifier map overview [194](#)

## R

recon category

description [288](#)

reference data collection [154](#)

reference data collections [139](#)

reference sets

adding [141](#)

adding elements [143](#)

deleting elements [144](#)

exporting elements [144](#)

viewing [141](#)

viewing contents [142](#)

remote network groups

description [191](#)

remote networks and services

description [191](#)

remote networks object

adding [193](#)

remote service groups

description [192](#)

remote services object

adding [194](#)

remote services objects

configuring [194](#)

resetting SIM [67](#)

restarting [65](#)

restarting system [65](#)

restored data

verifying [178](#)

restoring

troubleshooting restored data [178](#)

restoring configuration information

different IP address [175](#)

same IP address [174](#)

retention buckets [97](#)

- retrieving [159](#)
- right-click menus
  - adding right-click actions [82](#)
- risk category
  - description [357](#)
- Risk Manager audit category
  - description [358](#)
- roles [11](#), [14](#), [17](#)
- routing options
  - configuring [242](#)
- routing rules
  - editing [242](#)
- rules
  - domain-aware [205](#)

## S

- scheduling your backup [168](#)
- searching
  - in domain-aware environments [204](#)
- security profile [18–20](#)
- security profiles
  - domain privileges [204](#)
- servers
  - discovering [199](#)
- services
  - authorized [165](#)
- sFlow [185](#)
- shutting down [65](#)
- shutting down system [65](#)
- SIM
  - resetting [67](#)
- SIM Audit category [326](#)
- SNMP traps
  - adding [270](#)
  - configuration overview [267](#)
  - configuring in customer rules wizard [267](#)
  - configuring trap output [268](#)
  - sending to different host [270](#)
- source
  - off-site [57](#)
- SSL certificate
  - configuring [33](#)
- store and forward
  - creating a new schedule [248](#)
  - deleting a schedule [249](#)
  - editing a schedule [249](#)
  - viewing the schedule list [245](#)
- store user information [160](#)
- suspicious category
  - description [308](#)
- syslog
  - forwarding [237](#)
- system [65](#)
- system and license management
  - log file collection [66](#)
- system authentication
  - configuring [25](#)
- system category
  - description [312](#)
- system health [45](#)
- system information [49](#), [63](#)
- system management [45](#)
- system settings [81](#)

- system time [51](#)
- system view
  - adding a host [60](#)

## T

- target
  - encryption [57](#)
  - off-site [57](#)
- thresholds [101](#)
- time server configuration [51](#)
- Tivoli Directory Integrator server [153](#), [155](#)
- TLS certificate
  - configuring [33](#)
- troubleshooting
  - restored data [178](#)

## U

- unknown category
  - description [319](#)
- update history [78](#)
- updates
  - scheduling [77](#)
- upload [41](#)
- user accounts [21](#)
- User Defined category
  - description [323](#)
- user information [154](#), [160](#)
- user information source [155](#), [157](#)
- user information sources [153](#), [157](#), [159](#)
- user interface [7](#)
- user management
  - authentication [23](#)
- user roles [11](#)
- users [11](#), [21–23](#)

## V

- variable binding
  - SNMP traps [268](#)
- viewing the schedule list [245](#)
- VIS host discovery category
  - description [327](#)

## W

- what's new [1](#), [5](#)



