

IBM QRadar  
7.4.3

*What's New Guide*



**Note**

Before you use this information and the product that it supports, read the information in [“Notices” on page 27](#).

---

# Contents

- Introduction to what's new in the QRadar family of products .....v**
  
- Chapter 1. What's new in QRadar 7.4.3..... 1**
  - QRadar..... 1
    - Operational efficiency..... 1
    - Flow improvements..... 2
    - What's changed or removed.....4
  - QRadar Network Insights.....5
  - QRadar Incident Forensics..... 6
  
- Chapter 2. What's new in QRadar 7.4.2..... 9**
  - QRadar.....9
    - Operational efficiency..... 9
    - DSM Editor enhancements.....10
    - Flow improvements.....10
    - What's changed or removed..... 11
  - QRadar Network Insights..... 12
  
- Chapter 3. What's new in QRadar 7.4.1..... 15**
  - QRadar.....15
    - DSM Editor enhancements.....15
    - Security enhancements..... 15
    - Workflow enhancements in QRadar..... 16
    - Flow improvements.....16
  - QRadar Network Insights..... 17
  
- Chapter 4. What's new in QRadar 7.4.0..... 19**
  - QRadar.....19
    - Performance optimization.....19
    - Security enhancements..... 21
    - Workflow enhancements..... 21
    - Flow improvements.....22
    - What's changed or removed..... 22
  - QRadar Network Insights..... 22
  - QRadar Incident Forensics..... 24
  - QRadar application framework.....25
  - QRadar Vulnerability Manager and QRadar Risk Manager..... 26
  
- Notices.....27**
  - Trademarks..... 28
  - Terms and conditions for product documentation..... 28
  - IBM Online Privacy Statement..... 29
  - General Data Protection Regulation.....29



# Introduction to what's new in the QRadar family of products

---

Administrators review new features for IBM® QRadar® to help determine whether to upgrade, plan training for the users that they support, and to become aware of new capabilities.

## Intended audience

This guide is intended for existing QRadar users who are responsible for investigating and managing network security.

## Technical documentation

To find IBM 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](http://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 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 QRadar.



# Chapter 1. What's new in QRadar 7.4.3

The IBM QRadar 7.4.3 family of products includes enhancements to operational efficiency and flow improvements.

## QRadar

IBM QRadar 7.4.3 includes a new forwarding destination protocol, flow improvements, and enhancements to operational efficiency.

### Operational efficiency

The operational efficiency improvements in QRadar 7.4.3 include adjusting the Asset Cleanup Batch Size Threshold.


#### Asset Cleanup Batch Size Threshold

In QRadar 7.4.3, you can adjust the number of assets at which a batch of assets is cleaned. You can configure this value if the number of assets might exceed the maximum time that is allowed by the DB connection pool. Generally, if the asset cleanup agent does not have connection pool problems, you do not need to change this configuration value.

Enter the number in the **Asset Cleanup Batch Size Threshold** field in the **Asset Profiler Configuration** window.

Figure 1. Asset Profiler Configuration window

Asset Profiler Configuration	
<b>Asset Profile Settings</b>	
Asset Profile Retention Period	Use Advanced
Enable DNS Lookups for Host Identity	True
Enable WINS Lookups for Host Identity	True
Enable Real-Time DNS Lookups for Asset Profiles	True
<b>Asset Profiler Configuration</b>	
Asset Profiler Audit Events Per Minute Threshold	6,000
Number of Grey List Ports Per Asset	100
Enable Identity Profiling	True
Enable Client Application Profiling	True
Enable Open Port Profiling	True
Number of IPs Allowed for a Single Asset	96
Number of MAC Addresses Allowed for a Single Asset	10
Unified Asset Name	NetBIOS Name
Enable IP Reconciliation Blacklisting	True
Asset Identity Coalescing	15 minutes <input type="checkbox"/> Coalesce Ownership Changes
<b>Asset Profiler Retention Configuration</b>	
<b>Asset Cleanup Batch Size Threshold</b>	1,000
Clean Entire Asset	False
Retain Assets with Vulnerabilities	False

 To learn more about tuning the Asset Profiler retention settings, see the *IBM QRadar Administration Guide*.

## Flow improvements

IBM QRadar 7.4.3 introduces support for ICMPv6 applications, new flow fields, and APIs for managing flows.

### Support for ICMPv6 messages

QRadar now shows more information about ICMPv6 traffic from NetFlow v9 and IPFIX records.

In earlier versions, the ICMPv6 data was collected, but the application was shown as **Other**. Now, on the **Network Activity** tab, the **Application** field shows the application for the ICMPv6 traffic. The application is set only when the ICMPv6 type and code are populated in icmpTypeCodeIPv4 (IANA Element ID 32).


If the flow record uses an ICMPv6 type and code that is unassigned by IANA, the application appears as **Other**.

### New "Flow Source Types" field

QRadar 7.4.3 includes a new **Flow Source Types** field.

The new field shows you the types of flow sources that are exported or received on the network. For example, the field might show that a flow record was sourced from IPFIX or NetFlow v9, or one of the many other supported flow types. The new field appears on the **Flow Information** window, under the **Flow Analysis Metadata** category.

You can also include the new field as a column on the **Network Activity** tab. In this view, the field shows only the numeric value for the flow source type. If there are multiple flow source types, the field shows **Multiple (x)**. You can use the Ariel lookup AQL function to see the flow type.

 To learn more about viewing flow data, see the *IBM QRadar User Guide*.

### Support for more fields from AWS

QRadar can now receive more information from Amazon Web Services (AWS) flow logs.

QRadar 7.4.3 introduces support for the following fields:

- Region

The **Region** field is supported for AWS Flow Logs and AWS Network Firewall Logs.

- Firewall Name

The **Firewall Name** field is supported for AWS Network Firewall Logs.

When an IPFIX flow record includes these fields, QRadar shows the information on the **Flow Details** page under the **Cloud** category.


 To learn more about viewing AWS flow data, see the *IBM QRadar User Guide*.

### New API for managing flow applications

QRadar 7.4.3 introduces a new API for managing flow applications.

In earlier versions of QRadar, you had to manually update the application configuration (`apps.conf`) file. Now, you can use the API to manage the flow applications that are defined in your system.

When you change the flow application configuration, edit the configuration in the staging area. After you update the application configuration in the staged configuration area, you can deploy the changes to propagate the updates to the system.

 To learn more about defining new applications, see the *IBM QRadar Application Configuration Guide*.




## New API for managing common destination ports

QRadar 7.4.3 introduces a new API for specifying which ports are considered common destination ports. In earlier versions of QRadar, you had to manually update the `appid_map.conf` configuration file to edit the list of common destination ports.

Access the API at `/api/config/flow/common_destination_ports`.

When you use the API to change the common destination ports, the QFlow process automatically loads the configuration. You do not need to deploy the configuration to propagate the changes to the system.

 To learn more about flow direction and common destination ports, see the *IBM QRadar User Guide*.

## Support for categorizing flow information fields

QRadar 7.4.3 includes support for categorizing flow information fields.

The new categorization of tagged fields groups like information together and improves readability of the **Flow Information** window. All existing tagged fields are categorized by default.

Flow Data	
Accumulated Source Bytes	454
Accumulated Source Packets	5
Accumulated Destination Bytes	0
Accumulated Destination Packets	0

Encapsulation	
VLAN ID	0
Enterprise VLAN ID	0
Customer VLAN ID	0
VLAN ID (reverse)	0


  

Flow Analysis Metadata	
Flow Direction Algorithm	Arrival time (3)

Figure 2. Field categories on the **Flow Information** window

To change the way that the fields are grouped and sorted on the **Flow information** window, use the Ariel Tagged Fields API. You can use these endpoints to view and manage the tagged field categories:


- `/api/ariel/taggedfields`
- `/api/ariel/taggedfieldcategories`

 [Learn more about using the QRadar RESTful API ...](#)

## Web.SecureWeb application is renamed

In IBM QRadar 7.4.3, the `Web.SecureWeb` application is renamed to `SSL/TLS`. The new name more accurately reflects that SSL/TLS encryption is used in a wide variety of applications, and not just HTTPS traffic.

Rules and searches that use the `Web.SecureWeb` application name must be updated to use the new name.

 To learn more about the applications that are recognized by QRadar, see the *IBM QRadar Application Configuration Guide*.


## What's changed or removed

In IBM QRadar 7.4.3, some features were changed or removed.

### Encrypted log files

You can now set your own password for encrypted log files. When you send encrypted log files to IBM Customer Support, you must also provide the password so that the log files can be decrypted.

In previous releases, you weren't able to specify a password and encrypted log files were decrypted only by IBM Customer Support.

 To learn more about collecting log files, see the *IBM QRadar Administration Guide*.

### Authorized service tokens no longer visible after creation

When you create an authorized service token, the token is displayed in the **Authorized Service Created Successfully** dialog. As of QRadar 7.4.3, the authorized service token cannot be made visible again after you close the **Authorized Service Created Successfully** dialog. Copy the token to a secure location before you close the dialog.

### Authorized services with invalid configurations


When you upgrade to QRadar 7.4.3 or later, any authorized services with the "System Administrator" permission are expired, unless they are assigned to the "Admin" security profile.

To re-enable an expired authorized service after an upgrade, you must update the user role and security profile of the authorized service to a valid combination and reset the expiration date.

1. On the **Admin** tab, click **Authorized Services**.
2. Select the authorized service to re-enable.
3. Click **Edit Authorized Service Name**
4. Assign a valid user role and security profile combination.
5. Set the authorized service expiration date to a time in the future, or remove the expiration date if you don't want the authorized service to expire.

### Normalization of custom properties

During the upgrade to 7.4.3, and when you install content after the upgrade, alias properties are created for custom properties that don't conform to naming best practices. Those custom properties are linked to these alias properties. Any rules, searches, indexes, accumulated data, routing rules and domains that used the old custom property names are updated to use the aliases instead. The old custom property names remain on the system so they can still be used with existing apps, scripts, and other tools.

 [Learn more about the renamed and merged default custom properties ...](#)

### SAML certificate file names

When you select the QRadar\_SAML certificate under **Certificate for signing and encryption**, the file names of the QRadar root CA and root CA CRL files are changed.

- **vault-qrd\_ca.pem** is changed to **root-qradar-ca\_ca**
- **vault-qrd\_ca.crl** is changed to **root-qradar-ca\_ca.crl**

**Important:** You must reconfigure SAML after you update to QRadar 7.4.3.


 To learn more about SAML single sign-on authentication, see the *IBM QRadar Administration Guide*.

## New forwarding destination protocol

IBM QRadar 7.4.3 includes a new **TCP over TLS 1.1 and above** forwarding destination protocol that ensures a more secure connection to the forwarding host.

Using the new protocol, you can validate that the destination host matches the *Common Name* or *Subject Alternate Name* of the certificate that is presented by the destination server.

When you configure the forwarding destination, you can enable client authentication and use the QRadar Certificate Management App to upload the client certificate that you want to use for authentication.

 To learn more about configuring QRadar to forward data to other systems..., see the *IBM QRadar Administration Guide*.

## QRadar Network Insights


---

IBM QRadar Network Insights 7.4.3 is now easier to install. It includes new inspectors for Kerberos and TFTP network traffic, and also announces deprecation for some inspectors in a future release.

### Simplified installation process

Now you can install QRadar Network Insights directly from the QRadar installation media. With this simplified installation process, you do not have to download a separate installation file for QRadar Network Insights.

This change affects new installations only. The process to upgrade your deployment does not change.

 To learn more about installing and upgrading QRadar Network Insights, see the *QRadar Network Insights Installation and Configuration Guide*.

### New inspector for Kerberos

QRadar 7.4.3 includes a new Kerberos inspector that you can use to parse Kerberos traffic that is sent to trusted third-party authentication providers. The new inspector makes it easier to identify the user or device that requested the access, and the service for which access was requested.

When the flow application is Kerberos, you can use the following new flow fields to identify more information about the network traffic:

#### **Kerberos Realm**

Shows the Active Directory domain.

#### **Kerberos Client Principal Name**

Shows the user or device that requested the access.

#### **Kerberos Server Principal Name**

Shows the service for which access was requested.

#### **Kerberos Presented Ticket Hash**

Shows the hash of the ticket that was provided when access to the resource was requested.

#### **Kerberos Issued Ticket Hash**

Shows the hash of the ticket that was issued to allow access to the resource.

#### **Kerberos Cipher Suite**

Shows the set of ciphers that were used to encrypt the ticket.

The existing HTTP and SMB inspectors were also updated to parse the data when Kerberos is used for authentication.

 To learn more about the supported protocol inspectors, see the *QRadar Network Insights User Guide*.

## New inspector for TFTP

QRadar 7.4.3 introduces a new inspector for Trivial File Transfer Protocol (TFTP) network traffic. The TFTP inspector introduces the following new flow fields to show information about the file transfer:

### TFTP Status

Shows whether the TFTP client issued a read or write command.

### TFTP Mode

Shows if the file was transferred in ASCII or binary mode.

### TFTP Requested Options

Shows the options that were negotiated prior to the file transfer, including the block size, time out interval, and the file transfer size.


You can use the new flow fields in combination with the source and destination ports to help you trace a data flow back to the original transfer request.

 To learn more about the supported protocol inspectors, see the *QRadar Network Insights User Guide*.

## Deprecation notice for some inspectors

IBM QRadar Network Insights 7.4.3 announces deprecation for all domain inspectors, and for the Myspace and SPDY protocol inspectors.

You can still use the deprecated inspectors in QRadar Network Insights 7.4.3, but they will be removed in a future release.

 To learn more about the types of inspectors that are supported, see the *QRadar Network Insights User Guide*.

## QRadar Incident Forensics

---

IBM QRadar Incident Forensics 7.4.3 introduces new Kerberos and BitTorrent inspectors.

### New Kerberos inspector

QRadar Incident Forensics 7.4.3 includes a new Kerberos inspector that you can use to parse Kerberos traffic that is sent to trusted third-party authentication providers. The new inspector makes it easier to identify the user or device that requested the access, and the service for which access was requested.

When the flow application is Kerberos, you can use the following new flow fields to identify more information about the network traffic:

#### Kerberos Realm

Shows the Active Directory domain.

#### Kerberos Client Principal Name

Shows the user or device that requested the access.

#### Kerberos Server Principal Name

Shows the service for which access was requested.

#### Kerberos Presented Ticket Hash

Shows the hash of the ticket that was provided when access to the resource was requested.

#### Kerberos Issued Ticket Hash


Shows the hash of the ticket that was issued to allow access to the resource.

#### Kerberos Cipher Suite

Shows the set of ciphers that were used to encrypt the ticket.

The existing HTTP and SMB inspectors were also updated to parse the data when Kerberos is used for authentication.

In QRadar Incident Forensics, the protocol metadata also includes an additional field, **Kerberos Ticket SHA1 Hash**, that includes both the presented and the issued ticket hash together. You can use this field to find all of the Kerberos traffic that is involved in a single session.

 To learn more about the supported protocols and document types, see the *IBM QRadar Incident Forensics Administration Guide*.

## **New TFTP inspector**

QRadar Incident Forensics 7.4.3 introduces a new inspector for Trivial File Transfer Protocol (TFTP) network traffic. The TFTP inspector introduces the following new flow fields to show information about the file transfer:

### **TFTP Status**

Shows whether the TFTP client issued a read or write command.


### **TFTP Mode**

Shows if the file was transferred in ASCII or binary mode.

### **TFTP Requested Options**

Shows the options that were negotiated prior to the file transfer, including the block size, time out interval, and the file transfer size.

In QRadar Incident Forensics, the protocol metadata also includes additional information about the client and server ports, and error code information.

 To learn more about the supported protocols and document types, see the *IBM QRadar Incident Forensics Administration Guide*.



## Chapter 2. What's new in QRadar 7.4.2

The IBM QRadar 7.4.2 family of products includes enhancements to operational efficiencies, DSM Editor workflow, and flow improvements.

### QRadar

IBM QRadar 7.4.2 includes enhancements to operational efficiency, DSM Editor enhancements, and flow improvements.

#### Operational efficiency

The operational efficiency improvements in QRadar 7.4.2 include adjusting the number of MAC addresses allowed for an asset.

##### Adjusting the number of MAC addresses allowed for an asset


In QRadar 7.4.2, you can adjust the number of MAC addresses that are allowed for a single asset. In previous versions of QRadar, administrators were not able to adjust this number, which resulted in an error message that stated that there were too many MAC addresses for the asset. Enter the number in the **Number of MAC Addresses Allowed for a Single Asset** field in the **Asset Profiler Configuration** window.

If you have users who log in from multiple wireless access points, or multiple users who log in remotely through a VPN, you can set the number of MAC addresses that are allowed for the asset in the same way that you can for IP addresses.

Figure 3. Asset Profiler Configuration window

Asset Profiler Configuration	
Asset Profile Settings	
Asset Profile Retention Period	Use Advanced
Enable DNS Lookups for Host Identity	True
Enable WINS Lookups for Host Identity	True
Enable Real-Time DNS Lookups for Asset Profiles	True
Asset Profiler Configuration	
Asset Profiler Audit Events Per Minute Threshold	6,000
Number of Grey List Ports Per Asset	100
Enable Identity Profiling	True
Enable Client Application Profiling	True
Enable Open Port Profiling	True
Number of IPs Allowed for a Single Asset	75
<b>Number of MAC Addresses Allowed for a Single Asset</b>	10
Unified Asset Name	NetBIOS Name
Enable IP Reconciliation Blacklisting	True
Asset Identity Coalescing	15 minutes
<input type="checkbox"/> Coalesce Ownership Changes	
Asset Profiler Retention Configuration	
Clean Entire Asset	False
Retain Assets with Vulnerabilities	False

Ensure that the **Asset Profile Retention Period** is set to **Use Advanced**, otherwise any of the the following retention periods that you select will not be applied.

 To learn more about adjusting the number of MAC addresses allowed for an asset, see the *IBM QRadar Administration Guide*.

## DSM Editor enhancements

The DSM Editor enhancements in QRadar 7.4.2 include generating regex to parse event properties.

### Generating regex for parsing event properties

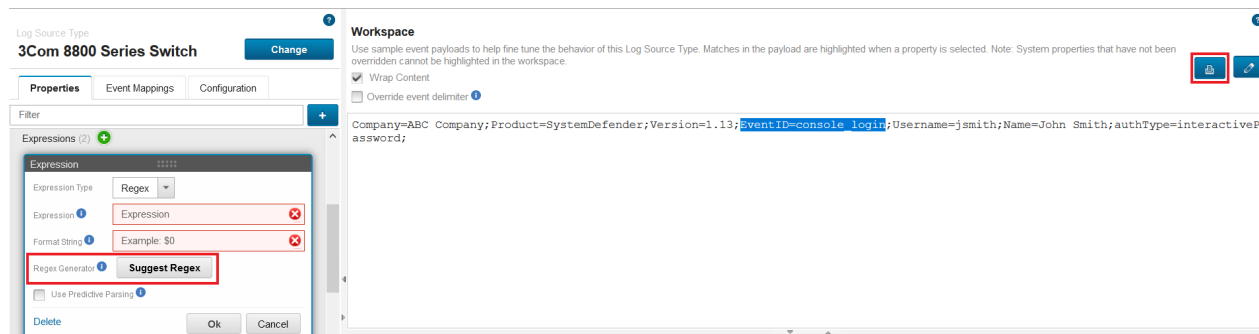
QRadar 7.4.2 can suggest regular expressions (regex) when you enter event data in the **Workspace**. If you are not familiar with creating regex expressions, use this feature to generate your regex.

Highlight the payload text that you want to capture and in the **Properties** tab, click **Suggest Regex**. The suggested expression appears in the **Expression** field. Alternatively, you can click the **Regex** button in the **Workspace** and select the property that you want to write an expression for. If QRadar is unable to generate a suitable regex for your data sample, a system message appears.

**Tip:** The regex generator works best for fields in well-structured event payloads. If your payload consists of complex data from natural language or unstructured events, the regex generator might not be able to parse it and does not return a result.

The following figure shows how you can generate your regex with the **Suggest Regex** button in the **Properties** tab, or with the **Regex** button in the **Workspace**.

Figure 4. Suggest Regex button



 To learn more about the DSM Editor workspace, see the *IBM QRadar Administration Guide*.

## Flow improvements

QRadar 7.4.2 introduces new flow algorithms, new accumulated byte and packet counters, and support for MAC address fields.


### Accumulated byte and packet counters

Flows are reported in 1-minute intervals, and can span several minutes, hours, or even days. For sessions that span more than a minute, IBM QRadar reports on the current metrics for the flow at the end of each 1-minute interval. The byte and packet counters show the number of bytes and packets that were received in that 1-minute interval.

In QRadar 7.4.2, you can now see the total number of bytes and packets that accumulated over the duration of the flow session. The byte and packet counters for each 1-minute interval that the flow is observed are also preserved.

You can view the accumulated counters by including the following fields in your search results.

- Accumulated source bytes
- Accumulated source packets
- Accumulated destination bytes
- Accumulated destination packets

 To learn more about creating custom searches, see the *IBM QRadar User Guide*.



## New "Common Destination Port" flow direction algorithms


IBM QRadar provides information about which algorithm was used to determine the flow direction.

QRadar 7.4.2 introduces two new common destination port algorithms for use when the flow matches the criteria, but the flow direction is unchanged:

- Single common destination port (unaltered) (5)
- Both common destination ports, RFC 1700 preferred (unaltered) (6)

In previous versions of IBM QRadar, the common destination port algorithms were reported only when the flow direction was reversed. Most other flows used the **Arrival time** algorithm, including the flows that matched the common destination port criteria but did not have the flow direction reversed.

Now, the only flows that show the **Arrival time** annotation in the **Flow Direction Algorithm** field are the flows that do not match the criteria for any other flow direction algorithm.

 To learn more about flow direction, see the *IBM QRadar User Guide*.


## MAC address support

IBM QRadar can now receive MAC address information from IPFIX and NetFlow V9 exporters.

The following MAC address fields are supported in QRadar 7.4.2:

- sourceMacAddress (IANA Element ID 56)
- postDestinationMacAddress (IANA Element ID 57)
- destinationMacAddress (IANA Element ID 80)
- postSourceMacAddress (IANA Element ID 81)

You can use the new MAC address fields in filters, searches, and rules.

 To learn more about creating filters, searches, and rules, see the *IBM QRadar User Guide*.

## What's changed or removed

In IBM QRadar 7.4.2, some features were changed or removed.


### Active Directory

User authentication with Active Directory (AD) is no longer supported as of QRadar 7.4.2. Use Lightweight Directory Access Protocol (LDAP) for user authentication to an AD server instead.

 [Learn more about why Active Directory was removed...](#)

### GlusterFS no longer supported

GlusterFS is no longer supported in QRadar. You must migrate any Event Collectors in your deployment to Distributed Replicated Block Device before you upgrade to QRadar 7.4.2. You must be running QRadar 7.3.2 fix patch 3 or later before you can upgrade to QRadar 7.4.2.

 To learn more about Upgrading to 7.4.2, see the *IBM QRadar 7.4.2 Upgrade Guide*.

## QRadar Network Insights


---

IBM QRadar Network Insights 7.4.2 introduces stacking support for the new QRadar Network Insights 1940 appliance, as well as improvements to flow direction, content flows, and entity alerts.

### QRadar Network Insights 1940 appliance stacking

You can stack the new QRadar Network Insights 1940 appliances (appliance type 6600) to scale performance by balancing the network packet data load across multiple appliances. By distributing the data processing and analysis, stacked appliances can help you handle higher data volumes and improve flow throughput performance at the highest inspection levels.

In a stacked configuration, the QRadar Network Insights 1940 appliances provide one port for incoming traffic and one port for outgoing traffic. Each appliance stack must include the same type of appliance. For example, you can't have one appliance stack that includes both QRadar Network Insights 1920 and 1940 appliances.

 To learn more about stacking appliances, see the *IBM QRadar Network Insights Installation and Configuration Guide*.


### Content flows are more easily identified

In earlier versions of IBM QRadar, content flows that were received from IBM QRadar Network Insights were identified as a **Standard flow** with 0 bytes and 0 packet counters.

QRadar 7.4.2 makes it easier to identify content flows that are received from QRadar Network Insights:

- In the **Flow Information** window, the **Flow Type** field shows **Standard Flow (Content Flow)**.
- On the **Network Activity** tab, the tooltip for the **Flow Type** icon shows **Standard Flow (Content Flow)**.

The new **Standard Flow (Content Flow)** annotation is for display purposes only. You can't use this information in queries and filters.

 To learn more about content flows, see the *IBM QRadar Network Insights User Guide*.

### New TCP flow direction algorithms

IBM QRadar Network Insights now includes two new flow direction algorithms that are used when a TCP handshake is observed.

The new algorithms appear in the **Flow Direction Algorithm** field in the **Flow Information** window, and provide a clear indication of whether the flow direction was flipped.

- **QNI TCP Handshake Observed (reversed) (7)**
- **QNI TCP Handshake Observed (unaltered) (8)**

Previously, the flow direction was determined exclusively by the QFlow process based on common destination ports or other flow information, resulting in the flow's direction to be incorrectly flipped.

Now, when QRadar Network Insights observes a TCP handshake, the QFlow process relies on the information from QRadar Network Insights to determine the flow direction. All other flows rely on the algorithms that are used by the QFlow process.

 To learn more about flow direction, see the *IBM QRadar User Guide*.


### Easily determine the direction of a content flow

When you drill down on a content flow, the **Flow Information** window now includes a **Content Flow Direction** field. The direction of the content flow is indicated by one of the following annotations:

- **Unknown (0)**
- **Default Direction (1)**

- **Source to Destination (2)**
- **Destination to Source (3)**

You can use this information to help you interpret the attributes within the content flow. For example, the direction of the content flow can help you determine whether files were exfiltrated or brought into the organization.

 To learn more about flow direction, see the *IBM QRadar User Guide*.

### **More descriptive entity alerts**


An entity alert indicates that IBM QRadar Network Insights found suspicious content, such as credit card numbers, social security numbers, IP addresses, and email addresses, in a network flow.

Previously, the entity alert didn't provide visibility into the type of suspect content that caused the alert. Now, the entity alert includes more information about the type of suspicious content that was found so that you can triage each type of entity alert separately.

The following entity alerts are new in QRadar Network Insights 7.4.2:

- entity alert - IP address
- entity alert - MAC address
- entity alert - Phone number
- entity alert - Credit Card Number
- entity alert - Email Address
- entity alert - Social Security Number
- entity alert - UK NINO
- entity alert - UK postal code
- entity alert - Zip Code

You can view the entity alerts in the **Suspect Content Descriptions** field on the **Flow Information** window.

 To learn more about IBM QRadar Network Insights flow data, see the *IBM QRadar Network Insights User Guide*.



## Chapter 3. What's new in QRadar 7.4.1

The IBM QRadar 7.4.1 family of products includes enhancements to performance, workflow, security, and user experience.

### QRadar

IBM QRadar 7.4.1 includes enhancements to performance, security, workflow enhancements, and flow improvements.

### DSM Editor enhancements

The DSM Editor enhancements in QRadar 7.4.2 include generating regex to parse event properties.

#### Generating regex for parsing event properties

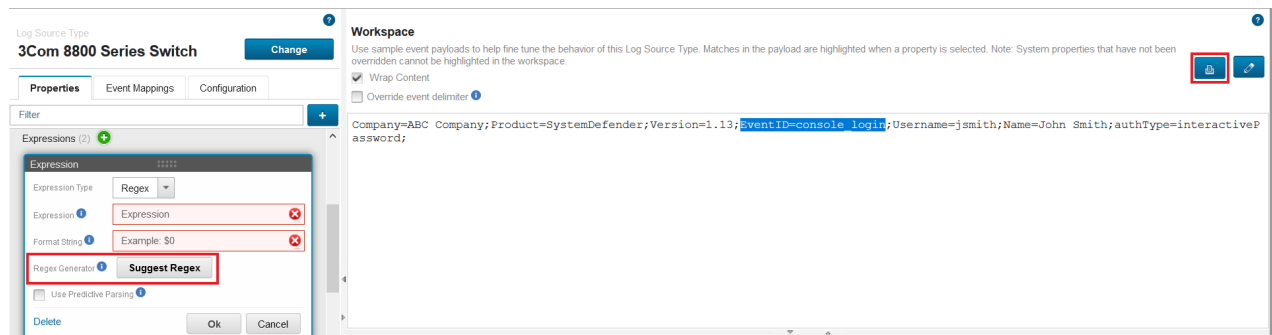
QRadar 7.4.2 can suggest regular expressions (regex) when you enter event data in the **Workspace**. If you are not familiar with creating regex expressions, use this feature to generate your regex.

Highlight the payload text that you want to capture and in the **Properties** tab, click **Suggest Regex**. The suggested expression appears in the **Expression** field. Alternatively, you can click the **Regex** button in the **Workspace** and select the property that you want to write an expression for. If QRadar is unable to generate a suitable regex for your data sample, a system message appears.

**Tip:** The regex generator works best for fields in well-structured event payloads. If your payload consists of complex data from natural language or unstructured events, the regex generator might not be able to parse it and does not return a result.

The following figure shows how you can generate your regex with the **Suggest Regex** button in the **Properties** tab, or with the **Regex** button in the **Workspace**.

Figure 5. Suggest Regex button



 To learn more about the DSM Editor workspace, see the *IBM QRadar Administration Guide*.

### Security enhancements

Stronger security capabilities in IBM QRadar 7.4.1 include a more secure operating system.

#### More secure operating system

QRadar 7.4.1 runs on Red Hat® Enterprise Linux® version 7.7. The update to RHEL V7.7 is necessary to continue receiving security updates from Red Hat Enterprise Linux.

## Workflow enhancements in QRadar

Improvements to workflow in IBM QRadar for 7.4.1 include the QRadar Use Case Manager and an analyst workflow for investigating offenses.

### IBM QRadar Use Case Manager app installed by default

In QRadar 7.4.1, the QRadar Use Case Manager app is installed by default. Use the guided tips in QRadar Use Case Manager to help you ensure that QRadar is optimally configured to accurately detect threats throughout the attack chain. QRadar Use Case Manager includes a rule explorer that offers flexible reports that are related to your rules. QRadar Use Case Manager also exposes pre-defined mappings to system rules and to help you map your own custom rules to MITRE ATT&CK tactics and techniques.

**Important:** User roles with the system administrator permission are updated automatically to include the required permissions for the apps installed by default. All other user roles must be modified to include the app permissions as needed.

### QRadar Analyst Workflow to help you investigate offenses

IBM Security QRadar Analyst Workflow provides new methods for filtering offenses and events, and graphical representations of offenses, by magnitude, assignee, and type. The improved offenses workflow provides a more intuitive method to investigate offenses to determine the root cause of an issue and work to resolve it. Use the built-in query builder to create AQL queries by using examples and saved or shared searches, or by typing plain text into the search field.

The workflow includes a redesigned offenses page, an AQL search page, and access to compatible apps that are already installed on your QRadar Console. QRadar Analyst Workflow is supported on QRadar 7.4.0 or later.

For more information about the QRadar Analyst Workflow, see the *IBM QRadar User Guide*.

## Flow improvements

QRadar 7.4.1 introduces support for 40 Gbps Napatech cards and support for the `flowId` field in NetFlow V9 data exports.

### Support for the flow ID field in NetFlow V9 flow records

IBM QRadar now supports the `flowId` field (IANA element 148) in NetFlow Version 9 data exports. In QRadar, the field appears in the **Vendor Flow ID** field on the **Flow Details** window.

The flow ID is used as part of the flow's unique identifier so that only flow records with the same flow ID value are aggregated together. Sessions with different flow IDs are kept separate and mapped to different Flow ID values.

You can use the `flowId` field in filters and searches to quickly identify all of the flow records in a particular session.

### Support for 40 Gbps Napatech card

The QFlow component of IBM QRadar now supports the new Napatech NT200A02 (2 x 40 Gbps) SmartNIC. Network connectivity is not indicative of the data throughput levels that each appliance is capable of.

Napatech has deprecated support for the NT20E SmartNIC.

## QRadar Network Insights

---

IBM QRadar Network Insights 7.4.1 introduces support for 40 Gbps network connectivity. This release also announces deprecation of IP reputation suspect content warnings, and the removal of the DNS Query and DNS Response fields.

### Support for 40 Gbps connectivity

The IBM QRadar portfolio expands its threat detection capabilities with the addition of the IBM QRadar Network Insights 1940 appliance, providing the ability to deploy a dedicated appliance on a 40 Gbps network.


The IBM QRadar Network Insights 1940 appliance is available on both Lenovo (1940) and Dell (1940-C) hardware platforms with appliance ID 6600.

Network connectivity is not indicative of the data throughput levels that each appliance is capable of.

### Deprecation of IP reputation suspect content warnings

Suspect content warnings that are based on X-Force IP reputation categories are deprecated and will be removed in a future QRadar Network Insights release.

To prepare for this change, rules or queries that use IP reputation suspect content descriptions must be updated to use direct X-Force IP reputation lookups. Using the direct X-Force lookups ensures that the IP reputation classifications are more up-to-date, and provides additional classifications that were not available as part of the former suspect content warnings.

 To learn more about using X-Force lookups for IP reputation, see the IBM QRadar Network Insights *User Guide*.

### DNS Query and DNS Response fields removed

The **DNS Query** and **DNS Response** fields were removed in QRadar Network Insights 7.4.1. You can still view these fields in data that was received in the past, but the fields are not included in new data captures.

Use the following DNS data fields instead. These fields are available at the **Enriched** and **Advanced** inspection levels:

- DNS Query ID
- DNS Domain Name
- DNS Request Type
- DNS Response Code
- DNS Flags
- DNS Answers (formatted list of strings)





# Chapter 4. What's new in QRadar 7.4.0

The IBM QRadar 7.4.0 family of products includes enhancements to performance, workflow, security, and user experience.

## QRadar

IBM QRadar 7.4.0 includes enhancements to performance, security, workflow enhancements, and flow improvements.

### Performance optimization

The performance improvements in QRadar 7.4.0 include enhanced parsing support for name value pairs and generic list events, the ability to remove reference data when you uninstall a content extension, a faster way to export content from the DSM Editor, and updates to flow records.

#### Enhanced parsing support for XML events in the DSM Editor

In the DSM Editor, you can now easily parse both standard and custom properties from events in XML format without writing regular expressions (regex). When you enable **Property** autodiscovery for log source types that consume XML events, all available fields are parsed as custom properties. With these new capabilities, administrators and users who have permission to create custom properties, can quickly and easily parse these events.

Use the DSM Editor to create a custom log source type to handle XML events in IBM QRadar. Add custom properties to help parse an existing log source type. Use simple XML expressions instead of regex to define how to parse custom properties. The DSM Editor automatically provides expressions for system properties based on their predefined keys in the XML specification.

Turn on XML property autodiscovery to discover custom properties for all XML fields in any events that are received for the log source type. Use XML expressions in the **Custom Event Property Editor** and when you manually create log source extensions.

The following figure shows where you parse XML events in the DSM Editor.

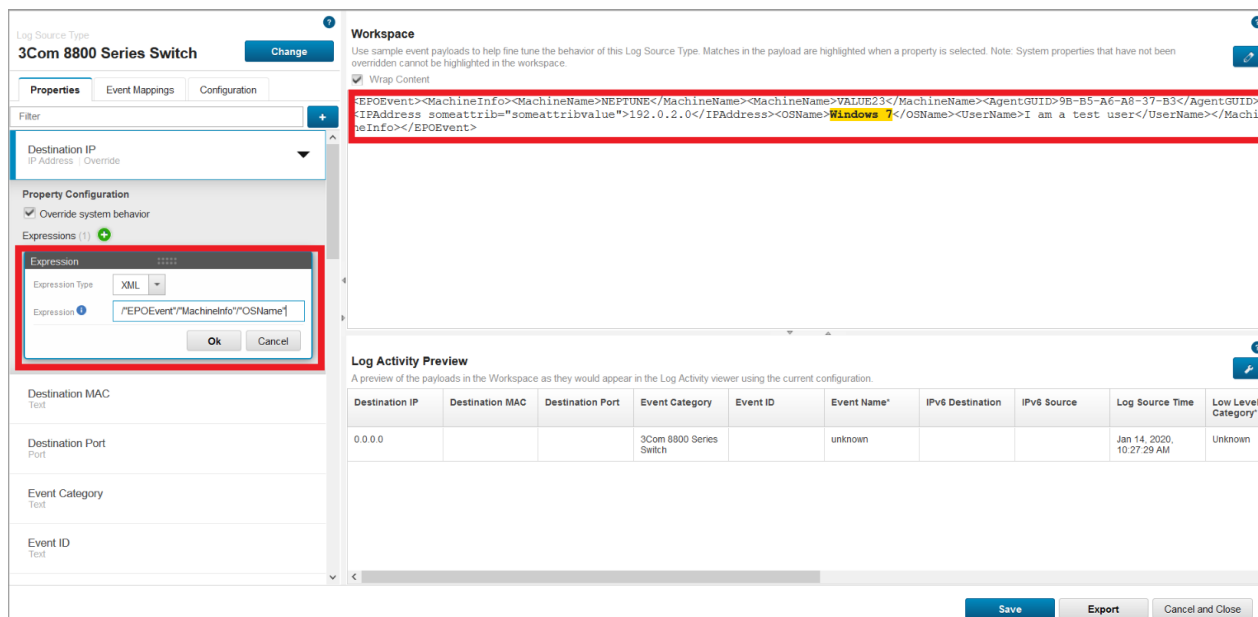

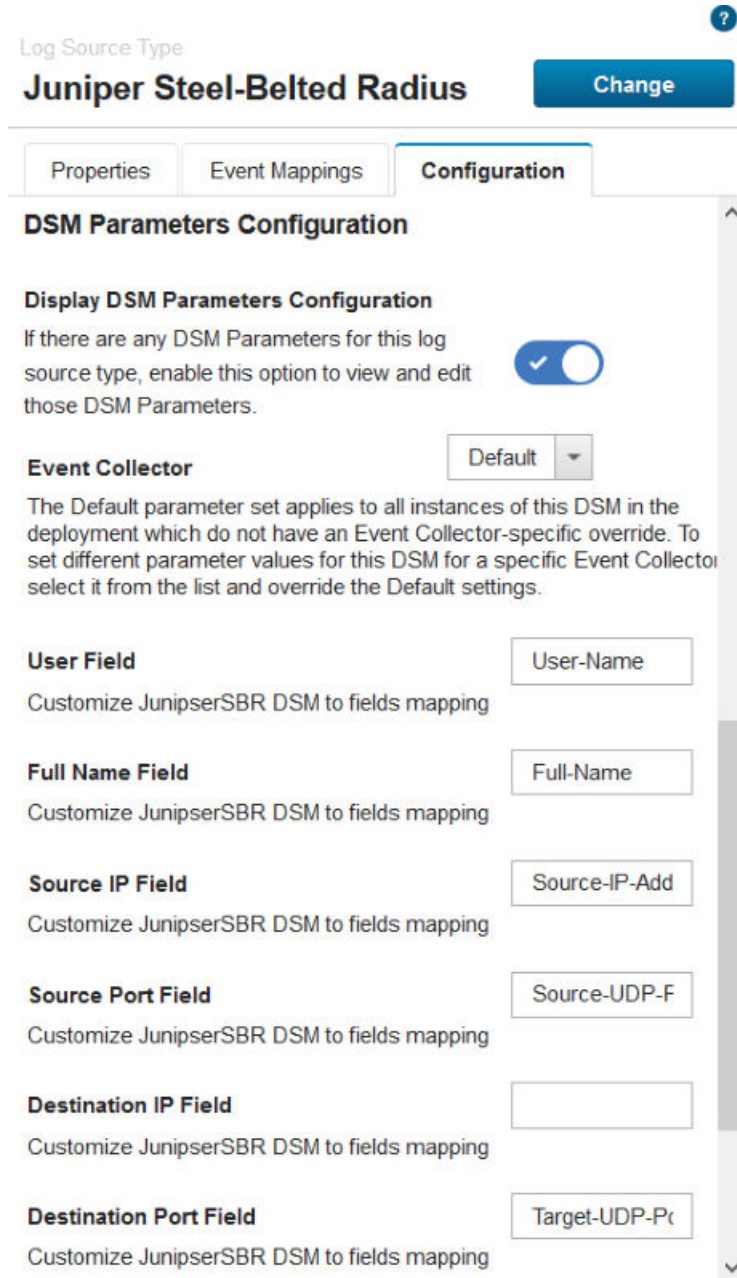


Figure 6. XML structured data type

 To learn more about enhanced parsing support for XML events, see the *IBM QRadar Administration Guide*.

## DSM Parameter support in the DSM Editor

In QRadar 7.4.0, if your log source type has DSM parameters, you can use the DSM Editor to configure the DSM parameters. Enable the **Display DSM Parameters Configuration** option to view and edit the DSM parameters.



Log Source Type ?

### Juniper Steel-Belted Radius Change

Properties | Event Mappings | **Configuration**


#### DSM Parameters Configuration

**Display DSM Parameters Configuration**  
If there are any DSM Parameters for this log source type, enable this option to view and edit those DSM Parameters.

**Event Collector** Default

The Default parameter set applies to all instances of this DSM in the deployment which do not have an Event Collector-specific override. To set different parameter values for this DSM for a specific Event Collector select it from the list and override the Default settings.

<b>User Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text" value="User-Name"/>
<b>Full Name Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text" value="Full-Name"/>
<b>Source IP Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text" value="Source-IP-Add"/>
<b>Source Port Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text" value="Source-UDP-F"/>
<b>Destination IP Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text"/>
<b>Destination Port Field</b> Customize JunipserSBR DSM to fields mapping	<input type="text" value="Target-UDP-Pc"/>

 To learn more about configuring DSM parameters in the DSM Editor, see the *IBM QRadar Administration Guide*.

## Additional standard fields for events

View additional details about your events. These details provide increased visibility into how events are internally processed by QRadar.

 To learn more about event details, see the *IBM QRadar User Guide*.

## Security enhancements


Stronger security capabilities in IBM QRadar 7.4.0 include modifying the inactivity timeout for user accounts.

### More secure operating system

QRadar 7.4.0 runs on Red Hat Enterprise Linux version 7.6. The update to RHEL V7.6 is necessary to continue receiving security updates from Red Hat Enterprise Linux.

### Reverse tunnel initiation


The SSH tunnel between two managed hosts can now be initiated from the remote host instead of the local host. For example, you have a connection from an Event Processor in a secure environment to an Event Collector that is outside of the secure environment. You also have a firewall rule that prevents you from having a host outside the secure environment connect to a host in the secure environment. In QRadar 7.4.0, you can switch which host creates the tunnel so that the connection is established from the Event Processor by selecting the Remote Tunnel Initiation checkbox for the Event Collector.

 To learn more about configuring Secure email server, see the *IBM QRadar Administration Guide*.

### Secure email server

Send email to distribute alerts, reports, notifications, and event messages to mail servers that require authentication.

You can configure an email server for your entire QRadar deployment, or multiple email servers.

 To learn more about configuring Secure email server, see the *IBM QRadar Administration Guide*.

## Workflow enhancements in QRadar

Improvements to workflow in IBM QRadar for 7.4.0 include three apps previously only available on the IBM Security App Exchange.

### Apps installed by default

In QRadar 7.4.0, the IBM QRadar Assistant app, the IBM QRadar Pulse app, and the IBM QRadar Log Source Management app are installed by default.

Use the IBM QRadar Assistant app to manage your app and content extension inventory, view app and content extension recommendations, follow the QRadar Twitter feed, and get links to other information.

IBM QRadar Pulse is a dashboard app that you can use to communicate insights and analysis about your network. Take the pulse of your SOC with dynamic real-time dashboards that provide meaningful insights into your security posture and threat landscape. Visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, a built-in 3D threat globe, and auto updating charts. Import and export dashboards to share with colleagues. See offenses unfold near real time and track your security threats from around the globe.

The IBM QRadar Log Source Management app provides an easy-to-use workflow that helps you quickly find, create, edit, and delete log sources. Use the simplified workflow to change parameters for a number of log sources at the same time. To configure log sources in 7.4.0, you must use the IBM QRadar Log Source Management app.

User roles with the system administrator permission are updated automatically to include the required permissions for the apps installed by default. All other user roles must be modified to include the app permissions as needed.

## Flow improvements

QRadar 7.4.0 gives you more control over flow timestamps.

### Improved flow timestamp handling

Two new configuration settings provide more control over the way that flow timestamps are handled when Netflow V9 begins sending records with overflowed system uptime values. The new settings eliminate the need to reset the first and last switched times.

The new configuration options and the default values are shown here:

- NORMALISE\_OVERFLOWED\_UPTIMES=YES
- UPTIME\_OVERFLOW\_THRESHOLD\_MSEC=86400000

The timestamps are corrected when the system uptime value is less than the first and last switched packet times by more than the value that is specified in the UPTIME\_OVERFLOW\_THRESHOLD\_MSEC configuration. The timestamps are corrected based on the assumption that the system uptime wrapped around the maximum 32-bit value.

 To learn more about managing flow timestamps, see the *IBM QRadar Administration Guide*.

## What's changed or removed

IBM QRadar V7.4.0 includes enhancements to existing features and updated browser conformance specifications.

### Clicking Log Sources icon opens IBM QRadar Log Source Management app

When you click the Log Sources icon in the **Admin** menu, the IBM QRadar Log Source Management app opens, which is the new method for configuring log sources in 7.4.0.

### Asset Profiler Configuration changes

In QRadar 7.4.0, the **QVM Configuration** and **Manage Identity Exclusion** sections of the **Asset Profiler Configuration** now have their own icons in the **Admin** menu.

### Browser conformance change

The Microsoft Internet Explorer web browser is no longer supported as of QRadar 7.4.0.

### Global System Notifications configuration

Global System Notifications are now local, making them host specific and more useful. As a result, the thresholds are now set automatically by QRadar and the Global System Notification section of the Admin tab was removed.


## QRadar Network Insights

---

IBM QRadar Network Insights 7.4.0 introduces a software-only installation, a new BitTorrent inspector, deprecated suspect content warnings, and improved flow interface data and domain segmentation.

### QRadar Network Insights software installation is now available

Now you can install QRadar Network Insights on your own hardware or as a virtual machine. This new capability provides the same type of flow analysis that was previously available only with a physical appliance that used a Napatech network interface card.

 To learn more about installing QRadar Network Insights, see the *QRadar Network Insights Installation and Configuration Guide*.

## Separate installation file for QRadar Network Insights

In previous releases, the QRadar Network Insights installation files were combined with the QRadar Incident Forensics installation files in a single .iso file. In 7.4.0, each product is installed by using a separate .iso file.

The process to upgrade your deployment does not change, and only a single file is required. You must ensure that you download the correct .sfs file for your deployment.

### Note:

If your deployment does not include QRadar Incident Forensics, you can upgrade to QRadar Network Insights 7.4.0 by using the QRadar patch update file.

If your deployment includes both QRadar Network Insights and QRadar Incident Forensics, you can upgrade to QRadar Network Insights 7.4.0 by using the QRadar Incident Forensics patch update file.

Both patch update files are available on IBM Fix Central.

The following examples show what the file names might look like on IBM Fix Central:

- To install QRadar Network Insights in a new deployment, the .iso file name looks similar to this example:

`Rhe764qni<build_version>.stable-<identifier>.iso`

- To upgrade QRadar Network Insights in a deployment that does not include QRadar Incident Forensics, the .sfs file name looks similar to this example:


`<identifier>_QRadar_patchupdate-<build_number>.sfs`

This .sfs file upgrades the entire QRadar deployment.

- To upgrade QRadar Network Insights in a deployment that does include QRadar Incident Forensics, the .sfs file name looks similar to this example:

`<identifier>_Forensics_patchupdate-<build_number>.sfs`

This .sfs file upgrades the entire QRadar deployment, including QRadar Incident Forensics and QRadar Network Insights.

 To learn more about installing and upgrading QRadar Network Insights, see the QRadar Network Insights *Installation and Configuration Guide*.

## New BitTorrent inspector

Earlier versions of QRadar relied on the application signatures file to detect the BitTorrent protocol.

In QRadar Network Insights 7.4.0, the new BitTorrent inspector makes it easier to identify BitTorrent traffic, especially in environments where the BitTorrent client is using UDP with the uTorrent transfer protocol.

This release also includes a new suspect content description that is labeled **BitTorrent Handshake verification failure**.

 To learn more about the supported protocol inspectors, see the *QRadar Network Insights User Guide*.


## Easily identify where flows originated from

In previous versions of QRadar Network Insights, the **Flow Source** and **Flow Interface** columns on the **Network Activity** tab showed information about the QFlow appliance that received the flows from QRadar Network Insights, with no visibility into the interface that is being inspected. Depending on your deployment, this information might come from the QRadar Console, or a Flow Processor or Flow Collector.

In 7.4.0, default flow sources are automatically detected and added to the deployment configuration. On the **Network activity** tab, the **Flow Source** column shows the hostname of the managed host that


received the flow. The **Flow Interface** column shows the network interface on the managed host that received the flow.

For standard network interfaces, the **Flow Interface** column shows the name that is used in the underlying Red Hat Enterprise Linux operating system. For appliances that have a Napatech card, it shows **napatech0**.

 To learn more about working with QRadar Network Insights flows, see the *QRadar Network Insights User Guide*.

## Domain management for QRadar Network Insights flow sources


Now you can assign domains or tenants based on a QRadar Network Insights flow source or interface that the traffic originated from. By segmenting your network into different domains, you can ensure that information is available only to those users who need it.

 To learn more about segmenting data based on flow sources, see the *IBM QRadar Network Insights Installation and Configuration Guide*.

## Deprecation of IP reputation suspect content warnings

Suspect content warnings that are based on X-Force IP reputation categories are deprecated and will be removed in a future QRadar Network Insights release.

To prepare for this change, rules or queries that use IP reputation suspect content descriptions must be updated to use direct X-Force IP reputation lookups. Using the direct X-Force lookups ensures that the IP reputation classifications are more up-to-date, and provides additional classifications that were not available as part of the former suspect content warnings.

 To learn more about using X-Force lookups for IP reputation, see the *IBM QRadar Network Insights User Guide*.

## Deprecation of DNS Query and DNS Response fields

The **DNS Query** and **DNS Response** fields will be deprecated in a future QRadar Network Insights release.

To prepare for this deprecation, use the following DNS data fields instead. These fields are available at the **Enriched** or **Advanced** inspection levels:

- DNS Query ID
- DNS Domain Name
- DNS Request Type
- DNS Response Code
- DNS Flags
- DNS Answers (formatted list of strings)

## QRadar Incident Forensics

---

IBM QRadar Incident Forensics 7.4.0 introduces changes to the files that are used to install and upgrade your deployment, and a new BitTorrent inspector.

### Isolated installation file for QRadar Incident Forensics

In previous releases, the QRadar Incident Forensics installation and upgrade files included QRadar Network Insights. In 7.4.0, each product has a separate `.iso` file for new installations.

The process to upgrade your deployment does not change. Only a single file is required, but you must ensure that you download the `.sfs` file that includes QRadar Incident Forensics.

The following examples show what the file names might look like on IBM Fix Central:


- New QRadar Incident Forensics installations:

`Rhe764forensics<build_version>.stable-<identifier>.iso`

- Upgrades to existing QRadar installations that include QRadar Incident Forensics:

`<identifier>_Forensics_patchupdate-<build_number>.sfs`

This `.sfs` file upgrades the entire QRadar deployment, including QRadar Incident Forensics and QRadar Network Insights.


 To learn more about installing and upgrading QRadar Incident Forensics, see the *IBM QRadar Incident Forensics Installation Guide*.

## New BitTorrent inspector

Earlier versions of QRadar relied on the application signatures file (`signatures.xml`) to detect the BitTorrent protocol.

In QRadar Incident Forensics, the new BitTorrent inspector provides summary information about the connection, including the number of messages and the session duration. The protocol metadata includes information about the peers and the actual torrent file. You can use peer identifiers to track a BitTorrent client instance over time, or to identify when an IP address changes.

The protocol metadata also includes a new `InfoDictionaryHash` field that serves as a unique identifier for the torrent that is being transferred. Use this identifier in a forensics investigation to trace back and show the files that were being transferred.

 To learn more about the supported protocols and document types, see the *IBM QRadar Incident Forensics Administration Guide*.


## Change to search query syntax

The QRadar Incident Forensics search engine no longer supports spaces in field-specific searches. For example, the following queries are invalid:

- `Content: text`
- `TcpPort: 80 AND IPAddress: "192.168.2.36"`

These queries are valid:

- `Content:text`
- `TcpPort:80 AND IPAddress:"192.168.2.36"`

 To learn more about search query syntax, see the *IBM QRadar Incident Forensics User Guide*.

## QRadar application framework

---

The IBM QRadar V7.4.0 application framework introduces support for multi-tenanted apps.

### Run apps in a multi-tenant environment


QRadar V7.4.0 includes support for multi-tenanted apps. Several apps, such as IBM QRadar Pulse, IBM QRadar Assistant, and IBM Log Source Management, can now be used in a multi-tenant environment.

App developers can now mark that their app has been tested and works in a multi-tenanted environment. There are two forms of multi-tenancy support:

1. The app is tested and works with multi-tenancy, but it is not multi-tenancy aware. When a user installs the app, they are presented with the option to create a default instance. Users can select this option if they only want a single instance of the app, or the app does not need to support multi-tenancy. If

a user does not select the **Default Instance** option, they must create a separate instance for each customer and associate each instance with a security profile to keep all client data separate.

2. The app is tested and is multi-tenancy aware. In this case, only one instance of the app is necessary. This type of app is also beneficial if the app is designed to be used only by administrators.

 To learn more about app multi-tenancy, see the *IBM QRadar Application Framework Developer Quick Start Guide*.

## QRadar Vulnerability Manager and QRadar Risk Manager

---

QRadar Vulnerability Manager 7.4.0 introduces a new search parameter to identify controversial vulnerabilities, and enhancements to vulnerability exceptions. IBM QRadar Risk Manager 7.4.0 introduces improved support for Juniper Networks JUNOS Network Address Translation.

### Controversial vulnerabilities search parameters

QRadar Vulnerability Manager v7.4.3 includes new search parameters that leverage vulnerability data that is retrieved from multiple scanners. The **Found by Scanner** and **Not Found by Scanner** parameters provide the following benefits:

- Reduce data set redundancy through the removal of duplicate vulnerabilities.
- Improve quality of results by reducing potential false positives.
- Compare vulnerabilities discovered by multiple scanners to improve scanning techniques and identify shortcomings.

### Enhancement to vulnerability exceptions

QRadar Vulnerability Manager v7.4.2 removes a limitation that allowed users to create exceptions for only one vulnerability instance in an exception rule. You can now create rules that include exceptions for multiple vulnerabilities.

For more information, see the [IBM QRadar Vulnerability Manager User Guide](#).

### QRadar Risk Manager support for JUNOS Network Address Translation (NAT)

IBM QRadar Risk Manager v7.4.1 introduces improved support for Network Address Translation (NAT) functionality in Juniper Networks JUNOS devices to cater to service-sets. NAT provides increased security for your IBM QRadar deployment because requests are managed through the conversion process and internal IP addresses are hidden. Unlike other devices that perform NAT, JUNOS NAT functions use expansion cards to perform the NAT process.

For more information about the Juniper Networks JUNOS adapter, see the [Supported adapters](#) section of the [QRadar Risk Manager adapter configuration guide](#).



## 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.

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

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

## 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”.

## 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>





