

# Log Source Management App

Colin Hay  
Chief Software Architect

Keith Degrace  
Software Developer

Chris Collins  
Team Lead, QRadar  
Integrations

Corey Ferguson  
Software Developer

Michael Richards  
Product Owner,  
QRadar Integrations

Michael Hume  
Manager, QRadar  
Integrations

Jeff Rusk  
Development Manager

Steven Savage  
Iteration Manager & QA Lead

Jonathan Pechta  
Support Content Lead

**IBM Security**

27 February 2020



# Agenda

<b>Announcements</b>	<b>03</b>
<b>About the Log Source Management app</b>	<b>04</b>
<b>0: Core functionality</b>	<b>05</b>
<b>1: Data visibility</b>	<b>06</b>
<b>2: Manage log sources</b>	<b>09</b>
<b>3: Filter and search functions</b>	<b>12</b>
<b>Functionality overview (demo)</b>	<b>13</b>
<b>4: Troubleshooting</b>	<b>14</b>
<b>Troubleshooting protocols (demo)</b>	<b>18</b>
<b>5: Keep your apps updated</b>	<b>19</b>
<b>6: Submitting enhancements</b>	<b>20</b>

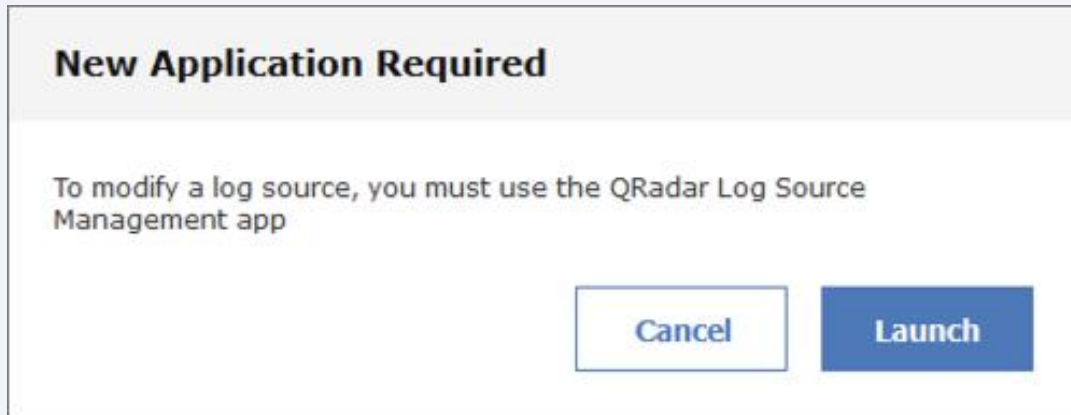
# Announcements

- New test tools are available: JDBC Protocol includes log source tests **PROTOCOL-JDBC-7.3-20200110201324.noarch.rpm** (or later)
- New support pages coming soon for Parsing 101
- Official Support Forums are moving at the end March, more details coming soon. Bookmark the following IBM short URLs:  
<https://ibm.biz/qradarceforums> (QRadar Community Edition Q&A) or  
<https://ibm.biz/qradarforums> (QRadar Support Forum)

# About the Log Source Management App

API driven app that allow users to configure event sources and associate incoming data to protocols in QRadar.

- QRadar 7.4 (unreleased) deprecates the legacy log source user interface for the Log Source Management app.
- Compatible with QRadar 7.3.1 and later
- Low memory requirements (100 MB)
- Download the latest version or use the QRadar Assistant App to install new applications: (<https://ibm.biz/getqradarlsm>)
- QRadar on Cloud and QRadar Community Edition ready



# 0: Core functionality

## IBM QRadar Log Source Management

### Filter

#### Status (5)

[Clear](#)

- ☒ OK 14
- ☐ Warning 0
- ☐ Error 15
- ☐ Not Available 0
- ☐ Disabled 0

#### Enabled (2)

- ☐ Yes 14
- ☐ No 0

#### Log Source Type (14)

- ☐ Amazon AWS CloudTrail 1
- ☐ Anomaly Detection Engine 1
- ☐ Custom Rule Engine 1

[+ New Log Source](#)

### Log Sources (14)

<input type="checkbox"/>	Name ^	Log Source Type	Creation Date ^	Last Event	ID	Enabled	Language	
<input type="checkbox"/>	<a href="#">Amazon_AWSCloudTrail_</a>	Amazon AWS CloudTrail	Nov 11, 2019 10:46 AM	Feb 25, 2020 8:04 PM	1612	<input checked="" type="checkbox"/>	English	...
<input type="checkbox"/>	<a href="#">WinCollect @ XGSLAB</a>	WinCollect	Oct 31, 2019 12:47 PM	Feb 25, 2020 8:14 PM	1362	<input checked="" type="checkbox"/>	English	...
<input type="checkbox"/>	<a href="#">Bind @ infoblox.nios.test.com</a>	ISC BIND	Sep 4, 2019 8:21 AM	Feb 25, 2020 8:15 PM	566	<input checked="" type="checkbox"/>	English	...
<input type="checkbox"/>	<a href="#">SP LAB</a>	IBM Proventia Management SiteProtector	Aug 23, 2019 8:03 AM	Feb 25, 2020 6:58 PM	564	<input checked="" type="checkbox"/>	English	...

### Data visibility:

- Status visibility improved
- Customizable column view
- Status updates

### Manage your sources:

- Add and edit easier
- Bulk add improvements
- Export your log source as a CSV file
- API functionality

### Filtering options:

- Detailed filtering
- Improved event view
- Search vs select your log source

### Troubleshoot:

- Protocol test functionality
- Debug and improved support experience

# 1: Data visibility

- Locate log sources quickly
- Select the source to view details
- Edit the log source
- View events

IBM QRadar Log Source Management

Filter

Status (5)

Clear

☐ OK0

☐ Warning0

☒ Error3

☐ Not Available0

☐ Disabled0

Enabled (2)

☐ Yes3

☐ No0

Log Source Type (13)

☒ Linux OS2

☒ Apache HTTP Server1

Search by name, description or log source identifier

Log Sources (3)

☐ Name ^

☐ Apache @

☐ LinuxServer @

☐ LinuxServer @

# View status and history

Log Source Summary

Apache @

Apache HTTP Server

Status: Error

Last Updated 14 days ago

Events have not been received from this Log Source in over 720 minutes.

Overview

Protocol

Log Source Summary

Cisco IronPort Web Content

Cisco IronPort

Status: OK

127.0.0.1

Last Updated an hour ago

Authentication Status: Successful

File Transfer Status: No new files to transfer

Event Collection Status: No new events to process

Overview

Protocol

Test

ID

2517

Name

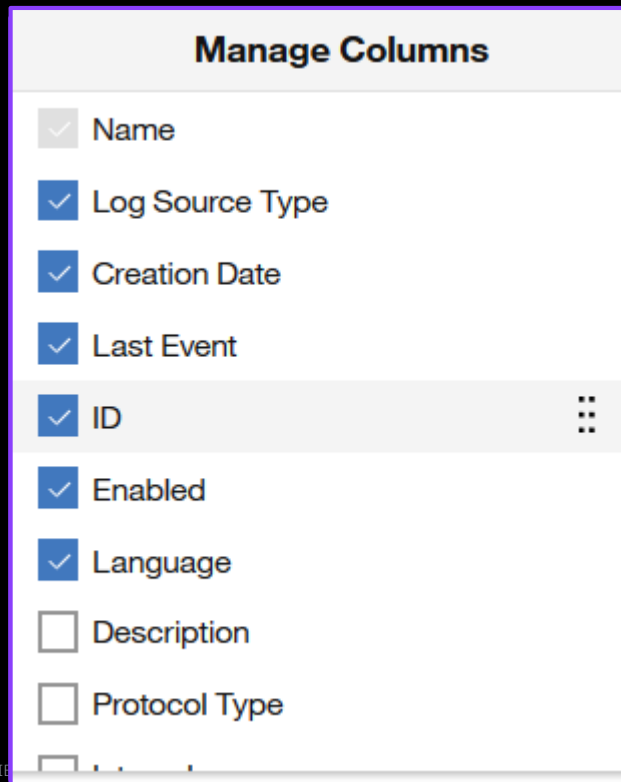
Cisco IronPort Web Content

Description

Web Content Filtering logs

# Configure or rearrange columns

Enable columns you want to view and arrange them for your team.



The screenshot shows a 'Manage Columns' dialog box with a list of columns. Each column has a checkbox and a three-dot menu icon. The columns are: Name, Log Source Type, Creation Date, Last Event, ID, Enabled, Language, Description, Protocol Type, and a partially visible 'Internal' column at the bottom. The 'ID' column is currently selected.

Manage Columns	
<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Log Source Type
<input checked="" type="checkbox"/>	Creation Date
<input checked="" type="checkbox"/>	Last Event
<input checked="" type="checkbox"/>	ID
<input checked="" type="checkbox"/>	Enabled
<input checked="" type="checkbox"/>	Language
<input type="checkbox"/>	Description
<input type="checkbox"/>	Protocol Type
<input type="checkbox"/>	Internal

## Column options

- Log Source Type
- Creation Date
- Last Event
- ID (Log Source ID)
- Enabled
- Language
- Description
- Protocol Type
- Internal
- Credibility
- Coalescing Events
- Store Event Payloads
- Deployed
- Status
- Auto Discovered
- Average EPS
- Modified Date
- Target Event Collector
- Extension
- Target Internal Destination
- Target External Destinations
- Log Source Identifier

# Exporting log source information

ID	Name	Enabled	Log Source Type	Average EPS	Creation Date	Last Event
312	IBM DNS Analyzer	Yes	IBM DNS Analyzer	141	10/13/2017 8:59	2/25/2020 20:00
562	WindowsAuthServer @ [REDACTED]	Yes	Microsoft Windows Security Event Log	13	8/19/2019 7:44	2/25/2020 20:00
563	WebGateway @ [REDACTED]	Yes	McAfee Web Gateway	9	8/19/2019 7:44	2/25/2020 20:01
564	SP LAB	Yes	IBM Proventia Management SiteProtector	88	8/23/2019 8:03	2/25/2020 18:58
566	Bind @ [REDACTED]	Yes	ISC BIND	64	9/4/2019 8:21	2/25/2020 20:01
612	QRadarAdvisorWithWatson	Yes	Universal LEEF	12	3/15/2018 8:57	2/25/2020 19:58
1612	Amazon_AWSCloudTrail	Yes	Amazon AWS CloudTrail	231	11/11/2019 10:46	2/25/2020 20:01


- Data is exported in CSV format
- Administrators have the option to export a filtered view or all log source data

### Download Log Sources

☒ Include all log source data ☐ Include only displayed columns

Start

### Download Log Sources



Preparing log sources  
0/???  
Calculating remaining time...

Cancel



# 2: Manage log sources

Adding individual log sources

1. Select Log Source Type

2. Select Protocol Type

3. Configure Log Source Parameters

4. Configure Protocol Parameters

This screenshot shows the first step of the configuration process. On the left, a vertical progress bar has four steps: 1. Select Log Source Type (active), 2. Select Protocol Type, 3. Configure Log Source Parameters, and 4. Configure Protocol Parameters. The main panel is titled "Select a Log Source type". It features a search bar with "Aruba" entered. Below the search bar, three options are listed: "Aruba ClearPass Policy Manager" (highlighted with a blue bar), "Aruba Introspect", and "Aruba Mobility Controller". At the bottom right, there is a button labeled "Step 2: Select Protocol Type".

This screenshot shows the second step. The progress bar on the left now has step 2, "Select Protocol Type", as the active step. The main panel is titled "Select a protocol type". It contains a search bar labeled "Look up Protocol Type". Below the search bar, two options are listed: "Forwarded" and "Syslog" (highlighted with a blue bar).

This screenshot shows the third step. The progress bar on the left has step 3, "Configure Log Source Parameters", as the active step. The main panel is titled "Configure the Log Source parameters". It contains a form field labeled "Name \*" with the value "Aruba lab" entered. Below the field, a small text label reads "The name of the log source." At the bottom right, there is a button labeled "Step 3: Configure Log Source Parameters".

This screenshot shows the fourth step. The progress bar on the left has step 4, "Configure Protocol Parameters", as the active step. The main panel is titled "Configure the protocol parameters". It contains two form fields: "Log Source Identifier \*" with the value "aruba.example.lab" entered, and "Incoming Payload Encoding" with a dropdown menu set to "UTF-8". At the bottom right, there is a button labeled "Finish".

# Adding multiple log sources

1. Select Log Source Type
2. Select Protocol Type
3. Configure Common Log Source Parameters
4. Configure Common Protocol Parameters
5. Configure individual Parameters

The screenshot shows the 'Select a Log Source type' screen. On the left, a vertical progress bar has five steps: 1. Select Log Source Type (active), 2. Select Protocol Type, 3. Configure Common Log Source Parameters, 4. Configure Common Protocol Parameters, and 5. Configure Individual Parameters. The main area has a search bar with 'ama' entered. Below the search bar, a list of log source types is displayed: Akamai KONA, Amazon AWS CloudTrail (highlighted), Amazon AWS Security Hub, and Amazon GuardDuty. At the bottom right, there is a button labeled 'Step 2: Select Protocol Type'.

The screenshot shows the 'Select a protocol type' screen. The progress bar on the left now shows step 2 as active. The main area has a search bar labeled 'Look up Protocol Type'. Below the search bar, a list of protocol types is displayed: Amazon AWS S3 REST API (highlighted) and Amazon Web Services.

The screenshot shows the 'Configure the common Log Source parameters' screen. The progress bar on the left shows step 3 as active. The main area has a heading 'Configure the common Log Source parameters' and a sub-heading 'Select the check box for any parameters that you want to set for all log sources. Clear the check box for any parameters that you want to set individually in step 5.' Below this, there are several checkboxes for parameters.

The screenshot shows the 'Configure the common protocol parameters' screen. The progress bar on the left shows step 4 as active. The main area has a heading 'Configure the common protocol parameters' and a sub-heading 'Select the check box for any parameters that you want to set for all log sources. Clear the check box for any parameters that you want to set individually in step 5.' Below this, there are several checkboxes for parameters, including 'Authentication Method'.

The screenshot shows the 'Configure the individual parameters' screen. The progress bar on the left shows step 5 as active. The main area has a heading 'Configure the individual parameters' and a sub-heading 'Upload from a file, or specify values manually.' Below this, there are two tabs: 'File Upload' (active) and 'Manual'. The 'File Upload' tab has a section for 'Upload a CSV file containing the individual log source parameter values. One log source will be created for each line in the file.' and a button labeled 'Upload File'. There is also a section for 'Having trouble? You can use our Bulk Template to help you get started.' and a button labeled 'Upload File'.

# Editing multiple log sources (bulk)

- Any log sources can be multi-selected and then edited if they have parameters or protocols in common.
- Bulk add no longer requires that log sources be initially added as a bulk log source group.
- Eliminates issues where log sources could not be easily removed after added in bulk.
- Converts legacy bulk sources for use in the Log Source Management app.

### Edit a Legacy Bulk Added Log Source

You can now edit log sources in bulk with this app.

If you proceed, you can no longer edit this log source in bulk using the legacy interface.

Would you like to proceed?

☐ Don't show this message again

CancelProceed


IBM

# When bulk changes are helpful

As an administrator, I need to:

1. Update the password on a number of log sources that have the same protocol type (1,000).
2. Move log sources to a new Target Event Collector as the network is changing.
3. Reassigning log source groups at scale.
4. Update naming conventions.
5. Update log sources easily if a mistake was made, such as a few log sources added use a unique payload encoding.

### Log Source Summary



**Multiple Log Sources (2)**  
Multiple Log Source Types  
Status: Not Available

Overview

Protocol

☐ Log Source Identifier \*

aruba.example.lab

☒ Incoming Payload Encoding

Shift\_JIS

# 3: Filter and search functions

IBM QRadar Log Source Management

Filter

Status (5)

Clear

☒ OK13

☐ Warning0

☐ Error

☐ Not Available

☐ Disabled

Enabled (2)

☒ Yes

☐ No

Log Source Type (12)

☐ Microsoft Windows Security Log

☐ Anomaly Detection Engine

☐ Custom Rule Engine

Group (5)

+ Add Group

☐ Other

☐ Test1

☐ Test2

☐ UBA : Systems with Honeytoken Accounts

☐ UBA : Trusted Log Source Group

Advanced: enabled=true and type\_id > 4000 🔍

## Filterable categories:

- Status (OK, Warning, Error, Not available, Disabled)
- Enabled (Yes or No)
- Log Source Type (Amazon AWS, Microsoft..)
- Protocol (Syslog, Log File, JDBC, TLS Syslog)
- Group (add or search by name)
- Extension (Name)
- Target Event Collector (Name)
- WinCollect Agent (Name)
- Internal (Yes or No)
- Deployed (Yes or No)
- Coalescing (Yes or No)
- Auto Discovered (Yes or No)

# Functionality overview (Demo)

Ask questions in the Q&A panel


# 4: Troubleshooting

Test cases are added by protocol and update through QRadar's weekly auto update system.

Protocols that support test cases:

1. TLS Syslog
2. Microsoft Office 365
3. Amazon Web Service
4. JDBC
5. Log File
6. MQ JMS
7. Cisco Firepower eStreamer

Log Source Summary



O365\_test\_lab

Microsoft Office 365

Status: Not Available


O365 Example

Last Updated 2 minutes ago

Overview

Protocol


Test



**Test this log source configuration to ensure that the parameters are correct.**

The test runs from the host specified by the Target Event Collector parameter. If there is high network latency between the console and this host, it may take a moment for the results to appear.

The test collects sample event data from the target system. This feature can be disabled in the settings.



Start Test

Close

Delete

Edit

# Types of test available

Each protocol type contains a unique set of test. All tests either succeed or fail with a description:

☒

✓

Testing SSL connection to [login.windows.net:443]

Initiating SSL handshake to [login.windows.net:443] with a timeout of 10000 ms  
Successful SSL handshake using Protocol [TLSv1.2] and Cipher Suite [SSL\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256]  
Certificate Principal [CN=graph.windows.net]

☒

✗

Testing credentials

Testing ClientID [REDACTED] :: TenantID [REDACTED]  
Error: Failed to obtained Azure AD Access Token with supplied credentials

Log Source Summary

O365\_test\_lab

Microsoft Office 365

Status: Not Available

O365 Example

Last Updated 2 minutes ago

Overview

Protocol

Test

←

↓ ⚙

✗

Restart

Results (7):

> ✓ Testing DNS resolution of [manage.office.com]

> ✓ Testing TCP connection to [manage.office.com:443]

> ✓ Testing SSL connection to [manage.office.com:443]

> ✓ Testing DNS resolution of [login.windows.net]

> ✓ Testing TCP connection to [login.windows.net:443]

> ✓ Testing SSL connection to [login.windows.net:443]

> ✗ Testing credentials

Close

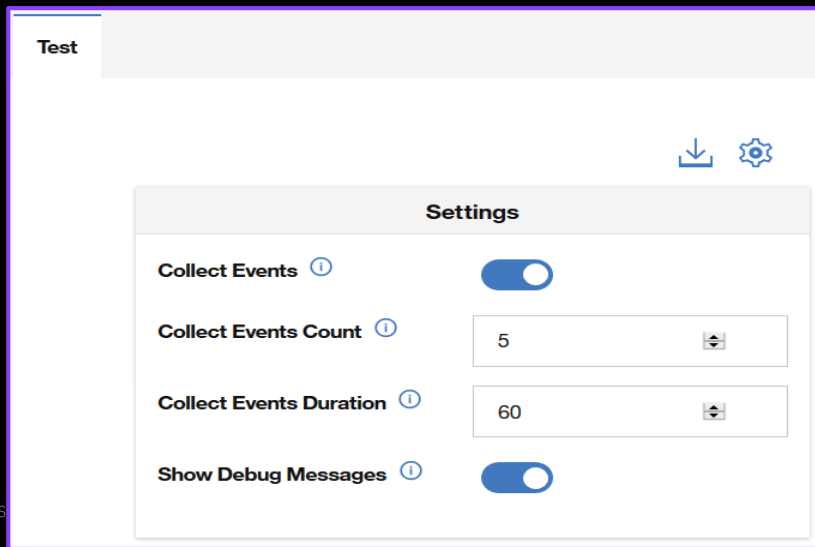
Delete

Edit

IBM Security / © 2020 IBM Corporation

# Protocol test settings

- Collect Events (Default: Enabled)
- Collect Events Count (Default: 5)
- Collect Events Duration (Default: 10)
- Show Debug Messages {on screen} (Default: Disabled)



## Comparing events

Events that are retrieved can be compared to the DSM Guide for potential issues or to understand the event format when adding new protocols.

Events (5):

Log Source Identifier	Payload
Amazon_AWSCloudTrail_	{"eventVersion":"1.02","userIdentity":{"type":"AssumedR...
Amazon_AWSCloudTrail_	{"eventVersion":"1.02","userIdentity":{"type":"AssumedR...
Amazon_AWSCloudTrail_	{"eventVersion":"1.02","userIdentity":{"type":"AssumedR...
Amazon_AWSCloudTrail_	{"eventVersion":"1.02","userIdentity":{"type":"AssumedR...
Amazon_AWSCloudTrail_	{"eventVersion":"1.02","userIdentity":{"type":"AssumedR...



# Getting help from support

Downloading logs from the application is helpful when support assistance is required. When you enable debug, the Log Source Management app displays the full error information on screen for troubleshooting with support over a WebEx session.

- Download the test results and attach the txt file to your case. This file includes debug information and there is no need to turn on debug unless you want to display the information in the interface.
- If your protocol does not include test tools, you need to submit logs for review from the Admin tab. (<https://ibm.biz/qradarlogs>)

The screenshot displays the 'Log Source Summary' interface. At the top, it shows 'O365\_test\_lab' with details 'Microsoft Office 365' and 'Status: Not Available'. A 'Test' tab is selected, showing a list of results under 'Results (7):'. The results include 'Testing DNS', 'Testing TCP', and 'Testing SSL', each with a green checkmark. A large red 'X' is overlaid on the interface, indicating an error or a failed action. A file download dialog is open, titled 'Opening test-results.txt'. It shows the file 'test-results.txt' (32.1 KB) and asks 'What should Firefox do with this file?'. The 'Open with' option is selected, and 'Notepad (default)' is chosen. There are 'OK' and 'Cancel' buttons at the bottom of the dialog. At the bottom of the interface, there are 'Close', 'Delete', and 'Edit' buttons.

Log Source Summary

O365\_test\_lab  
Microsoft Office 365  
Status: Not Available

O365 Example  
Last Updated 11 minutes ago

Overview Protocol Test

Results (7):

- > ✓ Testing DNS
- > ✓ Testing TCP
- > ✓ Testing SSL
- > ✓ Testing DNS
- > ✓ Testing TCP
- > ✓ Testing SSL

Opening test-results.txt

You have chosen to open:

test-results.txt  
which is: Text Document (32.1 KB)  
from: blob:

What should Firefox do with this file?

☒ Open with Notepad (default)

☐ Save File

☐ Do this automatically for files like this from now on.

OK Cancel

Initiating SSL handshake to [login.windows.net:443] with a timeout of 10000 ms

Close Delete Edit

# Troubleshooting protocols (Demo)

Ask questions in the Q&A panel

# 5: Keep the Log Source Manage App updated

Use the QRadar Assistant App to ensure you get the latest functionality and improvements.

- Update all apps with one click
- Update individual apps and queue installs (5)

The image displays two screenshots of the IBM QRadar Assistant application interface. The top screenshot shows the 'Applications To Update' dialog box, which lists several applications for update: IBM Resilient QRadar Integration, Threat Intelligence, QRadar Assistant App, IBM QRadar Content Extension for Amazon AWS, and QRadar Advisor With Watson. The bottom screenshot shows the 'Updates Available' section of the IBM QRadar Assistant interface, listing several applications with 'UPDATED' status indicators. The bottom screenshot also shows the 'IBM QRadar Content Extension for Amazon AWS' application details, including an 'Update' button.

**Applications To Update**

By Clicking "Agree", you confirm that you have reviewed the applicable license agreement terms, found by clicking the application name link below and that you agree to be bound by such terms and that such terms govern your use of the software that you are about to download.

- ☒ IBM Resilient QRadar Integration
- ☒ Threat Intelligence
- ☒ QRadar Assistant App
- ☒ IBM QRadar Content Extension for Amazon AWS
- ☐ QRadar Advisor With Watson

Cancel Agree Update

**Updates Available**

IBM QRadar Assistant

Home Applications

**IBM QRadar Content Extension for Amazon AWS**

QRadar, by IBM QRadar

IBM Validated

**Update**

**Overview**

Amazon Web Services CloudTrail is a service that enables operational and risk auditing of your AWS account. CloudTrail allows you to continuously monitor your AWS account activity, including actions taken through the Management Console, AWS SDKs, command lines, and other services.

**Content**

Custom Property	25
Custom QIDMap Entry	13

# 6: Submitting enhancements

Requests for enhancement allow users to submit features to QRadar Offering teams and product owners for review.

- QRadar enhancements  
(<https://ibm.biz/qradarrfe>)
- QRadar integration requests:  
DSMs, protocols, scanners, rules,  
and reports  
(<http://ibm.biz/qradarintegration>)
- QRadar app enhancements  
(<https://ibm.biz/qradarapprfe>)

## What to include in every RFE

- A description of the request
- Your security use case
- Impact on your business and deliverables

## What to include in integration requests

- Use case information for the security issue this integration, rule, or report solves
- The software/firmware versions to be integrated
- Scrubbed events, if available

## What to include in app requests

- Description of your app feature
- Your current app version and QRadar version
- Information for expected functionality or results

# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

**IBM Security**



