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

IBM

Agenda

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

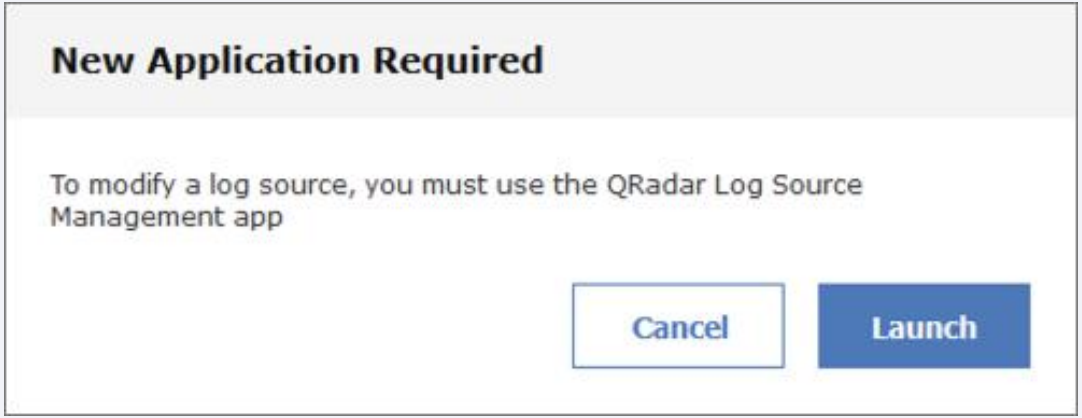
- Official Support Forums are moving at the end March, more details coming soon. Bookmark the following IBM short URLs:

  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

- [x] 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

Search by name, description or log source identifier

+ New Log Source

Log Sources (14)

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

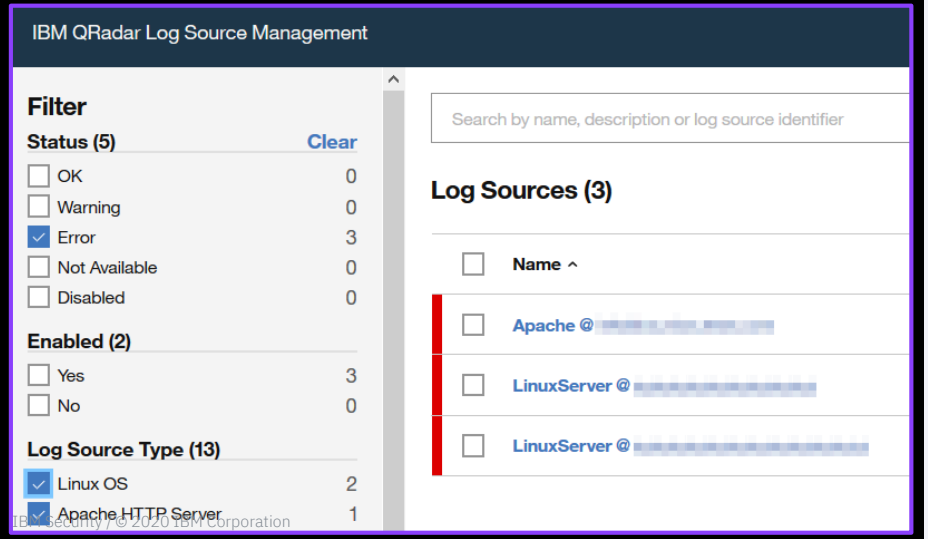
- Detailed filtering
- Improved event view
- Search vs select your log source

Troubleshoot:

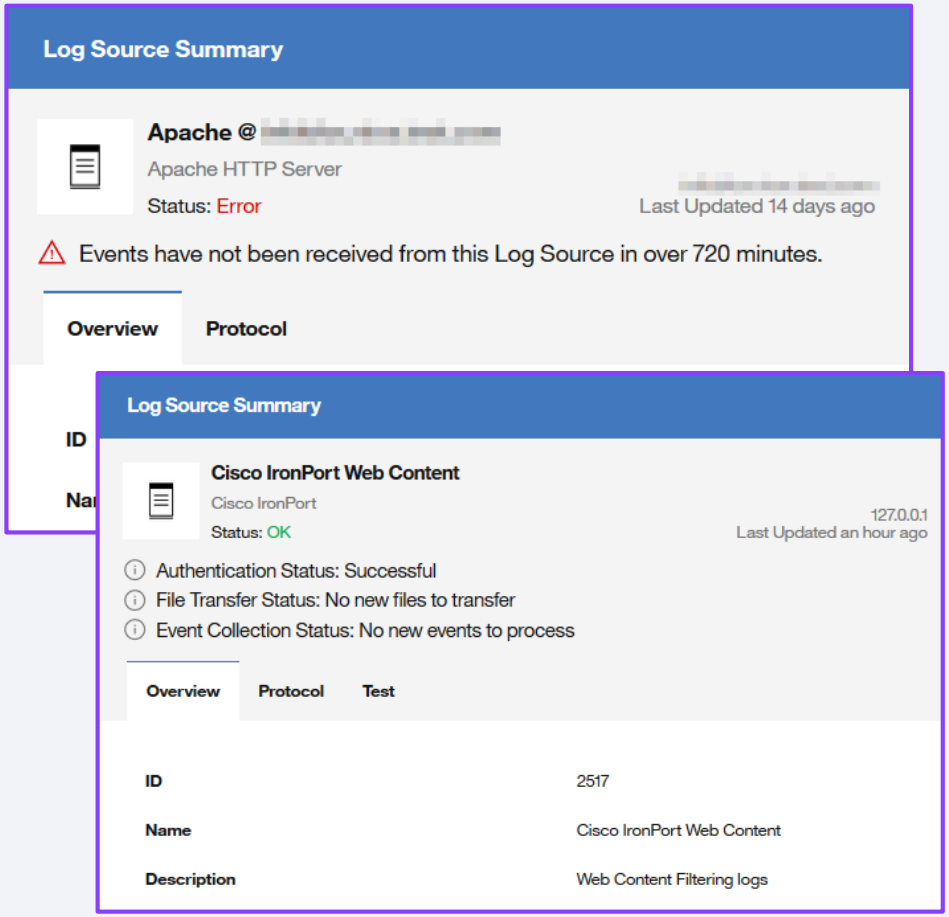
- Protocol test functionality
- Debug and improved support experience

1: Data visibility

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

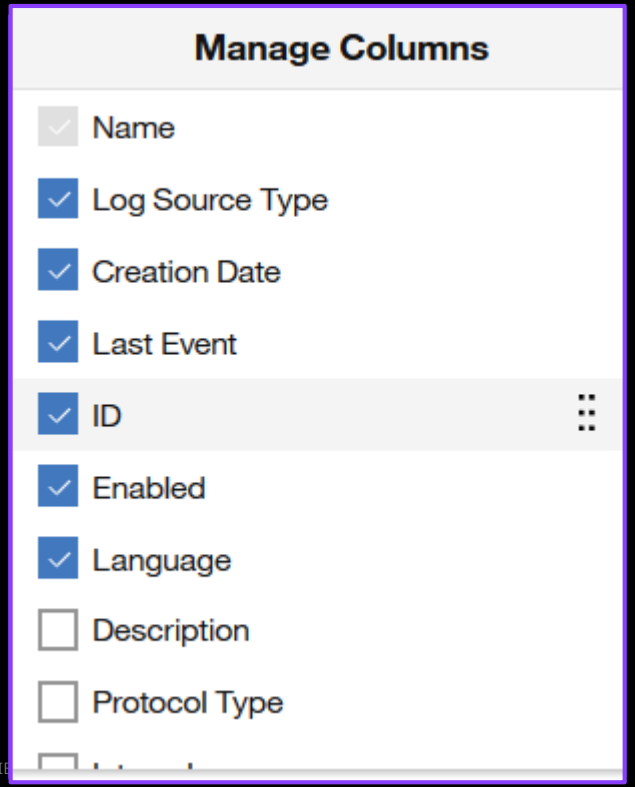


View status and history



Configure or rearrange columns

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



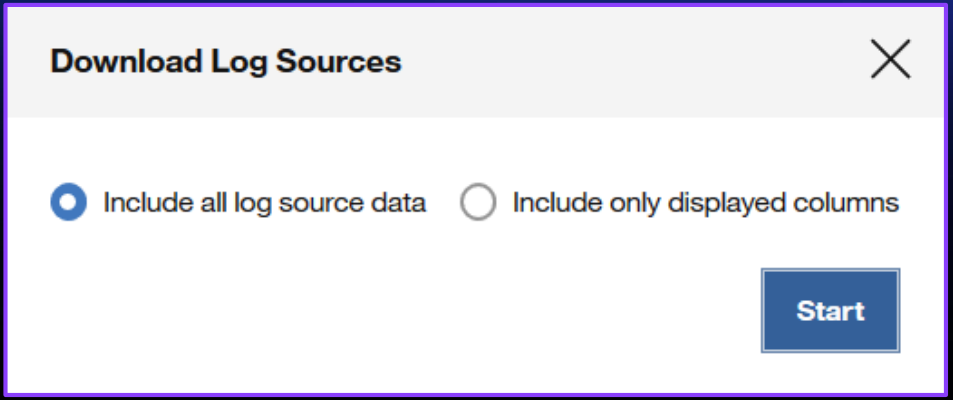
Column options

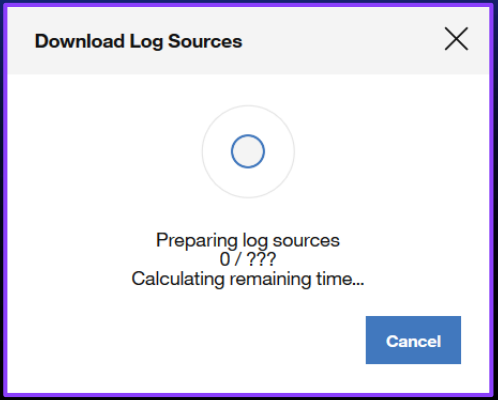
- Log Source Type
- Creation Date
- Last Event
- ID (Log Source ID)
- Enabled
- Language
- Description
- Protocol Type
- Internal
- Credibility
- Coalescing Events
- Store Event Payloads
- Deployed
- Status
- Auto Discovered
- Average EPS
- Modified Date
- Target Event Collector
- Extension
- Target 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 @	Yes	Microsoft Windows Security Event Log	13	8/19/2019 7:44	2/25/2020 20:00
563	WebGateway @	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 @	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

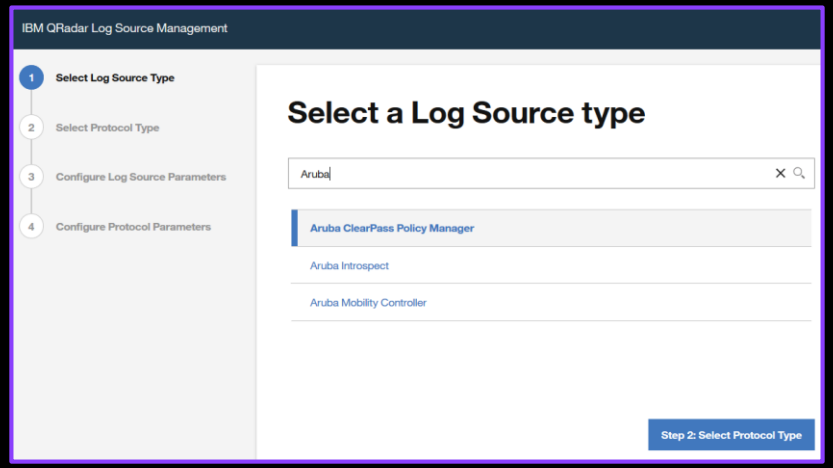


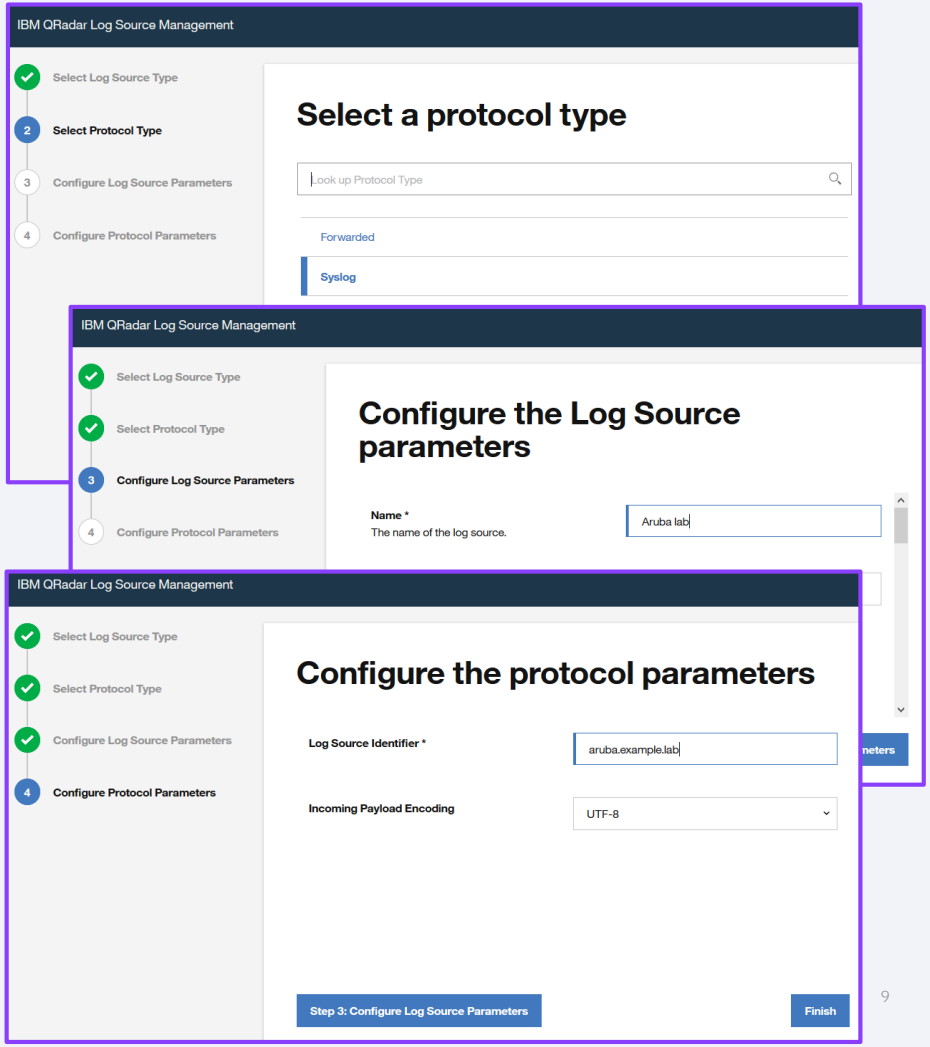


2: Manage log sources

Adding individual log sources

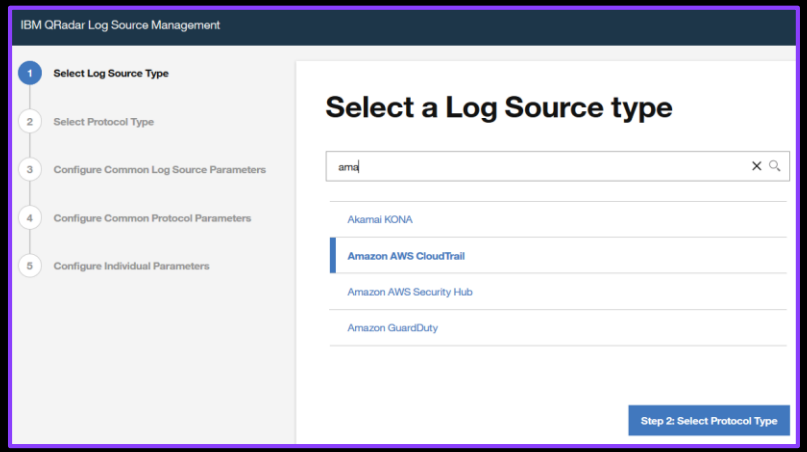
1. Select Log Source Type
2. Select Protocol Type
3. Configure Log Source Parameters
4. Configure Protocol Parameters

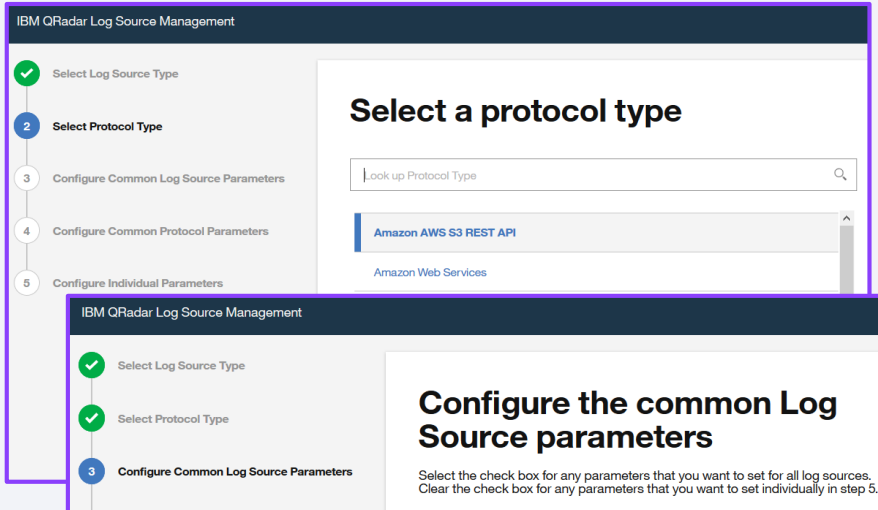


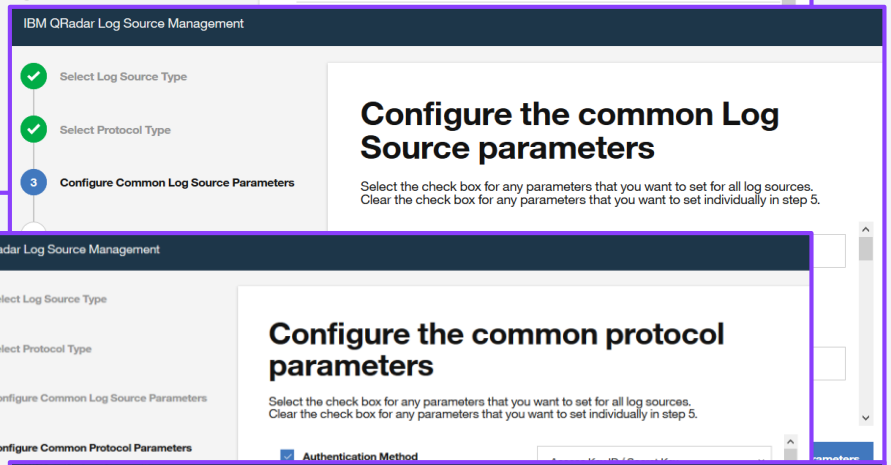


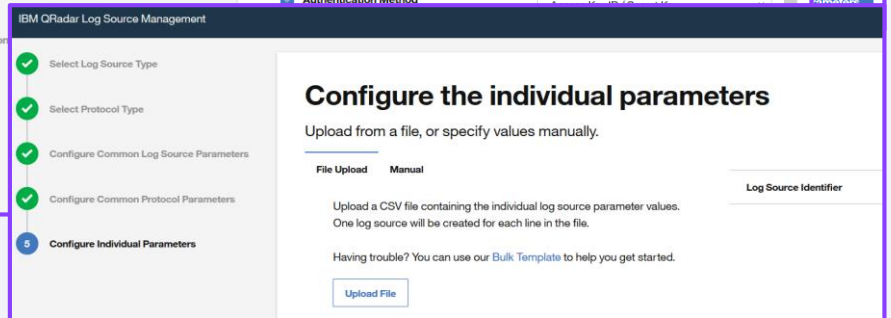
Adding multiple log sources

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



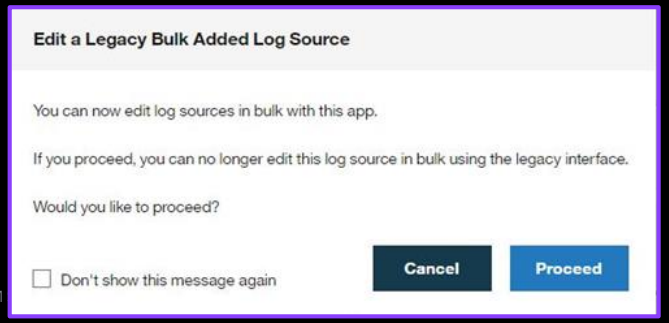






Editing multiple log sources (bulk)

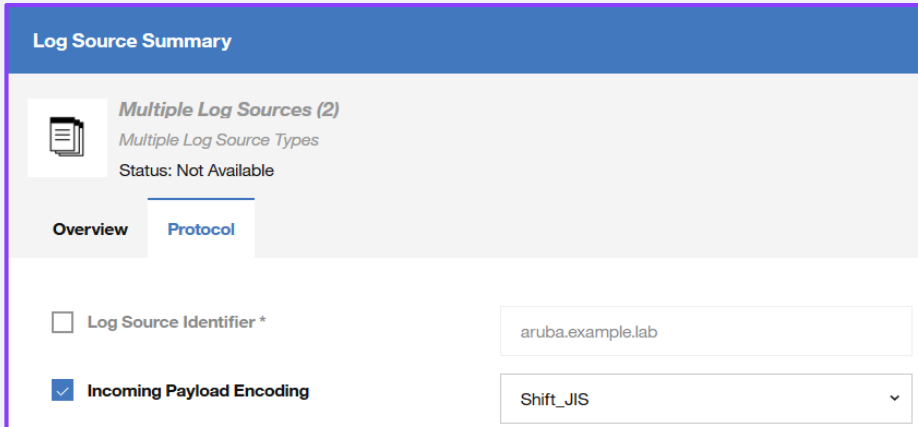
- Any log sources can be multi-selected and then edited if they have parameters or protocols in common.
- Bulk add no longer requires that log sources be initially added as a bulk log source group.
- Eliminates issues where log sources could not be easily removed after added in bulk.
- Converts legacy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



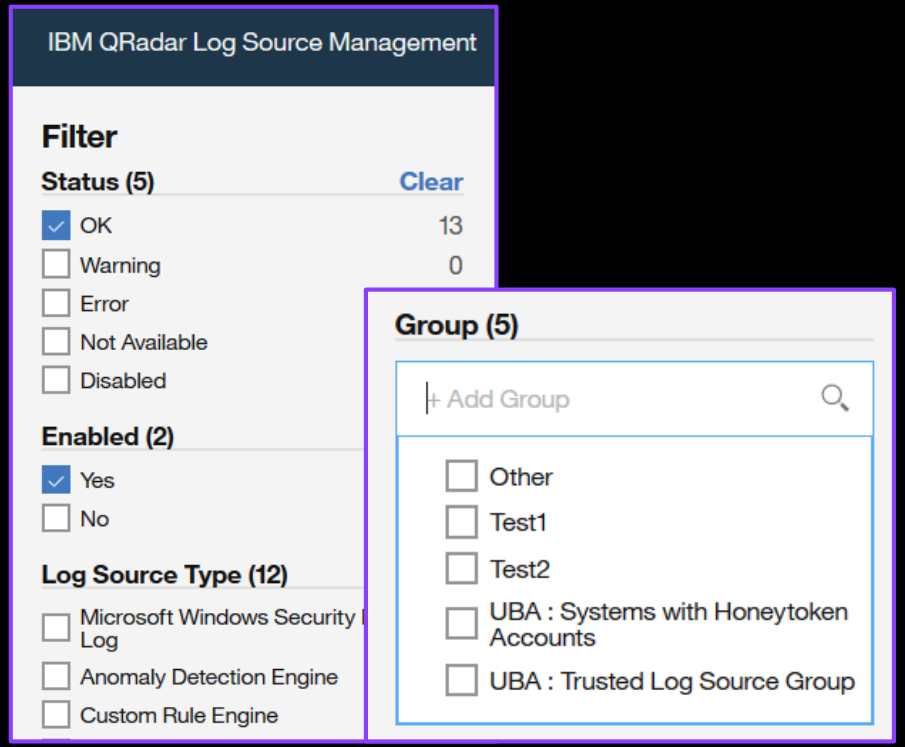
When bulk changes are helpful

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.



3: Filter and search functions



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)

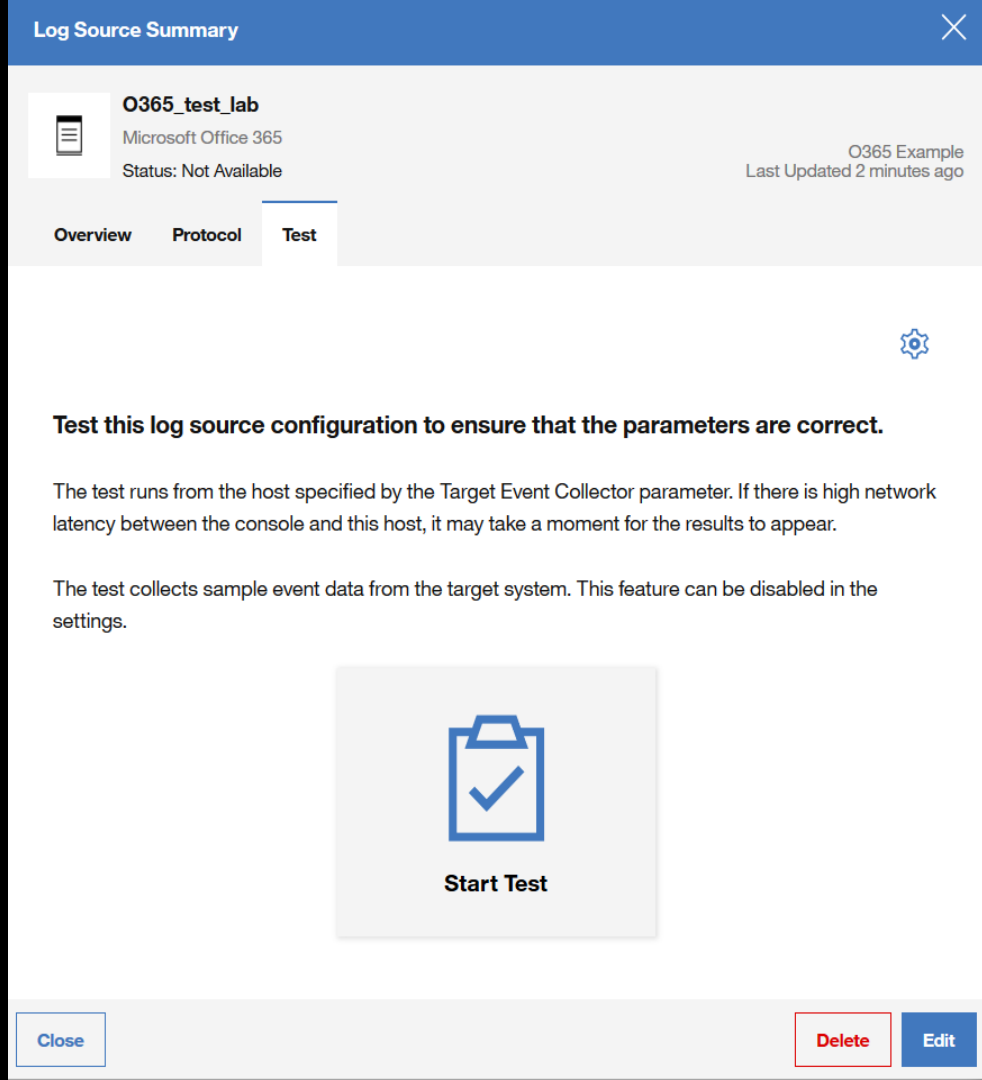
Ask questions in the Q&A panel

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



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

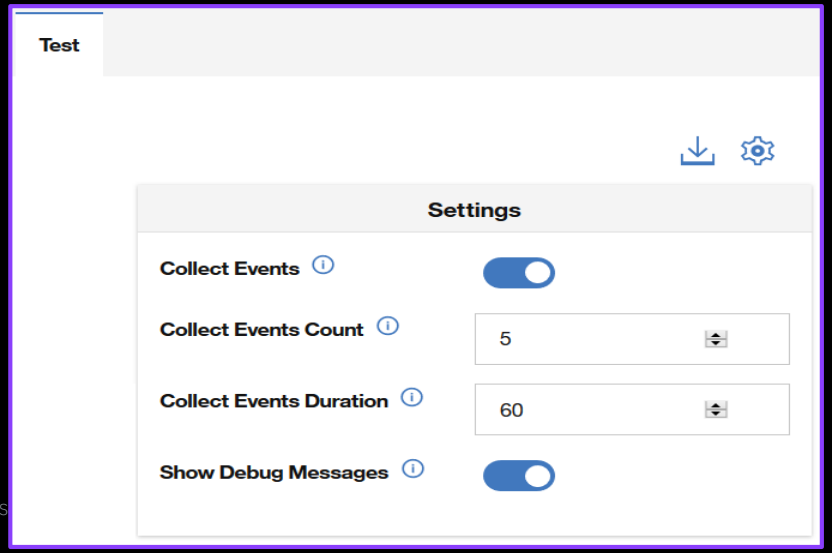
Results (7):

- 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

Protocol test settings

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



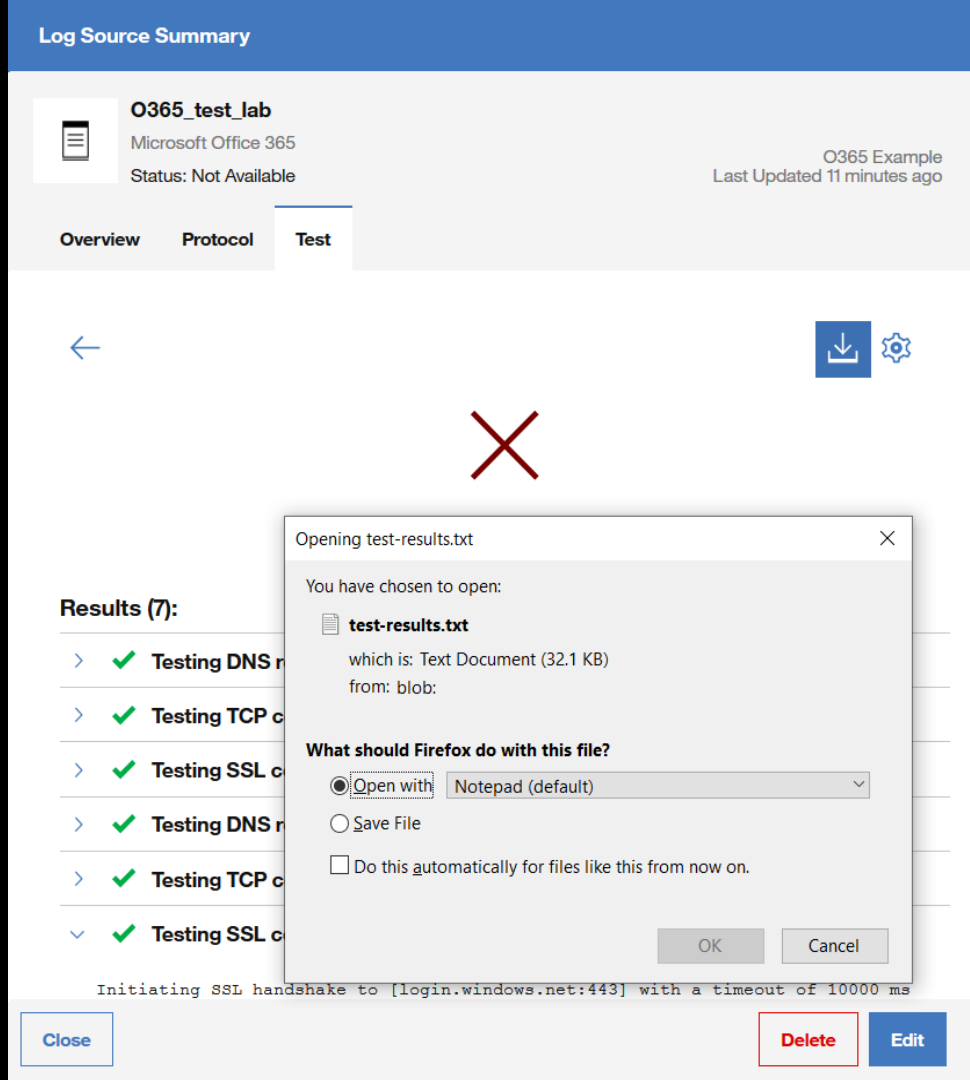
Comparing events

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

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)



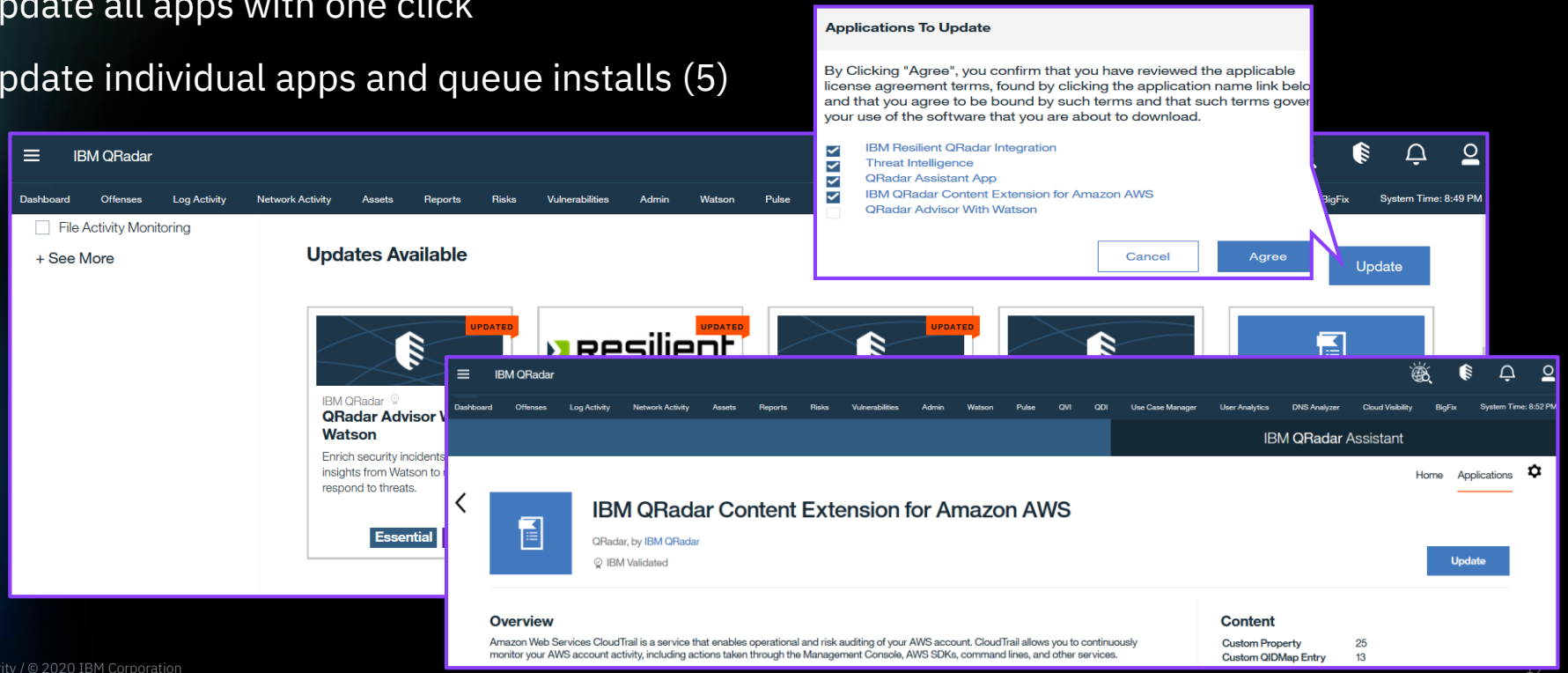
Troubleshooting protocols (Demo)

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)



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

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions