IBM Security

QRadar Advisor with Watson: Requirements & Overview

IBM SECURITY SUPPORT OPEN MIC #21

Slides and additional dial in numbers: **http://ibm.biz/openmic21**

February 23, 2017

NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.

IBM®

Panelists

- Vijay Dheap – Program Director: Cognitive, Cloud, Analytics
- Suzy Deffeyes –Security Analytics Architect
- Cameron Will – Threat Intelligence Engineer
- Christopher Hankins – Cybersecurity Specialist
- Matthew Ouellete – Software Engineer, App Development
- Adam Frank – Principal Solutions Architect
- Milan Patel - Program Director Security Offerings Management
- Jonathan Pechta – Support Content Lead & Technical Writer

Announcements

QRadar Open Mics – Coming soon

- QRadar Open Mic #22: Vulnerability & Risk Management with QRadar (March 8th)
- QRadar Open Mic #23: QRadar 7.3 Feature Discussion (Live – March 21st)

To subscribe to the newsletter, send an email to isssprt@us.ibm.com with: **snl subscribe SecIntel** in the subject line.

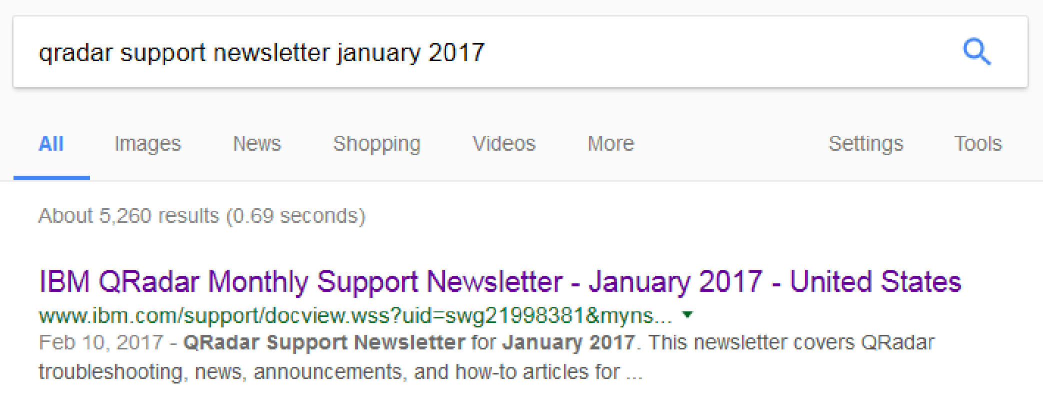
In a future newsletter, we are going to send a survey of topics for customers to set the schedule for the rest of the open mics in 2017. The goal is to come up with a list of topics customers want to see for the remainder of the year and schedule these sessions.

Make sure you are signed up for the QRadar Support Newsletter to participate in this survey!

QRadar forums

Reminder that we have a new forum at http://ibm.biz/qradarforums.

This is a great place to get questions answered from support, developers, and other QRadar users and administrators.


qradar support newsletter january 2017

About 5,260 results (0.69 seconds)

IBM QRadar Monthly Support Newsletter - January 2017 - United States
www.ibm.com/support/docview.wss?uid=swg21998381&myns...
Feb 10, 2017 - **QRadar Support Newsletter** for **January 2017**. This newsletter covers QRadar troubleshooting, news, announcements, and how-to articles for ...

User Behavioral Analytics – Early Access Program (Next Generation App)

Requirements:

- QRadar 7.2.7 or above.
- 64 GB of RAM on the QRadar Console or All-in-One appliance.
- LDAP or Active Directory is recommended
- Users with existing UBA experience is recommended

Benefits:

- New insights in to Individual behavioral models for the 2,000 most risky users, generated using machine learning algorithms (MLA).
- Work directly with IBM development to tune and customize ML algorithms to their environment to leverage the next generation of the UBA application.
- Ability to influence the direction of the next generation of UBA algorithms.
- One-on-one time with QRadar UBA developers and product management to give feedback and ask for features!

What's expected from you:

- Applicants must fill out the EAP form and return it to Milan Patel (milpatel@us.ibm.com).
- Time commitment of approximately 1 hour per week to test/tune the application.
- 30 minutes for a call with IBM team for feedback, questions, and discussion.

Timeline:

Starts on February 6th, 2017 and the program last 4 weeks.

If interested, see this forum post: http://ibm.biz/ubabeta

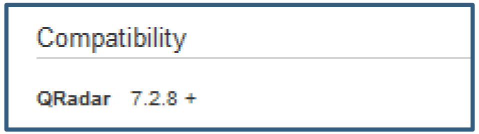
Updating QRadar to 7.2.8

Why QRadar 7.2.8?

New apps that extend the functionality for QRadar are leveraging new SDK features and options that make them only compatible with QRadar 7.2.8.

These apps are tagged for compatibility with QRadar 7.2.8 on the IBM Security App Exchange:

- QRadar Advisor with Watson
- Qualys App for QRadar
- IBM QRadar Operations (Early Access)
- BluVector Cyber Hunting



Compatibility

QRadar 7.2.8 +

ESR (Extended Service Release)
As we move forward with new software releases, such as QRadar 7.3.0 (coming soon), this release will shift our Extended Service Release (ESR) from QRadar 7.2.7 to QRadar 7.2.8. Meaning that issues and vulnerabilities are released for the ESR version and not older product versions.

Coming soon
QRadar 7.2.8 Patch 4. Keep your eye out on the forums and for information on this release. This is a big update (35 APARs resolved) and a recommended update from QRadar Support.

QRadar 7.2.8 Patch 4 is the recommended release for QRadar Advisor with Watson; however, any version of QRadar 7.2.8 is supported.

QRadar Software Release Frequency

QRadar releases generally follow the following schedule:

1. **Major releases / maintenance releases**

   Major releases, such as 7.2.7 -> 7.2.8 are typically released approximately 3 times a year. Major releases are the only release type that contains new QRadar features.

   For QRadar 7.3.0, only an ISO file is being issued to upgrade customers from 7.2.8 Patch 1 to QRadar 7.3.0.

   Correction: WinCollect 7.2.5 is a **NEW** baseline requirement for QRadar 7.3.0. Administrators with managed agents must have WinCollect 7.2.5.

2. **Fix Pack Updates**

   Patches to major releases are scheduled approximately every 4-6 weeks to resolve issues. Patches can contain a number of fixes reported in the field and can be released for our current QRadar versions, such as QRadar 7.1 or QRadar 7.2.

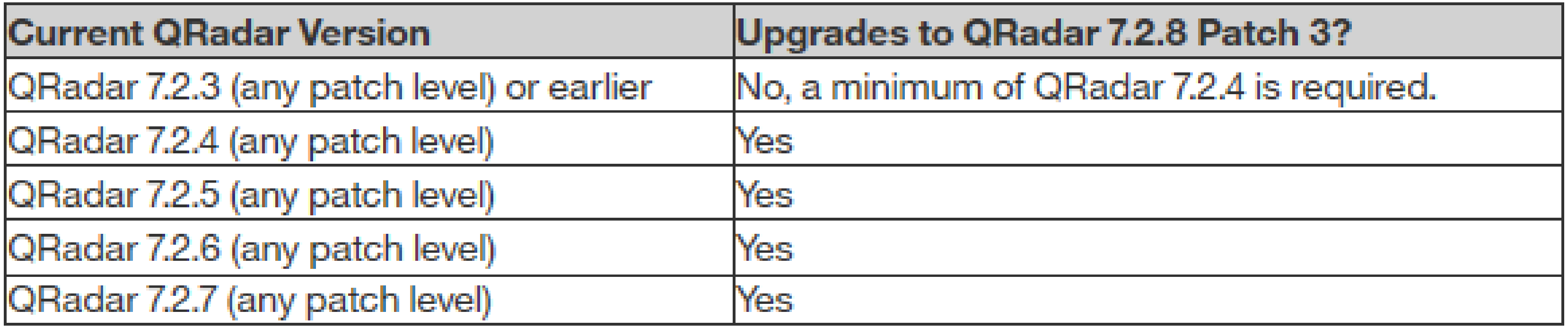
3. **Interim fixes**

   Interim fixes are released as required, but only for the latest software version. For example, if the latest QRadar software version is 7.2.3 Patch 1, then the interim fix 01 can only be applied to 7.2.3 Patch 1.

Upgrading to QRadar 7.2.8 (any patch level)

The 7.2.8 Patch 3 fix pack can upgrade QRadar 7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for QRadar.

What is the baseline version to get to QRadar 7.2.8?
QRadar 7.2.4 is the minimum version to be able to upgrade to QRadar 7.2.8 (any patch level).



Current QRadar Version	Upgrades to QRadar 7.2.8 Patch 3?
QRadar 7.2.3 (any patch level) or earlier	No, a minimum of QRadar 7.2.4 is required.
QRadar 7.2.4 (any patch level)	Yes
QRadar 7.2.5 (any patch level)	Yes
QRadar 7.2.6 (any patch level)	Yes
QRadar 7.2.7 (any patch level)	Yes

Let’s talk about updating QRadar deployments

There are two methods of upgrading a deployment:

1. Using an SFS file and selecting the “All” option.

   The “All” option installs the patch to the Console, then updates each appliance in the network one at a time.

   - Pros: Systems are only patched one at a time, easy method to update a deployment.

   - Cons: Large deployments can take time to update, not knowing when a specific host is patched.

2. Install the SFS on the Console, then copy the SFS file to all appliances and install the patch locally.

   - Pros: All hosts after the Console are updated simultaneously, least amount of overall downtime.

   - Cons: More difficult to deploy, no master summary for issues as each system must be verified that the patch completed successfully.

Full Support Article here: **http://ibm.biz/qradarupdate**

Question: Why not launch all installs in parallel?

Patching in parallel, instead of in series like how “Patch all” works right now for managed hosts to speed up installations is being worked on in development.

As a summary of the discussion:

1. **Patch all** - is a fire and forget method of updating an entire deployment, but it is not the fastest method. The Console is patched, then the system walks through patching the deployment in series.

2. **Parallel updates** – is the fastest method of updating a deployment. Administrators of large deployments or regionally separated deployments can manually copy the SFS file to all appliances using SCP. Run the Console installation first and when complete, run installs from the local SFS in parallel on managed hosts to update all other appliances.

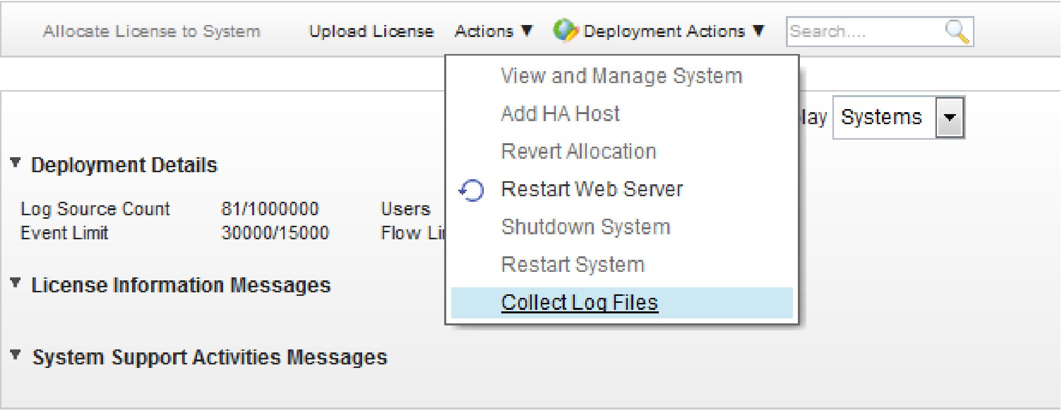
Patches and error messages

When a system is updated, there are 3 possible error messages that can be displayed in the summary.

1. **Success** – The patch was successful and no issues were detected.
2. **Success (with errors)** – The patch installed properly, however, the system detected an issue during the install.
3. **Failed** – The patch failed to install on an appliance. RPM dependency issues can cause a patch to fail.

What to do next:
Anytime you experience a success (w/errors) or failed patch you should contact QRadar Support.

Before opening a ticket, you must run **Collect Log Files** from the System and License Management Screen or from the command line, type:
/opt/qradar/support/get_logs.sh –s



Common questions about QRadar updates

1. **Does the upgrade order matter when I apply a patch to my system?**

   Yes, you must always upgrade the Console first. After the Console is upgraded, the order that patches are applied is no longer a concern.

2. **Is there a minimum amount of disk space required for a patch?**

   As a general rule of thumb, a system should have enough space equivalent to twice the size of the fix pack in the root directory.

   If the system does not have enough disk space to install the fix pack, the appliance is bypassed and a summary details which managed hosts were installed successfully and which were unsuccessful.

3. **How much memory is required to update my software?**

   The QRadar Upgrade Guides cover the memory requirements. The requirements are based off of the the appliance type that you are attempting to upgrade. Administrators who intend to update their deployment should review the memory requirements before they start an upgrade.

QRadar Advisor with Watson Pre-requisites

Configuration Pre-Requisites

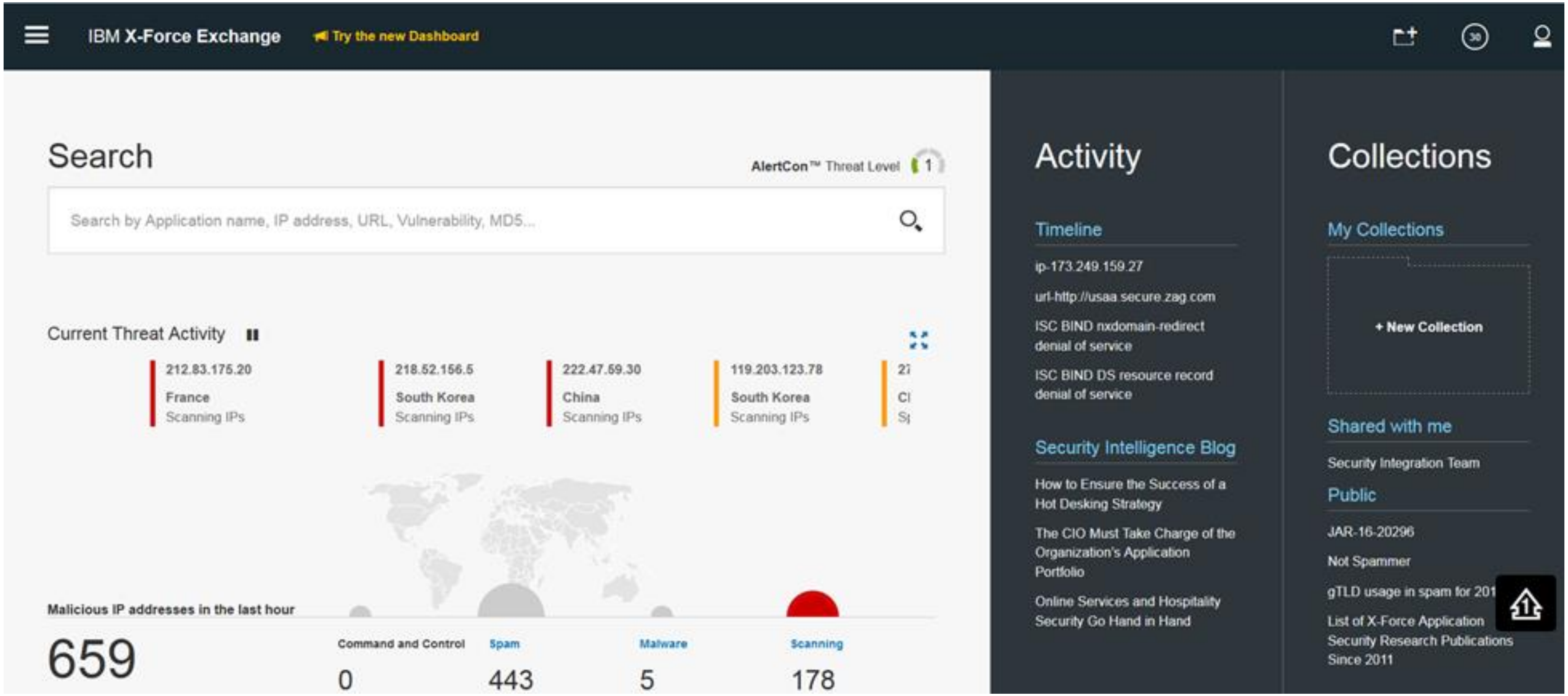
- ❑ QRadar 7.2.8 (any patch level) is required.
- ❑ QRadar Support recommends all QRadar Advisor w/Watson users install QRadar 7.2.8 Patch 4 (coming soon).
- ❑ You must Enable X-Force Threat Intelligence Feed in QRadar 7.2.8 in your QRadar System Settings.
- ❑ You must generate an authorized service token in QRadar for the application.
- ❑ Internet access is required.
- ❑ A secure proxy can be configured (if required)
- ❑ Submit an IBM® X-Force® Exchange authorization key for the QRadar Advisor with Watson app.
- ❑ Create an authorized and limited access service token for the QRadar Advisor with Watson application.
- ❑ Map custom properties from QRadar to the QRadar Advisor with Watson application property names.

QRadar Advisor with Watson: Installation & Configuration

Common questions about QRadar updates

All QRadar apps must be downloaded from the IBM Security App Exchange:

https://exchange.xforce.ibmcloud.com/hub



Search

AlertCon™ Threat Level 1

Search by Application name, IP address, URL, Vulnerability, MD5...

Current Threat Activity

212.83.175.20
France
Scanning IPs

218.52.156.5
South Korea
Scanning IPs

222.47.59.30
China
Scanning IPs

119.203.123.78
South Korea
Scanning IPs

Malicious IP addresses in the last hour

659

Command and Control	Spam	Malware	Scanning
0	443	5	178

Activity

Timeline

ip-173.249.159.27

url-http://usaa.secure.zag.com

ISC BIND nxdomain-redirect denial of service

ISC BIND DS resource record denial of service

Security Intelligence Blog

How to Ensure the Success of a Hot Desking Strategy

The CIO Must Take Charge of the Organization's Application Portfolio

Online Services and Hospitality Security Go Hand in Hand

Collections

My Collections

+ New Collection

Shared with me

Security Integration Team

Public

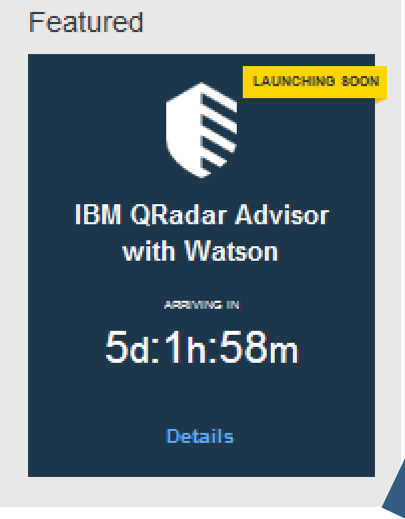
JAR-16-20296

Not Spammer

gTLD usage in spam for 201

List of X-Force Application Security Research Publications Since 2011

Downloading QRadar Advisor with Watson



Featured

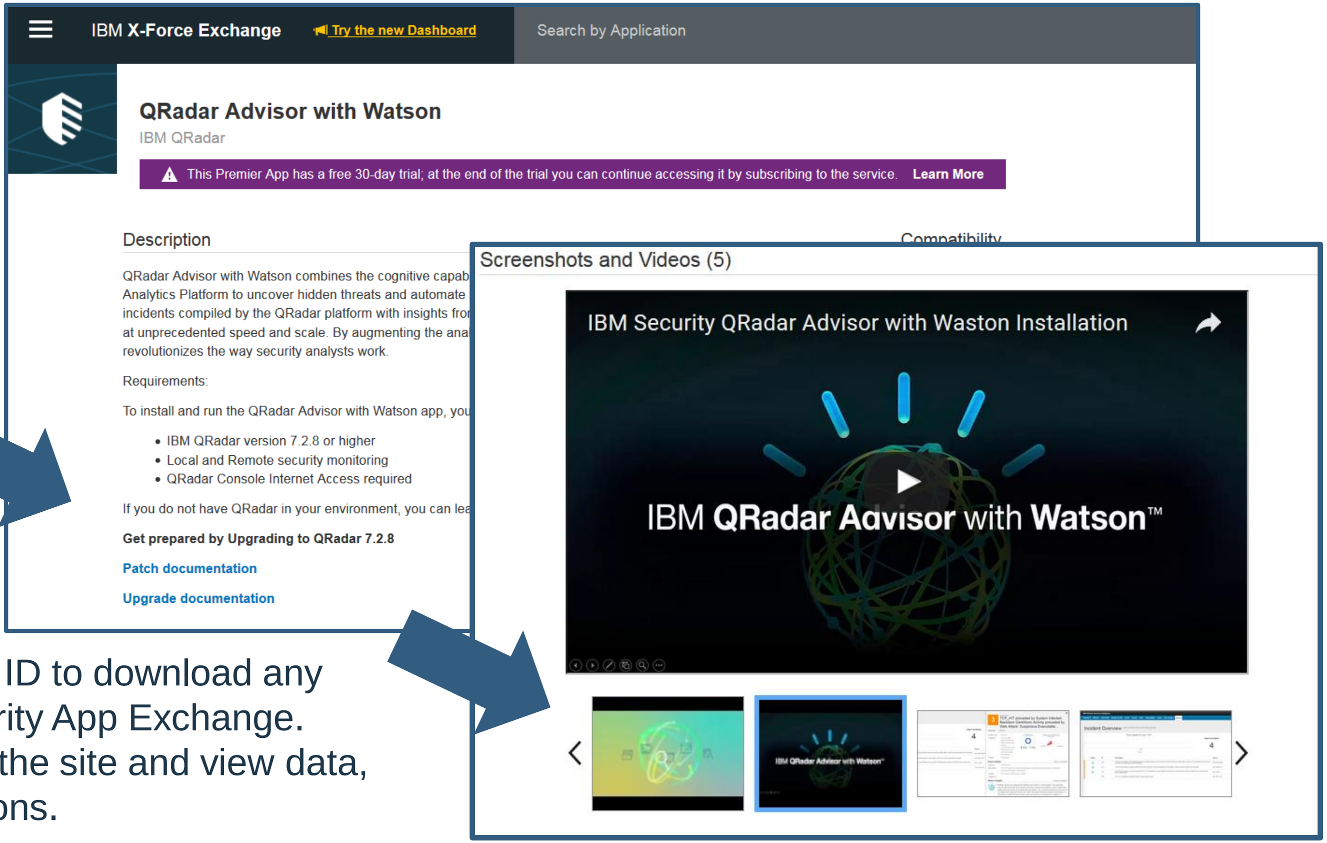
LAUNCHING SOON

IBM QRadar Advisor with Watson

ARRIVING IN

5d:1h:58m

Details



QRadar Advisor with Watson

IBM QRadar

This Premier App has a free 30-day trial; at the end of the trial you can continue accessing it by subscribing to the service. Learn More

Description

QRadar Advisor with Watson combines the cognitive capab
Analytics Platform to uncover hidden threats and automate
incidents compiled by the QRadar platform with insights fro
at unprecedented speed and scale. By augmenting the ana
revolutionizes the way security analysts work.

Requirements:

To install and run the QRadar Advisor with Watson app, you

- IBM QRadar version 7.2.8 or higher
- Local and Remote security monitoring
- QRadar Console Internet Access required

If you do not have QRadar in your environment, you can lea

Get prepared by Upgrading to QRadar 7.2.8

Patch documentation

Upgrade documentation

Compatibility

Screenshots and Videos (5)

IBM Security QRadar Advisor with Waston Installation

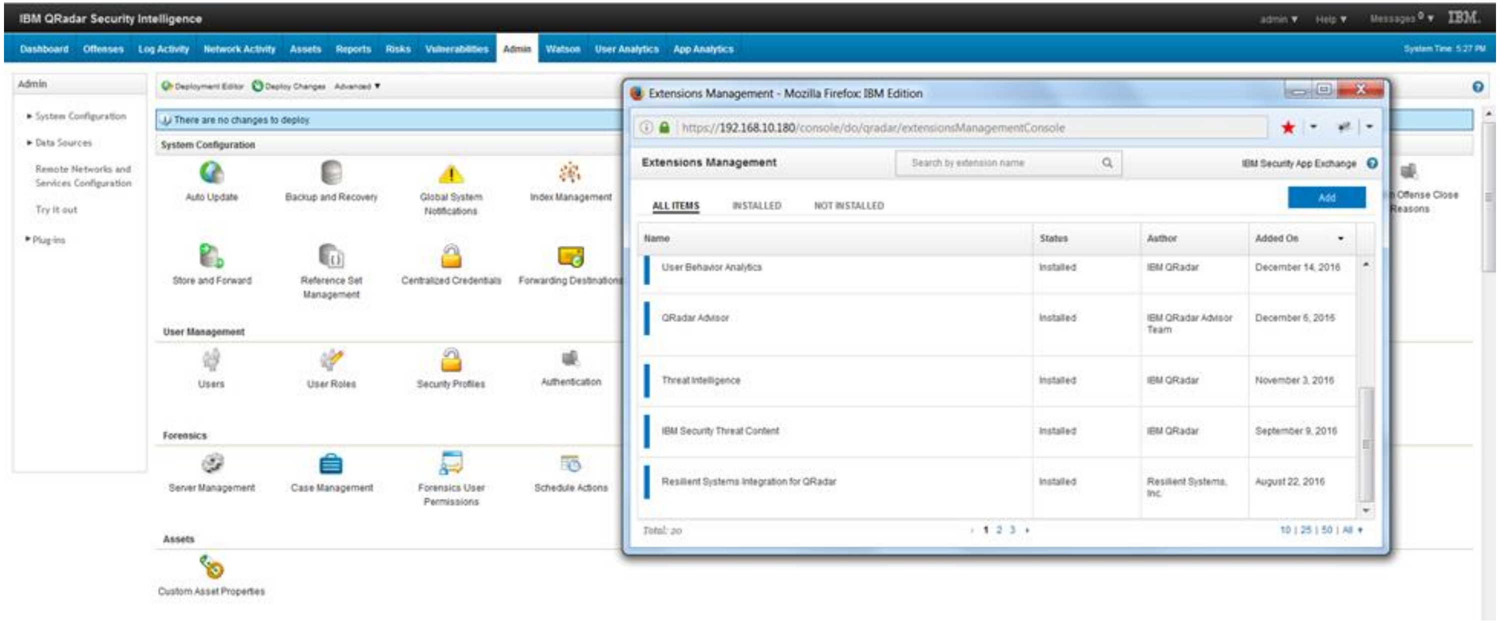
NOTE: You must have an IBM ID to download any application from the IBM Security App Exchange. Guests are allowed to browse the site and view data, but cannot download applications.

Registration for IBM IDs is free.

Installing QRadar Advisor with Watson

The QRadar Advisor with Watson application installs just like any other QRadar application using the Extension Management interface. You must be a QRadar administrator to install any application.

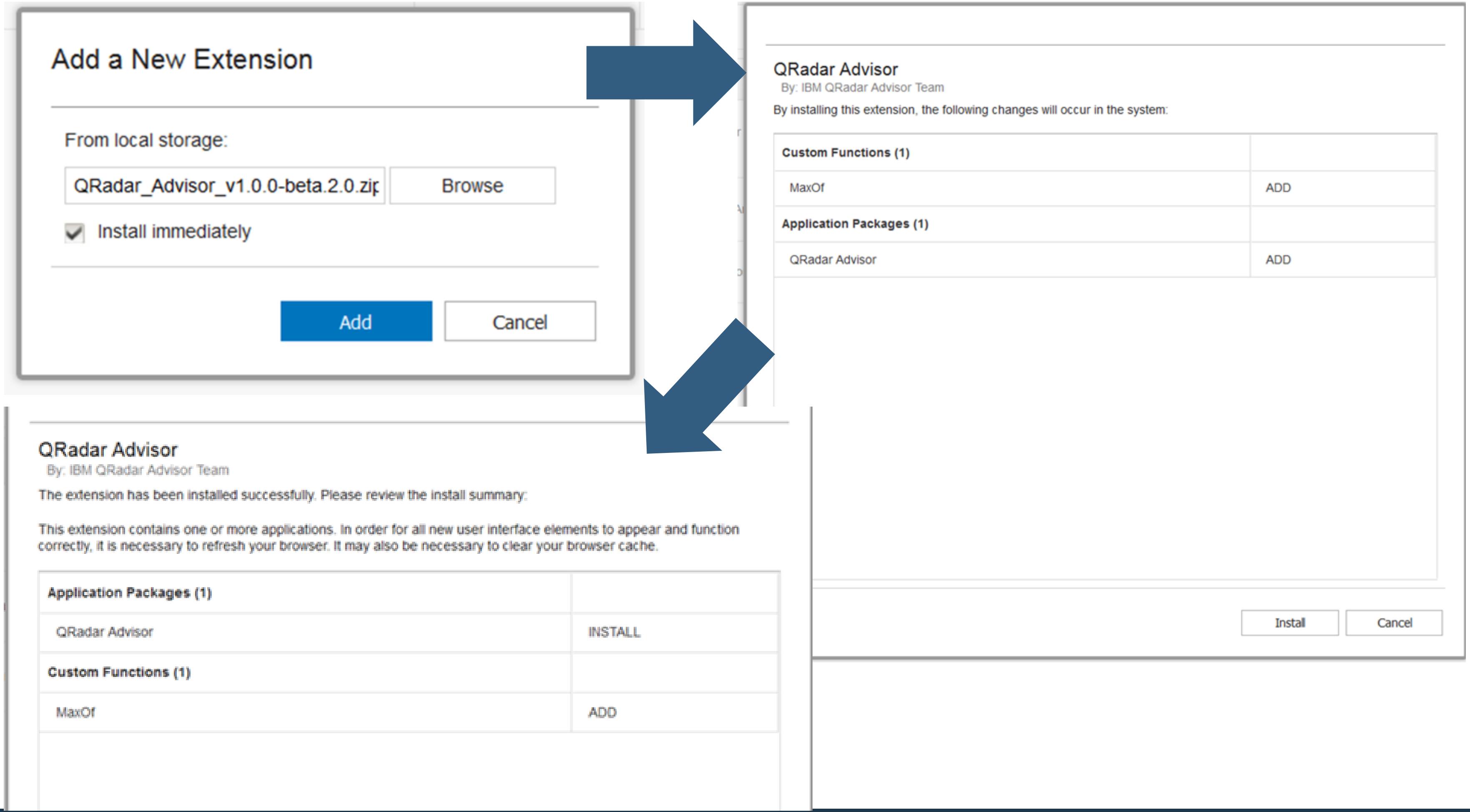
Question: I was part of the QRadar Advisor with Watson beta, how do I proceed when the application is officially released?



Name	Status	Author	Added On
User Behavior Analytics	Installed	IBM QRadar	December 14, 2016
QRadar Advisor	Installed	IBM QRadar Advisor Team	December 6, 2016
Threat Intelligence	Installed	IBM QRadar	November 3, 2016
IBM Security Threat Content	Installed	IBM QRadar	September 9, 2016
Resilient Systems Integration for QRadar	Installed	Resilient Systems, Inc.	August 22, 2016

Total: 20

Installing QRadar Advisor with Watson – Extension Management



Add a New Extension

From local storage:

QRadar_Advisor_v1.0.0-beta.2.0.zip | Browse

☑ Install immediately

Add | Cancel

QRadar Advisor

By: IBM QRadar Advisor Team

By installing this extension, the following changes will occur in the system:

Custom Functions (1)	
MaxOf	ADD
Application Packages (1)	
QRadar Advisor	ADD

Install | Cancel

QRadar Advisor

By: IBM QRadar Advisor Team

The extension has been installed successfully. Please review the install summary:

This extension contains one or more applications. In order for all new user interface elements to appear and function correctly, it is necessary to refresh your browser. It may also be necessary to clear your browser cache.

Application Packages (1)	
QRadar Advisor	INSTALL
Custom Functions (1)	
MaxOf	ADD

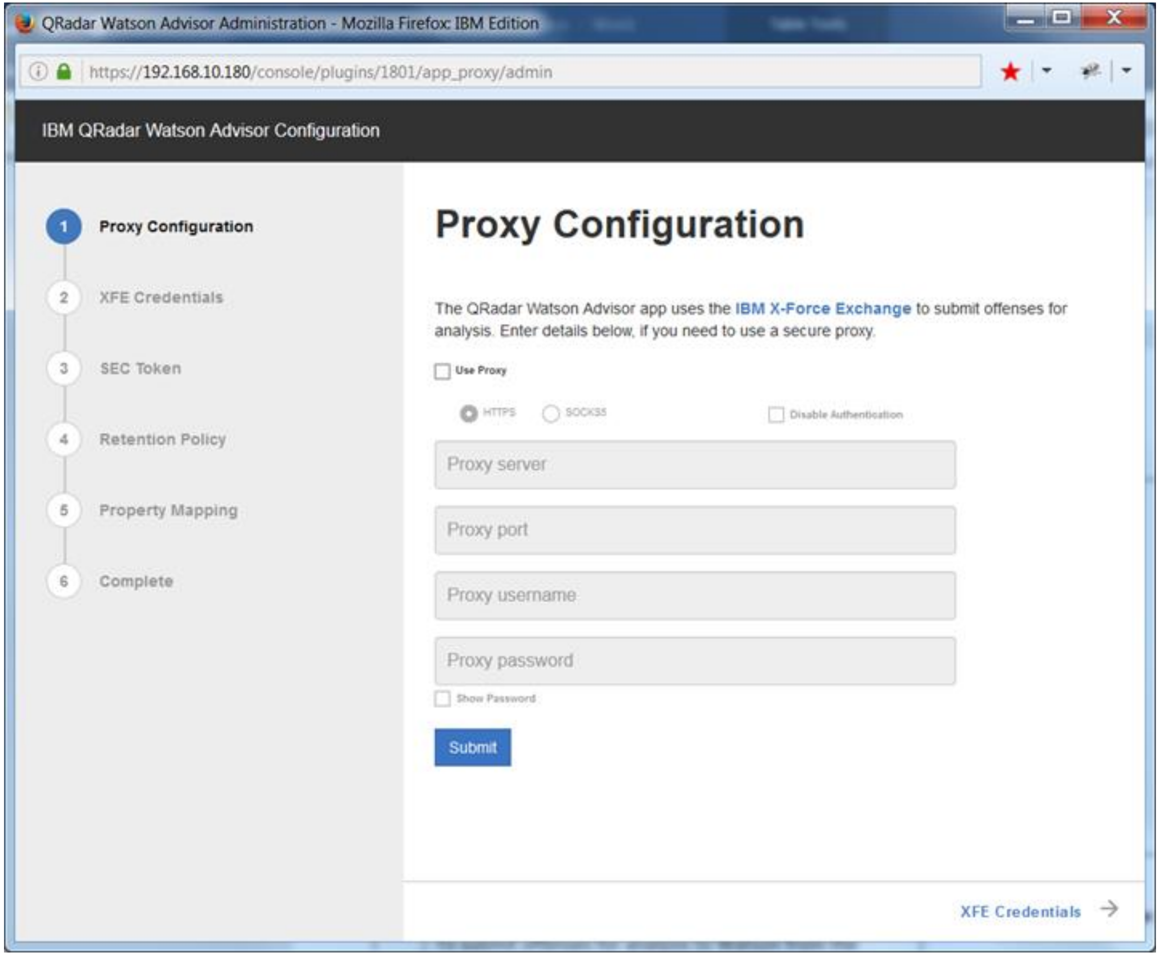
Configuring a Secure Proxy Server

© 2017 IBM Corporation

Installing QRadar Advisor with Watson – Proxy Requirements

During the configuration of the QRadar Advisor with Watson application, administrators will be prompted to enter proxy information.

NOTE: This proxy is built in to the application. You must fill out this proxy information, event if you have proxy information setup in the QRadar Auto Update interface.



QRadar Watson Advisor Administration - Mozilla Firefox: IBM Edition

https://192.168.10.180/console/plugins/1801/app_proxy/admin

IBM QRadar Watson Advisor Configuration

1 Proxy Configuration
2 XFE Credentials
3 SEC Token
4 Retention Policy
5 Property Mapping
6 Complete

Proxy Configuration

The QRadar Watson Advisor app uses the IBM X-Force Exchange to submit offenses for analysis. Enter details below, if you need to use a secure proxy.

□ Use Proxy

● HTTPS ○ SOCKS5 □ Disable Authentication

Proxy server

Proxy port

Proxy username

Proxy password

□ Show Password

Submit

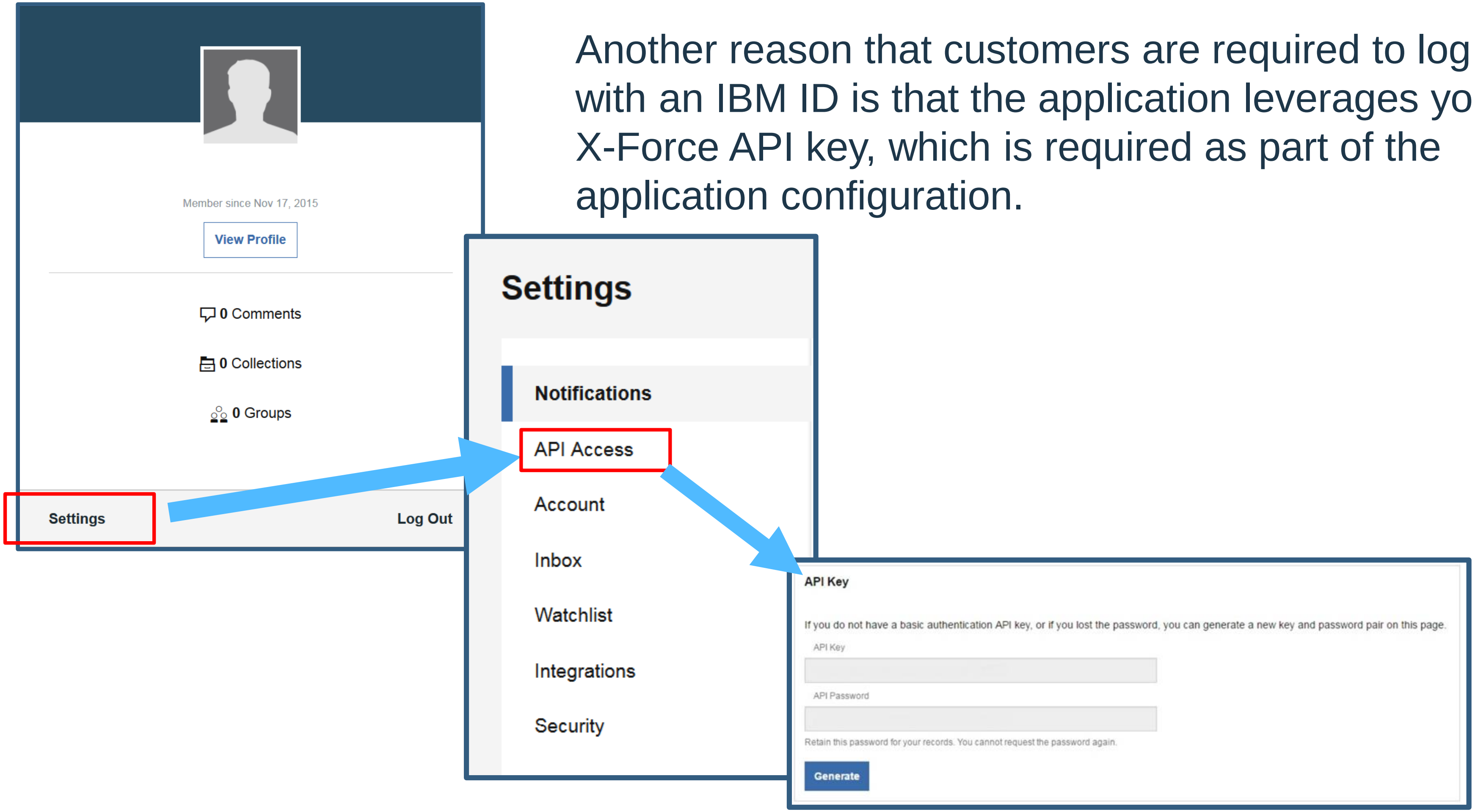
XFE Credentials →

Submitting an authorization Key

© 2017 IBM Corporation

QRadar Advisor with Watson: X-Force API Key

Another reason that customers are required to log in with an IBM ID is that the application leverages your X-Force API key, which is required as part of the application configuration.



API Key

If you do not have a basic authentication API key, or if you lost the password, you can generate a new key and password pair on this page.

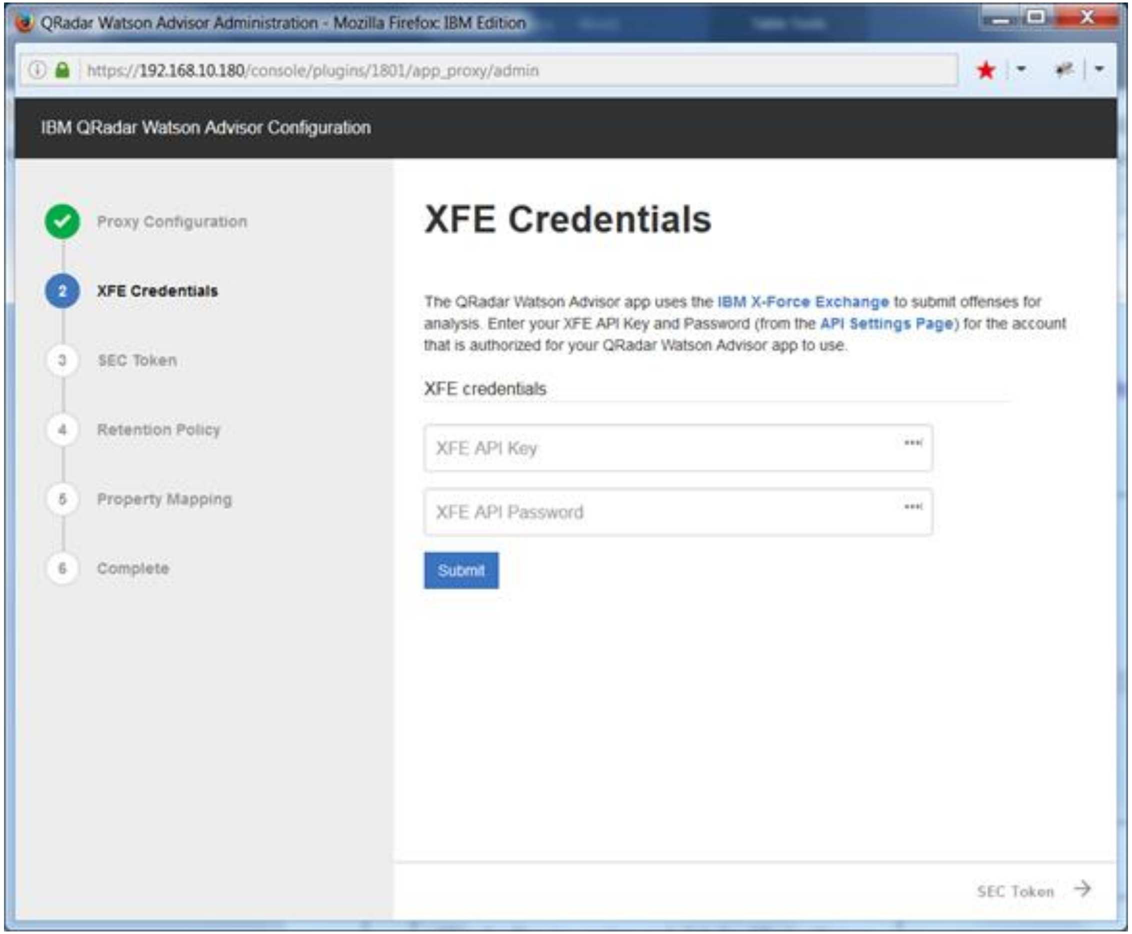
API Key

API Password

Retain this password for your records. You cannot request the password again.

QRadar Advisor with Watson: X-Force Credentials

Specify your X-Force Exchange API credentials to submit offense data for analysis by Watson.



QRadar Watson Advisor Administration - Mozilla Firefox IBM Edition
https://192.168.10.180/console/plugins/1801/app_proxy/admin
IBM QRadar Watson Advisor Configuration
Proxy Configuration
2 XFE Credentials
3 SEC Token
4 Retention Policy
5 Property Mapping
6 Complete

XFE Credentials

The QRadar Watson Advisor app uses the IBM X-Force Exchange to submit offenses for analysis. Enter your XFE API Key and Password (from the API Settings Page) for the account that is authorized for your QRadar Watson Advisor app to use.

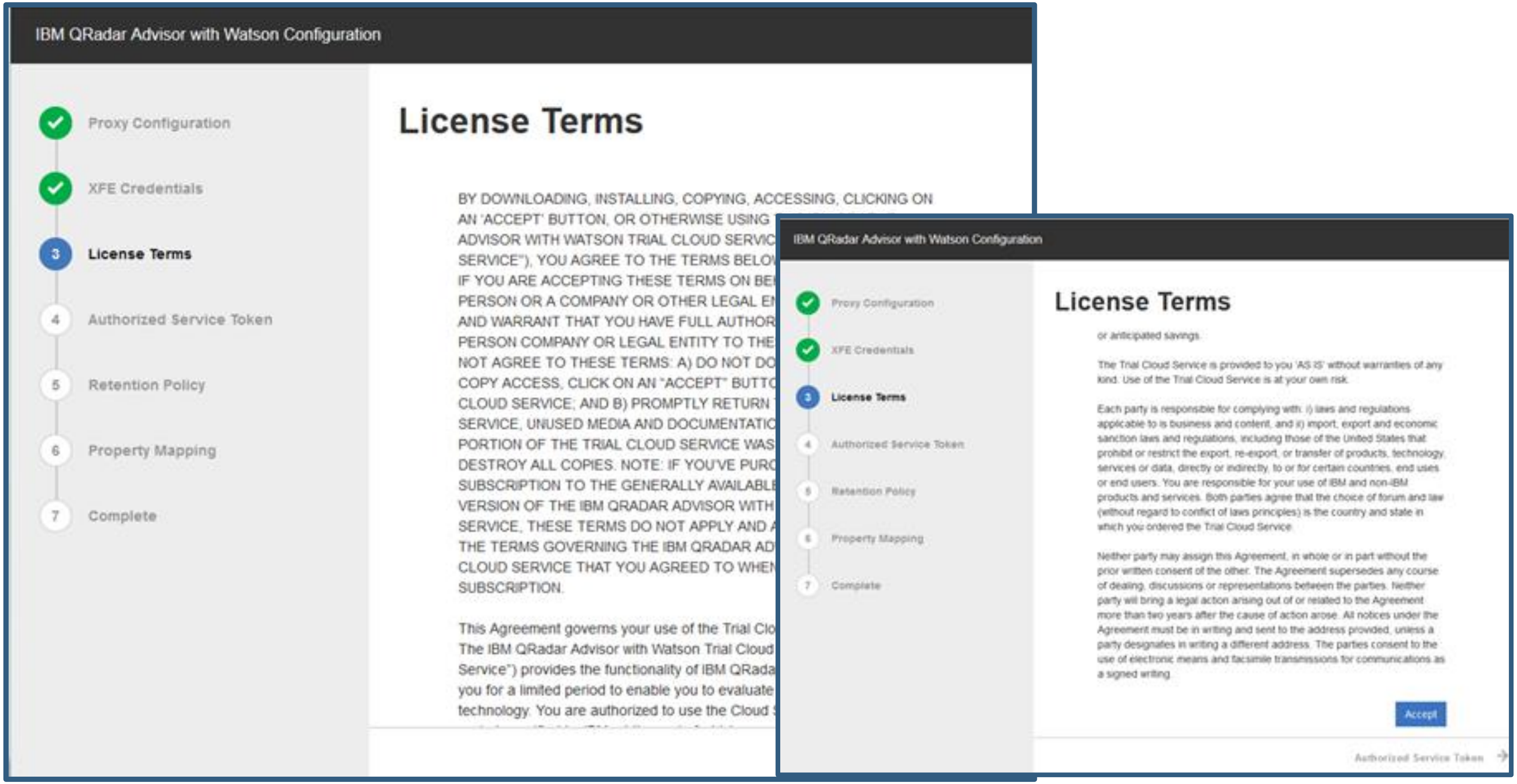
XFE credentials

XFE API Key
XFE API Password
Submit
SEC Token →

License Terms & Agreement

© 2017 IBM Corporation

QRadar Advisor with Watson: License Terms



License Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON
AN 'ACCEPT' BUTTON, OR OTHERWISE USING
ADVISOR WITH WATSON TRIAL CLOUD SERVIC
SERVICE"), YOU AGREE TO THE TERMS BELO
IF YOU ARE ACCEPTING THESE TERMS ON BE
PERSON OR A COMPANY OR OTHER LEGAL E
AND WARRANT THAT YOU HAVE FULL AUTHOR
PERSON COMPANY OR LEGAL ENTITY TO THE
NOT AGREE TO THESE TERMS: A) DO NOT DO
COPY ACCESS, CLICK ON AN "ACCEPT" BUTTO
CLOUD SERVICE; AND B) PROMPTLY RETURN
SERVICE, UNUSED MEDIA AND DOCUMENTATIO
PORTION OF THE TRIAL CLOUD SERVICE WAS
DESTROY ALL COPIES. NOTE: IF YOU'VE PURC
SUBSCRIPTION TO THE GENERALLY AVAILABLE
VERSION OF THE IBM QRADAR ADVISOR WITH
SERVICE, THESE TERMS DO NOT APPLY AND A
THE TERMS GOVERNING THE IBM QRADAR AD
CLOUD SERVICE THAT YOU AGREED TO WHEN
SUBSCRIPTION.

This Agreement governs your use of the Trial Clo
The IBM QRadar Advisor with Watson Trial Cloud
Service") provides the functionality of IBM QRada
you for a limited period to enable you to evaluate
technology. You are authorized to use the Cloud

License Terms

or anticipated savings.

The Trial Cloud Service is provided to you 'AS IS' without warranties of any kind. Use of the Trial Cloud Service is at your own risk.

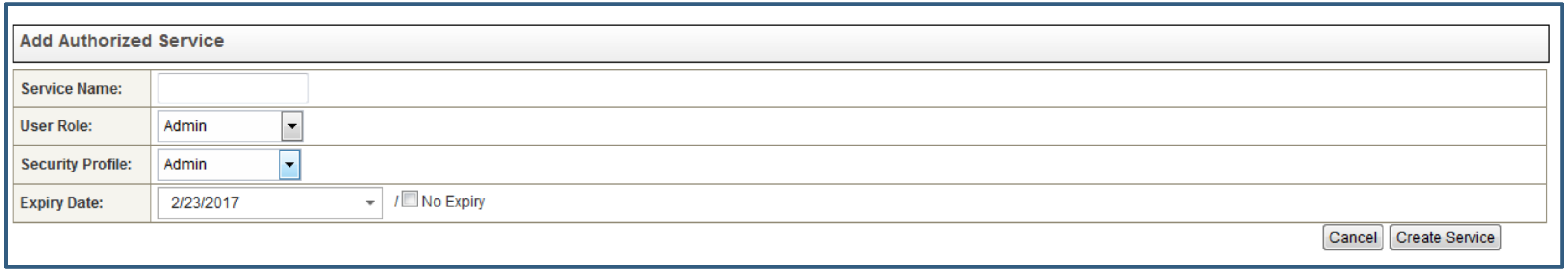
Each party is responsible for complying with: i) laws and regulations applicable to is business and content, and ii) import, export and economic sanction laws and regulations, including those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. You are responsible for your use of IBM and non-IBM products and services. Both parties agree that the choice of forum and law (without regard to conflict of laws principles) is the country and state in which you ordered the Trial Cloud Service.

Neither party may assign this Agreement, in whole or in part without the prior written consent of the other. The Agreement supersedes any course of dealing, discussions or representations between the parties. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose. All notices under the Agreement must be in writing and sent to the address provided, unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing.

Create a Security Token

© 2017 IBM Corporation

QRadar Advisor with Watson: Authorized Service Token



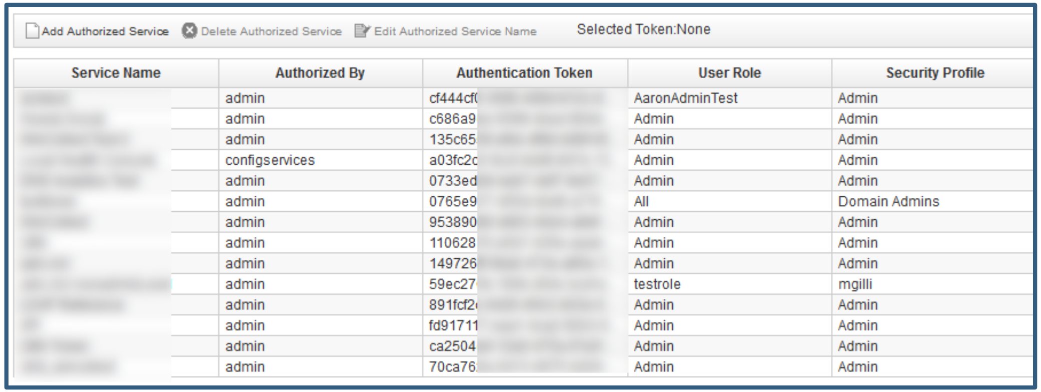
Add Authorized Service

Service Name:	
User Role:	Admin
Security Profile:	Admin
Expiry Date:	2/23/2017 / □ No Expiry

An administrator must create an authorized service token that includes:

- User Role: Admin
- Security Profile: Admin

A limited authorized service token is also required (next slide)

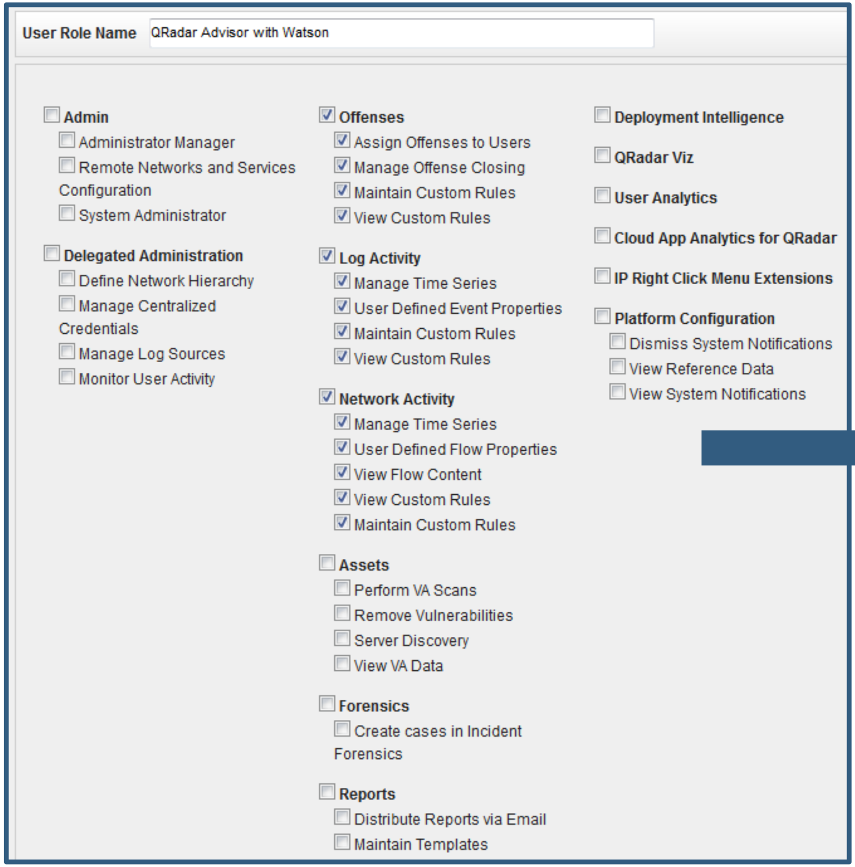


Selected Token:None

Service Name	Authorized By	Authentication Token	User Role	Security Profile
[redacted]	admin	cf444cf[redacted]	AaronAdminTest	Admin
[redacted]	admin	c686a9[redacted]	Admin	Admin
[redacted]	admin	135c65[redacted]	Admin	Admin
[redacted]	configservices	a03fc2c[redacted]	Admin	Admin
[redacted]	admin	0733ed[redacted]	Admin	Admin
[redacted]	admin	0765e9[redacted]	All	Domain Admins
[redacted]	admin	953890[redacted]	Admin	Admin
[redacted]	admin	110628[redacted]	Admin	Admin
[redacted]	admin	149726[redacted]	Admin	Admin
[redacted]	admin	59ec27[redacted]	testrole	mgilli
[redacted]	admin	891fcf2[redacted]	Admin	Admin
[redacted]	admin	fd91711[redacted]	Admin	Admin
[redacted]	admin	ca2504[redacted]	Admin	Admin
[redacted]	admin	70ca76[redacted]	Admin	Admin

NOTE: A QRadar Deploy must take place to ensure the Authorization Token is recognized by the application

QRadar Advisor with Watson: Limited Authorized Service Token



User Role Name: QRadar Advisor with Watson

☐ Admin
- ☐ Administrator Manager
- ☐ Remote Networks and Services Configuration
- ☐ System Administrator

☐ Delegated Administration
- ☐ Define Network Hierarchy
- ☐ Manage Centralized Credentials
- ☐ Manage Log Sources
- ☐ Monitor User Activity

☑ Offenses
- ☑ Assign Offenses to Users
- ☑ Manage Offense Closing
- ☑ Maintain Custom Rules
- ☑ View Custom Rules

☑ Log Activity
- ☑ Manage Time Series
- ☑ User Defined Event Properties
- ☑ Maintain Custom Rules
- ☑ View Custom Rules

☑ Network Activity
- ☑ Manage Time Series
- ☑ User Defined Flow Properties
- ☑ View Flow Content
- ☑ View Custom Rules
- ☑ Maintain Custom Rules

☐ Assets
- ☐ Perform VA Scans
- ☐ Remove Vulnerabilities
- ☐ Server Discovery
- ☐ View VA Data

☐ Forensics
- ☐ Create cases in Incident Forensics

☐ Reports
- ☐ Distribute Reports via Email
- ☐ Maintain Templates

☐ Deployment Intelligence

☐ QRadar Viz

☐ User Analytics

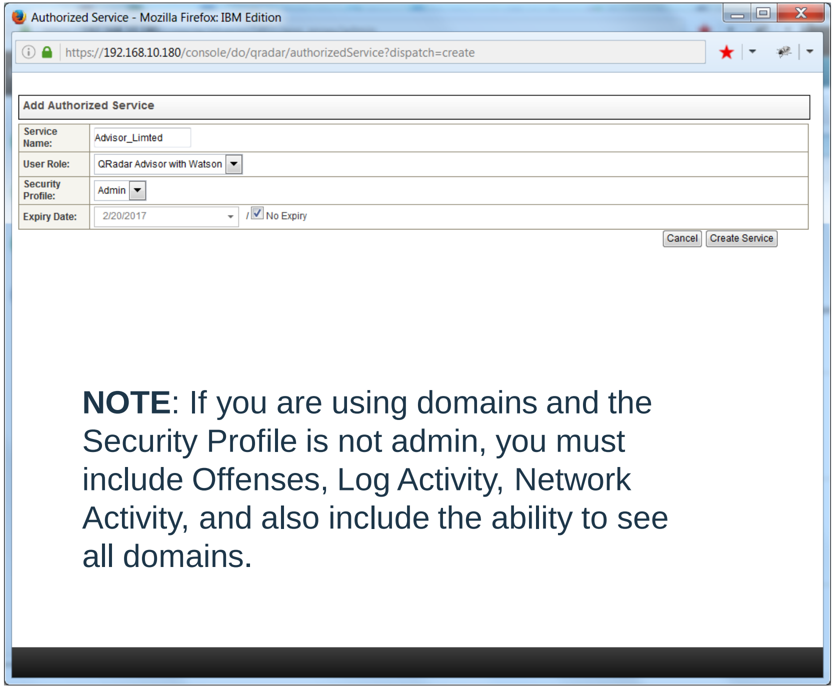
☐ Cloud App Analytics for QRadar

☐ IP Right Click Menu Extensions

☐ Platform Configuration
- ☐ Dismiss System Notifications
- ☐ View Reference Data
- ☐ View System Notifications

A limited authorized service tokens requires:

- **Offenses** (all user options)
- **Log Activity** (all user options)
- **Network Activity** (all user options)



Authorized Service - Mozilla Firefox: IBM Edition

https://192.168.10.180/console/do/qradar/authorizedService?dispatch=create

Add Authorized Service

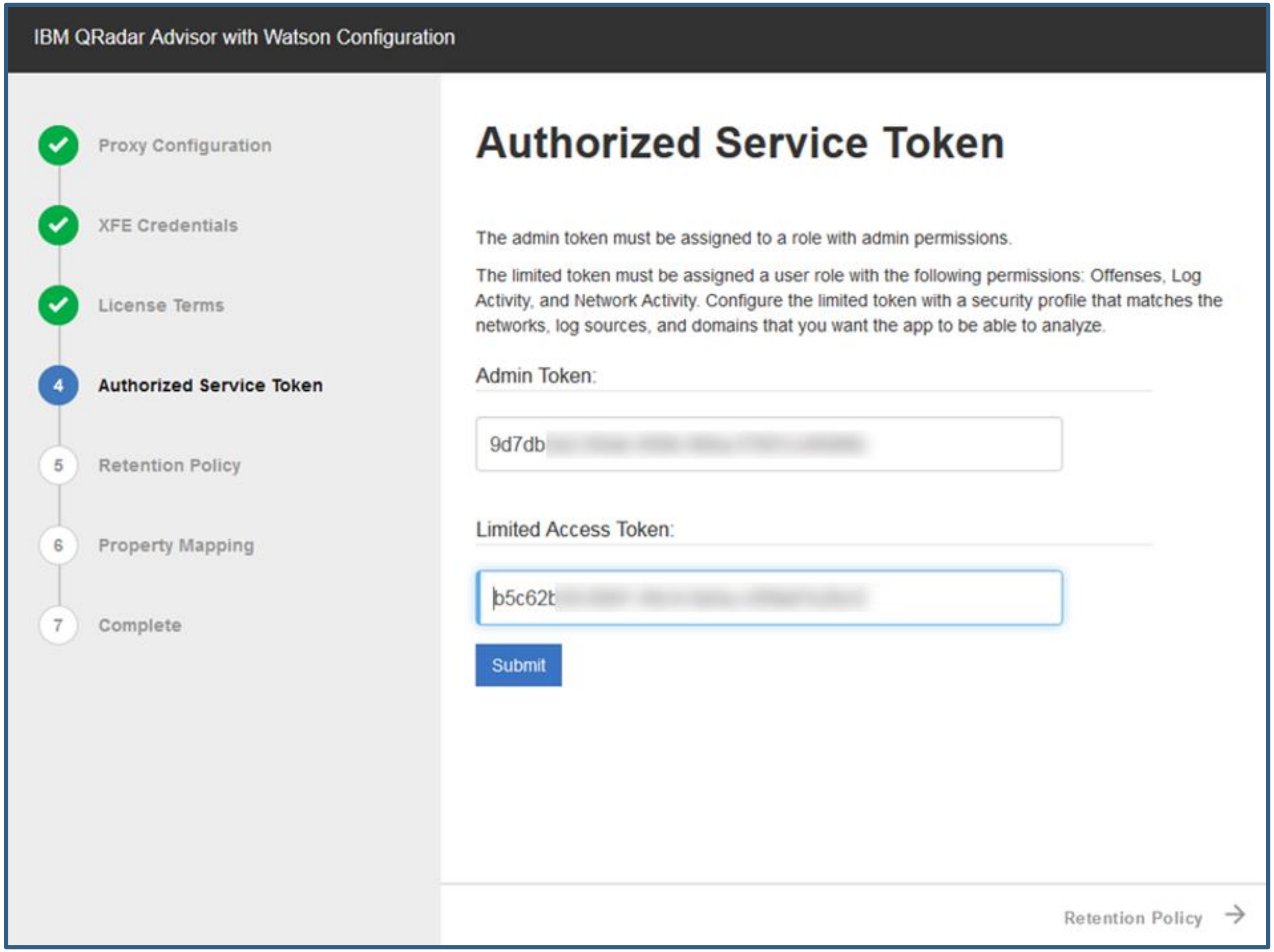
Service Name:	Advisor_Limted
User Role:	QRadar Advisor with Watson ▾
Security Profile:	Admin ▾
Expiry Date:	2/20/2017 ▾ / ☑ No Expiry

NOTE: If you are using domains and the Security Profile is not admin, you must include Offenses, Log Activity, Network Activity, and also include the ability to see all domains.

NOTE: A Deploy Changes is required after a User Role is created.

QRadar Advisor with Watson: Authorized Service Token

Enter both the Admin token and the limited access token in to the QRadar Advisor with Watson configuration screen.



IBM QRadar Advisor with Watson Configuration

Authorized Service Token

The admin token must be assigned to a role with admin permissions.

The limited token must be assigned a user role with the following permissions: Offenses, Log Activity, and Network Activity. Configure the limited token with a security profile that matches the networks, log sources, and domains that you want the app to be able to analyze.

Admin Token: 9d7db[redacted]

Limited Access Token: b5c62b[redacted]

Retention of Analyzed Results

© 2017 IBM Corporation

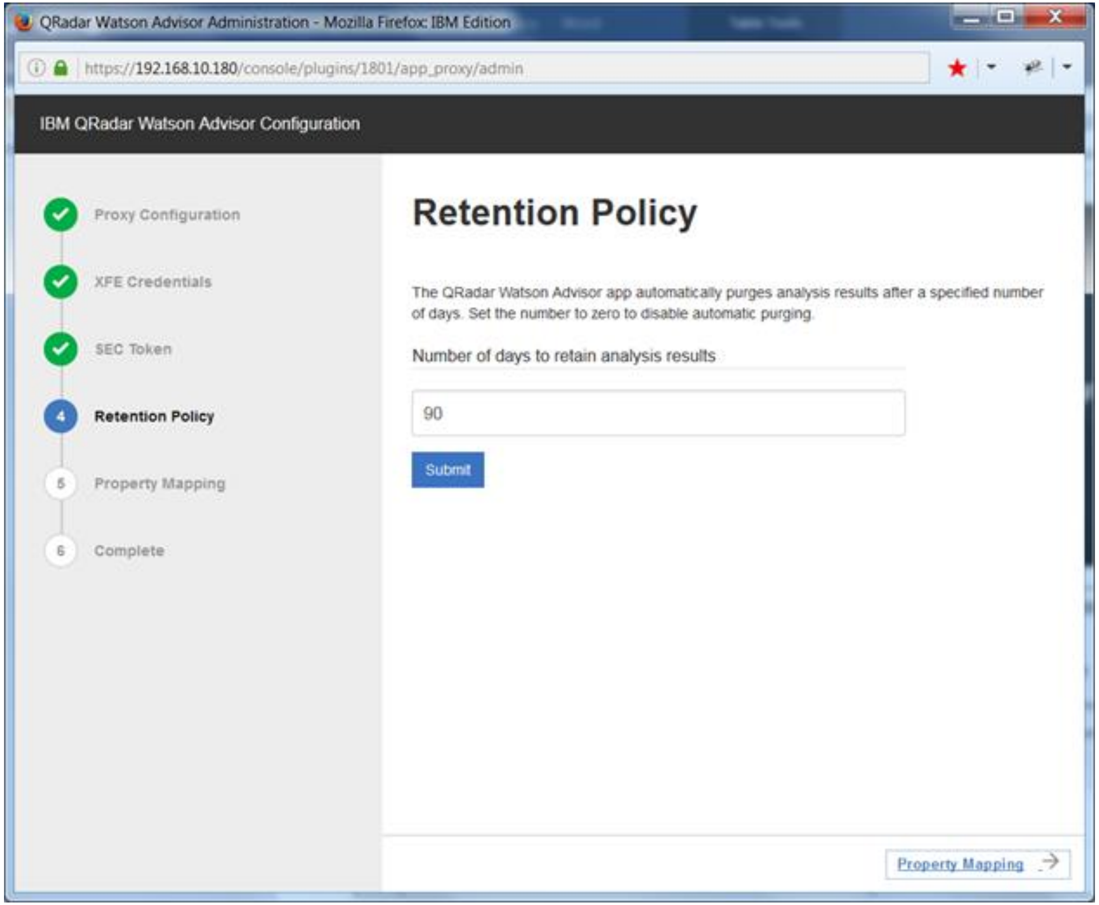
QRadar Advisor with Watson: Data Retention

Administrators have the option to specify how long the analysis data is retained on the XFE / Watson site.

After the number of days specified is reached, analysis data older than this date is automatically purged from the site.

Common questions:

- What else do I need to know about analysis data that is offsite?
- Does IBM use this data for other purposes?



QRadar Watson Advisor Administration - Mozilla Firefox: IBM Edition
https://192.168.10.180/console/plugins/1801/app_proxy/admin
IBM QRadar Watson Advisor Configuration
Proxy Configuration
XFE Credentials
SEC Token
4 Retention Policy
5 Property Mapping
6 Complete

Retention Policy

The QRadar Watson Advisor app automatically purges analysis results after a specified number of days. Set the number to zero to disable automatic purging.

Number of days to retain analysis results: 90

Submit
Property Mapping →

Mapping Custom Properties

© 2017 IBM Corporation

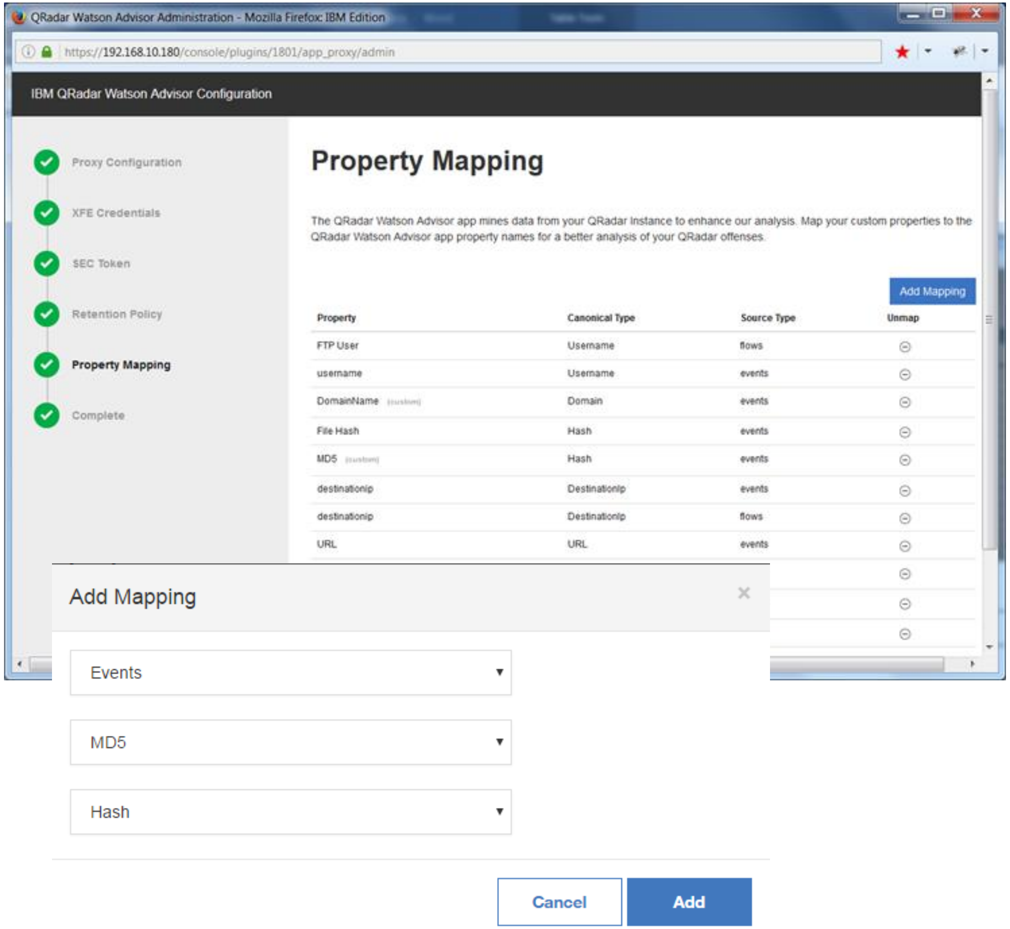
QRadar Advisor with Watson: Data Retention

Administrators must select what custom property and other data they feel is important for analysis should go to Watson.

This allows administrators to specify what data is sent for analysis.

Common question:

What types of data make good candidates for Watson analysis?



QRadar Watson Advisor Administration - Mozilla Firefox: IBM Edition

https://192.168.10.180/console/plugins/1801/app_proxy/admin

IBM QRadar Watson Advisor Configuration

Property Mapping

The QRadar Watson Advisor app mines data from your QRadar Instance to enhance our analysis. Map your custom properties to the QRadar Watson Advisor app property names for a better analysis of your QRadar offenses.

Property	Canonical Type	Source Type	Unmap
FTP User	Username	flows	⊖
username	Username	events	⊖
DomainName (custom)	Domain	events	⊖
File Hash	Hash	events	⊖
MD5 (custom)	Hash	events	⊖
destinationip	DestinationIp	events	⊖
destinationip	DestinationIp	flows	⊖
URL	URL	events	⊖
			⊖
			⊖
			⊖

Add Mapping

Events ▾

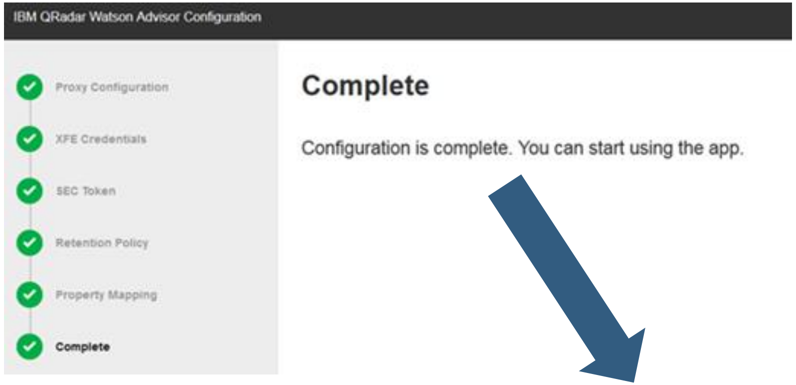
MD5 ▾

Hash ▾

QRadar Advisor with Watson: Configuration is complete!

To send Offenses to Watson for analysis, a new button is added in QRadar to the Offense details screen.

After the QRadar Advisor app is installed, this button will be visible in the user interface.

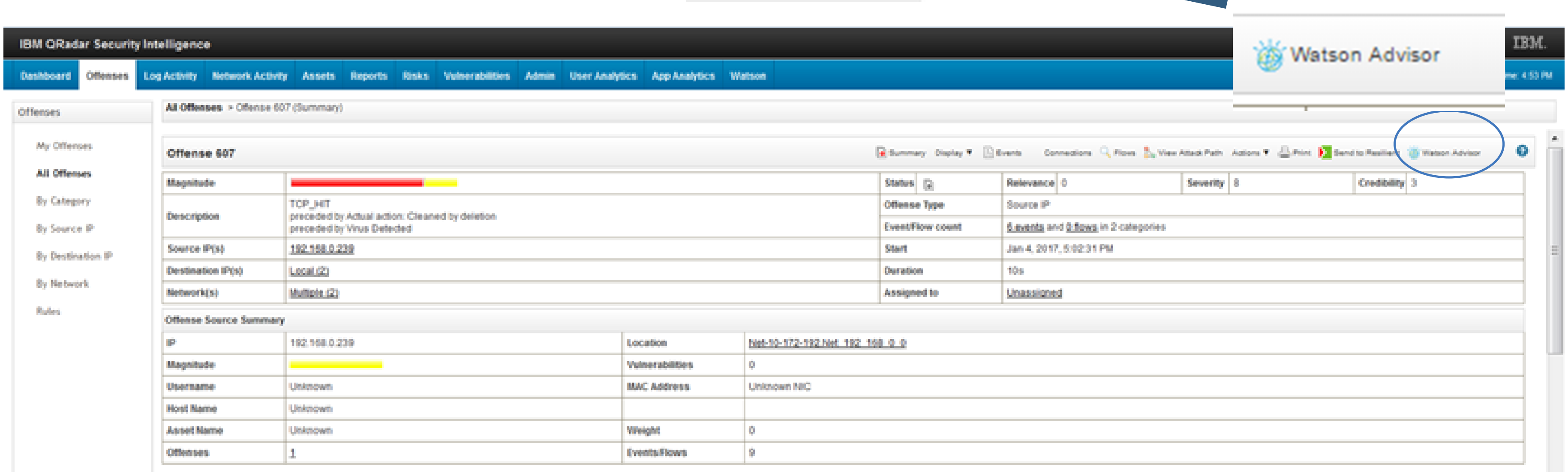


IBM QRadar Watson Advisor Configuration

- ✓ Proxy Configuration
- ✓ XFE Credentials
- ✓ SEC Token
- ✓ Retention Policy
- ✓ Property Mapping
- ✓ Complete

Complete

Configuration is complete. You can start using the app.



All Offenses > Offense 607 (Summary)

Offense 607

Magnitude	🟥🟨	Status	Relevance 0 · Severity 8 · Credibility 3
Description	TCP_HIT preceded by Actual action: Cleaned by deletion preceded by Virus Detected	Offense Type	Source IP
		Event/Flow count	6 events and 0 flows in 2 categories
Source IP(s)	192.158.0.239	Start	Jan 4, 2017, 5:02:31 PM
Destination IP(s)	Local (2)	Duration	10s
Network(s)	Multiple (2)	Assigned to	Unassigned

Offense Source Summary

IP	192.158.0.239	Location	Net-10-172-192.Net_192_168_0_0
Magnitude	🟨	Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	9

QRadar Advisor with Watson: Demonstration

More Information

© 2017 IBM Corporation

QRadar Advisor with Watson: Getting more information

- QRadar Advisor Forums (forum tag = qradar-watson):

  https://developer.ibm.com/answers/topics/qradar-watson.html

- QRadar Advisor Landing Page (QRadar App Developer Center):
  - Documentation
  - Forum links
  - Troubleshooting information
  - Videos
  - and more…

  https://developer.ibm.com/qradar/advisor (Coming very soon!)

- QRadar Support: http://ibm.biz/qradarsupport

  (Installation troubleshooting. General QRadar Advisor questions should go to the forums for all support, development, and other users to see)

IBM Security

THANK YOU

FOLLOW US ON:

https://www.facebook.com/IBMSecuritySupport

QRadar Forums: https://ibm.biz/qradarforums

youtube/user/ibmsecuritysupport

@askibmsecurity

securityintelligence.com

xforce.ibmcloud.com

© Copyright IBM Corporation 2016. 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®