How To Setup Manual QRadar Weekly Auto Update

IBM Federal Sales Engineering

By: Christian L. Reyes

Date: April 5, 2024

Updated:

Table of Contents

DISCLAIMER

IBM QRadar will automatically update the deployment nightly if connected to the internet, retrieving updates, and applying any changes automatically. This how to guide is not for clients whose QRadar is currently pulling automatic updates from IBM. This how to guide is for clients whose systems are in completely air-gapped environments or are unable to retrieve automatic updates. Examples of such environments are SCIF's and other highly sensitive areas where the organization has deemed the risk of being connected to the public internet too great and has instead opted to remove internet connection. Ensuring that the clients QRadar deployment stays up to date is of critical importance. These weekly updates provide updates to DSMs for enhanced parsing, configuration updates which help to eliminate false positives and protects the deployment from the latest malicious sites, botnets, and other suspicious activity. Below is a description of all the information which updates provide to the client. Below is also the IBM link to the official explanation if desired.

Update files can include the following updates:

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

IBM QRadar Automatic Updates: https://www.ibm.com/docs/en/qsip/7.5?topic=tasks-automatic-updates

Prerequisites

Prior to working with the client on this engagement, ensure that you have addressed the client's data transfer procedures and policies. This is critical as ensuring the Data Transfer Agent (DTA) is aware of their role within this engagement. If the DTA is unaware this will cause delays in the ability to complete this task.
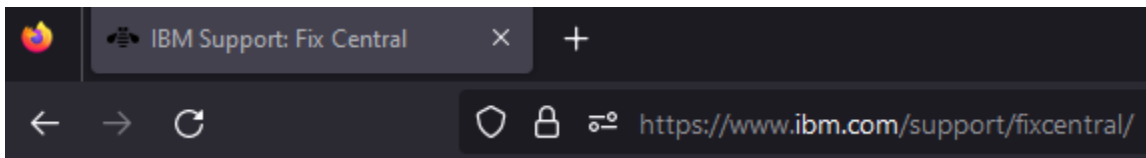
Obtaining QRadar Auto Update from Fix Central

1. Open desired browser; ex: Firefox, Chrome, etc..

2. Enter the following URL within the browser URL Address bar, as shown:

    https://www.ibm.com/support/fixcentral/

3. Scroll down on the page to the "Product selector" section, as shown.

Documentation ⌄   Forums   Cases ⌄   Monitoring ⌄   Manage support account ⌄

Notice

ⓘ Fix Central maintenance is scheduled for **Mon, 31 July 2023, at 14:00 GMT (10am ET)** and should last less than **one hour**. Note: IBM i **Virtual image orders using Download Director** must be resumed prior to this maintenance window or they will need to be reordered once complete. We apologize for any inconvenience.

Fix Central provides fixes and updates for your system's software, hardware, and operating system. Not looking for fixes or updates? Please visit Passport Advantage to download most purchased software products, or My Entitled Systems Support to download system software.

For additional information, click on the following link.
📋 Getting started with Fix Central

Find product	Select product

Type the product name to access a list of product choices.

When using the keyboard to navigate the page, use the **Tab** or **down arrow** keys to navigate the results list.

Product selector*

`<Start typing your product name>` ❯

4. Within the "Product selector" window, type qradar and select the "IBM Security QRadar SIEM", as shown.

5. After selecting the "IBM Security QRadar SIEM", you will be brought to the following selectors. Modify the below selections as shown:

- Installed Version: 7.5.0
- Platform: Linux
- Click Continue

Find product

Type the product name to access a list of product choices.

When using the keyboard to navigate the page, use the **Tab** or **down arrow** keys to navigate the results list.

Product selector*

IBM Security QRadar SIEM 〉

Installed Version*

7.5.0 ⌄

Platform*

Linux ⌄

Continue

6. The following "Identify Fixes" page will appear. Click Continue as shown.

Identify fixes

IBM Security, IBM Security QRadar SIEM (7.5.0, Linux)

Search for fixes for your specific product, type, and platform or search for a fix by ID.

● Browse for fixes	Browse for all fixes for your specific product, release, and platform.
○ APAR or SPR	Search for fixes by entering one or more APAR or SPR numbers each separated by a comma. (e.g. PK10998).
○ Individual fix IDs	Search for updates by entering one or more fix IDs each separated by a comma. (e.g., ibm_fw_aacraid_8kl-5.2.0-15411_linux_32-64).
○ Text	Search for fixes containing all the entered key words, such as problem area, exception, or message ID, in any order.

Additional query options

Continue   Back

7. After clicking "Continue" on the previous page, you will be brought to the "Select fixes" page. Click on "AUTOUPDATE", as shown.

Select fixes
IBM Security, IBM Security QRadar SIEM (7.5.0, Linux)

Continue	Select all	Clear selections		Show fix details	

↓ APPLIANCE FIRMWARE   ↓ DLC   ↓ ISO   ↓ SCRIPT

↓ AUTOUPDATE   ↓ DSM   ↓ PROTOCOL   ↓ UPDATEPACKAGE

↓ CLOUD MARKET PLACE   ↓ INTERIM FIX   ↓ SCANNER   ↓ WINCOLLECT

↓ DataCollector

8. This will automatically bring you to the "AUTOUPDATE" section of the webpage. Look at the "Release date" in the far-right column and ensure to select the latest update, as shown.

AUTOUPDATE

Filter fix details: [_____]

	▲	⬦ Description	⬦ Release date
☐	1	interim fix: → QRADAR-QRAUTO-1712260903 QRadar 7.3, 7.4 and 7.5 Autoupdate	2024/04/04
☐	2	interim fix: → QRADAR-QRAUTO-1707508930 QRadar 7.3, 7.4 and 7.5 Autoupdate	2024/02/09
☐	3	interim fix: → QRADAR-QRAUTO-1705953693 QRadar 7.3, 7.4 and 7.5 Autoupdate	2024/01/22
☐	4	interim fix: → QRADAR-QRAUTO-1701708663 QRadar 7.3, 7.4 and 7.5 Autoupdate	2023/12/04

9. After selecting the latest update, you will be brought to the login page. Have the client login with their IBMid credentials.

IBM

Log in to IBM

IBMid

Press the 1Password icon in your browser's
toolbar to unlock

Continue   →

☐ Remember me   ⓘ

Don't have an account?

Create an IBMid   →

Forgot IBMid? Contact the IBMid help desk

10. After the client successfully logs in, the following download page will appear, as shown.

Download files using HTTPS

IBM Security, IBM Security QRadar SIEM (7.5.0, Linux)

Download files using your web browser

Right-click the download link next to each file and choose 'Save link as' or similar.

Order number:	608146854
Total size:	763.36 MB

Show normalized list | Hide normalized list

interim fix: QRADAR-QRAUTO-1712260903

QRadar 7.3, 7.4 and 7.5 Autoupdate

The following files implement this fix.

⬇ autoupdate-1712260903.tgz (763.36 MB)

⬇ autoupdate-1712260903.tgz.sig (512 bytes)

⬇ wau-readme.04042024.txt (234 bytes)

11. Select the autoupdate .tgz file. Example: autoupdate-1712260903.tgz.

Download files using HTTPS

IBM Security, IBM Security QRadar SIEM (7.5.0, Linux)

Download files using your web browser

Right-click the download link next to each file and choose 'Save link as' or similar.

Order number:	608146854
Total size:	763.36 MB

Show normalized list | Hide normalized list

interim fix: QRADAR-QRAUTO-1712260903

QRadar 7.3, 7.4 and 7.5 Autoupdate

The following files implement this fix.

⤓ autoupdate-1712260903.tgz (763.36 MB)

⤓ autoupdate-1712260903.tgz.sig (512 bytes)

⤓ wau-readme.04042024.txt (234 bytes)

12. This will automatically begin to download. Once completed navigate to the clients' "Downloads" folder and verify the verify has completed.

▢ 📁 autoupdate-1712260903.tgz	4/5/2024 12:39 PM

13. Provide the downloaded autoupdate file to the DTA. Ensure with the client that the file was transferred into the air gapped environment.

Configure Console for Local Auto Update

1. Login to the Console CLI via Putty or other terminal emulator.

2. Enter the IP address of the QRadar Console within the "Host Name (or IP address) field and click Open, as shown.
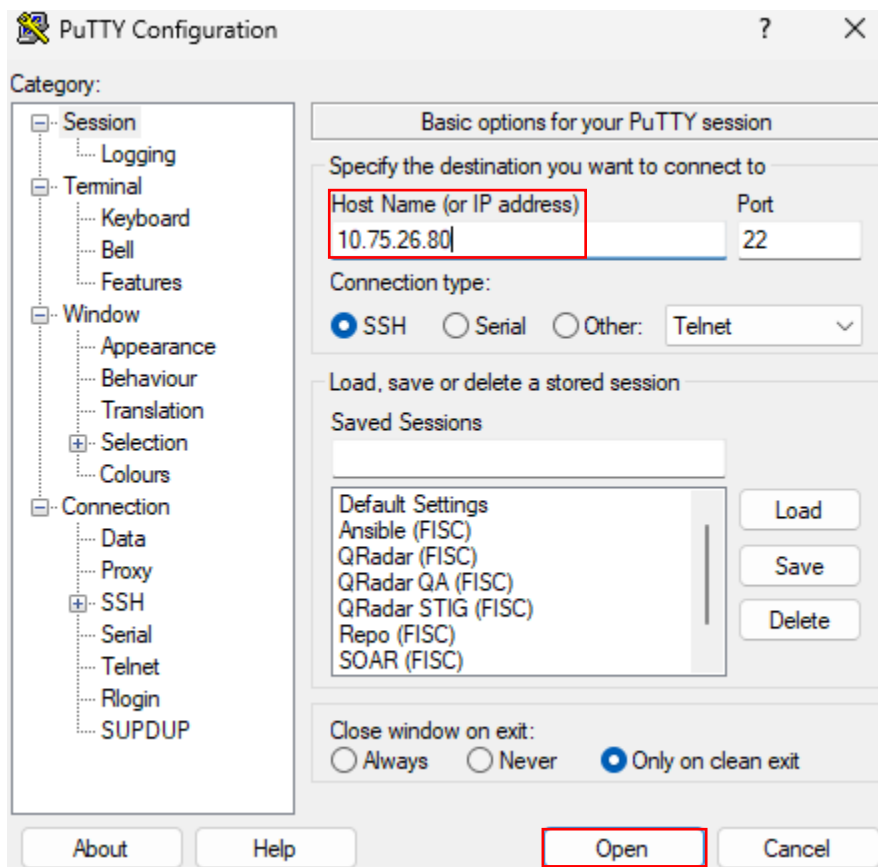
3. Login with the user provided by the client, for demonstration purposes the root user will be used.

4. Verify that the /opt directory has available space, use the following command:

command: df -h

```
[root@qrqacon ~]# df -h
Filesystem                     Size  Used Avail Use% Mounted on
devtmpfs                        32G     0   32G   0% /dev
tmpfs                           32G  792K   32G   1% /dev/shm
tmpfs                           32G  3.2G   29G  10% /run
tmpfs                           32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rootrhel-root       13G  3.4G  9.2G  27% /
/dev/mapper/rootrhel-storetmp   15G   37M   15G   1% /storetmp
/dev/mapper/rootrhel-tmp       3.0G   49M  3.0G   2% /tmp
/dev/sda3                       32G  5.3G   27G  17% /recovery
/dev/mapper/rootrhel-home     1014M   35M  980M   4% /home
/dev/mapper/storerhel-transient 76G   38M   76G   1% /transient
/dev/mapper/storerhel-store    301G   41G  261G  14% /store
/dev/mapper/rootrhel-opt        13G  3.7G  8.9G  29% /opt
/dev/sda2                     1014M  317M  698M  32% /boot
/dev/mapper/rootrhel-var       5.0G  381M  4.7G   8% /var
/dev/mapper/rootrhel-varlog     15G  523M   15G   4% /var/log
/dev/mapper/rootrhel-varlogaudit 3.0G  101M  2.9G   4% /var/log/audit
shm                             63M   20K   63M   1% /store/docker-data/engine/overlay-containers/8694f001503a3650e4b2810
3d20028d1b41c28dedbe74e6fb6efee2f76286797/userdata/shm
overlay                        301G   41G  261G  14% /store/docker-data/engine/overlay/ad2ca61945c3643f742f318ff008148220
f85677697235acea1cf10a96bd9cae/merged
shm                             63M     0   63M   0% /store/docker-data/engine/overlay-containers/1c87e288b82ece106ca39b2
aab68701d50fdd4fda7675b83b8cc00467956c11f/userdata/shm
overlay                        301G   41G  261G  14% /store/docker-data/engine/overlay/c39dea26acdac40deaa2a2e1823c375bb4
236117ce78531664aa4bd3b2a022ae/merged
shm                             63M     0   63M   0% /store/docker-data/engine/overlay-containers/ff43dbd34538b44776986d1
72cd3ed0b83f00d6ea273fbced5119d00837c9934/userdata/shm
overlay                        301G   41G  261G  14% /store/docker-data/engine/overlay/806d2c82f48287b03bd55354c5ee47075d
c52d6e2ea8bad5079a9ae3a21f8f54/merged
tmpfs                          6.3G     0  6.3G   0% /run/user/0
shm                             63M     0   63M   0% /store/docker-data/engine/overlay-containers/eaaaf45ccc1f1f974c33ca8
21532d07cc0ad333cafb0addd2e48fefd45af7f57/userdata/shm
overlay                        301G   41G  261G  14% /store/docker-data/engine/overlay/ff7e6883776a78a9b3e8969a31e82c5832
4afc8485a3804ec5f11ff828b36b54/merged
[root@qrqacon ~]#
```

5. Verify the autoupdates directory is not present within the /opt/qradar/www directory, run the following command:

command: ls /opt/qradar/www

```
[root@qrqacon ~]# ls /opt/qradar/www
favicon.ico  favicon.ico.qrd  forensics  help  help-core  help-core.bak  index.html  qrmhelp
[root@qrqacon ~]#
```

6. If the autoupdates directory is present, then delete it via the following command:

command: rm -rf autoupdates

7. Create the /store/downloads/autoupdates directory, as shown:

command: mkdir -p /store/downloads/autoupdates

```
[root@qrqacon ~]# mkdir -p /store/downloads/autoupdates
[root@qrqacon ~]#
```

8. Create a symbolic between /store/downloads/autoupdates and /opt/qradar/www, via the following command:

Command: ln -s /store/downloads/autoupdates /opt/qradar/www

```
[root@qrqacon ~]# ln -s /store/downloads/autoupdates /opt/qradar/www
[root@qrqacon ~]#
```

9. Verify the contents of the /opt/qradar/www directory via the following command:

command: ll /opt/qradar/www/

```
[root@qrqacon ~]# ll /opt/qradar/www/
total 36
lrwxrwxrwx  1 root root       28 Apr  5 16:33 autoupdates -> /store/downloads/autoupdates
-r-xr-xr-x  1 root root    15086 Mar 27 14:26 favicon.ico
-r-xr-xr-x  1 root root    15086 Mar  2 19:49 favicon.ico.qrd
lrwxrwxrwx  1 root root       23 Mar 21 18:13 forensics -> /opt/ibm/forensics/html
lrwxrwxrwx  1 root root       25 Mar 27 14:30 help -> /opt/qradar/www/help-core
drwxr-xr-x 13 root nobody    119 Jul 21  2021 help-core
drwxr-xr-x 13 root nobody    119 Jul 21  2021 help-core.bak
-r-xr-xr-x  1 root root      103 Mar  2 19:49 index.html
drwxr-xr-x  6 root root      155 Mar 27 14:24 qrmhelp
[root@qrqacon ~]#
```

10. Transfer the autoupdate.tar.gz to the QRadar Console via WinSCP, FileZilla or other file transfer program as shown.
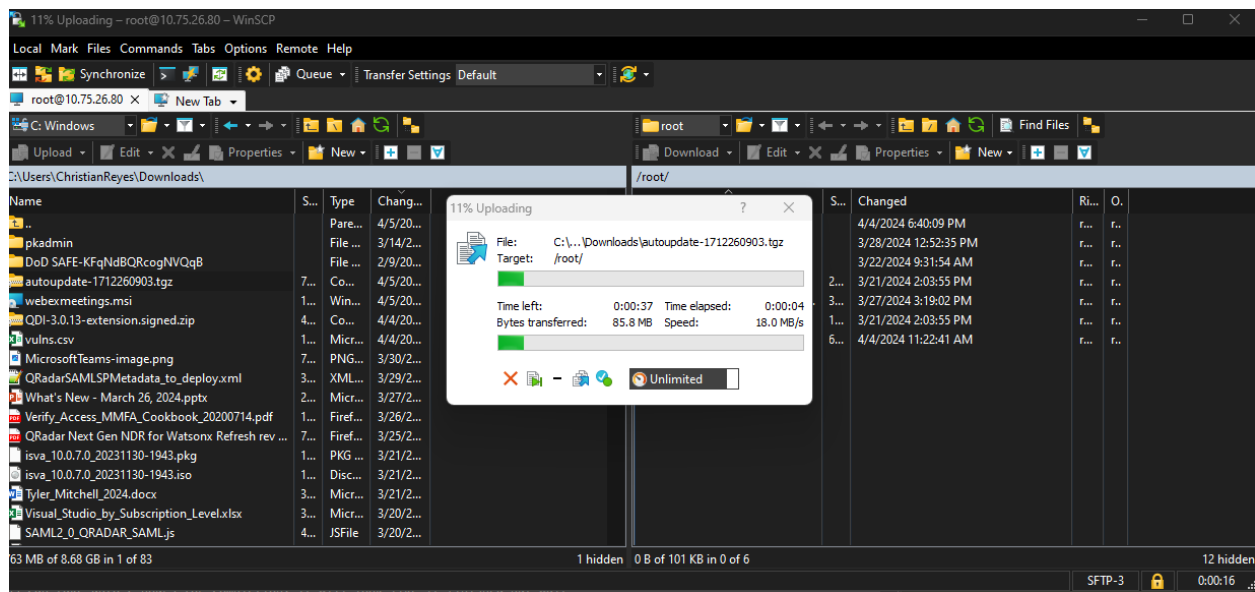
11. Verify the autoupdate.tar.gz successfully transferred via the WinSCP.
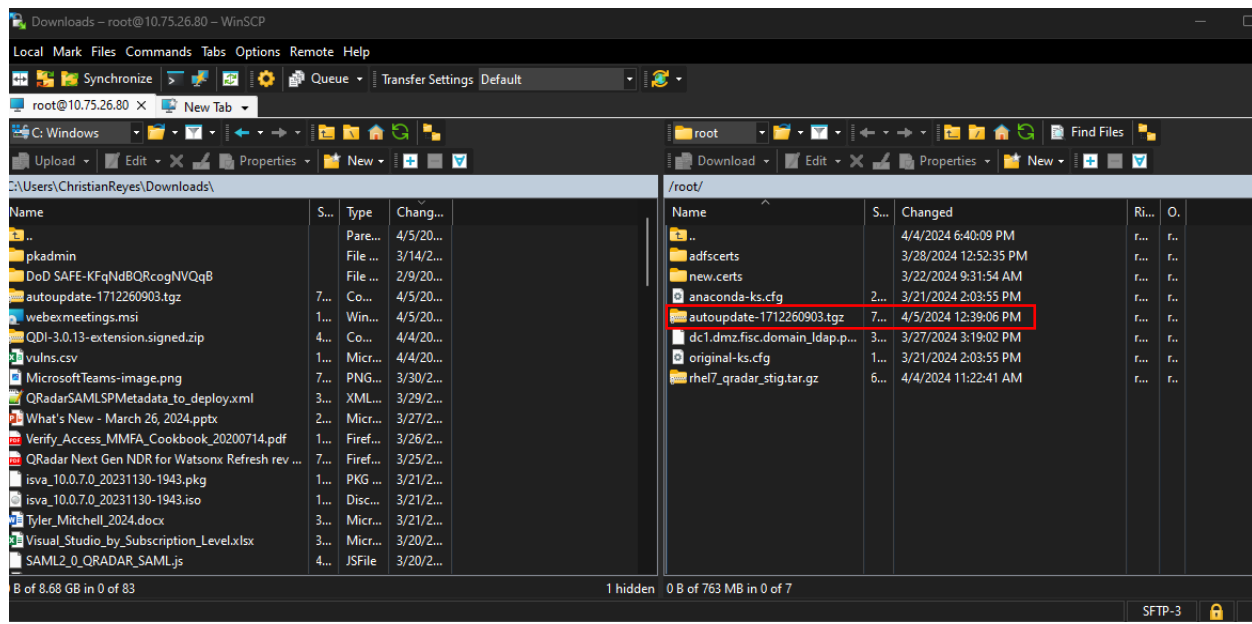
12. Within the QRadar Console CLI ensure that the autoupdate was successfully transferred via the following command:

    command: ls

13. Transfer the autoupdate file to the /opt/qradar/www/autoupdates/ directory, as shown.

    comcmand: cp autoupdate-1712260903.tar.gz /opt/qradar/www/autoupdates/

14. Change directories to /opt/qradar/www/autoupdates/ via the following command:

    command: cd /opt/qradar/www/autoupdates

15. Extract the autoupdate.tgz within the current directory, via the following command:

    command: tar -xvzf autoupdate-1712260903.tgz

16. Verify the .tgz file extracts completely and successfully as shown.

```
wau/qidmap/1710744773445.qidmap-import.xml.gz
wau/qidmap/1710757696180.qidmap-import.xml.gz
wau/qidmap/1710848659387.qidmap-import.xml.gz
wau/qidmap/1710911956768.qidmap-import.xml.gz
wau/qidmap/1710912794281.qidmap-import.xml.gz
wau/qidmap/1710914246954.qidmap-import.xml.gz
wau/qidmap/1710921578012.qidmap-import.xml.gz
wau/qidmap/1710998273552.qidmap-import.xml.gz
wau/qidmap/1711011352286.qidmap-import.xml.gz
wau/qidmap/1711084673062.qidmap-import.xml.gz
wau/qidmap/1711085444437.qidmap-import.xml.gz
wau/qidmap/1711086597475.qidmap-import.xml.gz
wau/qidmap/1711171077753.qidmap-import.xml.gz
wau/qidmap/1711173562440.qidmap-import.xml.gz
wau/qidmap/1711259289649.qidmap-import.xml.gz
wau/qidmap/1711432064639.qidmap-import.xml.gz
wau/qidmap/1711452496510.qidmap-import.xml.gz
wau/qidmap/1711516625602.qidmap-import.xml.gz
wau/qidmap/1711518408256.qidmap-import.xml.gz
wau/qidmap/1711604858064.qidmap-import.xml.gz
wau/qidmap/1711627222882.qidmap-import.xml.gz
wau/qidmap/1711627745169.qidmap-import.xml.gz
wau/qidmap/1711628420725.qidmap-import.xml.gz
wau/qidmap/1711689645507.qidmap-import.xml.gz
wau/qidmap/1711690321156.qidmap-import.xml.gz
wau/qidmap/1711691451363.qidmap-import.xml.gz
wau/qidmap/1711949297883.qidmap-import.xml.gz
wau/qidmap/1712036721819.qidmap-import.xml.gz
wau/qidmap/1712054140499.qidmap-import.xml.gz
wau/qidmap/1712121386369.qidmap-import.xml.gz
wau/qidmap/1712207766876.qidmap-import.xml.gz
wau/qidmap/1712209510666.qidmap-import.xml.gz
wau/qidmap/1712217548822.qidmap-import.xml.gz
wau/qidmap/1712223781909.qidmap-import.xml.gz
wau/wau.manifest.xml
wau/wau.manifest.xml.cosign.sig
wau/wau.manifest.xml.new.sig
[root@qrqacon autoupdates]#
```
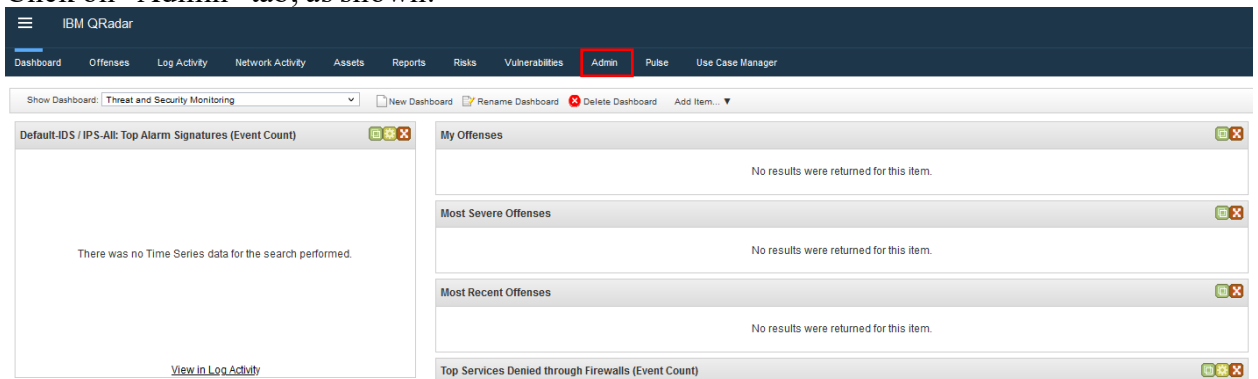
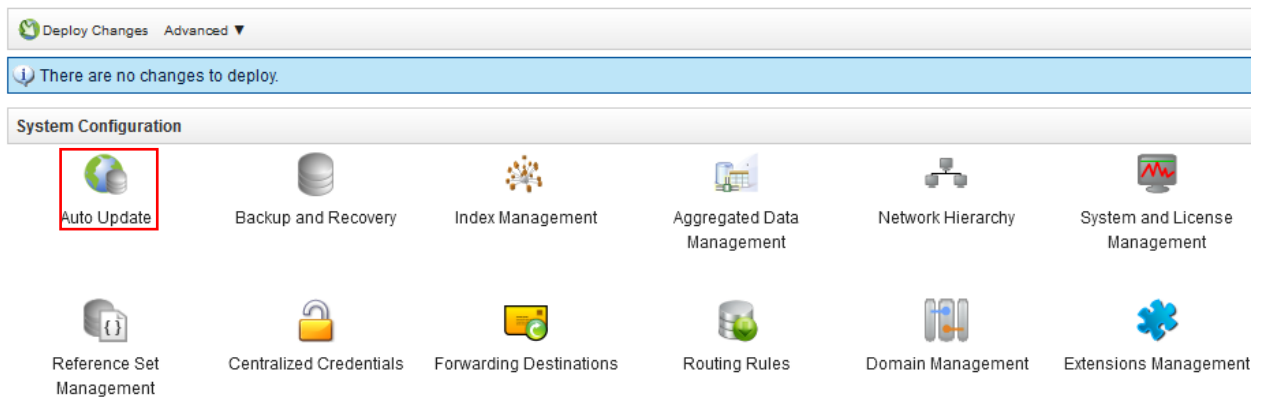# Modification to QRadar Auto Update

1. Login into to QRadar webpage as shown.

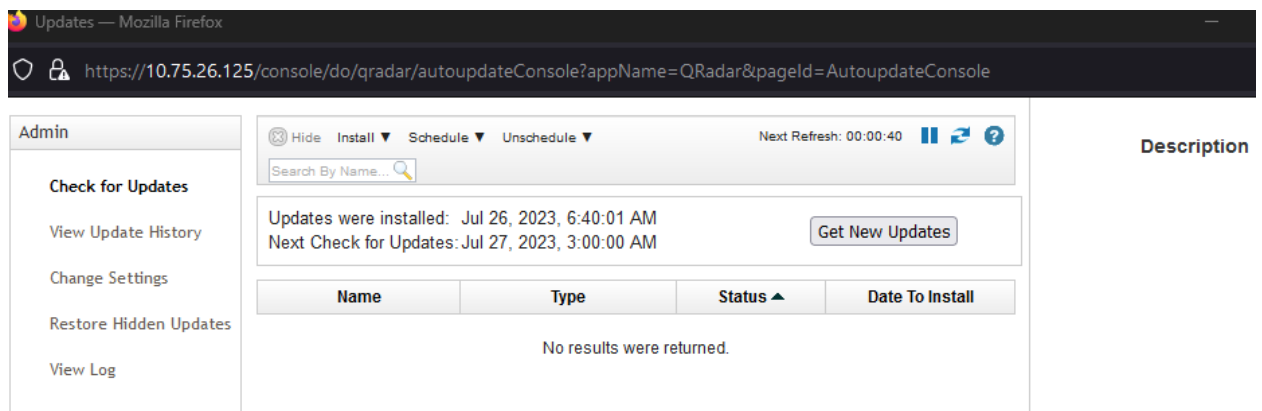2. The default "Dashboard" page will appear, as shown.
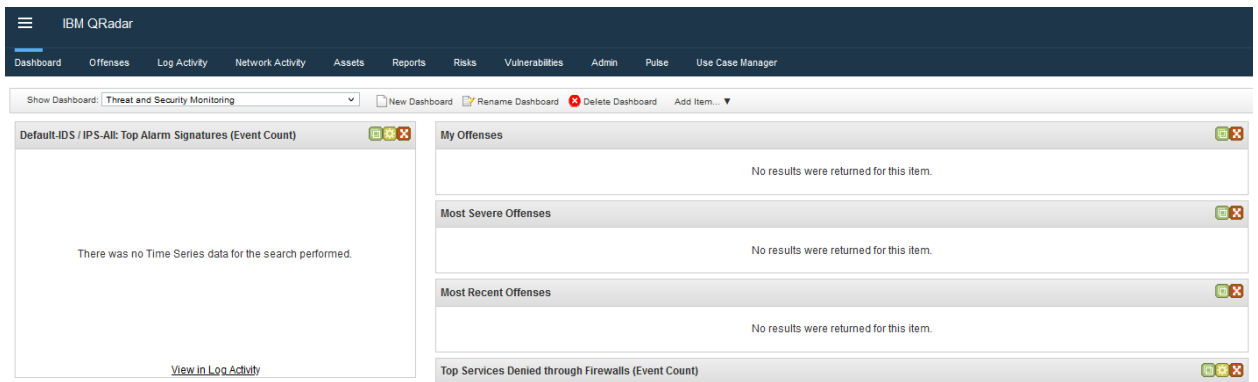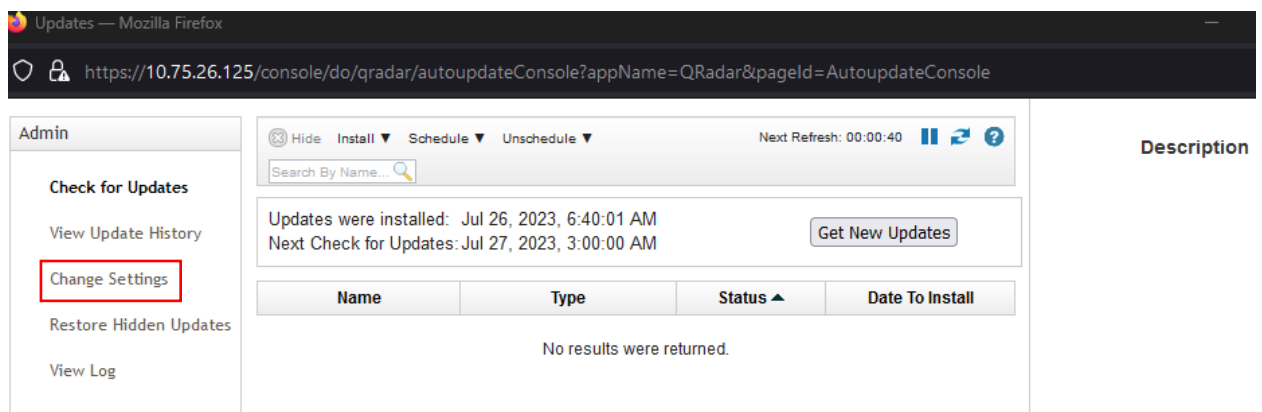

3. Click on "Admin" tab, as shown.

4. Once at the "Admin" page, locate and select the "Auto Update" icon as shown.

5. The following pop-up window will appear.

6. Click on Change Settings.

7. The "Change Settings" window will appear. Click on the "Advanced" tab.

8. The advanced options will appear as shown.

9. Change the Web Server field from the default to the IP address of the QRadar Console, and then click "Save", as shown.

10. The "Application Restart Required" pop-up window will appear as shown. Click "Yes".

Admin

Check for Updates

View Update History

Change Settings

Restore Hidden Updates

View Log

Update Configuration

Basic | Advanced

Server Config

Web Server: https://10.75.26.80/

Directory: autoupdates/

Proxy Server:

Proxy Port:

Proxy Username: test

Proxy Password: ●●●●●●●●

Other Settings

Backup Retention Period(days): 30
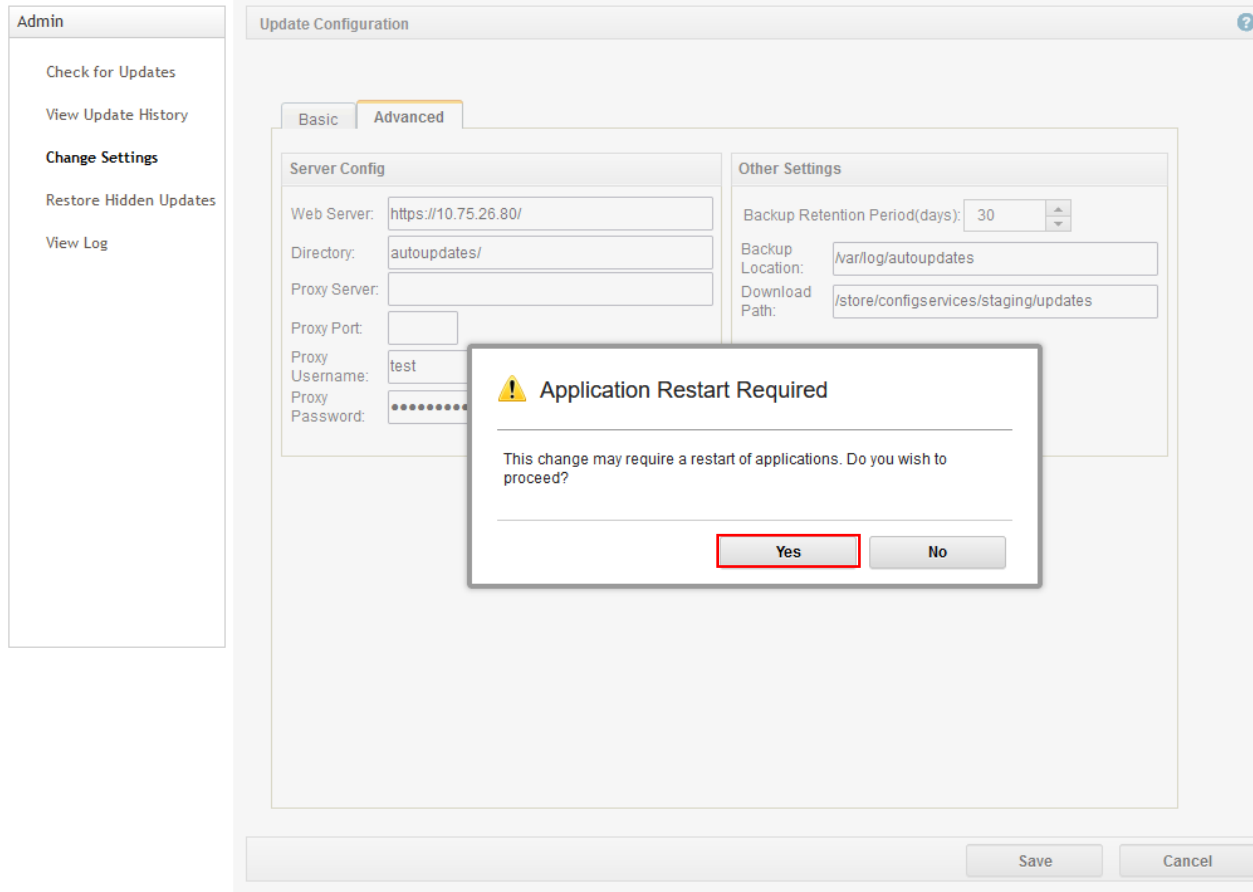
Backup Location: /var/log/autoupdates

Download Path: /store/configservices/staging/updates

⚠ **Application Restart Required**

This change may require a restart of applications. Do you wish to proceed?

Yes | No

Save | Cancel

11. After clicking "Yes", you will be returned to the advanced settings page. There will be the following message shown about Updates failing, as shown. This is not an issue.

12. On the Admin panel click "Check for Updates" and then click "Get New Updates", as shown.

13. You will receive a pop-up windows asking you to confirm you want to run the new updates verses waiting on the scheduled time, click "OK" as shown.
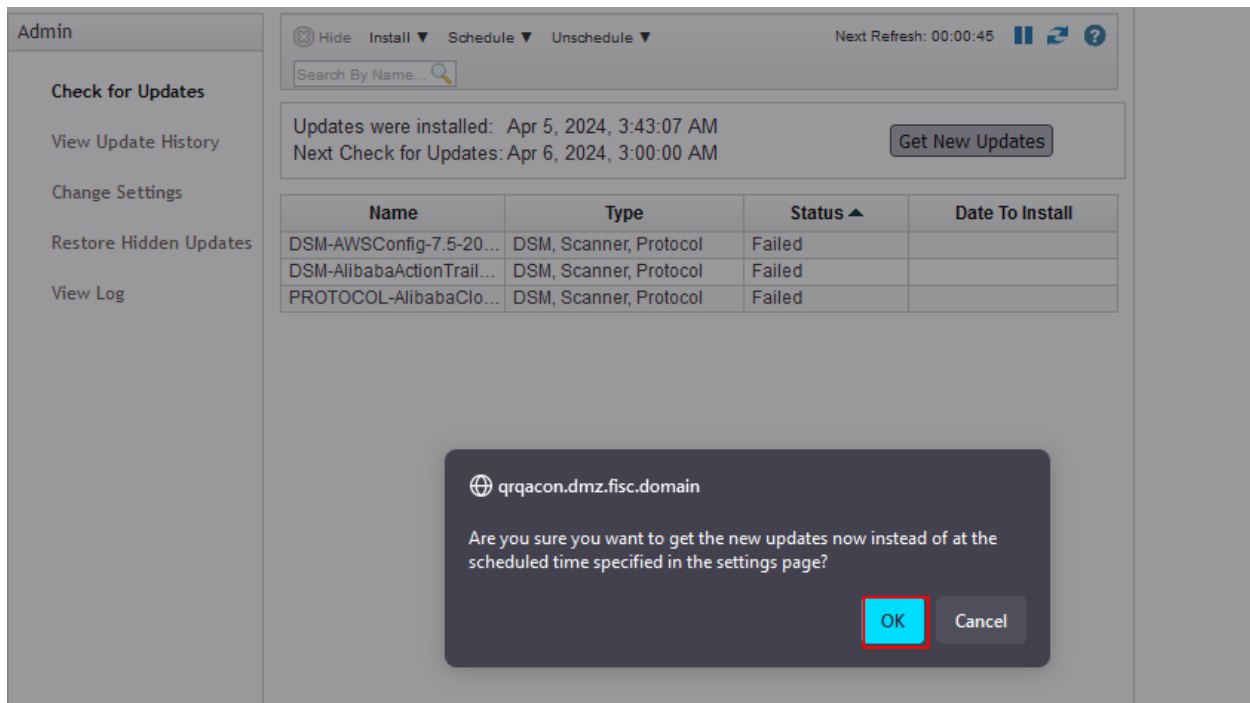
14. This will return you back to the "Check for Updates" screen as shown. The updates will start as indicted by the banner message.
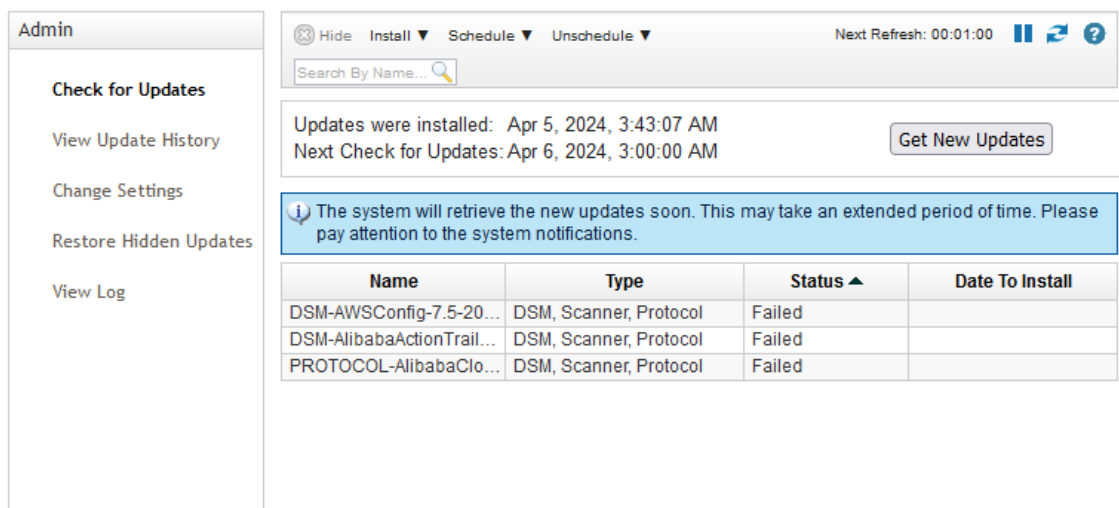
15. Return to the QRadar Console CLI and enter the following command and watch the output. Verify the Auto Updates complete successfully as shown.

Command: tail -f /var/log/qradar.log | grep -i update*

```
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: PERL: Attempting to retrieve https://qrqacon.dmz.fisc.domain/autoupdates/scripts/AUS
cripts.tgz.new.sig?version=7.5.0%20UpdatePackage%208&iv=2021.6.8.20240302192142&customer=IBM%20Corp.&lastau=1712260903&lastpatch=1712260903&vendo
r=Q1%20Labs -- scripts/AUScripts.tgz.new.sig
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Attempting to retrieve https://qrqacon.dmz.fisc.domain/autoupdates/scripts/AUScripts
.tgz.new.sig?version=7.5.0%20UpdatePackage%208&iv=2021.6.8.20240302192142&customer=IBM%20Corp.&lastau=1712260903&lastpatch=1712260903&vendor=Q1%2
0Labs
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Response ------------   1
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Downloading "au-cert-chain.pem" and placing in "/store/autoupdates/".
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: PERL: Attempting to retrieve https://qrqacon.dmz.fisc.domain/autoupdates/au-cert-cha
in.pem?version=7.5.0%20UpdatePackage%208&iv=2021.6.8.20240302192142&customer=IBM%20Corp.&lastau=1712260903&lastpatch=1712260903&vendor=Q1%20Labs
-- au-cert-chain.pem
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Attempting to retrieve https://qrqacon.dmz.fisc.domain/autoupdates/au-cert-chain.pem
?version=7.5.0%20UpdatePackage%208&iv=2021.6.8.20240302192142&customer=IBM%20Corp.&lastau=1712260903&lastpatch=1712260903&vendor=Q1%20Labs
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Response ------------   1
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_cert subject was verified
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_intermediate subject was verified
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_cert subject was verified
Apr  5 17:32:03 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_intermediate subject was verified
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Version: 9.18
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Supplied Version: 9.18
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Manifest type is DAU
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Latest DAU is already installed with serial 1712260903 from 04/04/2024 at 20:01.
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_cert subject was verified
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_intermediate subject was verified
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Version: 9.18
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Supplied Version: 9.18
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Manifest type is Patches
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Latest patches are already installed with serial 1712260903 from 04/04/2024 at 20:01
.
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_cert subject was verified
Apr  5 17:32:04 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: /tmp/au_intermediate subject was verified
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Version: 9.18
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Supplied Version: 9.18
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Manifest type is WAU
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Latest WAU is already installed with serial 1712260903 from 04/04/2024 at 20:01.
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Status: 6
Apr  5 17:32:05 qrqacon.dmz.fisc.domain AUTOUPDATE[3573105]: Auto updates has completed installing.
```

16. Finally, return to the Auto Update window, click on View Log and verify that the update completed successfully as shown.

Admin	Autoupdate Log
Check for Updates	
View Update History	
Change Settings	Last update status: **All updates completed successfully.**
Restore Hidden Updates	Latest DAU is already installed with serial 1712260903 from 04/04/2024 at 20:01. Latest patches are already installed with serial 1712260903 from 04/04/2024 at 20:01. Latest WAU is already installed with serial 1712260903 from 04/04/2024 at 20:01.
View Log	