UPGRADING TO QRADAR

RELEASE 7.0 MAINTENANCE RELEASE 5

FEBRUARY 2012

This Upgrade Guide provides information on the following:

Before You Upgrade

Before you upgrade, review each of the following sections:

Impact of an Upgrade on Your Data

This section only applies if you are upgrading from QRadar 6.3.1 to QRadar 7.0. If you are upgrading from a previous QRadar 7.0 release to 7.0 maintenance release, you do not need to read this section.

Upgrading to QRadar 7.0 provides significant improvements to Security Information and Event Management (SIEM) and network monitoring functionality. QRadar 7.0 merges log and flow data using visualizations, rules, and offenses. Due to the extent of the changes, the upgrade process removes any data that is no longer required by QRadar.

CAUTION

While an upgrade is in progress, data marked for removal during the upgrade cannot be recovered.

The following table specifies the data and functionality changes that occur during the upgrade process:

Table 1-1 Upgrade Impact on Data

Feature	Maintained in QRadar 7.0?	Description of Changes
Sentries	No	QRadar 7.0 replaces sentry functionality with Anomaly Detection Rules, adding the following rule types: • Threshold • Behavioral • Anomaly Custom sentry alert information is not available in QRadar 7.0. Before upgrading to QRadar 7.0, we recommend that you backup the following sentry items: • Sentry data • Sentry settings • Sentry user roles For more information on backing up your data, see the *QRadar Administration Guide*.
Custom Views	No	QRadar 7.0 replaces custom views with enhanced charting functionality in the **Network Activity** tab. We recommend that you recreate your custom views using the **Network Activity** tab in QRadar 7.0.
Active Offenses	Yes	During the upgrade process, active offenses are transitioned to the inactive (closed) state. ***Note:*** *In QRadar 7.0, you can search for and view closed offenses using the offense search feature. Closed offenses are available until the offense retention period has elapsed. The default offense retention period is 3 days.*
Dashboard Customization	Yes	Existing custom dashboard items from QRadar 6.3.1 are still available in QRadar 7.0.
Custom Rules	Yes, depending on the selected tuning template option.	QRadar 7.0 provides new and updated common, event, and flow rules. The upgrade process maintains rule data according to the tuning template option you selected. For more information on the tuning template options, see **Upgrading Your Tuning Template**.

Table 1-1 Upgrade Impact on Data (continued)

Feature	Maintained in QRadar 7.0?	Description of Changes
Network Surveillance	No	QRadar 7.0 removes the **Network Surveillance** tab. Network surveillance functionality is now provided in the **Log Activity** and **Network Activity** tabs. In the **Log Activity** and **Network Activity** tabs, you can configure time series searches to display time series charts with your search results and on your Dashboard. Data related to network surveillance is no longer available. Before upgrading to QRadar 7.0, we recommend that you backup your network surveillance data. For more information on backing up your data, see the *QRadar Administration Guide*.
Saved Searches	Yes, depending on the selected tuning template option.	We recommend that you evaluate the tuning template options before upgrading to determine how the tuning template options impact your saved searches. For more information on the tuning template options, see **Upgrading Your Tuning Template**.
Flow and Event Log Data	Yes	Flow and event log data captured in QRadar 6.3.1 is available in QRadar 7.0.
Network Anomalies	No	QRadar 7.0 replaces network anomaly functionality with anomaly rules on the Rules page of the **Log Activity** and **Network Activity** tabs. The Network Anomalies option is removed from the navigation menu on the **Offenses** tab.
Generated Reports	Yes, depending on the selected tuning template option.	We recommend that you evaluate the tuning template options before upgrading to determine how the tuning template options impact your previously generated reports. For more information on the tuning template options, see **Upgrading Your Tuning Template**.
Report Templates	Yes, depending on the selected tuning template option.	Time series and TopN Time Series charts are removed from the **Reports** tab, therefore, reports based on these chart types are no longer available. We recommend that you evaluate the tuning template options before upgrading to determine how the tuning template options impact your report templates. For more information on the tuning template options, see **Upgrading Your Tuning Template**.

Table 1-1 Upgrade Impact on Data (continued)

Feature	Maintained in QRadar 7.0?	Description of Changes
Remote Services and Networks	Yes	Remote Services and Remote Network groups created in QRadar 6.3.1 are still available in QRadar 7.0.
Application Signatures	Yes	Application mappings and signatures are available in QRadar 7.0, however, you can no longer add custom applications using QRadar. You must manually add your custom application mappings to the configuration file. For more information on configuring your application mappings, see the *QRadar Application Configuration Guide.*
Asset Data	Yes	All asset data is available in QRadar 7.0, including port and vulnerability data.
Asset Map	No	The Asset map is no longer available in QRadar 7.0.
Deployment Editor	Yes	The **Flow View** tab no longer exists in the deployment editor and its functionality is incorporated in the **Log Activity** tab. Pre-existing deployment configurations are converted for use with QRadar 7.0.
Branch Filtering	No	New load balancing and flow routing capabilities replace branch filtering in QRadar 7.0. If your previous deployment was configured for branch filtering, you must reconnect the QFlow Collector to Event Collectors using the deployment editor. ***Note:*** *QRadar 7.0 introduced a new flow communication protocol, changing the way components communicate. We recommend that you upgrade all systems in your deployment to QRadar 7.0; however, if you do not upgrade systems in your deployment hosting off-site flow sources, additional configuration is required. For more information, see the Configuring Flow Forwarding From Pre-7.0 Off-Site Flow Sources appendix in the QRadar Administration Guide.*
Appliance Migrations	Yes	Flow Processor software components, including the Classification Engine and Flow Processor, are migrated to the Event Collector and Event Processor in QRadar 7.0.
User Role Definitions and Permissions	Yes	User role and permission data is maintained. The Manage User Role window has been updated to allow you to manage the permissions for new and updated functionality in QRadar 7.0.

Table 1-1 Upgrade Impact on Data (continued)

Feature	Maintained in QRadar 7.0?	Description of Changes
Custom Event Properties	Yes, depending on the selected tuning template option.	We recommend that you evaluate the tuning template options before upgrading your system. For more information on tuning template options, see **Upgrading Your Tuning Template**.
Qualys Vulnerability Scanners	Yes	Qualys scanners using **Import -Technical Report** as the collection type are converted to the new collection type **Scheduled - Technical Report**. For more information, see the *Managing Vulnerability Assessment Guide*.
System Settings	Yes	The following system settings are no longer available in QRadar 7.0: • Asset Profile Views • Database Storage Location • Sentry Database Location • Dynamic Custom View Deploy Interval • Database Settings - Network View Graph Retention Period • Database Settings - All Views - Group Database Retention Period • Database Settings - All Views - Object Database Retention Period • Ariel Database Settings - Custom View Retention Period

Upgrading Your Tuning Template

This section only applies to you if you are upgrading from QRadar 6.3.1 to QRadar 7.0. If you are upgrading from a previous QRadar 7.0 release to 7.0 maintenance release, you do not need to read this section.

QRadar 7.0 provides significant changes to the way rules and reports are stored. During the upgrade process, you are prompted to select one of four tuning template options. The options are described in the upgrade script, however, we recommend you carefully evaluate the following tuning template options before you begin upgrading your system:

1 Reset the system to the default security template.

This is the recommended option as it ensures the cleanest set of rules for your system. The system is reconfigured to factory settings.

This option:

- Maintains all your data, including offenses, events, flows, assets, and reports.
- Removes all previous rules, report templates, saved searches, and system tuning.

We recommend that you recreate any custom rules, searches, reports, and retune the system, if necessary.

2 Apply the new default template and maintain the existing configuration.

This option:

- Enables new default rules and time series accumulations without modifying any existing rules or searches.
- Maintains all your data, including offenses, events, flows, assets, and reports.
- Provides all new reports and accumulations.
- Resets all modified default reports to the default state, overwriting any customizations.
- Maintains all custom-created reports.

Choosing this option introduces duplicate rules, as the system contains both existing and new rules.

We recommend that you:

- Review your system for duplicate rules and building blocks that may cause false positive offenses and tune your system accordingly.
- Recreate reports that require time series data using the new time series data options.

3 Apply the new template and maintain the current configuration, while enabling only new flow rules, common rules, and specific event rules that are required for new reports.

This option:

- Maintains all your data, including offenses, events, flows, assets, and reports.
- Maintains all new reports and accumulations.
- Configures all modified default reports to the default state, overwriting any customizations.
- Maintains custom-created reports.
- Maintains existing rules and saved searches.
- Enables flow rules that detect activity from flow data that was removed during the upgrade process.

We recommend that you:

- Review all common rules and enable the rules you want to use for flow-based analysis.
- Review your system for duplicate rules and building blocks that could cause false positive offenses and tune your system accordingly.

- Recreate reports that require time series data using the new time series data options.

4 Apply only the new rules and enable a minimal set of these rules.

This option:

- Maintains all your data, including offenses, events, flows, assets, and reports.
- Maintains all existing reports.
- Prevents installation of new default saved searches and reports.
- Maintains existing saved searches and reports.

We recommend that you:

- Review newly installed common rules and flow rules that are disabled by default, and enable the appropriate rules.
- Review duplicate rules and building blocks that could cause false positive offenses and tune your system accordingly.
- Recreate reports that require time series data using the new time series data options.

Upgrade Requirements

Before you upgrade, you must verify your deployment meets the following requirements:

- To upgrade to QRadar 7.0, you must be running QRadar 6.3.1 build 190775, including the latest patches. If you are not running at least QRadar 6.3.1 build 190775, download and install QRadar 6.3.1 and patches from the IBM Fix Central website. In the QRadar user interface, click **Help > About** to view your QRadar version information.
- If you are installing QRadar on your own hardware, ensure you have downloaded the Redhat 5.7 DVD ISO. The upgrade process requires files from the Redhat ISO to complete the QRadar software upgrade.
- If you install QRadar software on your own hardware, your system must include a minimum of 12 GB of memory.
- All QRadar appliances are 64-bit. Make sure that you download the correct installation software for your OS. In rare circumstances, hardware with 32-bit operating systems could require a fresh QRadar installation to upgrade to QRadar 7.0. This only applies to QFlow 1101 appliances purchased before 08/22/2006.
- Close all open QRadar sessions to avoid access errors in your log file.
- Appliances cannot upgrade if they do not meet the minimum memory requirements, as specified in the following table:

Table 1-2 Appliance Memory Requirements

Appliance	Minimum Memory Requirement
QFlow 1101	2 GB

Table 1-2 Appliance Memory Requirements (continued)

Appliance	Minimum Memory Requirement
QFlow 1201	6 GB
QFlow 1202	6 GB
QFlow 1301	6 GB
QFlow 1302	6 GB
QFlow 1310	6 GB
QRadar 1601	12 GB
QRadar 1605	12 GB
QRadar 1701	12 GB
QRadar 1801	12 GB
QRadar 2000	12 GB
QRadar 2100	24 GB
QRadar 3100	24 GB
QRadar 3105	24 GB

- Regardless of appliance type, we recommend that all systems running an Event Collector or Event Processor include a minimum memory of 12 GB.
- We recommend that you upgrade all of the systems in your deployment from QRadar 6.3.1 to QRadar 7.0. If a QFlow Collector does not meet the minimum memory requirements or is unable to be upgraded, you must add the QFlow Collector as a Pre-7.0 Off-site Flow Source. For more information on adding flow sources, see the *QRadar Administration Guide*.
- The Java Runtime Environment must be installed on the desktop system you use to view QRadar. You can download Java version 1.6.0_u24 at the following website: *http://www.java.com*.
- Adobe Flash 10.x must be installed on the desktop system you use to view QRadar.
- The upgrade process validates the disk space required for your QRadar configuration and determines if enough disk space is available. If your system does not have enough free disk space, the upgrade process stops and a message is displayed warning you that additional disk space is required to perform the upgrade. The QRadar 7.0 upgrade requires the following minimum free disk space:
  - `/` partition must have at least 3 GB free space.
  - **`/store`** partition must have at least 4 GB free space.
  - **`/var/log`** partition must have at least 500 MB free space.
  - **`/store/tmp`** partition must have at least 800 MB free space.

Pretesting Your System

Before you upgrade to QRadar 7.0, you must perform a pretest on all the systems in your deployment to ensure that your deployment meets the requirements for the upgrade. We recommend that you schedule the pretest during non-peak hours.

To pretest your system:

Step 1 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

Step 2 Select one of the following options:

- If your system is running CentOS, go to **Step 3**.
- If your system is Red Hat Enterprise Linux 5.3, go to **Step 4**.

Step 3 Download and mount the QRadar 7.0 software:

a To create the **/store/iso** folder, type the following:

```
mkdir /store/iso
```

b Go to the IBM Fix Central website to download the QRadar 7.0 MR5 Patch 2 appliance ISO (7.0.0-QRADAR-QRFULL-342942):

```
http://www.ibm.com/support/fixcentral/
```

c Copy the file to the **/store/iso** folder on your system.

d To mount the ISO, type the following command:

```
mount –o loop /store/iso/<ISO file name> /media/cdrom
```

e Go to **Step 5**.

CAUTION

Ensure there are no CDs in the disk drive before you proceed.

Step 4 Download and mount the QRadar 7.0 software and Red Hat Enterprise Linux 5.7 DVD ISO:

a To create the **/store/iso** and **/media/redhat** folders, type the following:

```
mkdir /media/redhat
mkdir /store/iso
```

b Obtain Red Hat Enterprise Linux 5.7 DVD ISO and copy the file to **/store/iso**.

NOTE

QRadar supports 64-bit OS upgrades. Ensure that you download the correct Red Hat Enterprise Linux 5.7 DVD ISO for your platform.

c To mount the Red Hat Linux 5.7 DVD ISO, type the following command:

```
mount -o loop /store/iso/<name of Red Hat Linux 5.7 DVD ISO>
/media/redhat
```

d Go to the IBM Fix Central website to download the QRadar 7.0 MR5 Patch 2 software ISO (7.0.0-QRADAR-QRFULL-342942SW):

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

NOTE

QRadar supports 64-bit OS upgrades. Ensure you download the correct QRadar ISO for your platform. To download previous QRadar versions, you can view superseeded fixes list on IBM Fix Central.

e Copy the QRadar 7.0 ISO to the **/store/iso** folder on your system.

f To mount the QRadar 7.0 ISO, type the following command:

mount -o loop /store/iso/<name of ISO> /media/cdrom

CAUTION

Ensure there are no CDs in the disk drive before you proceed.

g Go to **Step 5**.

Step 5 To perform the pretest, type the following:

/media/cdrom/setup -t

The following message is displayed:

```
About to run pretests in preparation for upgrade from version
6.3.1.<Build version> to 7.0.0.<Build version>

Do you wish to continue (Y/[N])?
```

Step 6 Type **Y** to continue the pretest.

NOTE

The pretest might prompt you to delete patch files that are no longer required by the system.

The following message is displayed:

```
WARNING: This release offers new and updated functionality that
results in a change to our data collection process. Upgrading
your system will result in some data (as defined below) being
removed from your system. Removed data cannot be recovered once
the upgrade is in process and will no longer be available by the
system. If you require this data, back up the data before
continuing with the upgrade process.

The upgrade will remove the following data:

- Sentries: /store/sentry that uses XX(K/M/G) of disk space.
- Network Surveillance Views: /store/db that uses XX(K/M/G) of
disk space.
- Offenses: Current offenses will not be lost during the
upgrade, however all open offenses will be closed.

For more information, see the Upgrade Guide and Release Notes.

Are you sure you want to proceed with the upgrade (Y/[N])?
```

```
NOTE: Data will only be deleted when you perform the upgrade.
Press ENTER to continue the pretest.
```

Step 7 Press Enter to continue.

CAUTION

When pretesting your system, you are prompted to run PRETESTDOWN scripts after the initial PRETEST is complete. The PRETESTDOWN scripts require all services to be stopped to test the integrity of the database, resulting in a data outage.

The following message is displayed:

```
Completed all PRETEST scripts successfully.
**************** WARNING *****************
About to run PRETESTDOWN scripts which will cause tomcat and
hostcontext services to be stopped and cause a data outage.
These test scripts will be run:
check_db_upgrade.sh
check_permissions.sh
*************** WARNING ******************
Proceed (Y/[N]) (default to N after 55 seconds)?
Are you absolutely sure? THERE WILL BE A DATA OUTAGE!
Proceed (Y/[N]) (default to N after 50 seconds)?
```

Step 8 Type **Y** to run the PRETESTDOWN scripts.

The output of the pretest determines if your system meets the upgrade system requirements, such as:

- Memory requirements
- Partitioning
- Supported and required RPMs
- Log source limits
- Licensing
- Out of memory notifications
- Disk sentry notifications
- Invalid passwords
- Failed logins
- PostgreSQL issues
- Table constraint/key issues

Third-party RPMs are not supported on QRadar systems. If the pretest discovers unsupported RPMs, remove the unsupported RPMs before upgrading your system. If the pretest discovers that required RPMs have been removed, you must re-install the required RPMs before continuing with your upgrade.

If the pretest indicates a problem, contact Customer Support.

Preparing to Upgrade

You must complete the upgrade process on your QRadar Console first and you must be able to access the QRadar user interface on your desktop system before upgrading your secondary Console and other systems in your deployment.

Any QFlow appliance with less than a 80 GB hard drive must use a fresh installation to use the latest software. For more information, see the *QRadar Installation Guide*.

QRadar 7.0 introduced a new flow communication protocol, changing the way components communicate. We recommend that you upgrade all systems in your deployment to QRadar 7.0. However, if you do not upgrade systems in your deployment hosting off-site flow sources, additional configuration is required. For more information, see the *Configuring Flow Forwarding From Pre-7.0 Off-Site Flow Sources* appendix in the *QRadar Administration Guide*.

If your deployment consists of a software-based (non-appliance) installation and you have questions concerning your deployment, contact Customer Support for assistance. For information on QRadar appliances and hardware, see the *QRadar Hardware Installation Guide*.

You must upgrade your QRadar systems in the following order:

1. Console
2. The following systems can be upgraded concurrently:
   - Event Processors
   - Event Collectors
   - Flow Processors
   - QFlow Collectors

If you are upgrading QRadar systems in an HA deployment, you must upgrade in the primary system before upgrading the associated secondary system. The primary host must be the active system in your deployment. If the secondary host displays active, the upgrade of the primary host to QRadar 7.0 cancels. For more information on system and license management, see the *QRadar Administration Guide*.

CAUTION

*Disk replication and failovers are disabled until the primary and secondary hosts synchronize and the **needs upgrade** or **failed** status is cleared from the secondary host.*

During the upgrade of any secondary host, the System and License Management screen changes the status of the secondary host to **upgrading**. After the upgrade of the secondary host is complete, you must restore the configuration of the

secondary host. For more information on restoring a failed host, see the *QRadar Administration Guide*.

You are now ready to upgrade to QRadar 7.0

- If your system is running CentOS, go to **Upgrading Appliances to QRadar 7.0 Using CentOS**.
- If your system is running Red Hat Enterprise Linux, go to **Upgrading to QRadar 7.0 Using Red Hat Enterprise Linux 5.7**.

Upgrading Appliances to QRadar 7.0 Using CentOS

Ensure you backup your data before you begin a software upgrade. For more information on backup and recovery, see the *QRadar Administration Guide*.

To upgrade your appliances to QRadar 7.0:

Step 1 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

Step 2 To create the **/store/iso** folder, type the following:

```
mkdir /store/iso
```

Step 3 Go to the IBM Fix Central website to download the QRadar 7.0 MR5 Patch 2 appliance ISO (7.0.0-QRADAR-QRFULL-342942):

```
http://www.ibm.com/support/fixcentral/
```

Step 4 Copy the file to the **/store/iso** folder on your system.

Step 5 To mount the ISO, type the following command:

```
mount –o loop /store/iso/<ISO file name> /media/cdrom
```

CAUTION

Ensure there are no CDs in the disk drive before you proceed.

Step 6 Type the following setup command:

```
/media/cdrom/setup
```

The End User License Agreement (EULA) is displayed.

Step 7 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The following prompt is displayed:

```
About to upgrade your QRadar from 6.3.1-<build> to 7.0-<build>.
Continue (Y/[N])?
```

Step 8 To continue, type **Y**.

The following message is displayed during the upgrade.

```
WARNING: This release offers new and updated functionality that
results in a change to our data collection process. Upgrading
your system will result in some data (as defined below) being
removed from your system. Removed data cannot be recovered once
the upgrade is in process and will no longer be available by the
system. If you require this data, back up the data before
continuing with the upgrade process.

The upgrade will remove the following data:

- Sentries: /store/sentry that uses XX(K/M/G) of disk space.
- Network Surveillance Views: /store/db that uses XX(K/M/G) of
disk space.
- Offenses: Current offenses will not be lost during the
upgrade, however all open offenses will be closed.

For more information, see the Upgrade Guide and Release Notes.

Are you sure you want to proceed with the upgrade (Y/[N])?
NOTE: Data will only be deleted when you perform the upgrade.
```

Step 9 Type **Y** to continue the upgrade.

The upgrade to QRadar 7.0 is now in progress. You must not cancel or turn off the appliance when an upgrade is in process.

This process can take an extended period of time to complete. The installation might prompt you to delete patch files that are no longer required by the system to save storage space.

The following message is displayed:

```
WARNING: Carefully review the Upgrade Guide before selecting one
of the following options:

1. Reset the system to the default template (Recommended). This
removes all previous rules, reports, searches, and tuning.
Selecting this option requires you to recreate custom rules,
searches, reports, and retune the system.

2. Apply the new default template over the current configuration
with default rules and new time series accumulations enabled
without modifying existing rules or searches. This option resets
default reports and overwrites any changes the user has made to
default reports. User created reports are not affected.
Selecting this option can introduce duplicate rules and will
require significant tuning, however all new reports and
accumulations are available. Reports that required time series
data may need to be recreated.

3. Apply the new template over the current configuration and
enable only new flow rules, common rules, and specific event
rules that are required for new reports or detection of activity
```

```
from flow data which was removed during the upgrade. Existing
rules and saved searches are not modified. This option resets
default reports and overwrites any changes the user has made to
default reports. User created reports are not affected. Some
reports that required time series data may need to be recreated.

4. Apply only new rules and enable a minimal set of these rules.
New saved searches and reports are not installed. Existing saved
searches and reports are not modified. Some reports that
required time series data may need to be recreated. You should
carefully evaluate newly installed common and flow rules that
are disabled by default and enable appropriate rules.

Enter a selection (1-4) or press enter to see the options again:
Is this correct? [y/n]:
```

Step 10 Read these options carefully before upgrading your tuning template. Your selection affects data and customization retention. For more information, see **Upgrading Your Tuning Template**.

Step 11 Type the number for your template option selection and type **Y** to confirm your selection.

Wait for QRadar to complete the upgrade. This process can take several minutes, depending on your system.

CAUTION

You must not cancel or turn off the appliance when an upgrade is in progress.

Step 12 To restart QRadar and complete the upgrade process, type the following:

```
reboot
```

Step 13 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

The following message is displayed:

```
This server was upgraded to QRadar 7.0.0.<build> on <date>.
```

Upgrading to QRadar 7.0 Using Red Hat Enterprise Linux 5.7

QRadar 7.0 supports Red Hat Enterprise Linux 5.7. This section includes Red Hat Enterprise requirements and instructions on how to upgrade QRadar.

When you upgrade to QRadar 7.0 using Red Hat Enterprise Linux on a 64-bit enabled platform, you must use Red Hat Enterprise Linux 5.7 64-bit.

To upgrade to QRadar 7.0 using Red Hat Enterprise Linux, you must:

- Verify your systems meet the minimum upgrade free disk space requirements. See **Upgrade Requirements**.
- Review the data changes to your system before you upgrade. See **Impact of an Upgrade on Your Data**.
- Pretest all the systems in your deployment to verify your hardware meets the minimum requirements for the upgrade. See **Pretesting Your System**.
- Plan your deployment upgrade order. See **Preparing to Upgrade**.
- Verify your command-line package management utility Yellowdog Updater, Modified (YUM) is configured properly, because QRadar software requires specific versions of some libraries.
- Perform the upgrade. See **Upgrading to QRadar 7.0**.
- Upgrade Endace Network Monitoring Interface Card drivers. See **Upgrade Endace Network Monitoring Interface Card Drivers**.

Upgrading to QRadar 7.0

Before you begin the upgrade process, review the **Preparing to Upgrade** section.

To upgrade to QRadar 7.0 maintenance release 5 patch 2 (7.0.0.342942):

Step 1 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

Step 2 To create the **/store/iso** and **/media/redhat** folders, type the following:

```
mkdir /media/redhat
mkdir /store/iso
```

Step 3 Obtain Red Hat Enterprise Linux 5.7 DVD ISO and copy the file to **/store/iso**.

NOTE QRadar supports 64-bit OS upgrades. Make sure that you download the correct Red Hat Enterprise Linux DVD ISO for your platform.

Step 4 To mount the Red Hat Linux 5.7 DVD ISO, type the following command:

```
mount -o loop /store/iso/<name of Red Hat Linux 5.7 DVD ISO>
/media/redhat
```

Step 5 Go to the IBM Fix Central website to download the QRadar 7.0 MR5 Patch 2 software ISO (7.0.0-QRADAR-QRFULL-342942SW):

```
http://www.ibm.com/support/fixcentral/
```

NOTE

QRadar supports 64-bit OS upgrades. Ensure you download the correct QRadar upgrade for your platform. To download previous QRadar versions, you can view superseeded fixes list on IBM Fix Central.

Step 6 Copy the QRadar 7.0 ISO to the **/store/iso** folder on your system.

Step 7 To mount the QRadar 7.0 ISO, type the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Step 8 Type the following setup command:

```
/media/cdrom/setup
```

NOTE

If your system has multiple volumes and a DRAC card, the following message is displayed, indicating that the upgrade process might cancel due to an unsupported configuration: `ERROR: Upgrade on systems without sda drive not supported` or `ERROR: Upgrade on PowerEdge 2950 only supported on single RAID 10 logical disk`. If this error is displayed, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 9 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The following prompt is displayed:

```
About to upgrade your QRadar from 6.3.1-<build> to 7.0-<build>.
Continue (Y/[N])?
```

Step 10 To continue, type **Y**.

The following message is displayed:

```
WARNING: This release offers new and updated functionality that
results in a change to our data collection process. Upgrading
your system will result in some data (as defined below) being
removed from your system. Removed data cannot be recovered once
the upgrade is in process and will no longer be available by the
system. If you require this data, back up the data before
continuing with the upgrade process.

The upgrade will remove the following data:

- Sentries: /store/sentry that uses XX(K/M/G) of disk space.
- Network Surveillance Views: /store/db that uses XX(K/M/G) of
disk space.
- Offenses: Current offenses will not be lost during the
upgrade, however all open offenses will be closed.

For more information, see the Upgrade Guide and Release Notes.

Are you sure you want to proceed with the upgrade (Y/[N])?
```

```
NOTE: Data will only be deleted when you perform the upgrade.
```

Step 11 Type **Y** to continue the upgrade.

The upgrade to QRadar 7.0 is now in progress. You must not cancel or turn off the appliance when an upgrade is in progress. The upgrade might prompt you to delete patch files that are no longer required by the system to save storage space.

The following message is displayed:

```
WARNING: Carefully review the Upgrade Guide before selecting one
of the following options:

1. Reset the system to the default template (Recommended). This
removes all previous rules, reports, searches, and tuning.
Selecting this option requires you to recreate custom rules,
searches, reports, and retune the system.

2. Apply the new default template over the current configuration
with default rules and new time series accumulations enabled
without modifying existing rules or searches. This option resets
default reports and overwrites any changes the user has made to
default reports. User created reports are not affected.
Selecting this option can introduce duplicate rules and will
require significant tuning, however all new reports and
accumulations are available. Reports that required time series
data may need to be recreated.

3. Apply the new template over the current configuration and
enable only new flow rules, common rules, and specific event
rules that are required for new reports or detection of activity
from flow data which was removed during the upgrade. Existing
rules and saved searches are not modified. This option resets
default reports and overwrites any changes the user has made to
default reports. User created reports are not affected. Some
reports that required time series data may need to be recreated.

4. Apply only new rules and enable a minimal set of these rules.
New saved searches and reports are not installed. Existing saved
searches and reports are not modified. Some reports that
required time series data may need to be recreated. You should
carefully evaluate newly installed common and flow rules that
are disabled by default and enable appropriate rules.

Enter a selection (1-4) or press enter to see the options again:
Is this correct? [y/n]:
```

Step 12 Read these options carefully before upgrading your tuning template. Your selection affects data and customization retention. For more information, see **Upgrading Your Tuning Template**.

Step 13 Type the number for your template option selection and type **Y** to confirm your selection.

Wait for the upgrade process to complete. The upgrade process could take several minutes, depending on your system.

CAUTION

You must not cancel or turn off the appliance when an upgrade is in progress.

Step 14 To restart QRadar and complete the upgrade process, type the following command:

`reboot`

Step 15 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

The following message is displayed:

```
This server was upgraded to QRadar 7.0.0.<build> on <date>.
```

Upgrade Endace Network Monitoring Interface Card Drivers

To use our pre-built Endace Network Monitoring Interface Card drivers, you must use the Red Hat Enterprise Linux 5.7 kernel (kernel-2.6.18-274.7.1.el5), which is provided on the QRadar 7.0 ISO.

NOTE

If you are using custom Endace Network Monitoring Interface drivers, see your Red Hat Enterprise documentation for more information.

To upgrade your pre-built Endace Network Monitoring Interface Card kernel and drivers:

Step 1 To mount the QRadar 7.0 ISO, type the following command:

`mount -o loop <path to the QRadar ISO> /media/cdrom`

Step 2 To upgrade the kernel, type the following:

`cd /media/cdrom/`

`rpm –Uvh updates/kernel* 3rdparty/dag*.rpm 3rdparty/kmod-dag*.rpm`

Step 3 To verify that the upgraded kernel is listed first and the default is zero (0) in the /etc/grub.conf file, type the following:

`cat /etc/grub.conf`

The output should resemble the following:

```
# grub.conf generated by anaconda
## Note that you do not have to rerun grub after making changes
to this file
# NOTICE:  You have a /boot partition.  This means that
# all kernel and initrd paths are relative to /boot/, eg.
```

```
# root (hd0,0)
# kernel /vmlinuz-version ro root=/dev/sda6
# initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.18-274.7.1.el5)
     root (hd0,0)
     kernel /vmlinuz-2.6.18-274.7.1.el5 ro root=LABEL=/
     initrd /initrd-2.6.18-274.7.1.el5.img
title Red Hat Enterprise Linux Server (2.6.18-274.7.1.el5)
     root (hd0,0)
     kernel /vmlinuz-2.6.18-238.19.1.el5 ro root=LABEL=/
     initrd /initrd-2.6.18-238.19.1.el5.img
```

CAUTION

The kernel must be listed first and the default must be zero (0). If the kernel is not listed first or the default is not zero (0), you must edit the file to change the parameters. The Kernel version for 64-bit systems is 2.6.18-274.7.1.el5.

Step 4 To reboot your system, type the following command:

```
reboot
```

Step 5 To verify that the drivers are loading correctly, type the following:

```
lsmod | grep dag
```

The output should resemble the following:

```
dag 90560 0
dagmem 125600 1 dag
```

If you experience problems loading the drivers, you can review the log file located at /var/log/daginit.log. For further assistance, contact Customer Support.

Clearing the Cache

If you have trouble accessing the QRadar user interface after you upgrade to QRadar 7.0, we recommend that you clear your Java cache. Before you clear the cache, ensure you have only one instance of your browser open. If you have multiple versions of your browser open, the cache fails to clear.

NOTE

The Java Runtime Environment must be installed on the desktop system you use to view QRadar. You can download Java version 1.6.0_u24 at the following website: http://java.com/.

To clear your cache and access the QRadar user interface:

Step 1 Clear your Java cache:

a On your desktop, select **Start > Control Panel**.

The Control Panel is displayed.

b Double-click the **Java** icon.

The Java Control Panel is displayed.

NOTE

If you are using Microsoft Windows 7 as your operating system, the **Java** icon is typically located under the **Programs** pane, depending on how your Control Panel is configured to display features.

c In the **Temporary Internet Files** pane, click **View**.

The Java Cache Viewer is displayed.

d Select all QRadar Deployment Editor entries.

e Click the **Delete** icon.

f Click **Close**.

g Click **OK**.

Step 2 Open your web browser.

Step 3 Clear the cache of your web browser:

a If you are using Internet Explorer 7.0 or 8.0, select **Tools > Delete Browsing History**.

b If you are using Internet Explorer 9.0, click the gear icon in the right corner of the browser window, select **Internet Options > General**, and then click **Delete** in the **Browsing History** pane.

c If you are using Mozilla Firefox 3.6.x and above, select **Tools > Clear Recent History > Clear Now**.

NOTE

If you are using Mozilla Firefox, you must clear the cache in Internet Explorer and Mozilla Firefox.

Step 4 Log in to QRadar:

`https://<IP Address>`

Where **`<IP Address>`** is the IP address of the QRadar system. The default values are:

Username: **admin**

Password: **<password>**

Where **`<password>`** is the password assigned to QRadar during the QRadar installation process.

For more information on accessing and using QRadar, see the *QRadar Users Guide* or the *QRadar Administration Guide*.

After You Upgrade

After you upgrade, make sure you have completed the following:

- Reconnect any off-site components using the deployment editor to maintain forwarded event and flow data between deployments. For more information on using the deployment editor, see the *QRadar Administration Guide*.
- Connect your QFlow Collectors to the correct Event Collector using the deployment editor. For more information on using the deployment editor, see the *QRadar Administration Guide*.
- Update your DSMs, scanners, protocols and Juniper NSM plug-in to QRadar 7.0 versions. If your deployment includes DSMs or scanners installed using an .rpm file, the following error is displayed in the log files after you upgrade your system to QRadar 7.0:

  ```
  ErrorStream ExecuteAutoUpdate-Deploy: Can't load
  '/opt/qradar/perl5libs/lib/site_perl/5.6.1/i686-linux-thread-
  multi/auto/XML/Parser/Expat/Expat.so' for module XML::Parser
  ::Expat:/opt/qradar/perl5libs/lib/site_perl/5.6.1/i686-linux-
  thread-multi/auto/XML/Parser/Expat/Expat.so: wrong ELF class:
  ELFCLASS32 at/usr/lib64/perl5/5.8.8/x86_64-linux-thread-multi
  /DynaLoader.pm line 230
  ```

  This error does not affect the upgrade process or system functionality and can be ignored. For more information, go to the IBM Fix Central website.
- Validate your system to determine if any of the following rules or reports are required. If any of the following reports are required for your system, you must enable the associated rule:

Table 1-3 Rules Required for Default Reports

Rule Number	Rule Description	Report Name
1279	Compliance: Compliance Events Become Offenses	Systems and Users Involved in Compliance Offenses
1296	System: Device Stopped Sending Events	PCI 10 - Audit of Data
1296	System: Device Stopped Sending Events	PCI 10 - Audit of Data (Weekly)
1296	System: Device Stopped Sending Events	PCI 10 - Audit of Data (Monthly)
1302	Vulnerabilities: Vulnerability Reported by Scanner	Systems and Users Involved in Compliance Offenses
1346	Compliance: Excessive Failed Logins to Compliance IS	Systems and Users Involved in Compliance Offenses
1427	Authentication: Login Failure to Disabled Account	Weekly Login Failures to Disabled or Enabled Accounts

Table 1-3 Rules Required for Default Reports (continued)

Rule Number	Rule Description	Report Name
1428	Authentication: Login Failure to Expired Account	Weekly Login Failures to Disabled or Enabled Accounts
1553	Compliance: Multiple Failed Logins to a Compliance Asset	Systems and Users Involved in Compliance Offenses
1559	Compliance: Traffic from Untrusted Network to Trusted Network	Systems and Users Involved in Compliance Offenses
1560	Compliance: Traffic from DMZ to Internal Network	Systems and Users Involved in Compliance Offenses
1562	Compliance: Configuration Change Made to Device in Compliance network	Systems and Users Involved in Compliance Offenses
1564	Compliance: Auditing Services Changed on Compliance Host	Systems and Users Involved in Compliance Offenses

For more information on enabling rules or reports, see the *QRadar Administration Guide*.