F5® BIG-IQ® Centralized Management: Upgrading Version 5.x to Version 5.3

Version 5.3

Table of Contents

Table of Contents

4

Upgrading BIG-IQ Centralized Management Version 5.x to Version 5.3

What you need to do before you upgrade BIG-IQ from version 5.x to 5.3

Before upgrading F5® BIG-IQ® Centralized Management, perform the following tasks.

Tasks	Additional information
Re-activate the BIG-IQ system license.	You must do this on both the active and the secondary BIG-IQ if they are running in an HA pair. For specific instructions about how to reactivate a license, refer to the *F5® BIG-IQ® Central Management: Licensing and Initial Setup* guide.
Create a backup of the BIG-IQ system's current compressed user configuration set (UCS) and store it on a remote server.	The UCS file includes: system-specific configuration files, license, user account and password information, and SSL certificates and keys. You can use this backup in the event you want to restore to the previous version of BIG-IQ.
Decide which disk volume you want to install the upgrade on. You must have at least two volumes to upgrade BIG-IQ.	If you are running BIG-IQ Virtual Edition and you don't have two volumes, refer to: *K17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at: *support.f5.com/csp/article/K17406*
Deploy any staged configuration changes to your managed devices.	This step is required only if you are going to use the script to re-discover and re-import BIG-IP devices and services after the upgrade (as outlined in the section titled, *Re-discover devices and re-import services in bulk using a script*). You must deploy configuration changes you have staged for your devices if you use this script, because they'll be overwritten on BIG-IQ after you run the script. If you'd rather re-discover devices and re-import services from the BIG-IQ user interface (instead of in bulk) so you can address any potential configuration conflicts for each BIG-IP device, refer to the section titled, *Re-discover devices and re-import services from the user interface*.

Gather the following information:

Required information	For my configuration
You'll need to create a passphrase for the Master Key. The passphrase must contain: • At least 16 characters • Contain at least 1 capital letter • Contain at least 1 lower case letter	

Required information	For my configuration
• Contain at least 1 number • Contain at least 1 special character *Important: You must use the same Master Key Passphrase for each BIG-IQ system in an HA pair and every device in a logging node cluster. The upgrade will complete without it, but the HA pair or logging node cluster will not function if the pass phrases don't match.*	
Get the discovery address you specified on the BIG-IQ system during setup. This is the same IP address that the peers in a high availability confirmation use to communicate. You can find this IP address on the BIG-IQ HA screen.	
Get your BIG-IQ administrator and root passwords.	
Get the name for the secondary HA BIG-IQ system if configured in an HA pair.	

If you're currently running a version of BIG-IQ prior to version 5.0, you must first upgrade to version 5.0 before you can upgrade to version 5.3. For more information, refer to the guide titled, *F5 BIG-IQ Centralized Management: Upgrading BIG-IQ to Version 5.0*.

If you're upgrading BIG-IQ Data Collection Device clusters, refer to the guide titled, *F5 BIG-IQ Centralized Management: Upgrading Data Collection Device clusters to version 5.3*.

Which upgrade workflow should I use?

The user interface for BIG-IQ® Centralized Management has changed between releases. Before you start the upgrade process, decide which workflow is appropriate for you.

If you're upgrading from:	Use this guide:	Note:
Version 5.0	*F5 BIG-IQ Centralized Management: Upgrading Version 5.0 to Version 5.1*	For all tasks and references of v5.1.0, substitute v5.3.0.
Version 5.1	*F5 BIG-IQ Centralized Management: Upgrading Version 5.x to Version 5.2*	For all tasks and references of v5.1.0 or v5.2.0, substitute v5.3.0.
Version 5.2	*F5 BIG-IQ Centralized Management: Upgrading Version 5.x to Version 5.3*	N/A

Summary of procedures to upgrade BIG-IQ from version 5.x to 5.3

To upgrade F5® BIG-IQ® Centralized Management from BIG-IQ version 5.x to 5.3, perform these procedures. Upgrading BIG-IQ to the most recent version requires that you update its configuration to incorporate new features introduced. It's a good idea to set aside at least a few hours to complete this process.

Note: It is important that you follow these procedures in the order stated.

---

1. Complete all of the prerequisites outlined in the topic titled, *What you need to do before you upgrade BIG-IQ from version 5.x to 5.3*.
2. Download the BIG-IQ version 5.3 `iso` file from the F5 Downloads site to your desktop.
3. Upload the software image to, and install the new software on your primary BIG-IQ.
4. If you're upgrading an HA pair:

   - Remove the peer BIG-IQ from the primary BIG-IQ.
   - Upload the software image to, and install the new software on the peer BIG-IQ.
   - Re-establish the HA configuration.
5. Upgrade the BIG-IP® framework on your managed devices.
6. Rediscover devices, and re-import LTM®, ASM®, AFM®, and DNS® services. You must also remove, and recreate or reimport any existing access groups for devices running APM services.

Note: You have the option to use a script from the command line to re-discover and re-import services (in bulk) for devices running LTM, ASM, AFM, and DNS, or individually through the BIG-IQ user interface. For devices running the APM® service, you must remove and recreate access groups for devices running the APM service. For more information, refer to, Use a script to remove and recreate access groups in bulk for devices running APM services,Remove and recreate access groups (with SWG data) from the user interface for devices running APM services or Reimport access groups (without SWG data) from the user interface for devices running APM services.

Download the BIG-IQ version 5.3 software image from F5 Networks

Downloading a software image from F5 Networks is the first step to making it available to install on the BIG-IQ system.

1. Log in to the F5 Downloads site, `downloads.f5.com`.
2. Click the **Find a Download** button.
3. Click the name of the product line.
4. Click the product name, **Centralized Management**.
5. Click **V5.3.0**.
6. Read the End User Software License agreement and click the **I Accept** button if you agree with the terms.
7. Click the BIG-IQ version 5.3 `.iso` file name.
8. Click the name of the closest geographical location to you.
   The software image downloads to your local system.

The software image is now available for you to upload.

Upload the BIG-IQ version 5.3 software image

Before you can upload the software image to the BIG-IQ® system, you must have first downloaded it from the F5 Downloads site.

Upload the BIG-IQ version 5.3 software image to the primary BIG-IQ system to make it available for this upgrade.

1. At the top of the screen, click **System**.
2. On the left, click **THIS DEVICE** > **SOFTWARE MANAGEMENT** > **Available Images**.

3. Click the **Upload Image** button.
4. Click the **Choose File** button and go to the location to which you downloaded the image, and click the **Open** button to upload it to BIG-IQ.
5. Click the **Upload** button.

   The screen refreshes to display the progress of the upload.

When the image is done uploading, it shows in the Available Images list.

Remove the secondary BIG-IQ from the HA pair

If the F5®BIG-IQ® Centralized Management system is configured in an HA pair, you must remove the secondary BIG-IQ system before you upgrade the primary BIG-IQ.

1. Log in to the primary BIG-IQ with your admin user name and password.
2. At the top of the screen, click **System**.
3. On the left, click **BIG-IQ HA**.
4. Click **Remove Secondary**.
   A dialog box opens, prompting you to confirm that you want to remove the HA secondary device from this group.
5. Click **Remove** to confirm you want to take the HA secondary device out of the group.
   The system logs you out of the BIG-IQ while it removes the secondary device.
6. Log back in to the primary BIG-IQ with your admin user name and password.

   For a while, both the primary and the secondary BIG-IQ devices continue to display. After a few minutes, the screen updates to display a single standalone device.

Upgrade BIG-IQ to version 5.3

You need at least two volumes to upgrade F5® BIG-IQ® Centralized Management. If you are running BIG-IQ Virtual Edition and don't have two volumes, refer to: *K17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at `support.f5.com/csp/article/K17406.html`

Before upgrading the primary BIG-IQ you must download the BIG-IQ version 5.3 `.iso` image from the F5 downloads site.

Warning: These procedures require that the BIG-IQ system is temporarily unavailable, and unable to manage BIG-IP® devices until the upgrade is complete. BIG-IP devices can continue to manage traffic during this time. This process can take up to an hour.

Upgrade BIG-IQ to take advantage of the newest functionality and features.

1. Log in to the BIG-IQ system with your admin user name and password.
2. At the top of the screen, click **System**.
3. On the left, expand **THIS DEVICE** > **Software Management**, then click Available Images.
   The Available Images screen lists the software image files that are available for install on this BIG-IQ.
4. Select the check box for the image you want to install and click **Install**.
5. From the **Target Volume** list, select the volume you want to install the image on.
6. To prompt BIG-IQ to reboot into the new software installation volume, select the **Reboot into Target Volume** check box.
7. Click the **Install** button.

8. Click the **Continue** button.

9. Wait while BIG-IQ loads the new software and reboots.

   Depending on your configuration and the number of devices you are managing, this could take up to an hour. During this time, it is important that you not interrupt the installation process by restarting services or the server.

10. If needed, extend the /var partition.

    The default size of the /var file system in a newly installed node is 10 GB. This volume size might be insufficient to store your data. You can see how to extend this file system to a larger size in knowledge article K16103. refer to: K16103: Extending disk space on BIG-IQ Virtual Edition at support.f5.com/csp/article/K16103. Because upgrading a node requires at least two volumes, you must ensure that both volumes can have their /var file system extended to the same size, or upgrades might fail.

Even though you can log in to this BIG-IQ system after the software is installed, the system continues some database re-indexing processes in the background. For larger configurations, that can take up to an hour. If you perform any searches on objects before it's done re-indexing, BIG-IQ might not return the expected results. During this time, you can continue with the rest of the upgrade process.

Install version 5.3 on the peer BIG-IQ system

After you upgrade the primary BIG-IQ® Centralized Management system to version 5.3, you can upgrade a secondary BIG-IQ system for an HA configuration.

You need at least two volumes to install BIG-IQ software. If you are running BIG-IQ Virtual Edition and you don't have two volumes, refer to: *K17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at `https://support.f5.com/csp/article/K17406`.

Important: Be sure you have the Master Key pass phrase you used for the primary BIG-IQ system; you'll need this when you complete the setup wizard after you reboot. You must use the same Master Key pass phrase on both systems for the pair to successfully communicate and synchronize.

Install version 5.3 on the peer BIG-IQ system so it'll be running the same version as the peer BIG-IQ system you just upgraded.

1. Log on to the system you are going to establish as the secondary BIG-IQ system's command line as **root** and type the following command: `/usr/bin/clear-rest-storage`.

   While this step is not required, it clears the database storage on the system so the upgrade goes more quickly. After you upgrade both peer systems and re-establish the HA pair, the peer BIG-IQ will synchronize its database with this BIG-IQ system and repopulate the database.

2. Log on to the system you are going to establish as the secondary BIG-IQ system's user interface.

3. If you ran the `clear-rest-storage` command, complete the setup wizard. Otherwise, continue to step 4.

4. At the top of the screen, click **System**.

5. On the left, expand **THIS DEVICE** > **Software Management**, then click Available Images.
   The Available Images screen lists the software image files that are available for install on this BIG-IQ.

6. Select the check box for the image you want to install and click **Install**.

7. From the **Target Volume** list, select the volume you want to install the image on.

8. To prompt BIG-IQ to reboot into the new software installation volume, select the **Reboot into Target** volume check box.

9. Click the **Install** button.

A confirmation dialog box appears.

10. Click the **Continue** button.

11. Wait while BIG-IQ loads the new software and reboots.

    Depending on your configuration and the number of devices you are managing, this could take up to an hour. During this time, it is important that you not interrupt the installation process by restarting services or the server.

12. Log in to the BIG-IQ that will be the secondary BIG-IQ system to confirm that the upgrade succeeded and complete the setup wizard.

    To complete the setup task, you must supply a master key pass phrase that all devices in the logging node cluster must share. Make note of the phrase you use. Each logging node, as well as the primary and secondary BIG-IQ systems must use this phrase before they can join the cluster.

13. Complete the setup wizard.

You can now re-establish the BIG-IQ HA configuration.

Re-establish the HA configuration after upgrading to BIG-IQ version 5.3

After you upgrade both F5® BIG-IQ® Centralized Management systems in a HA configuration, you can re-associate the secondary system with the primary BIG-IQ system.

1. Log in to primary BIG-IQ system with your administrator user name and password.

2. At the top of the screen, click **System**.

3. On the left, click **BIG-IQ HA**.

4. Click the **Add Secondary** button.

5. In the **IP Address** field, type the discovery address you specified on the BIG-IQ system during setup.

    This is the same IP address the peers in a high availability confirmation use to communicate.

6. In the **User name** and **Password** fields, type the administrative user name and password for the system.

7. In the **Root Password** field, type the root password for the system.

8. Click the **Add** button to add this device to this high availability configuration.

Even though you can log in to the secondary BIG-IQ after the you re-establish the HA configuration, the system continues some database re-indexing processes in the background. For larger configurations, that can take up to an hour. If you perform any searches on objects before it's done re-indexing, BIG-IQ might not return the expected results. During this time, you can use the primary BIG-IQ.

Next, you should verify that both BIG-IQ systems have the same configuration.

Upgrade the statistics agent

If you collected statistics in version 5.2, then when you finish upgrading the primary BIG-IQ to version 5.3, you need to upgrade the statistics agent on each BIG-IP device that had statistics enabled before the upgrade.

1. At the top of the screen, click **Devices**.

2. Select all of the BIG-IP devices selecting the check box next to **Status**.

3. Click **More** , and then select **Update Stats Agent**.
   The Statistics Collection Agent Upgrade screen opens.

4. For **Modules/Services**, select the check box next to the services you collected statistics for in BIG-IQ version 5.2.

5. For **Frequency** select how often you want to collect statistics for these services.

6. Click the **Continue** button.

7. Wait while the stats collection agent for each BIG-IP device is upgraded.

   Depending on the number of devices in your cluster, this could take several minutes to complete.

   When the agent is upgraded on each BIG-IP, the status icon turns to green.

Upgrade the BIG-IP framework

To properly communicate, BIG-IQ® Centralized Management and managed BIG-IP® devices must be running a compatible version of its framework. If the frameworks are incompatible, BIG-IQ displays a yellow triangle next to the device in the BIG-IP Device inventory.

When you upgrade a BIG-IP device running version 11.5.x to another 11.5.x version, or to an 11.6.x version (for example, from version 11.5.3 to 11.5.4, or from version 11.5.3 to version 11.6.1), you must upgrade the REST framework so BIG-IQ can manage the device.

When you upgrade BIG-IQ from version 5.x to 5.3, you must also upgrade the REST framework for all BIG-IP devices (currently in the BIG-IP Device inventory) running a version prior to 12.0.0.

1. At the top of the screen, click **Devices**.

2. Select the check box next to a device, click the **More** button, and select **Upgrade Framework**. A popup screen opens.

3. Into the fields, type the required credentials, and click the **Continue** button. A `REST Framework upgrade in progress` message displays.

After the framework is updated, you can successfully manage this device.

Repeat these steps for each device.

Re-discover devices and re-import LTM, ASM, AFM, and DNS services in bulk using a script

After you upgrade to BIG-IQ® Centralized Management version 5.3, you can use a script to re-discover devices and re-import the LTM, ASM, AFM, and DNS services in bulk. To run this script, you must have root access to the BIG-IQ command line.

Warning: Before you run this script, make sure you don't have any pending configuration changes staged for your managed BIG-IP devices. This script prompts BIG-IQ to import the configurations for all your BIG-IP devices. So, if you don't deploy staged configuration changes before you run this script, you will lose them after you run the script. If you need assistance, contact F5 Support.

Use this script to re-discover devices and re-import LTM, ASM, AFM, and DNS services all at once, so you can start managing your devices with the new version of BIG-IQ software.

Note: If you'd rather re-discover devices and re-import their services individually through the user interface, refer to Re-discover devices and re-import LTM, ASM, AFM, and DNS services from the user interface.

1. Log in to the `downloads.f5.com` site, click the **Find a Download** button, and click BIG-IQ **Centralized Management**.

2. Click the **v5.3.0** link.

3. Review the End User Software License agreement and click the **I Accept** button to accept the terms.

The Select a Download screen opens.

4. Click the `bulkDiscovery.zip` file name, and unzip it on your local system.

5. Log in to the BIG-IQ system as the root user and upload the script.

6. Enable executable permissions, by typing: `chmod +x ./bulkDiscovery.pl`

   Note: To access help for this script, type ./bulkDiscovery.pl -h

7. Export the IP addresses for the BIG-IP devices in your network to a CSV file, by typing: `./bulkDiscovery.pl -c masterDeviceList.csv -m -o`

8. Re-discover your BIG-IP devices and re-import their services, by using the associated command:

   Note: This command prompts BIG-IQ to import all the configurations from the specified BIG-IP devices. It's important that you've already deployed any configuration changes you have staged for these devices, because they'll be overwritten on BIG-IQ after you run this script. If you'd rather re-discover devices and re-import services individually so you can address any potential configuration conflicts for each device, you can do that from the BIG-IQ system's user interface instead of using this script. For more information, refer to, Re-discover devices and re-import services from the user interface.

   • For LTM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -m`

     Note: You must re-discover devices running the LTM service before re-discovering devices running any other service.

   • For ASM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -s -m`
   • For AFM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -f -m`
   • For DNS, type `./bulkDiscovery.pl -c myDeviceList.csv -l -d -m`

   You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.3.0.

Re-discover devices and re-import LTM, ASM, AFM, and DNS services from the user interface

After you upgrade F5® BIG-IQ Centralized Management to version 5.3, you must rediscover your managed devices and reimport the services you use so you can start using the new features introduced in this release. This process requires you rediscover each device individually and reimport its services.

Important: If you'd rather run a Perl script to perform a bulk rediscovery of your devices and reimport of their services, refer to Re-discover devices and re-import LTM, ASM, AFM, and DNS services using a bulk script.

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to rediscover and reimport services for.
3. On the left, click **Services**.
4. *Important: To avoid any unnecessary conflicts between services, re-discover and re-import the LTM service first, before any other services.*

   Click the **Re-discover** button next to a service.
   When BIG-IQ rediscovers the service, a yellow triangle next to the **Re-import** button displays to indicate you need to re-import the service.
5. Click the **Re-Import** button.

6. If there are conflicts, select one of the following options for each object that is different, and then click the **Continue** button:

   - **Use BIG-IQ** to use the configuration settings stored on BIG-IQ.
   - **Use BIG-IP** to override the configuration setting stored on BIG-IQ with the settings from the BIG-IP device.

Perform these steps for the rest of your managed devices.

Use a script to remove and recreate access groups in bulk for devices running APM services

After you upgrade F5 BIG-IQ Centralized Management to version 5.3, you must remove and recreate the access groups for devices running the APM service.

Warning: Before you run this script, make sure you don't have any pending configuration changes staged for your managed BIG-IP devices. This script prompts BIG-IQ to import the configurations for all your BIG-IP devices. So, if you don't deploy staged configuration changes before you run this script, you will lose them after you run the script. If you need assistance, contact F5 Support.

You can use this script to remove and recreate the access groups for devices running the APM service so you can start managing those devices with the new version of BIG-IQ.

Note: If you'd rather do this from the user interface, refer to, Remove and recreate access groups (with SWG data) from the user interface for devices running APM services or Reimport access groups (without SWG data) from the user interface for devices running APM services.

1. Log in to the BIG-IQ system as admin.
2. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
3. In a separate file (such as a Notepad or Excel file), make a note of:

   - Each access group and the IP addresses of the devices contained within each.
   - The source device, from which you want to copy the configuration to all devices in the access group.

   Note: You'll deploy the configuration from this source device to all of the devices in the access group.

4. Select the check box next to each access group and click the **Remove** button.
5. Log in to the `downloads.f5.com` site, click the **Find a Download** button, and click BIG-IQ **Centralized Management**.
6. Click the **v5.3.0** link.
7. Review the End User Software License agreement and click the **I Accept** button to accept the terms. The Select a Download screen opens.
8. Click the `bulkDiscovery.zip` file name, and unzip it on your local system.
9. Log in to the BIG-IQ system as the root user and upload the script.
10. Enable executable permissions, by typing: `chmod +x ./bulkDiscovery.pl`

    Note: To access help for this script, type `./bulkDiscovery.pl -h`

11. Export the IP addresses for the BIG-IP devices in your network to a CSV file, by typing: `./bulkDiscovery.pl -c masterDeviceList.csv -m -o`
12. For each access group:

      a) Create a device list, by typing `cp masterDeviceList.csv`
          `<access_group_name>_devices.csv`

      b) Edit the file as follows:

- Remove any devices that don't belong to the access groups by comparing it to the list you made in step 3.
- Place the source BIG-IP device you identified in step 3, at the top of the `<access_group_name>_devices.csv` file.
- Verify the credentials for each device (the script uses ADMIN/APWD by default).

      c) Save your changes to the file.

      d) Impot devices in the access group by, typing: `./bulkDiscovery.pl -c`
          `<access_group_name>_devices.csv -g <access_group_name> -l -p -o -v`

13. Log in to the BIG-IQ system as admin.

14. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .

15. Review the access groups to verify all the groups properly imported.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.3.0.

Re-import access groups (without SWG data) from the user interface for devices running APM services

After you upgrade F5® BIG-IQ Centralized Management to version 5.3, you must re-import the access groups running the APM service without SWG data.

Use this procedure to access groups for devices running APM services without F5 Secure Web Gateway configuration data so you can start using the new features introduced in this release.

Important: If you'd rather use a script to do this, Use a script to remove and recreate access groups in bulk for devices running APM services. If your APM configuration includes SWG data, refer to Remove and recreate access groups (with SWG data) from the user interface for devices running APM services.

1. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .

2. Click the name of the access group.

3. From the Device list, select from which to reimport the shared access policy configuration and click the **Reimport** button.

This device will share the access policy configuration with all other devices in this access group.

4. Select **Shared Access Group and Device Specific configuration** and click the **Reimport** button at the bottom of the screen.

5. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.

6. If the differences window displays for the APM service, click the **Accept** button.

7. For the remainder of the devices in this access group:

      a) Select the check box next to the device, and click the **Reimport** button.

      b) Select **Device specific configuration** and click the **Reimport** button at the bottom of the screen.

      c) If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.

      d) If the differences window displays for the APM service, click the **Accept** button.

8. Repeat steps 2-7 for the rest of the access groups.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.3.0.

Remove and recreate access groups (with SWG data) from the user interface for devices running APM services

After you upgrade F5® BIG-IQ Centralized Management to version 5.3, you must recreate the access groups running the APM service.

Use this procedure to remove and recreate access groups for devices running APM services with F5 Secure Web Gateway configuration data so you can start using the new features introduced in this release.

Important: If you'd rather use a script to do this, refer to Use a script to remove and recreate access groups in bulk for devices running APM services. If your APM configuration doesn't include SWG data, refer to Reimport access groups (without SWG data) from the user interface for devices running APM services.

1. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
2. In a separate file (such as a Notepad or Excel file), make a note of:

   • Each access group and the IP addresses of the devices contained within each.
   • The source device, from which you want to copy the configuration to all devices in the access group.

   Note: You'll deploy the configuration from this source device to all of the devices in the access group.

3. Select the check box next to each access group and click the **Remove** button.
4. Click the **Create** button.
5. Type a name for this access group in the **Name** field.
6. From the Device list, select from which to reimport the shared access policy configuration and click the **Reimport** button.

   This device will share the access policy configuration with all other devices in this access group.
7. Click the **Create** button at the bottom of the screen.
8. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
9. Click the name of the access group you added.
10. Click the **Add Device** button.
11. From the Device list, select a device to add to this access group.
12. Click the **Add** button at the bottom of the screen.
13. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
14. If the differences window displays for the APM service, click the **Accept** button.
15. Repeat these steps 10-14 for each device in each access group before creating the next access group.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.3.0.

Legal Notices

Legal notices

Publication Date

This document was published on October 12, 2017.

Publication Number

MAN-0671-00

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index

Index