F5 ®BIG-IQ® Centralized Management: Device

Version 5.1

Table of Contents

BIG-IQ Centralized Management Overview

About BIG-IQ Centralized Management

BIG-IQ® Centralized Management lets you centrally manage BIG-IP ® devices in several ways. From one location you can:

- Install new software images and configurations.
- Backup and restore configurations.
- Synchronize configurations between devices in a cluster.
- Distribute and monitor licenses and certificates.
- Keep an eye on the health of your devices.

Doing these tasks centrally from BIG-IQ saves you time because you don't have to go directly to a single BIG-IP device and log on and make changes only to that device. Instead, you can access devices remotely, and monitor and manage several devices at once.

Device Discovery and Basic Device Management

How do I start managing BIG-IP devices from BIG-IQ?

To start managing a BIG-IP® device, you must add it to the BIG-IP Devices inventory list on the BIG-IQ® system.

Adding a device to the BIG-IP Devices inventory is a two-stage process.

Stage 1:

- You enter the IP address and credentials of the BIG-IP device you're adding, and associate it with a cluster (if applicable).
- BIG-IQ opens communication (establishes trust) with the BIG-IP device.
- BIG-IQ discovers the current configuration for any selected services you specified are licensed on the BIG-IP system, like LTM® (optional).

Stage 2:

- BIG-IQ imports the licensed services configuration you selected in stage 1 (optional).

Note: *If you only want to do basic management tasks (like software upgrades, license management, and UCS backups) for a BIG-IP device, you do not have to discover and import service configurations.*

Adding devices to the BIG-IQ inventory

Before you can add BIG-IP® devices to the BIG-IQ® inventory:

- The BIG-IP device must be located in your network.
- The BIG-IP device must be running a compatible software version. Refer to *https://support.f5.com/kb/en-us/solutions/public/14000/500/sol14592.html* for more information.
- Port 22 and 443 must be open to the BIG-IQ management address, or any alternative IP address used to add the BIG-IP device to the BIG-IQ inventory. These ports and the management IP address are open by default on BIG-IQ.

If you are running BIG-IP version 11.5.1 up to version 11.6.0, you might need root user credentials to successfully discover and add the device to the BIG-IP devices inventory. Root user credentials are not required for BIG-IP devices running 11.5.0 - 11.5.1 and 11.6.0 - 12.x.

Note: *A BIG-IP device running versions 10.2.0 - 11.4.1 is considered a legacy device and cannot be discovered from BIG-IQ version 5.0. If you were managing a legacy device in previous version of BIG-IQ and upgraded to version 5.0, the legacy device displays as impaired with a yellow triangle next to it in the BIG-IP Devices inventory. To manage it, you must upgrade it to 11.5.0 or later. For instructions, refer to the section titled, Upgrading a Legacy Device.*

You add BIG-IP devices to the BIG-IQ system inventory as the first step to managing them.

Note: *The ADC component is automatically included (first) any time you discover or import services for a device.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.

3. At the top of the screen, click **Inventory**.
4. Click the **Add Device** button.
5. In the **IP Address** field, type the IPv4 or IPv6 address of the device.
6. In the **User Name** and **Password** fields, type the user name and password for the device.
7. If this device is part of a DSC group, from the **Cluster Display Name** list, select one of the following:

   - For an existing DSC group, select **Use Existing** from the list and select the DSC group from the list.
   - For a new DSC group, select **Create New** from the list and type a name in the field.

   For BIG-IQ to properly associate devices in the same DSC group, the **Cluster Display Name** must be the same for each member in a group.
8. If this device is configured in a DSC group, select an option:

   - **Initiate BIG-IP DSC sync when deploying configuration changes (Recommended)** Select this option if this device is part of a DSC group and you want this device to automatically synchronize configuration changes with other members in the DSC group.
   - **Ignore BIG-IP DSC sync when deploying configuration changes** Select this option if you want to manually synchronize configurations changes between members in the DSC group.
9. Click the **Add** button at the bottom of the screen.
   The BIG-IQ system opens communication to the BIG-IP device, and checks its framework.

   Note: *The BIG-IQ system can properly manage a BIG-IP device only if the BIG-IP device is running a compatible version of the REST framework.*
10. If a framework upgrade is required, in the popup window, in the **Root User Name** and **Root Password** fields, type the root user name and password for the BIG-IP device, and click **Continue**.
11. If in addition to basic management tasks (like software upgrades, license management, and UCS backups) you also want to centrally manage this device's configurations for licensed services, select the check box next to each service you want to discover.

    You can also select these service configuration after you add the BIG-IP device to the inventory.
12. Click the **Add** button at the bottom of the screen.

BIG-IQ displays a discovering message in the Services column of the inventory list.

If you discovered service configurations to manage, you must import them.

Importing service configurations for a device

You must add a device to the BIG-IP Device inventory list, and discover associated services, before you can import services to BIG-IQ for the device.

To manage a device's service configuration from BIG-IQ®, you must import the service configuration from the managed device to BIG-IQ.

Important: *You, or any other BIG-IQ system user, cannot perform any tasks on the BIG-IQ system while it is importing a service configuration. Large configurations can take a while to import, so let other BIG-IQ users know before you start this task.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Click the name of the device you want to import a service configuration from.
5. On the left, click **Services**.

6. For the device's configuration you are importing, select the **Create a snapshot of the current configuration before importing.** check box to save a copy of the device's current configuration.

   You're not required to create a snapshot, but it is a good idea in case you have to revert to the previous configuration for any reason.
7. Click the **Import** button next to the service you want to import to the BIG-IQ system.
   If the current configuration on the BIG-IQ is different than the one on the BIG-IP® device, BIG-IQ displays a screen for you to resolve the conflicts.
8. 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.

You can now manage the configuration of this service for this device from BIG-IQ.

Managing a device from the device properties screen

You can use a device's Properties screen to manage that device. You can log directly in to the device, remotely reboot it, and create an instant backup of its configuration. You can also view details about the managed device, such as:

- Host name
- Self IP Address
- Build Number
- Software Version
- Status
- Last Contact
- Management IP Address
- Cluster
- Boot Location

From this screen you can also perform the following tasks:

- Log directly into the device from BIG-IQ®.
- Reboot the device from BIG-IQ.
- Create an instant backup of the device's configuration.
- Associate the device to a cluster.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Click the name of the device you want to view.
   The device Properties screen opens.

Filtering the BIG-IP inventory list for specific BIG-IP components

With BIG-IQ®, you can easily search for specific sets of devices from one central location. For example, after you discover several devices, you might want to find a specific device by its name or IP address. To do this, you start by filtering on certain configuration objects. This centralized search saves time by displaying only those devices with the search criteria you specify.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.

4. To search for a specific object, in the **Filter** field at the top right of the screen, type all or part of an object's name and click the filter icon.
   BIG-IQ refreshes the screen to show only those devices that contain the object you filtered on.
5. To modify the filter to include or exclude certain objects, click the gear icon next to the **Filter** field and deselect or select objects.
6. To remove the filter, click the **X** icon next to it.

Exporting device inventory details to a comma separated values (CSV) file

To export the BIG-IP Device inventory to a CSV file, your browser must be configured to allow popup screens.

Using BIG-IQ®, you can quickly access and view the properties for all the devices you manage in your network. These properties include details about the device's IP addresses, platform type, license details, software version, and so forth. You (or another department in your company) can create custom reports containing this information to help manage these assets. To do this, you can export device properties to a CSV file and edit the data as required.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Click the **Export Inventory** button.

BIG-IQ creates a CSV file and downloads it locally.

What is a BIG-IP Device Service Clustering (DSC) group and how do I start managing it from BIG-IQ?

Device Service Clustering, or DSC®, is a BIG-IP® TMOS® feature that lets you organize BIG-IP devices in groups to share configurations. These groups are called *device service clusters* (also DSC). With BIG-IQ®, you can easily manage devices configured in a DSC from one centralized location.

Before you can manage BIG-IP systems configured in a DSC, you must:

- Add the DSC device members to the BIG-IP Devices inventory.
- Add the DSC group to the BIG-IP Clusters inventory.

When a device service cluster is in the BIG-IP Cluster inventory, you can view its properties and the devices within those groups, and synchronize their configurations, all without having to log in to each device individually.

Note: *For specific information about BIG-IP DSC groups, refer to the BIG-IP® Device Service Clustering: Administration guide.*

Discovering BIG-IP clusters

You must add the BIG-IP® devices configured in a DSC® to the BIG-IQ system's BIG-IP Device inventory before you can add any associated DSC cluster to the BIG-IP Cluster inventory.

All BIG-IP devices in a cluster must be running the same software version and the same settings for:

- Pools
- Traffic-groups
- VLANs
- Tunnels

- Route domains

The BIG-IQ® Clusters inventory screen shows you a centralized view specific to DSC clusters.

***Note:** The **Cluster Display Name** displays on this screen only for managed BIG-IP devices in a DSC.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IP CLUSTERS**.
5. Click the **Discover** button.
6. Select the devices in the **Available** list, and then click the right arrow to add them to the **Selected** list.

   This list is populated from the BIG-IP Device inventory list. If you can't see all of the available devices listed, left-click the right bottom corner of the list and use your cursor to expand the dialog box.
7. Click the **Discover** button.

If the BIG-IP devices are part of a DSC, the screen refreshes to show the BIG-IP cluster(s) you added.

Viewing the BIG-IP Clusters inventory and the properties of a DSC cluster

You must add a BIG-IP® device configured in a DSC® to the BIG-IP Devices inventory list, and discover the cluster from the BIG-IP Clusters inventory list before you can see the cluster listed on this screen.

Using the BIG-IP Clusters inventory screen, you can see the following details about each existing DSC cluster, including:

- synchronization status
- name
- cluster type
- last refresh dates

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IP CLUSTERS**.
5. To view the properties of a cluster, including the trust domain certificate associated with this DSC group, click the cluster's name.

Synchronizing configurations between BIG-IP devices in a DSC cluster

You must add a BIG-IP® device configured in a DSC® to the BIG-IP Devices inventory list and discover the cluster from the BIG-IP Clusters inventory list before you can synchronize BIG-IP devices configured in a DSC cluster.

Synchronizing configuration between BIG-IP devices in a DSC cluster saves you time because you don't have to log on to each BIG-IP device in the cluster individually.

***Important:** Unmanaged BIG-IP devices in a DSC do not display the **Sync** button.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IP CLUSTERS**.

5. Click the name of the cluster you want to synchronize.
6. Click the **Refresh Status** button to get the most current sync status for the devices in the DSC cluster.
7. For the **Sync Option** setting, select one of the options:
   - **Device to Group** - Select this option to prompt the BIG-IP device to synchronize its configuration with other device(s) in the DSC group.
   - **Group to Device** - Select this option to prompt the DSC group to load its configuration onto the BIG-IP device.
8. Click the **Sync** button.
9. To close the screen, click the **Close** button.

How can I organize the way devices display in BIG-IQ so they're easier to find and manage?

To more easily manage a large number of BIG-IP® devices, you can organize them into groups. The types of groups you can use are:

- Static groups
- Dynamic groups

A *static group* contains specific devices that you add to it, and those devices stay in that group until you remove them. For example you might want to create a static group named, `Seattle`, and add all of the devices located in Seattle to it.

In contrast, a *dynamic group* is basically a saved query on a group. For example, if you created a static group that contained all of your managed devices located in Seattle and you wanted to view only those devices running a specific application, you could create a dynamic group with that filter. If one of the devices stops running the specified application, the device no longer appears in that dynamic group.

If you delete a managed BIG-IP device from the parent group, you see that change when you view the dynamic group.

Creating a static group of managed devices

You must license and discover BIG-IP® devices before you can place them into a group.

To more easily manage a large number of devices, you can organize them into groups. For example, you could add devices to groups according to the running applications, geographical location, or department.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **DEVICE GROUPS**.
5. Click the **Add Group** button.
6. In the **Name** field, type the name you want to use to identify this group.

   You can change this name at any time, after you save this group.
7. In the **Description** field, type a description for this group.

   For example, `BIG-IP devices located in Seattle`.

   You can change this description at any time, after you save this group.
8. For the **Group Type** setting, select **Static**.
9. From the **Parent Group** list, select the source for the group you are creating.
10. For the **Available in Services** setting, select the services licensed for this device.

If this BIG-IP device is licensed for services you are not managing, you can reduce the number of devices displayed in the BIG-IP inventory by selecting the check box next to only the services you manage. If you are managing all aspects of BIG-IQ, select the check box next to each service running on this BIG-IP device.

11. From the **Hostname** list, select the device you want included in this group.

    To add additional devices, click the + sign and select a device from the new list that is displayed.
12. Click the **Save** button at the bottom of the screen.

If you want to further filter specific devices from within this group, you can create a dynamic group.

Creating a dynamic group of managed devices

You must create a static group before you can create a dynamic group.

To filter a static group on certain parameters, you can create a dynamic group. For example, if you have a static group for all devices located in a particular city, and you want to view only those running a specific version of software, you could create a dynamic group to filter on that version number.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. On the left, click **DEVICE GROUPS**.
4. Click the **Add Group** button.
5. In the **Name** field, type the name you want to use to identify this group.

   You can change this name at any time, after you save this group.
6. In the **Description** field, type a description for this group.
   For example, `BIG-IP Devices running version 12.0`

   You can change this description any time, after you save this group.
7. For the **Group Type** setting, select **Dynamic Group**.
8. From the **Parent Group** list, select the source for the group you are creating.
9. In the **Search Filter** field, type a term on which you want to filter the group.

   You can filter on a single term or, if you want to filter on more than one parameter, use the standard Open Data Protocol (OData) format.
10. For the **Available in Services** setting, select the services licensed for this device.

    If this BIG-IP device is licensed for services you are not managing, you can reduce the number of devices displayed in the BIG-IP inventory by selecting the check box next to only the services you manage. If you are managing all aspects of BIG-IQ, select the check box next to each service running on this BIG-IP device.
11. Click the **Save** button at the bottom of the screen.

This dynamic group reflects any changes made to the static group. For example, if a device is removed from its parent group, it no longer appears in the associated static group. Also, if a device no longer contains the object you filtered on, the device no longer displays in the dynamic group.

License Management

How do I manage software licenses for my devices?

A software license is specific to F5 product services (for example, BIG-IP® LTM®, BIG-IP APM®, and so forth), and is organized in a *license pool*. Each license pool contains a specific type of license. From BIG-IQ®Centralized Management, you can easily manage licenses in those pools for numerous devices. That means you don't have to log in to each individual BIG-IP VE device to activate, revoke, or reassign a license.

After you activate a pool license's registration key from BIG-IQ, you can assign the license to a managed, or unmanaged, BIG-IP VE device. If you assign a license from a license pool to a BIG-IP device and later decide you don't need that device licensed, you can revoke the license and assign it to another BIG-IP VE device. This process is similar to a library, where you loan (assign) a license to a BIG-IP device when it is required, and check the license back into the license pool on BIG-IQ (revoke it from the device) so it is available to assign to another BIG-IP VE. This flexible licensing model helps keep track of the licenses, and manage your operating costs.

Types of license pools

There are four types of license pools. You can assign, revoke, and reassign licenses from these pools as needed.

License Pool Type	Description
Purchased Pool	Prepaid pool of a specific number of concurrent license grants for a single BIG-IP® service. For example, a purchased pool of 25 licenses for BIG-IP® LTM® allows you to license up to 25 concurrent BIG-IP VE systems for LTM.
Utility Pool	Designed for service providers, utility pools contain licenses for BIG-IP services you grant for a specific unit of measure (hourly, daily, monthly, or yearly). This means you can pay for licenses as needed with no limit to the number of licenses you can grant. From BIG-IQ®Centralized Management, you can automatically submit a license usage report. F5 uses that report to calculate billing based on the licensed services, duration of the license grant, and the unit-of-measure pricing. To purchase a utility pool license, you must have a master service agreement.
Volume Pool	Prepaid subscription (1 and 3 year terms) for a fixed number of concurrent license grants for multiple BIG-IP services. To purchase a volume pool, you must have a master service agreement.
Registration Key Pool	A pool of single standalone BIG-IP VE registration keys for one or more BIG-IP services. Because you are managing these registration keys from BIG-IQ Centralized Management (instead of

License Pool Type	Description
	directly from the BIG-IP device), you can revoke and reassign a license to BIG-IP VE systems without having to contact F5 to allow the license to be moved.

Options for activating a pool license registration key

Activating a registration key is the first step to getting a BIG-IP® VE pool license onto F5® BIG-IQ® Centralized Management so you can start managing it. You can activate a registration key in these ways:

- Automatic - Use this procedure if BIG-IQ is connected to the public internet.
- Manual - Use this procedure if BIG-IQ is not connected to the public internet. If you are manually activating a volume or utility license, you must activate each offering individually.
- CCN - Use this procedure if BIG-IQ is in a closed-circuit network (CCN) that does not permit you to export any encrypted information. For this procedure, you must open a case with F5 Support.

Activate a purchased, volume, utility, or standalone registration key pool on a BIG-IQ connected to the internet (automatic method)

You get your base registration key from F5 Networks, typically in the form of an email.

You can use this procedure to automatically contact the F5 license server for activation if F5® BIG-IQ® Centralized Management system is:

- Connected to the public internet.
- Able to access the `activate.f5.com` site.
- Existing firewalls allow port 443 to pass through.

You activate a registration key for a purchased, volume, or utility pool license to get a BIG-IP license and make it available for assignment to BIG-IP® VEs in your network. When you activate a volume or pool license using this method, the BIG-IQ® Centralized Management system activates the associated offerings automatically.

1. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
2. At the top of the screen, click **Operations**.
3. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
4. Click the **New License** button.
5. In the **License Name** field, type a name to identify this license.
6. In the **Base Registration Key** field, type or paste the registration key, and into the **Add-on Keys** field, type or paste any associated add-on keys.
7. For the **Activation Method** setting, select **Automatic**.
8. Click the **Activate** button at the bottom of the screen.
9. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.

When the activation status displays as **Active**, you can assign a license from the pool to a BIG-IP® VE device.

Activate a purchased registration key pool license on a BIG-IQ not connected to the internet (manual method)

You get your base registration key from F5 Networks, typically in the form of an email.

Activate a registration key to get a BIG-IP pool license and make it available for assignment to BIG-IP® VEs in your network. If BIG-IQ® Centralized Management system is not connected to the public internet, you can use this procedure for activation, rather than automatically contacting the F5 license server.

1. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
2. At the top of the screen, click **Operations**.
3. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
4. Click the **New License** button.
5. In the **License Name** field, type a name to identify this license.
6. In the **Base Registration Key** field, type or paste the registration key, and into the **Add-on Keys** field, type or paste any associated add-on keys.
7. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
8. Select and copy the text displayed in the **Device Dossier** field.
9. Click the **Access F5 manual activation web portal** link.
   The F5 Product Licensing site opens.
10. Click the **Activate License** link.
11. Paste the dossier into the **Enter your dossier** text box and click the **Next** button.

    Alternatively, click the **Choose File** button and navigate to the location where you saved the dossier.
12. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
13. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
14. Click the **Activate** button at the bottom of the screen.

When the activation status displays as **Active**, you can assign a license from the pool to a BIG-IP® VE device.

Activate a volume or utility pool license on a BIG-IQ not connected to the internet (manual method)

You get your base registration key from F5 Networks, typically in the form of an email.

You activate a registration key to get a pool license to make it available for assignment to BIG-IP® VEs in your network. If the BIG-IQ® Centralized Management you're activating a license on is not connected to the public internet, you can activate the registration key using this manual procedure, rather than automatically contacting the F5 license server.

Volume and utility pool licenses contain *offerings*. Offerings are specific to the services based on F5 Networks' Good, Better, Best licensing structure. If you are manually contacting the F5 Networks license server to activate those registration keys, you must activate each associated offering individually.

1. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
2. At the top of the screen, click **Operations**.
3. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
4. Click the **New License** button.
5. In the **License Name** field, type a name to identify this license.
6. In the **Base Registration Key** field, type or paste the registration key, and into the **Add-on Keys** field, type or paste any associated add-on keys.
7. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
8. Select and copy the text displayed in the **Device Dossier** field.
9. Click the **Access F5 manual activation web portal** link.

The F5 Product Licensing site opens.

10. Click the **Activate License** link.
11. Paste the dossier into the **Enter your dossier** text box and click the **Next** button.

    Alternatively, click the **Choose File** button and navigate to the location where you saved the dossier.
12. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
13. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
14. Click the **Activate** button at the bottom of the screen.

    The license displays in the list as `Pending`.
15. Click the name of the license.
16. Click the name of a pending offering.
17. Copy the dossier.
18. Click the **Access F5 manual activation web portal** link.
    The F5 Product Licensing site opens.
19. Click the **Activate License** link.
20. Paste the dossier into the **Enter your dossier** text box and click the **Next** button.

    Alternatively, click the **Choose File** button and navigate to the location where you saved the dossier.
21. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
22. Click the **Activate** button at the bottom of the screen.
23. Repeat steps 17-23 for each pending offering.

When the activation status displays as **Active**, you can assign a license from the pool to a BIG-IP® VE device.

Create a registration key pool for standalone BIG-IP VE licenses

You create a registration key pool for standalone licenses to help you manage a group of standalone BIG-IP® VE registration keys.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
4. Click the **New RegKey Pool** button.
5. In the **Name** field, type a name to identify this pool.
6. In the **Description** field, type an optional description for this pool.
7. Click the **Save** button at the bottom of the screen.

The new standalone license key pool displays in the Licenses list.

You can now add registration keys to this pool.

Activate a standalone registration key on a BIG-IQ connected to the internet (automatic method)

You must have your base registration key before you can activate it. You get this from F5 Networks, typically in the form of an email. After you create a standalone registration key pool, you can add and activate registration keys for that pool.

You can automatically contact the F5 license server for activation if the F5® BIG-IQ® Centralized Management system meets these criteria:

- Is connected to the public internet.
- Is able to access the `activate.f5.com` site.
- Its existing firewalls allow port 443 to pass through.

You add and activate standalone registration keys to a registration key pool to make them available for assignment to BIG-IP® VE devices from BIG-IQ Centralized Management. This gives you the flexibility to assign and revoke licenses as needed for your managed devices, without requiring you to contact F5.

***Note:** You cannot re-activate (or import) registration keys from currently-active BIG-IP VE licenses. For devices in your network already licensed, contact F5 Support for assistance in transferring them to BIG-IQ for license management.*

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
5. Click on the name of the registration key pool you want to activate a license for.
6. Click the **Add RegKey** button.
7. In the **Registration Key** field, type or paste the registration key, and into the **Add-on Keys** field, type or paste an associated add-on keys.
8. For the **Activation Method** setting, select **Automatic**.
9. Click the **Activate** button at the bottom of the screen.
10. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.

When the activation status displays as **Active**, you can assign a license from the pool to a BIG-IP® VE device.

Activate a standalone registration key on a BIG-IQ not connected to the internet (manual method)

You must have your base registration key before you can activate it. You get this from F5 Networks, typically in the form of an email. After you create a standalone registration key pool, you can add and activate registration keys for that pool.

You add and activate standalone registration keys to a registration key pool to make them available for assignment to BIG-IP® VE devices from F5® BIG-IQ® Centralized Management. This gives you the flexibility to assign and revoke licenses as needed for your managed devices, without requiring you to contact F5. If your BIG-IQ system is not connected to the public internet, you can activate the registration key using this manual procedure, rather than automatically contacting the F5 license server.

***Note:** You cannot re-activate (or import) registration keys from currently-active BIG-IP VE licenses. For devices in your network already licensed, contact F5 Support for assistance in transferring them to BIG-IQ for license management.*

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
5. Click the **Add RegKey** button.
6. In the **Registration Key** field, type or paste the registration key, and into the **Add-on Keys** field, type or paste an associated add-on keys.
7. For the **Activation Method** setting, select **Manual**.

8. Select and copy the dossier.
9. Click the **Access F5 manual activation web portal** link.
   The F5 Product Licensing site opens.
10. Paste the dossier into the **Enter your dossier** text box and click the **Next** button.

    Alternatively, click the **Choose File** button and navigate to the location where you saved the dossier.
11. Click the **Activate License** link.
12. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
13. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
14. Click the **Activate** button at the bottom of the screen.

When the activation status displays as **Active**, you can assign a license from the pool to a BIG-IP® VE device.

Pool license assignment and revocation

Once you have activated a license on F5® BIG-IQ®Centralized Management, you can assign and revoke those licenses for your managed and unmanaged BIG-IP® VE devices in your network.

***Note:** Unmanaged devices are devices that are located in your network, but that are not in the BIG-IQ Centralized Management system's BIG-IP Inventory list.*

Assign a utility or volume pool license to a BIG-IP VE device

After you have activated a utility or volume pool license's registration key, you can assign it to a BIG-IP® VE device.

To assign a license to an unmanaged device in your network, you must have the device's admin user name and password.

You assign a pool license to a BIG-IP VE device to authorize the device to run F5 services that support your applications

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
5. Click the name of the license you want to assign to a device.
6. For utility or a volume license, click the **Offering** name.
7. Click the **License Devices** button.
8. For a managed devices, from the **Devices** list, select the device you want to license and move it to the **Member Devices** list.
9. For unmanaged devices (devices in your network, but you are not managing from BIG-IQ), type the device's address, user name, and password in the **Unmanaged Devices** section.
10. Click the **Assign** button at the bottom of the screen.

Revoke a utility or volume pool license from a BIG-IP VE device

Before you can revoke a utility or volume pool license for an unmanaged device in your network, you must have the device's admin user name and password.

When fewer devices are required for your applications, you can revoke licenses to reassign them to other BIG-IP® VE devices, as needed.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
5. Select the check box next to the device you want to remove a license from.
6. For an unmanaged device, you must type the admin user name and password in the popup screen.
7. Click the **Revoke** button at the bottom of the screen.

This license is now available for re-assignment to another BIG-IP VE device.

Change a pool license for a BIG-IP VE device

You must have activated and assigned a pool license to a BIG-IP® VE device before you can change the license.

F5®BIG-IQ® Centralized Management makes it easy to change a license offering on a BIG-IP VE as traffic increases, requirements for different services come up, or if you need to change the unit of measure for billing purposes for a utility pool license.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
5. Click the name of the device you want to change a license for.
6. Click the **Change License** button.
7. In the New Assignment area, from the **License Type** list, select the type of license pool you want to select another license from.
8. From **License** list, select the license you want to assign to this device.
9. If you selected a **Volume** or **Utility** pool for the **License Type**, select the **Offering** and **Unit of Measure** as well.
10. Click the **Assign** button at the bottom of the screen.

Pool license usage reports

Pool license usage reports give you insight into how you're using your pool licenses. You can run this report for both currently-assigned and previously-assigned pool licenses. These reports can help you budget for future license purchases. If you're using a utility license, a utility usage report provides F5 Networks the information it needs to accurately bill for your license usage.

Create an active usage report to see how the BIG-IP VE devices are currently licensed

You can create a usage report for licenses you have assigned to BIG-IP® VE devices.

Create an Active Usage report to see details about how the BIG-IP devices are currently licensed. This report is available in a downloadable CSV format to make it easy for you to reformat and share the information in any way you want.

1. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
2. At the top of the screen, click **Operations**.

3. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
4. Click the **Report** button at the top of the screen.
5. For the **Type** setting, select **Active Report**.
6. Select a license type from the list to narrow the results to that license type.
7. From the **Available** list, click the license you want to run a report for, and click the arrow to move it to the **Selected** list.
8. Click the **Download** button at the bottom of the screen to generate the report.

Create a historical usage report to see how the BIG-IP VE devices were licensed during a specific time period

You can create an historical usage report only for licenses that you have assigned to BIG-IP® VE devices.

You create an Historical Report to see how you've been using your licenses during a specific time period. This can help you plan and budget for future resources. This report is available in a downloadable CSV format to make it easy for you to reformat and share the information in any way you want.

1. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
2. At the top of the screen, click **Operations**.
3. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
4. Click the **Report** button at the top of the screen.
5. For the **Type** setting, select **Historical Report**.
6. Select a license type from the list to narrow the results to that license type.
7. From the **Available** list, click the license you want to run a report for, and click the arrow to move it to the **Selected** list.
8. In the Usage Period area, in the **Starting Date** and **Ending Date** fields, type the date range for the report. Alternatively, click the calendars and navigate to the dates.
9. Click the **Download** button and select an option to open the file, or save the file.

Create a utility pool license usage report and submit it to F5 Networks for billing

You must have assigned a utility license to a device before you can create a utility usage report for that license.

Note: *If F5®BIG-IQ® Centralized Management cannot access* `api.f5.com` *or pass traffic through port 443, you must manually submit the report to F5 Networks, instead of submitting automatically. For information about how to manually submit the report, contact F5 Support.*

You create and submit a utility pool license usage report to F5 for billing purposes, at the frequency specified in your license agreement.

Your first report includes all license activity (grants and revocations) from the time you activate the utility pool license to the day before the first report is generated. Reports that follow include all license activity that happened since the last report, up to the day before the current report is generated.

For example:

- If you activated your utility pool on 1-Jan-2016 and generate a report on 1-Feb-2016, the report includes all usage between 1-Jan-2016 and 31-Jan-2016, inclusive.
- If you generate another report on 1-Apr-2016, the report includes all usage between 1-Feb-2016 and 31-Mar-2016, inclusive.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.

3. At the top of the screen, click **Operations**.
4. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
5. Click the **Report** button at the top of the screen.
6. For the **Type** setting, select **Utility Billing Report**.
7. From the **Available** list, click the license you want to run a report for, and click the arrow to move it to the **Selected** list.
8. For the report options, select **Generate and automatically submit report to F5.**

   If you want to manually submit a report, contact F5 Support.
9. Click the **Submit** button at the bottom of the screen to create and submit the report to F5 Networks.

While BIG-IQ Centralized Management generates the report, the **Submit** button is not available (greyed out). When the report is successfully created and submitted to F5 Networks, it downloads to your local system and the **Submit** button becomes available. If the report fails to create properly, the system displays an error message.

BIG-IP Software Upgrades

How do I manage software for BIG-IP devices?

A key feature of BIG-IQ® is the ability to manage software images for multiple remote devices from one location. You can deploy software without having to log in to each individual BIG-IP® device.

There are three steps to managing software images for devices:

1. Download the software image from F5 Networks.
2. Upload the software image to BIG-IQ.
3. Install the software image on a device in the BIG-IP Device inventory in one of the following two ways:
   - Managed Device Upgrade - use this process for installing a software image on managed BIG-IP devices running version 11.5.0 or later.
   - Legacy Device Upgrade - use this process for installing a software image on BIG-IP devices running versions 10.2.4 to 11.4.1.

Note: *Before you can manage a legacy device running versions 10.2.0 - 11.4.1, you must upgrade the device to version 11.5.0 or later.*

Downloading a software image from F5 Networks

Downloading a software image from F5 Networks is the first step to making it available to install on a managed device.

1. Log in to the F5 Downloads site, `https://downloads.f5.com`, and click the **Find a Download** button.
2. Click the name of the product line.
3. Click the version of the product you want to download.
4. Read the End User License Agreement, and click the **I Accept** button if you agree with the terms.
5. Click the name of the file you want to download.
6. Click the name of the closest geographical location to you.
   The screen refreshes to display the progress of your download.

After you download the software image, you can upload it to BIG-IQ®.

Uploading a software image to BIG-IQ

Before you can upload a software image to BIG-IQ®, you must download it from the `https://downloads.f5.com` site.

You upload a software image to make it available to deploy to managed BIG-IP® devices.

Important: *To make sure the software image successfully uploads, don't log out of BIG-IQ or close the browser window until the software image name appears in the Software Image list.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.

4. On the left, click **SOFTWARE MANAGEMENT** > **Available Images**.
5. Click the **Upload Image** button.
6. Click the **Choose File** button and navigate to the location to which you downloaded the image, and click the **Open** button to upload it to BIG-IQ.
7. Click the **Upload** button.

   The screen refreshes to display the progress of the upload.

When BIG-IQ uploads the software, it verifies the image. This verification process can take several minutes. When BIG-IQ is finished uploading and verifying the image, the software image displays as `Verified` and is available for installation on a device.

Installing a software image onto a managed device

Before you can install a software image onto a device, you must download it from the F5 Downloads site, `https://downloads.f5.com`, and upload it to the BIG-IQ® system. To apply a hotfix, you must have the base software image (as well as the hotfix) uploaded to, and verified by, BIG-IQ.

***Note:** You can deploy software images only to BIG-IP® devices running version 11.5.0 or later. Refer to the Upgrading a legacy device section for specific instructions about upgrading devices running version 10.2.0 - 11.4.1.*

Install software images to your managed devices so the versions are up to date, and in sync. This helps you manage your network traffic more efficiently. When you install software images from BIG-IQ, you have the option to stage the software installation for deploying later, as well as the option to have the installation paused after the software image is copied to the device and before the device reboots. While the software installs on the BIG-IP devices, you can continue doing other tasks on the BIG-IQ system.

***Tip:** Install a software image during a maintenance window when you are not directing traffic to the target BIG-IP device.*

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **SOFTWARE MANAGEMENT** > **Available Images**.
5. Select the check box next to the software image you want to install and then click the **Managed Device Install** button at the top of the screen.
6. In the **Name** field, type a name to identify this installation.
7. For the **Options** setting, you can select any of the following:
   - If you want to copy the image to the device, but wait until later install it, select the check box next to :

     Pause after the software image is copied has been copied to devices.
   - If you want to wait to reboot the image to the new volume so you can verify the software installation, select the check box next to:

     Pause for reboot confirmation.
8. Click the **Add/Remove Devices** button to select devices to install this software on.
9. From the **Available** list, select the devices you want to upgrade and click **->** to move it to the **Selected** list.
10. When you're done adding devices to the **Selected** list, click the **Apply** button.
11. To set the location for where BIG-IQ installs this software image, select **Target Volume**.

12. To assign a new location to install the software image, select **New Volume** and type the volume and partition you want it installed.
13. If you want to set the target volume for all the BIG-IP devices you are upgrading, click the **Set Default Volume** button and select an option:
    - **Install at the next available volume** to install the software there.
    - **Volume Name** and type a new volume install the software there.
14. Click the **Run** button to start the installation immediately, or click the **Save** button to save this job for deploying at a later time.

The software installation deployment and its status display in the **Software Installations** list.

If you selected an option save the deployment or to pause the process at certain points, click the name of the software installation on the **Software Installation** list, and click the **Continue** button when you're ready to continue the software installation.

How do I upgrade the BIG-IP REST framework so I can manage it from BIG-IQ?

To properly communicate, BIG-IQ® and BIG-IP® devices must be running compatible versions of the REST framework. If the REST 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. If you upgraded BIG-IQ from version 4.6.0 to version 5.0, you must also upgrade the REST framework for all BIG-IP devices (not running version 12.0.0) currently in the BIG-IP Device inventory.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Hover over the yellow triangle to display a message to confirm that the reason it is yellow is because the REST framework for the device needs an update.
5. Select the check box next to the device you want to upgrade the framework for.
6. Click the **More** button, and select **Upgrade Framework**.
   A popup screen opens.
7. Into the fields, type the required credentials, and click the **Continue** button.
   A `REST Framework upgrade in progress` message displays.

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

Upgrading a legacy device (version 10.2.0 - 11.4.1)

Before you can upgrade a device, you must first download the software image from the F5 Downloads site, `https://downloads.f5.com` to the BIG-IQ® system. You need the root user name and password for the device to upgrade it.

A BIG-IP® device running versions 10.2.0 - 11.4.1 is considered a *legacy device*. You must upgrade a legacy device to version 11.5.0 or later before you can add it to the BIG-IP Device Inventory and start managing it from BIG-IQ.

If you were managing a device running versions 10.2.0 - 11.4.1 from a previous version of BIG-IQ, and upgraded to version 5.0, the device displays as impaired with a yellow triangle next to it in the BIG-IP Devices Inventory. To manage the legacy device, you must upgrade it to 11.5.0 or later.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.

3. At the top of the screen, click **Operations**.
4. On the left, click **SOFTWARE MANAGEMENT** > **Software Images**.
5. In the **Software Images** list, select the check box next to the image you want to install and click **Legacy Device Install** button at the top of the screen.
6. In the **Device IP Address** field, type the IP address for the legacy device that you want to upgrade.
7. In the **Admin User Name** and **Admin Password** fields, type the administrator's user name and password for this device.
8. In the **Root User Name** and **Root Password** fields, type the user name and password for the root user for this device.
9. Click the **Upgrade** button to start the upgrade.

When the upgrade to version 11.5.0 or later is complete, you can discover the device from BIG-IQ.

UCS File Backup and Restoration

How do I back up and restore a device's configuration?

The configuration details of managed devices (including the BIG-IQ® system itself) are kept in a compressed user configuration set (UCS) file. The UCS file has all of the information you need to restore a device's configuration, including:

- System-specific configuration files
- License
- User account and password information
- SSL certificates and keys

You can create a backup of a device's UCS file so that you can easily recover a configuration for a managed device.

Backing up a device's current configuration

Creating a backup (in the form of a UCS file) for all devices in your network, including the BIG-IQ system itself, on a regular basis allows you to easily restore a configuration if a system becomes unstable. It's a good idea to create a backup of a system immediately before performing a software upgrade or before you make a significant configuration changes.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Select the check box next to each device you want to create a backup for, click the **More** button and select **Back Up Now**.
5. Type a name to identify this backup, and an optional description for it.
6. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.

   If you save a copy of the SSL private key, you can reinstall it if the original one becomes corrupt.
7. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the passphrase.
8. Use the **Local Retention Policy** setting to specify how long you want to keep the backup file on BIG-IQ.

   - In the **Delete local backup copy** field, select the number of days to keep the backup copy before deleting it.
   - To keep copies of the backups indefinitely, select **Never Delete**.

   If you configured BIG-IQ to save backup files to a remote server and that server is unavailable during a scheduled backup, BIG-IQ ignores the local retention policy and retains the local copy of the backup file. This ensures that a backup is always available. To remove those local backups, you must delete them.
9. To keep copies of backups remotely on a SCP or SFTP server:

   a) For the **Archive** setting, select the **Store archive copy of backup** check box.
   b) For the **Location** setting, select **SCP** or **SFTP**.

c) In the **IP Address** field, type the IP address of the remote server where you want to store the archives.

d) In the **User Name** and **Password** fields, type the credentials to access this server.

e) In the **Directory** field, type the name of the directory where you want to store the archives on the remote server.

Storing a backup remotely means you can restore data to a BIG-IP device even if you can't access the archive in the BIG-IQ system directory.

Tip: *Archived copies of backups are kept permanently on the remote server you specify. If you want to clear space on the remote server, you have to manually delete the backups.*

10. Click the **Start** button at the bottom of the screen.

After the backup is created, it appears in the Backup Files list and you can restore a managed BIG-IP device. When BIG-IQ creates a backup, it saves it in the following format: **backup name_device name_time of backup.ucs**

Setting up a UCS backup schedule

It is important to create a UCS backup for your managed devices on a regularly scheduled basis, so that you can easily restore a recent configuration if necessary.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **BACKUP & RESTORE** > **Backup Schedules**.
5. Click the **Schedule Backup** button.
6. Type a name to identify this backup, and an optional description for it.
7. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.

   If you save a copy of the SSL private key, you can reinstall it if the original one becomes corrupt.
8. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the passphrase.
9. Use the **Local Retention Policy** setting to specify how long you want to keep the backup file on BIG-IQ.

   - In the **Delete local backup copy** field, select the number of days to keep the backup copy before deleting it.
   - To keep copies of the backups indefinitely, select **Never Delete**.

   If you configured BIG-IQ to save backup files to a remote server and that server is unavailable during a scheduled backup, BIG-IQ ignores the local retention policy and retains the local copy of the backup file. This ensures that a backup is always available. To remove those local backups, you must delete them.
10. For the **Backup Frequency** setting, select **Daily**, **Weekly**, or **Monthly** for the **Schedule Backup** to specify how often backups are created. Based on the frequency, you can then specify the days and time you want to create the backups..
11. For the **Start Date** setting, click the calendar and select the date you want BIG-IQ to start creating backups.
12. Select the **Groups** or **Individuals** option.
13. If you selected **Individuals**, from the **Available** list, click the individual devices you want to back up and **->** to move it to the **Selected** list.
14. To keep copies of backups remotely on a SCP or SFTP server:

a) For the **Archive** setting, select the **Store archive copy of backup** check box.
b) For the **Location** setting, select **SCP** or **SFTP**.
c) In the **IP Address** field, type the IP address of the remote server where you want to store the archives.
d) In the **User Name** and **Password** fields, type the credentials to access this server.
e) In the **Directory** field, type the name of the directory where you want to store the archives on the remote server.

Storing a backup remotely means you can restore data to a BIG-IP device even if you can't access the archive in the BIG-IQ system directory.

***Tip:** Archived copies of backups are kept permanently on the remote server you specify. If you want to clear space on the remote server, you have to manually delete the backups.*

15. Click the **Save** button

After the backup is created, it appears in the Backup Files list and you can restore a managed BIG-IP device. When BIG-IQ creates a backup, it saves it in the following format: `backup name_device name_time of backup.ucs`.

Restoring a device with a UCS backup file

You must create a backup UCS file before you can restore it to a device.

You restore a device's UCS configuration to reinstall, or to roll back to a previous version of the device's configuration, without having to recreate it.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **BACKUP & RESTORE** > **Backup Files**.
5. Select the check box next to the UCS backup file you want to restore.
6. Click the **Restore** button.

The BIG-IQ® system restores the saved UCS backup file to the device.

***Important:** If you restore a BIG-IP device with a backup that is older than its current configuration, any existing backups that are more recent no longer appear in the Backup Files list. Those files, however, are still stored in the `/shared/ucs_backups` directory until you delete them.*

Pausing and restarting a UCS backup schedule

If you need to make a change to a BIG-IP® device's configuration during a scheduled UCS backup, you can suspend the scheduled backup and restart it when you are finished changing the configuration.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **BACKUP & RESTORE** > **Backup Files**.
5. Select the check box next to the schedule you want to suspend.
6. Click the **Suspend Schedule** button.

BIG-IQ® suspends the UCS backup schedule until you restart the schedule.

To restart the scheduled UCS backup, select the device and click the **Restart Schedule** button.

SSL Certificate Monitoring

How do I monitor SSL certificate expiration dates for my managed devices?

When you manage BIG-IP® devices that load balance SSL traffic, you must monitor both their SSL traffic and SSL system certificates. *Traffic certificates* are server certificates that a device uses for traffic management tasks. *System certificates* are the web certificates that allow client systems to log in to the BIG-IP Configuration utility.

BIG-IQ® imports the certificates for every managed BIG-IP device you discover. This makes it easy to monitor the expiration dates all of your devices' SSL certificates from one location.

You can also:

- Set up alerts to let you know when a certain certificate is about to expire within a specified number of days.
- Download the data to a CSV file for reporting purposes.

Configuring SMTP for sending alerts

You must configure a DNS server before you can specify an SMTP server.

You set up an SMTP server to send email to alert certain people when a specific condition happens, such as when an SSL certificate is about to expire.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **LOCAL HOST SETTINGS** > **SMTP Configuration**.
5. Click the **Add** button at the upper right of the screen.
6. In the **Name** field, type a name for this SMTP configuration.
7. In the **SMTP Server Host** and **SMTP Server Port** fields, type the SMTP server and TCP port.

   By default, SMTP uses TCP 25.
8. In the **From Email Address** field, type the email address from which to send the alert email.
9. From the **Encryption** list, select the type of encryption to use for the email.
10. To require a user name and password, from the **Use Auth** list, select **Yes**, and type the required user name and password.
11. Click the **Save** button at the bottom of the screen.
12. For the **SMTP Email Recipients** setting, click the **Add** button.
13. In the **Name** and **Email Address** fields, type the name and the email address for the person you want to receive an email when a specified alert condition is met.
14. To add more recipients, click +.
15. When you're done adding email recipients for alerts, click the **Save** button at the bottom of the screen.
16. To verify that you can reach the server you configured, click the **Edit** button at the upper right of the screen, and click the **Test Connection** button.

    You must specify at least one email recipient to test the connection.

You can now set up the alert conditions that prompt the BIG-IQ® system to send an email when a certain event happens on a managed device.

Monitoring SSL certificate expiration dates

You must have discovered at least one device before any certificates display in the Certificate Management inventory.

You must also set up SMTP to receive notifications for alerts.

SSL certificates have a set expiration date, and do not renew automatically. So it is important to monitor the SSL certificate's expiration dates for your managed devices.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **CERTIFICATE MANAGEMENT**.
5. Click the **Alert Settings** button.
6. For the **Device Certificate Expiration** condition, select the **Enabled** check box, and in the **Threshold** field, type the number of days notice you want before the certificate expires.
7. To receive an alert when a certificate has expired, for the **Device Certificate Expired** setting, select the **Enabled** check box.
8. Click the **Save** button at the bottom of the screen.

If an SSL certificate is about to expire, or has expired, immediately contact the owner of the device.

Optimizing Configuration Management with Templates

About configuration templates

BIG-IQ® can manage multiple devices simultaneously. These devices can be located in several data centers that may be located in many different locations. To help you easily manage required configuration changes to DNS, NTP, SMTP, and Syslog for a large number of devices, you can use configuration templates.

To start, you create a configuration template, then deploy that template to certain devices. This can save a significant amount of time because you are not required to log in to each device individually to make configuration changes.

Creating a configuration template

You can create a configuration template to deploy a specific configuration to one or more managed devices. Centrally managing these deployments from BIG-IQ® Device eliminates the need to log in to each device individually to specify or update a configuration.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **CONFIG TEMPLATES** > **Templates**.
5. Click the **New Template** button at the top of the screen.
6. In the **Name** and **Description** fields, type a name and a short description to identify this template.
7. From the **Add New Object** list, select the object you want to add to this template, and then click the **Add** button.
   The screen refreshes to display the property fields for the object.
8. In each property field, define the new object property's values.

   You can add additional values for some properties by clicking the + sign next to the property field.

   For specific information about the configuration options for BIG-IP, refer to the BIG-IP system documentation.
9. For each property, select one of these conditions:

Option	Description
Fixed	The value you define for this option is fixed. A user cannot change this value when deploying the template.
Optional	The value you define for this option is the default. Users can leave this default or specify their own value when deploying the template.
Required	You do not define a value for this option. The users must specify a value when they deploy the template.

10. After you add all of the objects you want to this template, click the **Save** button at the bottom of the screen.

This template is now available for deployment to managed BIG-IP® devices.

Deploying a configuration template to managed devices

You must create a configuration template before you can deploy it to a managed device.

Deploying a configuration template saves time when you want to make a similar change to several managed BIG-IP® devices.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click **CONFIG TEMPLATES** > **Deployments**.
5. Click the **New Deployment** button at the top of the screen.
6. From the **Config Template** list, select the template you want to deploy.
7. In the **Name** field, specify the name for this configuration template deployment.
8. From the **Available** list, click the devices you want to deploy the configuration template to, and then click **->** to move it to the **Included** list.
9. Click the **Next** button at the bottom of the screen, navigating to the components required for this template, and specifying the configuration.
10. Click the **Deploy** button.

BIG-IQ® applies this configuration to the specified BIG-IP devices.

Determine DNS Sync Group Health

How do I check my sync group health?

Using the tools available on the BIG-IP® user interface, it can be difficult to determine the health of your DNS sync groups. When you use F5® BIG-IQ® Centralized Management to manage your DNS sync groups, the task becomes quite straightforward. You can do a quick health check, diagnose health issues, and even set up an alert to notify you if a sync group health issue occurs.

Check DNS sync group health

Before you can monitor the sync group health, you must add a BIG-IP® device configured in a DNS sync group to the BIG-IP Devices inventory list, and import the LTM® and DNS services.

When you use F5® BIG-IQ® Centralized Management to manage your DNS sync group, you can monitor the health status of the group. Sync group health relies on complete alignment of a variety of device configuration elements. Using BIG-IQ simplifies the process of determining the health of your DNS sync groups.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.

   Important: *You must log in as an Administrator to perform this task.*

2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IP CLUSTERS**.
5. Under **BIG-IP CLUSTERS**, select **DNS Sync Groups**.
   The screen displays the list of DNS sync groups defined on this device. An health indicator icon and a message describes the status of each group.
6. To view the general properties for a sync group, click the sync group name.

   Note: *For a list of Health Status error messages, refer to DNS sync group messages.*

   The screen displays the properties for the selected group. This screen shows an overview of your DNS sync group health. Under Status, you can see the current state (for example, `Required Services Down`, or `Health Check(s) Passed`) for each device in the group.
7. To view the health for an individual sync group member, click **Health** .
   The Health screen displays detailed information for each factor that contributes to the health of a DNS sync group. Following a definition of each factor, a Status row provides additional detail. For each indicator, the most serious issues impacting that indicator are listed first. Finally, if the status for a health indicator is not `Health Check(s) Passed`, the **Recommended Action** setting describes what you can do to correct the issue.
8. Resolve any reported issues on the managed devices, and then return to the DNS Sync Groups screen and click **Refresh Status**.
   Once you resolve all reported issues, the status for the DNS sync group changes to `Health Check(s) Passed`.

DNS sync group status messages

When BIG-IQ® Centralized Management completes health checks for a DNS sync group, an icon and a message display to indicate the current status. There are four icons, each with its own associated meaning.

Table 1: Health indicator icons

Icon	Meaning
🟢	Indicates that all health checks passed satisfactorily (green).
🔵	Indicates that the health status is unknown or uncertain (blue).
⚠	Indicates a warning, or that the group health is sub-optimal (yellow).
🔴	Indicates that a critical issue was found (red).

Table 2: Health indicator messages

Message	Health indicator color	Description	Corrective Action
Awaiting Sync	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP® device. If the configuration is not the same (for devices in the sync group and MCP), then the devices could handle traffic differently, depending on what the configuration differences are.	Recommended Action: Wait a few minutes for synchronization to each member to occur. If synchronization does not complete, refer to troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Certificate Expired	Red	BIG-IP DNS uses the device's Apache server certification to act as the server certification when establishing iQuery® connections. If this certificate expires, then all iQuery communication to and from this device is prevented. This indicator informs the DNS admin when one of the devices in a sync group has a device certificate that is near expiration, or is currently expired. This indicator only validates the expiration on the server certificate for each device. It does not examine the traffic certificates used in SSL profiles or DNSSEC certifications.	Renew the device certificate or import a new certificate. Related Solutions: SOL6353: Updating an SSL device certificate on a BIG-IP system.
Certificates Expiring	Yellow	The device certificate for this BIG-IP DNS device is near expiration. If the certificate expires, this BIG-IP DNS device will not be able to communicate with other BIG-IP devices using the iQuery protocol.	Either renew the device certificate or import a new certificate.

Message	Health indicator color	Description	Corrective Action
Changes Pending	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP device. If the configuration is not the same (for devices in the sync group and MCP), then the devices could handle traffic differently, depending on what the configuration differences are.	Recommended Action: Wait a few minutes for synchronization to each member to occur. If synchronization does not complete, refer to troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Collecting Data	Blue	Either the certificate has not yet been discovered by BIG-IQ or the device is unreachable.	If the certificate is the issue, the needed data should be collected automatically. If this condition persists, check the BIG-IQ logs for any error messages. If the device is unreachable, determine why BIG-IQ can not contact the BIG-IP device. There could be network issues, the device could be offline, or BIG-IQ Restjavad service could be is down.
Incompatible Device Versions	Red	A GTM sync group consists of one or more GTM devices. For sync to perform correctly, each device must have the same base version of TMOS installed. To determine the version of TMOS: view the version component of the output of `tmsh show sys version`.	Upgrade all BIG-IP devices in the sync group to the same version. Related Solutions: SOL8759: Displaying the BIG-IP Software Version. SOL13734: BIG-IP DNS

Message	Health indicator color	Description	Corrective Action
			synchronization group requirements.
Member Sync Disabled	Red	BIG-IP DNS devices have properties to control which sync group a device belongs to, and whether synchronization is enabled. A device can be a member of a sync group, but have synchronization disabled. Any changes made on a device on which synchronization is disabled cannot sync changes to the other devices. F5 recommends not having sync groups with synchronization disabled on some of the devices. We also recommend not making changes on devices if synchronization is disabled.	Enable synchronization on all devices in the group. Related Solutions: SOL13734: BIG-IP DNS synchronization group requirements.
Required Services Down	Red	For the BIG-IP DNS devices to be able to sync configuration changes, the following services (daemons) must be running on all the devices in the sync group: • `mcpd` • `gtmd` • `big3d` • `tmm` If any of these services is down, then configuration will not sync between the devices in the sync group. The sync group health is primarily concerned with reporting the health of only the sync group itself; not the health of the functionality provided by each device in the sync group.	Start stopped services Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.
Server Object Missing	Red	On the BIG-IP device, the DNS server objects define the IP address on which iQuery connections are made. There must be a server object for every DNS device in the sync group so that they can establish the necessary connections. This indicator validates that all devices have a server object, and that the necessary ports are open to allow the iQuery communication that happens over port 4353.	Verify that the DNS server objects have an associated self IP address. Related Solutions: SOL13734: BIG-IP DNS synchronization group requirements.
Syncing Changes	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP device. If the configuration is not the same	Recommended Action: Wait a few minutes for synchronization to each member to occur. If synchronization does not complete,

Message	Health indicator color	Description	Corrective Action
		(for devices in the sync group and MCP), then the devices could handle traffic differently, depending on what the configuration differences are.	refer to troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Unknown Device Availability	Blue	The BIG-IQ device must collect data from each device in a sync group to be able to determine if the overall sync group is healthy. If BIG-IQ cannot reach one of the devices, then it cannot detect changes that make the overall group unhealthy. If a device cannot be reached, then the group is marked as unhealthy because there is no other way to know the health of the group.	Determine and fix loss of device availability. Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.
Unreachable Devices	Red	The BIG-IQ device must collect data from each device in a sync group to be able to determine if the overall sync group is healthy. If BIG-IQ cannot reach one of the devices, then it cannot detect changes that make the overall group unhealthy. If a device cannot be reached, then the group is marked as unhealthy because there is no other way to know the health of the group.	Determine and fix loss of device availability. Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.

How do I set up an alert for DNS sync group issues?

You can configure a BIG-IQ® SMTP alert to send email notifications when specific DNS sync group issues occur.

The following issues can trigger an alert:

- A new health status is generated for a DNS sync group. For instance, you might have just discovered a new sync group.
- The overall health status changes. For example, a device group that was healthy becomes unhealthy.
- The primary indicator (the most significant reason for the group's current health status) changed. (For example, the group is still unhealthy, but the reason is different than before.)

You enable or disable DNS alerts from the **System Management** > **Alerts** screen. For detailed instructions on creating an SMTP alert, refer to *How do I set up BIG-IQ to work with SMTP?* in the *F5 BIG-IQ Centralized Management: Licensing and Initial Setup* guide on `support.F5.com`.

BIG-IP iHealth

What is iHealth?

iHealth® is a tool that helps you troubleshoot potential issues. It does this by analyzing configuration, logs, command output, password security, license compliance, and so on.

From F5® BIG-IQ® Centralized Management, you can create a snapshot of a configuration in the form of a QKView file and then upload it to the F5® iHealth service. The file is compared to the iHealth database, which contains known issues, common configuration errors, and F5 published best practices. F5 returns an iHealth report you can use to identify any potential issues that you need to attend to.

How do I get access to the F5 iHealth diagnostics server?

You must have a single sign on (SSO) to the F5® Support site before you can access the F5 iHealth® diagnostics server. To register, visit *https://login.f5.com/resource/login.jsp*

With access to the F5 iHealth diagnostics server you can upload QKView files and download iHealth reports. For this access, you must specify a F5 Support SSO user name and password on F5® BIG-IQ® Centralized Management.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, expand **BIG-IP iHealth** and click **Configuration**.
5. Click the **Add** button.
6. In the **Name** field, type a name to identify this user.
7. In the **Username** and **Password** fields, type this user's F5 Support SSO user name and password.
8. In the **Description** field, type an optional description for this user.
9. Click the **Test** button to verify you can reach the iHealth diagnostics site.
10. If you can successfully connect to the site, click the **Save** button to save this user.

You can now upload QKView files for managed devices to the F5 iHealth server to get iHealth reports.

Limit the number of simultaneous iHealth-related file transfers to and from BIG-IQ

If you want to save system resources, you can easily limit how much traffic is dedicated to file activity related to iHealth® if you need to. You do this by specifying a limit of simultaneous file transfers to and fromF5® BIG-IQ® Centralized Management.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, expand **BIG-IP iHealth** and click **Configuration**.
5. Click the **Edit** button near the top of the screen.
6. In the **QKView Transfer Limit** field, type the greatest number of QKView files you want to occur on BIG-IQ at one time.
7. Click the **Save** button at the bottom of the screen.

Troubleshoot issues for managed devices by uploading a QKView file to the F5 iHealth server

To upload a QKView file, you must have access to the F5 iHealth® server configured on BIG-IQ® Centralized Management.

You upload a QKView file to F5 to create an iHealth diagnostics report. You can use that report to troubleshoot any potential issues with a managed device.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, expand **BIG-IP iHealth** and click **New Upload**.
5. Click the **New Upload** button.
6. In the **Name** field, type a name to identify this task, and type an optional identifier in the **Description** field.
7. If you have (and want to associate) a support case number with this QKView file, type that into the **F5 Support Case**.

   This step is not required.
8. From the **Credential** list, select the credentials to log in to the iHealth diagnostic site.
9. Select BIG-IP devices to upload QKView files to the iHealth server by clicking the device in the **Available** field, and click **->** to move it to the **Selected** field.
10. Click the **Upload** button at the bottom of the screen.

When BIG-IQ finishes uploading the QKView file(s) to F5, it displays with a **Success** status in the uploads list. If the upload fails, the status displays as **Error**.

If the upload fails, click the report's **Name** link and view the error message for more information. After F5 successfully receives the QKView file, it creates an iHealth report, which you can download from the Reports screen.

Download an iHealth diagnostics report for BIG-IP devices

F5 creates a BIG-IP® iHealth® diagnostics report after you upload a managed device's QKView file to F5.

Downloading and reviewing a BIG-IP iHealth report for a device helps you troubleshoot any potential issues.

***Note:** The Reports screen displays a link only to the most recent BIG-IP iHealth report created for a device. The F5 iHealth server retains the report for approximately 5 days, after which it deletes the report, and the link from BIG-IQ® becomes invalid. This date is shown as the expiration date.*

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **Device Management** from the BIG-IQ menu.
3. At the top of the screen, click **Operations**.
4. On the left, click expand **BIG-IP iHealth** and click **Reports**.
5. In the **Report** column, click the **Download PDF** file link for the report you want.

F5® BIG-IQ® Centralized Management downloads the report you selected in the form of a PDF.

You can now open and review the BIG-IP iHealth diagnostics report.

Legal Notices

Legal notices

Publication Date

This document was published on April 14, 2017.

Publication Number

MAN-0498-06

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

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