F5 ®BIG-IQ® Centralized Management: Device

Version 5.2

Table of Contents

BIG-IQ Centralized Management Overview..... 5
About BIG-IQ Centralized Management..... 5

Device Discovery and Basic Device Management..... 7
How do I start managing BIG-IP devices from BIG-IQ?..... 7
Adding devices to the BIG-IQ inventory..... 7
Managing a device from the device properties screen..... 8
Filtering the BIG-IP device inventory list for specific BIG-IP components..... 9
Exporting device inventory details to a comma separated values (CSV) file..... 9
What is a BIG-IP Device Service Clustering (DSC) group and how do I start managing it from BIG-IQ?..... 9
Discover BIG-IP Device Service Cluster groups..... 10
Viewing the BIG-IP Clusters inventory and the properties of a DSC cluster..... 10
Synchronizing configurations between BIG-IP devices in a DSC cluster..... 11
How can I organize the way devices display in BIG-IQ so they're easier to find and manage?..... 11
Creating a static group of managed devices..... 11
Creating a dynamic group of managed devices..... 12

License Management..... 13
How do I manage software licenses for my devices?..... 13
Types of license pools..... 13
Options for activating a pool license registration key..... 14
Activate a purchased, volume, utility, or standalone registration key pool on a BIG-IQ connected to the internet (automatic method)..... 14
Activate a purchased registration key pool license on a BIG-IQ not connected to the internet (manual method)..... 14
Activate a volume or utility pool license on a BIG-IQ not connected to the internet (manual method)..... 15
Create a registration key pool for standalone BIG-IP VE licenses..... 16
Activate a standalone registration key on a BIG-IQ connected to the internet (automatic method)..... 16
Activate a standalone registration key on a BIG-IQ not connected to the internet (manual method)..... 17
Assign, revoke, and change a license or license pool..... 18
Assign a utility or volume pool license to a BIG-IP VE device..... 18
Revoke a utility or volume pool license from a BIG-IP VE device..... 18
Change a pool license for a BIG-IP VE device..... 19
Pool license usage reports..... 19
Create an active usage report to see how the BIG-IP VE devices are currently licensed..... 19
Create a historical usage report to see how the BIG-IP VE devices were licensed during a specific time period..... 20
Create a utility pool license usage report and submit it to F5 Networks for billing..... 20

BIG-IP Software Upgrades..... 23
How do I manage software for BIG-IP devices?..... 23

Downloading a software image from F5 Networks....23
Uploading a software image to BIG-IQ....23
Installing a software image onto a managed device....24
Upgrade the BIG-IP framework....25
Upgrading a legacy device (version 10.2.0 - 11.4.1)....25

SSL Certificates....27
How do I manage the local traffic SSL certificates for my BIG-IP devices from BIG-IQ ?....27
Convert an SSL certificate and key pair from unmanaged so you can deploy them to BIG-IP devices....27
Create a self-signed certificate on BIG-IQ for your managed devices....28
Pin a managed SSL certificate and key pair to a BIG-IP device....28
About managing CA-signed SSL certificates....29
About SSL certificates, keys, and PKCS #12 SSL archive files created outside of BIG-IQ....30

UCS File Backup and Restoration....33
How do I back up and restore a device's configuration?....33
Backing up a device's current configuration....33
Setting up a UCS backup schedule....34
Restoring a device with a UCS backup file....35
Pausing and restarting a UCS backup schedule....35

Optimizing Configuration Management with Templates....37
About configuration templates....37
Creating a configuration template....37
Deploying a configuration template to managed devices....37

Deploying Changes....39
How do I evaluate changes made to managed objects?....39
Evaluate configuration changes....39
How do I deploy changes made to managed objects?....42
Deploy configuration changes....42
Make an urgent deployment....42
Deploy to one device when a cluster member is down....45

Managing Configuration Snapshots....47
What is snapshot management?....47
Create a snapshot....47
Compare snapshots....47
Restore some objects from a snapshot....48
Restore all objects from a snapshot....50

Legal Notices....53
Legal notices....53

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 SSL certificates.
- Keep an eye on the health of your devices.
- Collect and review live and historical statistics.
- Search and view related objects across all devices for objects, users, tasks, profiles, and more with Global Search.

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 and 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 discover and add the device to the BIG-IP devices inventory. You don't need root user credentials for BIG-IP devices running 11.5.0 - 11.5.1 and 11.6.1 - 12.x.

Note: *A BIG-IP device running versions 10.2.0 - 11.5.0 is considered a legacy device and cannot be discovered from BIG-IQ version 5.2. If you were managing a legacy device in previous version of BIG-IQ and upgraded to version 5.2, 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. At the top of the screen, click **Devices**.
2. Click the **Add Device** button.
3. In the **IP Address** field, type the IPv4 or IPv6 address of the device.

4. In the **User Name** and **Password** fields, type the user name and password for the device.
5. If this device is part of a DSC pair, from the **Cluster Display Name** list, select one of the following:
   - For an existing DSC pair, select **Use Existing** from the list and select the name DSC group from the list.
   - To create a new DSC pair, select **Create New** from the list, and type a name in the field.

   For BIG-IQ to properly associate the two devices in the same DSC group, the **Cluster Display Name** must be the same for both members in a group.

   There can be only two members in a DSC group.
6. If this device is configured in a DSC pair, select an option:
   - **Initiate BIG-IP DSC sync when deploying configuration changes (Recommended)** Select this option if this device is part of a DSC pair and you want this device to automatically synchronize configuration changes with the other member 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 the two members in the DSC group.
7. 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.*
8. 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**.
9. 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 and then click **Continue**.

   You can also select these service configuration after you add the BIG-IP device to the inventory.
10. 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.

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
- Boot Location
- Cluster Properties

From this screen you can also perform the following tasks:

- Create an instant backup of the device's configuration.
- Change the boot location of the device.
- Edit cluster properties.
- Log directly into the device from BIG-IQ®.

- Reboot the device from BIG-IQ.
- Access details about the health of the device.
- Access statistics for the device (if applicable).
- Access services licensed for the device.

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to view.
   The device Properties screen opens.

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

From each BIG-IQ® screen that contains a list of objects, you can easily find specific objects. 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. Filtering on specific criteria saves you time because you can view only those objects associated with the criteria you specify.

1. At the top of the screen, click **Devices**.
2. 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.
3. 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. At the top of the screen, click **Devices**.
2. On the left, click **BIG-IP DEVICES**.
3. 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.*

Discover BIG-IP Device Service Cluster groups

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

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 DSC Groups 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.*

Important: *BIG-IQ supports only two BIG-IP system in a DSC.*

1. At the top of the screen, click **Devices**.
2. On the left, click **BIG-IP CLUSTERS** > **DSC groups**.
3. Click the **Discover** button.
4. 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.
5. Click the **Discover** button.

The DSC Groups list refreshes to display the discovered DSC group.

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 DSC Clusters inventory list before you can see the cluster listed on this screen.

From the DSC Groups inventory screen, you can see the following details about each existing DSC cluster, including:

- synchronization status
- name
- cluster type
- last refresh dates
- devices in the DSC group

1. At the top of the screen, click **Devices**.
2. On the left, click **BIG-IQ CLUSTERS** > **DSC Groups**.
   The screen displays the list of DSC groups defined on this device.

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 DSC from the DSC Groups inventory list before you can synchronize BIG-IP devices configured in a DSC.

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. At the top of the screen, click **Devices**.
2. On the left, click **BIG-IQ CLUSTERS** > **DSC Groups**.
   The screen displays the list of DSC groups defined on this device.
3. Click the name of the cluster you want to synchronize.
4. Click the **Refresh Status** button to get the most current sync status for the devices in the DSC group.
5. 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.
6. Click the **Sync** button.
7. 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. At the top of the screen, click **Devices**.

2. On the left, click **DEVICE GROUPS**.
3. Near the top of the screen, click the **Create** button.
4. 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.
5. 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.
6. For the **Group Type** setting, select **Static**.
7. From the **Parent Group** list, select the source for the group you are creating.
8. 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.
9. 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.
10. Click the **Save & Close** 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. At the top of the screen, click **Devices**.
2. On the left, click **DEVICE GROUPS**.
3. Click the **Add Group** button.
4. 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.
5. 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.
6. For the **Group Type** setting, select **Dynamic Group**.
7. From the **Parent Group** list, select the source for the group you are creating.
8. 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.
9. 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.
10. Click the **Save & Close** 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 of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
3. Click the **Add License** button.
4. In the **License Name** field, type a name to identify this license.
5. 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.
6. For the **Activation Method** setting, select **Automatic**.
7. Click the **Activate** button at the bottom of the screen.
8. 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 of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
3. Click the **Add License** button.
4. In the **License Name** field, type a name to identify this license.
5. 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.
6. 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.
7. Select and copy the text displayed in the **Device Dossier** field.
8. Click the **Access F5 manual activation web portal** link.
   The F5 Product Licensing site opens.
9. Click the **Activate License** link.
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. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
12. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
13. 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 of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT**.
3. Click the **Add License** button.
4. In the **License Name** field, type a name to identify this license.
5. 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.
6. 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.
7. Select and copy the text displayed in the **Device Dossier** field.
8. Click the **Access F5 manual activation web portal** link.
   The F5 Product Licensing site opens.
9. Click the **Activate License** link.

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. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
12. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
13. Click the **Activate** button at the bottom of the screen.

    The license displays in the list as `Pending`.
14. Click the name of the license.
15. Click the name of a pending offering.
16. Copy the dossier.
17. Click the **Access F5 manual activation web portal** link.
    The F5 Product Licensing site opens.
18. Click the **Activate License** link.
19. 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.
20. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
21. Click the **Activate** button at the bottom of the screen.
22. 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 Centralized Management with your admin user name and password.
2. At the top of the screen, click **Devices**.
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.

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 Centralized Management with your admin user name and password.
2. At the top of the screen, click **Devices**.
3. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
4. Click on the name of the registration key pool you want to activate a license for.
5. Click the **Add RegKey Pool** 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 **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 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 Centralized Management with your admin user name and password.
2. At the top of the screen, click **Devices**.
3. On the left, click **LICENSE MANAGEMENT** > **Licenses**.
4. Click the **Add RegKey Pool** button.
5. 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.
6. For the **Activation Method** setting, select **Manual**.
7. Select and copy the dossier.
8. Click the **Access F5 manual activation web portal** link.
   The F5 Product Licensing site opens.
9. 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.

10. Click the **Activate License** link.
11. Review the EULA, and if you agree with the terms, click the **Accept** button at the bottom of the screen.
12. Select the license and copy and paste it into the **License Text** field on BIG-IQ.
13. 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.

Assign, revoke, and change a license or license pool

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. At the top of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Click the name of the license you want to assign to a device.
4. For utility or a volume license, click the **Offering** name.
5. Click the **License Devices** button.
6. For a managed devices, from the **Devices** list, select the device you want to license and move it to the **Member Devices** list.
7. 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.
8. 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. At the top of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Select the check box next to the device you want to remove a license from.
4. For an unmanaged device, you must type the admin user name and password in the popup screen.
5. 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. At the top of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Select the check box next to the the name of the device you want to change a license for.
4. Towards the top of the screen, click the **Change License** button.
5. If this is an unmanaged device, into the **Username** and **Password** fields, type the BIG-IP system's administrator's user name and password.

   Unmanaged devices are devices that are located in your network, but are not in the BIG-IQ system's BIG-IP Inventory list. These fields do not display if this is a managed device.
6. In the New Assignment area, from the **License Type** list, select the type of license pool you want to select another license from.
7. From **License** list, select the license you want to assign to this device.
8. If you selected a **Volume** or **Utility** pool for the **License Type**, select the **Offering** and **Unit of Measure** as well.
9. 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 of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Click the **Report** button at the top of the screen.
4. For the **Type** setting, select **Active Report**.
5. Select a license type from the list to narrow the results to that license type.
6. 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.
7. 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 of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Click the **Report** button at the top of the screen.
4. For the **Type** setting, select **Historical Report**.
5. Select a license type from the list to narrow the results to that license type.
6. 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.
7. 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.
8. 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. At the top of the screen, click **Devices**.
2. On the left, click **LICENSE MANAGEMENT** > **Assignments**.
3. Click the **Report** button at the top of the screen.
4. For the **Type** setting, select **Utility Billing Report**.
5. 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.
6. For the report options, select **Generate and automatically submit report to F5.**

   If you want to manually submit a report, contact F5 Support.
7. 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. At the top of the screen, click **Devices**.
2. On the left, click **SOFTWARE MANAGEMENT** > **Software Images**.
3. Click the **Upload Image** button.

4. 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.
5. 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. At the top of the screen, click **Devices**.
2. On the left click **SOFTWARE MANAGEMENT** > **Software Installations**.
3. 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.
4. In the **Name** field, type a name to identify this installation.
5. 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.
6. Click the **Add/Remove Devices** button to select devices to install this software on.
7. From the **Available** list, select the devices you want to upgrade and click **->** to move it to the **Selected** list.
8. When you're done adding devices to the **Selected** list, click the **Apply** button.
9. To set the location for where BIG-IQ installs this software image, select **Target Volume**.
10. To assign a new location to install the software image, select **New Volume** and type the volume and partition you want it installed.
11. 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.

12. 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.

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 5.2, 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.

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

SSL Certificates

How do I manage the local traffic SSL certificates for my BIG-IP devices from BIG-IQ ?

BIG-IP® devices use traffic SSL certificates for secure communication. Certificates stored on BIG-IQ® Centralized Management are in one of the following states:

- *Unmanaged* - Each time you discover a BIG-IP device and import the LTM service, BIG-IQ imports the properties (metadata) of its SSL certificate and key pair, but not the actual certificate and key pair, themselves. These SSL certificates display as `Unmanaged` on BIG-IQ. You can monitor the expiration dates for unmanaged SSL certificates, and assign them to BIG-IP Local Traffic Manager™ `clientssl` or `serverssl` profiles (as long as the BIG-IP devices already have those SSL certificates on them), but you can't deploy unmanaged certificates to BIG-IP devices.
- *Managed* - A complete SSL certificate includes a public/private key pair. When you import an SSL certificate and key pair to BIG-IQ, it displays as `Managed`. You can assign these managed SSL certificates to Local Traffic Manager `clientssl` or `serverssl` profiles, and deploy them to BIG-IP devices.

From one centralized location, BIG-IQ makes it easy for you to request, import, and manage CA-signed SSL certificates, as well as import signed SSL certificates, keys, and PKCS #12 archive files created elsewhere. And if you want to create a self-signed certificate on BIG-IQ for your managed devices, you can do that too.

Once you've imported or created an SSL certificate and keys, you can assign them to your managed devices by associating them with a Local Traffic Manager `clientssl` or `serverssl` profile, and deploying it.

Convert an SSL certificate and key pair from unmanaged so you can deploy them to BIG-IP devices

When you discover a BIG-IP® device, BIG-IQ® Centralized Management imports its SSL certificates' properties (metadata), but not the actual SSL certificates and key pairs. These certificates display as `Unmanaged` on the BIG-IQ Certificates & Keys screen. This allows you to monitor each SSL certificate's expiration date from BIG-IQ, without having to log on directly to the BIG-IP device.

Convert an unmanaged SSL key certificate and key pair to managed so you can centrally manage it from BIG-IQ Centralized Management. This saves you time because you don't have to log on to individual BIG-IP devices to create, monitor, or deploy certificates.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Click the name of the unmanaged certificate.
4. For the Certificate Properties **State** setting, click the **Import** button and then:
   - To upload the certificate's file, select **Upload File** and click the **Choose File** button to navigate to the certificate file.
   - To paste the content of a certificate file, select **Paste Text** and paste the certificate's content into the **Certificate Source** field.
5. For the Key Properties **State** setting, click the **Import** button and then:

- To upload the key's file, select **Upload File** and click the **Choose File** button to navigate to the key file.
- To paste the content of a key file, select **Paste Text** and paste the key's content into the **Key Source** field.

6. Click the **Save & Close** button at the bottom of the screen.

The SSL certificate now displays as `Managed` on the Certificates & Keys screen.

You can now assign this SSL certificate and key pair to a Local Traffic Manager `clientssl` or `serverssl` profile, and deploy it to a BIG-IP device. For more information, refer to the topic titled *Deploying Changes*.

Create a self-signed certificate on BIG-IQ for your managed devices

Create a self-signed SSL certificate and key pair on BIG-IQ® Centralized Management so you can centrally manage it. This saves you time because you don't have to log on to individual BIG-IP® devices to create, monitor, or deploy certificates.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Near the top of the screen, click the **Create** button.
4. In the **Name** field, type a name for this certificate.
5. If the partition is anything other than `Common`, type it into the **Partition** field.
6. From the **Issuer** list, select **Self**.
7. Complete the details for this certificate.

Note: *A Subject Alternative Name is embedded in a certificate for X509 extension purposes. Supported names include email, DNS, URI, IP, and RID. For the* ***Subject Alternative Name*** *field, use the format of a comma-separated list of* `name:value` *pairs.*

---

8. In the Key Properties area, select the key type and size.
9. If the key is encrypted, from the **Key Security Type** list, select **Password** and type the password for the key in the **Key Password** field.

Important: *If you select* ***Normal****, BIG-IQ will store the key as unencrypted, which can put your data at risk.*

---

10. In the **Password** and **Confirm Password** fields, type and confirm the password for this key pair.
11. Click the **Save & Close** button at the bottom of the screen.

The certificate displays in the Certificates & Keys list.

You can now assign this SSL certificate and key pair to a Local Traffic Manager `clientssl` or `serverssl` profile, and deploy it to a BIG-IP device. For more information, refer to the topic titled *Deploying Changes*.

Pin a managed SSL certificate and key pair to a BIG-IP device

You can pin only managed SSL certificates and key pairs to a BIG-IP® device.

If you haven't yet assigned a managed SSL certificate and key pair to a profile, but you still want them to remain deployed to a BIG-IP device, you'll want to pin it to that device. This ensures BIG-IQ® Centralized Management doesn't delete the SSL certificate and keys from the device.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.

3. Click the name of the managed SSL certificate you want to assign to a BIG-IP device.
4. From the **Available** list, click the name of the BIG-IP device to which you want to assign this SSL certificate and move it to the **Selected** list.
5. When you're done selecting devices, click the **Save & Close** button at the bottom of the screen.

About managing CA-signed SSL certificates

You can create a Certificate Signing Request (CSR) directly from BIG-IQ® Centralized Management, so it's easy to create and renew CA-signed certificates for your BIG-IP® devices. BIG-IQ provides a centralized view into which BIG-IP devices have CA-signed certificates, and which are about to expire.

To create or renew a CA-signed SSL certificate, you:

- From BIG-IQ, create a Certificate Signing Request (CSR) for the SSL certificate.
- Send the CSR to your certificate authority (CA).
- Import the signed SSL certificate to BIG-IQ you received from your CA.

Create a CSR for a CA-signed certificate

You create a Certificate Signing Request (CSR) on BIG-IQ® Centralized Management as the first step to creating a CA-signed certificate.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Click the **Create** button.
4. In the **Name** field, type a name for this certificate.
5. If the partition is anything other than `Common`, type it into the **Partition** field.
6. From the **Issuer** list, select **Certificate Authority**.
7. Complete the details for this certificate.

   Note: *A Subject Alternative Name is embedded in a certificate for X509 extension purposes. Supported names include email, DNS, URI, IP, and RID. For the* ***Subject Alternative Name*** *field, use the format of a comma-separated list of* `name:value` *pairs.*

8. In the Key Properties area, select the key type and size.
9. If the key is encrypted, from the **Key Security Type** list, select **Password** and type the password for the key in the **Key Password** field.

   Important: *If you select* ***Normal****, BIG-IQ will store the key as unencrypted, which can put your data at risk.*

10. Complete any required Certificate Signing Request Attributes.
11. Click the **Save & Close** button at the bottom of the screen.

BIG-IQ creates the CSR and the key pair.

Submit the CSR to your CA for a signature. When you receive the signed certificate back from your CA, you can import it to BIG-IQ to start managing it.

Import a CA-signed SSL certificate to BIG-IQ for your managed devices

After you submit a CSR from BIG-IQ® Centralized Management, your CA sends you a CA-signed SSL certificate.

You import the signed CA-signed certificate and key pair to BIG-IQ so you can centrally manage the certificate from BIG-IQ. This saves you time because you don't have to log on to individual BIG-IP® devices to monitor or deploy certificates.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Near the top of the screen, click the **Import** button.
4. From the **Import Type** list, select **Certificate**.
5. Select **Create New**.
6. For the **Certificate Source** setting:
   - To upload the certificate's file, select **Upload File** and click the **Choose File** button to navigate to the certificate file.
   - To paste the content of the certificate file, select **Paste Text** and paste the certificate's content into the **Certificate Source** field.
7. Click the **Import** button at the bottom of the screen.

You can now assign this SSL certificate and key pair to a Local Traffic Manager `clientssl` or `serverssl` profile, and deploy it to a BIG-IP device. For more information, refer to the topic titled *Deploying Changes*.

About SSL certificates, keys, and PKCS #12 SSL archive files created outside of BIG-IQ

There might be some cases where you've created an SSL certificate, key, or a PKCS #12 SSL archive file on a system other than BIG-IQ® Centralized Management. In those cases, you can easily import the certificates, keys, and files to BIG-IQ so you can centrally manage them for your BIG-IP® devices.

Import an SSL certificate so you can deploy it to a BIG-IP device

You can import an SSL certificate to BIG-IQ® Centralized Management that you created on another system so you can manage it.

1. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
2. Near the top of the screen, click the **Import** button.
3. From the **Import Type** list, select **Certificate**.
4. If the partition is anything other than `Common`, type it into the **Partition** field.
5. For the **Certificate Name** setting, select **Create New** or **Overwrite Existing**.
6. If you selected **Overwrite Existing**, select the certificate you want to overwrite.
7. For the **Certificate Source** setting:
   - To upload the certificate's file, select **Upload File** and click the **Choose File** button to navigate to the certificate file.
   - To paste the content of the certificate file, select **Paste Text** and paste the certificate's content into the **Certificate Source** field.
8. Click the **Import** button at the bottom of the screen.

The certificate displays in the Certificates & Keys list.

You can now import the key for this certificate.

Import a key for an SSL certificate so you can deploy it to a BIG-IP device

After you import a certificate to BIG-IQ® Centralized Management, you can import its associated key pair.

Import a key pair for an SSL certificate you created on a different system so you can centrally manage the certificate from BIG-IQ. This saves you time because you don't have to log on to individual BIG-IP® devices to monitor and deploy certificates.

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

2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Near the top of the screen, click the **Import** button.
4. From the **Import Type** list, select **Key**.
5. If the partition is anything other than `Common`, type it into the **Partition** field.
6. For the **PKCS12 Name** setting, select **Create New** or **Overwrite Existing**.
7. If you selected **Overwrite Existing**, select the key you want to overwrite.
8. For the PKCS12 Source setting, click the **Choose File** button to navigate to the file.
9. If the file is encrypted, into the **PKCS12 Password** field, type the password for the file.
10. If the key is encrypted, into the **Key Password** field, type the password for the key.
11. Click the **Import** button at the bottom of the screen.

The PKCS12 file displays in the Certificates & Keys list.

Import a PKCS #12 SSL archive file so you can deploy it to a BIG-IP device

Import a PKCS #12 SSL archive file you created on another system to BIG-IQ® Centralized Management to centrally manage it. This saves you time because you don't have to log on to individual BIG-IP® devices to monitor or deploy it.

1. At the top of the screen, click **Configuration**.
2. On the left, click **LOCAL TRAFFIC** > **Certificate Management** > **Certificates & Keys**.
3. Near the top of the screen, click the **Import** button.
4. From the **Import Type** list, select **PKCS#12**.
5. For the **PKCS12 Name**, select **Create New** or **Overwrite Existing**.
6. If you selected **Overwrite Existing**, select the file you want to overwrite.
7. For the **PKCS12 Source** setting, select **Upload File** and **Choose File** to navigate to the file.
8. In the **PKCS12 Password** field, type the password.
9. If the key is encrypted, from the **Key Security Type** list, select **Password** and type the password for the key in the **Key Password** field.

   Important: *If you select **Normal**, BIG-IQ will store the key as unencrypted, which can put your data at risk.*

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

The certificate displays in the Certificates & Keys list.

You can now assign this SSL certificate and key pair to a Local Traffic Manager `clientssl` or `serverssl` profile, and deploy it to a BIG-IP device. For more information, refer to the topic titled *Deploying Changes*.

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. At the top of the screen, click **Devices**.
2. Select the check box next to each device you want to create a backup for, click the **More** button and select **Back Up Now**.
3. Type a name to identify this backup, and an optional description for it.
4. 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.
5. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the passphrase.
6. 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**.
7. 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.

If you configure 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.

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.*

8. 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. At the top of the screen, click **Devices**.
2. On the left, click **BACKUP & RESTORE** > **Backup Schedules**.
3. Near the top of the screen, click the **Create** button.
4. Type a name to identify this backup, and an optional description for it.
5. 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.
6. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the passphrase.
7. 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**.
8. 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..
9. For the **Start Date** setting, click the calendar and select the date you want BIG-IQ to start creating backups.
10. Select the **Groups** or **Individuals** option.
11. 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.
12. 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.

If you configure 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.

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.*

13. 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. At the top of the screen, click **Devices**.
2. On the left, click **BACKUP & RESTORE** > **Backup Files**.
3. Select the check box next to the UCS backup file you want to restore.
4. 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. At the top of the screen, click **Devices**.
2. On the left, click **BACKUP & RESTORE** > **Backup Files**.
3. Select the check box next to the schedule you want to suspend.
4. 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.

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. At the top of the screen, click **Devices**.
2. On the left, click **CONFIG TEMPLATES** > **Templates**.
3. Near the top of the screen, click the **Create** button.
4. In the **Name** and **Description** fields, type a name and a short description to identify this template.
5. 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.
6. 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.
7. 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.

8. After you add all of the objects you want to this template, click the **Save & Close** 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. At the top of the screen, click **Devices**.
2. On the left, click **CONFIG TEMPLATES** > **Deployments**.
3. Near the top of the screen, click the **Create** button.
4. From the **Config Template** list, select the template you want to deploy.
5. In the **Deployment Name** field, specify the name for this configuration template deployment.
6. 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.
7. Click the **Next** button at the bottom of the screen, navigating to the components required for this template, and specifying the configuration.
8. Click the **Deploy** button.

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

Deploying Changes

How do I evaluate changes made to managed objects?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Evaluating the changes you have made is the third step in this process.

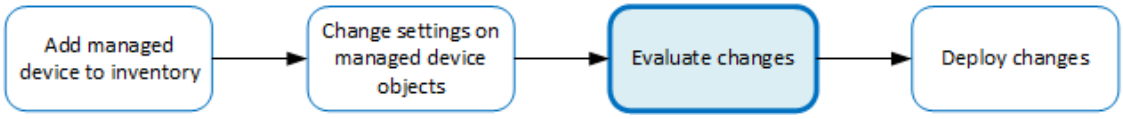


Figure 1: Overview of evaluating changes made to managed objects

---

Note: *If you need to make an urgent change, you can skip the evaluation step. However, we highly recommend evaluation in all but emergency situations. See Making an urgent deployment for details.*

Evaluate configuration changes

Evaluating your changes gives you a chance to spot critical errors and review your revisions one more time before deploying them.

Note: *When BIG-IQ® Centralized Management evaluates configuration changes, it first re-discovers the configuration from the managed device to ensure that there are no unexpected differences. If there are issues, the default behavior is to discard any changes made on the managed device, and then deploy the configuration changes.*

- To accept the default, proceed with the evaluation. The settings from the managing BIG-IQ overwrite the settings on the managed BIG-IP® device.
- To override the default, re-discover the device and re-import the service. The settings from the managed BIG-IP device overwrite any changes that have been made using the BIG-IQ.

Note: *Critical errors are issues with a configuration change that cannot be deployed successfully. Verification warnings are less serious in that they might not cause the deployment to fail, but you should review them,nonetheless.*

Note: *If you have Local Traffic & Network (LTM) changes to deploy, deploy the LTM changes before deploying changes to other components, or those deployments might fail.*

---

1. At the top of the screen, click **Deployment**.
2. Under **EVALUATE & DEPLOY**, select the component for which you want to make changes.
   The screen displays a list of evaluations and deployments defined on this device.
3. Under Evaluations, click **Create**.
   The New Evaluation screen opens.
4. In the **Name** field, type in a name for the evaluation task you are creating.
5. In the **Description** field, type in a brief description for the evaluation task you are creating.
6. For the **Source**, select what you want to evaluate.

- To compare the object settings currently on the managed device with the object settings in the pending version, select **Current Changes**.
- To compare the object settings currently on the managed device with the object settings in a stored snapshot, select **Existing Snapshot**, then choose the snapshot you want to use.

7. Unless you are evaluating changes for Access, determine the **Source Scope**; that is, choose whether you want to evaluate all of the changes from the selected source, or specify which changes to evaluate. Select either **All Changes** or **Partial Changes**.

   If you select **Partial Changes**, the screen displays additional controls.

   a) For a partial deployment, click **Add** to specify the configuration objects you want to include in the evaluation. A popup screen opens.

   Note: *If you include objects in an evaluation that have not been changed, and you later deploy this evaluation, the unchanged objects are not deployed to your BIG-IP device. Only objects that have been changed are deployed.*

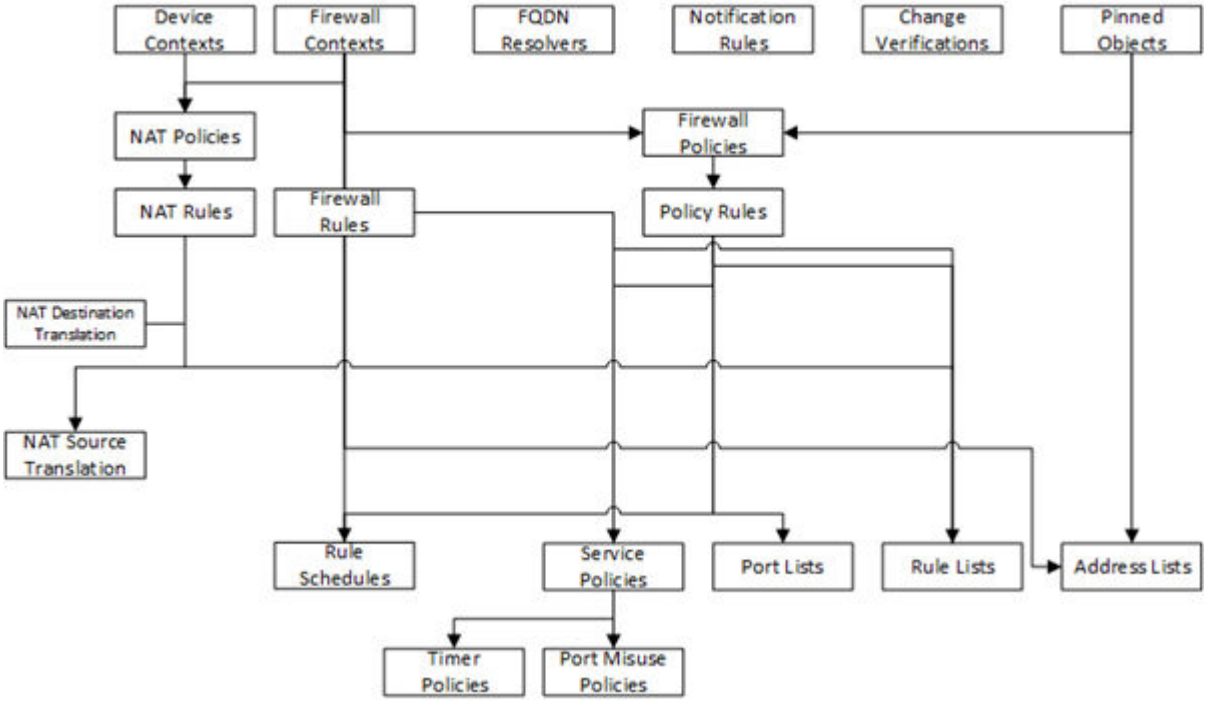
   b) On the **Available** tab, select the object type for which you want to evaluate changes.
   c) From the list of configuration changes, select the objects that you want to evaluate and click **Add**.
   d) If there are additional object types you want to include in this evaluation, repeat the last two sub-steps for each object type.
   e) If you add an object to the evaluation and then change your mind, you can click the **Selected** tab, select the object, and click **Remove**.
   f) When you have added all of the changes that you want to include in this evaluation, click **Save**.

   The objects you selected for inclusion are listed under Source Objects.

8. For **Supporting Objects**, your options depend on the component you are deploying changes for.

Option	Description
For Access	Clear the **Include associated LTM Objects** check box if you want to deploy changes only to the selected Access objects. It is almost always best to deploy changes to the associated local traffic objects as well.
For Network Security or Local Traffic & Network	If you are deploying only partial changes, clear the **Include** check box if you want to deploy changes only to the selected objects. It is almost always best to deploy changes to the associated objects as well.
For Web Application Security	Supporting objects are always included.

Note: *The objects that you manage using BIG-IQ depend on associations with other, supporting objects. These object associations form relationship trees that are sometimes quite complex. Generally, when you deploy a change to a managed object, it is a very good idea to include these supporting objects in the deployment. This diagram illustrates a typical relationship tree for a Network Services managed object. For Local Traffic or Web Application Security objects, the trees are equally complex and just as vital to include.*



9. Using the **Target Devices** settings, identify the devices for which you want to evaluate changes.
   a) If the devices are in a device group, select **Group**, and select the group from the list.
   b) If the devices are not in a device group, select **Device**.
   c) Select the devices from the **Available** list, and move the devices to the **Selected** list.

   Important: *If you deploy changes to a device that is in a DSC® cluster, you must include both devices before you can create the evaluation.*

   Important: *If the device in the* ***Selected*** *list has a filled circle in front of it, a deployment is needed for the BIG-IP device configuration to match the BIG-IQ working configuration for that BIG-IP device. This notification occurs only when creating Web Application Security evaluations.*

10. If you decide you want to remove one of the objects selected for deployment, you can select it and then click **Remove**.
11. Click the **Create** button at the bottom of the screen.
    The system adds the new evaluation to the list, and analyzes the changes for errors. When the configuration evaluation completes, you see how many changes or errors the evaluation found.
12. Review the evaluation to determine whether you are going to deploy it or not.
    a) If there are critical errors, you cannot deploy these changes. Click each error to see what it is, and then go back to where you made the change to fix it.

       After resolving any critical errors, you can come back and repeat the evaluation.
    b) If there are verification warnings, you can still deploy your changes, but you will probably want to resolve the warnings first. Click each warning to see what it is, and then go back to where you made the change to fix it.

       After resolving any verification warnings, you can come back and repeat the evaluation.
    c) If there are no critical errors or verification warnings, review the changes by clicking the **view** link.

       Each change is listed. You can review each one by clicking the name.
    d) When you finish reviewing the differences, click **Cancel**.

To apply these just-evaluated object changes to the managed device, they must be deployed. Refer to *Deploy configuration changes* for instructions.

How do I deploy changes made to managed objects?

Deploying changes applies the revisions that you have made on the BIG-IQ® Centralized Management system to the managed BIG-IP® devices.

This figure illustrates the workflow you perform to manage the objects on BIG-IP devices. Deploying the settings is the last step in this process.

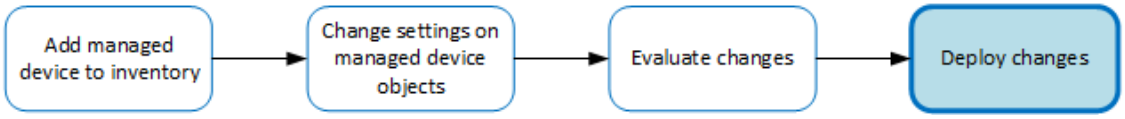


Figure 2: Change managed object workflow

Deploy configuration changes

To apply the changes you made on the BIG-IQ® Centralized Management system to your managed device, you must deploy those changes to the managed device.

1. At the top of the screen, click **Deployment**.
2. Under **EVALUATE & DEPLOY**, select the component for which you want to make changes.
   The screen displays a list of evaluations and deployments defined on this device.
3. Click the name of the evaluation that you want to deploy.
   The View Evaluation screen opens.
4. Specify whether you want to deploy the changes immediately or schedule deployment for later.
   - To deploy this change immediately:
     1. Select **Deploy Now**.
     2. Click **Deploy** to confirm.
   - To deploy this change later:
     1. Select the **Schedule for later** check box.
     2. Select the date and time.
     3. Click **Schedule Deployment**.

   The process of deploying changes can take some time, especially if there are a large number of changes. During this time, you can click **Cancel** to stop the deployment process.

   Important: *If you cancel a deployment, some of the changes might have already deployed.* ***Cancel*** *does not roll back these changes.*

The evaluation you chose is added to the list of deployments on the bottom half of the screen.

- If you chose to deploy immediately, the changes begin to deploy and the Status column updates as it proceeds.
- If you choose to delay deployment, the Status column displays the scheduled date and time.

Make an urgent deployment

If you need to make an urgent change, you can skip the *Evaluate configuration changes* task and deploy changes to your BIG-IP® device immediately. Changes to configuration objects are still validated; if there are critical errors, the deployment does not proceed. But you can avoid the task of creating an evaluation and viewing the changes and get right to deploying your changes.

Note: *Making a deployment without evaluating the changes first is not generally recommended. However, in situations where you need to deploy changes as quickly as possible, you can deploy the changes right away. The urgent deployment work flow skips the task of creating an evaluation, which speeds up the process of deploying your changes.*

1. At the top of the screen, click **Deployment**.
2. Under **EVALUATE & DEPLOY**, select the component for which you want to make changes.
   The screen displays a list of evaluations and deployments defined on this device.
3. Under Deployments, click **Create**.
   The New Deployment screen opens.
4. In the **Name** field, type in a name for the deployment task you are creating.
5. In the **Description** field, type in a brief description for the deployment task you are creating.
6. For the **Source** setting, select what you want to deploy.
   - To deploy your changes to the managed device, select **Current Changes**.
   - To deploy the object settings from a stored snapshot, select **Existing Snapshot**, then choose the snapshot you want to use.
7. Unless you are evaluating changes for Access, determine the **Source Scope**; that is, choose whether you want to evaluate all of the changes from the selected source, or specify which changes to evaluate. Select either **All Changes** or **Partial Changes**.

   If you select **Partial Changes**, the screen displays additional controls.

   a) For a partial deployment, click **Add** to specify the configuration objects you want to include in the evaluation. A popup screen opens.

   Note: *If you include objects in an evaluation that have not been changed, and you later deploy this evaluation, the unchanged objects are not deployed to your BIG-IP device. Only objects that have been changed are deployed.*

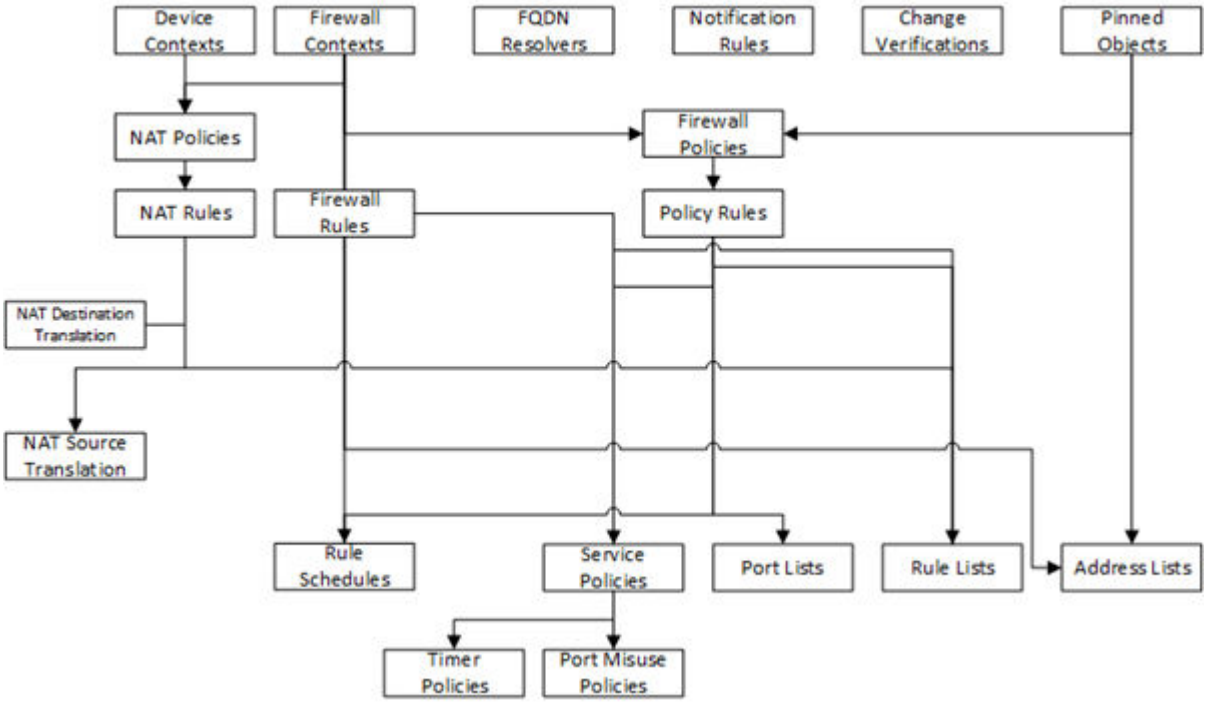
   b) On the **Available** tab, select the object type for which you want to evaluate changes.
   c) From the list of configuration changes, select the objects that you want to evaluate and click **Add**.
   d) If there are additional object types you want to include in this evaluation, repeat the last two sub-steps for each object type.
   e) If you add an object to the evaluation and then change your mind, you can click the **Selected** tab, select the object, and click **Remove**.
   f) When you have added all of the changes that you want to include in this evaluation, click **Save**.

   The objects you selected for inclusion are listed under Source Objects.
8. For **Supporting Objects**, your options depend on the component you are deploying changes for.

Option	Description
For Access	Clear the **Include associated LTM Objects** check box if you want to deploy changes only to the selected Access objects. It is almost always best to deploy changes to the associated local traffic objects as well.
For Network Security or Local Traffic & Network	If you are deploying only partial changes, clear the **Include** check box if you want to deploy changes only to the selected objects. It is almost always best to deploy changes to the associated objects as well.
For Web Application Security	Supporting objects are always included.

Note: *The objects that you manage using BIG-IQ depend on associations with other, supporting objects. These object associations form relationship trees that are sometimes quite complex.*

Generally, when you deploy a change to a managed object, it is a very good idea to include these supporting objects in the deployment. This diagram illustrates a typical relationship tree for a Network Services managed object. For Local Traffic or Web Application Security objects, the trees are equally complex and just as vital to include.



9. If you decide you want to remove one of the objects selected for deployment, you can select it and then click **Remove**.
10. Consider one more time how you want to deploy these changes.
    - If you want to review the changes, click **Create evaluation**.
    - To make the changes right now, click **Deploy immediately**.
11. Using the **Target Devices** settings, identify the devices for which you want to deploy changes.
    a) If the devices are in a device group, select **Group**, and select the group.
    b) If the devices are not in a device group, select **Device**.
    c) Select the devices from the **Available** list and use the arrow button to move the devices to the **Enabled** list.
12. Start the evaluation or deployment.

When you choose this Method:	Perform these steps
Create evaluation	1. Click **Evaluate**. 2. The evaluation begins. • If you are deploying changes for a specific object, when the evaluation is complete you can decide how and when you want to deploy it. • If you are deploying changes to a number of devices, the evaluation is added to the Evaluations list with a status of `Pending confirmation`.
Deploy immediately	1. Click **Deploy**.

When you choose this Method:	Perform these steps
	2. A confirmation screen notifies you that you are about to trigger a deployment. 3. Click **Deploy** again to deploy the changes to your device.

Deploy to one device when a cluster member is down

Deploying changes to a device in a cluster that has a device offline will generally fail. Normally, all device members must be available before you deploy changes to a cluster member. However, if you need to deploy changes before all cluster members are available you can do so.

1. At the top of the screen, click **Devices**.
2. Under Device Name, click the cluster member to which you want to deploy changes.
   The properties screen for this member opens.
3. Under Cluster Properties, click **Edit**.
   The Cluster Properties popup screen for this cluster opens.
4. For Deployment Settings, select **Ignore BIG-IP DSC sync when deploying configuration changes**.
5. Click **OK**, and then click **Close**.

With the **Ignore BIG-IP DSC sync when deploying configuration changes** option selected, you can now deploy changes to the member that is available, and BIG-IQ will not attempt to sync those changes to the member that is unavailable.

Use the *Deploy configuration changes* task to deploy changes to the available member. When you select the target device for deployment, do not select the unavailable device.

Managing Configuration Snapshots

What is snapshot management?

You can manage configuration snapshots for the configurations you have created on the BIG-IQ® Centralized Management system. A *snapshot* is a backup copy of a configuration. Configuration snapshots are created manually. This type of snapshot does not include events or alerts.

Note: *If an Access group version changes to a later BIG-IQ version and you attempt to restore a snapshot created during the previous version, then restoring that snapshot can cause working configuration changes that can cause a deployment failure.*

Create a snapshot

You create a configuration snapshot to compare it to another configuration snapshot, or so you can save the current working configuration and then restore from that snapshot if needed.

You create a configuration snapshot to preserve the configuration at that point. There are three things you can do with a snapshot:

- Deploy the preserved configuration to a managed device.
- Restore the BIG-IQ® Centralized Management device's current configuration to the preserved configuration.
- Compare the preserved configuration to the BIG-IQ device's current configuration to see what has changed.

1. At the top of the screen, click **Deployment**.
2. Expand **SNAPSHOTS**, and then select the component from which to create the snapshot.
   The screen displays a list of snapshots that have been created for the selected component on this device.
3. Click the **Create** button.
   The New Snapshot screen opens.
4. Supply the values on the New Snapshot screen, and click **Create**.

The system creates the snapshot and adds it to the list of snapshots on the Snapshot screen, along with information related to the snapshot, including the date it was created, what account created it, and any description.

Compare snapshots

You can compare a snapshot to another snapshot, or to the current working configuration so that you can view the differences between them.

1. At the top of the screen, click **Deployment**.
2. Expand **SNAPSHOTS**, and then select the component that contains the snapshots to compare.
   The screen displays a list of snapshots that have been created on this device.
3. Select the check box to the left of the snapshot that you want to use as the source snapshot.

4. Click **Compare**.
   The Compare Snapshots screen displays.
5. For the **Target**, select the snapshot that you want to compare to the Source snapshot.
   - To compare the Source snapshot to the current configuration, select **Configuration on BIG-IQ**.
   - To compare the Source snapshot to an existing snapshot, select that snapshot.
   - If you are working with an Access snapshot, select the access group to which you want to compare the Source snapshot.
6. If you are working with a Network Security or Web Application Security snapshot, choose the kind of differences you want to review:
   - For Network Security, to compare firewall object differences, click **Compare** in the Compare Firewall row.
   - For Network Security, or Web Application Security, to compare shared security object differences, click **Compare** in the Compare Shared Security row.
   - For Web Application Security, to compare ASM differences, click **Compare** in the Compare ASM row.
7. Analyze the configuration differences between the snapshot and the comparison target. When you are finished, click **Cancel** to close the Differences screen, then click **Close**.
   The screen closes and you return to the Snapshot screen.

Restore some objects from a snapshot

You can restore a snapshot to change the working configuration to that of the snapshot. Restoring the snapshot merges objects from the snapshot into the BIG-IQ® Centralized Management configuration and removes all active locks. No objects in the BIG-IQ configuration are removed. Once the restore process starts, you cannot modify the BIG-IQ configuration until the process is completed or canceled. If the process is canceled, all configuration settings are rolled back.

Important: *Restoring a snapshot in one component can impact other components that have dependent configuration objects. We recommend that when you restore configurations that involve multiple components, you use snapshots that were created at approximately the same time. Restoring the Local Traffic & Network component can require a restore of other dependent components.*

If you are restoring a snapshot for Local Traffic & Network, Network Security, or Web Application Security, you can select specific objects to restore. This process is called *partial restore*. For example, you might have changed hundreds of configuration objects since you created a specific snapshot, but by doing a partial restore, you could bring back the settings for twenty five of them.

There is another reason you might choose to do a partial restore. With a partial restore, you can either restore the snapshot immediately, or you can create a snapshot evaluation. You can use an evaluation to review the differences between a snapshot and the current working configuration and confirm that you are restoring to the preserved configuration that you are looking for.

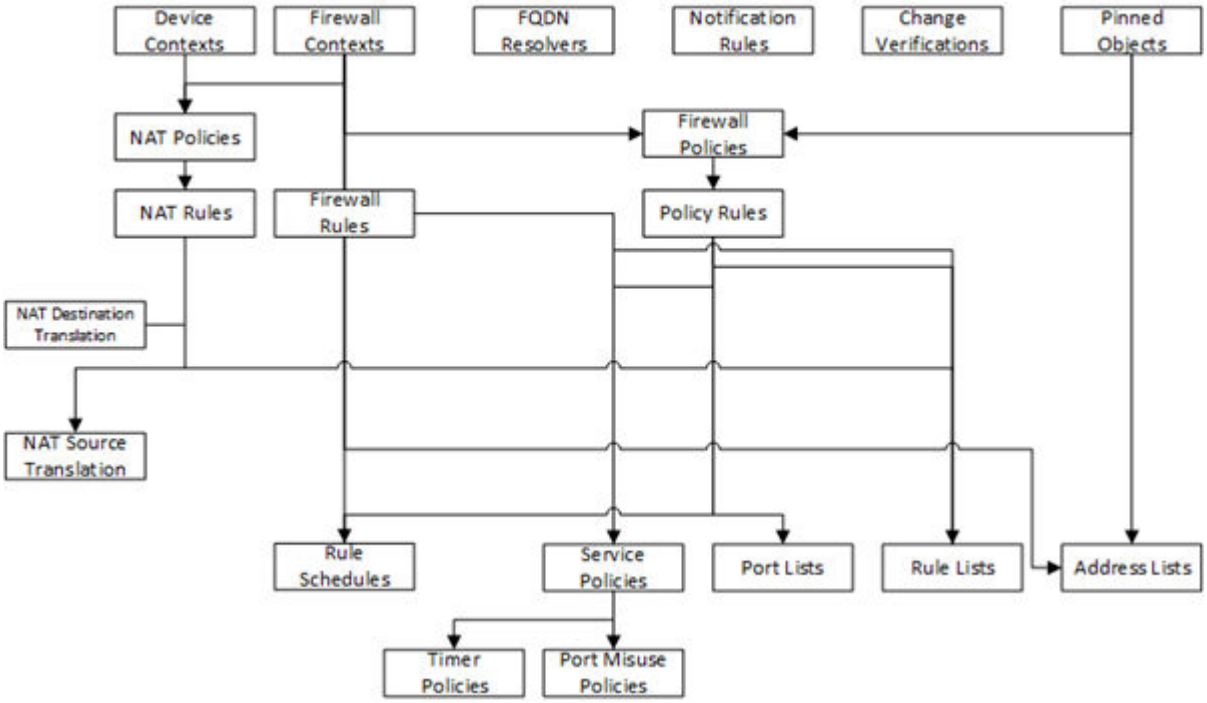
1. At the top of the screen, click **Deployment**.
2. Expand **RESTORE**, and click the component that contains the snapshot to restore.
   The screen displays a list of snapshot restores and evaluations that have been created for the selected component on this device.
3. Under Partial Restore Evaluations, click **Create**.
   The New Evaluation screen opens.
4. For **Name**, type a name for the snapshot restore.
5. For **Description**, describe the snapshot restore.
6. For **Snapshot**, select the snapshot you want to restore to.

7. If you want to create a snapshot that you can use to get back to your current configuration after the restore, for **Create Snapshot**, select **Create a snapshot prior to restoring**.
8. If you want the system to assess what the impact of deploying this snapshot would be on the managed devices, for **Offline Verification**, select **Run offline verification after restore**.
9. For the **Restore Scope**, select **Partial Restore**.

   The screen displays additional settings.
10. Click **Add** to specify which configuration changes to restore.
11. On the **Available** tab, select the object type that you want to restore.
12. From the list of configuration changes, select the objects that you want to restore and click **Add**.
13. If there are additional object types you want to include in this restore, repeat the last two steps for each object type.
14. If you add an object to the restore and then change your mind, you can click the **Selected** tab, select the object, and click **Remove**.
15. When you have added all of the changes that you want to include in this restore, click **Save**.
    The objects you selected for inclusion are listed under Source Objects.
16. For **Supporting Objects**, your options depend on the component you are restoring.

Option	Description
For Web Application Security	Supporting objects are always included.
For Network Security or Local Traffic & Network	Clear the **Include** check box if you want to restore changes only to the selected objects. It is almost always best to restore changes to the associated objects as well.

Important: *The objects that you manage using the BIG-IQ depend on associations with other, supporting objects. These object associations form relationship trees that are sometimes quite complex. Generally, when you restore a change to a managed object it is a very good idea to include these supporting objects in the deployment. This diagram illustrates a typical relationship tree for Network Services managed objects. For Local Traffic and Web Application Security, the trees are equally complex and just as vital to include.*



17. If you decide you want to remove one of the objects selected for restoration, you can select it and then click **Remove**.
18. You can either create an evaluation of the restore and review it, or restore the snapshot immediately. For **Method**, select **Create Evaluation** or **Restore immediately**.
19. Click **Create**.

Option	Description
If you selected Create Evaluation	1. The confirmation screen notifies you that you are about to create an evaluation. 2. Click **Evaluate**. The evaluation is added to the Evaluations list with a status of `Pending confirmation`. ***Note:*** *This process might take some time. You can cancel it if you change your mind.* 3. To review the changes between the snapshot and the current working configuration, click **View**. 4. If you decide to complete this restore, select this snapshot evaluation, and click **Restore**. When the restore finishes, the snapshot restore you created is listed under Restores with a status of `Restore complete`.
If you selected Restore immediately	1. The confirmation screen notifies you that you are about to trigger a snapshot restore. 2. Click **Restore**. The restore process begins. ***Note:*** *This process might take some time. You can cancel it if you change your mind.*

Restore all objects from a snapshot

You can restore a snapshot to change the working configuration to that of the snapshot. Restoring the snapshot merges objects from the snapshot into the BIG-IQ® Centralized Management configuration, and removes all active locks. No objects in the BIG-IQ configuration are removed. Once the restore process starts, you cannot modify the BIG-IQ configuration until the process is completed or canceled. If the process is canceled, all configuration settings are rolled back.

Important: *Restoring a snapshot in one component can impact other components that have dependent configuration objects. We recommend that when you restore configurations that involve multiple components, you use snapshots that were created at approximately the same time. Restoring the Local Traffic & Network component can require a restore of other dependent components.*

1. At the top of the screen, click **Deployment**.
2. Expand **RESTORE**, and click the component that contains the snapshot to restore.
   The screen displays a list of snapshot restores and evaluations that have been created for the selected component on this device.
3. Under Restores, click **Create**.
4. For **Name**, type a name for the snapshot restore.
5. For **Description**, describe the snapshot restore.
6. For **Snapshot**, select the snapshot you want to restore to.
7. If you want to create a snapshot that you can use to get back to your current configuration after the restore, for **Create Snapshot**, select **Create a snapshot prior to restoring**,.

8. If you want the system to assess what the impact of deploying this snapshot would be on the managed devices. for **Offline Verification,** select **Run offline verification after restore**.
9. For **Restore Scope**, select **Full Restore**.
10. Click **Restore**.
    The confirmation screen notifies you that you are about to trigger a snapshot restore.
11. Click **Restore** to begin the restore process.

Note: *This process might take some time. You can cancel it if you change your mind.*

Legal Notices

Legal notices

Publication Date

This document was published on April 14, 2017.

Publication Number

MAN-0498-07

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

A

active usage report
    for licenses *19*
automatic registration key activation
    for licenses *14*

B

backup
    creating a UCS backup on demand *33*
backup schedule
    creating for UCS files *34*
    stopping and restarting *35*
backup UCS files
    restoring *35*
backups
    about *33*
    creating for UCS files *33*
    creating schedule for UCS files *34*
BIG-IP device
    software installation *24*
BIG-IP devices
    downloading software image for upgrades *23*
    rebooting *8*
    uploading software images to BIG-IQ for upgrades *23*
    viewing trust certificates BIG-IP in a DSC cluster *10*
BIG-IP DSC properties
    viewing *10*
BIG-IP VE standalone licenses
    creating a registration key pool for *16*
BIG-IQ
    about centralized management *5*
BIG-IQ Device inventory
    dealing with a yellow indicator *25*
BIG-IQ inventory
    adding devices to *7*
BIG-IQ system
    downloading software image for *23*
    uploading software images *23*
billing
    for utility pool licenses *20*

C

CA-signed certificate
    creating *29*
    uploading *29*
centralized management
    of BIG-IP devices *7*
Certificate Signing Request
    creating on BIG-IQ *29*
    See also CSR
certificates
    about managing *27*
    creating CA-signed *29*
    importing PKCS #12 archive *31*
changes
changes *(continued)*
    about evaluating before deploying *39*
    evaluating before deploying *39*
cluster management
    about *9*
clusters
    about managing *9*
config template
    creating *37*
configuration changes
    about deploying *42*
    deploying to a device *42*
    deploying urgent *45*
    evaluating *39*
    making urgent *42*
configuration deployment
    about *42*
configuration snapshots
    about managing *47*
configuration templates
    about *37*
    applying *37*
    creating *37*
configurations
    about changing for devices *37*
    about creating backups *33*
    backing up *33*, *34*
    creating a template *37*
    deploying with a template *37*
    filtering for devices *9*
    rolling back to a previous version *35*
CSR
    creating *29*
CSV file
    exporting device properties to *9*

D

deployment
    making to one device *45*
    making urgent *42*
    of configuration changes *42*
device backup
    about *33*
    and USC files *33*
device configurations
    filtering *9*
device groups
    about dynamic *11*
    about static *11*
device inventory
    about *7*
    viewing details *9*
device management
    about *7*
    searching for BIG-IP components *9*
device properties
    exporting to a CSV file *9*

device properties *(continued)*
viewing *9*
device service clustering, *See* DSC
Device Service Clustering
defined *9*
See also DSC
device status
viewing for BIG-IP DSC *10*
devices
about discovering *7*
adding to BIG-IQ inventory *7*
backing up UCS files for *33*, *34*
discovering *7*
organizing in a static group *11*
upgrading *25*
viewing details *8*
discovery
defined *7*
DSC
defined *9*
viewing properties *10*
See also Device Service Clustering
DSC devices
and synchronization options *11*
synchronizing *11*
DSC groups
discovering *10*
dynamic device groups
about *11*
dynamic group
creating *12*

E

emergency deployment
of configuration changes *42*, *45*
evaluation of changes
before deploying *39*

F

F5 license server
about contacting for licensing *14*
framework
upgrading after upgrading BIG-IQ *25*

G

groups
about dynamic device groups *11*
about static device groups *11*
creating dynamic *12*
creating static *11*

H

health
viewing for a device *8*
historical usage report
creating for licenses *20*
hotfixes
hotfixes *(continued)*
installing on BIG-IP devices *24*
uploading to BIG-IQ *23*

I

inventory details
viewing for devices *8*

L

legacy devices
upgrading *25*
license
activating registration key automatically *14*
activating registration key manually *14*
changing assignment *19*
revoking and granting in one step *19*
license assignment
about *18*
license offerings
defined *15*
license options
for managed devices *13*
license pools
creating a standalone registration key pool *16*
creating historical usage report for *20*
defined *13*
license registration keys
activating manually *14*
license revocation *18*
license usage
reporting *20*
licenses
about activating registration key *14*
about managing for devices *13*
about usage reports *19*
activating registration key automatically *14*
adding and activating a standalone registration key by automatically contacting the F5 Licensing server *16*, *17*
assigning a pool license to a BIG-IP device *18*
revoking for a BIG-IP device *18*
licensing
creating reports for *20*
for managed devices *13*

M

managed devices
about discovering *7*
about upgrading software *23*
creating dynamic groups *12*
managed objects
about evaluating changes before deploying *39*
evaluating changes before deploying *39*
managed SSL certificates
defined *27*
manual activation
for licenses *14*

O

offerings
defined *15*

P

partial restore *48*
PKCS #12 archive
importing *31*
PKCS #12 SSL archive files
created on a system other than BIG-IQ *30*
pool license
activating registration key automatically *14*
activating registration key manually *14*
pool licenses
about usage reports *19*
revoking, assigning, and changing *18*
purchased license pools
creating active usage report for *19*
creating for historical license usage *20*
purchased pool license
activating registration key automatically *14*
activating registration key manually *14*

R

reboot
for BIG-IP devices *8*
recovery
for a BIG-IP device *35*
registration key
activating manually for a pool license *14*
activation options *14*
registration key license pools
creating for historical license usage *20*
Registration Key Pool
adding and activating license for by automatically
contacting the F5 Licensing server *16*, *17*
creating for standalone registration keys *16*
registration key pool license
activating registration key automatically *14*
registration key pools
creating active usage report for *19*
defined *13*
reports
creating for historical license usage *20*
creating for license usage *19*
creating for utility license *20*
REST framework
updating *25*

S

self-signed key
creating *28*
snapshot management
about *47*
snapshots
about managing *47*
comparing *47*
creating *47*
snapshots *(continued)*
restoring all objects *50*
restoring some objects *48*
software
installing *24*
upgrading for devices *25*
uploading images to BIG-IQ *23*
software images
downloading *23*
uploading to BIG-IQ *23*
software upgrade
for managed devices *23*
SSL certificate
creating *28*
SSL certificate key
creating *28*
SSL certificate keys
importing *30*
SSL certificates
about managing *27*
created on a system other than BIG-IQ *30*
importing *30*
managed and unmanaged *27*
managing from BIG-IQ *29*
pinning to BIG-IP devices *28*
uploading CA-signed *29*
SSL key
import for an unmanaged SSL certificate *27*
standalone keys pools
defined *13*
standalone registration key
adding and activating by automatically contacting the F5
Licensing server *16*, *17*
standalone registration key pool
creating *16*
static device groups
about *11*
static group
creating *11*
status
for BIG-IP devices in a DSC cluster *10*
viewing for a device *8*
sync *11*
See also synchronization
synchronization
for devices in a DSC configuration *11*
synchronization options
for devices in a DSC configuration *11*
system snapshots
about managing *47*
comparing *47*
creating *47*
restoring all objects *50*
restoring some objects *48*

T

templates
about configuration templates *37*
creating for configuration *37*

U

UCS backup files
    restoring *35*
UCS backup schedule
    stopping and restarting *35*
UCS file
    about *33*
    defined *33*
UCS files
    creating a backup of a current configuration *33*
    creating backups on a schedule *34*
unmanaged devices
    defined *18*
unmanaged SSL certificate
    importing SSL certificate for *27*
unmanaged SSL certificates
    defined *27*
upgrades
    downloading software image *23*
    for BIG-IP devices *24*
    uploading software image *23*
urgent deployment
    making *42*
user configuration set, *See* UCS file
utility license pools
    creating active usage report for *19*
    creating historical usage report for *20*
    defined *13*
utility pool license
    activating registration key automatically *14*
    activating registration key manually *15*
    assigning to a BIG-IP device *18*
    revoking for a BIG-IP device *18*
utility pool license reports
    creating *20*
    submitting *20*

V

volume license pools
    creating active usage report for *19*
    creating historical usage report for *20*
    defined *13*
volume pool license
    activating registration key automatically *14*
    activating registration key manually *15*
    assigning to a BIG-IP device *18*
    revoking for a BIG-IP device *18*

Y

yellow indicator
    displaying in BIG-IP Device inventory *25*