F5® BIG-IQ® Centralized Management: Licensing and Initial Setup

Version 5.4

Table of Contents

BIG-IQ System Introduction

BIG-IQ Centralized Management documentation set

BIG-IQ Centralized Management documentation set is located on AskF5 at https://support.f5.com. Click the **Product Manuals** link under Resources, and select **BIG-IQ Centralized Management** from the product list, and select the appropriate version.

Title	Use to:
F5® BIG-IQ® Centralized Management: Licensing and Initial Setup	License and set up the BIG-IQ system in your network.
F5® BIG-IQ® Centralized Management: Authentication, Roles, and User Management	• Configure authentication through a 3rd-party provider (LDAP, RADIUS or TACAS+) . • Use built-in and custom roles to manage user access.
F5® BIG-IQ® Monitoring and Reports	• Set up health monitoring and alerts and statistics collections • Manage audit logs, run reports, and analyze statistics. • Troubleshooting Access reports.
F5® BIG-IQ® Centralized Management: Device	• Discover BIG-IP devices and import F5 services. • Deploy software images, licenses, SSL certificates, backup files, and configurations.
F5® BIG-IQ® Local Traffic & Network Implementations	Manage: • Local Traffic profiles • Virtual servers • Network objects • iRules • Applications and application templates As well as configuring an IPsec tunnel and event viewing.
F5® BIG-IQ® Centralized Management: Security	Manage: • Object pinning • Firewall contexts • Address and port lists • Rules, rule lists, policies, and rule reports • Service, timer, and port misuse policies • NAT policies and translations • FQDN resolvers • Change verifications • External logging devices

Title	Use to:
	• Shared security for virtual servers, DoS profiles, device DoS configurations, network whitelists, logging profiles, and SSH profiles • Bot signatures and bot signature categories • IP intelligence settings • External redirection settings • Application Securities Policies • Signature files, custom attack signatures and sets • Web Application Security event logs
F5® BIG-IQ® Centralized Management: Access	• Configure an Access group, HA pair, and cluster. • Manage access groups. • View and edit access configurations. • Configure authentication for Active Directory, SecuID, HTTP, Oracle Access Manager, OCSP responder, CRLDP, and Kerberos. • Manage audit logs
F5® Platform Guide: BIG-IQ® 7000 Series	Set up and manage the BIG-IQ 7000 hardware platform.

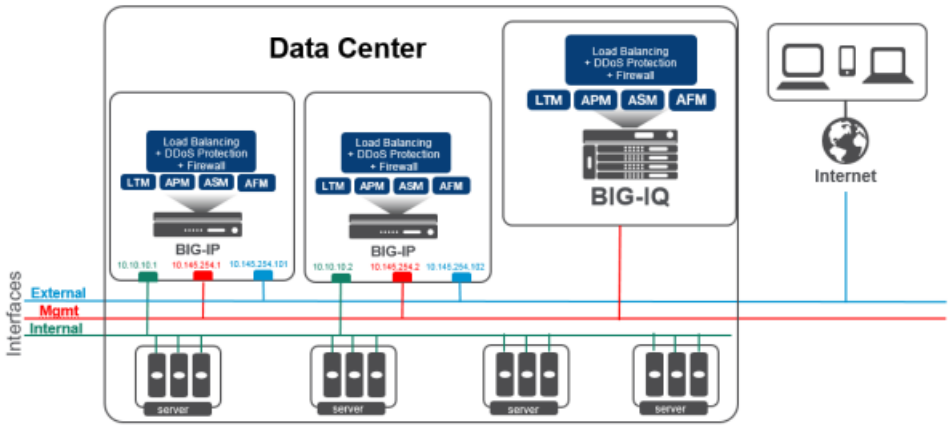
About BIG-IQ Centralized Management

F5® BIG-IQ® Centralized Management is a tool that helps you manage BIG-IP devices, and all of their services (such as LTM, AFM, ASM and so forth), from one location. BIG IQ can manage up to 200 (physical, virtual, or vCMP) BIG-IP devices and handle licensing for up to 5,000 unmanaged devices.

Using BIG-IQ helps you more efficiently manage your BIG-IP devices through a single pane of glass view. That means you and your co-workers don't have to log in to individual BIG-IP systems to get your job done. You can discover, upgrade, deploy policy changes, manage license, and more from just one location.

From BIG-IQ, you can manage a variety of tasks from software updates to health monitoring and traffic to security. And because permissions for users are role-based, you can limit access to just a few trusted administrators to minimize downtime and potential security issues. You also have the ability to allow users to view or edit only those BIG-IP objects they need to do their job.

Here's an example of how BIG-IQ can fit into a data center.



BIG-IQ navigation overview

F5® BIG-IQ® Centralized Management includes navigation, search tools, and a customizable user interface to help you complete your tasks efficiently and find objects easily.

- **Customized interactions with System and Network Security views** There are a few customizable viewing options for the System and Network Security views. You can specify the amount of time that passes before BIG-IQ logs you out when the system is idle and what screen displays when you log back in. If you're using the Network Security service, you can specify what types of firewalls are displayed in the menu, have rule lists in policies auto expand, treat terms you search for as a filter, and specify default values for columns.
- **Global search, related content, and preview pane**

  BIG-IQ has a robust and interactive global search feature that allows you to easily find a specific content and related content. From any screen, you can click the magnifying glass icon in the upper-right corner of the screen and type a search string. Search results are grouped by content type. From the results, you can click an object to go directly to that object's properties screen in BIG-IQ.
- **Flexible access to objects and configuration options**

  For some objects, you can view and edit settings that are located in other places in the user interface, without having to stop what you're doing and navigate to another part of BIG-IQ. For example, you could be editing a firewall policy and find an address list in the toolbox that you want to look at. Right there, you can click the address to access the details, and then view or edit it as you want.

  You can also configure some types of objects from different places in BIG-IQ, depending on what your user role is or what work flow you're in. For example, you can create an access group from the Configuration area of BIG-IQ, as well as from the Devices area. This makes it convenient for you to access during other tasks you're doing in different areas of BIG-IQ.
- **Filters**

  For each screen that contains a list, you can use a context-sensitive filter to search on a term, and then narrow your search further to view only those items that are relevant to you at the moment. For example, say you wanted to see local traffic and network audit logs. You can use the search on local traffic, and further refine what is displayed by filtering again on network audit logs.
- **Customization and sorting columns**

  You can customize the columns that display in each screen that has a list, hiding any information that isn't important to you, as well as rearrange the order the columns display, and sort objects in the list. This helps you to focus on only those attributes that are relevant to you.

Use global search to access associated objects from any screen

BIG-IQ® Centralized Management makes it easy for you to perform a search for specific details of your configuration across all your managed devices. From the content that is returned, you can access everything associated with that content, regardless of where it is on BIG-IQ. For example, if you search on a specific self-IP address, the results give you access to other content related to that self-IP address. We call this *global search*.

Global search is a powerful feature that gives you quick access to all objects that contain a certain string. This can give you insight about how objects are relate, even when they're running different services, devices, and so forth.

Important: *BIG-IQ global search returns only the content specific to your user role privileges. For example, if your user role doesn't have privileges for content associated with security, content specific only to security does not display.*

---

1. On any screen, click the  icon in the upper right corner.
   The global search popup screen opens.
2. Into the search field, type all or part of a string you want to search for.
3. If you want to specify search options, click the arrow next to the search field and select the options you want and click the Enter key.
   The screen refreshes to display content associated with your search term, organized by type.
4. Click the object link to view the details for an object.

   Tip: *You can navigate back to the results after you click on an object, by clicking the magnifying glass on upper right side of the screen again.*

   ---
5. If you want to clear the search results, click the **X** next to the **BIG-IQ Search** field of the popup window.

Customize how your object lists display

Only after you discover devices and their associated objects, can you view the devices and the related objects in object lists on various screens.

If you need to see only certain information about a list of objects and/or information displayed in a certain way, you can customize the way the screen lists content.

1. Navigate to a screen that contains a list of objects.

   For example, **Devices** > **SOFTWARE MANAGEMENT** > **Software Images**.
2. To limit the number of columns you want to view, click the gear icon on the far right of the screen and deselect the columns you don't want displayed.
3. To customize the order in which the columns display, click the name of the column, drag it to, and drop it in another location.
4. To sort a list in ascending or descending order, hover next to the column name and click the up or down arrow.

Filter an object list

For each screen that contains an object list, you can narrow the list to display only specific items, phrases, or numbers. This helps you easily navigate long lists and find what you need quickly.

1. Navigate to a screen that contains a list of objects.

For example, **Devices** > **BIG-IP DEVICES**.

2. In the **Filter** field located towards the top of the screen, type a term, phrase, or number, and press the Enter key.

   Tip: *By default, BIG-IQ uses this filter on anything that matches any field on the screen, so this can be a partial term, phrase or number. For example, if you wanted to see only objects that contained the number 191, you'd type* `191`.

   Tip: *To limit the filter to a specific object type, click the down arrow next to the search field and select the type of object you're looking for. To require the term match exactly, click* ***Exact***.

   The screen refreshes to display only those items that include or exactly match the term you used for a filter. The filter you used displays at the top of the list.
3. To further limit the results displayed, type another term in the **Filter** field, selecting options from the filter menu as you did before.
4. To view the properties of an object, click the object's name.

   Tip: *Click the back button to return to the filter results.*
5. To remove a filter, at the top of the list, click the **X** next to a filter.

Set preferences for BIG-IQ user interface

Only after you license and finish the initial setup for BIG-IQ® Centralized Management, can you specify a few preferences for the user interface.

Setting user preferences customizes your view into BIG-IQ.

Note: *The navigation objects and screens you see depend on your user role.*

1. At the top of the screen, click **System**.
2. On the left, click **USER PREFERENCES** towards the bottom of the screen.
3. You can edit the user preferences for the overall BIG-IQ system by clicking the **Edit** button.
4. Click **Network Security** and the **Edit** button to edit preferences for the Security service.

Click the  icon at the top right of the screen for more information about these options.

Licensing and Initial Setup

Default administrator and root user names and passwords

You access BIG-IQ with the following administrative user roles and a default password. For security purposes, you should change these passwords after you license the system (during initial setup), and at regular intervals.

Default User Type	Default Password	Access Rights / Role
admin	admin	This user type can access all aspects of the BIG-IQ system from the system's user interface.
root	default	This user has access to all aspects of the BIG-IQ system from the system's console command line.

Open ports required for device management

F5® BIG-IQ® Centralized Management must have bilateral communication with the devices in your network to successfully manage them. For this communication, the following ports must be open to allow for the required two-way communication. You might have to contact a firewall or network administrator to verify that these ports are open (they are by default), or have them opened if they aren't.

Open Port	Purpose
TCP 443 (HTTPS) and TCP 22 (SSH)	Discovering, monitoring, configuring BIG-IP devices running versions 11.5.0-11.6.0
TCP 443 (HTTPS)	Discovering, monitoring, configuring BIG-IP devices running versions 12.0.0 and later
TCP 443 (HTTPS)	Replicating and synchronizing BIG-IQ systems

How do I license and do the basic setup to start using BIG-IQ?

After you download the software image from the F5 Downloads site and start BIG-IQ® in your virtual environment, you can license the system using the base registration key provided by F5. The *base registration key* is a character string the F5 license server uses to provide BIG-IQ a license to access the subscription licensing feature.

You license BIG-IQ in one of the following ways:

- If the system has access to the Internet, you can have the BIG-IQ system contact the F5 license server and automatically activate the base registration key to get a license.
- If the system is not connected to the Internet, you can manually license the BIG-IQ using the F5 license server web portal.
- If the system is in a closed-circuit network (CCN) that does not allow you to export any encrypted information, you must open a case with F5 support at: *support.f5.com/csp/my-support/home*.

When licensing BIG-IQ, you:

1. Activate the license.
2. Accept the EULA.
3. Specify the system personality as BIG-IQ Centralized Management.
4. Specify a host name, and IP addresses for the management port, DNS server, and network time protocol (NTP) servers.
5. Specify the master key pass phrase.
6. Change the default admin and root passwords.

Automatic license and initial setup for BIG-IQ

You must have a base registration key before you can license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (`f5.com`).

If the BIG-IQ® system is connected to the public internet, you can follow these steps to automatically perform the license activation and perform the initial setup.

1. Use a browser to log in to BIG-IQ by typing `https://<management_IP_address>`, where `<management_IP_address>` is the address you specified for device management.
2. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.

   Important: *If you are setting up a data collection device, you have to use a registration key that supports a data collection device license.*

3. In the **Add-On Keys** field, paste any additional license key you have.
4. To add another additional add-on key, click the + sign and paste the additional key in the new **Add-On Keys** field.
5. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.
6. Click **Next**.

   If you are setting up this device for the first time, the Accept User Legal Agreement screen opens.
7. To accept the license agreement, click the **Agree** button.
8. Click the **Next** button at the bottom of the screen.
   If your license supports both BIG-IQ Data Collection Device and BIG-IQ Central Management Console, the System Personality screen displays. Otherwise the Management Address screen opens.
9. If you are prompted with the System Personality screen, select the option you're licensed for, and then click **OK**. If you are not prompted, proceed to the next step.

   Important: *You cannot undo this choice. Once you license a device as a BIG-IQ Management Console, you can't change your mind and license it as a Data Collection Device.*

   The Management Address screen opens.
10. In the **Hostname** field, type a fully-qualified domain name (FQDN) for the system.

    You cannot change this name after you add it. The FQDN can consist of letters and numbers, as well as the characters underscore (_), dash (-), or period (.).
11. In the **Management Port IP Address** and **Management Port Route** fields, type the IP address for the management port IP address and route.

    Note: *The management port IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`.
12. Specify what you want the BIG-IQ to use for the **Discovery Address**.
    - To use the management port, select **Use Management Address**.
    - To use the internal self IP address, select **Self IP Address**, and type the IP address.

Important: *If you are configuring a data collection device, you must use the internal self IP address.*

Note: *The self IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`.

13. In the **DNS Lookup Servers** field, type the IP address of your DNS server.
    You can click the **Test Connection** button to verify that BIG-IQ can reach that IP address.
14. In the **DNS Search Domains** field, type the name of your search domain.
    The DNS search domain list allows the BIG-IQ system to search for local domain lookups to resolve local host names.
15. In the **Time Servers** field, type the IP addresses of your Network Time Protocol (NTP) server.
    You can click the **Test Connection** button to verify that BIG-IQ can reach the IP address.
16. From the **Time Zone** list, select your local time zone.
17. Click the **Next** button at the bottom of the screen.
    The Master Key screen opens.
18. For the **Passphrase**, type a phrase that satisfies the requirements specified on screen, and then type the same phrase for **Confirm Passphrase**.

    Important: *You can enter this pass phrase only once. You cannot change it without resetting the device. The system uses the pass phrase to generate a Master Key. For you to configure High Availability or a Data Collection Device cluster, this pass phrase must be the same on all devices. If the pass phrase is not the same, you must reset and configure those devices with the same pass phrase.*

19. In the **Old Password** fields, type the default admin and root passwords, and then type a new password in the **Password** and **Confirm Password** fields.
20. Click the **Next** button at the bottom of the screen.
    The screen Summary displays the details you just specified for this device configuration.
21. If the details are as you intended, click **Launch** to continue; if you want to make corrections, use the **Previous** button to navigate back to the screen you want to change.

Manual license and initial setup for BIG-IQ

You must have a base registration key before you can license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (`f5.com`).

If the BIG-IQ® system is not connected to the public internet, you can follow these steps to contact the F5 license web portal then perform the initial setup.

1. Use a browser to log in to BIG-IQ by typing `https://<management_IP_address>`, where `<management_IP_address>` is the address you specified for device management.
2. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.

   Important: *If you are setting up a data collection device, you have to use a registration key that supports a data collection device license.*

3. In the **Add-On Keys** field, paste any additional license key you have.
4. 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.
5. Select and copy the text displayed in the **Device Dossier** field.
6. Click the **Access F5 manual activation web portal** link.
   The Activate F5 Product site opens.

7. Into the **Enter your dossier** field, paste the dossier.

   Alternatively, if you saved the file, click the **Choose File** button and navigate to it.

   After a pause, the screen displays the license key text.
8. Click **Next**.

   If you are setting up this device for the first time, the Accept User Legal Agreement screen opens.
9. To accept the license agreement, select **I have read and agree to the terms of this license**, and click **Next**. button.
   The licensing server creates the license key text.
10. Copy the license key.
11. In the **License Text** field on BIG-IQ, paste the license text.
12. Click the **Activate License** button.
13. Click the **Next** button at the bottom of the screen.
    If your license supports both BIG-IQ Data Collection Device and BIG-IQ Central Management Console, the System Personality screen displays. Otherwise the Management Address screen opens.
14. If you are prompted with the System Personality screen, select the option you're licensed for, and then click **OK**. If you are not prompted, proceed to the next step.

    Important: *You cannot undo this choice. Once you license a device as a BIG-IQ Management Console, you can't change your mind and license it as a Data Collection Device.*

    The Management Address screen opens.
15. In the **Hostname** field, type a fully-qualified domain name (FQDN) for the system.

    You cannot change this name after you add it. The FQDN can consist of letters and numbers, as well as the characters underscore (_), dash (-), or period (.).
16. In the **Management Port IP Address** and **Management Port Route** fields, type the IP address for the management port IP address and route.

    Note: *The management port IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`.
17. In the **DNS Lookup Servers** field, type the IP address of your DNS server.

    You can click the **Test Connection** button to verify that BIG-IQ can reach that IP address.
18. In the **DNS Search Domains** field, type the name of your search domain.

    The DNS search domain list allows the BIG-IQ system to search for local domain lookups to resolve local host names.
19. In the **Time Servers** field, type the IP addresses of your Network Time Protocol (NTP) server.

    You can click the **Test Connection** button to verify that BIG-IQ can reach the IP address.
20. From the **Time Zone** list, select your local time zone.
21. Click the **Next** button at the bottom of the screen.
    The Master Key screen opens.
22. For the **Passphrase**, type a phrase that satisfies the requirements specified on screen, and then type the same phrase for **Confirm Passphrase**.

    Important: *You can enter this pass phrase only once. You cannot change it without resetting the device. The system uses the pass phrase to generate a Master Key. For you to configure High Availability or a Data Collection Device cluster, this pass phrase must be the same on all devices. If the pass phrase is not the same, you must reset and configure those devices with the same pass phrase.*
23. Click the **Next** button at the bottom of the screen.
    The Password screen opens.

24. In the **Old Password** fields, type the default admin and root passwords, and then type a new password in the **Password** and **Confirm Password** fields.
25. Click the **Next** button at the bottom of the screen.
    The screen Summary displays the details you just specified for this device configuration.
26. If the details are as you intended, click **Launch** to continue; if you want to make corrections, use the **Previous** button to navigate back to the screen you want to change.

Change your BIG-IQ user password

For security reasons, you need to occasionally change your user password.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click your user name.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click the **Save & Close** button at the bottom of the screen.

BIG-IQ High Availability

How do I manage BIG-IQ systems in a high availability configuration?

Setting up BIG-IQ®in a high availability configuration ensures that you always have access to the BIG-IP® devices you are managing. In a BIG-IQ high availability configuration, the BIG-IQ system replicates configuration changes since the last synchronization from the primary device to the secondary device every 30 seconds. If it ever becomes necessary, you can have the secondary peer take over management of the BIG-IP devices.

Add a peer BIG-IQ system for a high availability configuration

Before you can set up F5® BIG-IQ® Centralized Management in a high availability (HA) pair, you must have two licensed BIG-IQ systems.

For the high-availability pair to synchronize properly, each system must be running the same BIG-IQ version, and the clocks on each system must be synchronized to within 60 seconds. To make sure the clocks are in sync, take a look at the NTP settings on each system before you add a peer.

Configuring BIG-IQ in a high availability (HA) pair means that you can still manage your BIG-IP® devices even if one BIG-IQ systems fails.

1. At the top of the screen, click **System**.
2. On the left, click **BIG-IQ HA**.
3. Click the **Add Secondary** button.
4. Type the properties for the BIG-IQ system that you are adding.

   The IP address you use for device discovery must be the same on both peers in a high availability configuration.
5. Click the **Add** button at the bottom of the screen.

The BIG-IQ system synchronize. Once they are finished, both appear as ready (green).

Promote the secondary BIG-IQ system to primary for an HA pair

If the primary BIG-IQ® in an HA pair is having any type of system issue, you might want to make the secondary BIG-IQ the primary system until you can fix the problem.

You can promote the secondary system to primary when you are logged in to either BIG-IQ system in the pair.

This task describes how to promote the secondary BIG-IQ system while logged in to the primary BIG-IQ system.

1. At the top of the screen, click **System**.
2. On the left, click **BIG-IQ HA**.
3. Click the **BIG-IQ HA Settings** button and then click the **Promote** button.

The secondary BIG-IQ system synchronizes with the primary BIG-IQ system, and promotes to being the primary BIG-IQ system.

Remove the secondary BIG-IQ system from a high availability pair

To change or reconfigure (including upgrading) a BIG-IQ® Centralized Management system in a high availability (HA) pair, you must first split the HA relationship by removing the secondary system.

1. At the top of the screen, click **System**.
2. On the left, click **BIG-IQ HA**.
3. Select the check box next to the secondary BIG-IQ system, and click the **Remove Secondary** button.
4. Click the **Remove** button.

The BIG-IQ systems are now standalone.

Additional Network Configuration Options

Optional VLAN for device management

During the licensing and initial configuration procedures, you specify the management port for BIG-IQ®. This is all the networking configuration required to start managing devices. However, if you would prefer to manage devices from a VLAN address, you have the option to configure that.

Configure a VLAN to manage BIG-IP devices

You must have licensed the BIG-IQ® system before you can configure a VLAN.

If you decide you want to manage BIG-IP devices from a VLAN rather than the BIG-IQ system's management port, you can configure it using this procedure.

1. At the top of the screen, click **System**.
2. On the left, click **NETWORK SETTINGS** > **VLANs**.
3. Click the **Create** button.
4. In the **Name** and **Description** fields, type a unique name and description to identify this new VLAN.
5. In the **Tag** field, type an optional tag number.

   A VLAN *tag* is a unique ID number between 1 and 4094. All messages sent from a host in this VLAN includes the tag as a header in the message to identify the specific VLAN where the source or destination host is located. If you do not assign a tag, BIG-IQ assigns one automatically.
6. From the **Interface** list, select the port that you want this VLAN to use.

   The *interface* is a physical or virtual port that you use to connect the BIG-IQ system to managed devices in your network.
7. In the **MTU** field, type an optional frame size value for Path Maximum Transmission Unit (MTU).

   By default, BIG-IP devices use the standard Ethernet frame size of 1518 bytes (1522 bytes if VLAN tagging is used) with the corresponding MTU of 1500 bytes. For BIG-IP devices that support Jumbo Frames, you can specify another MTU value.
8. Click the **Save & Close** button at the bottom of the screen.

Specify a self-IP address for a VLAN

You need to configure BIG-IQ® with at least a VLAN before you can associate a self IP address with it.

If you've configured a VLAN to manage BIG-IP® devices, you can then associate a self IP address with that VLAN.

1. At the top of the screen, click **System**.
2. On the left, click **NETWORK SETTINGS** > **Self IPs**.
3. At the top of the screen, click the **Create** button.
4. In the **Name** field, type a unique name to identify this new self IP address.
5. In the **Address** field, type the self IP address and netmask.

   The format is `<self IP address/netmask>`.
6. In the **Description** field, type a description for this self IP address.
7. From the **VLAN** list, select the VLAN to associate with this self IP address.

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

Specify a web proxy for secure communication

Before you can specify a web proxy, you must license and perform the initial configuration for BIG-IQ® Centralized Management.

For security purposes, you can specify a web proxy for BIG-IQ to use for communication with the F5® iHealth® server and the F5 license server.

1. At the top of the screen, click **System**.
2. On the left, click **PROXIES**.
3. Near the top of the screen, click the **Add** button.
4. In the **Name** field, type a name to identify this web proxy.

   Important: *You must use the exact same proxy name on all BIG-IQ systems in a cluster.*
5. In the **Address** and **Port** fields, type the IP address and port for the web proxy server.

   The proxy address and port don't have to be the same for all BIG-IQ systems in a cluster.
6. If the web proxy server requires authentication, provide the credentials in the **User Name** and **Password** fields.
7. For the **Functions** setting, select the check box next to each function you want to use this web proxy for communication between BIG-IQ and the internet.
8. Click the **Save & Close** button at the bottom of the screen.

BIG-IQ will now use this web proxy for communication when accessing the internet for the functionality you specified.

UCS Backup Management for the BIG-IQ System

How do I back up and restore a BIG-IQ system's configuration?

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

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

Create an immediate backup of the BIG-IQ system's current UCS file

1. At the top of the screen, click **System**.
2. On the left, click **BACKUP & RESTORE** > **Backup Schedules**.
3. Click the **Back Up Now** 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. 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.*

---

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

When UCS backup file is complete, you can restore the BIG-IQ system.

Schedule BIG-IQ system's UCS file backups

Back up the BIG-IQ system's UCS file on a regular schedule to be sure you have a current copy of its configuration in case you ever have to perform a system recovery.

Note: *If your BIG-IQ system is part of an HA pair, create a backup schedule only for the primary BIG-IQ system.*

---

1. At the top of the screen, click **System**.
2. On the left, click **BACKUP & RESTORE** > **Backup Schedules**.
3. the **Schedule Backup** button.
4. Near the top of the screen, click the **Create** button.
5. Type a name to identify this backup, and an optional description for it.
6. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.

   If you save a copy of the SSL private key, you can reinstall it if the original one becomes corrupt.
7. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the passphrase.
8. 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. 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**.
11. 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.*

    ---
12. In the **OID** field, type the object identifier (OID) you want to associate with this user.

13. Click the **Save & Close** button at the bottom of the screen to save your changes.

Restore the BIG-IQ system with a UCS file backup stored remotely

You must create a backup of a F5® BIG-IQ® Centralized Management system's UCS file and store it to a remote system before you can restore it. To perform these steps, you must have access to the command line of the BIG-IQ system.

If for some reason your BIG-IQ system becomes inoperable or corrupt, you can use a backup UCS file to restore the BIG-IQ system without having to recreate all of the BIG-IQ system's content. You can also use a backup to restore BIG-IQ to a previous version after you upgrade, if necessary.

Use this procedure if you stored your UCS backup file remotely.

Important: *Restoration might take several minutes, during which time the system might be unavailable. Restoring the system requires a reboot.*

---

1. Using SSH, log in to the BIG-IQ system with the root user name and password.
2. From the BIG-IQ system you want to restore, open the Traffic Management Shell (tmsh) by typing, `tmsh`.
3. Choose the backup you want to restore, and copy it to `/var/local/ucs` by typing, `scp root@<IP address and port for UCS archive server>:<path of UCS file> /var/local/ucs/<backup name>.ucs`
4. Load the UCS file on the BIG-IQ system by typing, `load sys ucs <backup name>.ucs`
5. Restart rest javad by typing, `bigstart status restjavad`.

After restoration is complete, you can log back into the BIG-IQ system. If your BIG-IQ system is part of an HA pair, you must re-create the HA configuration.

Restore the BIG-IQ system with a UCS file backup stored locally

You must create a backup of a F5® BIG-IQ® Centralized Management system's UCS file and store it to a remote system before you can restore it.

If for some reason your BIG-IQ system becomes inoperable or corrupt, you can use a backup UCS file to restore the BIG-IQ system without having to recreate all of the BIG-IQ system's content. You can also use a backup to restore BIG-IQ to a previous version after you upgrade, if necessary.

Use this procedure to restore a configuration you stored locally on the BIG-IQ system.

Important: *Restoration might take several minutes, during which time the system might be unavailable. Restoring the system requires a reboot.*

---

1. At the top of the screen, click **System**.
2. On the left, click **BACKUP & RESTORE** > **Backup Files**.
3. Select the check box next to the backup file you want to restore and click the **Restore** button.

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

Important: *If you restore a BIG-IQ 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.*

After restoration is complete, you can log back into the BIG-IQ system. If your BIG-IQ system is part of an HA pair, you must re-create the HA configuration.

Legal Notices

Legal notices

Publication Date

This document was published on December 29, 2017.

Publication Number

MAN-0497-09

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

O

P

S

T

U

V