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

Version 5.3

Table of Contents

BIG-IQ System Introduction

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. That means you and your co-workers don't have to log in to individual BIG-IP systems to get your job done. From BIG-IQ, you can manage a variety of tasks from licensing to health monitoring and traffic to security. And because access to each area of BIG-IQ is role based, you can limit access to users to maximize work flows while minimizing errors and potential security issues.

How do I navigate the BIG-IQ user interface and find what I need quickly?

F5® BIG-IQ® Centralized Management includes navigation and search tools and customization features to help you complete your tasks efficiently and find objects easily.

Note: *What you see as a user in the BIG-IQ user interface depends on the privileges assigned to your user role. For example, a user logged in as an administrator sees the content for all managed devices, while a security administrator might see only objects associated with security.*

- **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's row and a preview displays in a panel. Clicking a link takes you directly to the content'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**

  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. This helps you to focus on only those attributes that are relevant to you. You can also sort on most columns in the list.

Find content and access associated objects from any screen (global search)

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*. This powerful feature gives you quick access to specific content and insight to how it relates to different areas of your managed devices.

It's important to note that the content BIG-IQ returns for a search is 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 magnifying glass in the upper right corner.
   The global search popup screen opens.
2. Into the search field, type all or part of a term you want to search for.
3. If you want to narrow the search results, click the arrow next to the search field to select search tools.

Option	Description
Contains	Opens the search up to any content that contains the search term.
Include ranges (IP Address & Port)	Returns a wider range of IP addresses and port numbers that match formats representing numeric ranges.
Exact Match	Returns only content that exactly matches the search term.
Search only	Narrows the content returned to include only a specific kind of object.

4. Press the Enter key.
   The screen refreshes to display content associated with your search term, organized by type.
5. To view a list of related content for a specific search result, click a row, and click the **Show** button.
6. To navigate directly to a specific screen associated with content, click the content.
7. To return back to the search results, click the magnifying glass.
8. To clear a search, click the X in the search field of the popup screen.

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** text box, type a term, phrase, or number.

   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`.

   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, select **Exact** from the list.

   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 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**.
   The System User Preferences screen opens.
3. Click the **Edit** button.
4. In the **Idle Timeout** field, type the maximum number of minutes of inactivity you want BIG-IQ to allow before it logs you out of the system.

   To keep your system and network secure, BIG-IQ logs you out of the system once it reaches the time you specify.
5. From the **Default View** list, select the area you want BIG-IQ to display when you initially log in to the system.
6. Click the **Save & Close** button at the bottom of the screen.

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?

F5® BIG-IQ® Centralized Management runs as a virtual machine in supported hypervisors, or on the BIG-IQ 7000 series platform. After you download the software image from the F5 Downloads site and upload it to BIG-IQ, you can license the system using the base registration key you purchased. The *base registration key* is a character string the F5 license server uses to provide BIG-IQ a license to access the features you purchased.

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: *https://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 (BIG-IQ Centralized Management or Data Collection Device).
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.

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.

Users, User Groups, Roles, and Authentication

How do I limit privileges for users based on their role in the company?

F5® BIG-IQ® Centralized Management provides you the tools you need to customize user access to your managed devices, and to BIG-IQ itself, through the use of role-based privileges. These privileges are based on the responsibilities of your users.

This type of role-specific access also provides you insight into your work flows. You can easily see which user interacted with any given service, and what the interaction was. This can help you quickly troubleshoot any introduced conflicts.

You can set up BIG-IQ to authorize users, giving them access only to the specific information, using these methods:

- **Local authorization** - for this option, BIG-IQ authenticates users.
- **External authorization** - for this option, you can configure BIG-IQ to use your LDAP, RADIUS, or TACACS+ server to authenticate users.

The responsibilities and roles each of your users has probably depend on the number of people who have access to BIG-IQ.

Assigning more than one role to a user

For example, if you have only two people managing your devices from BIG-IQ, they both most likely need to have full access to all aspects of BIG-IQ at one time or another. For these users, you'd assign them both the Administrator role.

Assigning more granular/specialized privileges to a user

On the other hand, if you're working for a larger company that has specialized roles to manage different services, or different parts of services, you can provide more granular access. For example, if you have two people who manage BIG-IP devices used only for network security purposes, you could assign them both the role of Network Security Manager. Or, if you have two people managing devices used for network security, but you want only one of them to write and edit policies, and the other to (only) deploy the policies, you could assign the first person the Network Security Editor role, and the other person the Network Security Deploy role. In this case, the Network Security Editor can only create, view, and edit policies, but not deploy them. The Network Security Deploy person can view and deploy policies, but cannot create or edit them.

Adding a new Pool Member Operator or Virtual Server Operator role

In addition to the standard roles that ship with BIG-IQ®, there are two roles specific only to LTM that you can add to your available options. These roles are:

- **Pool Member Operator** - This role has access to enable, disable, or force offline pool members on pools to which the administrator has granted them access.
- **Virtual Server Operator** - This role has access to enable or disable virtual servers to which the administrator has assigned them access.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Roles**.
3. Click the **Add** button.

4. In the **Name** field, type a name to identify this new role.
5. From the **Role Type** list, select the kind of role you want to add.
6. From the **Active Users and Groups** list, select the user or group you want to associate with this new role.
7. Click the + sign if you want this role to have access to another user or group, and select the device group from the list.
8. Click the **Save & Close** button at the bottom of the screen.

Add a user and assign them a role

Once you understand exactly who you want to perform certain tasks, you can provide them access to particular areas of F5® BIG-IQ® Centralized Management by adding them as a user and assigning the appropriate standardized role. You can assign as many roles as required to cover the user's responsibilities.

Important: *Since some roles have access only to certain areas or screens in the BIG-IQ user interface, it's important to communicate that to the user. When you assign a role to a user, be sure you outline the responsibilities and restrictions for their role. Clarifying this helps avoid any potential confusion. Also note,these roles do not have access to the global search functionality: Network Security Manager, Network Security Edit, Network Security View, and Trust Discovery Import.*

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
4. From the **Auth Provider** list, select the authentication method you want to use for this user.
5. In the **User Name** field, type the user name for this new user.
6. In the **Full Name** field, type a name to identify this user.

   The full name can contain a combination of symbols, letters, numbers and spaces.
7. In the **Password** and **Confirm Password** fields, type the password for this new locally-authenticated user.

   You can change the password any time.
8. To associate this user with an existing user group, select the group from the **User Groups** list.

   You aren't required to associate a user group at this point; you can do that later if you want. If you want to associate another user group with this user, click +.
9. From the **User Roles** list, select a user role to associate with this user.

   Each role has a set of unique privileges. If you want to associate another user role with this user, click +.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
10. Click the **Save & Close** button at the bottom of the screen.

This user now has the privileges associated with the role(s) you selected and BIG-IQ will authenticate this user locally

You can now tell this user how their BIG-IQ access aligns with their responsibilities. Make sure they understand they might not see every screen you or one of their peers does. Also let them know that if they try to log in more than 5 times in 5 minutes with the wrong user name and/or password, they might get the following error: `Maximum number of login attempts exceeded.` If that happens, the user must wait 5 minutes before trying to log back in.

Note: *If your BIG-IQ is in an HA pair, you must synchronize this change by refreshing the secondary BIG-IQ.*

Synchronize new users and user groups with secondary BIG-IQ

You must configure two BIG-IQ® Centralized Management systems in a high availability (HA) pair before you can synchronize users and user groups with a secondary BIG-IQ

Users and user groups are handled differently than other data that's synchronized between BIG-IQ® systems in an HA pair. For that reason, you must refresh the secondary BIG-IQ system in an HA pair after you add a new user or user group. Refresh the secondary BIG-IQ system so new users and user groups can successfully log in to the secondary system.

1. At the top of the screen, click **System**.
2. On the left, click **BIG-IQ HA**.
3. At the top of the screen, click the **BIG-IQ HA Settings** button.
4. Click the **Log Out and Refresh** button.
5. Click **OK**, then **Log Out**.
   BIG-IQ logs you out of the system.

You should now be able to log in to the secondary BIG-IQ system with the new user and/or user group you added.

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.

Remove a BIG-IQ user from a role

If a job or responsibilities change for an employee, you can use this procedure to disassociate that BIG-IQ user from an assigned role.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. On the Users inventory list, click the name of the user.
   The screen refreshes to display the properties for this user.
4. From the **User Roles** list, select the user role to disassociate from this user and click the **X**.

   The selected user role is removed from the list of privileges assigned to this user.
5. Click the **Save & Close** button at the bottom of the screen.

This user no longer has the privileges associated with the role you deleted.

Use my LDAP server to authenticate BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's LDAP server (LDAP server versions 2 and 3, and OpenLDAP directory, Apache Directory Server, and Active Directory). After you set up BIG-IQ to use your LDAP server, you can add users and user groups that authenticated by your LDAP server.

Before integrating BIG-IQ with your LDAP server for authentication

Before integrating LDAP authentication with the F5® BIG-IQ® Centralized Management system, you must complete these tasks.

Task	Notes	For my LDAP server
Use an LDAP browser to review the groups and users in your directory's structure and determine where they are located in the organizational units (OUs). Then, decide how you want to map those names.	There are two ways you can do this. The first option is to map users directly to their Distinguished Name (DN) in the directory with a user bind template in the form of `uid=<username>, ou=people, o=sevenSeas`. For example, you'd map John Smith's user name to his DN as `uid=<jsmith>, ou=people, o=sevenSeas` and he would log in as `jsmith` and would be correctly authenticated with his user name in the directory through his DN. The second option is to allow users to log in with names that do not map directly to their DN by specifying a `userSearchFilter` in the form of `(&(uid=%s))` when creating the provider. For example, if John Smith's DN is `cn=John Smith,ou=people,o=sevenSeas`, but you would like him to be able to log in with `jsmith`, specify a `userSearchFilter` in the form of `(&(jsmith=%s))`. If your directory does not allow anonymous binds, you must also specify a `bindUser` and `bindPassword` so that the BIG-IQ system can validate the user's credentials.	
Decide which groups in your directory to map with BIG-IQ groups.	If you configured a `bindUser` and `bindPassword` for users, the BIG-IQ system displays a list of groups from which to choose. If you haven't configured this for your users, you must know the DN for each group.	
Find out the DN where you can query or view for all users and groups.	This is the root bind DN for your directory, defined as `rootDN`, when you create a provider. The BIG-IQ system uses the root bind DN as a starting point when it searches for users and groups.	

Task	Notes	For my LDAP server
Find the host IP address for the LDAP server.	The default port is 389, if not specified otherwise, or 636 if SSL is enabled.	

Set up BIG-IQ to use your LDAP server for user authentication

Before you can set up BIG-IQ to authenticate users against your LDAP server, you have to specify your LDAP server settings on F5® BIG-IQ® Centralized Management and perform all the tasks outlined in the section titled, *Before integrating BIG-IQ with your LDAP server*.

You can configure BIG-IQ to use one or more of your company's LDAP server(s) to authenticate users.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **LDAP**.
5. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.
6. In the **Host** field, type the IP address of your LDAP server.
7. For the **Servers** setting, type in the **Port** that your Active Directory server uses.

   If you want BIG-IQ to use an SSL port to communicate with your LDAP server, type port `636` , otherwise leave it at the default port, **389**.
8. To use an SSL port to communicate with the LDAP server, for the **SSL Enabled** setting, select the **Enabled** check box.
9. If your LDAP server does not allow anonymous binds, in the **Bind User** and **Bind User Password** fields, type the full distinguished names and passwords for users with query access.
10. In the **Root DN** field, type the root context that contains users and groups.

    The root context must be a full distinguished name.
11. For the **Authentication Method** setting, specify a method.
    - **Simple** - Select this option to require a user name and password for authentication.
    - **None** - Select this option to prompt the LDAP server to ignore the user name and password.

    Warning: *No password authentication is used if you select* ***None****.*
12. For the **Search Scope** setting, select an option to specify the depth at which searches are made.
13. In the **Search Filter** field, type the LDAP filter expression that determines how users are found.

    The search filter depends on your LDAP implementation.
14. In the **Connect Timeout** field, type the number of milliseconds after which the BIG-IP system stops trying to connect to the LDAP server.
15. In the **Read Timeout** field, type the number of seconds the BIG-IP system will wait for a response to a query.
16. In the **User Display Name Attribute** field, type the LDAP field to use for the name that BIG-IQ displays.

    When using Active Directory, this is typically `displayName`.
17. To direct bind to a distinguished name, in the **User Bind Template** field, type the name.
    For example, `cn={username},ou=people,o=sevenSeas`.

    Now, when a user logs in, BIG-IQ inserts the user name into the template in place of the token, and the resulting distinguished name is used to bind to the directory.

18. To prompt the LDAP provider to search for groups based on a specific display name attribute, in the **Group Display Name Attribute** field, type an attribute.

    This attribute is typically `cn`.

19. Leave the **Group Search Filter** at its default query to return all groups under the provided rootDN.

    Alternatively, if you have a large number of groups (more than 100), you can base the search on a specific term by typing a query with a `{searchterm}` token in this field.

    For example: `(&(objectCategory=group)(cn={searchterm}*))`

20. To specify a query for finding a users group, in the **Group Membership Filter** field, type a query string.

    Use the token `{userDN}` anywhere that the user's distinguished name should be supplied in the LDAP query.

    You can use a `{username}` token as a substitute for the user's login name in a query.

    Leave this setting at the default `(|(member={username})(uniqueMember={username}))` unless the provider is Active Directory.

21. To specify a query attribute for finding users in a particular group, in the **Group Membership User Attribute** field, type the attribute.

    When using Active Directory, use `memberof`. For example:
    `(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)`

    For other LDAP directories, use `groupMembershipFilter`. For example:
    `(groupMembership=cn=group_name,ou=organizational_unit,o=organization)`

22. Select the **Perform Test** check box to test this provider.
23. Click the **Save & Close** button at the bottom of the screen.

Create an LDAP-authenticated user group

Before you can add an LDAP-authenticated user group, you must set up BIG-IQ® to use your company's LDAP server for user authentication (using the **USER MANAGEMENT** > **Auth Providers** screen).

You create a user group to offer a set of individual users authentication from the same LDAP server.

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **LDAP**.
6. In the **Remote Group** field, type a term to search for remote groups.
7. In the **Group DN** field, type the domain name for this group.
8. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
9. Click the **Save & Close** button at the bottom of the screen.

Use my RADIUS server to authenticate and authorize BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's RADIUS server. After you set up BIG-IQ to use your RADIUS server, you can add users and user groups authorized by that server.

Before integrating BIG-IQ with your RADIUS server for authentication and authorization

Before you set up BIG-IQ® Centralized Management for authentication and authorization with your RADIUS server, gather the following information.

Required Information	This is	For my RADIUS server
Name	The name of your RADIUS server.	
Host	The IP address or host name of your RADIUS server.	
Port	The port number of your RADIUS server.	
Secret	The case-sensitive text string used to validate communication.	
Test user name and password	A user name and password, authenticated on your RADIUS server.	
Key and Value properties for your RADIUS server	The RADIUS server uses this for authentication and encryption.	

Set up BIG-IQ to use my RADIUS server for user authentication

Before you can set up authentication, you must have specified your DNS settings. You usually do this when you license F5® BIG-IQ® Centralized Management.

You can set up BIG-IQ to use your company's RADIUS server. You can add two additional backup RADIUS servers in case the primary server is not available for authentication.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **RADIUS.**
5. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.
6. For the **Servers** setting, In the **Host** and **Port** fields, type the RADIUS server's IP address (or fully qualified domain name) and port number for each of the servers you want to configure.

   The primary server is mandatory. A secondary server and tertiary server, which will be used if the primary or secondary servers fail, are optional.
7. In the **Secret** field, type the case-sensitive text string used to validate communication.
8. In the **Test User** and **Test Password** fields, type a user and password, then click the **Test** button to verify that BIG-IQ can reach the RADIUS server
9. Click the **Save & Close** button at the bottom of the screen.

You can now associate RADIUS server users and groups with BIG-IQ system roles.

Update BIG-IQ dictionary with vendor-specific RADIUS attributes

You must have root access to the BIG-IQ system's command line through SSH for this procedure.

Some RADIUS deployments include non-standard, vendor-specific attributes in the dictionary files. For these deployments, you must update the BIG-IQ system's default dictionary.

1. Copy the TinyRadius .jar file from the BIG-IQ system.
2. Extract the contents of the TinyRadius `.jar` file.
3. Update the file `org/tinyradius/dictionary/default_dictionary` file, by adding the vendor-specific attributes.
4. Repack the contents into a new `.jar` file.
5. Replace the old TinyRadius `.jar` on each BIG-IQ system with the new TinyRadius .jar file you created in step 4.

For example:

1. From a Linux machine, copy the TinyRadius `.jar` file to your BIG-IQ system by typing: `scp <big-iq-user>@<BIG-IQ-Address>:/usr/share/java/TinyRadius-1.0.jar ~/tmp/tinyrad-upgrade/`
2. Extract the file on your Linux Machine by typing: `jar -xvf TinyRadius-1.0.jar`
3. Edit the `org/tinyradius/dictionary/default_dictionary`, adding the vendor-specific attribute.

```
rm TinyRadius-1.0.jar
jar cvf TinyRadius-1.0.jar *
```

4. Update the jar on the BIG-IQ system by typing: `scp TinyRadius-1.0.jar <your_user>@<BIG-IQ address>:/var/tmp/`
5. SSH to the BIG-IQ system and type the following commands:

```
mount -o remount,rw /usr
cp /var/tmp/TinyRadius-1.0.jar /usr/share/java
mount -o remount,ro /usr
bigstart restart restjavad
```

6. Repeat steps 4 and 5 for each BIG-IQ in a HA configuration.

Now you can use the vendor-specific attributes RADIUS to create your user groups on BIG-IQ.

Create a user group authorized by your RADIUS server

Before you can add a RADIUS-authenticated user group, you must set up BIG-IQ to use your company's RADIUS server for user authentication on the **USER MANAGEMENT** > **Auth Providers** screen

Create a user group to offer individual users the same privileges on F5® BIG-IQ® Centralized Management. This user group will be authorized by your RADIUS server.

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **RADIUS**.
6. In the **Key** and **Value** fields, type the properties for your RADIUS server.
7. From the **User Roles** list, select the user role you want to associate with this user.

   You aren't required to associate a user role at this point; you can do that later. If you want to add another user role, click +.
8. Click the **Save & Close** button at the bottom of the screen.

You can now associate users with this user group.

Using my TACACS+ server to authenticate and authorize BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's TACACS+ server. After you set up BIG-IQ to use your TACACS+ server, you can add users and user groups that are authenticated by your TACACS+ server.

Before integrating BIG-IQ with your TACACS+ server for authentication and authorization

Before you set up BIG-IQ® Centralized Management for authentication and authorization with your TACACS+ server, you should gather this information.

Required Information	This is	For my TACACS+ server
Name	The name of your TACACS+ server.	
Host	The IP address or host name of your TACACS+ server.	
Port	The port number of your TACACS+ server.	
Secret	The case-sensitive text string used to validate communication.	
Primary Service	The service that the authorization requests are made for, such as system, shell, or connection.	
Protocol	An optional subset of a service, such as `telnet`, `ip`, or `http`.	
Test user name and password	A user name and password, authenticated on your TACACS+ server.	

Set up BIG-IQ to use my TACACS+ server for user authentication

Before you can set up authentication, you must have specified your DNS settings. You usually do this when you license F5® BIG-IQ® Centralized Management. You must also complete all the tasks outlined in *Before integrating BIG-IQ with your TACACS+ server*.

You can set up BIG-IQ to use your company's TACACS+ server for user authentication.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **TACACS+.**
5. For the **Servers** setting, in the **Host** and **Port** fields, type the TACACS+ server's IP address (or fully qualified domain name) and port number for each of the servers you want to configure.

   To add more servers, just click the + button.
6. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.

7. In the **Primary Service** field, specify what type of authorization requests will be made for this service.

   For example: `system`, `connection`, or `PPP`.
8. In the **Protocol** field, specify an optional subset of a service.

   For example: `ip`, `telnet`, or `http`.
9. To encrypt the data, select the **Yes** check box for the **Encrypt** setting.
10. To verify that BIG-IQ can reach the TACACS+ server, in the **Test User** and **Test Password** fields, type a valid user name and password, and click the **Test** button.
11. Click the **Save & Close** button at the bottom of the screen.

You can now associate TACACS+ server users with BIG-IQ system roles.

Create a TACACS+-authenticated user group

Before you can add a TACACS+-authenticated user group, you must set up BIG-IQ® to use your company's TACACS+ server for user authentication (using the **USER MANAGEMENT** > **Auth Providers** screen).

You create a user group to offer a set of individual users authentication from the same TACACS+ server.

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **TACACS+**.
6. For the **Authorization Attributes** setting, in the **Attribute** and **Value** fields, type the attribute and value pair for this group's TACACS+ server.
7. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
8. Click the **Save & Close** button at the bottom of the screen.

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 August 10, 2017.

Publication Number

MAN-0497-08

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

N

O

P

R

S

T

U

V