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

Version 5.1

Table of Contents

BIG-IQ System Introduction

About BIG-IQ System Management

From the BIG-IQ® system, you can easily manage the following aspects of its operation:

- Licensing
- Network settings
- High availability settings
- User authorization and role management
- Alerts
- Logging and health monitoring
- Backups and restoration

Additionally, you can review reports about the usage of BIG-IQ system resources. This helps you keep an eye on the health of your system.

About secure communication with BIG-IQ

To manage devices in your network, including BIG-IQ peer systems, the BIG-IQ system communicates over HTTPS port 443.

Open ports required for device management

The BIG-IQ system requires bilateral communication with the devices in your network in order to successfully manage them. For this communication, the following ports are open by default to allow for the required two-way communication.

Open Port	Purpose
TCP 443 (HTTPS)	Discovering, monitoring, and configuring managed devices
TCP 443 (HTTPS) and TCP 22 (SSH)	Upgrade BIG-IP devices running version 11.4.0-11.6.0
TCP 443 (HTTPS)	Upgrade BIG-IP devices running version 12.0.0
TCP 443 (HTTPS)	Replicating and synchronizing BIG-IQ systems

What is the default administrator and root user names and passwords?

You access BIG-IQ with the following administrative user roles and a default password. You can change these passwords after you license the system.

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.

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

Licensing, Initial Setup, and Upgrades

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

The BIG-IQ® system 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 system.

You get a license for BIG-IQ 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.

After you license BIG-IQ, you:

- Specify a host name for the system.
- Assign a management port IP address.
- Specify the IP address of your DNS server and the name of the DNS search domain.
- Specify the IP address of your Network Time Protocol (NTP) servers and select a time zone.
- Change the administrator's default admin and root passwords.

Automatically licensing BIG-IQ and performing initial setup

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 (`http://www.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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
3. Click **Activate**.
   The Base Registration Key field is added to the screen.
4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
5. In the **Add-On Keys** field, paste any additional license key you have.
6. To add another additional add-on key, click the + sign and paste the additional key in the new **Add-On Keys** field.
7. For the **Activation Method** setting, select **Automatic**, and click the **Activate License** button.
   The End User Software License Agreement (EULA) displays.
8. To accept the license agreement, click the **Agree** button.
9. Click the **Next** button at the right of the screen.
   If the license you purchased supports both Logging Node and BIG-IQ Central Management Console, the License Feature Selection popup screen opens. Otherwise the Management Address screen opens.

10. If you are prompted with the License Feature Selection, select **BIG-IQ Central Management Console**, and then click **OK**. If you are not prompted, proceed to the next step.

    Important: *This choice cannot be undone. Once you license a device as a BIG-IQ Management Console, you cannot change your mind and license it as a Logging Node.*

    The Management Address screen opens.
11. In the **Host Name** 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 (.).
12. In the **Management Port IP Address** field, type the IP address for the management port IP address.

    Note: *The management port IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`.
13. In the **Management Port Route** field that the system creates, type the IP address for the management port route.
14. 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.

      Note: *The self IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`.
15. Click the **Next** button at the right of the screen.
16. In the **DNS Lookup Servers** field, type the IP address of your DNS server.

    You can click the **Test Connection** button to verify that the IP address is reachable.
17. 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.
18. In the **Time Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.

    You can click the **Test Connection** button to verify that the IP address is reachable.
19. From the **Time Zone** list, select your local time zone.
20. Click the **Next** button at the right of the screen.
21. 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.
22. Click the **Next** button at the right of the screen.

Manually licensing BIG-IQ and performing initial setup

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 (`http://www.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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
3. Click **Activate**.
   The Base Registration Key field is added to the screen.
4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.

5. In the **Add-On Keys** field, paste any additional license key you have.
6. For the **Activation Method** setting, select **Manual** and click the **Generate Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
7. Select and copy the text displayed in the **Device Dossier** field.
8. Click the **Access F5 manual activation web portal** link.
   The Activate F5 Product site opens.
9. 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 license key text displays.
10. Click the **Next** button.

    The Accept User Legal Agreement screen opens.
11. To accept the license agreement, select the **I have read and agree to the terms of this license**, and click **Next**. button.
    The licensing server creates the license key text.
12. Copy the license key.
13. In the **License Text** field on BIG-IQ, paste the license text.
14. Click the **Activate License** button.
15. Click the **Next** button at the right of the screen.
    If the license you purchased supports both Logging Node and BIG-IQ Central Management Console, the License Feature Selection popup screen opens. Otherwise the Management Address screen opens.
16. If you are prompted with the License Feature Selection, select **BIG-IQ Central Management Console**, and then click **OK**. If you are not prompted, proceed to the next step.

    Important: *This choice cannot be undone. Once you license a device as a BIG-IQ Management Console, you cannot change your mind and license it as a Logging Node.*

    The Management Address screen opens.
17. In the **Host Name** 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 (.).
18. In the **Management Port IP Address** field, type the IP address for the management port IP address.

    Note: *The management port IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`*.*
19. In the **Management Port Route** field that the system creates, type the IP address for the management port route.
20. 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.

      Note: *The self IP address must be in Classless Inter-Domain Routing (CIDR) format. For example:* `10.10.10.10/24`*.*
21. Click the **Next** button to save your configuration.
22. In the **DNS Lookup Servers** field, type the IP address of your DNS server.

    You can click the **Test Connection** button to verify that the IP address is reachable.
23. 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.

24. In the **Time Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.

    You can click the **Test Connection** button to verify that the IP address is reachable.
25. From the **Time Zone** list, select your local time zone.
26. Click the **Next** button at the right of the screen.
27. 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.
28. Click the **Next** button at the right of the screen.

Additional Network Configuration Options

About additional network configuration options

During the licensing and initial configuration procedures, you configure a single VLAN and associated self IP addresses. This is all the networking configuration required to start managing devices. However, if you find you need additional VLANs and self IP addresses, the BIG-IQ® system provides you with the ability to add them as required.

Adding an additional VLAN

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

You have the option to configure an additional VLAN after you license and perform the initial configuration of the BIG-IQ system.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. On the left, click **NETWORK SETTINGS** > **VLANs**.
4. Click the **Add VLAN** button.
5. In the **Name** and **Description** fields, type a unique name and description to identify this new VLAN.
6. 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.
7. 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.
8. 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.
9. Click the **Add** button at the bottom of the screen to save this VLAN.

Adding an additional self-IP address

You must have configured BIG-IQ® with at least one VLAN before you can add an additional self IP address.

You have the option to configure an additional self IP address after you license and perform the initial configuration of the BIG-IQ system.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **NETWORK SETTINGS** > **Self IPs**.
5. In the **Name** field, type a unique name to identify this new self IP address.
6. In the **Address** field, type the self IP address and netmask.
7. In the **Description** field, type a description for this self IP address.
8. From the **VLAN** list, select the VLAN to associate with this self IP address.
9. Click the **Add** button at the bottom of the screen to save this new self IP address.

How do I manage access to BIG-IQ and my managed BIG-IP devices?

As a network or system manager, you need a way to differentiate between users, and to limit user access based on how they interact with F5® BIG-IQ® Centralized Management and your managed devices.

You can specify how you want users to be authenticated: locally on BIG-IQ, or remotely through your RADIUS or LDAP server. Additional security is provided through bidirectional trust and verification through key and certificate exchange (AuthN and AuthZ).

To help you manage all of this, it's important that you understand the following concepts:

- *Users* - are individuals for whom you are providing access to BIG-IQ resources, including access to managed BIG-IP® devices.
- *User groups* - are a way to organize individuals into groups so that you can grant or change the same privileges to several users at once.
- *Roles* - are associated with specific privileges, which you grant to users, allowing them to do a set of tasks on BIG-IQ, and on your managed devices.

Changing the default password for the administrator user

When you license and do the initial setup, F5® BIG-IQ® Centralized Management system prompts you to automatically create the administrator user.

For security reasons, it is important to change the administrator role password from the default, `admin`.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **USER MANAGEMENT** > **Users**.
5. In the User Name column, click **admin**.
   The Admin User properties screen opens.
6. In the **Old Password** field, type the password.
7. In the **Password** and **Confirm Password** fields, type a new password.
8. Click the **Save** button at the bottom of the screen.

Add a locally-authenticated user

Create a user to provide access to F5® BIG-IQ® Centralized Management.

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

4. On the left, click **USER MANAGEMENT** > **Users**.
5. Click the **Add** button.
6. From the **Auth Provider** list, select **Local**.
7. In the **User Name** field, type the user name for this new user.
8. 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.
9. In the **Password** and **Confirm Password** fields, type the password for the new user.
10. 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.
11. From the **User Roles** list, select a user role to associate with this user.

    Each role has a set of unique privileges.
12. Click the **Save** button at the bottom of the screen.

Create a locally-authenticated user group

You create a user group so that you can easily manage privileges for several users at one time.

1. Log in to BIG-IQ with your admin user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
5. Click the **Add** button.
6. In the **Name** field, type a name for this new user group.
7. From the **Auth Provider** list, select **Local**.
8. From the **Users** list, select the user you want to associate with this user group.

   You aren't required to add users at this point; you can do that later.
9. 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.
10. Click the **Save** button at the bottom of the screen.

The new group displays in the User Groups list.

You can now add users and associate user roles to this new group.

Can I 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

Before integrating LDAP authentication with the BIG-IQ® system, you must first perform the following tasks:

- Use an LDAP browser to review the groups and users in your directory's structure and where they're located in the hierarchy of organizational units (OUs).
- Decide how you want to map user names.

  - 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, when you map John Smith's user name with his DN as `uid=<jsmith>, ou=people,o=sevenSeas` and he logs in as `jsmith`, he is 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-I system can validate the user's credentials.
- Decide which groups in your directory to map into 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 for all users and groups. This is the root bind DN for your directory, defined as 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.
- Find the host IP address for the LDAP server. The default port is 389, if not specified otherwise.

Set up BIG-IQ to use an LDAP 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 F5 BIG-IQ Centralized Management to user your company's LDAP server to authenticate users. You can specify multiple LDAP servers for user authentication.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **USER MANAGEMENT** > **Auth Providers**.
   The Auth Providers screen opens.
5. Click the **Add** button.
6. From the **Provider Type** list, select **LDAP**.
7. 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.
8. In the **Host** field, type the IP address of your LDAP server.
9. If your Active Directory server uses a port other than the default, 389, in the **Port** field, type the number of the alternative port.
10. If you want BIG-IQ to use an SSL port to communicate with the LDAP server, for the **SSL Enabled** setting, select the **Enabled** check box.

    Note that the **Port** setting automatically changes to **636**.
11. 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.
12. In the **Root DN** field, type the root context that contains users and groups.

    The root context must be a full distinguished name.
13. From the **Authentication Method** list, select an option.
    - **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.

14. In the **Search Scope** field, type a number to specify the depth at which searches are made.

    Alternatively, you can specify `0` for search only on the named object or `1` for a one-level search scope.
15. In the **Search Filter** field, type the LDAP filter expression that determines how users are found.

    The search filter is determined by your LDAP implementation.
16. In the **Connect Timeout** field, type the number of milliseconds after which the BIG-IP system stops trying to connect to the LDAP server.
17. In the **Read Timeout** field, type the number of seconds the BIG-IP system will wait for a response to a query.
18. 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`.
19. 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.
20. 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`.
21. 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}*))`
22. 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.
23. 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)`
24. Select the **Perform Test** check box to test this provider.
25. Click the **Save** button at the bottom of the screen.

BIG-IQ Centralized Management now authenticates users against the configured LDAP server.

Add a BIG-IQ user authenticated by my LDAP server

If you want to add a user authenticated against your LDAP server, you first have to set up F5® BIG-IQ® Centralized Management with your LDAP server settings.

You create a user so you can then associate that user with a particular role to define access to F5® BIG-IQ® Centralized Management system resources.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. On the left, click **USER MANAGEMENT** > **Users**.

3. Click the **Add** button.
4. From the **Auth Provider** list, select **LDAP**.
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 the new user.
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.
9. From the **User Roles** list, select a user role to associate with this user.

   Each role has a set of unique privileges.
10. Click the **Save** button at the bottom of the screen.

Create an LDAP-authenticated user group

You create a user group to offer individual users authentication from an LDAP server.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
5. Click the **Add** button.
6. In the **Name** field, type a name for this new user group.
7. From the **Auth Provider** list, select **LDAP**.
8. To associate this user group with an existing LDAP group, leave the **Remote Group Filter** field blank, click the **Search** button, and select it from the **Remote Group** list.
9. In the **Group DN** field, type the group's distinguished name.
10. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
11. Click the **Save** button at the bottom of the screen.

Can I use my RADIUS server to authenticate 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 authenticated by that server.

Set up BIG-IQ to use a 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.

Before you can set up authentication, you must have specified your DNS settings. You usually do this when you license the F5 BIG-IQ Centralized Management system. You can set up F5 BIG-IQ Centralized Management 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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.

3. At the top of the screen, click **Inventory**.
4. On the left, click **USER MANAGEMENT** > **Auth Providers**.
5. Click the **Add** button.
6. From the **Provider Type** list, select **RADIUS.**
7. 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.
8. 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.
9. In the **Secret** field, type the case-sensitive text string used to validate communication.
10. 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
11. Click the **Save** button at the bottom of the screen.

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

Pre-defined RADIUS groups for authentication

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. Follow these steps if you want to use pre-defined RADIUS user groups on BIG-IQ.

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.

Add a BIG-IQ user authenticated by my RADIUS server

If you want to add a user authenticated against your RADIUS server, you first have to set up F5® BIG-IQ® Centralized Management with your RADIUS server settings.

You create a user so you can then associate that user with a particular role to define access to F5® BIG-IQ® Centralized Management resources.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **USER MANAGEMENT** > **Users**.
5. Click the **Add** button.
6. From the **Auth Provider** list, select **RADIUS**.
7. In the **Name** field, type a name for this server.

   This must be a unique name and a maximum of 152 characters.
8. 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.

   A primary server is mandatory. A second and tertiary server (used only if the primary or secondary servers fail) are optional.
9. In the **Secret** field, type the case-sensitive text string the RADIUS server uses to validate communication.
10. In the **Test User** and **Test Passwords** fields, type a user name and password, then click the **Test** button to verify that BIG-IQ can reach the RADIUS server.
11. Click the **Save** button at the bottom of the screen.

Create a RADIUS-authenticated user group

You create a user group to offer individual users authentication from a RADIUS server.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
5. Click the **Add** button.
6. In the **Name** field, type a name for this new user group.
7. From the **Auth Provider** list, select **RADIUS**.
8. For the **Connect Properties** setting, into the **Key** and **Value** fields, type the key and value for this group's RADIUS server.
9. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
10. Click the **Save** button at the bottom of the screen.

How do I limit privileges for users?

As a system manager, you need a way to limit user privileges based on their responsibilities. To help you do that, F5® BIG-IQ® Centralized Management ships with a set of default roles that you can assign to users. Roles are shared between BIG-IQ systems in a high availability pair, so they remain assigned to users even if the primary BIG-IQ system fails over.

Standard roles shipped with BIG-IQ

F5® BIG-IQ® Centralized Management ships with several standard roles, which you can assign to individual users, or to a user group. Roles are shared between BIG-IQ systems in a high availability pair, so they remain assigned to users even if the BIG-IQ system fails over.

Role	Role Description / Access
Administrator	This role has access to all licensing aspects of System Management and Device Management. This includes access for adding individual users, assigning roles, discovering BIG-IP® systems, installing updates, activating licenses, and setting up BIG-IQ® in a high availability (HA) configuration.
ADC Deployer	This role has access to deploy and view ADC configuration objects for managed ADC devices.
ADC Editor	This role has access to edit all ADC configuration objects.
ADC Manager	This role has access to all aspects of ADC, including areas involved in creating, viewing, modifying, and deleting Local Traffic and Network objects.
ADC Viewer	This role has view-only access for all ADC objects and features.
Access Auditor	This role has access to all Access reports and dashboard.
Access Deployer	This role has deploy access to Access configuration objects. This role cannot discover and edit devices or policies.
Access Editor	This role has edit access to Access configuration objects. This role cannot discover and deploy devices or policies. This role includes the ability to add, update, and delete pools and pool members from the Access configuration object editor.
Access Manager	This role has deploy and edit access to Access configuration objects, and has access to Access Reports and Dashboard. This role cannot add or remove devices and device groups, and cannot discover, import, or delete services.
Access Viewer	This role has view-only access to Access configuration objects and tasks for Access devices that have been discovered. This role cannot edit, discover, or deploy devices or policies.
Device Manager	This role has access to all aspects of Device Management, including areas involved in device discovery, group creation, licensing, software image management, UCS backups, templates, connectors, certificates, self IP addresses, VLANs, and interfaces.
Device Viewer	This role has read-only access to all aspects of Device Management, including areas involved in device discovery, group creation, licensing, software image management, UCS backups, templates, connectors, certificates, self IP addresses, VLANs, and interfaces.
Fraud Protection Manager	This role has access to all aspects of the Fraud Protection Service functionality for Web Client Security.
Fraud Protection View	This role has view-only access to all Fraud Protection Service objects for Web Client Security .

Role	Role Description / Access
Network Security Deploy	This role has access to view and deploy Network Security objects.
Network Security Manager	This role has access to all aspects of Network Security, including areas involved in creating, viewing, modifying, and deleting shared and firewall-specific security objects.
Network Security Edit	This role has access to create, view, and modify objects for Network Security.
Network Security View	This role has view-only access to firewall objects for Network Security. This role cannot edit, discover, or deploy devices or policies.
Security Manager	This role has access to all aspects of Network Security, Web Application Security, and Web Client Security, including areas involved in device discovery, creating, viewing, modifying, and deleting Web Application Security, shared and firewall-specific security objects.
Trust Discovery Import	This role manages device trust establishment, service discovery, service import, removal of services and removal of trust.
Web App Security Deployer	This role can deploy and view ASM configuration objects for managed ASM devices.
Web App Security Editor	This role manages config objects within the ASM module.
Web App Security Manager	This role has access to all aspects of Web Application Security, including areas involved in creating, viewing, modifying, and deleting shared and web application-specific security objects.
Web App Security Viewer	This role permits read-only access to the ASM module.

Associating a user or user group with a role

Before you can associate a user or user group with a role, you must create a user or user group.

When you associate a user or user group with a role, you define the resources users can view and modify. You can associate multiple roles with a given user.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. From the **User Roles** list, select a user role to associate with this user.

   Each role has a set of unique privileges.
5. From the **Active Users and Groups** list, select the users or user groups to add to this role.
6. Click the **Save** button at the bottom of the screen.

This user or user group now has the privileges associated with the role you selected.

Disassociating a user from a role

Use this procedure to disassociate a user from an assigned role.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **USER MANAGEMENT** > **Users**.
5. On the Users inventory list, click the name of the user.

The screen refreshes to display the properties for this user.

6. 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.

7. Click the **Save** button to save your changes.

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

How can I get set up BIG-IQ to alert me when certain events happen on my managed devices?

You can easily integrate BIG-IQ® to work with SNMP and/or SMTP. After you set up SNMP and/or SMTP on BIG-IQ, you can choose alerts that prompt a message to be sent when the event or a threshold is met on a managed BIG-IP device.

How do I set up BIG-IQ to work with SNMP?

Simple Network Management Protocol (*SNMP*) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks. You can set up BIG-IQ® to work with SNMP so you can receive alerts when certain things happen on a managed device.

To set up BIG-IQ to work with SNMP, you must:

1. Set up the SNMP Agent
2. Configure SNMP Access
3. Specify settings for the SNMP Trap

Before you configure SNMP

Gather the following information before you start your SNMP configuration.

CONFIGURATION COMPONENT	CONSIDERATIONS
SNMP administrator contact information	Find out or decide who is responsible for SNMP administration. The contact information is a MIB-II simple string variable.
Machine location	Find out the location of the BIG-IQ system. The location is a MIB-II simple string variable.
BIG-IQ client allow list	Gather the IP or network addresses (with netmasks) of the SNMP managers from which the SNMP agent will accept requests.
Access	Find the OID for the top-most node of the SNMP tree to provide access to.
Community	Get the v1 and v2c communities and the IP addresses of the SNMP managers you want to grant access to.
Users	Get the v3 users you want to grant access to SNMP data, along with the privacy protocols and passwords, Community, Destination, and Port.

Configuring SNMP agent for sending alerts

You configure the SNMP on BIG-IQ® so the SNMP manager can collect data for receiving alerts when certain things happen on your managed devices.

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

3. At the top of the screen, click **Inventory**.
4. On the left, click **LOCAL HOST SETTINGS** > **SNMP Configuration** > **SNMP Agent**.
   The screen displays the SNMP settings.
5. At the top of the screen, click the **Download MIB** button to download the F5-required MIBs.
6. At the top of the screen, click **Edit**.
7. Edit the **Contact Information** and **Machine Location** fields to reflect your SNMP agent settings and click the **Save** button at the bottom of the screen.
8. For the **SNMP Access - Client Allowed List** setting, click the **Add** button.
9. In the **Addresses/Networks** and **Mask** fields, type the IP address and networks and the netmask (if applicable) that the SNMP manager is allowed to access.
10. To add another address, click the plus (+) sign.
11. Click the **Save** button when you are finished.

You can now configure SNMP access and SNMP traps.

Configuring Access and Traps for SNMP version 1 and 2C to send alerts

You configure SNMP access to allow the SNMP agent to accept requests from specific SNMP managers.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **LOCAL HOST SETTINGS** > **SNMP Configuration** > **SNMP Access (v1, v2C)**
5. Click the **Add** button.
6. In the **Name** field, type the SNMP manager's user name.
7. From the **Type** list, select the format for the IP address.
8. In the **Community** field, type the community string (password) for access to the MIB.
9. From the **Source** list, select a source or select **Specify** and type the source address for access to the MIB.
10. In the **OID** field, type the object identifier (OID) you want to associate with this user.
11. From the **Access** list, select an option:
    - **Read Only** - This user can only view the MIB.
    - **Read/Write** - This user can view and modify the MIB.

    The most secure access level or type takes precedence when there is a conflict. When you set the access level to read/write, and an individual data object has a read-only access type, access to the object remains read-only.
12. Click the **Save** button at the bottom of the screen to save your changes.
13. On the left, click **SNMP Traps**.
14. In the **Name** field, type a name for this SNMP trap.
15. From the **Version** list, select **v2 or 2C**.
16. In the **Community**, **Destination**, and **Port** fields, type, respectively, the community name, IP address, and port for the trap destination.
17. Click the **Save** button at the bottom of the screen to save your changes.

You can now specify alert conditions, by clicking **ALERTS** on the left.

Configuring Access and Traps for SNMP version 3 to send alerts

You configure SNMP access to allow the SNMP agent to accept requests from specific SNMP managers.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click On the left, click **LOCAL HOST SETTINGS** > **SNMP Configuration** > **SNMP Access (v3)**.
5. Click the **Add** button.
6. In the **Name** and **User Name** fields, type a name for this SNMP access and the user name.
7. If you want to specify the authentication protocol for SNMP traps, from the **Type** list, select an option.
   - **MD5** specifies digest algorithm.
   - **SHA** specifies secure hash algorithm.
8. If you selected an authentication protocol, in the **Password** and **Confirm Password** fields, type and confirm the password for access.
9. If you want to encrypt the SNMP traps, from the **Protocol** list, select an option.
   - **AES** specifies Advanced Encryption Standard
   - **DES** specifies Data Encryption Standard
10. In the **Password** and **Confirm Password**fields, type and confirm the password for access.

    The password must be between 8 and 32 characters, include alphabetic, numeric, and special characters, but no control characters.
11. In the **OID** field, type the object identifier (OID) you want to associate with this user.
12. In the **Destination**, and **Port** fields, type the IP address and the port for the trap destination.
13. From the Security Level list, select the level of security at which you want SNMP messages processed.
    - **Auth, No Privacy** process messages without encryption.
    - **Auth & Privacy** process messages using authentication and encryption.
14. In the **Security Name** field, type the user name the system uses to handle SNMP v3 traps.
15. In the **Engine ID** field, type an administratively unique identifier for an SNMP engine.

    This setting is optional. You can find the engine ID in the `/config/net-snmp/snmpd.conf` file as the value of the `oldEngineID` token.
16. From the **Authentication Protocol** list, select the type of authentication to use to authentication SNMP v3 traps.
17. In the **Password** and **Confirm Password** fields, type and confirm a password for this SNMP trap.
18. On the left, click **SNMP Traps**.
19. In the **Name** field, type a name for this SNMP trap.
20. From the **Version** list, select **V3**.
21. In the **Community**, **Destination**, and **Port** fields, type, respectively, the community name, IP address, and port for the trap destination.
22. Click the **Save** button at the bottom of the screen to save your changes.

You can now specify alert conditions, by clicking **ALERTS** on the left.

How do I set up BIG-IQ to work with SMTP?

To have a specific recipient receive an email message when an alert is triggered by a system event, configure BIG-IQ® to deliver locally-generated email messages using the internet-standard for electronic mail transmission, Simple Mail Transfer Protocol (SMTP). Sending an email alert ensures that administrators are immediately notified when a specific system event occurs so they can quickly troubleshoot potential issues.

To set up BIG-IQ to work with SMTP, you must:

1. Set up an SMTP Server
2. Add SMTP Email Recipients

Configuring SMTP for sending alerts

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

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

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

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

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

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

Setting up alert conditions

After you set up the SNMP and/or SMTP on BIG-IQ®, you can select the alerts that prompt BIG-IQ to send an email to the people you specified.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **ALERTS**.
5. Click the **Edit** button at the top of the list.
6. Select the **Enabled** check box next to alert conditions you want to enable, and (where applicable) in the **Threshold** field, type the maximum point the condition should reach before BIG-IQ notifies you.
7. Click the **Save** button at the bottom of the screen.

How can I get set up BIG-IQ to alert me when certain events happen on my managed devices?

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 10 minutes. If it ever becomes necessary, you can have the secondary peer take over management of the BIG-IP devices.

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

Before you can configure BIG-IQ systems for high availability (HA), 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 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 you can still manage your BIG-IP® devices even if one BIG-IQ systems fails.

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. On the left, click **BIG-IQ HA**.
4. Click the **Add Device** button.
5. Type the properties for the BIG-IQ system you are adding, and then click the **Add** button at the bottom of the screen.

Promoting 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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IQ HA**.
5. Select the check box next to the secondary BIG-IQ system, and click the **Promote to Primary** button.

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

Deleting a BIG-IQ system from a high availability pair

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

1. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. Log in to the primary BIG-IQ system, using administrator credentials.
5. From the BIG-IQ list, select **System**.
6. Click the **Remove** button.
7. Click the **Delete** button.

The primary BIG-IQ system is now standalone.

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 systeme's configuration, including:

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

Creating a backup of the BIG-IQ system's UCS file

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

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

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

   If you configured BIG-IQ to save backup files to a remote server and that server is unavailable during a scheduled backup, BIG-IQ ignores the local retention policy and retains the local copy of the backup file. This ensures that a backup is always available. To remove those local backups, you must delete them.
10. To keep copies of backups remotely on a SCP or SFTP server:
    a) For the **Archive** setting, select the **Store archive copy of backup** check box.
    b) For the **Location** setting, select **SCP** or **SFTP**.
    c) In the **IP Address** field, type the IP address of the remote server where you want to store the archives.
    d) In the **User Name** and **Password** fields, type the credentials to access this server.
    e) In the **Directory** field, type the name of the directory where you want to store the archives on the remote server.

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

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

11. Click the **Save** button

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

Scheduling BIG-IQ system's UCS file backups

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

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

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

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

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

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

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

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

You must create a backup of a BIG-IQ system's UCS file before you can restore it.

If you need to roll back to a previous configuration, 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. 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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BACKUP & RESTORE** > **Backup Files**.
5. 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.

BIG-IP iHealth

What is iHealth?

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

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

How do I get access to the F5 iHealth diagnostics server from BIG-IQ?

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

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

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

You can now upload BIG-IQ QKView files to the F5 iHealth server to get iHealth reports.

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

You can easily limit how much traffic is dedicated to file activity related to iHealth® if you need to. You do this by specifying a limit of simultaneous file transfers to and from F5® BIG-IQ® Centralized Management.

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

Troubleshoot BIG-IQ issues by uploading a QKView file to the F5 iHealth server

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

You upload a QKView file to F5 Networks to create an iHealth diagnostics report. You can use that report to troubleshoot any potential issues with the BIG-IQ system.

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

   This step is not required.
8. From the **Credential** list, select the credentials to log in to the iHealth diagnostic site.
9. Click the **Upload** button at the bottom of the screen.

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

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

Download an iHealth diagnostics report for BIG-IQ

F5 creates a BIG-IQ® iHealth® diagnostics report after you upload the BIG-IQ® Centralized Management system's QKView file to F5.

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

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

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

BIG-IQ downloads the report you selected in the form of a PDF.

You can now open and review the iHealth diagnostics report.

Legal Notices

Legal notices

Publication Date

This document was published on September 14, 2016.

Publication Number

MAN-0497-06

Copyright

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

Trademarks

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

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

Patents

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

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Index