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

Version 4.6

# Table of Contents

# Legal Notices

## Legal notices

### Publication Date

This document was published on November 23, 2015.

### Publication Number

MAN-0497-04

### Copyright



### Trademarks



### 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.

# BIG-IQ System Introduction

## Overview: BIG-IQ Centralized Management

The BIG-IQ® system is a tool that streamlines the management of F5 devices in your network. Because it is based on the same platform as BIG-IP® devices, it includes full product support, security patches, and internal and external security audits (AuthN and AuthZchecks).

Firewall managers use the BIG-IQ system to manage security firewalls for multiple devices from a central location. Firewall management includes discovering, editing, and deploying firewall configurations, as well as consolidating shared firewall objects. Once a firewall device is designated for central management, it is no longer managed locally unless there is an exceptional need.

Web-Application Security managers also use the BIG-IQ system to centrally manage policy files and attack-signature files. Multiple BIG-IP® devices can share the same policy and attack-signature files for filtering HTTP, HTTPS, and other web traffic for known attack patterns.

Network administrators use BIG-IQ Device to interact with all of the managed F5 devices in their network. This centralized management includes the ability upgrade F5 devices, update configurations, and reallocate licenses as needed.

Application Delivery Controller (ADC) offers you the flexibility to deploy software images, and configurations, and monitor and distribute licenses and license pools for managed BIG-IP devices.

## About incorporating BIG-IQ system securely into your network

To successfully manage devices in your network, including BIG-IQ peer systems, the BIG-IQ system requires communication over HTTPS port 443. The BIG-IQ administrator can provide fine-grained access to various roles, which are verified by authorization checks (AuthN and AuthZ). Authenticated users have access only to the resources explicitly granted by the BIG-IQ administrator. Additional security is provided through bidirectional trust and verification through key and certificate exchange and additional support for LDAP and RADIUS authentication.

### 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 |

| Open Port | Purpose |
|---|---|
| TCP 443 (HTTPS) | Replicating and synchronizing BIG-IQ systems |

## Additional resources and documentation for BIG-IQ systems

You can access all of the following BIG-IQ® system documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`.

| Document | Description |
|---|---|
| BIG-IQ® Centralized Management Virtual Editions Setup guides | BIG-IQ® Virtual Edition (VE) runs as a guest in a virtual environment using supported hypervisors. Each of these guides is specific to one of the hypervisor environments supported for the BIG-IQ system. |
| *BIG-IQ® Centralized Management: Licensing and Initial Setup* | This guide provides the network administrators with basic BIG-IQ system concepts and describes the tasks required to license and set up the BIG-IQ system in their network, including how to add users and assign roles to those users. |
| *BIG-IQ® Centralized Management: Device* | This guide provides details about how to deploy software images, licenses, and configurations to managed BIG-IP® devices. |
| *BIG-IQ® Centralized Management: ADC* | This guide provides details about how to centrally manage BIG-IP® Local Traffic Manager™ applications. |
| *BIG-IQ®Centralized Management: Security* | This guide contains information used to centrally manage BIG-IP® firewalls, policies, rule lists (as well as other shared objects), and users. |
| *Platform Guide: BIG-IQ® 7000 Series* | This guide provides information about setting up and managing the BIG-IQ 7000 hardware platform. |
| Release notes | Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds. |
| Solutions and Tech Notes | Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information. |

## About the BIG-IQ system user interface

The BIG-IQ® system interface is composed of panels. Each panel contains objects that correspond to a BIG-IQ feature. Depending on the number of panels and the resolution of your screen, some panels may be collapsed and show as colored bars on either side of the screen. You can cursor over the collapsed panels to locate the one you want, and click the panel to open. To associate items from different panels, click an object, and drag and drop it onto the object with which you want to associate it.

## Filtering for associated objects

The BIG-IQ® system helps you easily see an object's relationship to another object, even if the objects are in different panels.

1. To display only items associated with a specific object, hover over the object, click the gear icon, and then select **Show Only Related Items**.
   The screen refreshes to display only associated objects in each panel.
2. To highlight only items associated with a specific object, hover over the object, click the gear icon, and then select **Highlight Related Items**.
   The screen refreshes, highlighting only associated objects in each panel, and displaying unassociated objects in a gray font.
3. To remove a filter, click the **X** icon next to the filtered object in a panel or click **Clear All** to clear all of the filters.

## Searching for specific objects

The BIG-IQ® system interface makes it easy to search for a specific object. This can be especially helpful as the number of objects increase when you add more users, applications, servers, and so forth.

1. To search for a specific object, in the Filter field at the top of the screen, type all or part of an object's name.
2. Click the **Apply** button.
   The screen refreshes to display only the objects associated with the term you typed in the Filter field.
3. To further refine the filter, type another term into the Filter field, and click the **Apply** button again.
4. To remove a filter term, click the **X** icon next to it.

## Customizing panel order

You can customize the BIG-IQ® system interface by reordering the panels.

1. Click the header of a panel and drag it to a new location, then release the mouse button.
   The panel displays in the new location.
2. Repeat step 1 until you are satisfied with the order of the panels.

# Software Download, Licensing, and Upgrades

## About downloading software, licensing, and upgrading the BIG-IQ system

BIG-IQ® system runs as a virtual machine in specifically-supported hypervisors or on the BIG-IQ 7000 series platform. After you set up your virtual environment or your platform, you can download the BIG-IQ software, and then license the BIG-IQ system. You initiate the license activation process with the base registration key.

The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license. If the system has access to the internet, you select an option to automatically contact the F5 license server and activate the license. If the system is not connected to the internet, you can manually retrieve the activation key from a system that is connected to the internet, and transfer it to the BIG-IQ system.

### Downloading a software image from F5 Networks

Downloading a software image is the first step to making it available for new installations, upgrades, or hot fixes.

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

The software image is now available for you to upload to the BIG-IQ system and make it available for managed devices.

### Uploading a software image to the BIG-IQ system

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

Upload a software image to make it available for new installations, upgrades, or hot fixes.

1. Log in to BIG-IQ Device with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Images panel, and click the + icon when it appears, and then click **New Software Image**.
4. Click the **Choose File** button and navigate to the location to which you downloaded the image, and click it to upload it to BIG-IQ Device.
   The software image appears in the Images panel.

The software image is now available for you to deploy.

## Installing BIG-IQ System software

Before you perform an initial BIG-IQ® System software installation, you must perform the following tasks:

- Activate, or reactivate, your current license to ensure that you have a valid service check date.
- Download the ISO file for the upgrade from `https://downloads.f5.com` and upload it to the BIG-IQ system's Images panel.

Use this procedure when you are ready to perform an initial BIG-IQ System software installation or upgrade to a more recent software version.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, expand **Management Group** or **HA Peer Group** by clicking the arrow next to it.
4. Click the gear icon next to **localhost**, and then click **Properties**.
5. Click **Software Update**.
6. Click the **Update** button.
7. From the **Software Image** list, select the new image.
8. From the **Install Location** list, select the volume to which you want to install the image.
9. For the **Options** setting, select one:
   - To automatically reboot the BIG-IQ System to the specified volume immediately after the software is installed, select **Reboot into Target Volume**.
   - To manually reboot the BIG-IQ System at another time from the **System** > **Properties** screen, select **Set Default Boot Location**.
10. Click the **Apply** button.

BIG-IQ System installs the selected software. For upgrades, BIG-IQ System also rolls forward the UCS file.

## Automatic license activation

You must have a base registration key to 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 use this procedure to activate its license.

1. Using a browser on which you have configured the management interface, type `https://<varname><management_IP_address><varname>` where `<management_IP_address>` is the address you specified for device management.

   This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.
   The License Agreement displays.
6. To accept the License Agreement, click the **Agree** button.

7. Click **User Administration**.
8. 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.
9. Click **Properties**.
10. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.

    The FQDN can consist of letters and numbers, as well as the characters underscore ( _ ), dash ( - ), or period ( . ).
11. Click the **Save** button to save your configuration.

## Manual license activation

You must have a base registration key to 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, this procedure can activate its license.

1. Using a browser on which you have configured the management interface, type `https://<varname><management_IP_address><varname>` where `<management_IP_address>` is the address you specified for device management.

    This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. 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.
6. Copy the text displayed in the **Device Dossier** field, and click the **Click here to access F5 Licensing Server** link.

    Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
7. Click **Activate License**.
   The Activate F5 Product page opens.
8. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
   After a pause, the license key text will display.
9. Copy the license key.
10. In the **License Text** field on the BIG-IQ Device, paste the license key text.
11. Click **User Administration**.
12. 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.
13. Click **Properties**.
14. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.

    The FQDN can consist of letters and numbers, as well as the characters underscore ( _ ), dash ( - ), or period ( . ).
15. Click the **Save** button to save your configuration.

# About the upgrade process for BIG-IQ systems configured in a high availability (HA) configuration

When a new version of the BIG-IQ software is available, you can upgrade. The upgrade process involves installing the new version of the software, booting into that new version, and making any other changes that might be required.

***Note:*** *BIG-IQ® Security version 4.6.0 supports upgrades only from version 4.4.0 and higher. This restriction does not apply for other BIG-IQ functionality.*

When the BIG-IQ system is in a high availability (HA), you must also perform the following procedures:

1. Delete peer BIG-IQ systems in a HA configuration.
2. Upgrade each BIG-IQ system.
3. Re-establish the HA configuration.

## Separating an HA configuration running version 4.3 software

The upgrade process disconnects the high availability (HA) redundant system configuration during upgrade and reinstates the configuration again as the upgrade is completed. This procedure separates an HA configuration running version 4.3 software.

1. Separate the HA configuration by removing the standby device from the device group.
   a) Log in to the active BIG-IQ device and at the top-right corner of the BIG-IQ Security screen, select **System** and **Overview**.
   The Localhost screen opens.
   b) On the left, click **High Availability**.
   The screen displays the configuration for the Peer device (the standby node).
   c) Click the **Delete** button at the top-right corner of the Localhost screen.
   A pop-up screen appears to confirm that you want to remove the standby device from the device group.
   d) Click the **Remove** button to confirm.
   e) Watch the HA-status indicator at the top-left corner of the screen. When the HA configuration is separated, the indicator changes from `Active (Primary)` to `Standalone`.

   The status indicator at the top-left of the screen now reports Standalone on both BIG-IQ devices.
2. Use a secure copy method to copy the image (ISO) to the `/shared/images` directory on both devices formerly in the HA configuration.

   You can use SCP, FTP, SFTP or any other means of securely transferring ISOs between hosts.

   `scp <big-iq-iso-name> root@<big-iq-standby-node-url>:/shared/images/.`

Both devices are now standalone and have the same ISO file on them.

## Separating an HA configuration running version 4.4 software

The upgrade process disconnects the HA redundant system configuration during upgrade and reinstates the configuration again as the upgrade is completed. This procedure separates an HA configuration running version 4.4 software.

1. Separate the HA configuration by removing the standby device from the management group.
   a) Log in to the active BIG-IQ device, and from the BIG-IQ option list at upper left, select **System**.
   b) In the BIG-IQ Systems panel, expand **Management Group**.
   c) Select the standby device.
   d) Hover over the gear icon, click it and select **Properties**.
   The Localhost screen opens.
   e) In the expanded screen, click **Remove**.

   The status indicator at the top-left of the screen now reports `Standalone` on both BIG-IQ devices.
2. Use a secure copy method to copy the image (ISO) to the `/shared/images` directory on both devices formerly in the HA configuration.

   You can use SCP, FTP, SFTP or any other means of securely transferring ISOs between hosts.

   `scp <big-iq-iso-name> root@<big-iq-standby-node-url>:/shared/images/.`

Both devices are now standalone and have the same ISO file on them.

## Separating an HA configuration running version 4.5 software

The upgrade process disconnects the HA redundant system configuration during upgrade and reinstates the configuration again as the upgrade is completed. This procedure separates an HA configuration running version 4.5 software.

1. Separate the HA configuration by removing the standby device from the management group.
   a) Log in to the active BIG-IQ device, and from the BIG-IQ option list at upper left, select **System** and click **Configuration**.
   b) In the BIG-IQ Systems panel, expand **HA Peer Group**.
   c) For the standby device, hover over the gear icon, click it, and select **Properties**.
   The Properties screen for that device opens.
   d) Near the top right of the Properties screen, click **Remove**.
   A dialog box opens prompting you to confirm that you want to remove the device from this group.
   e) Click **Delete** in the dialog box to confirm the removal.

   The status indicator at the top-left of the screen now reports `Standalone` on both BIG-IQ devices.
2. Use a secure copy method to copy the image (ISO) to the `/shared/images` directory on both devices formerly in the HA configuration.

   You can use SCP, FTP, SFTP or any other means of securely transferring ISOs between hosts.

   `scp <big-iq-iso-name> root@<big-iq-standby-node-url>:/shared/images/.`

Both devices are now standalone and have the same ISO file on them.

## Upgrading BIG-IQ system (system interface)

After you have disconnected the HA redundant system configuration, you need to upgrade BIG-IQ® through the system user interface.

1. This step applies to BIG-IQ devices running version 4.3 software; skip this step if your devices are running version 4.4 or 4.5 software, or if you use are using BIG-IQ Security which does not support upgrading from version 4.3. For version 4.3, repeat these substeps on both devices to upgrade the image on each.

---

***Note:*** *BIG-IQ Security only supports upgrading from version 4.4 or 4.5 to version 4.6. Upgrading BIG-IQ Security from version 4.3 is not supported.*

---

a) Log in to the active BIG-IQ device and at the top-right corner of the screen, select **System** and **Overview**.
The Localhost screen opens.
b) Select **Software Update** from the options on the left.
Information about the current software displays in the viewing area.
c) From the **Software Image** list, select the image to use for the update. This is the image you downloaded.
d) From the **Install Location** list, select the location to use for the update.
e) For the **Option** setting, select both options.
f) Click the **Apply** button in the lower-right corner of the panel.
A pop-up screen prompts you to confirm that you want to reboot the device.
g) Click the **OK** button in the pop-up screen.
The BIG-IQ system loads the new software and reboots.

**2.** This step applies to devices running version 4.4 software; skip this step if your devices are running version 4.3 or 4.5 software. For version 4.4, repeat these substeps on both devices to upgrade the image on each.

a) On the BIG-IQ Systems panel, expand **Management Group**.
b) Hover over the gear icon, then click it and select **Properties**.
c) Click **Software Update**.
d) Click **Update**.
e) From the **Software Image** list, select the image to use for the update. This is the image you downloaded.
f) From the **Install Location** list, select the location to use for the update.
g) For the **Options** setting, click **Reboot After Live Install**.

**3.** This step applies to devices running version 4.5 software; skip this step if your devices are running version 4.3 or 4.4 software. For version 4.5, repeat these substeps on both devices to upgrade the image on each.

a) Log in to the active BIG-IQ System as administrator, and click **Configuration**.
b) On the BIG-IQ Systems panel, expand **HA Peer Group**.
c) Hover over the localhost device, click the gear icon, and select **Properties**.
d) Click **Software Update**.
e) Click **Update**.
f) From the **Software Image** list, select the image to use for the update. This is the image you downloaded.
g) From the **Install Location** list, select the location to use for the update.
h) For the **Options** setting, click **Reboot After Live Install**.

**4.** For both devices, verify that the image is booted on the correct volume using the command `tmsh show sys software`.

**5.** On the BIG-IQ System user interface, re-establish the HA redundant system configuration.

When re-establishing the HA configuration, the source device copies its common configuration data to the target device. The source device is the device where you start the process of re-instating the HA configuration. Select a source device whose configuration data is the most up-to-date.

a) On the device you have selected to be the Primary/Active device, navigate to the BIG-IQ Systems panel, and hover over the gear icon for the **HA Peer Group**.

b) Click **Add Device**.
The New Device screen opens.
c) Enter the HA Communication Address of the peer device, and administrator credentials for the secondary BIG-IQ device.
d) For Network Security configurations, select **Active-Standby** as the **High Availability Mode**.
e) Click the **Add** button.
f) Affirm the confirmation to start the re-instatement process.

6. On the BIG-IQ Systems panel, expand the **HA Peer Group** and monitor the status changes for the newly-added device.
   a) Monitor the status updates in the new device entry under the management group.
   b) Monitor the device/cluster status indicator at the top left of the screen.
   When the indicator changes to `Active (Primary)` the reinstatement of the redundant system configuration has completed successfully.

7. Visually examine the configuration of both devices to verify that they are synchronized.

Each device has been upgraded and reinstated into a redundant system configuration. The upgrade is complete.

After the upgrade, to prevent potential BIG-IQ system user interface issues, clear the cache in the web browser you use to access the BIG-IQ system.

# About the upgrade process for a standalone BIG-IQ system

When a new version of the BIG-IQ software is available, you can upgrade. The upgrade process involves installing the new version of the software, booting into that new version, and making any other changes that might be required.

***Note:*** *For BIG-IQ® Security version 4.6.0 supports upgrades only from version 4.3.0 and higher. This restriction does not apply for other BIG-IQ functionality.*

## Upgrading the software for a standalone BIG-IQ system

Before you perform an upgrade for the BIG-IQ® system software, you must perform the following tasks:

- Reactivate your current license to ensure that you have a valid service check date.
- Download the ISO file for the upgrade from `https://downloads.f5.com` and upload it to the BIG-IQ system's Images panel.
- Create a backup of the user configuration set (UCS), locate it in the `/var/local/ucs` directory on the source installation location, and copy the UCS file to another system for safe keeping.

Use this procedure when you are ready to perform an initial BIG-IQ System software installation or upgrade to a more recent software version.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, expand **Management Group** or **HA Peer Group** by clicking the arrow next to it.
4. Click the gear icon next to **localhost**, and then click **Properties**.

5. Click **Software Update**.
6. Click the **Update** button.
7. From the **Software Image** list, select the new image.
8. From the **Install Location** list, select the volume to which you want to install the image.
9. For the **Options** setting, select one:
   - To automatically reboot the BIG-IQ System to the specified volume immediately after the software is installed, select **Reboot into Target Volume**.
   - To manually reboot the BIG-IQ System at another time from the **System** > **Properties** screen, select **Set Default Boot Location**.
10. Click the **Apply** button.

BIG-IQ System installs the selected software. For upgrades, BIG-IQ System also rolls forward the UCS file.

# Initial Configuration for the BIG-IQ System

## Defining DNS and NTP servers for the BIG-IQ system

After you license the BIG-IQ® system, you can specify the DNS and NTP servers.

Setting your DNS server and domain allows the BIG-IQ system to properly parse IP addresses. Defining the NTP server ensures that the BIG-IQ system's clock is synchronized with Coordinated Universal Time (UTC).

1. Log in to BIG-IQ System with your administrator user name and password.
2. On the BIG-IQ Systems panel, click the gear icon next to the group name for which you want to define the DNS and NTP servers, and then click **Properties**.
3. Click **Services**.
4. In the **DNS Lookup Servers** field, type the IP address of your DNS server.
5. 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.
6. In the **Time Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.
7. Click the **Save** button to save your configuration.

## Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system to automatically create the administrator user.

After you initially license and configure the BIG-IQ system, it is important to change the administrator role password from the default, `admin`.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, for **Admin User**, click the gear icon and then **Properties**.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click **Save**.

## Setting the time zone on a BIG-IQ system

To set the time zone for the BIG-IQ system, you must have root access.

After you license and perform the initial configuration for the BIG-IQ system, you can set the time zone. Setting the time zone from the command line ensures it displays the same in the BIG-IQ system's user interface as well as the logs. The default time zone is United States Pacific Time zone.

1. Log in to the BIG-IQ system command line.
2. To view the available time zones, type `ls -laR /usr/share/zoneinfo`
3. To set the time zone, type the following command: `tmsh modify sys ntp timezone <timezone_filename>`

   For example, for the United States Pacific Time zone, type `tmsh modify sys ntp timezone America/Los_Angeles`

Logs and the user interface now display the same time zone.

# Overview: SNMP and SMTP alerts

You can easily manage the health of your network by configuring the BIG-IQ® system to alert you when specific events occur for your managed devices. You can receive notifications by having the BIG-IQ system send traps to your SNMP manager and you can also configure the BIG-IQ system to send alerts for certain events to a specified individual. SNMP is an industry standard protocol for monitoring devices on IP networks. BIG-IQ Device integrates easily with your SNMP manager, allowing you to centrally manage collected data. Once configured, the SNMP agent sends data collected from BIG-IQ Device to your third-party SNMP manager. BIG-IQ Device is compatible with SNMPv1, SNMPv2c, and SNMPv3. Additionally, you can specify SNMP events to also trigger SMTP alerts.

## Configuring SNMP version 3 for alerts

You configure the SNMP agent and provide specific access to BIG-IQ® Device so that the SNMP manager can collect data.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Click the gear icon next to name of the BIG-IQ system for which configure SNMP, and then click **Properties**.
4. Click **SNMP Config**.
   The screen displays the SNMP settings.
5. In the **Contact Information** field, type the name and email address of the person who is responsible for SNMP administration, and in the **Machine Location** field, type the location of the SNMP manager system.

   These details are for informational purposes only and have no impact on how BIG-IQ Device interfaces with your SNMP manager.
6. To download the F5-specific MIBs, click the **Download MIB** link.
7. 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.
8. To add another address, click the plus ( + ) sign.
9. Click the arrow next to **Access**.
   The SNMP Access settings display.
10. For the **Record Type** setting, select **V3**.

11. In the **User Name** field, type the SNMP manager's user name.
12. If you want to specify the authentication protocol for SNMP traps, from the **Auth Type** list, select the type that you want the system to use.
    - **MD5** specifies digest algorithm.
    - **SHA** specifies secure hash algorithm.
13. If you selected an encryption type from the **Privacy Protocol** list, also select the type of encryption you want the system to use to encrypt SNMP traps.
    - **AES** specifies Advanced Encryption Standard
    - **DES** specifies Data Encryption Standard
14. In the **Privacy Password** field, type the required password for access.

    SNMPv3 has special requirements when you create plain-text passwords on a router or switch:
    - The password must be at least eight characters long.
    - The password can include alphabetic, numeric, and special characters, but it cannot include control characters.
15. In the **OID** field, type the object identifier (OID) you want to associate with this user.
16. Click the arrow next to **Trap**.
17. From the **Version**, select the version of SNMP you are using.
18. In the **Destination** and **Port** fields, type, respectively, the IP address and system port for the SNMP management system.
19. 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 and Privacy** process messages using authentication and encryption.
20. In the Security Name field, type the user name the system uses to handle SNMP v3 traps.
21. 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.
22. From the **Auth Protocol** list, select the type of authentication to use to authentication SNMP v3 traps.
23. In the **Auth Password** field, type the password the system uses for an SNMP v3 trap.

    The password must be at least 8 characters in length and no more than 32 and can include alphabetic, numeric, and special characters, but it cannot include control characters.
24. If you selected **Auth and Privacy** from the **Security Level**l list, then from the **Privacy Protocol** list, select the algorithm the system uses to encrypt SNMP v3 traps. When you set this value, you must also enter a value in the **Privacy Password** field.
25. To configure additional SNMP trap destination, click the plus ( + ) sign and specify the settings
26. When you've finished adding traps, click the **Save** button located at the top of the panel.

You can now specify alert settings. You set alert conditions from the BIG-IQ System group properties screen.

## Configuring SNMP version 1 or 2 for alerts

You configure the SNMP agent and provide specific access to BIG-IQ® Device so that the SNMP manager can collect data.

1. Log in to BIG-IQ System with your administrator user name and password.

2. At the top of the screen, click **Configuration**.
3. Click the gear icon next to name of the BIG-IQ system for which configure SNMP, and then click **Properties**.
4. Click **SNMP Config**.
   The screen displays the SNMP settings.
5. In the **Contact Information** field, type the name and email address of the person who is responsible for SNMP administration, and in the **Machine Location** field, type the location of the SNMP manager system.

   These details are for informational purposes only and have no impact on how BIG-IQ Device interfaces with your SNMP manager.
6. To download the F5-specific MIBs, click the **Download MIB** link.
7. 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.
8. To add another address, click the plus ( + ) sign.
9. When you've finished adding traps, click the **Save** button located at the top of the panel.
10. Click the arrow next to **Access**.
    The SNMP Access settings display.
11. In the New v1/v2 Access Records section, from the **Type** list, select the appropriate protocol for the SNMP manager's IP address.
12. In the **Community** field, type the name of the associated community.
13. Click the arrow next to **Trap**.
14. In the New v1/v2c Destinations section, from the **Version** list, select the version of SNMP you are using.
15. In the **Community**, **Destination**, and **Port** fields, type, respectively, the community name, IP address, and port for the trap destination.
16. To configure additional SNMP trap destination, click the plus ( + ) sign and specify the settings
17. When you've finished adding traps, click the **Save** button located at the top of the panel.

You can now specify alert settings. You set alert conditions from the BIG-IQ System group properties screen.

## Configuring SMTP for alerts

Before you define an SMTP server, you must first configure a DNS server.

Configure SNMP alerts to send specified recipients email when an alert condition happens.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover on the HA Peer Group, click the gear icon when it appears, then click **Properties**.
4. Click **SMTP Config**.
5. In the **Name** and **Email Address** fields, type the name and the email address for the person you want to receive and email when a specified alert condition is met.
6. To add an additional recipient, click the + sign and repeat step 5.
7. Click **Server**.
8. In the **Name** field, type a name for this SMTP configuration.
9. In the **SMTP Server Host** and **SMTP Server Port** fields, type the SMTP server and TCP port.

   By default, SMTP uses TCP 25.
10. In the **From Address** field, type the email address from which to send the alert email.

11. From the **Encryption** list, select the type of encryption to use for the email.
12. To require a user name and password, select **Yes** from the **Use Auth** list and type the required user name and password.
13. To save this configuration, click **Save**.

You can now specify the alert conditions that prompt the BIG-IQ system to send an email to the specified receipient when the condition is met.

### Specifying alert conditions

After you configure SNMP and or SMTP integration, you can specify the alerts that prompt BIG-IQ® System to send an email to the specified recipients.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Click the gear icon next to the group for which you want to specify alert conditions, and then click **Properties**.
4. Click **Alert Conditions**.
5. Select the check box next to each event that should trigger an alert email.
6. If a threshold is associated with the condition, in the adjacent **Threshold** field, type a value on which you want to trigger an alert email.
7. Click **Save**.

## About authentication integration

Integrating BIG-IQ® systems with your authentication server allows you to remotely manage user access based on specific BIG-IQ system roles and associated permissions.

The BIG-IQ system is compatible with RADIUS and LDAP protocols.

### Configuring authentication with RADIUS

You must first license the BIG-IQ system and specify DNS settings before you can specify authentication settings.

When you configure the BIG-IQ® system for user authentication through your company's RADIUS service, you can associate existing and new users added to the RADIUS service with specific BIG-IQ roles. The permissions associated with those roles are based on the user credentials. You can add two additional backup RADIUS servers in case the primary server is not available for authentication.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, click the gear icon next to the HA Peer Group you are configuring, and then click **Properties**.
4. Click **Auth Provider**.
5. If you do not want to display the local host provider on the initial log on screen, select the **Do not display Local Host provider option on the login screen if a 3rd-party provider is configured** check box.

6. From the **User Directory** list, select **Remote RADIUS**, and click the **Add** button.
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 **Failback Time** field, type the number of minutes to wait to contact the primary RADIUS server if it was previously unreachable and authentication was being performed by the secondary or tertiary RADIUS server.
9. 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.
10. In the **Secret** field, type the case-sensitive text string used to validate communication.
11. To verify the RADIUS server settings, in the **Username** and **Password** fields, type a valid user name and password and click **Test Connection**.
12. Click the **Save** button.

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

## Configuring BIG-IQ system to to use pre-defined RADIUS groups

To perform this procedure, you must have root access to the BIG-IQ system's command line through SSH.

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. Use this procedure if you are using pre-defined RADIUS groups to define user groups on the BIG-IQ system.

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 system in this cluster.

Now you can use the user defined RADIUS attribute value pairs to create your user groups on the BIG-IQ system.

## Before configuring LDAP authentication

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

- Use an LDAP browser to familiarize yourself with the groups and users in your directory's structure and their position 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 properly 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.
- Determine 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 have not, you must know the DN for each group.
- Identify the DN under which all users and groups can be found. This is the root bind DN for your directory and is expressed as `rootDN` when you create a provider. The BIG-IQ system uses the root bind DN as a starting point when searching for users and groups.
- Determine the host IP address for the LDAP server. The default port is 389, if not specified otherwise.

## Configuring authentication with LDAP

When you configure the BIG-IQ system for user authentication through your company's LDAP service, you can associate existing and new users added to the LDAP service with specific BIG-IQ roles. The permissions associated with those roles are based on the user credentials. The BIG-IQ system integration is compatible with LDAP server versions 2 and 3, and OpenLDAP directory, Apache Directory Server, and Active Directory. You can add multiple LDAP servers.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. On the BIG-IQ Systems panel, click the gear icon next to the HA Peer Group you are configuring, and then click **Properties**.
4. Click **Auth Provider**.

5. If you do not want to display the local host provider on the initial log on screen, select the **Do not display Local Host provider option on the login screen if a 3rd-party provider is configured** check box.
6. From the **User Directory** list, select **Remote LDAP** and then click the **Add** button.
   The screen refreshes to display LDAP provider properties.
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 System to use an SSL port to communicate with the LDAP server, select the **Enabled** check box for the **SSL Enabled** setting.

    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.

    - **None** - Select this option to prompt the LDAP server to ignore the user name and password.
    - **Simple** - Select this option to require a user name and password for authentication.
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 after which the BIG-IP system stops waiting for a response to a query.
18. In the **User Display Name Attribute** field, type LDAP field to use for the name BIG-IQ System 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 System inserts their 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 narrow 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 to 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.

The BIG-IQ system now authenticates users against the configured LDAP server.

# Users, User Groups, and Roles

## Overview: Users, user groups, and roles

A *user* is an individual to whom you provide resources. You provide access to users for specific BIG-IQ® system functionality through authentication. You can associate a user with a specific role, or associate a user with a user group and then associate the group with a role.

A *role* is defined by its specific privileges. A *user group* is a group of individuals that have access to the same resources. When you associate a role with a user or user group, that user or user group is granted all of the role's corresponding privileges.

By default, the BIG-IQ® system provides the following default user types:

| Default user type | Default password | Access rights |
|---|---|---|
| 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. |

User types persist and are available after a BIG-IQ system failover. You can authenticate users locally on the BIG-IQ system or remotely through LDAP or RADIUS.

### About default passwords for pre-defined users

When you initially license the BIG-IQ® system, it creates the following administrative roles with a default password.

- admin
- root

---

***Note:*** *Refer to the Changing the default password for the administrator user for instructions for changing the default password.*

---

### Adding a locally-authenticated BIG-IQ user

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

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. Hover over the Users header, and click the + icon when it appears.
   The panel expands to display the User properties.
4. From the **Auth Type Provider** list, select **Local**.

5. 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.
6. In the **Password** and **Confirm Password** fields, type the password for the new user.
7. Click the **Add** button.

You can now associate this user with a role.

## About user roles

As a system manager, you need a way to differentiate between users and to limit user privileges based on their responsibilities. To assist you, the BIG-IQ® system has created a default set of roles you can assign to a user. Roles persist and are available after a BIG-IQ system failover.

### Roles definitions

BIG-IQ® system ships with several standard roles, which you can assign to individual users.

| Role | Description |
|---|---|
| Administrator | Responsible for overall administration of all licensed aspects of the BIG-IQ system. These responsibilities include adding individual users, assigning roles, discovering BIG-IP® systems, installing updates, activating licenses, and configuring a BIG-IQ high availability (HA) configuration. |
| Device Manager | Responsible for device administration including device discovery, group creation, licensing, and management of software images, UCS backups, templates, connectors, certificates, self IP addresses, VLANs, and interfaces. This role must first create a group before discovering and managing devices. |
| Network Security Deploy | Can view and deploy firewall configuration objects associated with managed firewall devices. |
| Network Security Edit | Can view and modify configuration objects associated with managed firewall devices, including the ability to create, modify, or delete all shared and firewall-specific objects. |
| Network Security Manager | Has all of the privileges assigned to the Network Security View, Network Security Edit, and Network Security Deploy roles. |
| Network Security View | Can only view configuration objects and tasks for all firewall devices under management. |
| Security Manager | Has all of the privileges assigned to the Network Security View, Network Security Edit, and Network Security Deploy roles. |
| Web App Security Manager | Responsible for administration of the individual components of web application security, including |

| Role | Description |
| --- | --- |
| | associated devices, policies, virtual servers, signature files, and deployments. |

## 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 BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users or User Groups panel, click the name you want to associate with a role, and drag and drop it on a role on the Roles panel.
   A confirmation popup screen opens.
4. Click the **Confirm** button to assign the user or user group to the selected role.

This user or user group now has access to the resources associated with the role you specified.

## Disassociating a user from a role

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

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **System >Users**.
3. Click the name of the user you want to edit.
4. For the User Roles property, delete the user role that you want to disassociate from this user.
5. Click the **Save** button to save your changes.

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

# 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, the BIG-IQ® system provides you with the ability to add them as required.

## Configuring 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 BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the VLANs panel and click the + sign when it appears.
4. In the **Name** and **Description** fields, type a name and description to identify this new VLAN.
5. From the **Device** list, select the BIG-IQ system to associate with this new VLAN.
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. Click the **Add** button to save this VLAN.
8. Hover on the Self IP Addresses panel and click the + when it appears.
9. In the **Name** and **Address** and **Description** fields, type the name, and self IP address.
10. From the Device list, select the BIG-IQ system to associate with this new self IP address.
11. From the **VLAN** list, select the VLAN to which you want to associate this self IP address.
12. Click the **Add** button to save this self IP address.

# BIG-IQ High Availability

## About high availability configurations

To ensure that you always have access to the BIG-IP® devices under BIG-IQ® system management, install two BIG-IQ systems in a high availability (HA) configuration. Configuring for high availability is optional.

---

***Note:*** *Currently, a BIG-IQ HA configuration is limited to two systems, a primary and a secondary, configured as peers. Only the primary BIG-IQ system can manage BIG-IP devices.*

---

With BIG-IQ high availability, the BIG-IQ system periodically replicates the entire BIG-IQ system state from the primary peer to the secondary to keep the two systems synchronized. This synchronization allows the secondary peer to be promoted to be the primary and take over management of the BIG-IP devices if the primary system is not fully functional. There is no automatic fail over from the primary to the secondary.

How often the primary and secondary are synchronized is configurable. In the BIG-IQ HA data replication model, this synchronization interval determines how many minutes is acceptable for the secondary peer to be out-of-date with the primary. By default, the secondary is synchronized with the primary every 10 minutes.

When you initially set up an HA pair, the systems are synchronized and you can see the configuration of what was on the primary updated on the secondary. Subsequently, when you synchronize the systems, you will not see the configuration change since the changes will be copied to the secondary system, but will not be used to update the configuration at that time. If you want to have the configuration updated on the secondary BIG-IQ system, log in to the secondary system and use the **Restart with Last Update from Primary** option.

If the primary BIG-IQ system in an HA cluster fails, then you need to log in to the secondary BIG-IQ system and promote it to being the primary BIG-IQ system.

If you restore a BIG-IQ system configuration using a compressed user configuration set (UCS) file, there are additional tasks you need to perform if that system is in an HA cluster. After restoring the BIG-IQ system configuration, you need to split the HA cluster that system is part of and then recreate the HA cluster.

## About high availability terminology

Terminology is crucial in understanding the status of the high availability (HA) relationship. The following list defines some important terms used in HA configurations.

**primary**
The node you are logged in to when establishing the pair is deemed the *primary node*; the system added is deemed the *secondary node*.

**secondary**
Any node added to the configuration is deemed the *secondary node*. Currently, the BIG-IQ ® system supports a 2-node pairing.

**pairing**
Adding a secondary node to the BIG-IQ system configuration is called *pairing*. During the pairing process, the primary BIG-IQ system discovers information on the secondary node. When it is finished

discovering the secondary system, the primary node creates a storage checkpoint of the current state of the storage on the primary node. When complete, the storage checkpoint is copied to the secondary node, and the secondary node then assumes its new role.

---

***Note:*** *Data is always transferred from the primary node to the secondary node. Storage configuration data is not copied from the secondary node to the primary node, so configuration edits should never be made on the secondary node.*

---

**cluster**

A synonym for a high availability configuration is *cluster*. A cluster comprises at least two BIG-IQ systems (fully installed and licensed, and running the same version of software), and is configured in a high availability relationship through the **BIG-IQ** > **BIG-IQ Systems** > **Properties** screen.

## Pairing BIG-IQ systems for high availability

Before you can configure BIG-IQ® systems for high availability (HA), you must have two licensed BIG-IQ systems, installed with the required system components. For the high-availability pair to synchronize properly, each must be running the same BIG-IQ version, and the clocks on each system must be synchronized within 60 seconds, and remain synchronized. Prior to establishing the pair, examine the NTP settings at the BIG-IQ system level and the current system time value.

You pair two BIG-IQ systems to create a high availability cluster.

1. Select the BIG-IQ system to act as the primary in the HA cluster.

   The configuration of this system is the one that will be preserved.
2. Log in to the selected BIG-IQ system, using administrator credentials.
3. From the BIG-IQ main list, select **System**.
4. Hover over the HA Peer Group, click the gear icon and select **Add Device**.
5. In the New Device screen, complete the following settings:

   These settings define the secondary peer in the HA cluster.
   a) In the **IP Address** field, type the self IP address.
   b) In the **User name** field, type the administrative user name.
   c) For **Password**, type the administrative password.
   d) In the **Root Password** field, type the root password.
   e) From the **Group** list, select **HA Peer Group**.
6. Click **Add**.

When you expand the HA Peer Group, you see both nodes of the HA cluster. The localhost node is the system you are on.

## Splitting a high availability pair

To change or reconfigure peers that are in a BIG-IQ® high availability (HA) pair, you must first delete the HA relationship.

1. Log in to the primary BIG-IQ system, using administrator credentials.

2. From the BIG-IQ list, select **System**.
3. On the BIG-IQ Systems panel, expand the HA Peer Group.
4. Hover over the secondary peer and when the gear icon appears, click it and select **Properties** to open the screen.
5. In the expanded screen, click **Remove**.

The pair is now split. Consult the status line at the top of the screen for the status. Both nodes display a status of Standalone.

## Manually synchronizing the BIG-IQ systems

The BIG-IQ® systems in an HA Peer Group are synchronized automatically. If you need the systems to be synchronized immediately, you can manually synchronize the systems and view information about the synchronization using the properties screen of the primary BIG-IQ system.

1. Log in to the primary BIG-IQ system, using administrator credentials.
2. From the BIG-IQ main list, select **System**.
3. On the BIG-IQ Systems panel, expand the HA Peer Group.
4. Hover over the primary BIG-IQ system and when the gear icon appears, click it and select **Properties** to open the screen.
5. In the expanded screen, on the Properties tab, review the information in the **HA Sync Interval** setting.
   - The number displayed at the top field of this setting is the number of minutes to wait before synchronizing the BIG-IQ systems. By default, this number is 10, but it can be any whole number from 5 to 60.
   - **Next** displays the time the BIG-IQ systems will next be synchronized.
   - The area below the **Next** line lists whether the synchronization succeeded or failed. If it succeeded, the time when the synchronization occurred is listed. If it failed, an error message is listed.
6. Click **Sync Now** to cause the BIG-IQ systems to be synchronized immediately.

The configuration of the primary BIG-IQ system is copied to the secondary BIG-IQ system. You do not see these changes on the secondary system until that system is promoted to being the primary system, or until the secondary system is updated and restarted using the **Restart with Last Update from Primary** option available on the secondary BIG-IQ system.

## Changing how often BIG-IQ systems are synchronized

The BIG-IQ® systems in an HA Peer Group are synchronized automatically at a regular interval. If you need to lengthen or shorten the synchronization interval, you can change it using the properties screen of the primary BIG-IQ system.

1. Log in to the primary BIG-IQ system, using administrator credentials.
2. From the BIG-IQ main list, select **System**.
3. On the BIG-IQ Systems panel header, expand the HA Peer Group.
4. Hover over the primary BIG-IQ system, in this case labeled as localhost, and when the gear icon appears, click it and select **Properties** to open the screen.

5. In the screen on the Properties tab, in the **HA Sync Interval** settings, review the number displayed, and change it if needed.

   This value is the number of minutes to wait before synchronizing the BIG-IQ systems. You can change this value to a whole number from 5 to 60.

6. Click **Save** to save your changes.

## Promoting the secondary from the primary BIG-IQ system

You may want to make the secondary BIG-IQ® system the primary system, such as when the current primary system is having system difficulties. You can promote the secondary BIG-IQ system to be the primary BIG-IQ system while logged on to the primary or the secondary BIG-IQ system. This task describes how to promote the secondary BIG-IQ system while on the primary BIG-IQ system.

1. Log in to the primary BIG-IQ system, using administrator credentials.
2. From the BIG-IQ main list, select **System**.
3. On the BIG-IQ Systems panel, expand the HA Peer Group.
4. Hover over the secondary BIG-IQ system name, and when the gear icon appears, click it and select **Properties** to open the screen.
5. In the expanded screen on the Properties tab, in the **Actions on this Device** setting, click **Promote this Device to Primary**.

The secondary BIG-IQ system is synchronized with the primary BIG-IQ system and promoted to being the primary BIG-IQ system. The primary system assumes the role of the secondary.

## Promoting the secondary from the secondary BIG-IQ system

You may want to make the secondary BIG-IQ® system the primary system, such as when the current primary system is having system difficulties. You can promote the secondary BIG-IQ® system to be the primary BIG-IQ system while logged on to the primary or secondary BIG-IQ system. This task describes how to promote the secondary BIG-IQ system while on the secondary BIG-IQ system.

1. Log in to the secondary BIG-IQ system, using administrator credentials.
2. From the BIG-IQ main list, select **System**.
3. On the BIG-IQ Systems panel, expand the HA Peer Group.
4. Hover over the secondary BIG-IQ system, in this list labeled as localhost, and when the gear icon appears, click it and select **Properties** to open the screen.
5. In the expanded screen on the Properties tab, in the **Actions on this Device** setting, click **Promote this Device to Primary**.

The secondary BIG-IQ system is synchronized with the primary BIG-IQ system and promoted to being the primary BIG-IQ system. The primary system assumes the role of the secondary.

If the primary system goes down, the secondary detects this and displays the Peer Down status at the top of the screen. When you click **Promote this Device to Primary** in this scenario, the secondary becomes a standalone system and restarts. At this point, the HA cluster is broken.

***Note:*** *If the former primary peer comes back online, it still considers itself a primary in an HA cluster, so you need to log in to that system and break the HA pair, resulting in it becoming a standalone system.*

## Updating the secondary BIG-IQ system with changes from the primary

Because configuration changes from the primary BIG-IQ® system are not automatically used to update the configuration of the secondary BIG-IQ system, you may want to periodically update the configuration of the secondary BIG-IQ system manually.

1. Log in to the secondary BIG-IQ system, using administrator credentials.
2. From the BIG-IQ main list, select **System**.
3. On the BIG-IQ Systems panel, expand HA Peer Group.
4. Hover over the secondary BIG-IQ system, in this case, `localhost`, and when the gear icon appears, click it and select **Properties** to open the screen.
5. In the expanded screen on the Properties tab, in the **Actions on this Device** setting, click **Restart with Last Update from Primary**.

The secondary system applies the last set of configuration changes it received from the primary system, and then restarts.

# UCS Backup Management for the BIG-IQ System

## About UCS files

The configuration details of managed devices (including the BIG-IQ® system itself) are contained in a compressed user configuration set (UCS) file. The UCS file contains all of the information required to restore a device's configuration, such as:

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

You can back up devices at regularly scheduled intervals and select the amount of time to save the backups.

### Creating a backup UCS file for the BIG-IQ system

It is best practice to create a backup of the UCS file for each device in your network, including the BIG-IQ® system itself, on a regular basis and before performing a software upgrade. The UCS file backup provides your network with added stability in the event that a system needs to be restored.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Backups panel header, click the + sign when it appears.
4. In the **Name** and **Description** fields, type a file name and description to identify this UCS backup file.

   The file name should match the name of the BIG-IQ system. For example, if the name of the BIG-IQ system is

   `bigiq1`, then the name of the archive file should be `bigiq1.ucs` .
5. From the **Device** list, select the BIG-IQ system for which you want to create the UCS file backup.
6. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.
7. To encrypt the backup file, select the **Encrypt Backup Files** check box, and type and verify the password.
8. To immediately create a backup of the selected device, for the **Schedule Backup** setting, select **Backup Now**.

   Use this option, for example, if you are going to make a significant configuration change that you might want to reverse, or before you upgrade a device.
9. To schedule a backup at regular intervals, select **Daily**, **Weekly**, or **Monthly** for the **Schedule Backup** setting.
   a) If you select **Weekly**, select the check box next to the day of the week you want BIG-IQ Device to create the UCS file backup.
   b) If you select **Monthly**, specify the day of the month you want BIG-IQ Device to create the UCS file backup.
10. For scheduled backups,specify the details:

a) Use the **Start Date** calendar to indicate a day to start this schedule.
b) In the associated field, type the time you want BIG-IQ Device to start this scheduled backup.
c) To specify an end date for the scheduled backup, use the **End Date** field and click a date on the calendar, or run scheduled backups indefinitely, by selecting **No End Date**.

**11.** To store copies of UCS backup archives permanently, select the **Store archive copy of backup** check box and provide credentials for the server to which you want BIG-IQ Device to archive a copy of the UCS file. This provides an extra level of protection by preserving the configuration data on a remote system. In the unlikely event that you need to restore the data and you are unable to access the archive in the BIG-IQ system directory, you still have a backup copy of the configuration data.
a) Select **SCP** or **SFTP**.
b) Specify the **Directory** and **IP Address**.
c) Specify the **User Name** and **Password**.

---

***Tip:*** *Archived copies of UCS backups are retained permanently in the location you specify for the* ***Archiving*** *setting. If you want to clear space and remove archived copies of UCS backups you created, you must navigate to the archive location and manually delete them.*

---

**12.** Use the **Local Retention Policy** setting to specify how you want to keep the backup files.

- In the **Delete local backup copy** field specify the number of days to keep the backup copy before deleting it.
- To retain copies of the UCS backup in the Backups panel indefinitely, select **Never Delete**.

---

***Important:*** *If the location you configure the BIG-IQ system to archive UCS backups is unavailable during the backup procedure, the BIG-IQ systems does not delete the local copy of the UCS backup file as defined by the local retention policy. If the archive server is frequently unavailable, you must navigate to the archive location and manually delete them to free up storage on the BIG-IQ system. By default, the UCS file is saved to the* `/shared/ucs_backups` *directory.*

---

**13.** Click the **Create** button
**14.** To view the status of a scheduled backup or change its description, click the gear icon.

This UCS backup file is now available for restoration.

## 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 BIG-IQ System with your administrator user name and password.
**2.** At the top of the screen, click **Configuration**.
**3.** Hover on the Backups panel, click the gear icon next to the backup that you want to restore, and then click **Properties**.
**4.** Click the **Restore** button.

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

After restoration is complete, you can log back into the BIG-IQ system.

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

You must create a backup of a BIG-IQ 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 any reason your BIG-IQ system becomes inoperable or corrupt, you can use a backup UCS file you stored remotely to restore the BIG-IQ system without having to recreate all of the BIG-IQ system's content.

***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`.

The BIG-IQ system is now running the backup configuration.

# Index

## I



## L



## M



## N



## O



## P



## R



## S

## T



## U



## V



## W