BIG-IQ® Cloud: Cisco APIC Administration

Version 1.0

Table of Contents

Legal Notices....5
Legal Notices....5

BIG-IQ System Introduction....7
About incorporating BIG-IQ system securely into your network....7
Open ports required for device management....7
Overview: BIG-IQ system....7
Additional resources and documentation for BIG-IQ systems....8

Software Licensing and Initial Configuration....9
About software licensing and initial configuration....9
Automatic license activation....9
Manual license activation....10
Confirming the Management Address....10
Defining DNS and NTP servers for the BIG-IQ system....11
Changing the default passwords....11

Users, User Groups, and Roles....13
Overview: Users, user groups, and roles....13
About default passwords for pre-defined users....13
Changing the default password for the administrator user....13
Adding a locally-authenticated BIG-IQ user....14
About user roles....14
Roles definitions....14
Associating a user or user group with a role....15
Disassociating a user from a role....15

License Management....17
Overview: Licensing options....17
About pool licenses....17
Automatically activating a pool license....17
Manually activating a pool license....17
Assigning a pool license to a BIG-IP VE....19
Revoking a pool license from a BIG-IP VE....19

Device Discovery....21
About device discovery and management....21
Discovering a BIG-IP device in your network by its IP address....21

Integrating with Cisco APIC....23
BIG-IQ and Cisco APIC Integration....23
About F5 and Cisco APIC integration....23
About configuring the BIG-IQ device for a Cisco APIC integration....27
About configuring the Cisco APIC for BIG-IQ integration....29

Cloud Tenant Management....39
About creating cloud tenants 39
Creating a tenant....39
Creating a cloud user....39
Associating a user with a tenant's role....40

BIG-IQ High Availability....41
About setting up a high availability cluster 41
Configuring a high availability configuration....41

Glossary....43
BIG-IQ Cloud terminology....43

Legal Notices

Legal Notices

Publication Date

This document was published on February 4, 2016.

Publication Number

MAN-0604-00

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-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

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.

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 11.5.3 and later
TCP 443 (HTTPS)	Upgrade BIG-IP devices running version 12.0.0
TCP 443 (HTTPS)	Replicating and synchronizing BIG-IQ systems

Overview: BIG-IQ system

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). The specific functionality offered is dependent on your software license.

Cloud administrators use BIG-IQ Cloud to provide cloud tenants self-service access to shared computing resources such as networks, servers, storage, applications, and services. Cloud resources can be private or public, depending on the customer's requirements. Each tenant has restricted and dedicated access to cloud resources based on a specific user account or tenant role, ensuring that tenants have access only to their own resources. Cloud resources are easily expanded and reallocated as needed, providing flexible resource balancing.

When integrated with Cisco APIC, BIG-IQ Cloud provides the ability to insert services into the APIC network. APIC administrators can create new device packages that expose APIC function profiles that are based on F5 iApps®. With iApps, you can make changes to Cisco APIC and BIG-IP device interaction without waiting for a new software release from F5. This integration requires APIC version 1.1 or 1.2.

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® Systems 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.
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.

Software Licensing and Initial Configuration

About software licensing and initial configuration

BIG-IQ® Cloud runs as a virtual machine in specifically-supported hypervisors. 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.

There are two methods for activating the product.

- If the system has access to the internet, you select the option to automatically contact the F5 license server and activate the license.
- If the system is not connected to the internet, you manually retrieve the activation key from a system that is connected to the internet, and transfer it to the BIG-IQ system.

Task List

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 has outbound access 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://<management_IP_address>` 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 **Next**. button.
   The End User Software License Agreement (EULA) displays.
6. To accept, click the **Agree** button.
7. Click the **Next** button.
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. 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 (.).
10. Click the **Next** 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://<management_IP_address>` 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 **Get 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 **Access F5 manual activation web portal** 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 displays.
9. Select the check box next to the **I have read and agree to the terms of this license** to agree to the license terms, and then click the **Next** button.
   After a brief pause, the license key text displays.
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Next** button at the top of the page.

You still need to confirm the management address, set up your DNS and NTP services, and update your passwords before you can launch.

Confirming the Management Address

Before you confirm the management address, you must have activated the license.

You need to specify the details of how the BIG-IQ® device communicates.

1. 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 (.).
2. In the **Management Port IP Address** field, type the self IP address of your internal VLAN. The self IP address must be in Classless InterDomain Routing (CIDR) format. For example: `10.10.10.10/24`. This is the self IP address that managed devices use to communicate with the BIG-IQ system. This address is also referred to as the *discovery address*
3. In the **Management Port Route** field, type the default gateway address for the management port.

4. Select the **Use Management Address for HA Peer Communication** check box if you want to use the management port IP address for communication between peer BIG-IQ systems in a high availability configuration.
5. To specify a unique self IP address for communication between peer BIG-IQ systems in a high availability configuration, clear the **Use Management Address for HA Peer Communication** check box and type the self IP address for the HA IP Address in the **Self IP Address** field.

   Note: *The IP address must be specified in CIDR format.*

6. To save your configuration, click the **Next** button.

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. 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.
2. 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.
3. 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.
4. From the **Time Zone** list, select your local time zone
5. Click the **Next** button to save your configuration.

Changing the default passwords

After you initially license and configure the BIG-IQ system, you must confirm or change the administrator role password from the default, `admin`.

1. For the admin account, in the **Old Password** field, type `admin`.
2. In the **New Password** and **Confirm New Password** fields, type a new password.
3. For the root account, in the **Old Password** field, type `default`.
4. In the **New Password** and **Confirm New Password** fields, type a new password.
5. To save this configuration, click the **Next** button.

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.

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

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® Cloud with the 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. For the admin account, in the **Old Password** field, type admin.
5. In the **New Password** and **Confirm New Password** fields, type a new password.
6. For the root account, in the **Old Password** field, type `default`.

7. In the **New Password** and **Confirm New Password** fields, type a new password.
8. To save this configuration, click the **Next** button.

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® Cloud with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users panel, hover over a user, and click the gear 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.
Tenant	A tenant is an entity that can consist of one or more users accessing resources provided by an administrator. Responsibilities include: customizing and deploying application templates, and monitoring the health statistics and performance of applications and servers. ***Note:*** *The BIG-IQ system creates a new role when an administrator creates a new tenant. The*

Role	Description
	connectors each tenant can access are specified when the tenant is created. The name of the new role is based on the tenant name. For example, creating a new tenant named `headquarters-user`*, produces a new role named* `headquarters-user (Cloud Tenant)`.

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® Cloud with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users or User Groups panel, click the name you want to associate with a role, and drag and drop it on a role in the Roles panel.
   A confirmation pop-up 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® Cloud with the 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.

License Management

Overview: Licensing options

You can centrally manage BIG-IP® virtual edition (VE) licenses for a specific set of F5 offerings (for example, BIG-IP LTM® 25M, BIG-IP LTM 200G, and BIG-IP LTM 1G). When a device is no longer needed, you can revoke the license instance and assign it to another BIG-IP VE device. This flexibility keeps operating costs fixed, and allows for a variety of provisioning options. *Pool licenses* are purchased once, and you assign them to a number of concurrent BIG-IP VE devices, as defined by the license. These licenses do not expire.

About pool licenses

Pool licenses are purchased for a particular product offering for a fixed number of devices, but are not permanently tied to a specific device. As resource demands change, you can use BIG-IQ® Device to revoke and reassign those licenses to other BIG-IP® VE devices as required. Pool licenses do not expire.

Automatically activating a pool license

You must have a base registration key before you can activate the license pool.

If the resources you are licensing are connected to the public internet, you can automatically activate the license pool.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears.
   The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.
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 **Automatic**.
   The End User Software License Agreement (EULA) displays.
7. To accept, click the **Accept** button.
   The system reads your license key and adds the activated license to the License panel.

Manually activating a pool license

You must have a base registration key before you can activate the pool license.

If the BIG-IQ® Device you are licensing is not connected to the public internet, you can activate the pool license manually.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears.
   The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.
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 **Get Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
7. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.

   Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
8. Click **Activate License**.
   The Activate F5 Product page opens.
9. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
   After a pause, the license key text displays.
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Activate** button.

    If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

Manually activating offering licenses

Before you can activate the individual offering licenses, you must first activate the license itself.

Activating the offering licenses makes them available for assignment.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the arrow next to the license you previously activated.
   The list expands to display the license offerings associated with this license.
4. Hover over an offering license and click the gear icon when it appears.
5. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.

   Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
6. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
   After a pause, the license key text displays.
7. Copy the license key.
8. On BIG-IQ Device, into the **License Text** field, paste the license key.
9. Click the **Activate** button.

   If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this offering license to a BIG-IP® VE device.

Assigning a pool license to a BIG-IP VE

Before you can assign a pool license to a BIG-IP® VE device, you must activate the license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign the license.

Pool licenses provide you with the flexibility to easily manage resources and operating costs. Use this procedure if you have activated a pool license, but have not yet assigned it to a BIG-IP VE.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device you want to license by clicking the arrow next to it.
   The panel expands to display the list of devices contained in this group.
4. Click the gear icon next to the device you want to license, and then click **License Device**.
5. In the **Name** field, type a name for this license.
6. From the **Licensing** list, select **Use a Pool License**.
7. From the **Pool License** list, select the pool license you want to assign to this device.
8. Click the **Deploy** button.
9. To confirm that the license was successfully deployed, click the gear icon next to the license you deployed, click **Properties**, and then click **Assignments**.
   The device you licensed displays with the license status and the last contact from the BIG-IQ system.

Revoking a pool license from a BIG-IP VE

If traffic decreases to the applications on some of your managed BIG-IP® devices, you can use BIG-IQ® Device to revoke those licenses and assign them to other resources as needed.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device for which you want to revoke a license by clicking the arrow next to it.
4. Click the gear icon next to the device for which you want to revoke a license, and then click **License Device**.
5. From the **Licensing** list, select **Revoke a License**.
6. Click the **Deploy** button.

You can now assign this license to another BIG-IP® device.

Device Discovery

About device discovery and management

You use BIG-IQ® Device to centrally manage resources located on BIG-IP® devices.

The first step to managing devices is making BIG-IQ Device aware of them through the discovery process. To discover a device, you provide BIG-IQ Device the device IP address, user name, and password. Alternatively, you can upload a CSV file to discover a large number of devices. When you discover a device you place it into a group. These groups help you organize devices with similar features, like those in a particular department or running a certain software version.

After you discover devices, you can view and export inventory details about those devices for easy asset management, and you can modify device configurations as required without having to log in to each device individually.

Discovering a BIG-IP device in your network by its IP address

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP™ devices running version 11.5.3 HF3 and later or 11.6 HF6 and later. For proper communication, you must configure the BIG-IQ system with a route to each F5 device you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

Important: *The BIG-IQ system will attempt discovery of BIG-IP devices running versions other than those noted (above) as fully supported. Discovering unsupported devices is not recommended.*

There are two ways to discover F5 devices in your network.

- You can discover a device you previously imported to the BIG-IQ system.
- You can discover a device in your local network.

Important: *When you discover a device, BIG-IQ software will install necessary components on the device, which can cause the traffic management interface (TMM) on the BIG-IP device to restart. Therefore, before discovering a device, verify that no critical network traffic is targeted to the BIG-IP device.*

---

1. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**. The Devices panel expands to show the Discover Device screen.
2. To discover a device:
   - If you previously imported the device to the BIG-IQ system:
     1. For **Source**, select the **BIG-IQ Inventory** option.
     2. Click the device located in the **Available** field, and click the Move button to move it to the **Include** field.
     3. Click **Save** to start the discovery task
   - If the device is in your local network:
     1. For the **Source**, select **IP Address**.

2. For the **IP Address**, specify the device's internal self-IP address.
3. For the **Device Group**, select the group to which you want to add the device.
4. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.

Important: *For successful device discovery, you must use the admin account; not the root account. If root access is needed, the system prompts you for it.*

3. Click **Save** to start the discovery task.

The BIG-IQ system populates the properties of the device that you added in the Devices panel.

Integrating with Cisco APIC

BIG-IQ and Cisco APIC Integration

About F5 and Cisco APIC integration

F5® products integrate with Cisco Application Policy Infrastructure Controller (APIC) using a Device Package. The F5 BIG-IP® Device Package for Cisco APIC downloads from a BIG-IQ device, and then is imported into APIC. The file contains:

- A device model, which describes the features and functions available to APIC on the BIG-IP system
- A device script, which implements the features and functions described by the device model

APIC is built with a standard application programming interface (API) used to configure services implemented by integrated vendor devices, such as F5. The F5 BIG-IP device package for Cisco APIC implements the API specific to the semantics of the BIG-IP system.

Using Cisco APIC, a customer can configure tenants, device clusters containing one or two BIG-IP devices, and service graphs. When a service graph is pushed to the BIG-IP system, the F5 BIG-IP Device Package for Cisco APIC running on Cisco APIC uses iApps® to configure all aspects of the supported service.

Each Tenant context is assigned a unique partition on the BIG-IP system, in the form of `apic_XXXX`, where `XXXX` is the Tenant ID. Similarly, each Tenant is assigned a random, unique route domain ID. After successfully deploying a service graph on the BIG-IP system, you can log in to the BIG-IP system to view the configuration.

Cisco APIC uses a single admin-level userid and password to configure the BIG-IP system on behalf of all tenants. Tenants are not expected to log in to the BIG-IP system to diagnose issues: that is the responsibility of the provider administrator.

When you are choosing BIG-IP devices to integrate with Cisco APIC, F5 recommends you use dedicated device(s), and not a BIG-IP system that is already being used (or will be used) for another purpose. This is mainly because parts of this configuration, especially the device cluster HA setup, are managed by the device package.

Figure 1: The logical flow between Cisco APIC and the BIG-IP system

1. An administrator uses the northbound API or the user interface on APIC for configuration.
2. Service graphs created with the device package cause APIC to push configuration to the BIG-IP system, ascertain health, and obtain statistics (interface counters).
3. The APIC API for L4-L7 services is implemented by the F5 device script.
4. The device script uses iApp calls to translate the standard APIC API calls into BIG-IP system calls to implement the service.
5. Status and information from these calls are packaged and returned to APIC for processing.

APIC-related documentation

- For detailed information about Cisco ACI, see http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html.
- For detailed information about Cisco APIC, see http://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html
- For more information about APIC, refer to your Cisco APIC documentation set.

About network topology using the BIG-IP system integrated with Cisco APIC

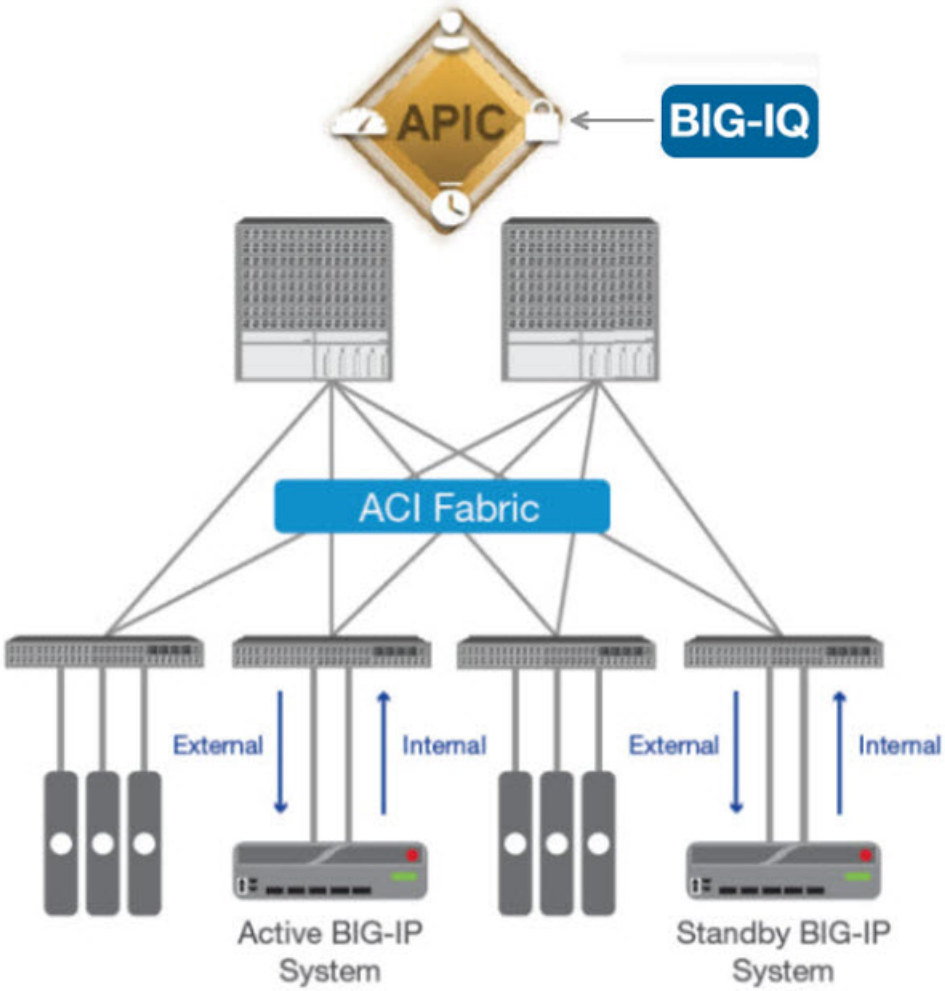

Figure 2: A typical network topology using the BIG-IP® system integrated with Cisco ACI

The internal and external interfaces on the BIG-IP system are connected to leaf nodes in the ACI architecture. Items such as web servers, database engines, and application tiers are also connected to leaf nodes. Spine nodes handle the routing between the BIG-IP system and the various other end points necessary to deliver an application service.

The management port of the BIG-IP system is connected out-of-band to a switch outside of the ACI architecture (not shown in the diagram) to provide management access.

This diagram is not meant to illustrate all possible architectures but rather communicate a typical architecture showing where the BIG-IP system fits into the Cisco ACI architecture.

Important: *Make sure you are using the most recent version of this guide, available at* `http://www.askf5.com`.

Version requirements

Be sure your environment meets or exceeds the requirements described here before you integrate the F5® BIG-IQ® Cloud with Cisco APIC.

- Cisco APIC and Switch software .

Note: *Some features and functions described in this guide require APIC version 1.2. These features will be noted as encountered.*

- F5 BIG-IQ Cloud version 1.0.

Minimum Cisco APIC requirements

Be sure your environment meets or exceeds these requirements before you integrate the F5® BIG-IQ® Cloud with Cisco APIC.

- You must have access to an administrator-level account on the Cisco APIC.
- All external network configuration must be complete.
- The Layer 3 networks must be defined and operational.
- The initial configuration of APIC and ACI must be complete. This includes racking and cabling the hardware, powering on the devices, installing the Cisco APIC and Switch version v1.1 (or v1.2) software, configuring the management IP address and verifying that it is reachable.
- The AAA configuration (such as RADIUS or LDAP) must be completed and operational. You might need to create an application EPG to reach external AAA servers to verify the AAA configuration is functioning properly.
- Any APIC tenants, security domains, private network(s), bridge domain(s), and related objects must be configured and operational.
- Any inter-EPG application filters, contracts, and application profiles (if needed) to facilitate traffic flow between EPGs must be created.
- You must have created a management EPG, which is required for APIC to reach the management IP addresses of the BIG-IP® system(s).
- If you are testing multi-tenancy, you must have access to an account assigned to a tenant.
- If you plan on using the BIG-IP Virtual Edition (VE) in your environment, you must have created a Virtual Machine Mobility (VMM) domain and configured vCenter integration.
- If you plan on using a physical BIG-IP appliance in your environment, you must have created a physical domain.

Refer to the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide* for specific details about how to configure APIC.

Minimum F5 BIG-IP requirements

Be sure your environment meets or exceeds these requirements before you attempt to integrate the F5® BIG-IQ® Cloud with Cisco APIC. Refer to the BIG-IP® system documentation on the F5 technical support site (`http://support.f5.com/kb/en-us/products/big-ip_ltm.html`) for specific information about how to configure the BIG-IP system to meet these requirements.

- You must have access to an administrator-level account on the BIG-IP system.
- The BIG-IP system must be running version 11.5.3 HF2 or version 11.6.0 HF6.
- The BIG-IP system must be cabled to a leaf switch and powered on (if using an appliance) or started in a VMware environment (if using a Virtual Edition).
- You must have discovered the BIG-IP devices you plan to use with the BIG-IQ system.

Important: *Although you can discover BIG-IP devices from BIG-IQ Device, successful integration with the Cisco APIC requires that you perform discovery using BIG-IQ Cloud.*

About configuring the BIG-IQ device for a Cisco APIC integration

Some of the tasks you perform to deploy BIG-IQ® Cloud in a Cisco APIC environment are performed on the BIG-IQ device. You discover devices, create a connector and a custom template, and then export a device package. This device package is the key element of the integration from the Cisco APIC perspective. The parameters and values communicated when you import the package contains the configuration information the Cisco environment needs to perform the integration.

Adding a Cisco APIC connector

Before you add a Cisco APIC connector, you must discover the F5 devices that you plan to include in your Cisco APIC integration.

To enable integration between an APIC and BIG-IQ® Cloud, you must create a connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

Important: *Do not create more than one Cisco APIC connector.*

---

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Connectors header, and click the + icon when it appears..
   The New Connector screen opens.
3. In the **Name** and **Description** fields, type a name and description.

   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
4. From the **Cloud Provider** list, select **Cisco APIC**.
5. Click the **Save** button.

Creating a customized application template

Before you can customize an application template for a tenant, you must discover the F5 devices that you plan to include in your Cisco APIC integration, and add a Cisco APIC connector.

An *iApp* is an application template located on F5 devices. When you discover an F5 device, all iApps® application templates installed on that device are imported to the BIG-IQ® system.

You must create at least one custom catalog template, based on an iApps template, that provides the network settings, levels of services, and so forth, that you expect to see in your APIC environment. You can modify the base template, choosing default values for selected parameters and specifying which parameters can be edited by the tenant. The values specified in the application templates you create are included in the device package that you export to Cisco APIC.

Note: *Once you customize and save an application as a catalog entry, you cannot modify it.*

Important: *If you make modifications to an iApp, you need to save it with a new name. Once an iApp has been imported, it will not be imported again. When an iApp with a new name is saved on a managed BIG-IQ device, BIG-IQ software imports it automatically.*

---

1. In the BIG-IQ Cloud system, hover over the Catalog header and click the + icon when it appears.
   The New Template screen opens.

2. In the **Name** field, type a name for this new template.
3. For the **Input Parameters**, select the option that displays the parameters you want to work with.

   The setting you choose here determines which parameters from the base template that you select display in subsequent fields and areas on the screen.

   - Select **Accept Defaults** if you do not want to edit any parameters.
   - Select **Common Options** if you only want to edit a subset of the template parameters. This option displays parameters that:
     - are marked as tenant-editable
     - describe the virtual server or pool
   - Select **All Options** to view all of the parameters for the template you select. You can then expand individual template sections, or click **Expand All** to view every parameter in every section.
4. For the **Cloud Connector** select the APIC connector you created earlier.
5. From the **Application Type** list, select the base template that contains the parameters that provide the network settings and levels of services that you want to have available in your APIC environment.
6. Expand sections as necessary and then specify parameter values as needed. You can provide default values in that column, and select which parameters the user can revise.

   Tip: *The template options that you can view depend on which option you chose in step 3.*

   Important: *There are two parameters that you must select as Tenant Editable: the parameter that identifies the pool address and the parameter that defines the pool member table. You can specify default values and allow user revision for as many parameters as you want. The names of these two parameters varies from one template to the next.*
7. Click the **Save** button.

You can now use this connector to complete the Cisco APIC integration.

Creating a custom device package

Before you create a device package, you must discover BIG-IP® devices, then create a Cisco APIC connector and an application template.

To enable integration between a APIC and BIG-IQ® Cloud, you must create a device package that Cisco can import. A *device package* is a resource that the Cisco architecture parses and uses to identify the network resources needed to suit your integration requirements.

1. In the BIG-IQ Cloud system, in the Connectors panel, hover over the name of the connector you created previously, click the gear icon (), and then select **Properties**.
   The screen displays properties for that connector.
2. Under APIC Device Package, click the **F5DevicePackage.zip** link.
   The zip file will be copied to your Downloads folder.
3. Click the **Save** button.

About configuring the Cisco APIC for BIG-IQ integration

After you finish configuring BIG-IQ® Cloud for integration, there are some tasks to perform in the Cisco APIC environment to complete the integration. You install the device package, create a device cluster, and then create a service graph.

A *device cluster* is a logical representation of one or more concrete devices acting as a single device. *Concrete devices* are physical (or virtual) BIG-IP® devices added to the device cluster. For more information, refer to the Cisco APIC documentation.

Installing the F5 BIG-IP device package on Cisco APIC

Before you install the F5® BIG-IP® device package on your Cisco APIC, you must have fully set up and configured your Cisco APIC environment.

Install the BIG-IP device package after you have downloaded the device package but before you create device clusters.

Note: *The steps and illustrations in this task make reference to the Cisco APIC version 1.1. Controls of the version 1.2 user interface are likely to differ slightly.*

---

1. Log into Cisco APIC as an administrator.
2. On the menu bar, click **L4-L7 SERVICES**, and then click **PACKAGES**.
3. In the right pane, click **Import a Device Package**.

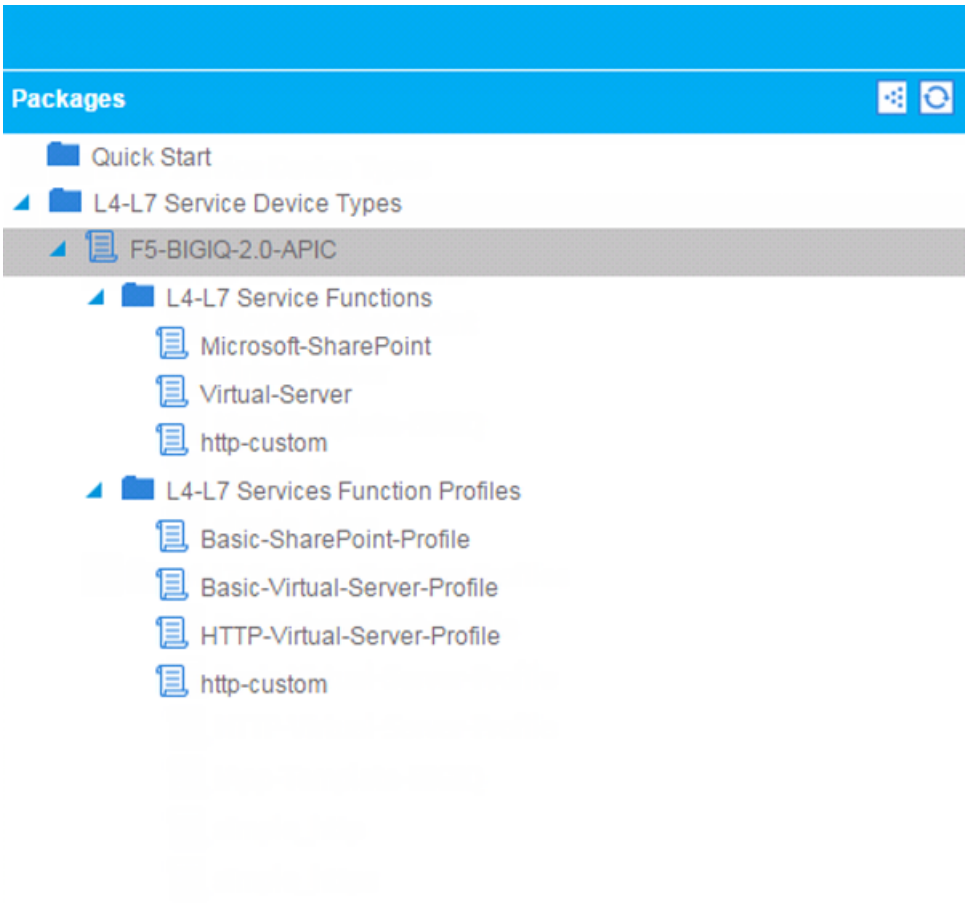

Figure 3: Importing the Device Package

4. Click **BROWSE**, and then navigate to the location where you downloaded and saved the device package.
5. Click **SUBMIT** to start the installation process.
6. Once the installation is complete, verify the device package is accepted by APIC.
   a) In the left pane, click **L4-L7 Service Device Types** to open the folder.
   b) Click the device service package that you want, such as **F5-BIGIQ-2.0**, to expand the F5 BIG-IQ device package for Cisco APIC.
   c) Click **L4-L7 Service Functions**.

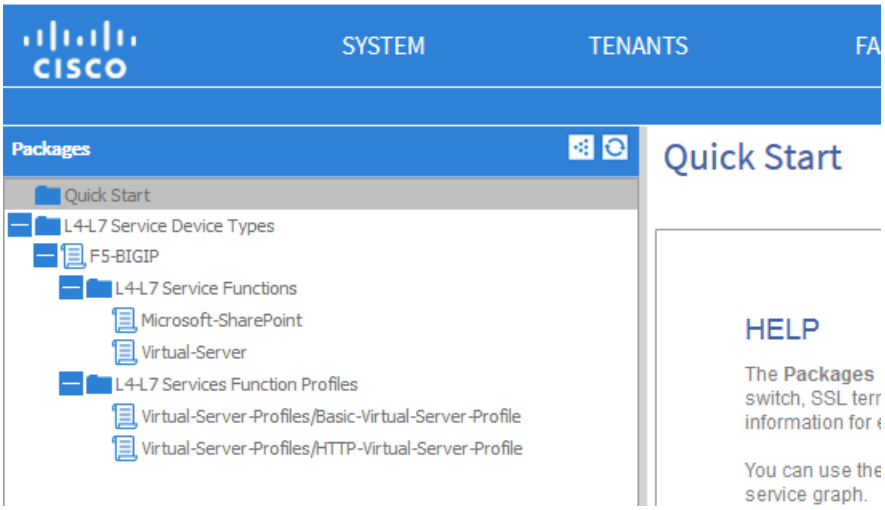

Figure 4: Verifying successful installation of the package

Once the F5 BIG-IQ device package is successfully installed, you are ready to use Cisco APIC to deploy the services supported by the custom iApp templates you created previously. Each template you created is represented by a unique service package listed under **L4-L7 Service Types** > **L4-L7 Services Function Profiles**.

After you install the device package, you must fully configure your base Cisco APIC network settings. Consult your Cisco documentation for details. At a minimum you must:

- Confirm that you have specified the tenants for whom you plan to make services available. If you have not, then create and configure those tenants.
- Create and configure the end point groups and bridge domains that your tenants require.
- Create the Physical Domain with associated VLAN and VXLANs name space.

About Chassis Manager and Device Manager

For Cisco APIC version 1.2 users, you can use Device Manager and Chassis Manager to extend the function of the Cisco APIC user interface to provide support for BIG-IQ® high availability and vCMP®.

If you are going to enable Device Manager and Chassis Manager, you must do so before you create the device cluster.

Enabling the Device Manager

You need to know the name of the APIC connector so that you can correctly form the content of the XML file used as part of this task.

The Device Manager makes it possible for you to specify the parameters needed to support BIG-IQ® HA. When you enable Device Manager on a Cisco APIC Version 1.2, additional controls are added to the device cluster user interface so you can add the necessary configuration details.

1. Use a text editor to create an XML file named `CreateMDevMgr.xml`.
   Use the following for the file content, replacing <*APIC-Connector*> with the name of the APIC connector you created on the BIG-IQ system.

```
<polUni>
  <infraInfra>
    <vnsMDevMgr vendor="F5" model="BIGIQ" version="2.0-<APIC-Connector>">
```

```
      <vnsRsMDevMgrToMDev tDn="uni/infra/mDev-F5-BIGIQ-2.0-<APIC-Connector>" />
    </vnsMChassis>
  </infraInfra>
</polUni>
```

2. Submit a REST POST containing your login credentials to the APIC API.
   The API response contains an authentication cookie.
3. Submit a REST POST to the Cisco APIC API, including the authentication cookie in your HTTP header and the content of `CreateMDevMgr.xml` in the payload.
   Form your post as shown in the following example, replacing *<apic-ip>* with the IP address of the Cisco APIC. `POST https://<apic-ip>/api/node/mo/.xml`

The Cisco APIC processes the POST and enables the Device Manager.

Enabling the Chassis Manager

You need to know the name of the APIC connector so that you can correctly form the content of the XML file used as part of this task.

The Chassis Manager makes it possible for you to specify the parameters needed to support vCMP® guests on BIG-IQ® Cloud. When you enable Chassis Manager on a Cisco APIC Version 1.2, additional controls are added to the device cluster user interface so you can add the necessary configuration details for the vCMP devices.

1. Use a text editor to create an XML file named `CreateMChassis.xml`.
   Use the following for the file content, replacing *<APIC-connector>* with the name of the APIC connector you created on the BIG-IQ.

```
<polUni>
  <infraInfra>
    <vnsMChassis vendor="F5" model="BIGIQ" version="2.0-<APIC-Connector>">
      <vnsRsMChassisToMDev tDn="uni/infra/mDev-F5-BIGIQ-2.0-<APIC-Connector>" />
    </vnsMChassis>
  </infraInfra>
</polUni>
```

2. Submit a REST POST containing your login credentials to the APIC API.
   The API response contains an authentication cookie.
3. Submit a REST POST to the Cisco APIC API, including the authentication cookie in your HTTP header and the content of `CreateMChassis.xml` in the payload
   Form your post as shown in the following example, replacing *<apic-ip>* with the IP address of the Cisco APIC. `POST https://<apic-ip>/api/node/mo/.xml`

The Cisco APIC processes the POST and enables the Chassis Manager.

Creating a device cluster for BIG-IP devices

As part of the BIG-IQ® Cloud and Cisco APIC integration, you need to create an L4-L7 device cluster. Creating the cluster using the F5 Device Package tells APIC a number of things about the F5 devices:

- Their network topology
- Access credentials
- IP addresses
- Configuration details

Additionally, when you create the device cluster, you specify all of the configuration details that Cisco APIC needs for the cluster.

1. In the Cisco APIC user interface create an L4-L7 device cluster.

   For details on the correct settings to specify when you create the cluster, refer to *Device cluster creation guidelines*.

   Important: *BIG-IQ Cloud, version 1.0 supports Cisco APIC version 1.1 and 1.2. Because the user interface for these versions vary significantly, and version 1.2 is still in flux at the time of this release, refer to the Cisco APIC user documentation for details on creating the L4-L7 device cluster.*

2. When the parameters for the new device cluster are correctly specified, click **SUBMIT** to start the device cluster creation.

Cisco APIC processes the information you provided and creates the device cluster. After a pause, the **Device State** displays `Init`, and then eventually changes to `Stable`.

Note: *Do not be alarmed if this process takes some time. It can take several minutes to complete.*

Device cluster creation guidelines

When you create the APIC device cluster, there are a number of parameter settings to specify. The following table serves as a guide for specifying the correct settings for a BIG-IQ® Cloud integration.

Parameter	Factors to consider when specifying
Tenant	Choose the tenant for whom you want to create the device cluster. • If the BIG-IP® devices are to be shared between tenants, choose the pre-configured management tenant. • If the BIG-IP devices are to be used by a single tenant, choose that tenant.
L4-L7 device	Specify the F5 BIG-IQ® device package that you imported.
Model	Select the model that best describes the BIG-IP device that will service your applications. The model you choose also controls which interfaces you can select. • Select **BIG-IP GENERIC** if you are connecting to a physical BIG-IP device. • Select **BIG-IP VE-GENERIC** if you are connecting to a BIG-IP Virtual Edition (VE) that is part of the APIC fabric. • Select **Unknown (Manual)** if the interfaces you need do not show up.
Mode	Select **single node** if you have a single BIG-IP device in the cluster, or HA Cluster if you have two BIG-IP devices in a cluster.
Physical Domain	Select the physical domain you created previously.
APIC to Device Management Connectivity	Select **Out of Band**.
Credentials	Specify a BIG-IQ user with administrative privileges. ***Important:*** *For APIC version 1.1 users, the user name and password must be the same for both the BIG-IP Cloud and the BIG-IQ devices you intend to add to the device cluster instance.*
Device	Specify the management IP address for the BIG-IP device.

Parameter	Factors to consider when specifying
Cluster	Select **https** for the management port. Identify each of the physical interfaces that connect to the ACI fabric. ***Important:*** *BIG-IQ Cloud, version 1.0, supports Cisco APIC version 1.1 and 1.2.* For Cisco APIC version 1.1 users: • If the F5 devices are either physical BIG-IP devices or BIG-IP Virtual Edition (as opposed to vCMP® guests), you can use BIG-IQ Cloud version 1.0 with one BIG-IQ device, but there is no support for BIG-IQ HA. • If the F5 devices are vCMP guests, there is no support for using BIG-IQ Cloud, version 1.0. • If the F5 devices are vCMP guests, you must use the same credentials for both the vCMP guests and the vCMP host. For Cisco APIC Version 1.2 users, you can use Device Manager and Chassis Manager to extend the function of the Cisco APIC user interface to provide support for BIG-IQ HA and vCMP. • Use the Device Manager to extend the Cisco APIC user interface so that you can specify multiple BIG-IQ Clouds and use different credentials for the BIG-IQ and BIG-IP devices. Refer to *Enabling the device manager* for details. • If you specify multiple BIG-IQ hosts, they must be in the same BIG-IQ HA cluster so that if one is down, the device package can contact one of the other hosts in the cluster. • Use the Chassis Manager to extend the Cisco APIC user interface so that you can specify unique credentials for the vCMP host and guest. Refer to *Enabling the chassis manager* for details.

Device Configuration	For each parameter you want to specify for the device, double-click the parameter and specify the value. The device package configures the BIG-IP Cloud appropriately.
	• Use the device host configuration to set common parameters such as the host name, NTP server, and DNS server.
	• In most cases you will not need to specify the `DeviceInterface` or `DeviceRoute` parameters: these values are provided as part of the service graph.
	• The `HighAvailability` parameters are required when you have a device cluster with two BIG-IP devices.
	• For APIC version 1.1 users, if the BIG-IP devices are vCMP guests:
	  • vCMP® configuration is a required parameter.
	  • The vCMP host must use the same IP address as the cluster host.
	  • The vCMP guests must reside on the same vCMP host.
	• For APIC version 1.2 users, vCMP parameters are specified using the Chassis Manager.

Viewing the device cluster you created

You might want to view the device cluster to confirm that you successfully created it before you export it to the tenant.

1. On the menu bar, click **TENANTS**, and then click the tenant for whom the device cluster was created.
2. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.
3. Click **Device Clusters**.

You should be able to view the device cluster you created.

Exporting the device cluster to a tenant

An APIC administrator can choose which tenant(s) are permitted to use the device clusters created in APIC. Use the following steps to export a device cluster to a tenant.

1. On the menu bar, click **TENANTS**.
2. From the sub-menu, click the tenant where the device cluster was created. In our example, we created the device cluster in the management tenant, so click **mgmt**.
3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.
4. Click **L4-L7 Devices**.
5. From the **ACTIONS** list, select **Export Device Cluster**.
6. From the **Device Cluster** list, select the device cluster you want to export.
7. From the **Tenant** list, select the tenant to which you want to export the device cluster.
8. In the **Description** field, you can optionally type a description.
9. Click **SUBMIT**.

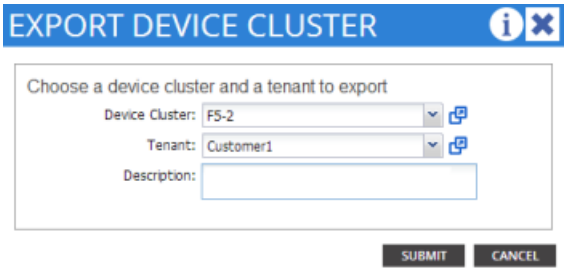

Figure 5: Exporting the device cluster

You should be able to view the device cluster you exported.

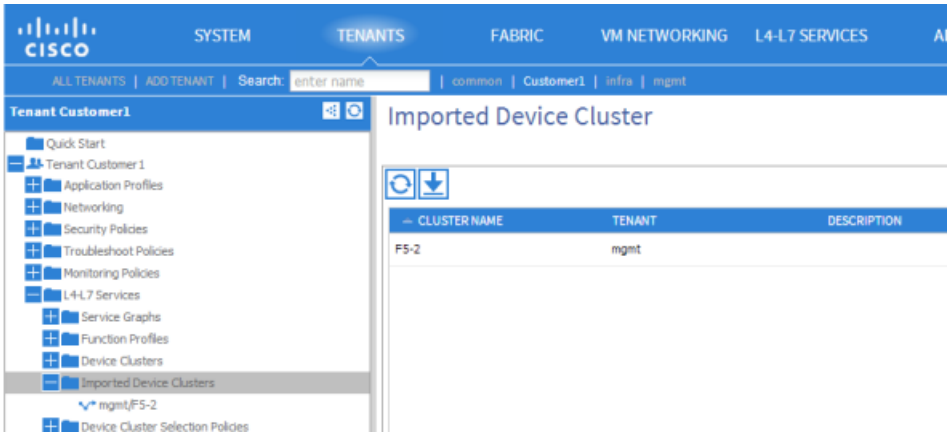

Figure 6: Viewing the device cluster

You can repeat these steps if you want to export the same device cluster to multiple tenants. This functionality is useful for assigning BIG-IQ® resources in your network to meet your end-user's requirements.

About service graphs

A *service graph* is a single listener (virtual server) with its associated configuration objects that are required to allow traffic to go through the BIG-IP® system to a destination pool and the nodes in that pool.

The virtual server itself is unique, so each service graph is one virtual server. You can associate configuration objects and you can share some of those objects between the service graphs (virtual servers). The virtual server port, protocol, and IP address are all unique.

A *multigraph* means that a BIG-IQ system has multiple service graphs that are associated with a single tenant on the BIG-IQ device.

Creating a service graph

Creating a service graph provides you with the controls for specifying the parameters defined by the iApp template you created for this integration.

1. On the menu bar, click **TENANTS**.
2. From the sub-menu, select the tenant in which you want to create the service graph, for example, **Customer1**.
3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.
4. Right-click **L4-L7 Service Graph Templates**, and then click **Create a L4-L7 Service Graph Template**.
5. In the **Name** field, type a name for the service.
6. From the **Type** list, select an appropriate type.

   This setting determines the node configuration. Select either **Single Node - ADC in One-Arm Mode** or **Single Node - ADC in Two-Arm Mode**, depending on your requirements.
7. For the **Device Function**, select the entry with the name that matches the catalog template you created on the BIG-IQ® device.
8. For the **Profile**, select the entry with the name that matches the catalog template you created on the BIG-IQ device.
9. Click **SUBMIT**.
   The system creates the service graph template as you specified it, and displays a model of it on screen.

At this point, the configuration has not yet been pushed to the BIG-IP® system(s); this occurs once you deploy the service graph.

Selecting your service graph for deployment

Deploying the service graph applies the parameter values to the BIG-IP® devices that are part of this integration.

1. On the menu bar, click **TENANTS**.
2. From the sub-menu, select the tenant that contains the service graph.
3. In the left pane, expand the **Tenant** folder and then the **L4-L7 Services** folder.
4. Expand the **L4-L7 Service Graph Templates** folder.
5. Right-click the service graph you created, and then select **Apply L4-L7 Service Graph Template**.

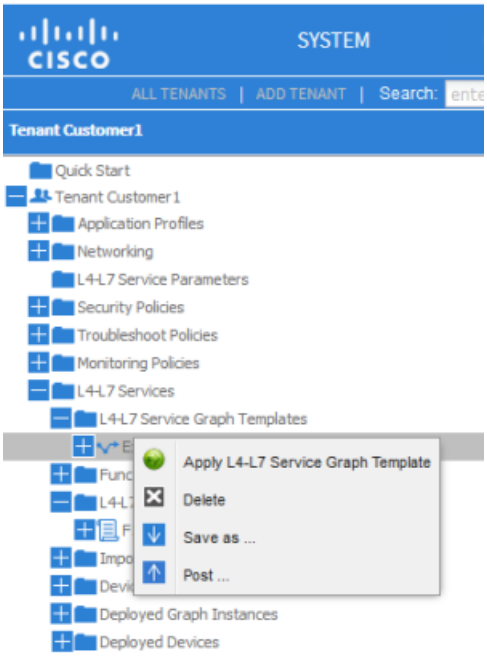

Figure 7: Applying the service graph template

Applying the L4-L7 service graph template

After selecting the service graph for deployment, you edit the service graph, EPGs, and contracts.

Note: *The following figure depicts the APIC version 1.1 user interface. The interface for version 1.2 will likely be slightly different.*

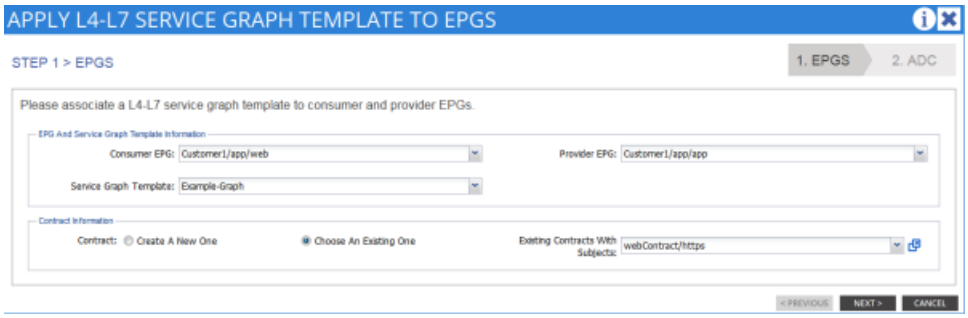

Figure 8: Applying the service graph template to EPGs

1. From the **Consumer EPG** list, select the appropriate EPG.
2. From the **Provider EPG** list, select the appropriate EPG.
3. In the Contract Information area, either select the appropriate existing contract, or create a new one.
4. Click **NEXT**.
   The L4-L7 SERVICE GRAPH TEMPLATE TO EPGS screen displays so that you can configure the graph parameters. The parameters and default values that display are the ones you configured on the BIG-IQ device. You can revise the parameters that you marked as tenant editable.
5. Under Device Config on the ALL PARAMETERS tab, configure the self IP addresses and floating IP addresses needed for each BIG-IP device in the cluster.

- If the BIG-IP devices are in an HA pair, configure internal and external self IP addresses for each BIG-IP device. Also; configure internal and external floating IP addresses for each HA pair.
- If the BIG-IP devices are standalone, only the internal and external self IP addresses for each BIG-IP device are needed.

6. Under Function Config on the ALL PARAMETERS tab, configure (at least) the required parameters for the iApp template you used to create the device package.

   At a minimum, you must specify the parameter that identifies the pool address and the parameter that defines the table of pool members.

7. Click **FINISH** to complete the process.
   The APIC deploys the iApp using the BIG-IQ device that you specified to the BIG-IP device(s) you specified.

If you log in to the BIG-IQ® device and look at the Applications tab, you can confirm that the application deployed successfully.

If you log in to one of the BIG-IP® devices and look at the **iApps** > **Application Services** screen, you can confirm that the iApp deployed successfully.

Note: *The iApps® are not placed in the* `Common` *partition. Instead, the Cisco APIC integration places the iApp in a new partition. Navigate to the new partition before you look to confirm deployment.*

Cloud Tenant Management

About creating cloud tenants

As a cloud administrator, you create tenants and allocate resources to them in the form of iApps® application templates. Tenants can then self-deploy the customized application templates to easily define network and application services for several devices, without requiring them to perform complicated networking procedures.

The process of providing resources for a tenant includes these tasks:

- Create a tenant - When you create a tenant, BIG-IQ® Cloud creates a unique role for the tenant and populates it in the Role panel.
- Create a user - When you create a user account, you assign a user name and a password.
- Associate a user with a tenant's role - You associate a user with a tenant to provide that user access to pre-defined cloud resources in the form of self-service customized applications. You can associate multiple users with a single tenant for access to specific resources.

Creating a tenant

You create a tenant to provide access to customized cloud resources and applications.

1. Hover over the Tenants header, and click the + icon when it appears.
   The panel expands to display property fields for the new tenant.
2. In the **Name** and **Description** fields, type a name and an optional description for this tenant.
   The name can consist of a combination of numbers and symbols, but cannot contain any spaces.
3. From the **Available Connectors** list, select the connector associated with the resources that you are going to provide to this tenant.
   To add another connector, click the plus (+) sign and select a connector from the additional **Available Connectors** list.
4. In the **Address**, **Phone**, and **Email** fields, type optional contact information for this tenant.
5. Click the **Save** button.

You can now associate a user with this tenant to provide access to applications and services.

Creating a cloud user

When you create a cloud user you provide that individual with access to specific resources.

1. Hover over the User header, and click the + icon when it appears.
   The panel expands to display property fields for the new user.

2. 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.
3. In the **Password** and **Confirm Password** fields, type the password for the new user.
4. Click the **Add** button.

You can now associate this user with an existing tenant to provide access to pre-defined cloud resources.

Associating a user with a tenant's role

Before you associate a user with a tenant's role, you must first create the tenant. You can associate multiple users with a tenant's role.

Attention: *The BIG-IQ system administrator creates roles from the* ***BIG-IQ System*** *>* ***Access Control*** *menu. For more information, refer to the BIG-IQ® System: Licensing and Initial Configuration guide.*

You associate user with a tenant's role to provide that user specific access to cloud resources in the form of self-service applications.

In the Users panel, click the user name that you want to associate with a role and drag and drop it onto that role, in the Roles panel.
This user now has access to all of the resources defined for the associated role.

BIG-IQ High Availability

About setting up a high availability cluster

You can ensure that the traffic management function is always available by configuring two or more BIG-IP® systems in a high availability (HA) configuration. Any configuration change that occurs on one BIG-IP system is immediately synchronized with its peer devices. If one BIG-IP® system in an HA configuration fails, a peer BIG-IP system takes over the traffic management.

The BIG-IP HA cluster that you create with this process is a single failover group that uses the default traffic group and automatic sync. For a complete discussion of the significance of these details, refer to the *BIG-IP® Device Service Clustering: Administration* guide, which is available on `http://support.f5.com/kb/en-us.html`.

The BIG-IQ device facilitates the integration between Cisco APIC and the HA cluster. The work flow for configuring this integration takes you back and forth between the two participants in this integration.

Configuring a high availability configuration

You must perform basic system setup and activate a license on two or more BIG-IQ® systems before you can configure a high availability cluster.

Configuring BIG-IQ® Cloud as part of a high availability (HA) cluster ensures that you do not lose management capability of the BIG-IP® devices in your network because one BIG-IQ Cloud system fails.

Important: *Do not confuse the BIG-IQ HA cluster you create in this process with a BIG-IP device cluster. Although the concept is similar, this process creates a cluster of BIG-IQ devices. BIG-IP HA cluster configuration is a separate process.*

Note: *Configuring an HA cluster is an optional task in this process.*

If you have a primary BIG-IQ system (it can either be brand new, or one that you have been using for a while), and you want to add one or more new BIG-IQ Cloud systems as backup, you simply add the new systems to the primary system's `cm-cloud-all-big-iqs` group.

Important: *To synchronize properly, the BIG-IQ systems must be running the same version of software. The exact configuration in terms of hardware is not required; however, the systems should have comparable resources. This is required because, in the event of a fail over, the peer must be able to maintain the process requirements for both systems. This is especially important in terms of disk space and data collection.*

Important: *The device that you add as an HA peer must be in an unconfigured state. That is, you should complete only the basic setup tasks. Specifying configuration details beyond those covered in the licensing and initial configuration process is likely to complicate the synching process.*

---

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. In System, hover over the BIG-IQ Systems header, and click the + icon when it appears.
   The New Device screen opens.

3. In the **IP Address** field, type the BIG-IQ System's self IP address.
4. In the **User name** and **Password** fields, type the administrative user name and password for the system.
5. For the **Group** setting, select **HA Peer Group**.
6. Click the **Add** button to add this device to this high availability cluster.

The system discovers its peer and displays its status.

If discovery of the newly configured BIG-IQ system fails, a **Delete** button displays. Verify the correct self IP address and credentials. Then click the **Delete** button to remove the incorrect information, and re-type the self IP address, user name, and password.

Glossary

BIG-IQ Cloud terminology

Before you manage cloud resources, it is important that you understand some common terms as they are defined within the context of the BIG-IQ® Cloud.

Term	Definition
application templates	An application template is a collection of parameters (in the form of F5 iApps® templates) that a cloud administrator defines to create a customized configuration for tenants. Cloud administrators add the configured application to a catalog from which a tenant can self-deploy it.
BIG-IQ Cloud	The BIG-IQ® Cloud system is a tool that streamlines management and access for tenants to services and applications hosted by local and/or cloud-based servers.
cloud administrator	Cloud administrators create application templates for tenants to centrally manage access to specific web-based applications and resources. Cloud administrators might also be referred to as cloud providers.
cloud bursting	Cloud bursting is a seamless way to manage an anticipated increase in application traffic by directing some traffic to another cloud resource. When demand falls back into normal parameters, traffic can be directed back to the original cloud resource. This elasticity enables efficient management of resources during periods of increased or decreased traffic to applications.
cloud connector	A cloud connector is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.
resources	A resource is any managed object, including devices, web applications, virtual servers, servers, cloud connectors, and so forth.
roles	A role defines specific privileges to which you can associate one or more users. There are two default roles for BIG-IQ Cloud: cloud administrator and cloud tenant.
tenant	A tenant is an entity that can consist of one or more users accessing resources provided by a cloud administrator.

Term	Definition
user	A user is an individual who has been granted access to specific tenant resources.

Index

A

active-active pair
  about configuring for the BIG-IQ system *41*
  configuring for the BIG-IQ system *41*
admin, See administrator
Administrator role
  defined *14*
administrator user
  and default password *13*
  changing password for *11*, *13*
administrator user password
  changing *11*, *13*
APIC
  about *23*
  integration *23*
application catalog *27*
applications
  customizing for tenants *27*
application templates
  about *27*
  creating custom *27*
  defined *43*
  using *27*
authorization checks
  for secure communication *7*

B

base registration key
  about *10*
BIG-IP and Cisco APIC requirements *26*
BIG-IQ Cloud
  about *7*
  defined *43*
BIG-IQ device package for Cisco APIC
  installing on Cisco APIC *29*
BIG-IQ integration
  about configuring Cisco APIC *29*
BIG-IQ system
  about activating *9*
  about licensing *9*

C

catalog
  for applications *27*
catalog entries
  creating for tenants *27*
chassis manager
  enabling *32*
Chassis Manager
  about *31*
Cisco APIC
  about configuring for BIG-IQ integration *29*
  installing BIG-IP device package *29*
Cisco APIC connector
  adding *27*
Cisco APIC requirements *26*
cloud administrator
  defined *43*
cloud bursting
  defined *43*
cloud connector
  defined *43*
cloud connector, local
  associating with a device *27*
cloud resources
  providing for tenants *27*, *39*
cloud tenants
  about creating *39*
  adding *39*
clusters
  for high availability *41*
communication
  between BIG-IQ and managed devices *7*
configuration
  and initial setup *9–10*
connector, local
  associating with a device *27*
custom device package
  creating *28*

D

device clusters
  about *29*
  confirming creation *34*
  creating *32*
  creation guidelines *33*
  exporting to tenant *35*
  parameter settings *33*
  viewing *34*
device discovery
  by scanning network *21*
device inventory
  about *21*
device management
  about *21*
device manager
  enabling *31*
Device Manager
  about *31*
device package
  creating a custom *28*
  installing *29*
devices
  about discovering *21*
  adding *21*
discovery address
  defined *9*
DNS server
  specifying for the BIG-IQ system *11*
documentation, finding *8*
dossier
  providing *9–10*

F

failover *41*

G

glossary *43*
guides, finding *8*

H

high availability
    configuring *41*
high availability configuration
    about *41*
HTTPS port 443
    required for communication *7*

I

iApps
    customizing for tenants *27*
    defined *27*
initial configuration
    for BIG-IQ system *9*
IP addresses
    for managed devices *21*

L

L4-L7 service graph template
    applying *37*
license
    activating automatically *9*
    activating manually *10*
    manually activate a pool license *17*
license activation
    for BIG-IQ system *9–10*
licenses
    about managing for devices *17*
    about pool licenses *17*
    for pools *19*
    revoking for managed device *19*
licensing
    activating pool license automatically *17*
    activating pool license manually *17*
    for managed devices *17*
    for pool license *17*
    for pools for BIG-IP devices *19*
local cloud connector
    associating with a device *27*

M

managed devices
    about discovering *21*
manual activation
    for pool license *17*
manuals, finding *8*
minimum requirements
    for BIG-IP system and Cisco APIC *26*
minimum requirements *(continued)*
    for Cisco APIC *26*

N

network
    incorporating BIG-IQ systems *9*
network configurations
    customizing for tenants *27*
network configurationsiApps
    customizing for tenants *27*
network security
    about *7*
network topology *25*

O

offering licenses
    activating for a license *18*

P

Pacific Standard Time zone
    as default for the BIG-IQ system *11*
password
    changing for administrator user *11*, *13*
pool license
    activating automatically *17*
    activating manually *17*
    revoking for a BIG-IP device *19*
pool licenses
    about *17*
    assigning to a BIG-IP device *19*
port 22
    using *7*
port 443
    required for communication *7*
    using *7*
ports
    required for communication with BIG-IQ *7*
    required open *7*
pre-defined users
    and administrator role *13*
    and root role *13*
PST zone, See Pacific Standard Time zone

R

related documentation *24*
release notes, finding *8*
requirements
    for BIG-IP system *26*
    for BIG-IP system and Cisco APIC *26*
    for Cisco APIC *26*
    for software version *25*
resources
    defined *43*
    providing access for user *40*
roles
    associating with users and user groups *15*
    defined *13*

roles *(continued)*
for users *13–14*
root user
and default password *13*

S

security
for communication *7*
service graph
applying a template *37*
creating *36*
selecting for deployment *36*
service graphs
about *36*
system overview
for BIG-IQ Cloud *7*
system user
adding *14*

T

TCP port 22
using *7*
TCP port 443
using *7*
tenant
adding *39*
Tenant role
defined *14*
tenants
about creating *39*
associating with a user *40*
creating applications for *27*
tenants users
and tenants *39*
and users *39*
terminology *43*
terms
defined *43*
time zone
and default for the BIG-IQ system *11*
changing for the BIG-IQ system *11*
specifying a DNS server for the BIG-IQ system *11*
time zone default
for the BIG-IQ system *11*

U

user groups
defined *13*
user roles
about *14*
associating with users and user groups *15*
users
adding *14*, *39*
associating with a tenant *40*
defined *13*, *39*
removing role from *15*
utility license
activating an offering license for *18*

V

version requirements
version *25*