

F5[®] iWorkflow[™]: Cisco APIC Administration

Version 2.3.0



Table of Contents

F5 iWorkflow Introduction.....	5
About incorporating iWorkflow securely into your network.....	5
Open ports required for device management.....	5
Overview: iWorkflow system.....	5
Additional resources and documentation for iWorkflow systems.....	5
Software Licensing and Initial Configuration.....	7
About software licensing and initial configuration.....	7
Automatic license activation.....	7
Manual license activation.....	7
Confirming the host connectivity options.....	8
Defining DNS and NTP servers for the iWorkflow system.....	9
Changing the default passwords.....	9
Upgrading iWorkflow.....	11
About upgrading iWorkflow.....	11
Upgrading a standalone system.....	11
About upgrading a standalone system.....	11
Upgrading a standalone system.....	11
Upgrading a cluster.....	13
Breaking a cluster.....	13
Upgrading a standalone system.....	13
Recreating a cluster.....	15
Installing a hotfix.....	17
About installing a hotfix.....	17
Breaking a cluster.....	17
Installing a hotfix on a standalone system.....	17
Recreating a cluster.....	19
Backing up and restoring iWorkflow.....	21
About backing up and restoring iWorkflow.....	21
About files names and locations.....	21
Backing up configuration data.....	21
Restoring configuration data.....	22
Users, User Groups, and Roles.....	23
Overview: Users, user groups, and roles.....	23
Changing the default password for the administrator user.....	23
Adding a locally-authenticated iWorkflow user.....	23
About user roles.....	24
Roles definitions.....	24
Associating a user or user group with a role	24
Disassociating a user from a role.....	25
License Management.....	27

Overview: Licensing options.....	27
About pool licenses.....	27
Automatically activating a pool license.....	27
Manually activating a pool license.....	27
Integrating with Cisco APIC.....	29
About F5 and Cisco APIC integration.....	29
APIC-related documentation.....	30
About network topology using the BIG-IP system integrated with Cisco APIC.....	31
Version requirements.....	32
Minimum Cisco APIC requirements.....	32
Minimum F5 BIG-IP requirements.....	32
About configuring the iWorkflow device for a Cisco APIC integration.....	33
Provisioning the vCMP feature.....	33
Create a vCMP connector.....	33
Creating a vCMP guest for Cisco APIC.....	34
Deploying a vCMP guest for Cisco APIC.....	35
Discovering a BIG-IP guest.....	36
Discovering a BIG-IP device in your network by its IP address.....	36
Adding a Cisco APIC connector.....	37
Exporting an iApps template.....	37
Importing an iApps template.....	38
Creating a customized service template.....	39
About configuring the Cisco APIC for iWorkflow integration.....	40
Installing the F5 BIG-IP device package on Cisco APIC.....	40
Creating a new chassis type.....	42
Creating a chassis manager.....	43
Creating a new device manager type.....	43
Creating a new device manager.....	43
Creating a device cluster for BIG-IP devices.....	44
Viewing the device cluster you created.....	46
Exporting the device cluster to a tenant.....	46
About service graphs.....	47
Cloud Tenant Management.....	51
About creating cloud tenants	51
Creating a tenant.....	51
Creating a cloud user.....	51
Associating a user with a tenant's role.....	52
iWorkflow High Availability.....	53
About setting up a high availability cluster	53
Configuring a high availability cluster.....	53
Glossary.....	55
iWorkflow terminology.....	55
Legal Notices.....	57
Legal notices.....	57

F5 iWorkflow Introduction

About incorporating iWorkflow securely into your network

To successfully manage devices in your network, including F5® iWorkflow™ peer systems, the iWorkflow system requires communication over HTTPS port 443. The iWorkflow 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 iWorkflow 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 F5® iWorkflow™ system requires bilateral (outbound and inbound) communication with other iWorkflow devices, and unilateral (outbound only) communication with BIG-IP® 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)	Discover, monitor, and configure managed devices. Replicate and synchronize iWorkflow systems.
TCP 22 (SSH)	Administer iWorkflow, REST API updates on remote systems.

Overview: iWorkflow system

The F5® iWorkflow™ system streamlines deployment of application delivery services policy. 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 AuthZ checks).

iWorkflow enables organizations to accelerate the deployment of applications and services while reducing exposure to operational risk. Available only as a virtual appliance, iWorkflow is a multi-tenant platform for deploying application delivery policies onto BIG-IP devices. Presented using services catalogues, iWorkflow tenants deploy highly-configurable, administrator-defined application services templates. Using these service templates (called F5 iApps®), you avoid operational delay, risk, and complexity while simplifying application delivery management.

When integrated with Cisco APIC, iWorkflow 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.

Additional resources and documentation for iWorkflow systems

You can access all of the following iWorkflow™ system documentation from the AskF5™ Knowledge Base located at <http://support.f5.com/>.

Document	Description
iWorkflow™ Systems Virtual Editions Setup guides	iWorkflow™ 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 iWorkflow 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

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

Important: Before you can perform software licensing and initial configuration tasks, you must set up your virtual environment. Use the appropriate iWorkflow™ Systems Virtual Editions Setup guide to set up your environment before proceeding.

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 iWorkflow system.

Automatic license activation

You must have a base registration key to license the iWorkflow™ system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the iWorkflow™ 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 iWorkflow system uses to communicate with its managed devices.

2. Log in to iWorkflow System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the iWorkflow 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 **Save And Continue** button. The End User Software License Agreement (EULA) displays.
6. To accept, click the **Agree** button. The Host Connectivity Options screen opens.

Continue with the setup process on the Host Connectivity Options screen.

Manual license activation

You must have a base registration key to license the iWorkflow™ system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the iWorkflow™ system is not connected to the public internet, use this procedure to activate its license.

1. Using a browser on which you have configured the management interface, type `https://<Management Interface IP address>/ui/system/setup`, where `<Management Interface IP address>` is the address you specified for device management.
This is the IP address that the iWorkflow system uses to communicate with its managed devices.
2. Log in to iWorkflow with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the iWorkflow 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 iWorkflow 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 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 iWorkflow Device, into the **License Text** field, paste the license key.
12. To save your configuration, click **Save And Continue**.
The Host Connectivity Options screen opens.

Continue with the setup process on the Host Connectivity Options screen.

Confirming the host connectivity options

Before you confirm the host connectivity options, you must have activated the license.

You need to specify the details of how the iWorkflow™ system communicates.

1. In the **Fully Qualified Hostname** 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 Interface IP Address** field, type the management interface IP address. The IP address must be in Classless InterDomain Routing (CIDR) format. For example: `10.10.10.10/24`.
This is the IP address that managed devices use to communicate with the iWorkflow system. This address is also referred to as the *discovery address*.
3. In the **Management Interface Default Route** field, type the default gateway address for the management port.
4. Specify the **High Availability Cluster Peer IP Address** for communication between peer iWorkflow systems in a high availability configuration.
 - To use the management port IP address for HA communication, select **Use Management Address for communicating with HA Cluster peers**.
 - To use a unique self IP address for HA communication:
 1. Clear the **Use Management Address for communicating with HA Cluster peers** check box.
 2. Type the self IP address in the **Self IP Address (Format: Self IP/Mask)** field.

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

Important: You must assign a static IP address that does not change to your iWorkflow virtual machine. DHCP assignment of IP addresses is not supported.

5. To save your configuration, click **Save And Continue**.
The Update Services screen opens.

Continue with the setup process on the Update Services screen.

Defining DNS and NTP servers for the iWorkflow system

After you license the iWorkflow™ system and confirm the host connectivity options, you can specify the DNS and NTP servers.

On the Update Services screen you set your DNS server and domain to allow the iWorkflow system to properly parse IP addresses. Defining the NTP server ensures that the iWorkflow 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 iWorkflow 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. To save your configuration, click **Save And Continue**.
The Update Password screen opens.

Continue with the setup process on the Update Password screen.

Changing the default passwords

After you initially license and configure the iWorkflow system, and define the DNS and NTP servers, 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 your configuration, click **Save And Continue**.
The Summary screen opens.
6. Review the settings listed on the Summary screen and if everything is as expected, click **Save And Continue** to complete the setup process.

Upgrading iWorkflow

About upgrading iWorkflow

You can upgrade an iWorkflow™ system under the following conditions:

- When you are running an iWorkflow standalone instance and you want to upgrade to a newer iWorkflow version.
- When you are running an iWorkflow cluster and you want to upgrade to a newer iWorkflow version.

To upgrade iWorkflow standalone systems and clusters to new versions, make sure that you have:

- Adequate disk space available to complete the installation.
- Administrator rights on the iWorkflow system.
- A recent user configuration set (UCS) backup of the iWorkflow system copied to a remote secure server for storage.
- An iWorkflow release ISO file that is copied to the `/shared/images` directory.
- Managed devices that are healthy.

Additional considerations when upgrading:

- You can expect a service disruption to the management plane.
- You should not expect a disruption to the data plane of the BIG-IP® systems that iWorkflow is managing.

Upgrading a standalone system

About upgrading a standalone system

During the upgrade process, the iWorkflow™ administrative interface is unavailable, but that does not impact the devices managed by iWorkflow. In most cases, after the iWorkflow upgrade is complete, you will need to update the representational state transfer (REST) framework on all managed BIG-IP® devices.

When installing new iWorkflow software images, you must run the software installation from an active boot location, and specify an inactive clean boot location as the target install location. This action is a result of the software installation copying the running configuration and license from the current boot location to the target install location.

It is possible to upgrade iWorkflow without importing the running configuration. For more information, see *K13438: Controlling configuration import when performing software installations (11.x - 12.x)* at support.f5.com.

Upgrading a standalone system

Before you start, make sure that you are running an iWorkflow™ standalone instance.

You upgrade a standalone system when you want to upgrade to a newer iWorkflow version.

Note: During the upgrade process, iWorkflow is not able to make changes, updates, or additions to any of the managed BIG-IP® systems.

1. Log in to the iWorkflow command line.
2. Run the command `tmsh` to access the `tmsh` utility.
3. Run the command `show /sys software` to check the status of the currently installed iWorkflow software.

The output displays something similar to the following example:

```
-----
Sys::Software Status
Volume      Product      Version      Build      Active  Status
-----
HD1.1       iWorkflow    2.0.0        0.0.9631   yes     complete
HD1.2       none        none         none        no      complete
-----
```

Note: If the output displays only one volume, you can create a new volume during the installation process.

4. Run the command `install /sys software image <iworkflow-image.iso> volume <inactive volume>` to install iWorkflow onto an existing inactive volume. `<inactive volume>` is the name of an inactive volume. For example, `install /sys software image iworkflow.iso volume HD1.2`.
5. Optional: Run the command `install /sys software image <iworkflow-image.iso> create-volume volume <new volume> reboot` to automatically reboot after creating a new volume and installing iWorkflow into the new location. `<new volume>` is the name of a new volume. For example, `install sys software image iWorkflow.iso create-volume volume HD1.3 reboot`.
6. Run the command `quit` to exit the `tmsh` utility.

Note: If there is an upgrade failure, reboot to the previously active volume on which the previous iWorkflow version was installed, and if required, restore the backup to get the storage state back.

7. After the installation is complete, if you did not use the `reboot` switch in your `tmsh install` command, you can manually reboot into the new volume by running the command: `tmsh reboot volume <new iWorkflow volume>`. `<new workflow volume>` is the name of the new volume. For example, `tmsh reboot volume HD1.2`.
8. Once the system completes the installation and reboots into the new active volume, log in to the iWorkflow command line to review the status. Review the managed BIG-IP devices and confirm that the representational state transfer (REST) framework versions are current. Rediscover any BIG-IP devices that are unhealthy to force the REST framework update.

Note: You can monitor the installation process by running the command: `watch tmsh show /sys software`. By default, the `watch` command automatically refreshes every two seconds.

The output displays something similar to the following example:

```
Every 2.0s: tmsh show /sys software                               Fri Sep 13 11:14:08
2016
-----
Sys::Software Status
-----
```

Volume	Product	Version	Build	Active	Status
HD1.1	iWorkflow	2.0.0	0.0.9631	yes	complete
HD1.2	iWorkflow	2.0.1	0.0.9855	no	installing 10.000 pct

In most cases, after the iWorkflow upgrade is complete, you will need to update the REST framework on all managed BIG-IP devices by rediscovering the BIG-IP system. You can do this using the **Discover Device** button. For more information, see the *Add a device* section of the *iWorkflow Ops guide* at devcentral.f5.com.

Upgrading a cluster

Breaking a cluster

Before you start, make sure that you are running an iWorkflow™ cluster.

You break a cluster by using a lead peer to evict the two sibling peers.

Note: During the upgrade process, iWorkflow is not able to make changes, updates, or additions to any of the managed BIG-IP® systems.

1. Log in to the iWorkflow administrative user interface with your administrator user name and password. For example: `https://10.10.99.5/ui/login`.
2. At the top of the screen, click **System settings**.
3. From the iWorkflow Cluster panel, select an iWorkflow server.
4. Click **Remove** to break the iWorkflow cluster.

Note: When you remove an iWorkflow cluster member from the cluster, iWorkflow removes all cluster state details from that device and resets it to the default state. The management IP and license details are not impacted by an update.

Note: If you want to perform this procedure using a REST call from the command line, see *K49398482: Managing F5 iWorkflow clusters at support.f5.com*.

Upgrading a standalone system

Before you start, make sure you have broken the iWorkflow™ cluster, and that there is only a single standalone iWorkflow instance running and managing the BIG-IP® system.

You upgrade a standalone system when you want to upgrade to a newer iWorkflow version.

1. Log in to the iWorkflow command line.
2. Run the command `tmsh` to access the `tmsh` utility.
3. Run the command `show /sys software` to check the status of the currently installed iWorkflow software.

The output displays something similar to the following example:

```

Sys::Software Status
Volume      Product          Version    Build      Active    Status
-----
HD1.1       iWorkflow        2.0.0     0.0.9631  yes      complete
HD1.2       none             none      none      no       complete

```

Note: If the output displays only one volume, you can create a new volume during the installation process.

4. Run the command `install /sys software image <iworkflow-image.iso> volume <inactive volume>` to install iWorkflow onto an existing inactive volume. `<inactive volume>` is the name of an inactive volume. For example, `install /sys software image iworkflow.iso volume HD1.2`.
5. Optional: Run the command `install /sys software hotfix <iworkflow-image.iso> create-volume volume <new volume> reboot` to automatically reboot after creating a new volume and installing iWorkflow into the new location. `<new volume>` is the name of a new volume. For example, `install sys software image iWorkflow.iso create-volume volume HD1.3 reboot`.
6. Run the command `quit` to exit the tmsh utility.

Note: If there is an upgrade failure, reboot to the previously active volume on which the previous iWorkflow version was installed, and if required, restore the backup to get the storage state back.

7. After the installation is complete, if you did not use the reboot switch in your tmsh `install` command, you can manually reboot into the new volume by running the command: `tmsh reboot volume <new iWorkflow volume>`. `<new workflow volume>` is the name of the new volume. For example, `tmsh reboot volume HD1.2`.
8. Once the system completes the installation and reboots into the new active volume, log in to the iWorkflow command line to review the status. Review the managed BIG-IP devices and confirm that the REST framework versions are current. Rediscover any BIG-IP devices that are unhealthy to force the REST framework update.

Note: You can monitor the installation process by running the command: `watch tmsh show /sys software`. By default, the watch command automatically refreshes every two seconds.

The output displays something similar to the following example:

```

Every 2.0s: tmsh show /sys software                               Fri Sep 13 11:14:08
2016
-----
Sys::Software Status
Volume      Product          Version    Build      Active    Status
-----
HD1.1       iWorkflow        2.0.0     0.0.9631  yes      complete
HD1.2       iWorkflow        2.0.1     0.0.9855  no       installing 10.000 pct

```

In most cases, after the iWorkflow upgrade is complete, you will need to update the REST framework on all managed BIG-IP devices by rediscovering the BIG-IP system. You can do this using the **Discover Device** button. For more information, see the *Add a device* section of the *iWorkflow Ops guide* at devcentral.f5.com.

Recreating a cluster

Before you start, make sure you have upgraded all three F5® iWorkflow™ nodes.

You recreate the cluster by using the lead peer to add the sibling peers to the cluster.

***Note:** The iWorkflow peer leader is the preferred cluster member for managing the iWorkflow cluster and BIG-IP® systems. You can use any of the cluster members for this purpose, but F5 recommends that once you have a cluster running you select one member of the cluster for administration and maintain that host until it is no longer preferred.*

1. Log in to the iWorkflow administrative user interface with your administrator user name and password. For example: `https://10.10.99.5/ui/login`.

***Note:** This is the only iWorkflow instance with knowledge of a BIG-IP system.*

2. At the top of the screen, click **System settings**.
3. From the iWorkflow Cluster panel, in the iWorkflow Cluster header, click the plus (+) icon.
4. In the New iWorkflow Cluster Member panel, type the **IP address**, **Admin Username**, and **Password**.
5. Click **Add**.
6. Click **OK**.
7. Repeat this procedure until all three iWorkflow cluster members are returned to the cluster.

***Note:** If you want to perform this procedure using a REST call from the command line, see K49398482: Managing F5 iWorkflow clusters at support.f5.com.*

Installing a hotfix

About installing a hotfix

We provide an F5® iWorkflow™ hotfix to meet a need or resolve an issue unique to your environment. F5 recommends that you run iWorkflow in a cluster. When applying a hotfix to an iWorkflow cluster, you must first evict the peers from the cluster (*breaking the cluster*) and then apply the hotfix to each instance before recreating the cluster.

To install a hotfix, make sure that you have:

- Adequate disk space available to complete the installation.
- Administrator rights on the iWorkflow system.
- A recent user configuration set (UCS) backup of the iWorkflow system copied to a remote secure server for storage.
- An iWorkflow release ISO file copied to the `/shared/images` directory.
- A target iWorkflow base ISO available under the `/shared/images` directory.

Breaking a cluster

Before you start, make sure that you are running an iWorkflow™ cluster.

You break the cluster in order for removed peers to return to a default state.

Important: *If you are running a standalone system (your environment contains a single iWorkflow server), skip all the steps for Breaking a cluster. Proceed to Installing a hotfix on a standalone system.*

Note: *When you break a cluster, the data stored on the peer that is evicted from the cluster will be lost.*

1. Log in to the iWorkflow administrative user interface with your administrator user name and password.
 2. At the top of the screen, click **System settings**.
 3. From the iWorkflow Cluster panel, double-click the peer you want to remove.
 4. In the Properties panel, click **Remove** to remove the peer you want to evict from the cluster ("break" the cluster).
 5. Repeat this task for each peer you want to evict from (break) the cluster.
-

Note: *From the time you remove the first peer, until the leader is a standalone instance, iWorkflow will report the cluster size as unsupported.*

Installing a hotfix on a standalone system

Before you start, make sure you are running a standalone system. That is, your environment is running a single iWorkflow™ server.

Important: If you are installing a hotfix on an iWorkflow cluster, you must first break the cluster before installing the hotfix on each iWorkflow instance. If you have an iWorkflow cluster, first perform the *Breaking the a cluster procedure* before you start this procedure.

You can install a hotfix to meet a need or resolve an issue unique to your environment.

Note: While you are updating the iWorkflow server, it is not available for administrative access. You cannot make changes, updates, or additions to any of the managed BIG-IP® systems. However, traffic on BIG-IP systems is not impacted.

1. Run the command `tmsh` to access the `tmsh` utility.
2. Run the command `show /sys software` to check the status of the currently installed iWorkflow software.

The output displays something similar to this example.

```
-----
Sys::Software Status
Volume      Product          Version    Build      Active    Status
-----
HD1.1       iWorkflow        2.0.0     0.0.9631   yes      complete
HD1.2       none             none      none       no       complete
-----
```

3. Run the command `install /sys software hotfix <iworkflow-hotfix.iso> volume <inactive volume>` to install an iWorkflow hotfix onto an existing inactive volume.

<iworkflow-hotfix.iso> is the name of the hotfix file.

<inactive volume> is the name of the inactive volume.

Example: `install /sys software hotfix Hotfix-iWorkflow-bigiq-mgmt-2.0.0.9999.9999-ENG.iso volume HD1.2.`

4. Optional: Run the command `install /sys software image <iworkflow-hotfix.iso> create-volume volume <new volume> reboot` to automatically reboot after creating a new volume and installing iWorkflow into a new location.
- <iworkflow-hotfix.iso> is the name of the hotfix file. For example, `install sys software hotfix Hotfix-iWorkflow-bigiq-mgmt-2.0.0.9999.9999-ENG.iso create-volume volume HD1.3.`

5. Run the command `quit` to exit the `tmsh` utility.

Note: You can monitor the installation process by running the command: `watch tmsh show /sys software`. By default, the `watch` command automatically refreshes every two seconds. If `tmsh` appears to stall and a `waiting for product image message` displays, confirm that you have the base ISO image available in the `/shared/images` directory.

The command output displays something similar to this example.

```
-----
Sys::Software Status
Volume      Product          Version    Build      Active    Status
-----
HD1.1       iWorkflow        2.0.0     0.0.9631   yes      complete
-----
```

```
HD1.2      iWorkflow      2.0.1      0.0.9631  no      installing  0.000 pct
```

Recreating a cluster

Before you start, make sure that the peers joining the cluster are clean builds.

You can recreate a cluster from any iWorkflow™ instance.

Important: *The cluster creation process does not support importing existing configurations from an existing iWorkflow system.*

1. Log in to the iWorkflow administrative user interface with your administrator user name and password.
2. At the top of the screen, click **System settings**.
3. From the iWorkflow Cluster panel, in the iWorkflow Cluster header, click the plus (+) icon.
4. In the New iWorkflow Cluster Member panel, type the **IP address**, **Admin Username**, and **Password**.
5. Click **OK** to acknowledge the data on the peer will be overwritten warning.
6. Repeat this procedure for the third iWorkflow member in the cluster.

Backing up and restoring iWorkflow

About backing up and restoring iWorkflow

You can back up or restore iWorkflow™ configuration data by using a user configuration set (UCS) archive. The UCS archive, by default, contains all of the files that the system requires to restore your current configuration to a new system, including configuration files, the product license, local user accounts, and Secure Socket Layer (SSL) certificate/key pairs.

To back up and/or restore a UCS file, make sure that you have:

- iWorkflow version 2.0.x or later installed.
- Root access to the iWorkflow instance.

Additional considerations:

- F5 recommends restoring the UCS archive to a system running the same version of iWorkflow as the source used to create the UCS archive.
- If you restore a UCS file from one system to a different system, you will have to re-license the iWorkflow instance. Alternatively, you may be able to replace the license file with the original license file from the destination device.
- If you restore the UCS file to another system, the destination server will acquire the source network settings.

About files names and locations

Unless you include the extension in a file name, by default the iWorkflow™ system saves the user configuration set (UCS) archive file with a `.ucs` extension. You can also specify a full path to the archive file, and the system saves the archive file to that specified location. If you do not include a path, the system saves the file to the default archive directory, `/var/local/ucs`.

Archives located in a directory other than the default do not appear when you use the traffic management shell (`tmsh`) list function for UCS archives. So that you can easily identify the file, F5 recommends that you include the iWorkflow host name and current time stamp as part of the file name.

Backing up configuration data

Before you start, make sure that there is adequate local storage available to create the user configuration set (UCS) file, and that iWorkflow™ version 2.0.x or later is installed.

As an iWorkflow administrator, you should back up the configuration data to ensure eases of recovery for your system.

1. Log in to the iWorkflow command line.
2. Run the command `tmsh` to access the `tmsh` utility.
3. Run the command `save /sys ucs {new-ucs-file}` to create the UCS archive.

For example: `save /sys ucs iwf-1-09092016`.

Note: Run the command `list /sys ucs` to list all of the UCS archive files on the system. If you use the configuration utility to create UCS files, when you use this command, the system will not display the files. By default, the system saves files in the `/shared/ucs_backups` directory.

By default, this creates a new UCS file in the `/var/local/ucs` directory.

- Optional: Run the command `save /sys ucs /path/to/{new-ucs-file}` to save the UCS file to another location.
For example: `save /sys ucs /var/run/iwf-2-09092016`.
- Optional: Run the command `save /sys ucs /path/to/{new-ucs-file} passphrase <password>` to encrypt the UCS archive with a passphrase.
`/path/to/<{new-ucs-file}>` is the full path to the UCS archive file.
`<password>` is the passphrase you want to use to encrypt the UCS archive.
For example: `save /sys ucs /var/local/ucs/iwf-2-09092016 passphrase password`.
- Optional: Run the command `save /sys ucs /path/to/{new-ucs-file} no-private-key` to exclude the SSL private keys from the UCS archive.
For example: `save /sys ucs /var/local/ucs/iwf-2-09092016 no-private-key`.
- Copy the UCS file to a remote, secure system and storage location.

Restoring configuration data

Before restoring a backup to an iWorkflow™ cluster, make sure that you have:

- Copied the remote archive files back to the destination iWorkflow.
- Evicted all peers from the cluster, leaving a standalone instance.
- A backup of the destination system.

Important: The local system partition is active during the restore process, and the system will entirely replace the partition with the data stored in the archive file. During the restore process, the iWorkflow system is not available for remote users or standard iWorkflow functions.

You restore a backup to an iWorkflow cluster when something goes wrong or when you need to get back to how things were when you made the backup.

- Log in to the iWorkflow command line.
- Run the command `tmsh` to access the `tmsh` utility.
- Run the command `load /sys ucs /path/to/{ucs-archive-file}` to restore the user configuration set (UCS) archive file.

`/path/to/{ucs-archive-file}` is the full path to the UCS archive file to restore.

For example: `load /sys ucs /var/local/ucs/iwf-2-09092016.ucs`.

Note: If the UCS archive was encrypted with a passphrase during backup, at the prompt, type the passphrase.

- Optional: Run the command `load /sys ucs /path/to/{ucs-archive-file} -no-license` to restore the backup without the license. This is when you are restoring to a host other than the UCS source.
For example: `load /sys ucs /var/local/ucs/iwf-2-09092016.ucs -no-license`.
- Run the command `reboot` to restart the system.

After completing the restore, recreate the cluster using the previously removed peers. The backed up iWorkflow version will then replicate to the other peers in the cluster.

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 iWorkflow™ 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.

The iWorkflow™ system creates two default users as part of the initial setup and licensing process. These user accounts cannot be revised (except for their passwords) or duplicated. After setup is complete, you can create additional user types and roles to meet your business needs.

Default user type	Default password	Access rights
admin	admin	This user type can access all aspects of the iWorkflow system from the system's user interface.
root	default	This user has access to all aspects of the iWorkflow system from the system's console command line.

User types persist and are available after an iWorkflow system failover. You can authenticate users locally on the iWorkflow system or remotely through LDAP or RADIUS.

Changing the default password for the administrator user

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

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

1. Log in to iWorkflow™ 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 iWorkflow user

You create a user and then associate that user with a particular role to define access to specific iWorkflow™ system resources.

1. Log in to iWorkflow™ 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 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. The iWorkflow™ system has a default set of roles you can assign to a user. Roles persist and are available after an iWorkflow system failover.

Roles definitions

iWorkflow™ 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 iWorkflow system. These responsibilities include: <ul style="list-style-type: none">• adding individual users• assigning roles• discovering BIG-IP® systems• installing updates• activating licenses• configuring an iWorkflow high availability (HA) configuration
Tenant	A tenant is an entity that can consist of one or more users accessing resources provided by an administrator. : These responsibilities include: <ul style="list-style-type: none">• customizing and deploying application templates• monitoring the health statistics and performance of applications and servers <hr/> <p><i>Note: The iWorkflow system creates a new role when an administrator creates a new tenant. When you create a tenant, you specify the connectors that tenant can access. The name of the new role is based on the tenant name. For example, creating a new tenant named <code>headquarters-user</code>, produces a new role named <code>headquarters-user (Cloud Tenant)</code>.</i></p> <hr/>

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 iWorkflow™ 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 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

If you want to change the resources a user can view and modify, you can use this procedure to disassociate a user from an assigned role.

1. Log in to iWorkflow™ with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the **Users** panel, for the user you want to edit, click the gear icon and then select **Properties**.
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 iWorkflow™ 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 iWorkflow™ with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, on the Licenses header, click the + icon. 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 iWorkflow 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 iWorkflow™ Device you are licensing is not connected to the public internet, you can activate the pool license manually.

1. Log in to iWorkflow™ with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, on the Licenses header, click the + icon. 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 iWorkflow 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 iWorkflow system refreshes and displays the dossier in the **Device Dossier** field.
7. 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/>.
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 iWorkflow 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.

Integrating with Cisco APIC

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 iWorkflow 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-<APIC Tenant>-<VRF Name>-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 on APIC cause device packages to push network configurations to BIG-IPs and iApp configuration to iWorkflow.
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. The iApp configuration is sent to iWorkflow by the device package. iWorkflow then translates this call and implements the service to the BIG-IP.
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

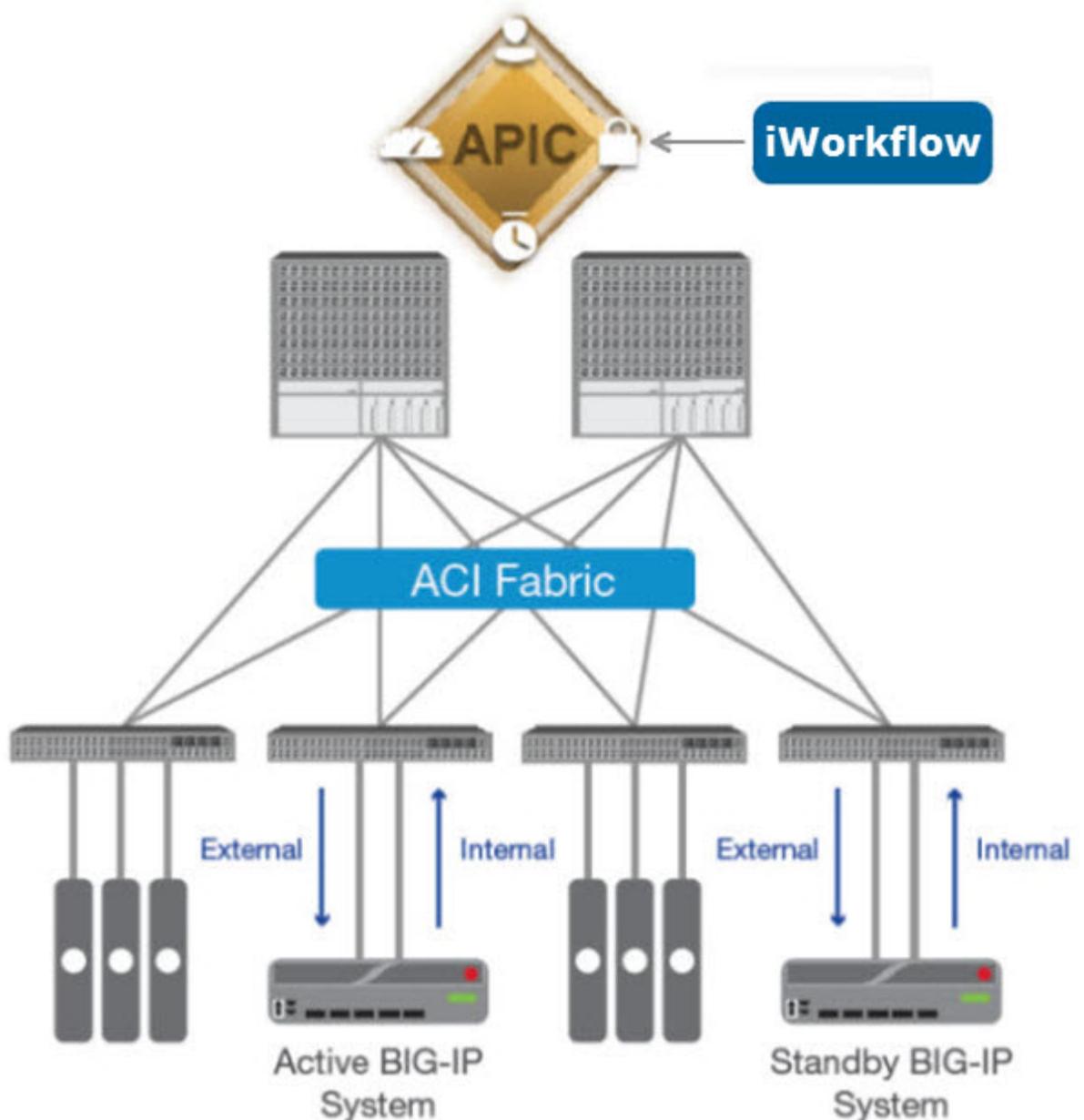


Figure 2: A typical network topology using the BIG-IP® system integrated with Cisco ACI

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 support.f5.com.

Version requirements

Make sure your environment meets or exceeds these requirements before you integrate F5® iWorkflow™ with Cisco APIC.

- Cisco APIC and Switch software
- F5 iWorkflow version 2.3.0

Minimum Cisco APIC requirements

Be sure your environment meets or exceeds these requirements before you integrate the F5® iWorkflow™ 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 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® iWorkflow™ with Cisco APIC. Refer to the BIG-IP® system documentation on the F5 technical support site (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 a supported version.

Note: For the most current list of compatible versions, refer to the *F5 iWorkflow compatibility matrix (K11198324)* on support.f5.com.

- 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 iWorkflow system.

About configuring the iWorkflow device for a Cisco APIC integration

Some of the tasks you perform to deploy iWorkflow™ in a Cisco APIC environment are performed on the iWorkflow 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.

Provisioning the vCMP feature

Before performing this task, ensure that the amount of reserve disk space that the provisioning process creates is sufficient. Attempting to adjust the reserve disk space after you have provisioned the vCMP® feature produces unwanted results.

Performing this task creates the vCMP host (the hypervisor) and dedicates most of the system resources to running vCMP.

Warning: *If the system currently contains any BIG-IP® module configuration data, this data will be deleted when you provision the vCMP feature.*

1. Log in to BIG-IP® device with the administrator user name and password.
2. On the Main tab, click **System > Resource Provisioning**.
3. Verify that all BIG-IP modules are set to **None**.
4. From the **vCMP** list, select **Dedicated**.
5. Click **Submit**.

After provisioning the vCMP feature, the system reboots TMOS® and prompts you to log in again. This action logs you in to the vCMP host, thereby allowing you to create guests and perform other host configuration tasks.

Create a vCMP connector

To enable integration between the vCMP® host and F5 iWorkflow™, you must configure a *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 that are required by third-party cloud providers.

1. Log in to iWorkflow™ with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, on the Clouds header, click the + icon. The **New Cloud** screen opens.
3. In the **Name** and **Description** fields, type a name and description for this connector.
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 **Connector Type** list, select **vCMP**.
The screen displays additional settings specific to vCMP.
5. In the **VCMP Host** field, type the IP address of the vCMP host.
6. For the **vCMP Host Certificate SHA-512 Hash** field, to avoid security threats, verify the SSL certificate hash of the host.

***Note:** Either manually enter or automatically retrieve the certificate hash. Run the command `openssl x509 -noout -fingerprint -sha512 -in <path to certificate file> | tr -d ':'` to verify with OpenSSL. If the iWorkflow certificate unexpectedly changes in the future, a warning displays and interactions with the host are prevented.*

7. In the **UserName** and **Password** fields, type the credentials that the iWorkflow device will use to authenticate to the vCMP host.

8. Click **Save**.

The vCMP connector begins managing the vCMP Host. vCMP guests will be automatically discovered and displayed in the **Devices** panel as they are created for this vCMP host.

During the automatic discovery of vCMP guests, you may need to enter the user name and password for the vCMP guest in the **Devices** panel. After you enter the credentials, click **Rediscover**.

It is important to associate a vCMP connector with each vCMP host before using the vCMP-based BIG-IP devices in an APIC deployment. The vCMP connector coordinates deployment of some network resources that affect vCMP guest and the vCMP host machines. These network resources include VLANs.

Creating a vCMP guest for Cisco APIC

Before creating a guest on the system, verify that you have provisioned the vCMP feature on the vCMP host.

The guests you create serve as virtual BIG-IP devices that manage traffic for your Cisco APIC integration.

***Note:** When creating a guest, if you see an error message such as `Insufficient disk space on /shared/vmdisks. Need 24354M additional space.`, you must delete existing unattached virtual disks until you have freed up that amount of disk space.*

***Important:** If you are planning to add this guest to a Sync-Failover device group and enable connection mirroring with a guest on another chassis, you must ensure that the two guests are configured identically with respect to slot assignment and core allocation. That is, the number of cores, the number of slots, and even the slot numbers on which the guests reside must be the same. Therefore, you must ensure that on each guest of the mirrored pair, the values match for the **Cores per Slot**, **Number of Slots**, **Minimum Number of Slots**, and **Allowed Slots** settings.*

1. Use a browser to log in to the vCMP® host, using the primary cluster management IP address.

2. On the Main tab, click **vCMP > Guest List**.

This displays a list of guests on the system.

3. Click **Create**.

4. From the **Properties** list, select **Basic**.

5. In the **Name** field, type a name for the guest.

6. In the **Host Name** field, type a fully-qualified domain name (FQDN) name for the guest.

If you leave this field blank, the system assigns the name `localhost.localdomain`.

7. From the **Cores Per Slot** list, select the total number of logical cores that the guest needs, based on the guest's memory requirements.

The value you select causes the host to assign that number of cores to each slot on which the guest is deployed. The host normally allocates cores per slot in increments of two (two, four, six, and so on).

Important: Cores for a multi-slot guest do not aggregate to provide a total amount of memory for the guest. Therefore, you must choose a **Cores per Slot** value that satisfies the full memory requirement of the guest. After you finish creating the guest, the host allocates this amount of memory to each slot to which you assigned the guest. This ensures that the memory is sufficient for each guest if any blade becomes unavailable. For blade platforms with solid-state drives, you can allocate a minimum of one core per guest instead of two. For metrics on memory and CPU support per blade model, see the vCMP® guest memory/CPU allocation matrix at <http://support.f5.com>.

8. From the **Number of Slots** list, select the maximum number of slots that you want the host to allocate to the guest.
9. From the **Management Network** list, select a value:

Value	Result
Bridged (Recommended)	Connects the guest to the management network. Selecting this value causes the IP Address setting to appear.
Isolated	Prevents the guest from being connected to the management network and disables the host-only interface.

Important: If you select **Isolated**, do not enable the **Appliance Mode** setting when you initially create the guest. For more information, see the step for enabling the **Appliance Mode** setting.

10. If the **IP Address** setting is displayed, specify the required information:
 - a) In the **IP Address** field, type a unique management IP address that you want to assign to the guest.
You use this IP address to access the guest when you want to manage the BIG-IP modules running within the guest.
 - b) In the **Network Mask** field, type the network mask for the management IP address.
 - c) In the **Management Route** field, type a gateway address for the management IP address.

Important: Assigning an IP address that is on the same network as the host management port has security implications that you should carefully consider.

11. From the **Initial Image** list, select the ISO image file for creating the guest's virtual disk that matches the other guests in the cluster.
12. From the **Initial Hotfix** list, select the hot fix for creating the guest's virtual disk that matches the other guests in the cluster.
13. Do not set up any VLANs.
14. In the **Requested State** list, retain the default value, **Configured**.
15. Click **Finish**.
The system installs the selected ISO image onto the guest's virtual disk and displays a status bar to show the progress of the resource allocation.

You now have a new vCMP guest on the system in the Configured state with an ISO image installed.

Deploying a vCMP guest for Cisco APIC

Setting a guest to the Deployed state makes it possible to provision and configure BIG-IP® modules on the guest.

1. Confirm that you are logged in to the vCMP host.
2. On the Main tab, click **vCMP > Guest List**.
The display lists the guests and their current configurations.

3. Select the guest to deploy.
4. Click **Deploy**.

When the vCMP® guest is in the Deployed state, you can provision and configure BIG-IP modules within the guest so that the guest can begin processing application traffic.

Discovering a BIG-IP guest

Before you can discover a vCMP guest, you must first create and deploy it on the vCMP host.

Discovering BIG-IP devices is the first step to managing them.

Important: *If you are configuring an integration with a BIG-IP device, use the Discovering a BIG-IP device in your network by its IP address task instead of this one.*

1. Log in to iWorkflow™ with the administrator user name and password.
2. On the Devices header, click the + icon, and then select **Discover Device**.
The Devices panel expands to show the Discover Device screen.
3. For the **IP Address**, specify the guest's management IP address.
4. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.
5. Click **Save** to start the discovery task.

The iWorkflow system populates the properties of the guest that you added in the Devices panel.

Repeat this task to create a second guest on a second BIG-IP host to serve as a high availability peer for this guest.

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

After you license and perform the initial configuration for the iWorkflow™ system, you can discover BIG-IP® devices running supported versions.

Note: *For the most current list of compatible versions, refer to the F5 iWorkflow compatibility matrix (K11198324) on support.f5.com.*

For discovery to succeed, you must configure the iWorkflow system with a route to each F5 device that you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

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

Important: *If you are configuring an integration with a BIG-IP guest, use the Discovering a BIG-IP guest task instead of this one.*

Important: *A vCMP® host cannot be discovered using the Device panel. To manage a vCMP host, you must create a vCMP Cloud connector.*

Important: *In this release of iWorkflow, guests in a VIPRION® cluster cannot be discovered using the Device panel.*

Discovering BIG-IP devices is the first step to managing them.

Important: When you discover a device, iWorkflow software installs components on the device. The installation process 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. Log in to iWorkflow™ with the administrator user name and password.
 2. Select either the **Clouds and Services** or **BIG-IP Connectivity** component.
 3. On the Devices header, click the + icon, and then select **Discover Device**.
-

Note: You can perform this step in either iWorkflow Device or iWorkflow Cloud.

The Devices panel expands to show the Discover Device screen.

4. For the **IP Address**, specify the device's internal self-IP address.
 5. 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.

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

The iWorkflow system populates the properties of the device that you added in the Devices panel.

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 use vCMP® with iWorkflow 2.3.0, you must create the vCMP connectors before you create an APIC connector.

To enable integration between an APIC and iWorkflow™, you must create a *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.

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

1. Log in to iWorkflow™ with the administrator user name and password.
2. On the Clouds header, click the + icon.
The New Cloud 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 **Connector Type** list, select **Cisco APIC**.
5. Click **Save**.

Exporting an iApps template

Before exporting an iApps® Template, make sure to discover a BIG-IP® device or guest in your network by its IP address.

You export an iApps Template on a BIG-IP system in order to continue the discovery process before importing an iApps Template to iWorkflow™.

1. Log in to a BIG-IP system with your username and password.

2. On the Main tab, click **iApps > Templates**.
The Templates list screen opens.
3. In the template list Name column, click **f5.http**.
The template properties screen opens.
4. Scroll to the bottom of the screen and click **Export**.
5. On the Export Templates and Scripts screen, for the **Archive File** setting, click **Download:<file name>** and save the file locally.
6. With a text editor, open the file you just downloaded. The default file name is `template.tmpl`.
7. Search for the template value within the iApps file; this is typically found toward the top of the file.
Example of the template value for `f5.http.iApp:sys application template /Common/f5.http`.
8. Update the version details in compliance with the iWorkflow requirements.
The version numbers are arbitrary, but must increment in ascending order for iWorkflow to automatically import updates. Use this format for an iApps file: `name.v#. #. #` or `name_v#. #. #`, where `name` is the file name and `v#. #. #` is the version number. Example using `f5.http:sys application template /Common/f5.http.v1.0.0`.
9. Click **Save**.

Importing an iApps template

Before you can import an iApps[®] Template, you must discover the F5[®] devices that you plan to include in your Cisco APIC integration, and add a Cisco APIC connector.

You manually import an iApps Template to the iWorkflow[™] system. [®]*iApps templates* create configuration-specific forms used by application services to guide authorized users through complex system configurations.

Important: *If you make a modification to an iApps Template, the version number in the file must change, but the file name can remain the same. It is a best practice to include the version number in the file. The version numbers are arbitrary, but must increment in ascending order for iWorkflow to automatically import updates. Use this format for an iApp file: `name.v#. #. #` or `name_v#. #. #`, where `name` is the file name and `v#. #. #` is the version number.*

1. Log in to iWorkflow with your administrator user name and password.
2. At the top of the screen, click **Clouds and Services**.
3. On the iApps Templates header, click the + icon.
The panel expands to display the New iApps Template.
4. For the **iApps Source** setting, either import a template from a local file or copy and paste the template content:
 - To select a file to import, click **Choose File**.
 - To paste template content that you have, first, from the drop-down list select **Paste TMPL file contents**, and then paste the contents of the template in the text box.
5. In the **iApps APL JSON** setting, either select a BIG-IP device to use, or paste JSON content.
 - Use an existing BIG-IP device:
 1. Leave the first list setting as **Retrieve JSON from BIG-IP**.
 2. From the second drop-down list, click **Select** and select a managed BIG-IP device to use to retrieve the JSON representation.
 - Provide custom JSON from a local file:

1. From the first drop-down list, select **Provide JSON**.
2. Then click **Choose File** to import a file.
- Provide custom JSON directly:
 1. From the first drop-down list, select **Provide JSON**.
 2. Then from the second drop-down list, select **Paste JSON file content**.
 3. In the text box, paste the contents of a template.
6. Optional: In the **Minimum Supported BIG-IP Version** field, type a minimum BIG-IP version supported for deployment with the iApps Template.
7. Optional: In the **Maximum Supported BIG-IP Version** field, type a maximum BIG-IP version supported for deployment with the iApps Template.
8. Optional: In the **Unsupported BIG-IP Versions** field, click the + icon to type each individual BIG-IP version you want to exclude.
Click the x icon to remove a version.
9. Click **Save**.

Creating a customized service 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.

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 have deployed a service using a template, the template cannot be modified until the associated services are removed. Alternatively, you can create a new template based on the template already in use.*

1. Log in to iWorkflow™ with your administrator user name and password.
2. At the top of the screen, click **Clouds and Services**.
3. On the Service Templates header, click the + icon.
The panel expands to display the New L4-L7 Service Template screen.
4. For the **Input method** setting, you can retain the default, import a template from a local file, or copy and paste the template content:
 - To retain the default:
 1. Verify that **Use Form** is selected.
 2. Proceed to the **iApps Template - Name & Version** setting, and step 5.
 - To select a file to import:
 1. From the list, select **Use pre existing JSON**.
 2. Then click **Choose File**.
 3. Click **Save**.
 - To paste template content that you have:
 1. From the list, select **Use pre existing JSON**.
 2. From the second list, select **Paste JSON file contents**, and then paste the contents of the template into the text box.
 3. Click **Save**.
5. For the **iApps Template - Name & Version** setting, select the name of the iApps template you want to use, and then select an iApps Template version.

- Optional: From the **Inherited Values** list, select an existing Service Template to inherit all the settings that have been configured.
- In the **Name** field, type a name for a new L4-L7 Service Template.
- From the **Cloud Availability** list, select the name of the cloud template previously created.
- For the **Displayed Parameters** setting, select **All** to view all of the parameters for the template you select.
- In the Service Tier Information area, define variable names in the drop-down lists.
Examples of variable names that are known to work with the `f5.http` iApps Template:
 - Name:** `base_template`
 - Virtual Address:** `pool_addr`
 - Virtual Port:** `pool_port`
 - Pool:** `pool_members`
 - Server Address:** `addr`
 - Server Port:** `port`
 - SSL Cert:** `ssl_cert`
 - SSL Key:** `ssl_key`
- In the Sections area that displays each of the variable names, either type a **Default Value**, or select the **Tenant Editable** check box to define each variable name. The exception is **Name**, which is not defined in the iApps Template.

Note: Wrong values can cause issues with deployments as Cisco APIC tries to set variable names that are not defined in the Service Template.

- Click **Save** to save the template.
The values set as **Tenant Editable** are now part of the defined Common Options for the newly created Service Template.

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

About configuring the Cisco APIC for iWorkflow integration

After you finish configuring iWorkflow™ 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 1.2(2h). Controls for later versions of the user interface are likely to differ slightly.

- Log into Cisco APIC as an administrator.
- On the menu bar, click **L4-L7 SERVICES**, and then click **PACKAGES**.

- In the right pane, click **Import a Device Package**.

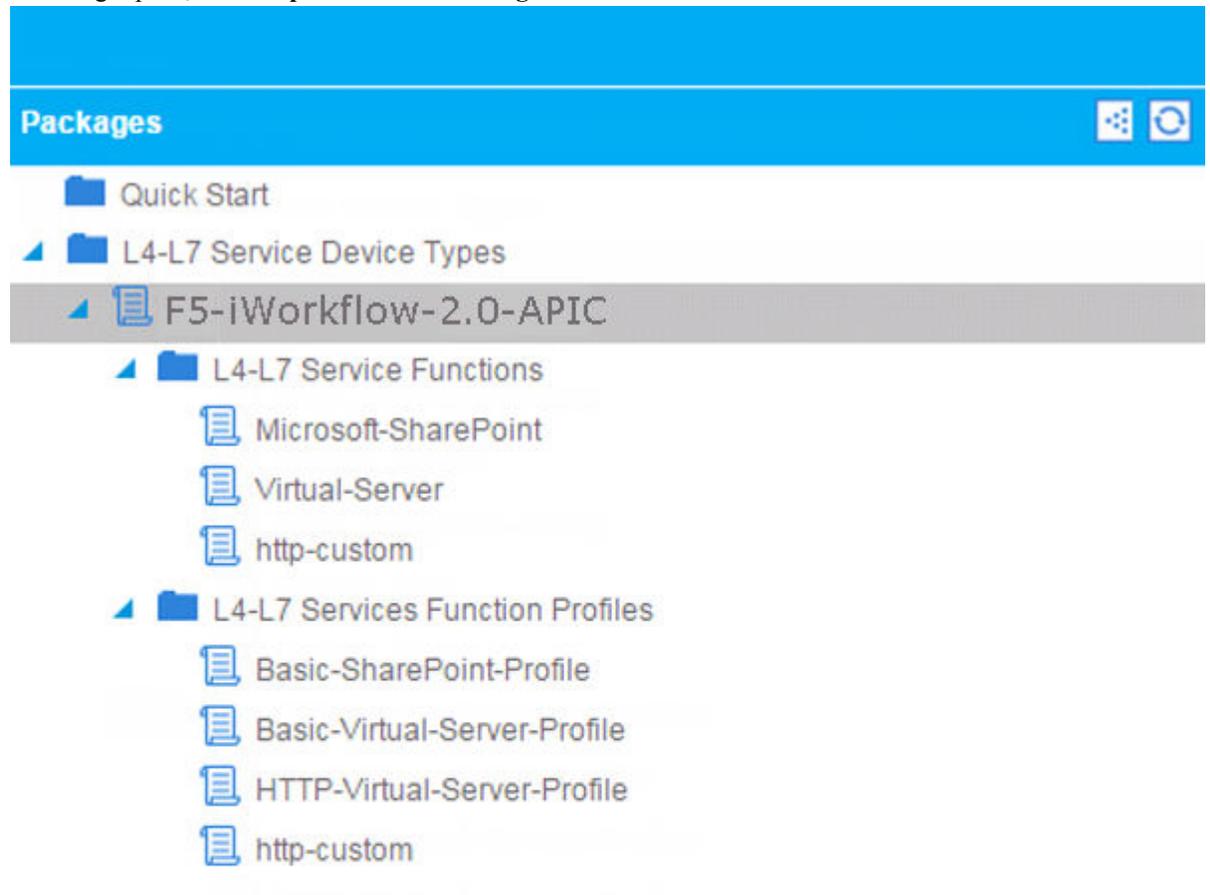


Figure 3: Importing the Device Package

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

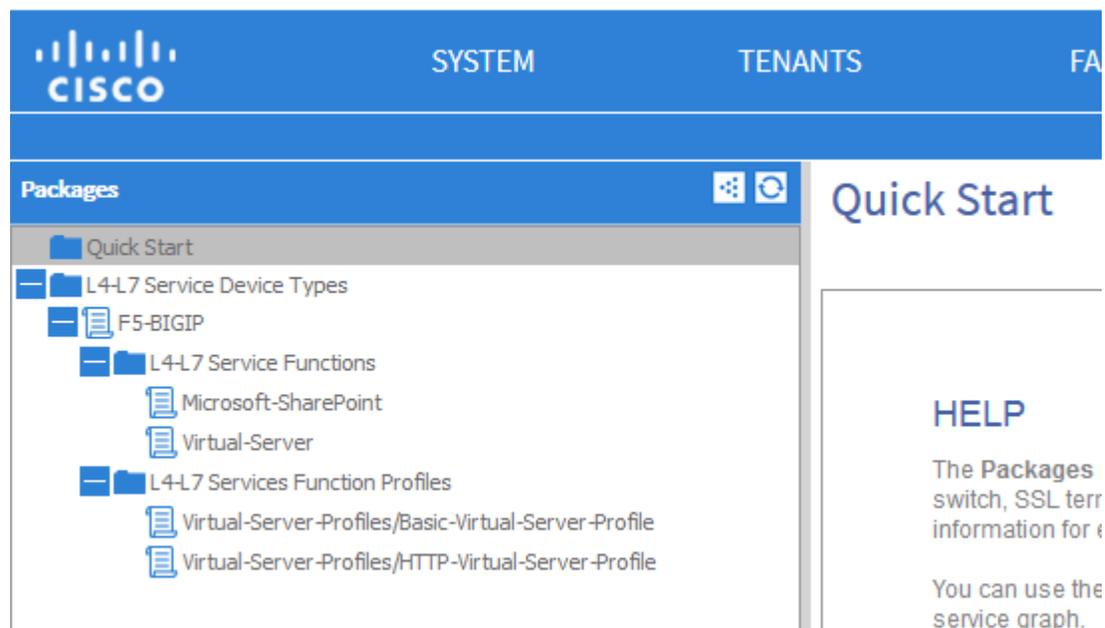


Figure 4: Verifying successful installation of the package

Once the F5 iWorkflow 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.

Creating a new chassis type

You must create a new L4-L7 chassis type before you can specify configuration details for it.

Note: If you are not using a vCMP[®] guest, you do not need to create a new chassis type.

1. On the menu bar, click **L4-L7 Services** and then click **Inventory**.
2. In the left pane, right-click **L4-L7 Chassis Types**, and select **Create L4-L7 Chassis Type**.
3. For the **Vendor**, type F5.
4. For the **Model**, type iWorkflow.
5. For the **Version**, type 2.0-apic.
6. For the **L4-L7 Service Device Type**, select the name of the device package you created for this integration.
7. Click **Submit**.

The new chassis type appears in the list under L4-L7 Chassis Types.

Creating a chassis manager

You need the management IP address, user name and password for the vCMP hosts on which your guests reside.

Using the chassis manager, you specify the configuration details for the vCMP hosts on which your vCMP guests reside. Cisco APIC needs these details so it can communicate with the guests. When you use multiple vCMP hosts to create a high availability cluster, create a new chassis for each host.

Note: Do not perform this procedure if you don't use vCMP guests to form your device cluster.

1. On the menu bar, click **Tenants**, and then double-click the tenant for whom you are creating configurations.

Note: You will probably want to create the chassis manager and the L4-L7 Devices in the same APIC tenant.

2. In the left pane, expand **L4-L7 Services**, then right-click **Chassis**, and select **Create Chassis**.
3. For the Chassis Name, type a name that will help you identify this chassis.
4. For the Chassis Type, select the type you just created.
5. Under Management, type in the IP address and port number for the vCMP host that house your guests.
6. Use the vCMP host credentials to fill in the Username and Password, and Confirm Password fields.
7. Click **Submit**.

Creating a new device manager type

You must create a new device manager type before you can create a new device manager and you need a device manager before you can create a new cluster.

1. On the menu bar, click **L4-L7 Services** and then click **Inventory**.
2. In the left pane, right-click **Device Manager Types**, and select **Create Device Manager Type**.
3. For the **Vendor**, type F5.
4. For the **Model**, type iWorkflow
5. For the **Version**, type 2.0-<name>
Where <name> is a descriptive name of your choosing.
6. For the **L4-L7 Service Device Type**, select the name of the device package you uploaded for this integration.
7. Click **Submit**.

The new device manager type appears in the list under L4-L7 Chassis Types. The name will appear as F5-iWorkflow-2.0-<name>

Creating a new device manager

You must create a new device manager before you can create a new device cluster.

1. On the Tenants tab select tenant for which you want to create a new device manager.
2. In the left pane, expand **L4-L7 Services**.
3. In the left pane, right-click **Device Manager**, and select **Create Device Manager**.
4. For the **Device Manager Name**, type a name for the new device manager.

5. Leave **Management EPG** blank, or if you are managing the iWorkflow system in-band, select the appropriate end-point-group.
6. For **Management**, specify the IP address and port for the iWorkflow system and then click **UPDATE**.
If you have additional iWorkflow systems managed by the device manager, click the + icon to add additional addresses and ports for each system. Click **UPDATE** for each new entry in the list.
7. For the **Username** and **Password**, type the credentials required to access the iWorkflow system.

Note: All of the iWorkflow systems managed by this device manager must use the same credentials.

8. Click **Submit**.

The new device manager type appears in the list under L4-L7 Chassis Types. The name will appear as F5-iWorkflow-2.0-<name>

Creating a device cluster for BIG-IP devices

If the devices in the cluster are vCMP[®] guests, before you create the device cluster, you must create the vCMP guests.

As part of the iWorkflow[™] and Cisco APIC integration, you create an L4-L7 device cluster. Creating the BIG-IP[®] device cluster using the F5 Device Package tells APIC a number of things about the F5 BIG-IP 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. On the menu bar, click **Tenants**, and then double-click the tenant for whom you are creating configurations.

Note: You will probably want to create your device clusters (L4-L7 Devices) in the tenant named Common. While not required, it is helpful to put these objects in a designated shared tenant.

2. In the left pane, expand **L4-L7 Services**, then right-click **L4-L7 Devices**, and select **Create L4-L7 Devices**.
3. Specify the settings under General:
 - a) For the **Name**, type in a name to identify this cluster.
 - b) For the **Physical Domain**, select **phys**.
 - c) For the **Mode**, select **Single Node** for a standalone device, or **HA Cluster**, if you are configuring a high availability vCMP cluster.
 - d) For the **Device Package**, select the one you created previously for this integration.
 - e) For **Model**, select **Unknown (Manual)**.
 - f) For **Context Aware**, click **Multiple**.
4. For **Credentials**, type in the user name and password for the iWorkflow device that you are using for this integration.
5. Specify the settings for **Device 1**:
 - a) For the **Management IP Address**, type in the IP address for the first device in your new cluster

Important: If you are configuring a vCMP integration, use the IP address of the guest.

- b) For the **Chassis**, select the chassis that you created that corresponds to the vCMP host that houses your guest.

Note: If you are not using vCMP, leave this field empty.

- c) For the **Management Port**, select **https**.
- d) For the **Device Interfaces**, identify each of the physical interfaces that connect to the ACI fabric.
6. Specify the settings for **Device 2**; just as you did for **Device 1**.
7. Specify the settings for the **Cluster**:
- a) For the **Management IP Address**, type in the IP address of the iWorkflow device you are using to manage this integration.
- b) For the **Management Port**, select **https**.
- c) For Device Manager, select the name of the manager you created for this integration.
- d) For the **Cluster Interfaces**, identify each of the physical interfaces that connect to the ACI fabric.

*Note: For the external interface, you select **consumer**; for the internal interface, you select **provider**.*

8. When you finish specifying the settings for the device cluster, click **NEXT**.
The Device Configuration screen opens.

9. Click **All Parameters**, then expand **High Availability**.

Note: These two settings are required for both pre-configured and APIC-configured BIG-IP® clusters.

- a) Identify the physical interfaces that connect each of your devices.
- b) Specify values for the following parameters for your both of your BIG-IP devices: **High Availability Interface Name**, **High Availability Self IP Address**, **High Availability Self IP Netmask**, and **High Availability VLAN**.
10. If you are creating a preconfigured BIG-IP cluster, specify the following settings:
- a) Under High Availability, for the **BIG-IP Cluster pre-configured?** setting, select **Yes** for both of your BIG-IP devices.
- b) Expand **Cluster** and select **All Parameters**.
- c) Expand **Cluster Preconfigured**, and then for **BIG-IP Cluster pre-configured?**, select **Yes**.

*Note: To complete this task, you must provide the required parameters in the High Availability folder. Although these parameters are required, APIC ignores the values you specify because you selected **Yes** in the **BIG-IP Cluster pre-configured?** field.*

11. If you are creating an APIC-configured BIG-IP cluster, specify the following settings:
- a) Click **All Parameters**, then expand **Device Host Configuration**.
- b) For the **Host Name**, type the host names for both devices; one under **Device 1 Value**, and the other under **Device 2 Value**. Click **Update**, when you finish.
- c) For the **NTP Server**, type the IP address of your NTP server under **Device 1 Value (Device 2 Value should then populate automatically)**.
- d) Expand **High Availability**, and identify the physical interfaces that connect each of your devices. Specify values in all four fields for both devices.

*Note: You do not need to specify a setting for the **VCMP Configuration** parameter. With APIC 2.0, the Chassis Manager supplies this information.*

*Note: If you selected a device manager, you do not need to specify an address for the iWorkflow Configuration. If you did not select a device manager, expand **iWorkflow Configuration** and type the management IP address of the iWorkflow system in the **BigiqHost** field.*

- Optionally, you can assign a label for each BIG-IP device. Expand the device cluster you just created, click a device, then click **Policy** near the top right. In **Context Label**, type a name that will help you recognize this device in the cluster.

Note: The context label will be useful when you fill in network information (such as self IP addresses) when you deploy a graph.

- Click **FINISH**.

Cisco APIC processes the information you provided and creates the device cluster. As part of the creation process, iWorkflow creates a new VLAN and associates both guests with it. 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.

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.

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

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



The screenshot shows a dialog box titled "EXPORT DEVICE CLUSTER". The dialog contains the following elements:

- Header: "EXPORT DEVICE CLUSTER" with an information icon.
- Text: "Choose a device cluster and a tenant to export"
- Device Cluster: A dropdown menu with "F5-2" selected.
- Tenant: A dropdown menu with "Customer1" selected.
- Description: An empty text input field.
- Buttons: "SUBMIT" and "CANCEL" at the bottom right.

Figure 5: Exporting the device cluster

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

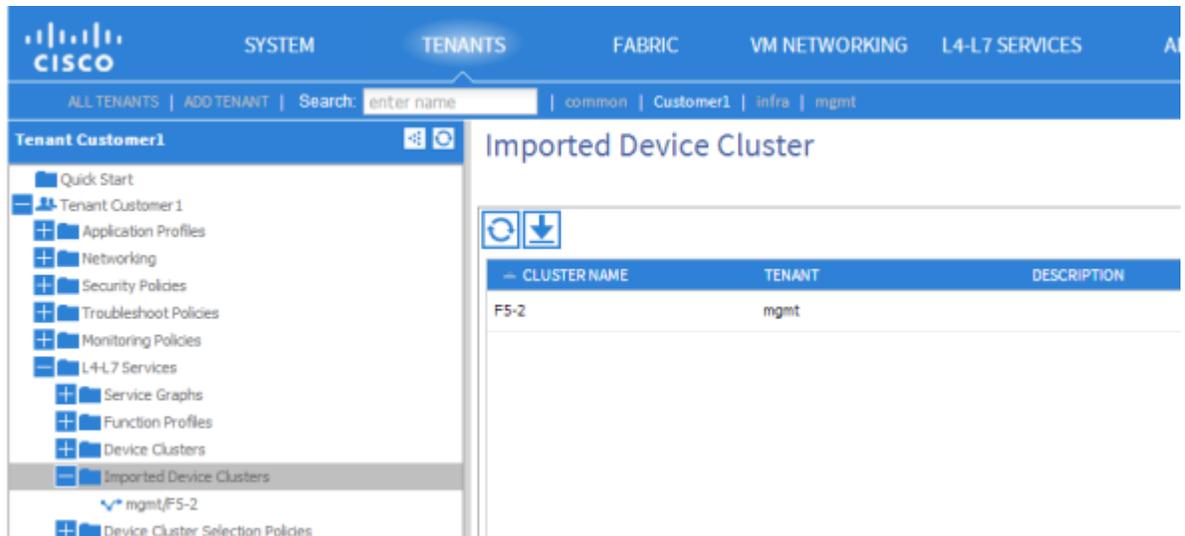


Figure 6: Viewing the device cluster

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

About service graphs

A *service graph* is a single listener (iApp) 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 iApp itself is unique, so each service graph is one iApp. You can associate configuration objects and you can share some of those objects between the service graphs (iApps). The iApp port, protocol, and IP address are all unique.

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

Managing SSL certificates and keys

To enhance security, SSL certificates and keys are managed locally in the SSL Certificate List under BIG-IP File Management.

Using the iWorkflow service catalog workflow, when you create a template, you can reference SSL certificates and keys that are stored in the Common partition. You must have Administrator rights to perform this task.

In the following example, the f5.http iApp template is being used to create a new template. It is referencing SSL certificates and keys that are stored in the /Common partition.

SSL Encryption 6/6			
Name	Description	Default Value	Tenant Editable
ssl_cert	Which SSL certificate do you want to use?	/Common/default.crt	<input type="checkbox"/>
ssl_client_ssl_pro...	Which Client SSL profile do you want to use?	/#create_new#	<input type="checkbox"/>
ssl_key	Which SSL private key do you want to use?	/Common/default.key	<input type="checkbox"/>

Figure 7: Managing SSL certificates and keys

As Administrator, you have the option to make this field tenant editable, which makes the SSL certificate and key fields visible in the Cisco APIC user interface.

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 **Graph Name** field, type a name for the service.
6. From the **Type** list, select either **Single Node - ADC in One-Arm Mode** or **Single Node - ADC in Two-Arm Mode**, depending on your requirements.
This setting determines the node configuration.
7. For the **Device Function**, select the entry with the name that matches the catalog template you created on the iWorkflow[®] device.

Note: You can do this step by dragging and dropping the device cluster you want to the center of the window.

8. For the **Profile**, select the entry with the name that matches the catalog template you created on the iWorkflow 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**.

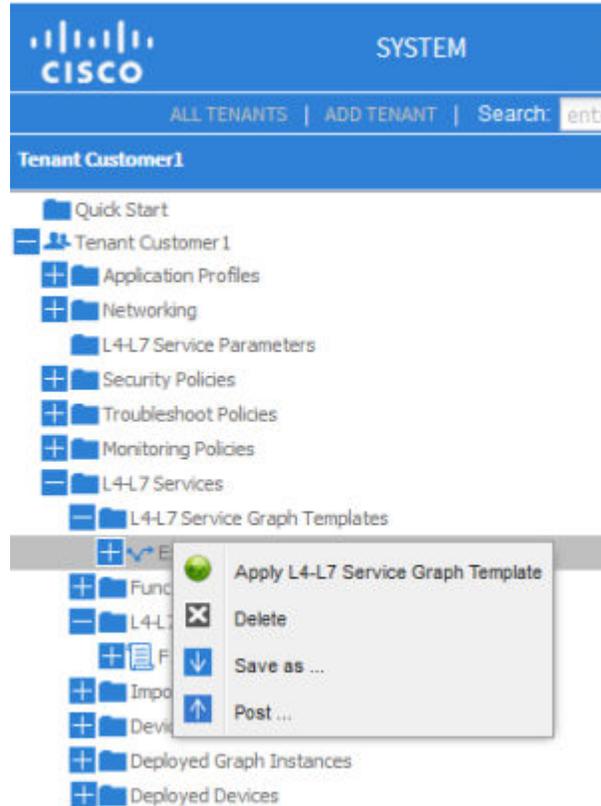


Figure 8: Applying the service graph template

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 1.2(2h) interface. Later versions will likely be slightly different.

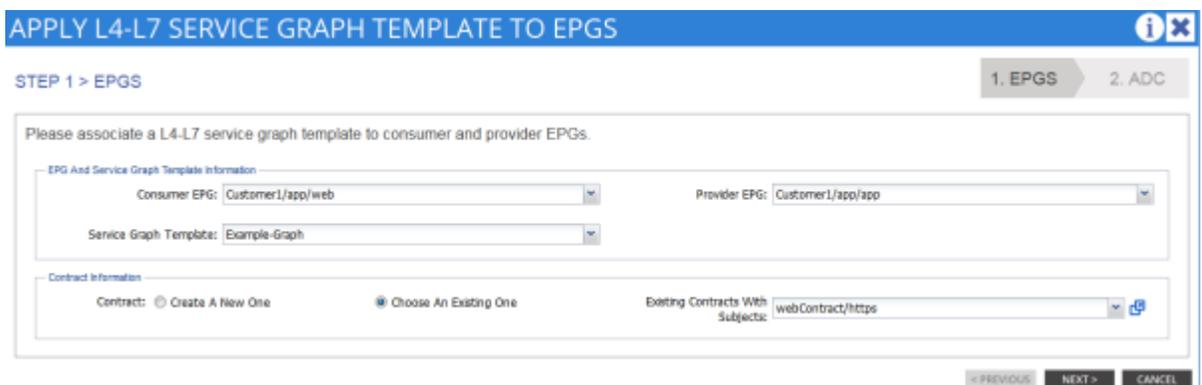


Figure 9: Applying the service graph template to EPGs

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 that you configured on the iWorkflow 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.

Required parameters appear in red text. Additionally, 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 iWorkflow device that you specified to the BIG-IP device(s) you specified.

If you log in to the iWorkflow™ device and look at the Services panel, 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 having to perform complicated networking procedures.

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

- Create a tenant - When you create a tenant, iWorkflow[™] 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. Log in to iWorkflow[™] with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, on the Tenants header, click the + icon. The panel expands to display property fields for the new tenant.
3. 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.
4. From the **Available Clouds** list, select the cloud 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 Clouds** list.
5. In the **Address**, **Phone**, and **Email** fields, type optional contact information for this tenant.
6. 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. Log in to iWorkflow[™] with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, on the Users header, click the + icon. The panel expands to display property fields for the new user.
3. In the **Username** field, type a name to identify this user.
4. From the **Auth Provider** list, select the provider that supplies the credentials required for authenticating this user. If you configured iWorkflow System to authenticate using LDAP or RADIUS, you have the option to authenticate this user through one of those methods. Refer to

Software Licensing and Initial Configuration for information about how to configure LDAP and RADIUS authentication.

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 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.

***Tip:** The iWorkflow™ system administrator creates roles from the **Access Control** menu. For more information, refer to *Users, User Groups, and Roles*.*

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

1. Log in to iWorkflow with the administrator user name and password.
2. At the top of the screen, click **Clouds and Services** and then, 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.

iWorkflow High Availability

About setting up a high availability cluster

You can ensure that your application management functions are always available by configuring three iWorkflow™ systems in a high availability (HA) configuration. If one device in an HA configuration fails, one of the HA peers takes over application delivery management.

Any configuration changes that occur on one iWorkflow system are immediately synchronized with its peer devices.

Configuring a high availability cluster

You must perform basic system setup and activate a license on all three iWorkflow™ systems before you can configure a high availability cluster.

Configuring iWorkflow™ as part of a high availability (HA) cluster ensures that you do not lose application delivery management capability because one iWorkflow system fails.

Important: You should designate one of the iWorkflow devices in the HA cluster as the lead device. Once you create the cluster, make configuration changes only to that device and let the automatic syncing process work.

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

Important: To synchronize properly, the iWorkflow systems must be running the same version of software. The exact configuration in terms of virtual 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 all systems. This is especially important in terms of disk space and data collection.

Important: The devices that you add as HA peers 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 syncing process.

Important: You can either operate the iWorkflow system in standalone mode, or as part of a three-peer cluster. Other configurations are not supported at this time.

1. Log in to iWorkflow™ with the administrator user name and password.
2. At the top of the screen, click **System Settings** and then, on the iWorkflow Cluster header, click the + icon.
The New iWorkflow Cluster Member screen opens.
3. In the **IP Address** field, type the address used to access the HA peer.
If you specified **Use Management Address** when you configured this device, then use the management IP address. Otherwise, use the device's self IP address.
4. In the **Admin Username** and **Password** fields, type the administrative user name and password for the system.

5. Click the **Add** button, and then click **OK** to add this device to the high availability cluster.
The system discovers its peer and displays its status.
6. Repeat steps 2 - 5 to add a third device to the HA cluster.

If discovery of the newly configured iWorkflow 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

iWorkflow terminology

Before you manage cloud resources, it is important that you understand some common terms as they are defined within the context of the iWorkflow™ system.

Term	Definition
<i>service templates</i>	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.
<i>iWorkflow</i>	The iWorkflow™ system streamlines management and access for tenants to services and applications hosted by local and/or cloud-based servers.
<i>cloud administrator</i>	Cloud administrators are iWorkflow users who 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.
<i>cloud connector</i>	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.
<i>peer leader</i>	A peer leader is a node in a cluster that you select for all iWorkflow administrative functions. A peer leader can be any member of the cluster. Changes and updates to the peer leader trigger a local write and replication to the peers.
<i>resources</i>	A resource is any managed object, including devices, web applications, virtual servers, servers, cloud connectors, and so forth.
<i>roles</i>	A role defines specific privileges to which you can associate one or more users. There are two default roles for iWorkflow: cloud administrator and cloud tenant.
<i>tenant</i>	A tenant is an entity that can consist of one or more users accessing resources provided by a cloud administrator.
<i>user</i>	A user is an individual who has been granted access to specific tenant resources.

Legal Notices

Legal notices

Publication Date

This document was published on August 28, 2017.

Publication Number

MAN-0610-05

Copyright

Copyright © 2017, F5 Networks, Inc. All rights reserved.

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

Trademarks

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

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

Patents

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

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Index

A

- active-active pair
 - about configuring for the iWorkflow system 53
 - configuring for the iWorkflow system 53
- admin, *See* administrator
- Administrator role
 - defined 24
- administrator user
 - changing password for 9, 23
- administrator user password
 - changing 9, 23
- APIC
 - about 29
 - integration 29
- APIC guests
 - setting to Deployed state 35
- application templates
 - about 33
 - defined 55
- authorization checks
 - for secure communication 5

B

- base registration key
 - about 7, 8
- BIG-IP and Cisco APIC requirements 32
- bridged network
 - setting 34

C

- catalog
 - for services 39
- catalog entries
 - creating for tenants 33
- chassis manager
 - creating 43
- chassis type
 - creating 42, 43
- Cisco APIC
 - about configuring for iWorkflow integration 40
 - installing BIG-IP device package 40
- Cisco APIC connector
 - adding 37
- Cisco APIC requirements 32
- cloud administrator
 - defined 55
- cloud bursting
 - defined 55
- cloud connector, local
 - associating with a device 37
- cloud connectors
 - defined 55
- cloud resources
 - providing for tenants 33, 51
- cloud tenants

- cloud tenants (*continued*)
 - about creating 51
 - adding 51
- cluster
 - breaking 13, 17
 - recreating 15, 19
- clusters
 - for high availability 53
- communication
 - between iWorkflow and managed devices 5
- configuration
 - and initial setup 7, 8
- configuration data
 - and vCMP provisioning 33
 - backing up 21
 - restoring 22
- connector, local
 - associating with a device 37
- core allocation
 - configuring 34

D

- Deployed guest state
 - purpose of 35
- device clusters
 - about 40
 - confirming creation 46
 - creating 44
 - exporting to tenant 46
 - viewing 46
- device discovery
 - by scanning network 36
- device package
 - installing 40
- devices
 - adding 36
 - discovering 36
- discover guest
 - using IP address 36
- discovery address
 - defined 7
- disk space
 - and vCMP provisioning 33
 - insufficient 34
- DNS server
 - specifying for the iWorkflow system 9
- documentation, finding 5
- dossier
 - providing 7, 8

F

- failover 53

G

- glossary 55
- guest
 - adding 36
- guest IP addresses
 - configuring 34
- guest states
 - configuring 34
- guests
 - creating 34
- guides, finding 5

H

- high availability
 - configuring 53
- high availability configuration
 - about 53
- hotfix
 - installing 17
- HTTPS port 443
 - required for communication 5

I

- iApps
 - customizing for tenants 33
 - defined 33
- iApps template
 - exporting 37
- iApps Templates
 - importing 38
- initial configuration
 - for iWorkflow system 7
- ISO images
 - installing 34
- isolated network
 - setting 34
- iWorkflow
 - about 5
 - defined 55
- iWorkflow device package for Cisco APIC
 - installing on Cisco APIC 40
- iWorkflow integration
 - about configuring Cisco APIC 40
- iWorkflow system
 - about activating 7
 - about backing up 21
 - about file names 21
 - about licensing 7
 - about locations 21
 - about restoring 21
 - about upgrading 11

L

- L4-L7 service graph template
 - applying 49
- license
 - activating automatically 7
 - activating manually 7, 8

- license (*continued*)
 - manually activate a pool license 27
- license activation
 - for iWorkflow system 7, 8
- licenses
 - about managing for devices 27
 - about pool licenses 27
- licensing
 - activating pool license automatically 27
 - activating pool license manually 27
 - for managed devices 27
 - for pool license 27
- local cloud connector
 - associating with a device 37

M

- management network mode
 - setting 34
- managing
 - SSL Certificates and keys 47
- manual activation
 - for pool license 27
- manuals, finding 5
- memory allocation
 - configuring 34
- minimum requirements
 - for BIG-IP system and Cisco APIC 32
 - for Cisco APIC 32

N

- network
 - incorporating iWorkflow systems 7
- network configurations
 - customizing for tenants 33, 39
- network configurationsiApps
 - customizing for tenants 33, 39
- network security
 - about 5
- network topology 31
- new connectors
 - adding a vCMP 33

P

- Pacific Standard Time zone
 - as default for the iWorkflow system 9
- password
 - changing for administrator user 9, 23
- peer leader
 - defined 55
- pool license
 - activating automatically 27
 - activating manually 27
- pool licenses
 - about 27
- port 22
 - using 5
- port 443
 - required for communication 5
 - using 5

- ports
 - required for communication with iWorkflow 5
 - required open 5
- privileges
 - removing from users 25
- provisioning
 - for vCMP feature 33
- PST zone, *See* Pacific Standard Time zone

R

- related documentation 30
- release notes, finding 5
- requirements
 - for BIG-IP system 32
 - for BIG-IP system and Cisco APIC 32
 - for Cisco APIC 32
 - for software version 32
- resources
 - defined 55
 - providing access for user 52
- roles
 - associating with users and user groups 24
 - defined 23
 - for users 23, 24
 - removing from a user 25

S

- security
 - for communication 5
- service catalog 39
- service graph
 - applying a template 49
 - creating 48
 - selecting for deployment 48
- service graphs
 - about 47
- service templates
 - creating custom 39
 - using 39
- services
 - customizing for tenants 39
- slots
 - assigning to guests 34
- software
 - installing for guests 34
- SSL Certificates and keys
 - managing 47
- standalone system
 - about upgrading 11
 - installing a hotfix 17
 - upgrading 11, 13
- system overview
 - for iWorkflow 5
- system provisioning
 - for vCMP feature 33
- system user
 - adding 23

T

- TCP port 22
 - using 5
- TCP port 443
 - using 5
- template
 - exporting for iApps 37
 - importing for iApps 38
- tenant
 - adding 51
- Tenant role
 - defined 24
- tenants
 - about creating 51
 - and creating users 51
 - associating with a user 52
 - creating services for 39
- terminology 55
- terms
 - defined 55
- time zone
 - and default for the iWorkflow system 9
 - changing for the iWorkflow system 9
 - specifying a DNS server for the iWorkflow system 9
- time zone default
 - for the iWorkflow system 9
- TMOS software
 - installing 34

U

- user groups
 - defined 23
- user roles
 - about 24
 - associating with users and user groups 24
 - removing 25
- users
 - adding 23, 51
 - and tenants 51
 - associating with a tenant role 52
 - defined 23
 - removing role from 25

V

- vCMP
 - creating a connector 33
- vCMP connectors
 - creating 33
- vCMP systems
 - provisioning 33
- version requirements
 - version 32
- virtual disks
 - creating 34
 - effect on disk space 34
- VLANs
 - configuring guest use of 34

