

F5[®] iWorkflow[™] : Administration

Version 2.3.0



Table of Contents

F5 iWorkflow Introduction.....	7
Overview: iWorkflow system.....	7
Additional resources and documentation for iWorkflow systems.....	7
About incorporating iWorkflow securely into your network.....	7
Open ports required for device management.....	7
Software Licensing and Initial Configuration.....	9
About software licensing and initial configuration.....	9
Automatic license activation.....	9
Manual license activation.....	9
Confirming the host connectivity options.....	10
Defining DNS and NTP servers for the iWorkflow system.....	11
Changing the default passwords.....	11
Upgrading iWorkflow.....	13
About upgrading iWorkflow.....	13
Upgrading a standalone system.....	13
About upgrading a standalone system.....	13
Upgrading a standalone system.....	13
Upgrading a cluster.....	15
Breaking a cluster.....	15
Upgrading a standalone system.....	15
Recreating a cluster.....	17
Installing a hotfix.....	19
About installing a hotfix.....	19
Breaking a cluster.....	19
Installing a hotfix on a standalone system.....	19
Recreating a cluster.....	21
Backing up and restoring iWorkflow.....	23
About backing up and restoring iWorkflow.....	23
About files names and locations.....	23
Backing up configuration data.....	23
Restoring configuration data.....	24
iWorkflow User Interface Basics.....	25
About the iWorkflow system user interface.....	25
Customizing panel order.....	25
Searching for specific objects.....	25
Users, User Groups, and Roles.....	27
Overview: Users, user groups, and roles.....	27
Changing the default password for the administrator user.....	27
Adding a locally-authenticated iWorkflow user.....	27
About user roles.....	28

Roles definitions.....	28
Associating a user or user group with a role	28
Disassociating a user from a role.....	29
Device Discovery.....	31
About device discovery and management.....	31
Adding BIG-IP devices to the iWorkflow inventory.....	31
Integrating with a vCMP Host.....	33
About vCMP integration.....	33
Network requirements for communication with vCMP hosts.....	33
Creating a vCMP connector.....	33
Creating a vCMP guest.....	34
Monitoring a vCMP guest.....	35
Creating a customized services template.....	35
Deleting a vCMP guest.....	36
License Management.....	39
Overview: Licensing options.....	39
About pool licenses.....	39
Automatically activating a pool license.....	39
Manually activating a pool license.....	39
BIG-IP Cloud Integration.....	41
What does a BIG-IP cloud connector do?.....	41
Adding BIG-IP devices to the iWorkflow inventory.....	41
Associating a BIG-IP cloud connector with a device.....	42
Cloud Tenant Management.....	43
About creating cloud tenants	43
Creating a tenant.....	43
Creating a cloud user.....	43
Associating a user with a tenant's role.....	44
Monitoring Services and Servers.....	45
About monitoring services and application servers.....	45
Monitoring services.....	45
Monitoring application servers.....	45
Viewing activity for cloud resources.....	46
Self-Service Application Deployment.....	47
About self-service application deployment	47
Tenant provisioning of L4-L7 services.....	47
iWorkflow High Availability.....	49
About setting up a high availability cluster	49
Configuring a high availability cluster.....	49
Glossary.....	51
iWorkflow terminology.....	51

Legal Notices.....	53
Legal notices.....	53

F5 iWorkflow Introduction

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.

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.

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.

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](https://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:

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.

- 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`.
- 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`.
- 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.

- 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`.
- 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.

1. Log in to the iWorkflow command line.
2. Run the command `tmsh` to access the `tmsh` utility.
3. 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.

4. 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`.
5. 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.

iWorkflow User Interface Basics

About the iWorkflow system user interface

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

Customizing panel order

You can customize the iWorkflow[®] system interface by reordering the panels.

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

Searching for specific objects

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

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

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.

Device Discovery

About device discovery and management

It takes a lot of time to manage multiple BIG-IP® devices. With F5® iWorkflow™, you save time by managing everything at once. This also helps reduce mistakes.

To manage BIG-IP devices, iWorkflow needs to be able to communicate with them. The discovery process creates the communication channel for device management.

After you discover devices, you can modify device configurations without having to log in to each device individually.

Adding BIG-IP devices to the iWorkflow inventory

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

The first step to managing BIG-IP devices is to add them to the iWorkflow system inventory.

***Important:** When you add a device, iWorkflow software installs packages on the device. This installation process can cause the traffic management interface (TMM) on the BIG-IP device to restart. Therefore, before adding a device, verify that no critical network traffic is targeted to the BIG-IP device.*

1. Log in to iWorkflow with your 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**.
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:** To add a device successfully, you must use the admin account; not the root account. If root access is needed, the system prompts you for it.*

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

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

7. If you are prompted to update the device framework, type the password for the root user in the **Root Password** field.

During the discovery process iWorkflow checks the version number of the software stack on the BIG-IP device—that is, the version number of the files necessary to support iWorkflow (such as iControl REST), not the BIG-IP device software version. iWorkflow automatically updates the software stack version when needed. For iWorkflow to discover and add BIG-IP devices, you need to enter an administrator user name and password for those BIG-IP devices. In rare cases the root password is also required to upgrade the REST management framework using SSH.

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

For devices located in a third-party cloud, you must associate the device with a cloud connector.

Integrating with a vCMP Host

About vCMP integration

You can integrate vCMP[®] hosts with the F5 iWorkflow[™] Networking connector. iWorkflow compatibility with BIG-IP[®] system releases is limited to explicit releases.

Note: For the most current list of compatible versions, refer to the F5 iWorkflow compatibility matrix (K11198324) at support.askf5.com.

Network requirements for communication with vCMP hosts

For proper communication, F5[®] iWorkflow[™] must have network access to the vCMP[®] host. Before you can manage cloud resources, you must define a network route between the iWorkflow device and the vCMP host network. This route can use either management or internal networks.

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

8. Click **Save**.

As part of the connection creation process, the iWorkflow system takes these actions:

- Verifies connectivity to the vCMP host.

- Displays any vCMP guests present on the vCMP host.

Important: Although existing guests are visible after you add the connector, you must discover them before you can use them.

Creating a vCMP guest

The following tasks must be complete before you can perform this task.

- Create a vCMP® connector.
- Install BIG-IP® software images on the vCMP host on which you plan to create guests.

You can specify a number of optional parameters when you create a guest. For the following optional parameters, you must know the capabilities of the vCMP host on which you plan to create the new guest:

- Hotfix level needed
- Number of cores per slot supported
- Names of existing VLANs

Creating a vCMP guest using the iWorkflow™ interface provides a straightforward method for managing your vCMP 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 Devices header, click the + icon, and then select **Create Virtual Device**.
The Create Virtual Device screen opens.
3. In the **Cloud** field, select the name of the vCMP connector you created previously.
4. In the **Device Image** field, select the version of BIG-IP software that you want the guest to use.
The software images that display (* .iso) are those that have been imported to the /shared/images folder on the vCMP host.

Tip: If you are going to specify a hot fix, this is not the place to do so. This field is only for the name of the base level installation file.

5. If you want the system to generate a password for you when it creates the guest, for **User Credentials**, you can select **Use "admin" and a random strong password**.
-

Important: Choose this setting to enable management authority of the guest by the iWorkflow device. Once this authority is established, you can only modify the guest from the iWorkflow.

6. For **Name**, type a unique name for the new guest.
Make a note of the name you choose for this guest. You will need this in the future.
7. If you want to specify a particular hotfix for the software version to install for this guest, type the name of the hotfix installation file in the **Device Hotfix** field.
Currently, the hotfix versions available for installation on the vCMP host are not suggested for you. Therefore, you must know which hotfixes are available for installation before you enter the name here.
8. If you want to specify a host name for this guest, type the name in the **Hostname** field.
9. If you want to specify the number of cores per slot that this guest occupies, type the number in the **Cores per Slot** field.
Currently, the number of cores per slot supported by the vCMP host is not suggested for you. Therefore, you must know the capabilities of the device on which the host is installed before you enter the number here.

Note: If you do not specify the number of cores, the system configures the minimum number of cores per slot that are supported by the platform on which your vCMP host resides.

10. If you want to specify the number of slots that this guest uses, type the number in the **Number of Slots** field.
11. For the **IP Address**, type the management IP address and mask that you want to assign to the new guest.
12. For the **Management Route**, type the subnet IP address for the gateway that you want to assign to access the guest.
13. Under VLAN List, specify the **Name** and **Local Address** for each VLAN that you want the guest to use.

You can check the BIG-IP device to determine which VLANs are available.

14. To start creating the guest that you just specified, click **Deploy**.
The Create Virtual Device screen closes.

The new guest name appears as a new entry in the Servers panel. As the creation and provisioning process progresses, the guest status displays on the properties panel for the new guest.

Additionally, when iWorkflow creates a new guest, it adds an entry to the Activities panel.

Monitoring a vCMP guest

A guest must have been discovered, or you must have added a vCMP[®] guest before you can monitor it.

You can monitor the health of the vCMP guests that exist on the vCMP host. Monitoring the health for vCMP guests provides you with the information you need to make resource management decisions.

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 Devices panel, click the gear icon next to the name of the guest that you want to monitor, and select **Properties**.
The panel expands to display the guest's properties.
3. To view the health statistics for the guest, click **Statistics**.
The current health status for the guest and host display as a decimal number between 0 and 1. (Where 1 indicates that the status is completely healthy.)

Creating a customized services template

Before you can customize a services template for a tenant, you must add a vCMP[®] connector.

An *iApp* is an application template located on F5 devices. An administrator can import iApps[®] templates to the iWorkflow[™] system.

With a services template, you can:

- Create custom catalog templates, based on iApps templates, that provide the network settings, levels of services, and so forth, that you expect to see in your vCMP environment.
- Modify the base template, choosing default values for selected parameters, and specifying which parameters the tenant can edit.

The values specified in the service templates you create are automatically exported to the vCMP guests.

Note: Until a tenant deploys an application that uses this service template, you can modify the options that define the settings for this template, but not the **Name**, **Application Type**, or **Application Tier Information**. Once an application deploys that uses this template, you can no longer modify settings for

that template. For options that you set to **Tenant Editable**, the values you specify just determine the default values.

Important: If you make modifications to an iApps template, you need to import it with a new version number in its name.

1. In the iWorkflow system, hover over the Service Templates header and click the + icon when it appears.
The New Template screen opens.
 2. In the **Name** field, type a name for this new template.
 3. For the **Input Parameters**, select the option that displays the parameters you want to work with.
The setting you choose here determines which parameters from the base template that you select display in subsequent fields and areas on the screen.
 - Select **All Options** to configure the Application Tier Information section. You can view all of the parameters for the template you select and then expand individual template sections, or click **Expand All** to view every parameter in every section.
 - Select **Common Options** if you only want to edit a subset of the template parameters. This option displays parameters that are:
 - Marked as tenant-editable.
 - Specified in the Application Tier Information section.
-

Important: If you are creating an L4-L7 service template based directly off on an iApps template, select **All Options**, and in the Application Tier Information section, set the required fields. The Application Tier Information section provides iWorkflow with information about the contents of the template for a given server tier, including the Virtual Server IP, Virtual Server Port, Pool Member IP, Pool Member Port, SSL/TLS Public Key, and SSL/TLS Private Key. If you are creating an L4-L7 service template based off of an existing service template, to accept the existing application tier information values and other defaults without having to view the complete set of options, select **Accept Defaults** or **Common Options**.

4. For the **Cloud Connector** select the vCMP connector you created earlier.
 5. From the **Application Type** list, select the base template that contains the parameters that provide the network settings and levels of services that you want to have available in your vCMP environment.
The screen displays sections specific to the template you selected.
 6. Expand sections as necessary, and then specify parameter values as needed. (You can provide default values in that column, and select which parameters the user can revise.)
-

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

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

7. Click the **Save** button.

You can now use this connector with your vCMP integration.

Deleting a vCMP guest

If you no longer need one of the guests on the vCMP® host, you can delete it.

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 Devices panel, click the gear icon next to the name of the guest that you want to delete, and click **Properties**.
The panel expands to display the guest's properties.
3. At the top of the properties panel, click **Delete**.
A Delete device confirmation popup screen opens.

Important: Make sure you no longer need this guest before confirming; you cannot recover a deleted guest.

4. Click **Delete** to permanently remove the guest from the vCMP host.

The guest is deleted from the vCMP host.

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.

BIG-IP Cloud Integration

What does a BIG-IP cloud connector do?

The BIG-IP® connector is the interface between F5® iWorkflow™ and your private cloud infrastructure. Using this interface, iWorkflow manages the BIG-IP® devices in your private cloud, and deploys and manages applications to the BIG-IP devices in that cloud. The local connector performs the same function as connectors for cloud-specific infrastructures, but it does not include the specific parameters that those vendor clouds require.

A *cloud connector* provides two services:

- First, it describes a set of devices in a network.
- Second, it provides integration with a private cloud infrastructure.

Adding BIG-IP devices to the iWorkflow inventory

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

The first step to managing BIG-IP devices is to add them to the iWorkflow system inventory.

Important: When you add a device, iWorkflow software installs packages on the device. This installation process can cause the traffic management interface (TMM) on the BIG-IP device to restart. Therefore, before adding a device, verify that no critical network traffic is targeted to the BIG-IP device.

1. Log in to iWorkflow with your 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**.
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: To add a device successfully, you must use the admin account; not the root account. If root access is needed, the system prompts you for it.

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

6. Click **Save** to start the task.
7. If you are prompted to update the device framework, type the password for the root user in the **Root Password** field.

During the discovery process iWorkflow checks the version number of the software stack on the BIG-IP device—that is, the version number of the files necessary to support iWorkflow (such as iControl REST), not the BIG-IP device software version. iWorkflow automatically updates the software stack version when needed. For iWorkflow to discover and add BIG-IP devices, you need to enter an administrator user name and password for those BIG-IP devices. In rare cases the root password is also required to upgrade the REST management framework using SSH.

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

For devices located in a third-party cloud, you must associate the device with a cloud connector.

Associating a BIG-IP cloud connector with a device

Before you associate a BIG-IP[®] cloud connector with a device, you must discover one or more devices.

To enable integration between a third-party cloud provider and iWorkflow[™], you must configure a BIG-IP cloud connector. A *BIG-IP 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.

1. Log in to iWorkflow with your administrator user name and password.
2. Select the **Clouds and Services** component.
3. On the Clouds header click the + icon.
The **New Cloud** screen opens.
4. 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.
5. From the **Connector Type** list, select **BIG-IP**.
6. From the **Devices** list, select the device you want to associate with this connector.
7. To select additional devices to associate with this connector, click the + icon at the right of the list. iWorkflow system discovers application servers associated with this connector, and populates them in the Servers panel. If the system discovers F5 devices, it populates the Devices panel with them.
8. If you use multiple networks within the cloud or if you use BIG-IP devices to support multi-tenancy, select **enable support for multiple networks**.
9. Click **Save**.

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.

Important: *Authentication providers should note that all user roles are managed by iWorkflow and not by external authentication providers.*

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 **Add**.

You can now associate this user with an existing tenant to provide access to predefined 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.

Monitoring Services and Servers

About monitoring services and application servers

As a tenant, you can use iWorkflow™ to monitor the health statistics and performance of applications and servers. In addition to the application itself, the health of an application is influenced by its associated objects, including:

- Application server nodes
- Virtual servers that optimize application traffic
- Clouds

Monitoring services

Before you can monitor a service, you must first deploy it.

Monitoring statistics and performance details for services and associated network objects provides you with the information you need to make resource management decisions. The statistics for services are collected by the managed BIG-IP® device and include various network statistics, such as connections, bits per second, and so forth. The performance data displays the services performance trend over a period of time.

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 L4-L7 Services header, click the gear icon next to the name of the services that you want to monitor.
The panel expands to display the properties of the services.
3. To view the statistics, click **Statistics**.
The statistics display and all of the associated objects for the services are highlighted in the applicable panels.

Monitoring application servers

A cloud provider must have discovered, or you must have added, an application server before you can monitor it.

Monitoring health and performance statistics for your application servers provides you useful information about the health and usage for your resources. This information helps you decide when to increase or decrease resources to support your application requirements.

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 Nodes panel, click the gear icon next to the name of the application server that you want to monitor.
The panel expands to display the application monitor's properties.
3. To view the statistics, click **Statistics**.
The statistics display and all of the associated objects for that application are highlighted in the applicable panels.

Viewing activity for cloud resources

Viewing activity for dynamic cloud resources gives you insight into how cloud resources are expanding to address increased traffic to applications.

To view specific activity details, place your cursor on an activity.

A popup window opens to display further details about the selected activity.

Self-Service Application Deployment

About self-service application deployment

Cloud service providers customize iApps[®] application templates based on your needs as a cloud tenant. For example, they specify such things as an IP address for a virtual server, identify hosts and server pools, set connection limits, and so forth. This customization eliminates the need for you to perform complicated networking tasks, and ensures that your settings are optimized for your resources. When these customized applications are associated with you as a tenant, you have the option to further modify the application parameters that your administrator has defined as tenant editable, and deploy them as needed.

Tenant provisioning of L4-L7 services

Before you can deploy an application-oriented L4-L7 service, your cloud service provider must add you as a user and a tenant, and associate you with at least one cloud connector.

When a cloud administrator adds you as a cloud tenant user, he determines which resources are available to you. These resources are provided by associating customized application templates with your account. Part of that customization task is to define the application parameters you can edit. As a cloud tenant user, you can customize these application templates and deploy them as needed.

1. Log in to iWorkflow[™] with the user name and password for the account provisioned for you by the Administrator.
2. At the top of the screen, click **Clouds and Services** and then, on the L4-L7 Services header, click the + icon.
3. In the **Name** field, type a name for this new application.
4. From the **Service Template** list, select an application.
5. From the **Cloud** list, select the cloud connector associated with the resource on which you want to deploy your application.

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.
6. To define a new SSL certificate and private key for this application, for the **SSL Certificate Options**, paste the PEM (CRT or CER) text representation of the certificate and private key.

The SSL certificate and private key must be unbundled Base64 encoded ASCII text with PEM header and footer.

This option is not available for all applications.
7. Alternatively, select the **Use Existing** option to use a SSL certificate and private key already stored on the device.
8. You can further customize this application by specifying an IP address for the virtual server and adding pool hosts.

If your cloud service provider assigned IP addresses for the **Servers**, **Pool Hosts**, and **Pool Members** for this application, the addresses display. If these addresses were specified as not editable, you cannot change them.
9. When you are finished, click the **Save** button located at the top of the New L4-L7 Service panel.

Self-Service Application Deployment

You can now use this new application, and any application server associated with this new application displays in the Nodes panel.

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-0611-04

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

Legal Notices

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 [49](#)
 - configuring for the iWorkflow system [49](#)
- activities
 - viewing for cloud resource activity [46](#)
- Activity entry
 - from guest creation [34](#)
- admin, *See* administrator
- Administrator role
 - defined [28](#)
- administrator user
 - changing password for [11, 27](#)
- administrator user password
 - changing [11, 27](#)
- application catalogs
 - about deploying [47](#)
- application servers
 - about monitoring health and performance [45](#)
- application services
 - about deploying [47](#)
- application templates
 - creating custom [35](#)
 - defined [51](#)
 - deploying as a Cloud Tenant user [47](#)
- application traffic
 - monitoring [45](#)
- applications
 - about monitoring health and performance [45](#)
 - customizing for tenants [35](#)
 - deploying [47](#)
 - deploying as a Cloud Tenant user [47](#)
- authorization checks
 - for secure communication [7](#)

B

- base registration key
 - about [9, 10](#)

C

- catalog
 - for applications [35](#)
- cloud administrator
 - defined [51](#)
- cloud bursting
 - defined [51](#)
- cloud connectors
 - defined [41, 42, 51](#)
- cloud connectors, local
 - associating with a device [42](#)
- cloud resources
 - providing for tenants [43](#)
- cloud tenants
 - about creating [43](#)
 - adding [43](#)

- cluster
 - breaking [15, 19](#)
 - recreating [17, 21](#)
- clusters
 - for high availability [49](#)
- communication
 - between iWorkflow and managed devices [7](#)
- configuration
 - and initial setup [9, 10](#)
- configuration data
 - backing up [23](#)
 - restoring [24](#)
- connectors, local
 - associating with a device [42](#)

D

- device discovery
 - by scanning network [31, 41](#)
- device inventory
 - about [31](#)
- device management
 - about [31](#)
- devices
 - about discovering [31](#)
 - adding [31, 41](#)
 - associating with a cloud connector [42](#)
- discovery address
 - defined [9](#)
- DNS server
 - specifying for the iWorkflow system [11](#)
- documentation, finding [7](#)
- dossier
 - providing [9, 10](#)
- dynamic cloud resources
 - viewing activity for [46](#)

E

- elasticity
 - viewing activity for [46](#)

F

- failover [49](#)

G

- glossary [51](#)
- guests
 - creating for vCMP [34](#)
 - deleting for vCMP [36](#)
 - monitoring for vCMP [35](#)
- guides, finding [7](#)

H

- health statistics
 - monitoring 45
- high availability
 - configuring 49
- high availability configuration
 - about 49
- hotfix
 - installing 19
- HTTPS port 443
 - required for communication 7

I

- initial configuration
 - for iWorkflow system 9
- IP addresses
 - for managed devices 31
- iWorkflow
 - about 7
 - defined 51
- iWorkflow system
 - about activating 9
 - about backing up 23
 - about file names 23
 - about licensing 9
 - about locations 23
 - about restoring 23
 - about upgrading 13
 - reordering panels 25
- iWorkflow Tenant users
 - deploying applications 47

L

- license
 - activating automatically 9
 - activating manually 9, 10
 - manually activate a pool license 39
- license activation
 - for iWorkflow system 9, 10
- licenses
 - about managing for devices 39
 - about pool licenses 39
- licensing
 - activating pool license automatically 39
 - activating pool license manually 39
 - for managed devices 39
 - for pool license 39
- local cloud connectors
 - about 41
 - associating with a device 42
- local connectors
 - defined 41

M

- managed devices
 - about discovering 31
- manual activation
 - for pool license 39

- manuals, finding 7
- monitoring health and performance 45

N

- network
 - incorporating iWorkflow systems 9
- network configuration
 - and requirements for using vCMP 33
- network configurationsiApps
 - customizing for tenants 35
- network security
 - about 7
- new connectors
 - adding a vCMP 33

O

- objects
 - searching for 25
- OpenStack application servers
 - monitoring traffic 45

P

- Pacific Standard Time zone
 - as default for the iWorkflow system 11
- panels
 - reordering 25
- password
 - changing for administrator user 11, 27
- peer leader
 - defined 51
- performance
 - for application servers 45
 - viewing for services 45
- pool license
 - activating automatically 39
 - activating manually 39
- pool licenses
 - about 39
- port 22
 - using 7
- port 443
 - required for communication 7
 - using 7
- ports
 - required for communication with iWorkflow 7
 - required open 7
- privileges
 - removing from users 29
- PST zone, *See* Pacific Standard Time zone

R

- release notes, finding 7
- resources
 - defined 51
 - providing access for user 44
- roles
 - associating with users and user groups 28

- roles (*continued*)
 - defined 27
 - for users 27, 28
 - removing from a user 29

S

- search function
 - finding specific objects 25
- security
 - for communication 7
- self-service application deployment 47
- server health
 - for OpenStack 45
- servers 45
- services
 - viewing statistics for 45
- standalone system
 - about upgrading 13
 - installing a hotfix 19
 - upgrading 13, 15
- statistics
 - about 45
 - for application server traffic 45
 - viewing for services 45
- system user
 - adding 27

T

- TCP port 22
 - using 7
- TCP port 443
 - using 7
- tenant
 - adding 43
- Tenant role
 - defined 28
- tenants
 - about creating 43
 - and creating users 43
 - associating with a user 44
 - creating applications for 35
- terminology 51
- terms
 - defined 51
- time zone
 - and default for the iWorkflow system 11
 - changing for the iWorkflow system 11
 - specifying a DNS server for the iWorkflow system 11
- time zone default
 - for the iWorkflow system 11

U

- user groups
 - defined 27
- user interface
 - and searching for specific objects 25
 - customizing 25
 - navigating 25
- user roles

- user roles (*continued*)
 - about 28
 - associating with users and user groups 28
 - removing 29

users

- adding 27, 43
- and tenants 43
- associating with a tenant role 44
- defined 27
- removing role from 29

V

- vCMP
 - about integration 33
 - and network configuration requirements 33
 - creating a connector 33
 - creating a guest 34
 - deleting a guest 36
 - monitoring a guest 35
- vCMP connectors
 - creating 33
- vCMP guests
 - creating 34
 - deleting 36
 - monitoring 35

