F5® iWorkflow™: VMware NSX Administration

Version 2.2.0

Table of Contents

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.

Confirming the host connectivity options
Defining DNS and NTP servers for the iWorkflow system
Changing the default passwords

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.

4. 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`.
5. 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`.
6. 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`.
7. 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.

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: • 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: • customizing and deploying application templates • monitoring the health statistics and performance of applications and servers ***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* `headquarters-user`*, produces a new role named* `headquarters-user (Cloud Tenant)`.

Associating a user or user group with a role

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

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

1. Log in to 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.

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.

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.

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 VMware NSX

Network requirements for communication with VMware cloud services

For proper communication, iWorkflow™ must have network access to the resources on which VMware software is installed. Before you can manage cloud resources, you must define a network route between the iWorkflow device's VLAN and the management VLAN on the VMware.

Discovering devices located in the VMware cloud

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.

You must know the IP address that the iWorkflow device will use to access the BIG-IP device.

Discover a device by providing the iWorkflow™ system with the device's IP address, user name, and password.

1. Log in to iWorkflow™ with the administrator user name and password.
2. On the Devices header, click the + icon, and then select **New Device**.
   The Devices panel expands to show the New Device screen.
3. In the **IP Address** field, type the device's IP address.

   The preferred address for discovering a BIG-IP device is its management IP address.
4. If the iWorkflow system and the BIG-IP device are on different subnets, then you need to specify an IP route between them.
   - If the iWorkflow device and the BIG-IP device communicate using the management IP address, then use SSH to issue a `route` command.
     1. Use SSH to log in to the iWorkflow system's management IP address as the root user.
     2. Type the following command: `route <route name> {gw <x.x.x.x> network default}`
   - If the iWorkflow device and the BIG-IP device use something other than the management IP address to communicate, then use SSH to issue a `tmsh route` command.
     1. Use SSH to log in to the iWorkflow system's management IP address as the root user.
     2. Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

     Note: *Where* `<route name>` *is a user-provided name to identify the new route, and* `<x.x.x.x>` *is the IP address of the default gateway for the internal network.*

     ---
5. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.

6. For the **Auto Update Framework** setting, select the **Update Automatically** check box to direct the iWorkflow system to perform any required REST framework updates on the BIG-IP device.

   For the iWorkflow system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework.
7. Click the **Add** button.

The iWorkflow system populates the properties of the device that you added, and displays the device in the Devices panel and its configuration files display in the Configuration panel.

To complete discovery of BIG-IP® devices and populate the Devices panel, provide the administrator user name and password when requested. You can then associate tenants with this resource.

About configuring the iWorkflow device for a VMware integration

The iWorkflow ™device facilitates the integration between the VMware NSX and the BIG-IP® device or device cluster. The work flow for configuring this integration takes you back and forth between the two participants in this integration.

You can either integrate with a standalone BIG-IP virtual machine, or with a high availability (HA) cluster of BIG-IP virtual machines. The process for setting up the two configurations is nearly identical. Optional steps and settings to enable HA are noted where applicable.

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

Note: *The maximum HA cluster size this iWorkflow release supports is two BIG-IP devices.*

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

Task summary

Prepare the iWorkflow devices for NSX integration
Prepare VMware NSX for integration
Prepare the new BIG-IP devices for integration
Complete the NSX integration

Prepare the iWorkflow devices for NSX integration

To begin the process of preparing the iWorkflow™ device for integration, you set up one or more iWorkflow devices, create an NSX call back user, and an NSX connector, and then create a new server image.

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 synching 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 synching 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.

About activating a pool license

When you integrate with VMware NSX to create BIG-IP® VE virtual machines, you must activate a pool license to license the BIG-IP virtual machines that that iWorkflow™ software creates using the VMware NSX connector.

You can choose not to use a pool license and skip to discovering devices. If you make this choice, the iWorkflow device still creates BIG-IP VE systems, but you need to license them before they can be used.

You initiate the license activation process with a base registration key. The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license. If the system has access to the internet, you select an option to automatically contact the F5 license server and activate the license. If the system is not connected to the internet, you must manually retrieve the activation key from a system that is connected to the internet, and then transfer it to the iWorkflow system.

Note: *If you do not have a base registration key, contact your F5 Networks sales representative.*

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.

Creating an NSX callback user

You need to create a user credential that the iWorkflow™ system can use to communicate with the VMware NSX system.

1. Log in to iWorkflow™ with the administrator user name and password.

2. On the User header, and click the + icon.
   The New User screen opens, displaying property fields for the new user.
3. In the **Username** field, type the name of the user account that VMware NSX will use when it interacts with the iWorkflow system.

   The entry can contain a combination of letters, numbers, periods, and hyphens.

   Note: *You need to recall this name when you configure the NSX.*
4. From the **Auth Provider** list, select **Local**.
5. In the **Full Name** field, type a (human friendly) name to identify the NSX account.

   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 callback user account.
7. Click the **Add** button.

Creating a connection between iWorkflow and NSX Manager

To enable integration between a third-party cloud provider and 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 required by third-party cloud providers.

For VMware NSX, iWorkflow also helps you manage VMware NSX load-balancing service insertion to BIG-IP® machines. Management tasks include discovering, creating, starting, and stopping VMware NSX application servers running in the private cloud. You can use this feature to accommodate seasonal traffic fluctuations by periodically adding and retracting devices and application servers as needed. Additionally, you can also provide tenants access to self-deployable iApps® through VMware integration.

Note: *Only one VMware NSX connector is supported per VMware NSX environment. For information about the compatibility of iWorkflow with VMware NSX releases, see K11198324: F5 iWorkflow compatibility matrix at* `support.f5.com`.

1. Log in to iWorkflow™ with the administrator user name and password.
2. On the Clouds header, and 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.

   Important: *You will need to recall the name you assign to this connector so that you can select it when you are configuring the VMware user interface. The name you specify is used as the service definition name in the VMware user interface.*
4. From the **Cloud Provider** list, select **VMware NSX**.
   The screen displays additional settings specific to VMware NSX.
5. In the **VMware NSX Address** field, type the IP address of the NSX server.

   The VMware IP address must be fully accessible from the iWorkflow device.
6. For the **VMware NSX 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 **VMware NSX User Name** and **VMware NSX Password** fields, type the credentials that the iWorkflow device will use to authenticate to the NSX Manager.
8. In the **VMware vCenter Server Address** field, type the IP address of the vCenter server.
9. In the **VMware vCenter Server User Name** and **VMware vCenter Server Password** fields, type the credentials that the iWorkflow device will use to authenticate to vCenter.
10. In the Device Provisioning area, from the **Time Zone** list, select your local time zone.
11. In the **NTP Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.
12. In the **DNS Servers** field, type the IP address of your DNS server.
13. In the **DNS Suffix(s)** 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.
14. In the Callback Settings area, from the **iWorkflow Callback User Name** list, select the user name that NSX Manager uses to authenticate to the iWorkflow system.

    Note: *Select the user name you specified when you created an NSX callback user.*
15. In the **iWorkflow Callback Password** field, type the password that NSX Manager uses to authenticate to the iWorkflow REST system.

    Note: *Specify the password you used when you created an NSX callback user.*
16. From the **iWorkflow Callback Address** list, select the IP address that this NSX Manager uses to access each iWorkflow device in the HA cluster.

    By default, the management IP address is used, but you can specify a self IP address if you choose.
17. From the **Licensing** list, select the name of the license pool that you created for the NSX integration.
18. Click the **Save** button.

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

- Creates a new default tenant for the new connector.
- Verifies connectivity to the NSX Manager and vCenter APIs, and registers the iWorkflow system as an NSX Partner Service provider.
- Creates a callback user role that enables NSX to access the iWorkflow software resources necessary for interaction with the iWorkflow REST API.

Creating a new server image

Before you create a new server image, you must know the accessible location of an F5 BIG-IP ®VE installation file. The accessible location must be either an HTTP URL, or a VCenter datastore. These installation files use the `.ovf` file extension.

When VMware NSX creates a new server as part of the iWorkflow™ and VMware NSX integration, it uses the server image file you specify as the template.

1. In the iWorkflow system Clouds panel, hover over the connector you created previously, click the gear icon (), and then select **Properties**.
   The properties screen for that connector opens.
2. Scroll down to Server Images, and click **New**.
   The New Server Image screen opens.
3. In the **Machine Image Name** field, type a name for the server image.

   It is helpful if the image name identifies the version of the BIG-IP software you are using.
4. In the **OVF URL** field, specify the accessible location of an F5 BIG-IP VE installation file.
5. Click the **Save** button.

   This saves the settings for the new device image.

6. Click the **Save** button.

   This saves the settings for the connector.

Prepare VMware NSX for integration

After you finish preparing the iWorkflow™ device for integration, there are a couple of tasks to perform in the VMware NSX environment to complete the integration. You need to create an NSX Edge Service Gateway and enable a load balancing service for it.

Creating an NSX Edge Services Gateway

The NSX Edge Service Gateway establishes the network within which network services such as firewall, NAT, and load balancing are deployed. To integrate a BIG-IP® device with NSX, you must create at least one Edge Service Gateway.

Important: *You perform the following task using the vSphere Web Client user interface. At time of release, these steps accurately describe the VMware user interface. For the most current instructions for performing these steps, refer to the VMware web site* `http://pubs.vmware.com/`.

In the vSphere web client user interface, create a new NSX Edge.

Important: *When you are configuring the Edge Services Gateway, make sure to observe the following:*

- Choose to create the gateway in undeployed mode.
- For Tenant, enter a tenant ID
  - iWorkflow uses an existing iWorkflow tenant name matching your tenant ID. If no matching tenant exists
  - iWorkflow creates a new tenant from this ID.
  - If you do not enter a tenant ID, NSX Edge and iWorkflow use an existing default tenant created when you created the NSX cloud connector.
- If you are configuring an HA cluster of BIG-IP virtual machines, select **Enable High Availability**, otherwise leave it cleared.
- Choose the **X-Large** Appliance size.
- Make sure that the NSX Edge you create identifies the Cluster/Resource Pool and the Datastore, but does not identify any interfaces. Otherwise, follow your standard practice for NSX Edge creation.

When you finish editing an Edge, it appears in the list under NSX Edges.

Enabling a service for the Edge

You must provision IP pools and port groups before you enable an Edge load balancer.

If you are configuring an HA cluster of BIG-IP® virtual machines for two-arm deployments, you need to configure four vNICs (1 for management, 2 for data, and 1 for HA). For one-arm deployments, you need three vNICs (management, data, and HA). If you are not using HA, you can use one less vNIC in each case.

The NSX Edge Service Gateway establishes the network within which network services such as firewall, NAT, and load balancing are deployed. To integrate a BIG-IP® device with NSX, you must create at least one Edge Service Gateway.

Important: *You perform the following step using the vSphere Web Client user interface. At time of release, these steps accurately describe the VMware user interface. For the most current instructions for performing these steps, refer to the VMware web site* `http://pubs.vmware.com/`.

1. In the vSphere web client user interface, select the NSX Edge you just created.
2. On the **Manage** tab for the selected Edge, select the **Load Balancer** tab and click **Edit**.
   The Edit Load balancer global configuration screen opens.
3. Select **Enable Load Balancer** and **Enable Service Insertion**.
   Additional options are enabled, so that you can specify additional details.
4. For the **Service Definition**, select the iWorkflow connector that you created previously.
5. For the **Service Configuration**, select **F5 ADC-Provision dedicated BIG-IP VE(s)**.
6. For the Deployment Specification, select the BIG-IP system server image you created previously.
7. Specify the configuration details for the Runtime NICs that you expect NSX to use as load balancers.

   Note: *The connectivity types you specify depend on whether you are configuring an HA cluster. For HA, you configure 1 management vNIC, 1 HA vNIC, and 1 or 2 data vNICs. For standalone, you configure 1 management vNIC and 1 - 3 data vNICs.*

   a) Configure **vnic0**.
      - For the **Connected To** setting, use the management port group you created as a prerequisite.
      - For **Connectivity type**, use **Management**.
      - For the **Primary IP Allocation Mode**, use **IP Pool**.
      - For the **IP Pool**, use the management pool you created as a prerequisite.

   b) Configure **vnic1**.
      - For the **Connected To** setting, use the external port group you created as a prerequisite.
      - For **Connectivity type**, use **Data**.
      - For the **Primary IP Allocation Mode**, use **IP Pool**.
      - For the **IP Pool**, use the external pool you created as a prerequisite.

   c) Configure **vnic2**.
      - For the **Connected To**, use the internal port group you created as a prerequisite.
      - For the **Connectivity type**, use **Data**.
      - For the **Primary IP Allocation Mode**, use **IP Pool**.
      - For the **IP Pool**, use the internal pool you created as a prerequisite.

   d) Configure **vnic3**.
      - For the **Connected To** setting, use the HA port group you created as a prerequisite.
      - For **Connectivity type**, use **HA** if you are configuring an HA cluster of BIG-IP virtual machines, otherwise use **Data**.
      - For the **Primary IP Allocation Mode**, use **IP Pool**.
      - For the **IP Pool**, use the HA pool you created as a prerequisite.
8. On the Edit Load balancer global configuration screen, select the **Typed Attributes** tab.
9. For the **Fully qualified host name of BIG-IP VE?** value, type a host name for the BIG-IP VEs that the NSX Edge will create.

The NSX Edge creates two new runtimes. These runtimes create BIG-IP virtual machines based on the specifications you provided. These virtual machines will be managed by the iWorkflow™ as an HA Cluster.

When iWorkflow discovers the virtual machines, it adds an entry for each BIG-IP virtual machine to the iWorkflow user interface in the Activities panel under Clouds and Services.

Prepare the new BIG-IP devices for integration

After the VMware NSX integration adds the BIG-IP® virtual edition instances into the high availability cluster, there are a couple of tasks to perform on the BIG-IP device environment to complete the integration. If the devices are configured in an HA cluster, you only perform these tasks on one device, after which the configuration is replicated on the other cluster members using Config sync.

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, to integrate a BIG-IP® device with NSX, you must create at least one Edge Service Gateway.

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. A best practice is 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 iApps 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 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 the earliest version of BIG-IP software that is supported for deployment with the iApps Template.
7. Optional: In the **Maximum Supported BIG-IP Version** field, type the latest version of BIG-IP software that is 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 the application template for the NSX integration, you must upload the template to the managed device, and then wait for it to be exported to the managing iWorkflow™ device.

You customize an iApps® Template, specifying which parameters to display, and which are tenant-editable. Once deployed, these parameters are available in the NSX user interface.

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 in 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.
6. Optional: From the **Inherited Values** list, select an existing Service Template to inherit all the settings that have been configured.
7. In the **Name** field, type a name for a new L4-L7 Service template.
8. From the **Cloud Availability** list, select the name of the cloud template previously created.
9. For the **Displayed Parameters** setting, select **All** to view all of the parameters for the template you select.
10. 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`
11. 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 VMware NSX tries to set variable names that are not defined in the Service Template.*

    ---

12. 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 NSX integration.

Complete the NSX integration

After you finish preparing the BIG-IP® devices for integration, there are a couple of tasks to perform in the BIG-IP device environment to complete the integration. Because the devices are configured in an HA cluster, you only perform these tasks on one device, after which the configuration is replicated on the other cluster members using Config sync.

Configuring a pool of virtual machines to handle data plane traffic

Before you can create a pool of virtual machines, you must allow NSX integration to create the virtual machines. You also must create and configure the web servers for which the virtual machines will manage traffic.

The web server pool services the data plane traffic generated by your applications.

Use the VMware NSX user interface to create a web server pool.

Populate the pool using the previously created web servers.

Note: *This task is performed entirely within the VMware NSX user interface. Refer to the appropriate VMware documentation for details on how to create a web server pool.*

Configuring the NSX virtual server

The virtual server you create here resides on the BIG-IP® virtual machine created by the NSX integration.

1. Log in to vSphere Web Client with your administrator username and password.

   Note: *This task is performed entirely within the VMware NSX user interface. Refer to the appropriate VMware documentation for details on how to create a web server pool.*

2. In the Navigator, click **Networking & Security**.
3. In the Navigator, click **NSX Edges**.
4. Double-click the name of the NSX Edge for which you defined a server pool previously.
5. Click the Manage tab, then click the Load Balancer tab, then click **Virtual Servers**.
6. On the New Virtual Server General tab, from the **Application Profile** list, choose the name of the custom application template you created on the iWorkflow system.

   The settings that can be specified on the Advanced tab are now determined by the parameters marked Tenant Editable in the application template.
7. For the **IP Address**, click **IP Pool**, and then select the external pool you created earlier to handle data plane traffic.
8. In the **Name** field, specify a name to identify this virtual server.
9. From the **Default Pool** list, select the just-created web server pool.
10. If you want to revise any of the tenant editable values, click the **Advanced** tab and make your changes.
11. Click **OK** to finish creating the new virtual server
    VMware NSX creates the new server.

The new server status is indicated by the Service Profile Status. If the status is other than `In Service`, you can get more information under Detailed Status, or even more information by viewing the new server on the iWorkflow™ device.

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.

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
service templates	An application template is a collection of parameters (in the form of F5 iApps® templates) that a cloud administrator defines to create a customized configuration for tenants. Cloud administrators add the configured application to a catalog from which a tenant can self-deploy it.
iWorkflow	The iWorkflow™ system streamlines management and access for tenants to services and applications hosted by local and/or cloud-based servers.
cloud administrator	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.
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.
peer leader	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.
resources	A resource is any managed object, including devices, web applications, virtual servers, servers, cloud connectors, and so forth.
roles	A role defines specific privileges to which you can associate one or more users. There are two default roles for iWorkflow: cloud administrator and cloud tenant.
tenant	A tenant is an entity that can consist of one or more users accessing resources provided by a cloud administrator.
user	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 May 25, 2017.

Publication Number

MAN-0609-05

Copyright

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

L

M

N

P

R

S

T

U

V