



Installing Cisco ICFPP on VMware

- [Cisco ICFPP Software, page 1](#)
- [Workflow for VMware Environments, page 2](#)
- [Installing Cisco ICFPP on VMware, page 2](#)
- [Post-Installation Task for VMware Environments, page 4](#)
- [Upgrading Cisco ICFPP, page 5](#)

Cisco ICFPP Software

The Cisco ICFPP software is available for download from [Cisco.com](https://www.cisco.com). For assistance, contact your Cisco representative.

The Cisco ICFPP software package (`ICFP-dk9-2.2.1-pkg.zip`), contains the following files:

File	Description
<code>icfpp-2.2.1.ova</code>	Cisco ICFPP OVA file. Use this file to install Cisco ICFPP in VMware environments. See Workflow for VMware Environments, on page 2 .
<code>icfpp-2.2.1.qcow2</code>	Cisco ICFPP QCOW2 file. Use this file to install Cisco ICFPP in OpenStack environments. See Workflow for OpenStack Environments .
README	README file. This file contains information about installing and using Cisco ICFPP.

The Cisco ICFPP software includes an evaluation license with support for 20 VMs. To view the license details in the GUI after you install Cisco ICFPP, choose **Administration** > **License**, and expand the entry in the **License Keys** table.

Workflow for VMware Environments

Cisco ICFPP should be implemented by all service providers that interface with Cisco Secure Cloud Extension. The only exceptions to this are Amazon EC2 and Windows Azure, which are available to Cisco Intercloud Fabric through their native public cloud APIs.

The high-level tasks involved in deploying Cisco ICFPP in a VMware environment are:

- 1 Confirm that you have met the installation requirements—See [Installation Requirements](#).
- 2 Gather the required information—See [Information Required for Configuration and Installation](#).
- 3 Install Cisco ICFPP—See [Installing Cisco ICFPP on VMware](#), on page 2.
- 4 Perform post-installation tasks—See [Post-Installation Task for VMware Environments](#), on page 4.
- 5 (Optional) Configure Cisco ICFPP virtual appliances for a multiple-node cluster—See [Configuring Multiple-Node Clusters](#).
- 6 Configure communications with Cisco Intercloud Fabric Director—See the *Cisco Intercloud Fabric Getting Started Guide*.

Installing Cisco ICFPP on VMware

This procedure describes how to install Cisco ICFPP in a VMware environment.

We recommend that you configure an NFS server for all Cisco ICFPP nodes. If NFS is not configured, all VM images that are uploaded from Cisco Intercloud Fabric Director are stored on the local disk. If NFS is not configured and a node fails, any images stored on that node will not be available and could cause template creation and VM migration to fail if the node is part of a cluster.

Before You Begin

- Set your keyboard to United States English.
- Unzip the Cisco ICFPP software package to obtain the OVA file and the README file.
- Copy the Cisco ICFPP OVA image to a location that is available from the VMware vSphere Client.
- Make sure that all requirements are met as specified in [System Requirements](#).
- Collect the information required for the installation. See [Information Required for Configuration and Installation](#).
- Review the README file for information related to Cisco ICFPP installation and operation.

Procedure

-
- Step 1** Using the **VMware vSphere Client**, log in to the vCenter server.
 - Step 2** Choose the host on which to deploy the Cisco ICFPP virtual appliance.
 - Step 3** Choose **File > Deploy OVF Template**.
 - Step 4** In the wizard, provide the information as described in the following table:

Screen	Action
Source	Choose the Cisco ICFPP OVA using one of the following methods: <ul style="list-style-type: none"> • Browse to the location, choose the file, and click Open. • Deploy from a URL on your local area network. Replace <i>FQDN</i> with the IP address or the fully qualified domain name, and click Next.
OVF Template Details	Verify the details.
End User License Agreement	Read the agreement and click Accept .
Name and Location	<ol style="list-style-type: none"> 1 Enter a name for the virtual appliance. 2 Choose the VMware data center or host where Cisco ICFPP will reside.
Deployment Configuration	Choose the type of deployment: <ul style="list-style-type: none"> • Standalone—Used for single-node deployments. • Primary Node—Used for HA deployment in a multiple-node cluster. • Service Node—Used in cluster deployments for handling requests.
Storage	Choose the location in which to store the Cisco ICFPP files.
Disk Format	Choose the required format for the virtual appliance disks: <ul style="list-style-type: none"> • Thick Provision Lazy Zeroed—Allocates storage immediately in thick format. • Thick Provision Eager Zeroed—Allocates storage in thick format. Creating disks might take longer using this option. • Thin Provision—Allocates storage on demand as data is written to disk.
Network Mapping	Choose the required network.
Properties Address any errors that are indicated in red-colored text below a selection box.	
Node Mode	Choose the type of deployment for this node: Standalone, Primary Node, or Service Node. The mode you choose should match the deployment type in the Deployment Configuration screen.

Screen	Action
ICFPP Hostname	Enter the hostname for the Cisco ICFPP node.
ICFPP Password	Enter and confirm the password to use for the admin, root, and ShellAdmin account access.
Static IP Address	Enter the static IP address to use for the Cisco ICFPP node.
Static IP Subnet Mask	Enter the subnet mask to apply to the node IP address.
IP Gateway	Enter the gateway IP address.
Primary Node IP Address for Service Node	For service nodes only, enter the IP address of the primary node or the virtual IP address (VIP) of the HA pair for database access.
NFS Server IP Address	Enter the IP address for an NFS server. Note If you do not configure NFS in a multiple-node cluster deployment, template creation and VM migration can fail if a service node fails.
NFS Server Directory to Mount	NFS server directory to be mounted.
Domain Name	Enter the domain name for the node, such as cisco.com.
DNS Server IP Address	Enter the DNS server IP address.
NTP Server IP (FQDN or IP Address)	Enter the NTP server IP address or fully qualified domain name.
Ready to Complete	Review the deployment settings for accuracy.

Step 5 Click **Finish**. A progress indicator displays the task status until Cisco ICFPP is deployed. For additional information, right-click the VM in the VMware vSphere Client and choose **Open Console**.

Step 6 After Cisco ICFPP is successfully deployed, power on the virtual appliance.

What to Do Next

Continue with [Post-Installation Task for VMware Environments](#), on page 4.

Post-Installation Task for VMware Environments

After installing Cisco ICFPP in a VMware environment, you might need to configure the Cisco ICFPP IP address for network access. For more information, see [Configuring the IP Address for Network Access](#), on page 5.

Configuring the IP Address for Network Access

The Cisco ICFPP IP address is configured during installation by using Open Virtualization Format (OVF) parameters. However, if the IP address is not configured correctly, you must configure the static IP address by using the ShellAdmin console options as described in this procedure.

Procedure

- Step 1** Using SSH, connect to the Cisco ICFPP ShellAdmin console by using the following information:
- Cisco ICFPP IP address
 - Username—shelladmin
 - Password—The password that you set when you installed Cisco ICFPP.
- Step 2** At the ShellAdmin prompt, choose the **Configure Network Interface** option to configure the static IP address.
- Step 3** Enter **S** to configure a static IP address.
- Step 4** Enter the Ethernet interface that you want to configure, such as eth0 or eth1.
- Step 5** When prompted for the IP version, choose **IPv4**.
- Step 6** Enter the static IP address, netmask, and gateway IP address.
- Step 7** Enter **Y** to confirm the information.
The Cisco ICFPP virtual appliance reboots and displays a screen with the URL for accessing Cisco ICFPP.
- Step 8** (Optional) To verify that the change has been applied, log in to the ShellAdmin console and choose the **Display Network Details** option.
-

Upgrading Cisco ICFPP

Cisco ICFPP enables you to upgrade standalone appliances and multiple-node clusters for bug fixes and updated adapters. For more information, see the following topics:

- [Upgrading a Standalone Node](#), on page 5
- [Upgrading a Multiple-Node Cluster](#), on page 6

Upgrading a Standalone Node

Use this procedure to upgrade a standalone node for bug fixes and updated adapters. To upgrade a multiple-node cluster, see [Upgrading a Multiple-Node Cluster](#), on page 6.

Before You Begin

- Obtain the Cisco ICFPP upgrade file (`icfpp-upgrade-2.2.1.tar.gz`) from cisco.com. For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFPP virtual appliance.

Procedure

Step 1 In the Cisco ICFPP GUI, choose **Install > Adapters**, and click **Install**.

Step 2 In the **Install Adapter** dialog box, enter the following information:

Field	Description
Adapter Type	Choose Cisco .
Adapter Name	This field displays CAPI by default. No input is required.
Adapter Description	Enter the desired description.
Adapter File	Browse to the Cisco ICFPP upgrade file and click Open .

Step 3 Click **Upload**.

Step 4 After the unload is complete, click **Submit**.

Step 5 Using SSH, log in to the ShellAdmin console for the virtual appliance.

Step 6 Choose the **Stop Services** option.

Step 7 Choose the **Start Services** option.

Cisco ICFPP is upgraded to the new version, and updated version information is displayed in the GUI in the **Adapters** tab.

Upgrading a Multiple-Node Cluster

Use this procedure to upgrade a multiple-node cluster for bug fixes and updated adapters. To upgrade a standalone (single-node) Cisco ICFPP virtual appliance, see [Upgrading a Standalone Node](#), on page 5.

The high-level tasks involved in upgrading a cluster are:

- 1 Upgrading the HA active node.
- 2 Stopping the virtual IP services on the upgraded HA active node.
- 3 Monitoring status while services fail over to the HA standby node.
- 4 Upgrading the HA standby node.
- 5 Stopping the virtual IP services on the upgraded HA standby node.
- 6 Starting the virtual IP services on the HA active node.
- 7 Starting the virtual IP services on the HA standby node.
- 8 Upgrading and restarting Infra services for each service node.

The following procedure describes how to perform these tasks.

Before You Begin

- Obtain the Cisco ICFPP upgrade file (`icfpp-upgrade-2.2.1.tar.gz`) from cisco.com. For assistance, contact your Cisco representative.
- Ensure that the upgrade file is accessible from the Cisco ICFPP virtual appliance.
- Confirm that HA has been configured on two Cisco ICFPP virtual appliances that are configured with the primary node role.

Procedure

-
- Step 1** Using the node management IP address instead of the virtual IP address for the HA pair, log in to the Cisco ICFPP GUI for the active node in the HA pair.
- Step 2** Upgrade the HA active node as follows:
- a) Choose **Install > Adapters > Install**.
 - b) In the Install Adapter dialog box, provide the required information.
For more information about the fields in this dialog box, see [Upgrading a Standalone Node](#), on page 5.
 - c) Click **Upload**.
 - d) After the upload is complete, click **Submit**.
- Note** Do NOT restart Infra services after upgrading the HA active node.
- Step 3** Log in to the ShellAdmin console for the HA active node that was upgraded in Step 2.
- Step 4** Stop the Virtual IP service on the active node as follows:
- a) Choose the **Setup HA** option.
 - b) When asked if you want to reconfigure HA, enter **Y**.
 - c) Enter **C** to stop the VIP service.
 - d) Enter **Y** to confirm the action.
 - e) Press **Enter** to return to the ShellAdmin menu.
- Step 5** Log in to the ShellAdmin console for the standby node for the HA pair.
- Step 6** In the ShellAdmin console for the HA standby node, choose **Display Services Status** to monitor the following events as they occur:
- HA services fail over to the standby node in the HA pair.
 - Infra services start running on the standby node.
 - The GUI for the standby node becomes available for logging in.
It can take a few minutes for the services to start and for the GUI of the standby node to be accessible from the browser.
- The node that was originally the HA standby node becomes the HA active node.
- Step 7** Using the node management IP address instead of the virtual IP address for the HA pair, log in to the Cisco ICFPP GUI for the node that is now the active node in the HA pair.
- Step 8** Upgrade the HA newly active node (the original standby node) by uploading and submitting the upgrade package as described in Step 2 of this procedure.
- Note** Do NOT restart Infra services after upgrading this node.

- Step 9** In the ShellAdmin console for the node that was upgraded in Step 8, stop the Virtual IP service as described in Step 4.
- Step 10** In the ShellAdmin console for the original active node that was upgraded in Step 2, start the Virtual IP service as follows:
- Choose the **Setup HA** option.
 - When asked if you want to reconfigure HA, enter **Y**.
 - Enter **D** to start the VIP service.
 - Press **Enter** to return to the ShellAdmin menu.
- Step 11** In the ShellAdmin console for the HA standby node that was upgraded in Step 8, start the Virtual IP service as described in Step 10.
- Step 12** For each service node in the cluster:
- Log in to the Cisco ICFPP GUI for the service node.
 - Upgrade the service node by uploading and submitting the upgrade package as described in Step 2.
 - Using the ShellAdmin console, restart Infra services by first choosing the **Stop Services** option and then choosing the **Start Services** option.
-