Cisco Intersight Managed Mode Transition Tool User Guide, 3.x

First Published: 2022-10-10

Last Modified: 2023-04-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CHAPTER 1

New and Changed Information

New and Changed Information

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 3.x

Table 1: New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 3.1.1

Feature	Description	Where Documented
Preservation of configuration identifiers while cloning an Intersight account	IMM Transition Tool, Release 3.1.1 enables you to clone an Intersight account while preserving the assigned IDs on the source server profiles.	Appendix C: Transition Settings
Support for conversion of UCS Central tags	IMM Transition Tool, Release 3.1.1, supports the conversion of UCS Central tags that are assigned to various pools, policies, and profiles/templates.	Appendix C: Transition Settings
Enabling proxy settings for individual devices	You can now enable/disable the proxy settings separately for each device.	Device Management
Bulk deletion of devices	You can now delete multiple devices with a single click on the device management page.	Device Management
Ability to backup and restore data	IMM Transition Tool, Release 3.1.1, provides the ability to back up and restore data on the tool.	Appendix E: Backup/Restore

Feature	Description	Where Documented
Validation of the firmware version of the added device.	IMM Transition Tool, Release 3.1.1, shows a warning if the firmware version of the added device is not compliant with the minimum supported version.	Device Management
Support for UCS 4.2(3) release	Support for UCS 4.2(3) release and conversion of Cisco UCS 6536 Fabric Interconnect in UCSM mode.	Appendix A: Supported Features for Conversion
Updated the list of supported hardware in IMM.	The updated list of supported hardware in IMM now includes IOM 2304, FEX 93180YC-FX3,Cisco UCS 6536 FI, all VIC 1300 models.	

Table 2: New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 3.0.2

Feature	Description	Where Documented
Generating Readiness Report without adding an Intersight device	You can now generate the conversion readiness report without having to add the configuration details of the destination Intersight device in the IMM Transition Tool.	Adding an IMM Transition for Conversion
Support for Private VLAN conversion	IMM Transition Tool, 3.0.2 supports the conversion of Private VLANs from UCSM to Intersight.	Appendix A: Supported Features for Conversion
Ability to define custom tags for transition	You can now customize the converted objects tags by adding, updating, and deleting the tags on the Transition Settings page.	Appendix C: Transition Settings
Bulk deletion of transitions	You can delete the listed IMM transitions in bulk.	Transition Management
Ability to upgrade the tool using the command-line interface (CLI).	In addition to the GUI, you can now upgrade the IMM Transition Tool from 3.0.1 to 3.0.2 using CLI.	Upgrading Tool
Ability to view all of the Inband and OutOfBand (Static/Pool) IP Addresses assigned to the Service Profiles in the Readiness Report.	You can now view the Management IP Addresses section in the Transition Readiness Report that lists IP Addresses assigned to UCSM/Central Service Profiles and physical server.	Interpreting Transition Readiness Report

Feature	Description	Where Documented
Support for Intersight V2 and V3 API Keys	You can now use OpenAPI V2 and V3 API Keys to connect to Intersight.	Adding an IMM Transition for Conversion

Table 3: New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 3.0.1

Feature	Description	Where Documented
Preservation of Configuration Identifiers	The Service Profile identifiers can be preserved when converting from UCSM/Central to Intersight.	Overview
Cloning an Intersight Account	Configuration attributes can be cloned between two Intersight instances.	Adding an IMM Transition for Cloning
Mapping UCS Organization to Intersight Organization	One or more source UCS organization(s) can be mapped to an Intersight organization.	Adding an IMM Transition for Conversion
View Push Summary	You can view the push status of each object using the **View Push Summary** option.	Adding an IMM Transition for Conversion and Adding an IMM Transition for Cloning
Default Transition Settings	You can define the default configuration settings that get applied to every new transition that is created in the tool.	Appendix C: Transition Settings
Auto-generated default password for converted policies	An auto-generated default password is used for converting policies.	Installing Cisco Intersight Managed Mode Transition Tool
Support for new IMM configurations such as breakout ports, static pin groups, FC Zoning Policy, Cisco UCS 6536 Fabric Interconnect.	Support has been added for the conversion of breakout ports and static pin groups from UCSM to Intersight. The tool also supports FC Zoning policy and Cisco UCS 6536 FI model in Intersight accounts.	Appendix A: Supported Features for Conversion

CHAPTER 2

Overview

Overview

Cisco Intersight Managed Mode (IMM) Transition Tool helps bootstrap new IMM deployments by replicating the configuration attributes of the existing Cisco UCS Manager (UCSM) and Cisco UCS Central infrastructure, and by converting the existing Service Profile and Templates to IMM Server Profile and Templates to accelerate deployment of new servers and to migrate existing servers to Intersight Managed Mode.

IMM Transition Tool, Release 3.0.1 and above, provides support for preserving the configuration identifiers that a physical server gets from a server profile. These include IP Addresses, MAC addresses, IQNs, UUIDs, WWNNs, and WWPNs. This support enables the migration of Service Profiles from UCS Manager/Central to IMM.

IMM Transition Tool offers the following functionality:

1. Ability to validate hardware compatibility for Cisco UCS Manager domain.
2. Fetching entire configuration from running UCS Manager domain or UCS Central instance.
3. Ability to validate what part of the configuration is available in Intersight.
4. Performing conversion of the UCS Manager or UCS Central configuration attributes to IMM.
   - Conversion of the running configuration of the UCS Manager domain is primarily done in two parts (you can selectively enable/disable each section for config conversion):
     - Convert the fabric configuration of the UCS Manager domain including VLANs/VLAN Groups/VSANs, Port roles, QoS, and administrative settings (NTP/DNS/SNMP/SYSLOG).
     - Convert the Service Profiles and Service Profile Templates from the UCS Manager domain and all the attached policies to the best extent possible.
   - Conversion of the running configuration of the UCS Central instance is primarily done as follows (you can selectively enable/disable each section for config conversion):
     - Convert the Service Profiles and Service Profile Templates from the UCS Central instance and all the attached policies to the best extent possible.

Note Fabric configuration conversion for UCS Central can be achieved by performing a fabric conversion of the corresponding UCS Manager domain(s).

- IMM Transition Tool, Release 3.1.1, supports the conversion of UCS Central tags that are assigned to various pools, policies, and profiles/templates.

5. Generation of IMM readiness report that can be used to get an overview of the compatibility of the hardware and configuration when the domain is converted from UCS Manager or UCS Central to IMM.

   Note As Cisco UCS Central can be registered with multiple UCS Manager domains, the Hardware Compatibility is only available for a UCS Manager domain and not for the UCS Central instance itself.

   The IMM readiness report provides:

   - A conversion score and overall summary showing an overview of readiness of the UCS Manager or UCS Central device for migration into IMM.
   - The detailed information for each configuration, such as converted objects and the objects that the tool could not convert.

6. Cloning of configuration attributes between two Intersight accounts

   From IMM Transition tool, 3.0.1 onwards, you can clone an Intersight account to another Intersight account. The feature is supported for SaaS and Virtual Appliance accounts. All standalone and IMM servers related pools/policies/profiles/templates can be cloned.

   IMM Transition tool, 3.1.1, enables you to clone an Intersight account while preserving the assigned IDs on all the UCS server profiles.

7. Mapping the source UCS organization(s) to the destination Intersight organization.

   IMM Transition Tool, Release 3.0.1, provides the ability to do mapping of organization(s). This new feature gives you more flexibility to control the conversion of org from UCS Manager/Central to Intersight. Through a one-to-one or many-to-one mapping, you can select the destination Intersight org or you can add a new destination Intersight org that you want for your source UCS org(s).

Note If your UCSM domain has any HyperFlex cluster deployed, do not migrate to IMM. HyperFlex servers are not currently supported in IMM.

CHAPTER 3

Getting Started with Cisco Intersight Managed Mode Transition Tool

Prerequisites

This section covers the minimum requirements for installing Cisco Intersight Managed Mode Transition Tool:

- Supported version of Cisco UCS Manager: 3.2(1d) or above.
- Supported version of Cisco UCS Central: 2.0(1a) or above.
- Supported ESX version - ESXi 6.0 and above.
- Minimum VM requirement - 2 vCPUs, 8 GB RAM, 100 GB storage.
- Virtual Hardware Version used by the OVA - 11
- Network Connectivity Requirements:
  - TCP Port 443(HTTPS) (from IMM Transition Tool, Release 1.0.2 onwards)
  - TCP Port 22 (SSH) for troubleshooting or advanced configuration.
  - Access to the following is required:
    - DNS (using TCP/UDP Port 53)
    - NTP (using UDP Port 123)
    - UCS Manager/UCS Central devices (using TCP Port 443 [HTTPS] only)
    - Intersight devices (using TCP Port 443 [HTTPS] only)
    - Connection to the proxy server settings (if any)
  - Pushing Config to Intersight requires HTTPS connectivity to the Intersight instance.

- For SaaS, the URL is https://www.intersight.com
- For Appliance, the URL is provided by the user.

Installing Cisco Intersight Managed Mode Transition Tool

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco Intersight Managed Mode Transition Tool OVA has a preinstalled operating system and includes application functionality that is necessary for the IMM Transition Tool functionality. The IMM Transition Tool as an OVA can be deployed on a VMWare Vsphere infrastructure.

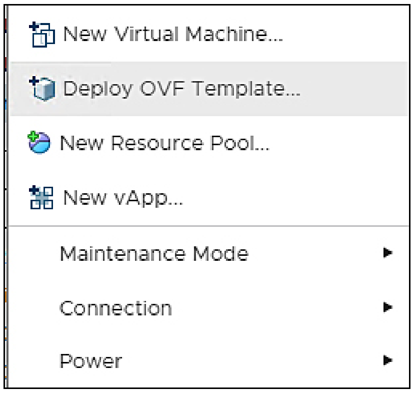
Note From IMM Transition Tool, 3.1.1 onwards, you can take a backup of the tool data and restore it on the same or another instance of the IMM Transition Tool. For more details, see Appendix E: Backup/Restore.

Before you begin

- From the UCS Tools page, download the IMM Transition Tool .ova file to your computer in a place that is easy to find when you start to deploy the OVF template.

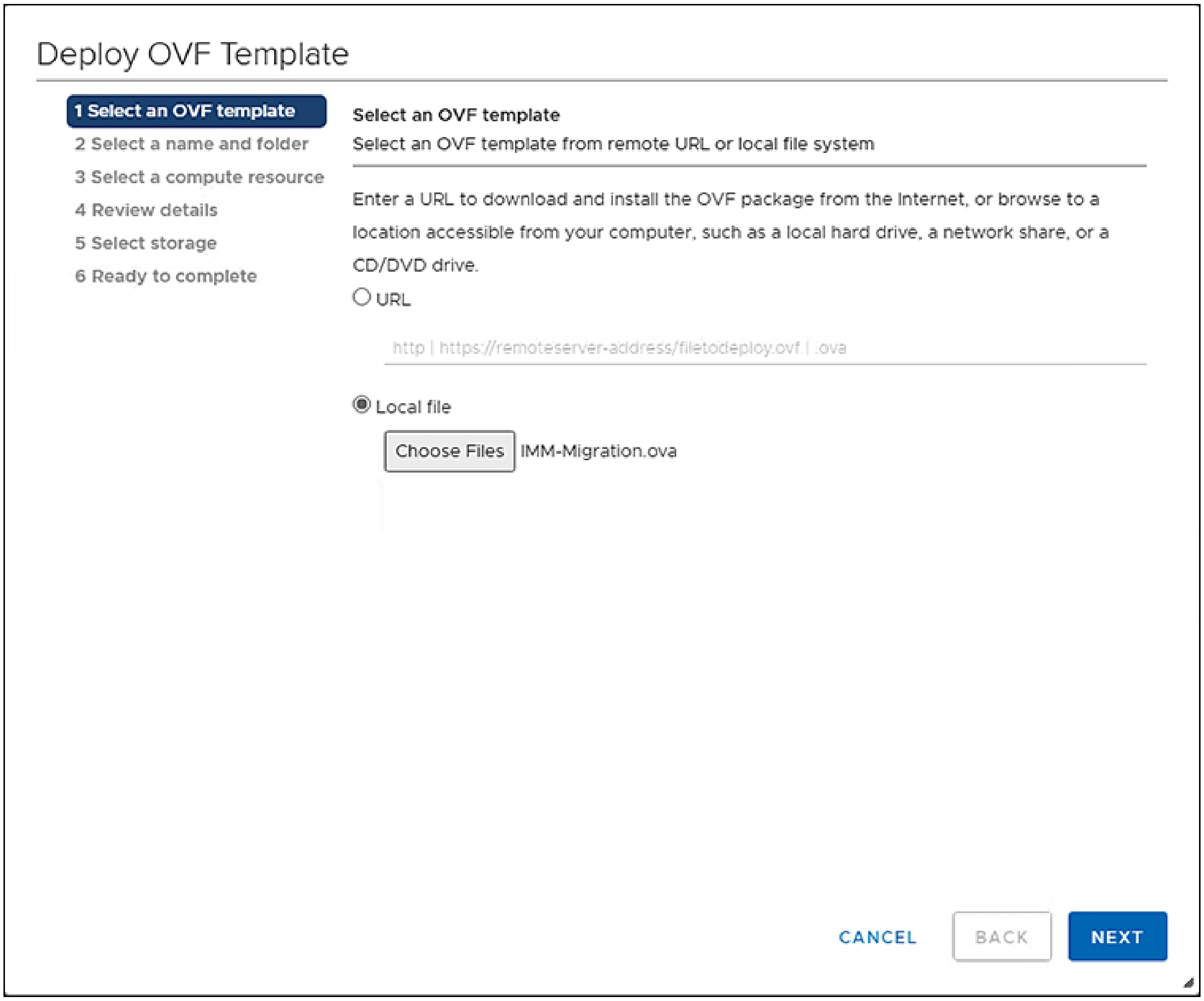
Step 1 Log into the HTML5 vSphere Web Client and go to the **VMs** tab.

Step 2 Add the **Deploy OVF Template** action button via the *Actions* dropdown list.



Step 3 Click the added **Deploy OVF Template** button.

A new window appears, asking to select a template.



Deploy OVF Template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

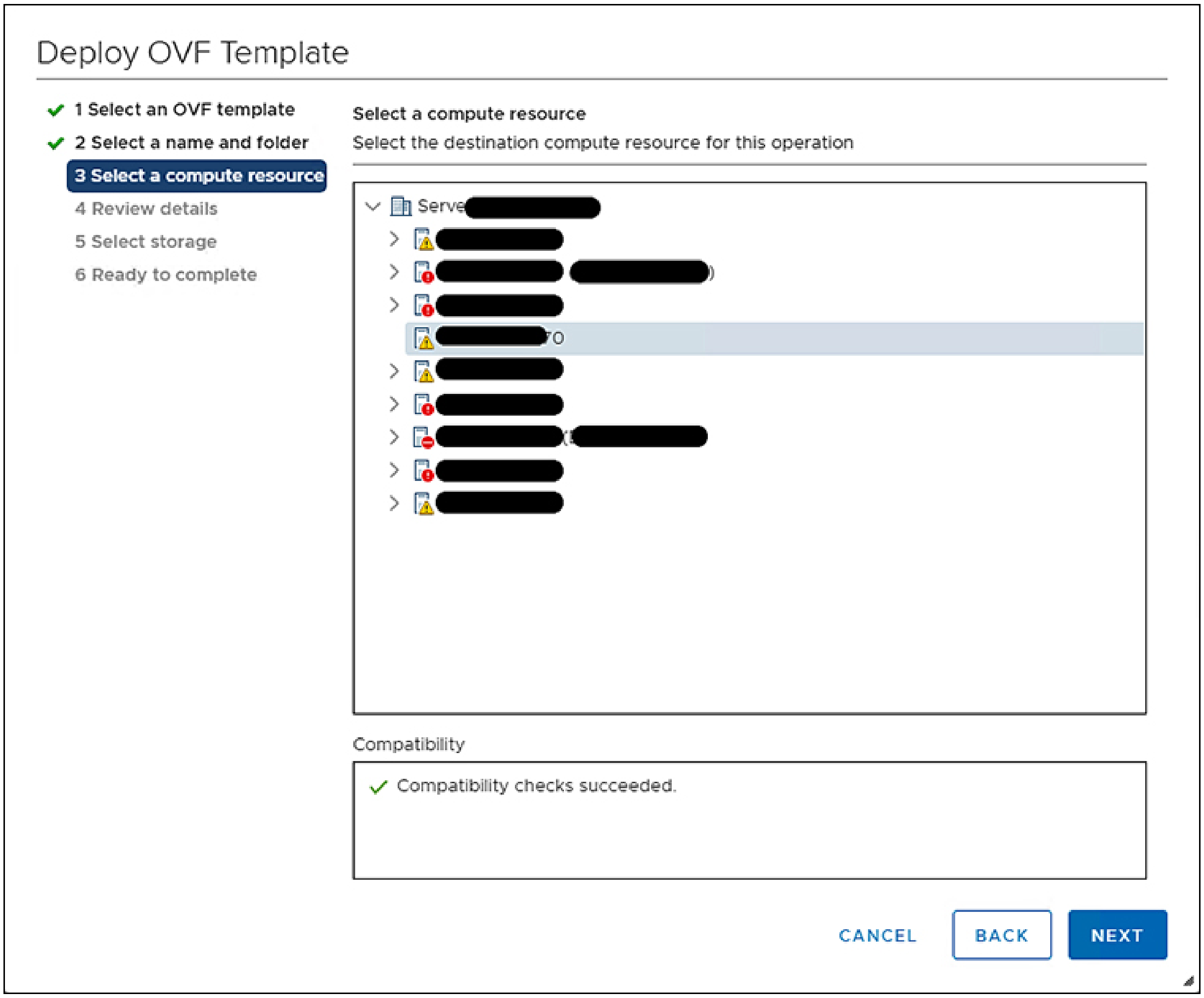
Choose Files IMM-Migration.ova

Step 4 Click **Choose Files**, select the downloaded OVA file.

Step 5 Click **Next**.

Step 6 Select the location where you want to deploy the virtual appliance, click **Next**.

Step 7 Select the resource you want to use to run the virtual appliance, click **Next**.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource

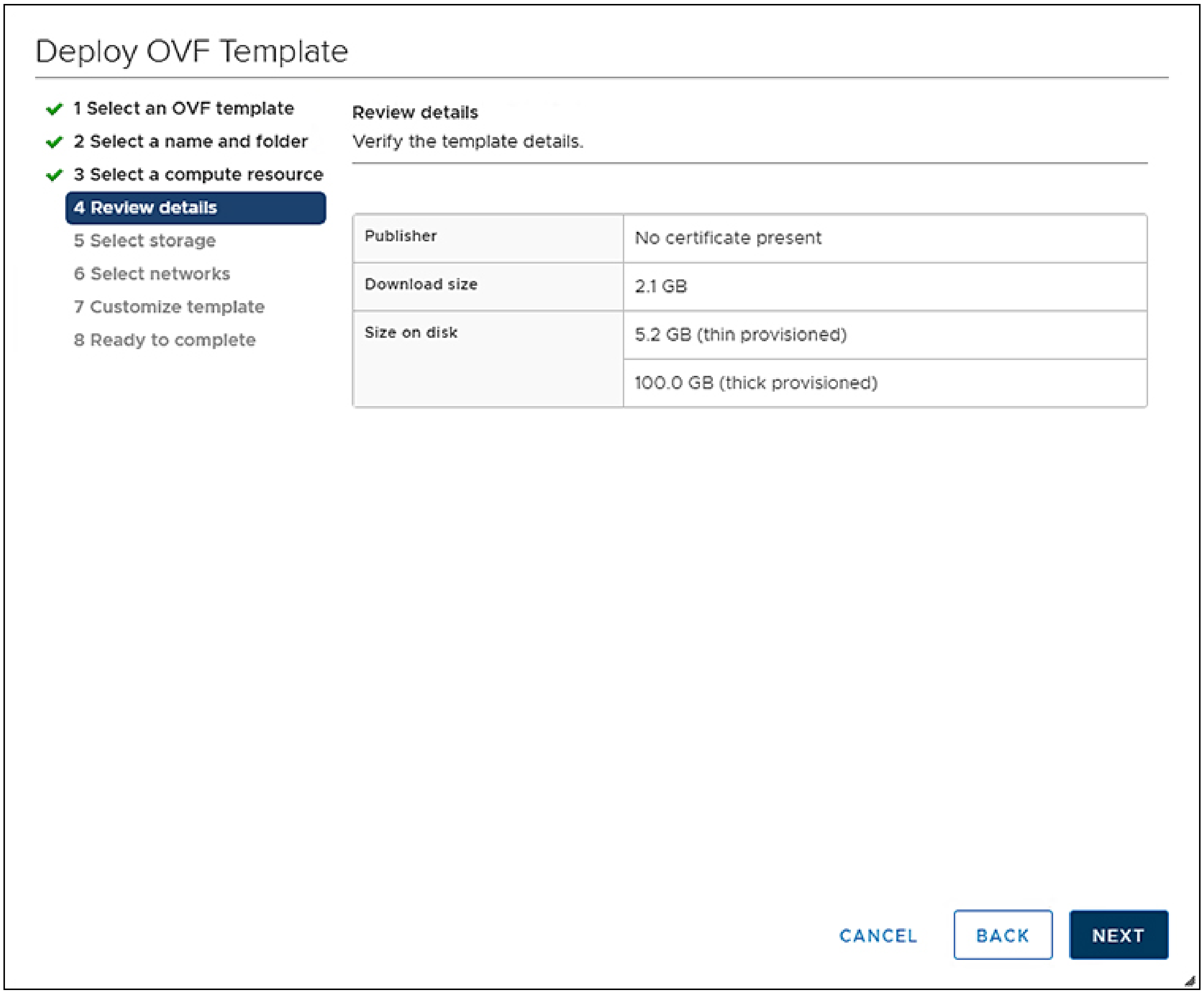
Select the destination compute resource for this operation

- Serve[redacted]
  - [redacted]
  - [redacted] [redacted])
  - [redacted]
  - [redacted]0
  - [redacted]
  - [redacted]
  - [redacted]([redacted]
  - [redacted]
  - [redacted]

Compatibility

✓ Compatibility checks succeeded.

Review the package details, that contain advanced configuration options.



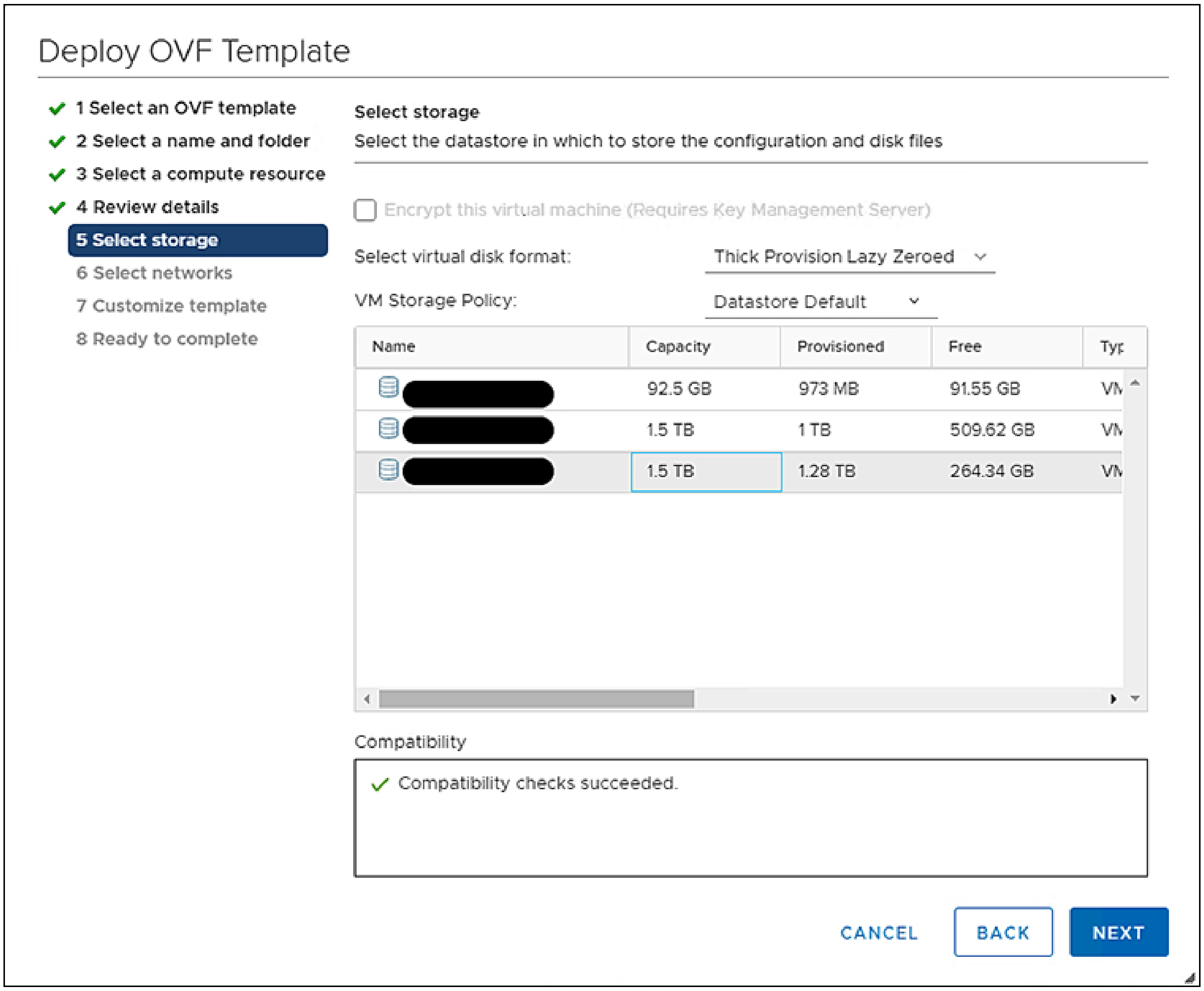
Review details

Verify the template details.

Publisher	No certificate present
Download size	2.1 GB
Size on disk	5.2 GB (thin provisioned)
	100.0 GB (thick provisioned)

Step 8 Click **Next** to accept these options.

Step 9 Select the desired storage location from the list of datastores, click **Next**.



Select storage

Select the datastore in which to store the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

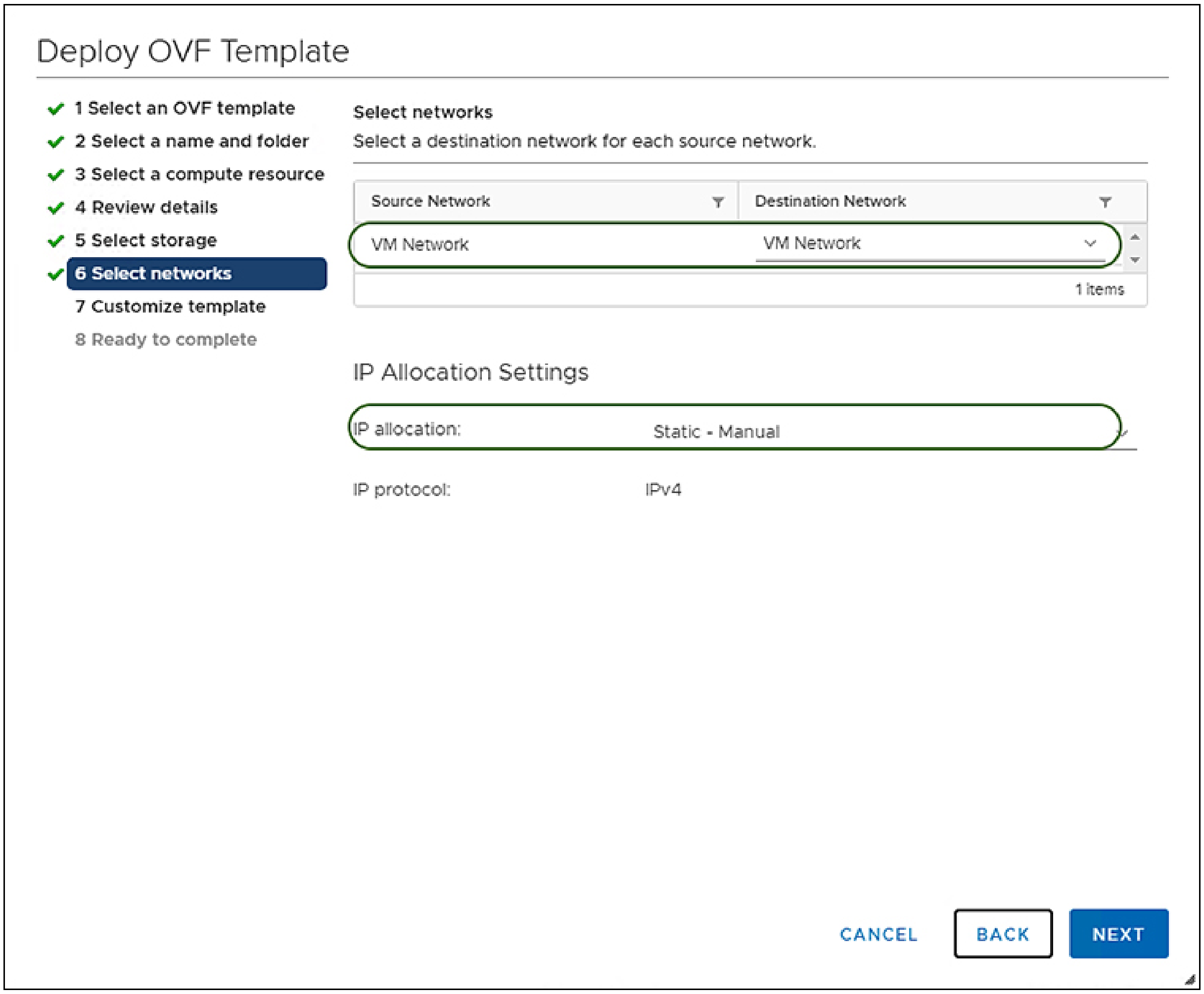
VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Typ
[redacted]	92.5 GB	973 MB	91.55 GB	VN
[redacted]	1.5 TB	1 TB	509.62 GB	VN
[redacted]	1.5 TB	1.28 TB	264.34 GB	VN

Compatibility

✓ Compatibility checks succeeded.

Step 10 Select a destination network from the dropdown list for each source network, click **Next**.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

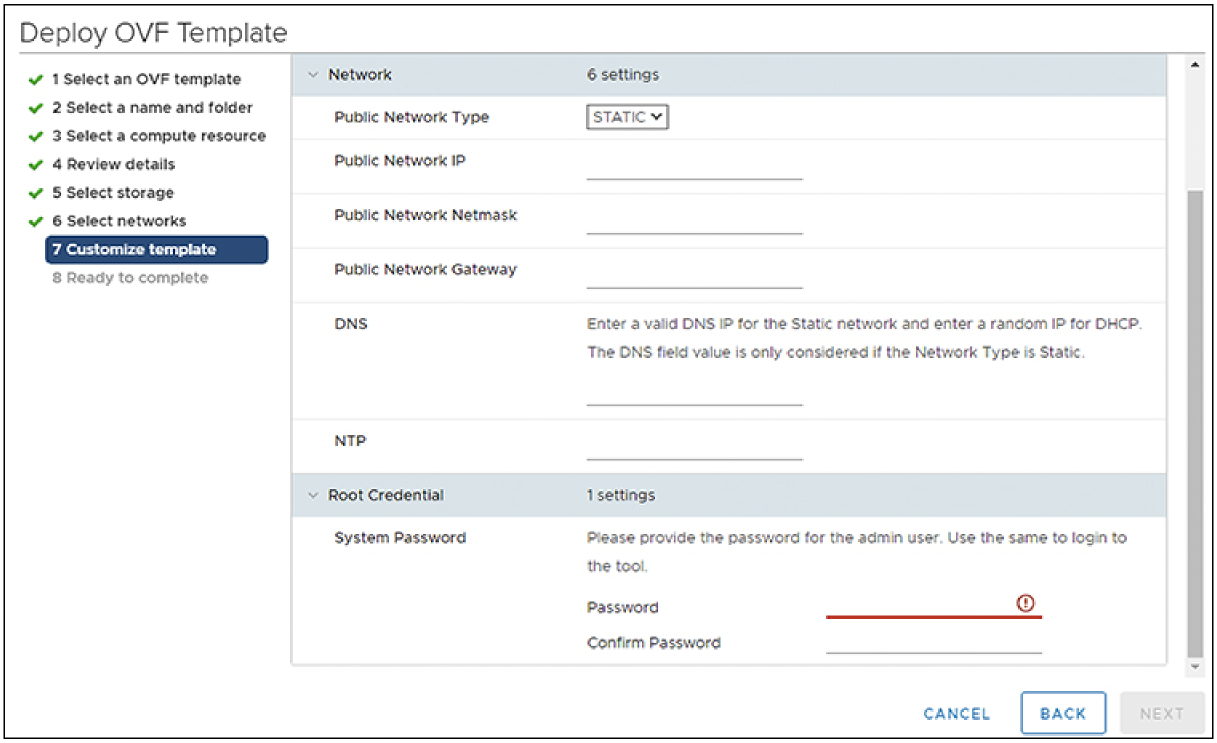
1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Step 11 Customize the deployment properties by entering the **Network** settings values and setting up the **System Password**.



Network 6 settings

Public Network Type STATIC

Public Network IP

Public Network Netmask

Public Network Gateway

DNS Enter a valid DNS IP for the Static network and enter a random IP for DHCP. The DNS field value is only considered if the Network Type is Static.

NTP

Root Credential 1 settings

System Password Please provide the password for the admin user. Use the same to login to the tool.

Password

Confirm Password

An auto-generated default password is used as a replacement for any existing password in UCS Manager/UCS Central policies such as Virtual Media, iSCSI Boot that are converted. Similarly, another auto-generated password is used for Mutual CHAP Authentication in iSCSI Boot Policy.

Note You should change the password for the converted policies after those are pushed to Intersight.

Step 12 Click **Next**.

Review the configuration data.

Step 13 Click the **Refresh** button to update the system.
The VM will be visible in the center windowpane.

Step 14 Select the VM and click **Power On**.

Step 15 Once the VM is powered on, click the **Open Console** icon to open the VM console in a new window.

You have successfully deployed the OVA template and powered on the VM.

Upgrading Cisco Intersight Managed Mode Tool

Perform the following steps to upgrade the tool from 3.0.1 or 3.0.2 to any of the higher version using CLI :

1. Take a SNAPSHOT of the VM before starting the upgrade.
2. Copy (SCP) the downloaded tar file of the higher version to the lower version VM.
3. Execute the below command:

```
sudo imm_upgrade -p <downloaded_tar_file>
```

This will take few minutes to complete.

The file validation and the upgrade process will get started as shown below:

INFO: File format validation success

INFO: Version validation success

INFO: MD5 hash validation success

INFO: Upgrading...

INFO: Upgrade Success. Restarting server

INFO: Server Restarted

Note It is recommended to roll back to the last snapshot of the VM in case of failure of the upgrade.

Accessing Cisco Intersight Managed Mode Transition Tool using the Graphical User Interface

You can access the user interface of the Cisco IMM Transition Tool through browser window, to generate transition readiness report, and convert UCS domain into IMM configuration.

Step 1 Launch a Web browser window.

Step 2 Enter `http://<VM IP address>` or `https://<VM IP address>`. VM IP address is the IP address of the VM where you have deployed Cisco IMM Transition Tool OVA.

IMM Transition Tool, Release 1.0.2 and above, provides HTTPS support. All the `http` URLs get redirected to `https`.

Step 3 In the Login dialog box, enter the user name and password.

User name: admin

Password: Enter the password set on the **Customize template** page during installation.

Step 4 Click **Sign In**.

To end the user session, click **Log Out** from the user settings in the top-right corner.

Note **Session Timeout**—In IMM Transition Tool, Release 1.0.2 onwards, if you remain inactive for 30 min, you are automatically logged out of the session. You have to relogin to use the application again.

CHAPTER 4

Working with Cisco Intersight Managed Mode Transition Tool

Adding an IMM Transition for Conversion

Converting Service Profiles from UCSM/Central to Server Profiles in Intersight

Perform the following steps to start with the IMM transition:

Before you begin

You can set the default settings for the transition that will get applied for the current running and all the subsequent transitions. You can also change the default settings during the **Add Transition** process. For details, refer **Default Transition Settings for Conversion** section in Appendix C: Transition Settings.

Step 1 Click **Add IMM Transition**.

Step 2 Enter a name for the Transition.

Step 3 Select a Transition Type.

(a) Select **Generate Readiness Report** if you only want to view the compatibility/readiness summary of the UCS Manager hardware and configuration or the compatibility of the UCS Central configuration.

(b) Select **Generate Readiness Report + Push Config to Intersight** if you want to view the readiness report and push the converted configuration to Intersight.

(c) Select **Clone Intersight** if you want to migrate from one Intersight account to another by cloning the configurations. For the detailed procedure, refer Adding an IMM Transition for Cloning.

Step 4 Click **Next**.

Step 5 Select the Source Device - UCS Manager or UCS Central.

Step 6 Enter the selected device details.

(a) Choose the **Select Existing UCS Manager/ Select Existing UCS Central** option if you want to migrate the configuration of an existing device.

(b) Choose the **Add New UCS Manager/Add New UCS Central** option if you want to add a new UCS Manager/UCS Central configuration. Enter the Device IP/FQDN, Username, and Password for the device. If required, enable the proxy for the newly added device by turning on the **Use Proxy** toggle button. Add proxy settings details in the **Proxy Settings** interface. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings

Step 7 Click **Refresh** to retrieve the latest configuration and inventory details from the UCS Manager/Central device.

If the selected source device is UCS Central, then you can choose the UCS Central instance from the **Choose UCS Central** drop-down list.

You can download the Configuration JSON file and Inventory JSON file for the current device using the **Download** link.

Configuration JSON file contains the detailed information of the software configuration present in the existing UCS Manager/UCS Central device.

Inventory JSON file contains the detailed information of the hardware inventory present in the UCS Manager domain or in all the UCS domains of the UCS Central instance.

These files can be shared with the technical support team for troubleshooting purpose.

Step 8 Click **Next**.

Step 9 Select the destination Intersight Account.

(a) Select **Choose from existing account** option if you want to migrate the configuration to an existing Intersight account. Go to Step 13.

(b) Select **Add new account** option if you want to migrate the configuration to a new **SaaS Intersight** or a new **Intersight Appliance VM** account. Go to Step 11.

(c) Select **Proceed without Intersight device** option if you want to generate the conversion readiness report without adding the details of the destination Intersight account. Go to Step 13.

Step 10 Perform the following steps to generate an API Key ID from Intersight.

a. Log into the Intersight application.

b. On the top-right corner, click on the Gear icon and select **Settings**.

c. Under the **API** section, click **API Keys**.

d. On the top-right of the page, click **Generate API Keys**.

e. Enter a name in the **Description** field and select **API Key for OpenAPI Schema Version 2 or Version 3**.

Note OpenAPI schema version 2 is not supported till IMM Transition Tool, Release 3.0.1. The support for API Keys with V2 and V3 schema is available from IMM Transition Tool, Release 3.0.2 onwards.

f. Click **Generate**.

The API Key ID and Secret Key get generated. Use the **Copy to Clipboard** blue icon to copy these values to the clipboard. Go back to the IMM Transition Tool application.

Step 11 Complete the following fields:

- API Key ID: Enter the API Key Id generated in the previous step.

- Secret Key: Enter the Secret Key generated in the Intersight.

Also, enter the FQDN if you have selected Intersight Appliance VM.

Step 12 Click **Next**.

Step 13 Configure the conversion options that you want for the transition.

- For details on each of the Transition Settings field, refer Appendix C: Transition Settings.
- For defining a default set of configurations for every new transition that you create, refer **Default Transition Settings** in Appendix C: Transition Settings.

Step 14 Click **Next**.

Step 15 Select the Service Profiles/Templates that need to be converted.

Next to the profile name, association details with the physical server can be viewed. Hover the mouse pointer over the service profile name to view the description of the Service Profile or Template.

You can search for a specific service profile/template using the search bar located on the top.

You can apply a filter to only display the Service Profile Templates, or both the Service Profiles and Templates in the **Show** drop-down list, located beside the search bar.

Step 16 Click **Next**.

Step 17 Keep **Advanced Organization Mapping** turned on if you want the selected source org(s) to be converted to the mapped destination Intersight org. To manually enter the name of the destination Intersight org, turn off the toggle button, and enter a Root Org name and go to Step 20. You can also retain the source UCS org name in the destination Intersight org by enabling the **Keep source Org path in Intersight Org name** option.

- This option gives the flexibility to control the mapping of converted objects from UCSM to Intersight. Unlike the same name mapping behavior, customized mapping avoids creating multiple Intersight orgs for an account. The **Advanced Organization Mapping** option can help map single or multiple UCS org(s) to an Intersight org.
- You can also add a new destination Intersight org with the **Add New** option.
- **Note** If **Keep source Org path in Intersight Org name** option is disabled, "root/PROD/WINDOWS" and "root/NONPROD/WINDOWS" would get converted to the same "WINDOWS" organization in Intersight. This could cause conflicts if policies/pools/profiles/templates objects are named the same in both source UCS orgs.

Step 18 Select the source UCS org, destination Intersight org, and click **Map Now**.
The source org and the destination org get mapped. Once mapped, you will see "Mapped" tag appearing next to the destination Intersight org name. You can also view the mapped source orgs in the mapping section present at the bottom of the **Advanced Organization Mapping** page.

Use the **Un-Map All** option to unmap all the existing source org to destination org mapping within a selected Intersight account. Also, you can unmap a single mapped entity by going to the mapping section, selecting the mapped entity, clicking on the three dots against it, and selecting the unmap option.

Step 19 Click **Next**.

Next will appear enabled only when the all the source UCS orgs have been selected and mapped to the respective destination Intersight org.

A readiness report gets generated. This process may take several minutes as the selected config attributes are fetched from UCS Manager/UCS Central, converted to IMM, and the resultant report is generated.

Note Depending on the size of UCS Manager/Central Configurations and number of servers connected, some operations may take a significant amount of time to complete (more than an hour).

Step 20 Click **View Report** to view the report or download the report in PDF format using the **Download** option.

Report generation for any selected config is a one-time activity and cannot be regenerated. This ensures that the history of transitions is maintained and can be referred anytime. If you want to edit the config and generate the report, you can clone the transition. For more details, see Transition Management.

Step 21 Click **Next**.
Push to Intersight page appears.

Note In IMM Transition Tool, Release 1.0.2 and above, you can download the available configuration file, manually edit it, and then upload the same using **Advanced Options**.

Step 22 Click **Advanced Options**, browse to the edited file, and click **Upload**.
The uploaded file is used for pushing the configuration to Intersight.

Step 23 Click **Next**.
A connection with Intersight is established, the converted config attributes get pushed to Intersight.

Note

- When a transition is being pushed to Intersight using an Intersight device or is fetching a config/inventory from a UCS Manager/UCS Central device, then the same device cannot be used by other transitions until the previous task on the device completes.
- Reset the default password for the converted polices if those have been pushed to Intersight.

Step 24 Click **View Push Summary** to view the push status of each of the converted object.

This summary lets you know the push status for each of the object. Clicking on the three dots (...) next to each object status displays the detailed commits performed by the IMM Transition Tool in order to push the object to Intersight. The status can be any one of the following:

- Success - The converted object has been pushed successfully to Intersight.
- Skipped - The converted object already exists in the destination Intersight account and has been skipped in the push operation.
- Failed - The converted object could not be pushed to Intersight.

  Click on the three dots present next to the object status to know the reason for push failure.

Adding an IMM Transition for Cloning

Cloning an account in Intersight

Perform the following steps to start with the cloning of an Intersight account:

Step 1 Click **Add IMM Transition**.

Step 2 Enter a name for the Transition.

Step 3 Select a Transition Type.

Select **Clone Intersight** if you want to migrate from one Intersight account to other by cloning the configurations. This option can be used for migrating the configuration policies between two SaaS Intersight accounts, two Virtual Appliance accounts, from a Virtual Appliance Intersight account to a cloud Intersight account and vice-versa. For details on the supported features for cloning, refer Appendix B: Supported Features for Cloning.

Step 4 Click **Next**.

Step 5 Select the source Intersight account.

(a) Select **Choose from existing account** option, in case you want to migrate the configuration of an existing Intersight account.

(b) Select **Add new account** option, in case you want to migrate the configuration of a new **SaaS Intersight** or a new **Intersight Appliance VM** account. Refer Step 8 and 9 for API Key ID and Secret key details. Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings.

Step 6 Select the destination Intersight Account.

(a) Select **Choose from existing account** option, in case you want to migrate the configuration to an existing Intersight account and then go to step 8.

(b) Select **Add new account** option, in case you want to migrate the configuration to a new **SaaS Intersight** or a new **Intersight Appliance VM** account and then go to step 9. Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings.

Step 7 Click **Refresh** to retrieve the latest configuration from the existing Intersight account and then go to step 11.

You can download the Configuration JSON file using the **Download** link.

Configuration JSON file contains the detailed information of the software configuration present in the existing Intersight account.

This file can be shared with the technical support team for troubleshooting purpose.

Step 8 Perform the following steps to generate an API Key ID from Intersight.

a. Log into the Intersight application.

b. On the top-right corner, click on the Gear icon and select **Settings**.

c. Under the **API** section, click **API Keys**.

d. On the top-right of the page, click **Generate API Keys**.

e. Enter a name in the **Description** field and select **API Key for OpenAPI Schema Version 2 or Version 3**.

f. Click **Generate**.

The API Key ID and Secret Key get generated. Use the **Copy to Clipboard** blue icon to copy these values to the clipboard. Go back to the IMM Transition Tool application.

Step 9 Complete the following fields:

- API Key ID: Enter the API Key Id generated in the previous step.
- Secret Key: Enter the Secret Key generated in the Intersight.

Also, enter the FQDN if you have selected Intersight Appliance VM.

Step 10 Click **Next**.

Step 11 Configure the conversion options that you want for the transition.

- From IMM Transition Tool, 3.1.1 onwards, you can preserve the assigned IDs on all the UCS server profiles while cloning an account. For more details, refer the **Transition Settings for Cloning** section in Appendix C: Transition Settings.

Step 12 Click **Next**.
Push to Intersight page appears.

Note In IMM Transition Tool, Release 1.0.2 and above, you can download the available configuration file, manually edit it, and then upload the same using **Advanced Options**.

Step 13 Click **Advanced Options**, browse to the edited file, and click **Upload**.
The uploaded file is used for pushing the configuration to Intersight.

Step 14 Click **Next**.
A connection with Intersight is established, the converted config attributes get pushed to Intersight.

Step 15 Click **View Push Summary** to view the push status of each of the converted object.

This summary lets you know the push status for each of the object. Clicking on the three dots (...) next to each object status displays the detailed commits performed by the IMM Transition Tool in order to push the object to Intersight. The status can be any one of the following:

- Success - The converted object has been pushed successfully to Intersight.
- Skipped - The converted object already exists in the destination Intersight account and has been skipped in the push operation.
- Failed - The converted object could not be pushed to Intersight.

  Click on the three dots present next to the object status to know the reason for push failure.

Transition Management

All the transitions that have been initiated by the user are listed on the **Transition** listing page. The page shows the name of the transition, the current status of the transition (Cancelled, Failed, Incomplete, In progress, Completed), type (Generate Readiness Report, Transition Config to Intersight, Clone Intersight), time of last modification.

Click **...** located against each transition record to perform the required action.

Step 1 Click **Report** to view the readiness report for the transition.

This option is not available for cancelled and failed transitions.

Step 2 Click **Edit** to change the transition name.

Step 3 Click **Delete** to delete the transition.

You can select multiple transitions and click the trash button located on upper-left of the list view to delete the selected transitions in bulk.

Step 4 Click **Clone** to copy the existing transition config.

4(a) Provide a name for the transition. It appears in the listing page with status as *Incomplete*.

4(b) Click **Transition** name to edit the config, generate the readiness report, and push the modified config to Intersight.

Note **Clone** option is not available for transitions with type as **Clone Intersight**.

Step 5 Click **Download Logs** to download the conversion logs to a file.

Device Management

IMM Transition Tool, Release 1.0.2 and above allows you to manage your UCS System and Intersight devices better. You can avoid duplicity of devices by providing unique Target IP or FQDN to each device.

Perform the following steps to add and manage a device.

Step 1 Navigate to **Device Management**.

Step 2 Click **Add Device**.

Step 3 Select the **Device Type** from the drop-down.

Step 4 Enter the Target IP/FQDN.

Step 5 If the Device Type selected in Step 3 is **UCS Manager** or **UCS Central**, enter the **Username** for the device else go to Step 7.

Step 6 Enter the **Password** for the device and go to Step 9.

Step 7 If the Device Type selected in Step 3 is **Intersight SaaS**, enter the API key/ Secret key. If the Device Type selected in Step 3 is **Intersight Appliance VM**, enter the Target/ API Key/Secret Key.

Step 8 Turn on the **Use Proxy** toggle button to enable proxy settings.

For more details on proxy settings, see Appendix D: Proxy Settings

Step 9 Click **Save**.
In IMM Transition Tool, 3.1.1 and above, a validation is performed by the tool to check if the firmware version of the added device is compliant with the minimum version supported by the transition tool. If found non-compliant, a warning message gets displayed.

You can opt-out of the validation check by turning on the **Bypass Validation** toggle button.

The added devices can be deleted or edited. The values that can be edited for the Intersight device are API Key and Secret Key and for a UCS device are Username and Password.

Note

- Deletion of an existing device is possible only when there is no transition associated with it.
- In IMM Transition Tool, 3.1.1, you can select multiple devices and click the trash button located on upper-left of the list view to delete the selected devices in bulk.

Interpreting Transition Readiness Report

The IMM transition readiness report summarizes the compatibility of the hardware inventory and software configuration of the UCS Manager or UCS Central device for transition into IMM.

The Readiness Report is divided into sections as follows:

1. **Conversion Score**- This section shows score meters for Hardware Compatibility (applicable only for UCS Manager domain), Fabric Configuration (applicable only for UCS Manager domain), and Server Policies Configuration.
    - The reading on the score meter can be interpreted as follows:
        - **Excellent**- Almost all of the hardware/configurations can be transitioned to Intersight with some minor discrepancies.
        - **Very Good**- Most of the hardware/configuration can be transitioned, while some hardware/configuration may not be supported or face some discrepancies in transition to Intersight.
        - **Good**- About half of the hardware/configuration can be transitioned to Intersight while rest of hardware/configuration may not be supported or face some discrepancies during transition to Intersight.
        - **Poor**- Only a minor set of hardware/configuration can be transitioned to Intersight while many of hardware/configuration may not be supported or face discrepancies during transition to Intersight.

Note Above assessment is based on general use cases. It is strongly recommended to review the detailed report for your specific environment to assess the transition impact for your domains.

2. **Overall Summary** - The overall summary section consists of IMM Conversion Attention Points, Hardware Compatibility Summary(only for UCS Manager domain), and IMM Config Conversion Summary.
    - **Intersight Managed Mode Conversion Attention Points**- This section lists the attention points that you must look into before starting with the conversion process. It shows the error and warning associated with the conversion process. Error shows the unsupported elements for conversion, Warning shows the list of elements that cannot be completely converted.
    - **Hardware Compatibility Summary** - Separate pie charts are displayed for each of the applicable hardware component such as Fabric Interconnects, Fabric Extenders, Adapters, IO Modules, Chassis, Blades, Racks. The color code in the pie chart can be interpreted as follows:
        - Green color represents that the hardware is compatible for transition.
        - Orange color represents that a firmware upgrade is required for hardware compatibility.
        - Red color represents that the hardware is incompatible for transition currently.

Note The Hardware Compatibility Summary is generated and displayed only for UCS Manager domain and not for UCS Central.

- **Intersight Managed Mode Config Conversion Summary** - This section shows the mapping tables for the UCS Manager and UCS Central objects and the corresponding converted object in Intersight. Separate tables are displayed for each logical object such as Server Profile Templates, Server Profiles, Domain Policies, Pools, Server Policies.

3. **Hardware Compatibility** - This section shows the compatibility report of each of the component of the inventory in detail for UCS Manager domain. It consists of Fabric Hardware Compatibility report, Chassis Hardware Compatibility report, Racks Hardware Compatibility report and so on. Clicking on each of the component shows compatibility report table. This table lists out the hardware details and shows whether the hardware and firmware is compatible or not. A yellow color heading on the left-hand side indicates a warning that few components need a firmware upgrade to become IMM ready. A red color heading on the left-hand side indicates an error that few components are not compatible for IMM transition. A blue color heading on the left-hand side shows an informational message.

4. **Config Conversion** - This section shows the detailed compatibility report for each of the logical object present in the selected service profile template of UCS Manager/Central. Clicking on each of the object heading shows descriptive tables. These tables list the attribute name and value used during conversion, mapping of source UCS Manager/Central and converted Intersight objects, boot order of the devices and so on. A yellow color icon indicates a warning that few objects could not be completely converted. A red color icon indicates an error that few objects are unsupported and cannot be converted. A blue color icon shows an informational message. You can take action according to this message.

5. **Source Config Reference**- This section shows the configuration details present in the source UCS device pools and provides the details of the IP Addresses assigned to Service Profiles and physical servers.

Converting UCS Manager/Central Configuration

When you add a UCS device in the IMM Transition Tool and click **Next**, a utility runs in the backend that validates the hardware inventory and the configuration to check if the device is compatible with IMM.

It connects to the device and replicates the existing logical attributes. These include profiles, policies, pools, and templates.

After the successful completion of the **Push to Intersight** task, the Intersight application reflects the converted objects on refresh.

Assumptions for Conversion

Following are the assumptions for the conversion process in IMM Transition Tool:

1. **Ethernet Network Control Policy** - Ethernet Network Control Policy of Intersight can be created using two different sources of information of UCS Manager/Central.

- Server vNICs - Maps to Network Control Policy of UCS Manager/Central
- Appliance Ports - Maps to Appliance Network Control Policy of UCS Manager

While creating Ethernet Network Control Policy of Intersight using Network Control Policy of UCS Manager/Central, name of the Ethernet Network Control Policy of Intersight will be same as Network Control Policy of UCS Manager/Central.

While creating Ethernet Network Control Policy of Intersight using Appliance Network Control Policy of UCS Manager, name of the Ethernet Network Control Policy of Intersight will be suffixed with **_appliance** to the name of Network Control Policy of UCS Manager.

2. **Ethernet Network Group Policy** - There is no Ethernet Network Group Policy equivalent in UCS Manager/Central. Ethernet Network Group Policy details can be retrieved from VLAN Groups. Each VLAN Group will have VLAN details and those details will be used to create Ethernet Network Group Policy. Name of Ethernet Network Group Policy will be same as the name of VLAN Group.
3. **Ethernet QoS Policy** - QoS Policy of UCS Manager/Central is split into Ethernet and FC QoS Policies in Intersight.
4. **Fibre Channel Network Policy** - There is no Fibre Channel Network Policy equivalent in UCS Manager/Central. Fibre Channel Network Policy details can be retrieved while creating Server Profile (Intersight). The name of Fibre Channel Network Policy is derived from the names of SAN Connectivity Policy and vHBA.
5. **Fibre Channel QoS Policy** - QoS Policy of UCS Manager/Central is split into Ethernet and FC QoS Policies in Intersight.
6. **IMC Access Policy** - Creation of IMC Access Policy for a Service Profile in UCS Manager/Central which has different IP Pools for IPv4 and IPv6 Address in Inband Network Configuration is not supported currently. There is no IMC Access Policy equivalent in UCS Manager/Central. IMC Policy details can be retrieved from Service Profile. Each Service Profile will have Inband Network, IPv4 and IPv6 pool. Using this information IMC Access Policy will be created.
    - Name of the IMC Access Policy is derived using the names of Inband Network VLAN and Inband Pool. The name can be maximum of 64 Characters.
    - In UCS Manager/Central, there are separate options to pick IPv4 and IPv6 pools in Service Profile, but in Intersight there is only one option to pick the IP Pool in IMC Access Policy. Recommendation is to merge IPv4 and IPv6 Pools of UCS Manager/Central into a single Pool, before creating IMC Access Policy in Intersight. But this is not very straight forward to implement. During conversion, if there is a Service Profile with Inband IPv4 and IPv6 addresses belonging to two different IP Pools, then only IPv4 specific Pool will be considered for IMC Access Policy creation.
7. **IPMI Over LAN Policy** - IPMI Over LAN Policy of Intersight is mapped to IPMI Access Profiles in UCS Manager/Central. IPMI User-related information in IPMI Access Profile is moved to Local User Policy in Intersight.
8. **iSCSI Boot Policy** - There is no iSCSI Boot Policy equivalent in UCS Manager/Central. iSCSI Boot Policy details can be retrieved from Service Profile. Each Service Profile will have its own iSCSI vNICs section. Details of iSCSI vNIC will be available inside iSCSI Boot Parameters section of Service Profile. Using this information iSCSI Boot Policy will be created.
    - Name of the iSCSI Boot Policy is derived using the names of Service Profile and iSCSI vNIC.

- In UCS Manager/Central, there is an option to provide the IQN Pool/Initiator Name for iSCSI vNICs Node as well as individual iSCSI vNICs. There is no such option in Intersight for individual iSCSI vNICs. In case of Intersight, IQN is at the LCP level (and not in vNICs).
- Usually in UCS Manager/Central, there will be an option to create two iSCSI Boot Targets for a vNIC and each Target has its own CHAP details. But in Intersight, there is only one option to provide CHAP details for iSCSI Target.
- For CHAP authentication, a default password will be considered during policy creation.

9. **iSCSI Static Target Policy** - There is no iSCSI Static Target Policy equivalent in UCS Manager/Central. iSCSI Static Target Policy details can be retrieved from Service Profile. Each Service Profile will have its own iSCSI Boot Parameters section. Using these iSCSI Boot Parameters, iSCSI Static Target Policy will be created in Intersight. For a single iSCSI interface, there can be multiple targets based on priority. Hence iSCSI target name is designed as a combination of Service Profile name, iSCSI interface name, and iSCSI target priority.

10. **LAN Connectivity Policy** - In UCS Manager/Central, vNIC can be configured in multiple ways:

    a. Inline vNIC

        - Using Standalone vNIC
        - Using vNIC Templates

    b. LAN Connectivity Policy

        - Using Standalone vNIC
        - Using vNIC Templates

    In UCS Manager/Central, it can be either a LAN/SAN Connectivity Policy, or inline vNIC/vHBA that can be using vNIC/vHBA Templates or not. All possible combinations are considered and accordingly converted into LAN/SAN Connectivity Policies in Intersight, as it is the only way to configure connectivity.

11. **Power Policy** - In UCS Manager, the Power-related section of Global Policies are translated as a Power Policy to be used in Chassis Profiles in Intersight.

12. **SD Card Policy** - There is no SD Card Policy equivalent in UCS Manager/Central. This policy can be created by reading the information from Local Disk Configuration Policy of UCS Manager/Central. If there is Flexflash configured in Local Disk Configuration Policy of UCS Manager/Central, then an equivalent SD Card Policy will be created in Intersight.

13. **Storage Policy**-

    - Auto Deploy in Local LUN of Storage Profile

      All Virtual Drives are **Auto Deploy** by default. If the option is set to **no-auto-deploy**, then the mapped VD in Service Profile and the Storage policy VD should have the same name. If the name is different, then it is an invalid configuration.

    - LUN Set in UCS Manager/Central is equivalent to Single Drive RAID Configuration in Intersight.

        - Merge all the disk slots in LUN Set into a single number array.

    - VD Configuration of all drives should be identical. If each LUN set has different VD Configuration, then flag it as invalid configuration.

- M.2 Drive Configuration
- LUN Size set to **Unspecified** in UCS Manager/Central should be only for Virtual Drives which has ExpandToAvail Flag set to True. If the Flag is set to False, it is an invalid Configuration.
- Service Profiles in UCS Manager/Central which has Specific Storage Profile and Generic Storage Profile are merged to form a Single Storage Profile in Intersight.

14. **VLAN Policy** -

    VLAN Policy of Intersight maps to VLAN Section in UCS Manager. In UCS Manager, there is an option to select the Fabric ID (A or B or Both) while creating the VLAN but same is not available in Intersight. As part of conversion, two different VLAN Policies get created if the Fabric ID value is set to **A** or **B** by suffixing Fabric ID to the name of VLAN Policy and single VLAN Policy gets created if the Fabric ID value is set to **Both**. You can also create a Private VLAN by choosing the sharing type as primary/isolated/community. Primary VLAN is a mandatory option. If it is not provided, Private VLAN configurations will be skipped. Thus, converting it to normal VLAN assigned with **default** Multicast Policy.

15. **VSAN Policy** -

    VSAN Policy of Intersight maps to VSAN Section in UCS Manager. In UCS Manager, there is an option to select the Fabric ID (A or B or Both) while creating the VSAN but same is not available in Intersight. As part of conversion, two different VSAN Policies get created if the Fabric ID value is set to **A** or **B** by suffixing Fabric ID to the name of VSAN Policy and single VSAN Policy gets created if the Fabric ID value is set to **Both**.

APPENDIX A

Appendix

Appendix A: Supported Features for Conversion

A. Supported Features for Conversion from UCS to IMM

This section provides a list of features that are supported for conversion in the IMM Transition Tool and a policy mapping between Cisco UCS Manager/Central and Intersight.

Note If the UCS Central configuration contains VLAN/VSAN aliasing, the IMM Transition Tool will automatically select one of the aliases when performing the conversion of the vNICs/vHBAs. Please review the resulting configuration carefully to make sure it is appropriate.

Table 4: (I) Conversion Mapping between UCS and Intersight Features

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Admin	Communication Services *3	SNMP Policy
	Organizations	Intersight Organizations
	Syslog *4	Syslog Policy
	Time zone Management	NTP Policy
	MAC Address Table Aging	Switch Control Policy
	VLAN Port Count Optimization	Switch Control Policy
	Inband Profile VLAN Group	Ethernet Network Group Policy
	Inband Profile Network	IMC Access Policy
	Inband Profile IP Pool Name	IMC Access Policy
	FC Uplink Trunking	VSAN Policy
	DNS *5	Network Connectivity Policy

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Server Policies and Chassis Policies	BIOS Policies	BIOS Policy
	Boot Policies	Boot Policy iSCSI Static Target Policy
	Disk Group Policies	Storage Policy
	IPMI Access Profiles	IPMI over LAN Policy
	iSCSI Adapter Policies	iSCSI Adapter Policy
	iSCSI Boot Policies	iSCSI Boot Policy
	KVM Management Policies	Virtual KVM Policy
	Local Disk Config Policies *6	Storage Policy, SD Card Policy
	QoS Policies	Ethernet QoS Policy/ FC QoS Policy
	Serial over LAN Policies	Serial over LAN Policy
	Service Profiles	Server Profile
	Service Profile Templates *7	Server Profile Template
	Storage Profiles	Storage Policy
	vMedia Policies	Virtual Media Policy
	vNIC/vHBA Placement Policies *8	LAN Connectivity Policy/SAN Connectivity Policy
	Ethernet Adapter Policies	Ethernet Adapter Policy
	Flow Control Policies	Flow Control Policy
	LACP Policies	Link Aggregation Policy
	LAN Connectivity Policies	LAN Connectivity Policy
	Link Protocol Policies	Switch Control Policy
	Multicast Policies	Multicast Policy
	Network Control Policies	Ethernet Network Control Policy
	Fibre Channel Adapter Policies	Fibre Channel Adapter Policy
	SAN Connectivity Policies	SAN Connectivity Policy
	Storage Connection Policies	FC Zoning Policy

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Pools	IP Pools	IP Pool
	IQN Suffix Pools	IQN Pool
	MAC Pools	MAC Pool
	WWNN Pools	WWNN Pool
	WWPN Pools	WWPN Pool
	Server Pools *9	Resource Pool

Following table lists the UCS Manager features that are supported for conversion in the IMM Transition Tool.

Table 5: (II) Conversion Mapping between UCS Manager and Intersight Features

UCS Manager Feature Category	Source UCS Manager Feature Name	Equivalent IMM Policy
Fabric Config *1	Appliance VLANs	VLAN Policy
	QoS System Class	System QoS Policy
	VLAN Groups	Ethernet Network Group Policy
	VLANs	VLAN Policy
	VSANs	VSAN Policy
	Storage VSANs *9	VSAN Policy
	LAN/SAN Pin Group *10	LAN/SAN Pin Group
Fabric Policies *2	Appliance Network Control Policies	Ethernet Network Control Policy
	UDLD Link Policies	Link Control Policy

UCS Manager Feature Category	Source UCS Manager Feature Name	Equivalent IMM Policy
Port Roles	Appliance Ports	Port Policy
	Appliance Port-Channels	Port Policy
	FCoE Uplink Ports	Port Policy
	FCoE Uplink Port-Channels	Port Policy
	LAN Uplink Ports	Port Policy
	LAN Uplink Port-Channels	Port Policy
	SAN Unified Ports	Port Policy
	SAN Uplink Ports	Port Policy
	SAN Uplink Port-Channels	Port Policy
	Server Ports	Port Policy
	FC Storage Ports *9	Port Policy
	SAN Storage Ports *9	Port Policy
	Breakout Port *10	Port Policy

*1 - Merged with regular VLANs

*2 - Merged with regular Network Control Policies

*3 - Sessions/HTTP settings are defined in Intersight Settings. Telnet/SSH settings are not supported

*4 - Only supports up to two remote destination servers

*5 - In UCS Manager, it is found under Admin > Communication Management > DNS Management

*6 - Replaced by Storage Policy. Local Disk Configuration policy supports only Manual creation not the Automatic policy option.

*7 - Only Updating Templates - no support for Initial Templates (though cloning can be achieved)

*8 - The placement is statically mapped to PCIe slots, with the following mapping:

- vCon 1: Slot MLOM
- vCon 2: Slot PCIe1
- vCon 3: Slot PCIe2
- vCon 4: Slot PCIe3

This placement can be manually adjusted as needed after conversion is performed.

*9 - Supported in IMM Transition Tool, Release 1.0.2 and above.

*10 - Supported in IMM Transition Tool, Release 3.0.1 and above.

Note Table containing aliases for aliased VLANs/VSANs are not supported for conversion.

B. Fabric Interconnect (FI) Mapping for Conversion

When a Port policy is converted from UCSM to IMM, the port configuration of that policy is adjusted by mapping the unsupported FI (Cisco UCS 6200 and 6300 Series) as shown below:

Table 6: Mapping between UCSM FI and IMM FI for Port Policy Conversion

UCSM FI	Equivalent IMM FI
Cisco UCS-FI-6248UP	Cisco UCS-FI-6454
Cisco UCS-FI-6296UP	Cisco UCS-FI-6454
Cisco UCS-FI-6296	Cisco UCS-FI-64108
UCS-FI-M-6324	Cisco UCS-FI-6454
Cisco UCS-FI-6332	Cisco UCS-FI-6536
Cisco UCS-FI-6332-16UP	Cisco UCS-FI-6536
Cisco UCS-FI-6454	Cisco UCS-FI-6454
Cisco UCS-FI-64108	Cisco UCS-FI-64108
Cisco UCS-FI-6536	Cisco UCS-FI-6536

Note

- Any existing Unified Port and SAN Port configuration will be ignored when converting from a Cisco UCS 6200 Series or Cisco UCS 6300 Series FI to IMM, because the Unified Ports hardware characteristics are different.
- For the migration of Cisco UCS-FI-6332-16UP to Cisco UCS 6536, all SFP+ Ports configuration is ignored, and all QSFP+ Ports configuration is shifted to the left by 16 ports (port 1/17 on Cisco UCS-FI-6332-16UP becomes port 1/1 on Cisco UCS-FI-6536).

Appendix B: Supported Features for Cloning

Supported Features for Cloning an Intersight account

This section provides the list of UCS Server, Chassis, and Domain Policies and the list of Profiles, Pools, Resources, Settings, and Templates supported for cloning an Intersight account.

Note

- Cloning of an Intersight account is supported only for configurations in standalone mode and in Intersight Managed Mode.
- Target devices claimed in the source Intersight account are not moved to the destination Intersight account on cloning.

Table 7: Supported Features for Cloning an Intersight Account

Feature Category	Supported Feature
UCS Server Policy	Adapter Configuration
	BIOS
	Boot Order
	Certificate Management
	Device Connector
	Ethernet Adapter
	Ethernet Network
	Ethernet Network Control
	Ethernet Network Group
	Ethernet QoS
	FC Zoning
	Fibre Channel Adapter
	Fibre Channel Network
	Fibre Channel QoS
	IMC Access
	IPMI over LAN
	iSCSI Adapter
	iSCSI Boot
	iSCSI Static Target
	LAN Connectivity
	LDAP
	Local User
	Network Connectivity
	NTP
	Persistent Memory
	Power
	SAN Connectivity
	SD Card
	Serial over LAN
	SMTP
	SNMP

Feature Category	Supported Feature
	SSH
	Storage
	Syslog
	Virtual KVM
	Virtual Media
UCS Domain Policy	Flow Control
	Link Aggregation
	Link Control
	Multicast
	Port
	Switch Control
	System QoS
	VLAN
	VSAN
UCS Chassis Policy	Thermal
Pools	IP
	IQN
	MAC
	Resource
	UUID
	WWNN
	WWPN
Profiles	UCS Server Profile
	UCS Chassis Profile
	UCS Domain Profile
Templates	UCS Server Profile Template

Feature Category	Supported Feature
Access and Permissions Settings	Users *1
	Groups *1
	Roles *1
	Organizations
	Resource Groups

*1 - Cloned only when the "Trim Intersight Settings" option is not set. By default, the object is not cloned.

Note

- A self-signed certificate is generated and pushed to Intersight while cloning an Intersight account having Certificate Management policy.
- Any policy containing a password is cloned using an automatically generated password.

Appendix C: Transition Settings

(I) Transition Settings for Conversion

The following are the conversion options present in the **Transition Settings** page of the IMM Transition Tool. You can set/unset these options to control the behavior of the transition.

1. **Fabric Policies Conversion**
   - This option is enabled by default. When enabled, UCS Fabric Configuration is converted to equivalent Intersight policies.
   - If enabled, following are converted:
     - VLANs / VLAN Groups / VSANs
     - FI Ports configuration
     - UCS domain settings (NTP, DNS, Syslog, SNMP, System QoS, and Switch Control policies)

Note Fabric policy conversion is supported for UCSM only.

   a. **Fabric Policies Name**

   It denotes the name of the Fabric policies (VLAN, VSAN, Port policies) after conversion. You can either provide a **Manual** name for the converted policy or opt to retain the UCS domain name after conversion.

   b. **Target Org Name for Fabric Policies**

It denotes the name of the organization to which the fabric policy belongs. You can either provide a **Manual** name for the organization or opt to retain the UCS domain name after conversion.

c. **Always create separate VLAN Policies**

   - This option is disabled by default.
   - When enabled, separate VLAN policies are created for Fabrics A and B. If disabled, the tool determines whether to create single or separate VLAN policies for Fabrics A and B.

d. **Always create separate VSAN Policies**

   - This option is disabled by default.
   - When enabled, separate VSAN policies are created for Fabrics A and B. If disabled, the tool determines whether to create single or separate VSAN policies for Fabrics A and B.

e. **Always create separate Port Policies**

   - This option is disabled by default.
   - When enabled, separate Port policies are created for Fabrics A and B. If disabled, the tool determines whether to create single or separate Port policies for Fabrics A and B.

2. **Server Policies Conversion**

   - This option is enabled by default.
   - When enabled, selected Server policies/Pools/Profiles/Templates are converted to equivalent Intersight Policies/Pools/Profiles/Templates

a. **Service Profiles Conversion**

   - This option is enabled by default.
   - When the conversion of Service Profiles is enabled, user can select the Profiles to be converted at the **Select Profiles/Templates** step.
   - When enabled, following identifiers may not be maintained:
     - IP
     - MAC
     - IQN
     - UUID
     - WWN

b. **Global Service Profiles Conversion**

   - This option is disabled by default.
   - When enabled, selected Global Service Profiles get converted to equivalent Intersight Server Profiles.

Note
This conversion is applicable only for UCSM.

c. **Preserve Identities**

- This option is enabled by default.
- When enabled, configuration identities such as IP, IQN, MAC, UUID,WWPN, WWNN are preserved during the conversion of service profiles from UCS to IMM.

d. **Use vCon placement info for vNIC/vHBA order**

- This option is disabled by default.
- When enabled, vNICs/vHBAs get statically mapped to different PCIe slots depending on their source vCon.
- vCon any, 1: "PCIe MLOM", vCon2: "PCIe slot 1", vCon3: "PCIe slot 2" and vCon4: "PCIe slot 3".
- When disabled, all vNICs/vHBAs get mapped to PCIe slot "MLOM".

e. **Automatically change long org names (>17 chars)**

- This option is disabled by default.
- If enabled, the organization names that are longer than 17 characters are changed to automatically generated names. This prevents errors when the combined length of the organization name and QoS policies exceeds 40 characters.

f. **UCS Central Tags Conversion**

- This option is enabled by default.
- When enabled, the UCS Central tags that are assigned to pools, policies, and profiles/templates are converted and can be easily viewed in the "Converted UCS Central tags" row of the corresponding Intersight objects in the readiness report.

Note
- This conversion is applicable only for UCS Central.
- The UCS Central tag type duplicate, with varying tag values, cannot be pushed to Intersight. It is due to the fact that Intersight does not allow for duplicate tag keys. However, the first occurrence gets pushed to Intersight.

g. **UCS Central Tags Prefix**

IMM Transition Tool, Release 3.1.1, supports adding prefix to the UCS Central tags. You can either provide a **Manual** prefix for the converted tags or opt for the default prefix after conversion.

Note This conversion is applicable only for UCS Central.

3. **Automatically tag converted objects**
   - This option is enabled by default.
   - When enabled, Intersight objects are tagged with "imm_transition_version": "3.0.1", "imm_transition_name": "transition_name", "source_device":"source_device_name" .
   - New tags can be added by clicking on **+ Add new** button and entering the **key-value** pair.
   - Existing tags can be modified and deleted.
   - Tags with keys "imm_migration_version" and "imm_transition_name" cannot be modified but can be deleted.
   - Every tag should have an unique key whereas values can be duplicated.
   - Duplicate tags with same **key-value** pairs are not allowed.

4. **Overwrite existing Intersight objects**
   - This option is disabled by default.
   - When enabled, existing Intersight objects are overwritten if objects with same name and type already exist in the organization. When disabled, any existing object is not changed.

5. **Default Password for Converted Policies**

   The default password is used as a replacement for any existing password in UCS Manager/Central policies that are converted, such as Virtual Media, iSCSI Boot, IPMI over LAN. This password gets auto-generated during tool installation. This password should be reset by the user after the converted policies are pushed to Intersight.

6. **Password for iSCSI Mutual Chap Authentication**

   This password is used for Mutual CHAP Authentication in iSCSI Boot Policy. It must be different from the **Default Password for Converted Policies**.

(II) Transition Settings for Cloning

The following are the cloning options present in the **Transition Settings** page of the IMM Transition Tool. You can set/unset these options to control the behavior of the transition.

1. **Overwrite existing Intersight objects**
   - This option is disabled by default.
   - When enabled, existing objects in the destination Intersight will be overwritten, if objects with the same name and type already exist in the source org.

2. **Trim Intersight Settings**
   - This option is enabled by default.

- When enabled, some of the Intersight settings get trimmed during cloning, such as user groups, users, and roles.

3. **Preserve Identities**
   - This option is enabled by default.
   - When enabled, you can clone an Intersight account while preserving the assigned IDs on all the UCS server profiles.

(III) Default Transition Settings for Conversion

You can set a default configuration that will get applied to every new transition, created in the tool. **Default Transition Settings** option is present under **Settings** on the top-right corner. This option can also be used to set/reset the default password for converted policies.

Custom tags defined through default transition settings get applied to all the transitions.

Appendix D: Proxy Settings

The IMM Transition Tool, 3.1.1, provides the option of enabling or disabling proxy settings at the device level. You can enable/disable the proxy settings for each device individually using the **Use Proxy** toggle button. When **Use Proxy** is enabled for a device, proxy settings are used for connecting to the device.

The proxy settings can be configured in the **Proxy Settings** page.

Perform the following steps to configure the proxy settings.

1. Click **Proxy Settings** present under the gear icon on the top-right corner.
2. Enter the Proxy Hostname or IP.
3. Enter the Proxy Port number.
4. If your proxy settings require authentication, toggle **Authentication** to turn it on, else go to step 7.
5. Enter the Username.
6. Enter the Password.
7. Click **Save**.

   The proxy settings get saved.

Note

1. Any proxy setting change cannot be done if any transition is in progress.
2. **Use Proxy** toggle button can be enabled during
   - adding a device in the **Device Management** page.
   - adding a new source UCS device/Intersight account in the **Add IMM Transition** procedure.

Appendix E : Backup/Restore

IMM Transition Tool, release 3.1.1 provides the ability to backup data from the tool and restore it on the same or another instance of the tool.

Perform the following steps to backup and restore the data.

1. Click **Backup/Restore** present under the gear icon on the top-right corner.
2. Enter a Private key to encrypt the backup data.
3. Click **Download**.

   The data gets downloaded in a compressed file and gets stored on your local system.
4. Log into the instance of the tool where the data needs to be restored.
5. Click **Backup/Restore** present under the gear icon on the top-right corner.
6. Go to **Restore** tab.
7. Enter the same key that was used while taking the data backup.
8. Browse and select the downloaded file on your system that contains the backup data.
9. Click **Restore**.

   The data present in the file gets restored.

Note

- Restoring the data deletes all the existing data of the tool and replaces it with the data present in the compressed file.
- Data can only be restored from a lower version of the tool to higher and not vice-versa.
- Backup/Restore action cannot be initiated if any transition is in progress.

Appendix F : Management Operations Using CLI

(I) Edit the Advanced Configuration Settings

You can edit the `convert_options.json` file for advanced configuration settings by performing the following steps:

1. SSH to the VM.
2. Edit `~/imm-migration/config/convert/convert_options.json` file as per your requirement.

Note To know the various transition settings available in the IMM Transition tool, refer Appendix C: Transition Settings.

(II) Edit the /etc/hosts File

You can edit the `/etc/hosts` file using the `host` command.

```
hosts [options...] -- Command to update the hosts file
options:
    add :adds the host to host file
    remove :remove the host from the host file
    list :lists the host in the host file
example:
    add:     $ sudo hosts add 1.2.3.4 localhost
    remove:  $ sudo hosts remove 1.2.3.4 localhost
    list:    $ sudo hosts (or) sudo hosts list
```

(III) Change the IP Address of the IMM Transition Tool VM

Perform the following steps to change the IP address of the IMM Transition Tool VM:

1. SSH to the VM.
2. Edit `/etc/network/interfaces` file using the below command:

   ```
   $ sudo vi /etc/network/interfaces
   ```

3. Change the IP, Netmask, Gateway, and DNS fields as per your requirement.
4. Save the file.
5. Reboot the VM using the below command:

   ```
   sudo reboot
   ```

(IV) Change the Admin Password

Perform the following steps to change the password of the admin:

1. SSH to the VM.
2. Run the below command:

   ```
   sudo passwd admin
   ```

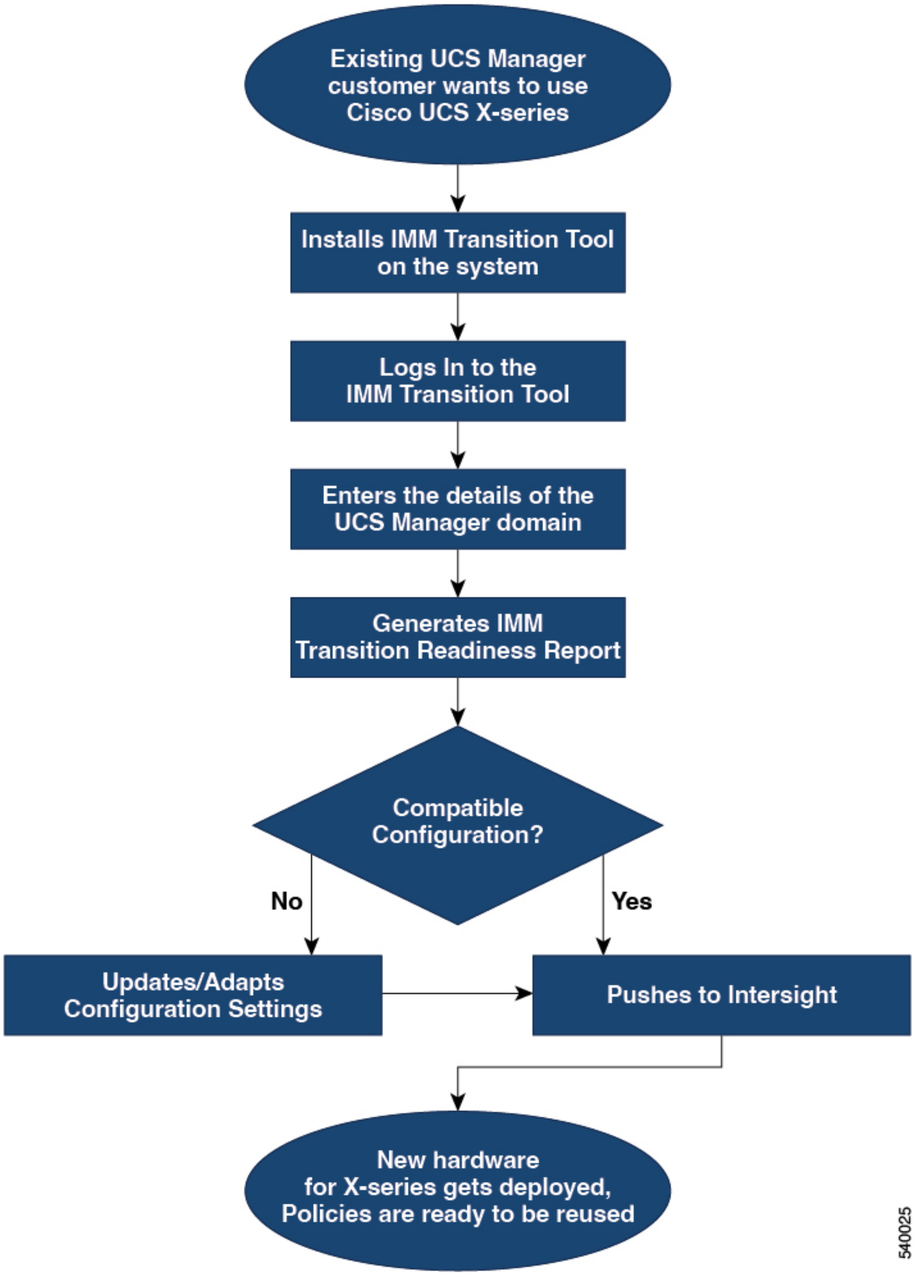
3. Enter the new password.

Appendix G: Sample Use Cases

(I) Accelerate deployments of UCS X-Series

When supporting the UCS X-Series, the fabric interconnects run in Intersight Managed Mode. If you are using Cisco UCS Manager and want to use UCS X-series, then you have to transition to IMM. This transition

- Extends existing Service Profile Templates to Intersight.
- Automatically converts related server policies such as Boot, BIOS, LAN/SAN connectivity.
- Converts fabric configuration such as VLANs/VSANs, port configuration.


Existing UCS Manager customer wants to use Cisco UCS X-series
Installs IMM Transition Tool on the system
Logs In to the IMM Transition Tool
Enters the details of the UCS Manager domain
Generates IMM Transition Readiness Report
Compatible Configuration?
No
Yes
Updates/Adapts Configuration Settings
Pushes to Intersight
New hardware for X-series gets deployed, Policies are ready to be reused
540025

Perform following steps to convert the existing UCS Manager domain objects to Intersight objects.

Before you begin

Your system must meet the prerequisites mentioned in the Prerequisites section.

Step 1 Install Cisco IMM Transition Tool in your system.

Follow the Installation procedure mentioned in Installing Cisco Intersight Managed Mode Transition Tool

Step 2 Log into the IMM Transition Tool.

Step 3 Enter the details of the UCS Manager domain.

Step 4 Generate the readiness report to check the compatibility for transition.

Step 5
a) If incompatible, update configuration settings.
b) When compatible, push the converted configuration to Intersight.

What to do next

The new hardware gets deployed. The software configuration of the UCS Manager domain, and the existing policies are ready to be reused. You can now monitor the Cisco UCS X-Series systems from anywhere and perform Policy-based management across the servers.

For the steps on performing this transition, see Adding an IMM Transition for Conversion

(II) Moving Profiles from UCSM to IMM

IP Addresses, MAC addresses, IQNs, UUIDs, WWNNs, and WWPNs are the typical identifiers that a physical server gets from a server profile. The identifiers can be reserved and referenced during conversion by a server profile. A typical use-case for reserved identifiers is ensuring WWPNs are retained during a UCSM to IMM transition, in order to maintain storage access (zoning).

The IMM Transition Tool, 3.0.1, has the ability to preserve the configuration identifiers on conversion from UCSM to IMM. With this added ability, you can now move the server profiles or migrate the physical servers from UCSM to IMM.

Note WWNN/WWPN/UUID/MAC identifiers do not show up under "Reserved Identifiers" in the Pools view, as those identifiers are allocated to the converted profiles as soon as they are created. However, IP and IQN identifiers are shown under "Reserved Identifiers" until the Server Profiles are deployed. This is because for IP and IQN identifiers, allocation is performed at Profile deployment stage, not at Profile creation. The reservations will still be honoured and the identifiers match the ones that were used in UCSM/Central once the Profiles are deployed.

Perform the following steps to move a profile from UCSM to IMM.

Before you begin

Your system must meet the prerequisites mentioned in the Prerequisites section.

Step 1 Install Cisco IMM Transition Tool in your system.

Follow the Installation procedure mentioned in Installing Cisco Intersight Managed Mode Transition Tool

Step 2 Log into the IMM Transition Tool.

Step 3 Enter the details of the source UCS device and the destination Intersight account.

Step 4 Ensure that **Preserve Identities** option is enabled on the **Transition Settings** page.

Step 5 Select the profiles that need to be converted and migrated to Intersight.

Step 6 Map the source UCSM and destination Intersight org. This step is optional.

Step 7 Generate the readiness report to check the compatibility for transition.

Step 8
a) If incompatible, update configuration settings.
b) When compatible, push the converted configuration to Intersight.

What to do next

The UCSM server profile gets converted to the IMM service profile retaining the same set of identifiers.

For the steps on performing this transition, see Adding an IMM Transition for Conversion

Appendix H: Technical Support

In case you need any assistance, you can share the logs file with the technical team.

Perform the following steps to send your query:

1. Go to the list view displaying all the transition records.
2. Scroll down to the transition record for which you need technical assistance.
3. Click **…** present against the record.
4. Click **Download Logs**.
5. Save the logs file in your computer.
6. Attach the saved logs file to the email and send the email with your queries/feedback to the imm-transition-feedback@cisco.com group.

Appendix I: Providing Feedback

Use the **Feedback** button on the top-right corner to provide feedback about the tool or information about the missing features.