



Cisco Intersight Managed Mode Transition Tool User Guide, 4.x

First Published: 2023-09-04

Last Modified: 2024-04-05

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



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](#), on page 1

New and Changed Information

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 4.1.2

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 4.1.2.

Feature	Description	Where Documented
Support for Cisco UCS M7 servers with 5th Gen Xeon scalable CPUs	IMM Transition Tool, Release 4.1.2 provides support for Cisco UCS M7 servers with 5th Gen Xeon scalable CPUs.	
Ability to add SSL certificate for the web server	IMM Transition Tool, Release 4.1.2 enables you to authenticate your secure connection to the tool. You can now upload secure sockets layer (SSL) certificate for the web server.	Certificate Settings
Ability to reset or renew the SSL certificates	You can renew or reset the CA-signed certificates through GUI and self-signed SSL certificate through a shell script.	Certificate Settings
Ability to upload the JSON configuration file and push it to Intersight	IMM Transition Tool, Release 4.1.2 introduces a new transition type "Upload Configuration + Push to Intersight". This new type reduces the steps involved in pushing your configuration to Intersight. You can now directly upload a JSON configuration file and push it to Intersight.	Adding an IMM Transition for Conversion Adding an IMM Transition to Push the Uploaded Configuration

Feature	Description	Where Documented
Ability to add an offline device to the IMM Transition Tool	You can now add a device to the IMM Transition Tool by choosing to skip the connection check between the tool and the device.	Adding Devices
Ability to upload custom file for devices	You can now upload the configuration and inventory files of a source device for working in "offline" mode. Subsequently, the tool will use these files as the source information for performing a transition instead of using live device information.	Uploading Custom Device File
Ability to view each profile's state on the Select Service Profile page	IMM Transition Tool, Release 4.1.2 shows each profile's state on the Select Service Profile page, allowing you to view and choose profiles for conversion based on their state.	Adding an IMM Transition for Conversion Adding an IMM Transition for Cloning
Support for VIC QinQ tunneling conversion and cloning	Support for VIC QinQ tunneling conversion and cloning.	Supported Features for Conversion
Support for VIC SRIOV conversion and cloning	IMM Transition Tool, Release 4.1.2 provides support for VIC SRIOV conversion and cloning.	Supported Features for Conversion
Ability to specify the domain name of the virtual machine (VM)	You can now specify the domain name of the VM during installation of the IMM Transition Tool.	Installing Cisco Intersight Managed Mode Transition Tool

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 4.1.1

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 4.1.1.

Feature	Description	Where Documented
Support for organization sharing in conversion and cloning transitions	IMM Transition Tool, Release 4.1.1 supports organization sharing in both conversion and cloning transition types. When converting a configuration, you can choose whether to leverage organization sharing in the converted configuration.	Adding an IMM Transition for Conversion, on page 23
Support for bulk claiming devices to Intersight	You can now simultaneously claim a list of devices to Intersight.	Adding Devices, on page 35

Feature	Description	Where Documented
Support for selective cloning for chassis and domain profiles	You can now select Chassis and Domain Profiles during cloning.	Adding an IMM Transition for Cloning

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 4.0.2

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 4.0.2.

Feature	Description	Where Documented
Support for conversion of Host Ports of Cisco UCS VIC 1300 Series adapters	You can now choose to use Host Port information for calculating vNIC/vHBA order.	Default Settings
Support for conversion of Service Profile Power Settings	IMM Transition Tool, Release 4.0.2 supports conversion of <i>Power Control Policy</i> and <i>Power Restore</i> settings to a <i>Power Policy</i> in Intersight Managed Mode Cisco UCS B-Series and Cisco UCS X-Series servers.	Default Settings
Ability to Display Disk Utilization in the Software Repository Page	You can now view the disk utilization in the Software Repository page.	Software Repository

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 4.0.1

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 4.0.1

Feature	Description	Where Documented
Change in the Operating System	The underlying operating system of the tool has changed from Ubuntu 18.04 to Ubuntu 22.04. Therefore, if you are an existing user using IMM Transition Tool, Release 3.1.1, you must backup data from the existing version of the tool, install the new ova file, and restore the data on the latest version of the tool.	Upgrading Cisco Intersight Manged Mode Tool

Feature	Description	Where Documented
Support for Software Repository	IMM Transition Tool, Release 4.0.1 includes a Software Repository feature, which allows you to host your ISO images or firmware packages. You can then leverage this to easily perform Operating System installations or firmware upgrades on your UCS servers.	Software Repository
Support for the New Intersight European Region	IMM Transition Tool, Release 4.0.1 supports US and EU regions for Intersight SaaS devices.	Adding an IMM Transition for Conversion Adding an IMM Transition for Cloning Device Management
Ability to Perform Selective Cloning	IMM Transition Tool, Release 4.0.1 provides the ability to select the Server Profiles/Templates of the transition that need to be cloned.	Adding an IMM Transition for Cloning
Ability to Preserve Service Profile Associations During Conversion	You can now choose to pre-assign each converted Server Profile to the same server serial number as the one it was assigned to in UCS Manager/Central.	Default Settings
Ability to Preserve Server Profile Associations During Cloning	You can now choose to pre-assign each cloned Server Profile to the same server serial number as the one it was assigned to in the source Intersight device.	Default Settings
Ability to Preserve Chassis/Rack Server IDs During Conversion	You can now choose to preserve the chassis/rack server IDs to the same server ports as what was defined in UCS Manager.	Default Settings
Ability to Customize the vCon to PCIe slots Mapping	You can now override the default mapping and manually provide the corresponding PCIe slot number for each source vCon value in a conversion.	Default Settings
Support for Additional Policies Such as Drive Security and Firmware Policies	IMM Transition Tool, Release 4.0.1 supports additional policies for conversion and cloning.	Supported Features



CHAPTER 2

Overview

- [Overview, on page 5](#)

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 later, 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.

With IMM Transition Tool, Release 4.0.1 onwards, you can use the Software Repository feature to install operating system and upgrade firmware on your servers.

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 and later, 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.

From IMM Transition Tool, 3.1.1 onwards, you can clone an Intersight account while preserving the assigned IDs on all the UCS server profiles.

From IMM Transition Tool, 4.0.1 onwards, you can perform selective cloning by choosing the Server Profiles to clone between Intersight accounts.

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

IMM Transition Tool, Release 3.0.1 and later, 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).

8. Using the Tool as a software repository

IMM Transition Tool, Release 4.0.1 and later, includes a Software Repository feature, which allows you to host your ISO images or firmware packages. You can then leverage this to easily perform Operating System installations or firmware upgrades on your UCS servers.



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

Prerequisites

- [Prerequisites, on page 9](#)

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
 - Extra 10GB to 5000GB (with default of 100GB) for the Software Repository feature
- 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.
- Accessing the Software Repository requires HTTPS (TCP port 443) connectivity to be open.
To use with Cisco UCS servers and Intersight OS Install, ensure that the connectivity between the CIMC IPs of the UCS servers and the IMM Transition Tool VM is open.



CHAPTER 4

Installing Cisco Intersight Managed Mode Transition Tool

- [Installing Cisco Intersight Managed Mode Transition Tool, on page 11](#)

Installing Cisco Intersight Managed Mode Transition Tool

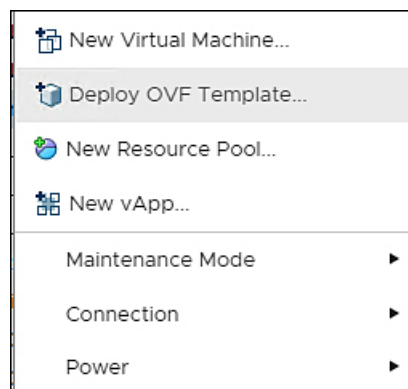
Before you begin:

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.

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.

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 [Backup/Restore](#).

1. Log into the HTML5 vSphere Web Client and go to the **VMs** tab.
2. Add the **Deploy OVF Template** action button via the *Actions* dropdown list.



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

A new window appears, asking to select a template.

4. Click **Choose Files**, select the downloaded OVA file.
5. Click **Next**.
6. Select the location where you want to deploy the virtual appliance, click **Next**.
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

Server [REDACTED]

- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]
- > [REDACTED]

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Review the package details, that contain advanced configuration options.

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 Select networks
- 7 Customize template
- 8 Ready to complete

Review details
Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	IMM Transition Tool
Vendor	Cisco
Download size	2.4 GB
Size on disk	5.5 GB (thin provisioned)
	200.0 GB (thick provisioned)
Extra configuration	nvrnm = IMM-Transition-4.0.2.nvrnm

CANCEL BACK NEXT

8. Click **Next** to accept these options.
9. Select the desired storage location from the list of datastores, 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 Select networks
- 7 Customize template
- 8 Ready to complete

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	Type
██████████	92.5 GB	973 MB	91.55 GB	VM
██████████	1.5 TB	1 TB	509.62 GB	VM
██████████	1.5 TB	1.28 TB	264.34 GB	VM

Compatibility

✓ Compatibility checks succeeded.

[CANCEL](#) [BACK](#) [NEXT](#)

10. Select a destination network from the dropdown list for each source network, 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 Select networks
- 7 Customize template
- 8 Ready to complete

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

CANCEL
BACK
NEXT

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

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 Select networks
- 7 Customize template
- 8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

General 2 settings

Hostname Enter the hostname (default: imm-transition) for the VM.

Domain Name Enter the domain name for the VM (e.g. cisco.com). Has to be set if you want to replace the self-signed certificate.

Network 6 settings

Public Network Type

Public Network IP

Public Network Netmask

Public Network Gateway

CANCEL
BACK
NEXT

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

**Note**

- You should change the password for the converted policies after those are pushed to Intersight.
- It is mandatory to enter the NTP field. The default value is *ntp.ubuntu.com*
- Software Repository Disk Size should have a minimum value of *10* and a maximum value of *5000*.

12. Click **Next**.
13. Review the configuration data.
14. Click **Finish**.

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 Select networks
- ✓ 7 Customize template
- 8 Ready to complete

Provisioning type	Deploy from template
Name	IMM-Transition-4.0.2-sampleee
Template name	IMM-Transition-4.0.2
Download size	2.4 GB
Size on disk	200.0 GB
Folder	ucs507-dc
Resource	[REDACTED]
Storage mapping	1
All disks	Datstore: perf-ds; Format: Thick provision lazy zeroed
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual
Properties	Hostname = Public Network Type = STATIC Public Network IP = Public Network Netmask =

CANCEL BACK FINISH

The system will import and deploy the file.

15. Click the **Refresh** button to update the system.
The VM will be visible in the center windowpane.
16. Select the VM and click **Power On**.
17. 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.



CHAPTER 5

Upgrading Cisco Intersight Managed Mode Tool

- [Upgrading Cisco Intersight Managed Mode Transition Tool, on page 19](#)

Upgrading Cisco Intersight Managed Mode Transition Tool

Upgrading 4.x Releases

Use one of the following options to upgrade the tool across 4.x releases:

- Use the CLI to upgrade the tool:
 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:

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

Enter the administrator password when prompted.

This will take few minutes to complete.

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

```
The log messages of the upgrade should be:
Have you taken a snapshot of the VM? (y/n) : y
Enter '[admin]' Password:
INFO: Password is correct. Continuing...
INFO: File format validation success
INFO: Successfully verified the authenticity of upgrade_file.
INFO: Version validation success
INFO: Upgrading... May take a few minutes
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.

- Alternatively, deploy a new OVA and perform a Backup/Restore operation as outlined in the **Upgrading from 3.x to 4.x** section.

Upgrading from 3.x to 4.x

Perform the following steps to upgrade the tool from 3.x to 4.x:

1. Take a backup of the data before starting the upgrade. For more details, see [Backup/Restore](#).
2. Download the IMM Transition Tool .ova file to your computer.
3. Deploy the .ova file. For more details, see [Installing Cisco Intersight Managed Mode Transition Tool](#).
4. Restore the data on the new instance of the tool. For more details, see [Backup/Restore](#).



CHAPTER 6

Accessing the Intersight Managed Mode Transition Tool

- [Accessing the Intersight Managed Mode Transition Tool, on page 21](#)

Accessing the Intersight Managed Mode Transition Tool

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.

1. Launch a Web browser window.
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`.
3. In the Login dialog box, enter the user name and password.



Note User name: admin
Password: Enter the password set on the Customize template page during installation.

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 7

Transition

- [Adding an IMM Transition for Conversion, on page 23](#)
- [Adding an IMM Transition for Cloning, on page 28](#)
- [Adding an IMM Transition to Push the Uploaded Configuration, on page 31](#)
- [Transition Management, on page 32](#)
- [Interpreting Transition Readiness Report, on page 33](#)

Adding an IMM Transition for Conversion

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 Settings](#).

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

Perform the following steps to start with the IMM transition:

1. Click **Add IMM Transition**.
2. Enter a name for the Transition.
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](#).
 - (d) Select **Upload Configuration + Push to Intersight** if you want to directly upload a JSON configuration file and push it to Intersight. For the detailed procedure, refer [Adding an IMM Transition to Push the Uploaded Configuration](#).
4. Click **Next**.
5. Select the Source Device - UCS Manager or UCS Central.
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 Domain 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 [Proxy Settings](#).

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.



Note

- While adding a transition, the configuration/inventory fetched from a live device is represented by , and the configuration/inventory fetched from a file (manually uploaded by user) is denoted by  on the **Select Source UCS/Intersight Device** page.
 - For more details, see [Uploading Custom Device File](#).
 - In case an error occurs, you can enable the **Force Fetch** toggle button to allow the tool to ignore the failed objects and proceed to fetch the configurations of the remaining devices.
-

8. Click **Next**.
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 10.



Note

From release 4.0.1 onwards, If you select **SaaS Intersight** account, you can also select the region to which the account belongs: **US** or **EU**.

- (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.

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.

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.
12. Click **Next**.
13. Configure the conversion options that you want for the transition.
 - For details on each of the Transition Settings field, refer **B. Transition Settings for Conversion** section in [Default Settings](#).
 - For defining a default set of configurations for every new transition that you create, refer **A. Default Transition Settings for Conversions** section in [Default Settings](#).
14. Click **Next**.
15. Select the Service Profiles/Templates that need to be converted.

Next to the profile name, profile state and association details with the physical server can be viewed.

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

You can apply a filter to only view the Templates, or Org, Profile, and Template in the **Show** drop-down list, located beside the search bar.



Note The system displays a warning for profiles in states such as pending reboot, configuration failure, or other invalid conditions, which could lead to a misconfigured setup.

16. Click **Next**.

17. Configure the mapping of converted objects from UCSM to Intersight.

The **Advanced Organization Mapping** option can help map single or multiple UCS org(s) to an Intersight Org. Do one of the following:

- Turn on **Advanced Organization Mapping**:
 - a. To add a new Destination Intersight Org, click **Add New**.
 - b. From the list of UCS Orgs, select one or more UCS Orgs and map it to a Destination Org in Intersight.
 - c. To configure a Destination Org as a Shared Org, select the **Share with Other Organizations** checkbox, and then click **Share**.

In this case, the UCS Orgs mapped to the Shared Intersight Destination Org will share the same Resources.



Note To maintain a similar resource inheritance as in Cisco UCSM/Central, you need to map the Root and Parent Orgs with a Shared Intersight Destination Org, and then map the Sub-orgs to the non shared Intersight Destination Orgs.



Note We can not have the same inheritance as in UCSM/Central because Intersight does not support transitive sharing.

Consider the scenario in UCSM with orgs: root, root/Org1, root/Org1/Org2. In UCSM, Org2 can inherit resources from both Org1 and root, while Org1 inherits resources from root. However, replicating the same inheritance structure in Intersight is not feasible due to the absence of transitive sharing.

In Intersight, sharing root with Org1 creates a constraint—Org1 cannot be a shared org. This is because, in Intersight, a sub-org (an Org to which a parent org is shared) cannot itself be a shared org. This distinction necessitates a thoughtful approach when translating UCSM inheritance structures to Intersight.

- Turn off **Advanced Organization Mapping**
 - a. To manually enter the name of the Destination Intersight Org, enter a Root Org name and go to Step 21.
Unlike the same name mapping behavior, customized mapping avoids creating multiple Intersight Orgs for an account.
 - b. To retain the Source UCS Org name in the Destination Intersight Org, turn on **Keep source Org path in Intersight Org name**.



Note If **Keep source Org path in Intersight Org name** 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.

- c. To configure all Sub-orgs to share resources with the Root Org, turn on the **Share Root with Sub-orgs** option.

If this option is disabled, the resources present in the Root Org that are used by profiles or templates in sub-orgs will be cloned to each corresponding converted Org.

18. Click Map Now.

When the Source Org and Destination Org mapping is complete, a **Mapped** tag is displayed next to the Destination Intersight Org. You can also review the mapped Source Orgs in the **Mapping** section present at the bottom of the **Advanced Organization Mapping** page.

You can use the **Un-Map All** option to unmap 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 the three-dot menu against it, and selecting the unmap option.

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).

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

For details on interpreting the report, refer [Interpreting Transition Readiness Report](#).

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](#).

21. Click Next.

Push to Intersight page appears.



Note In case an error occurs, you can enable the **Force Push** toggle button to allow the tool to ignore the failed objects and proceed to push the configurations to Intersight.

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**.

22. Click **Advanced Options**, browse to the edited file, and click **Upload**.

The uploaded file is used for pushing the configuration to Intersight.

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 policies if those have been pushed to Intersight.
-

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 the three-dot menu (...) 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 the three-dot menu present next to the object status to know the reason for push failure.

Adding an IMM Transition for Cloning

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

1. Click **Add IMM Transition**.
2. Enter a name for the Transition.
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 [Supported Features for Cloning](#).



4. Click **Next**.
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 [Proxy Settings](#).



Note

- While adding a transition, the configuration/inventory fetched from a live device is represented by , and the configuration/inventory fetched from a file (manually uploaded by user) is denoted by  on the **Select Source UCS/Intersight Device** page.
For more details, see [Uploading Custom Device File](#).
 - In case an error occurs, you can enable the Force Fetch toggle button to allow the tool to ignore the failed objects and proceed to fetch the configurations of the remaining devices.
-

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 10.
- (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 8. Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer [Proxy Settings](#).



Note

From release 4.0.1 onwards, If you select **SaaS Intersight** account, you can also select the region to which the account belongs: **US** or **EU**.

7. Click **Refresh** to retrieve the latest configuration from the existing Intersight account and then go to step 10.

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.

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

- Log into the Intersight application.
- On the top-right corner, click on the Gear icon and select **Settings**.
- Under the **API** section, click **API Keys**.
- On the top-right of the page, click **Generate API Keys**.
- Enter a name in the **Description** field and select **API Key for OpenAPI Schema Version 2 or Version 3**.
- 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.

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.
10. Click **Next**.
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 **C. Transition Settings for Cloning** section in [Default Settings](#).
12. Click **Next**.
13. Select the Server Profiles/Templates, Chassis Profile, or Domain Profile that need to be converted.
 - Next to the profile name, profile state and association details with the physical server can be viewed.
 - You can search for a specific Profile/Template using the search bar located on the top.
 - You can apply a filter to only view the Templates, or Org, Profile, and Template in the **Show** drop-down list, located beside the search bar.
 - If you disable the button, all the Server Profiles, Templates, and their associated policies get cloned.



-
- Note**
- With IMM Transition Tool, Release 4.0.1 you can select the specific Server Profiles that need to be cloned.
 - With IMM Transition Tool, Release 4.1.1, you can select the specific Server, Chassis, and Domain Profiles that need to be cloned. The associated policies and templates will also get cloned automatically.
 - The system displays a warning for profiles in states such as pending reboot, configuration failure, or other invalid conditions, which could lead to a misconfigured setup.
-

14. Click **Next**.
Push to Intersight page appears.



-
- Note** In case an error occurs, you can enable the **Force Push** toggle button to allow the tool to ignore the failed objects and proceed to push the configurations to Intersight.
-

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**.

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

16. Click **Next**.

A connection with Intersight is established, the converted config attributes get pushed to Intersight.

17. 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 to Push the Uploaded Configuration

Perform the following steps to directly upload the JSON configuration file and push it to Intersight account:

1. Click **Add IMM Transition**.
2. Enter a name for the Transition.
3. Select **Upload Configuration + Push to Intersight** to upload a JSON configuration file and push it to Intersight.
4. Click **Next**.
5. Select the destination Intersight Account.
 - (a) Select **Choose from existing account** option, in case you want to upload the configuration to an existing Intersight account and then go to step 8.
 - (b) Select **Add new account** option, in case you want to upload the configuration to a new **SaaS Intersight** or a new **Intersight Appliance VM** account.
6. 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.

7. 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.
8. Click **Next**.
Push to Intersight page appears.



Note In case an error occurs, you can enable the **Force Push** toggle button to allow the tool to ignore the failed objects and proceed to push the configurations to Intersight.

9. Click **Browse** to select the JSON configuration file.
10. Click **Upload**.
 The uploaded file is used for pushing the configuration to Intersight.
11. Click **Next**.
 A connection with Intersight is established, the uploaded config attributes get pushed to Intersight.
12. 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.

- Click **Report** to view the readiness report for the transition.
 This option is not available for cancelled and failed transitions.
- Click **Edit** to change the transition name.
- 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.

- Click **Clone** to copy the existing transition config.
 - (a) Provide a name for the transition. It appears in the listing page with status as *Incomplete*.
 - (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**.

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

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.



CHAPTER 8

Device Management

- [Adding Devices, on page 35](#)
- [Claiming Devices, on page 36](#)
- [Uploading Custom Device File, on page 37](#)

Adding Devices

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 devices.

1. Navigate to **Device Management**.
2. To add a single device:
 - a. Click **Add Device**.
 - b. Select the **Device Type** from the drop-down.
 - c. Enter the Target IP/FQDN.
 - d. If the **Device Type** selected in Step 3 is **Cisco IMC**, **UCS Manager** or **UCS Central**, enter the **Username** for the device else go to Step 7.
 - e. Enter the **Password** for the device and go to Step 9.
 - f. If the Device Type selected in Step 3 is **Intersight**:
 - (a) Select **Intersight SaaS** for a SaaS account and enter the API key/ Secret key.



Note From release 4.0.1 onwards, if you select **Intersight SaaS** account, you can also select the region to which the account belongs: **US** or **EU**.

- (b) Select **Intersight Appliance VM** for an appliance account and enter the Target/ API Key/Secret Key.
- g. Turn on the **Use Proxy** toggle button to enable proxy settings.
For more details on proxy settings, see [Proxy Settings](#)

- h. Turn on the **Bypass Connection Check** to bypass connection checks during device addition. This feature enables addition of offline devices to the transition tool.
3. To bulk add multiple devices:
 - a. Click **Upload CSV**.
 - b. Browse to a CSV file that contains the device type, target, username, and password details.

Sample CSV File

Device Type	Target	Username	Password
ucsm	192.0.2.1	admin	wiwdyh49
ucsc	192.0.2.20	admin	0un58gvb
cimc	192.0.2.78	admin	yebduskk

- c. Click **Upload**.

The **Progress** page indicates the progress of the device connections. If a connection fails, that device will not be added.

4. 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.

This option enables you to add a device which has an unsupported firmware version.

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.

Claiming Devices

To claim devices in Intersight:

1. Click **Claim to Intersight**.
2. In the **Select Devices** screen:
 - a. From the **Select Intersight Device** drop-down list, choose a target Intersight account to which you want to claim the devices.

- b. From the Table view, select the **Cisco IMC** or **UCS Manager** devices that you want to claim. If you want to add a new device, follow the steps in the **Adding Devices** section.
 - c. Click **Next**.
 3. In the **Device Connector** screen:
 - a. Enter the Access mode.
 - b. Enter the proxy details, used by the selected devices to connected to the Intersight account.



Note These options can also be configured from the Device Connector page of the UCSM or Cisco IMC devices.

- c. Click **Next**.
 - The configured settings will be pushed to the selected devices.
 - d. Monitor the progress of the claiming action from the **Progress** screen.

In the list view, devices that have been successfully claimed are indicated by a **Cloud** icon. You can hover over the **Cloud** icon to view additional information about the Intersight account linked to the claimed device.



Uploading Custom Device File

You can edit and upload a configuration or an inventory file for a device. This uploaded file can later be used while adding, cloning or pushing transitions to Intersight.

To add a custom file for a device:

1. Navigate to **Device Management**.
2. On the listing page, go to the device whose configuration or inventory needs to be updated.
3. Click the three-dot menu present against the device name.
4. Click **Upload Custom File**.
5. Browse and select the updated configuration file.
6. Click **Upload**.
7. Browse and select the updated inventory file.
8. Click **Upload**.
9. Click **OK**.

The uploaded file will get fetched next time the device is selected on the source or destination device pages while adding transitions.

While adding a transition, the configuration/inventory fetched from a live device is represented by , and the configuration/inventory fetched from a file (manually uploaded by user) is denoted by  on the **Select Source UCS/Intersight Device** page.



CHAPTER 9

Software Repository

- [Overview](#), on page 39
- [Creating Folders and Uploading Files](#), on page 39
- [Managing Folders](#), on page 41
- [Managing Files](#), on page 42

Overview

You can use the tool as a software repository to manage and host your Operating System images (ISO), Firmware packages, Server Configuration Utility (SCU) packages, OS configuration files. You can sync these images with Intersight, to make them available on Intersight.

You can create new folders, upload or download files in the software repository. For more information, refer to the following sections:

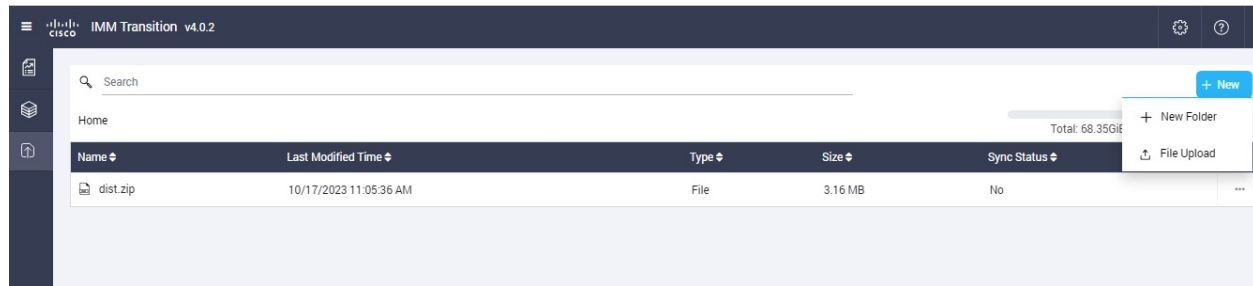
- [Creating Folders and Uploading Files](#)
- [Managing Folders](#)
- [Managing Files](#)

Creating Folders and Uploading Files

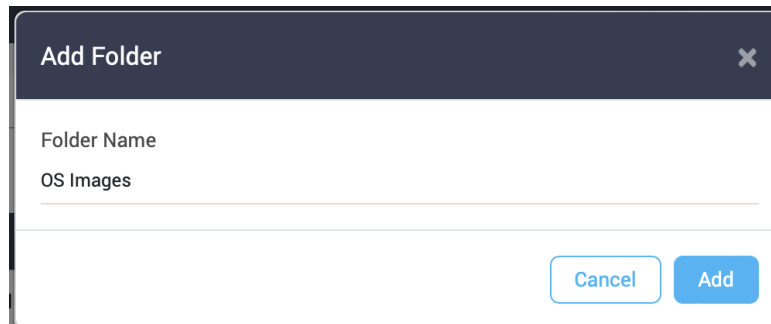
Adding Folder

You can group the iso files as per the requirement and keep them in separate folders. New folders can be created in the Software Repository of the IMM Transition Tool as described below:

1. Navigate to **Software Repository**.
2. Click **New** as shown in the screenshot below:



3. Click **New Folder**.
4. Enter a name for the folder.



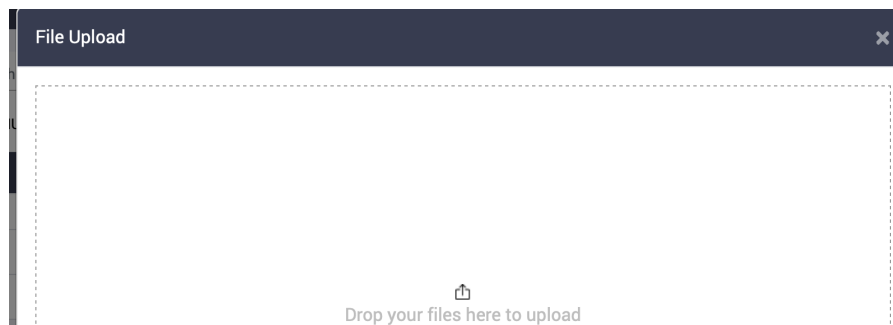
5. Click **Add**.
New folder gets created.

Uploading File

Perform the following steps to upload an iso file in the software repository.

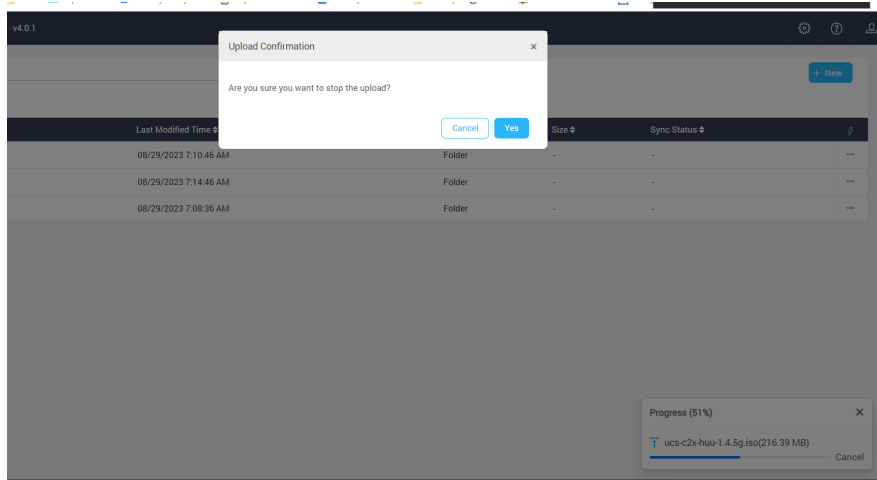
1. Navigate to **Software Repository**.
2. Click **New** as shown in the screenshot below:
3. Click **File Upload**.

File browse window appears.



4. Drop file from your local system.
5. Click **Upload**.

File gets uploaded to the software repository.



Note If you click **Cancel** in the Progress pop-up window, a confirmation dialog box appears. Click **Yes** to cancel the file **Upload** operation.

Managing Folders

The listing page on the **Software Repository** tab displays the list of folders and files that do not belong to any folder. You can manage the folders by renaming, moving, or deleting folder.

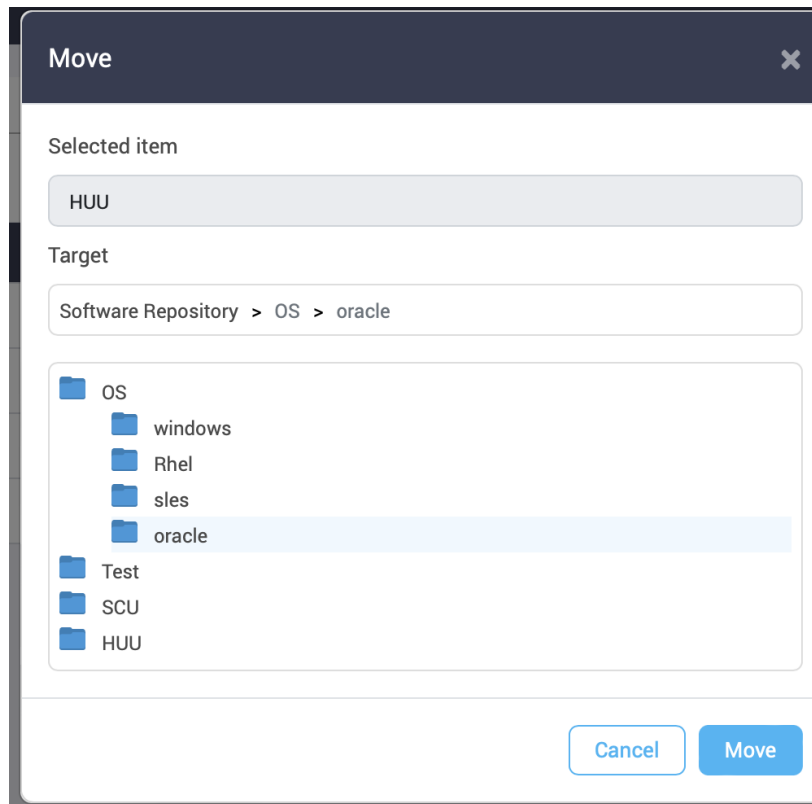
You can perform the following actions to manage the folders from the **Software Repository** listing page:

- Click **...** present besides the folder row that you want to manage.

Name	Last Modified Time	Type	Size	Sync Status	
OS	08/21/2023 5:27:03 PM	Folder	-	-	
Test	08/22/2023 12:37:21 PM	Folder	-	-	Rename
SCU	08/22/2023 1:48:51 PM	Folder	-	-	Move Delete

- Click **Rename** if you want to rename the folder.
 1. A pop-up window appears.
 2. Enter the new name for the folder.
 3. Click **Save**.
- Click **Move** if you want to move the folder inside some other folder.
 1. A pop-up window appears.

- Click on the folder into which the current folder needs to be moved.



- Click **Move**.

- Click **Delete** if you want to delete the folder from the repository.


Note

- When a folder is renamed, any external link to the files in this folder will need to be updated.
- When a folder is moved or deleted:
 - Any external link to the files in this folder will need to be updated.
 - Sync to Intersight** action will be disabled for all the files in this folder.
 - All the calculated checksums of files in this folder will be lost.

Managing Files

The uploaded iso file in the software repository can be viewed on the listing page if it does not belong to any specific folder or inside the specific folder into which it has been uploaded.

Perform the following steps to manage the files in the software repository.

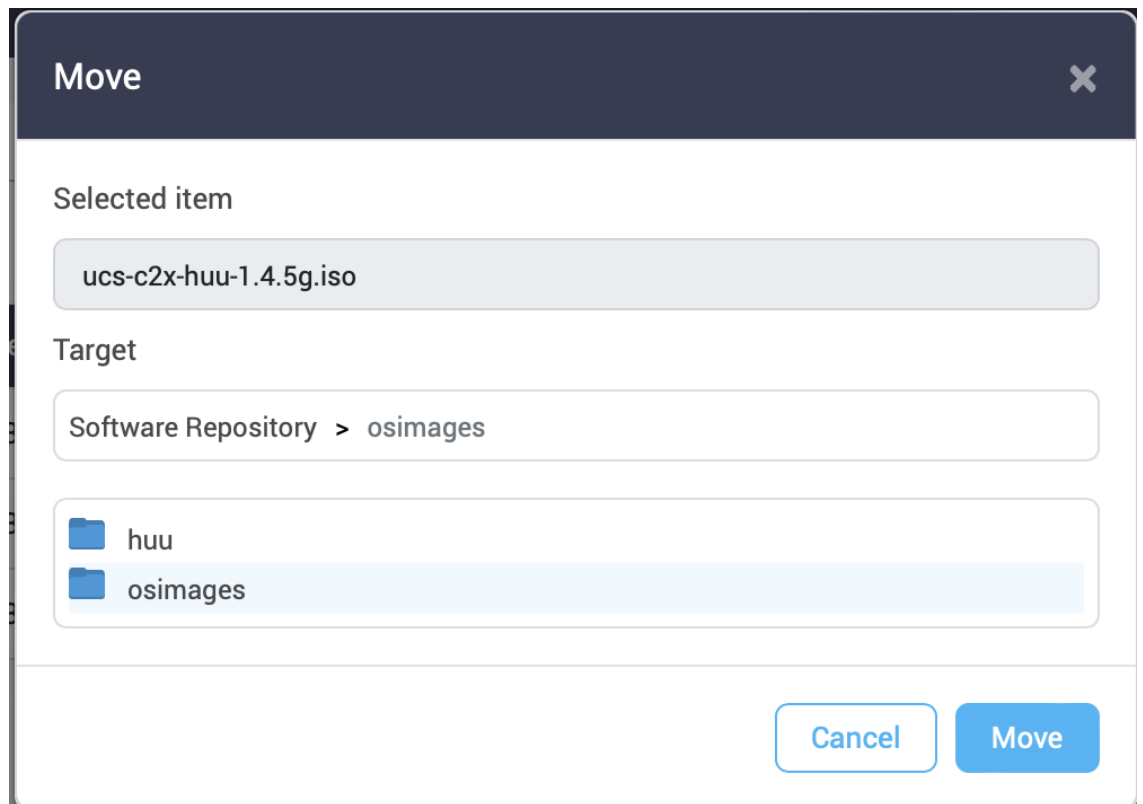
1. Navigate to the folder where the file is present.
2. Click ... present at the end of the file record that you want to manage.

For renaming a file:

- 1. Click **Rename**.
A pop-up window appears.
- 2. Enter the new name for the file.
- 3. Click **Save**.

For moving a file:

- 1. Click **Move**.
A pop-up window appears.
- 2. Click on the folder into which the file needs to be moved.



3. Click **Move**.

For deleting a file:

- Click **Delete**.

For sharing the file location with another tool:

- 1. Click **Share Link**.

A pop-up window appears

- 2. Click **Copy**.

The file location gets copied to the clipboard and can be used as required.

For calculating the checksum of the file:

- 1. Click **Checksum**.

File Checksums pop-up window appears.

- 2. Click **Calculate Checksums**.

The checksum value gets displayed.

File Checksums ✕

File Name : ucs-c2x-huu-1.4.5g.iso

md5

0fdd365fa8553034b217e328cb2d337a Copy

sha1

0247c97c0bce3746e7eb8cca66be3a0ab3ec0299 Copy

sha256

f1acedf649bc654e20d8844fef5c84d7662589b02199982a14846beff2 Copy

Calculate Checksums

For syncing the file to Intersight:

- Click **Sync to Intersight**.

For more information, see [Syncing File to Intersight](#).



-
- Note**
- When a file is renamed, any external link to the file will need to be updated.
 - When a file is moved or deleted:
 - Any external link to the file will need to be updated.
 - **Sync to Intersight** action will be disabled for such a file.
 - All the calculated checksums of the file will be lost.
-

For creating a vMedia Policy:

- Click **Create vMedia Policy**.

For more information, see [Creating vMedia Policy](#).

For downloading the file:

- Click **Download**.

The file gets downloaded to your computer from the Software Repository automatically.

Syncing File to Intersight

Any uploaded iso file in the software repository of the IMM Transition Tool can be synced to Intersight software repository by performing the following steps.

1. Navigate to the folder where the file is present.
2. Click ... present at the end of the file record that you want to sync.
3. Click **Sync to Intersight**.
A pop-up window appears.
4. Select the Intersight Device from the list of available devices.



-
- Note** It is recommended to click **Fetch OS/Firmware data** periodically. This ensures that all the latest OS and Firmware data are fetched from the Intersight account.
-

5. Select the Organization in which to store the Software Repository Link.
6. Select the Image type for the file manually if the auto-selected value is wrong, or if the tool is not able to auto-detect the file type.
7. Set or change the details for the OS image if the auto-selected value is wrong, or if the tool is not able to auto-detect the file type.
8. Click **Submit**.

The image gets synced to Intersight and appears in the **Firmware Links**, **OS Image Links**, **SCU Links**, or **OS Configuration Files** tab of **System > Software Repository** on the Intersight GUI.



Note Every time a file/folder is moved, the Software Repository link does not get automatically updated. You will have to manually remove the link and perform a **Sync to Intersight** again.

Creating vMedia Policy

You can create an Intersight vMedia Policy from a hosted ISO file in the Software Repository:

To create a vMedia Policy:

1. Navigate to the **Software Repository** page.
2. Click ... next to the ISO file that you want to use to create the vMedia policy, and then choose **Create vMedia Policy** from the drop-down list.

The **Create vMedia Policy** dialog box appears.

3. Select the Intersight Device from the list of available devices.
Note: It is recommended to click **Fetch OS/Firmware data** periodically. This ensures that all the latest OS and Firmware data are fetched from the Intersight account.
4. Select the Organization in which to store the Software Repository Link.
5. Enter a name for the policy.
6. [Optional] Enter a short description for the policy.
7. [Optional] Enter a tag in the key value format.
8. Turn on the **Enable Low Power USB** button to show the virtual drives on the boot selection menu after mapping the image and rebooting the host. This property is enabled by default.
9. Turn on the **Enable Virtual Encryption** button to enable encryption of the virtual media communications. This property is disabled by default.
10. By default, the vMedia mount name is set to the name of the ISO file used to create the vMedia Policy. You can modify the name if you want to.
11. Click **Submit**.



CHAPTER 10

Settings

- [Default Settings](#), on page 47
- [Proxy Settings](#), on page 52
- [Backup/Restore](#) , on page 53
- [Certificate Settings](#), on page 54

Default Settings

A. Default Transition Settings

You can set a default configuration that will get applied to every new transition, created in the tool. **Default 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.

For details on each of the settings field, refer the **Transition Settings for Conversion** and **Transition Settings for Cloning** sections below.

B. 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.

f. Preserve Chassis/Rack Server IDs

- This option is disabled by default.
- When enabled, the chassis/rack server IDs are preserved to the same server ports after transition as the one used in UCSM/Central.

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. Root Org Name

- You can manually enter the name of the Intersight Organization to which the UCS Org will get mapped.
- or opt for the default UCS Domain name for the destination Intersight Organization.

e. Keep source Org path in Intersight Org name

- This option is enabled by default.
- When enabled, the UCS org "root/Org1/Org2" is named as "Org1_Org2" in the destination Intersight org.
- When disabled, the UCS org "root/Org1/Org2" is named as "Org2" in the destination Intersight org.

f. 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".
- You can manually map the vCons to the PCIe slots by providing inputs and overwriting the default mapping.

The supported range for vCon slot value is : 1-15.

- When disabled, the vNICs/vHBAs are configured with Auto PCIe Slot, which will resolve to the first VIC adapter.

g. Use Host Port info for vNIC/vHBA order (use only for VIC1300):

- This option is disabled by default.
- When enabled, vNICs/vHBAs are placed on two PCI Links corresponding to the source Admin Host Port values. This should only be used if the converted profile are assigned to a server with a VIC 1300 model.
- When disabled, all vNICs/vHBAs are mapped to a single PCI Link.

h. 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.

i. Convert Power Policies (Disable it for C-series server)

- This option is disabled by default.
- Power Policy is now supported on Cisco UCS B-Series and Cisco UCS X-Series servers but remains unsupported on Cisco UCS C-Series servers. Enable this option only when converting profiles assigned to Cisco UCS B-Series and Cisco UCS X-Series servers.

j. 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.
-

k. 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.

l. Preserve Service Profile Associations

- This option is disabled by default.
- When enabled, Server Profiles are pre-assigned to the same server serial number after transition as the one used in UCSM/Central.

3. Automatically tag converted objects

- This option is enabled by default.
- When enabled, Intersight objects are tagged with "imm_migration_version": "4.0.1" and "imm_transition_name": "_imm_transition_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. Delete Resource Group Memberships For Shared Orgs

- This option is disabled by default.
Conversion and cloning of shared organizations is now supported.
- Resource group membership to shared organizations is not supported.
- When enabled, existing resource group memberships of an organization in Intersight are deleted if the same organization becomes a shared organization after conversion. Disabling this option will result in failures during pushing of the shared organization because Intersight does not support resource group mapping with a shared organization.

6. 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.

7. 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**.

C. 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.

4. Preserve Server Profile Associations

- This option is disabled by default.
- When enabled, the Server Profiles associations are preserved while cloning.

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.
-

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.
-

Certificate Settings

IMM Transition Tool, Release 4.1.2 allows you to authenticate your secure connection to the tool. You can now create and upload Certificate Authority (CA)-signed secure sockets layer (SSL) certificate for the web server. You can also reset or renew this certificate.

Creating and Uploading Certificate

Perform the following steps to create and upload a CA-signed SSL certificate:

- Click **Certificate Settings** present under the gear icon on the top-right corner.
- Create a certificate signing request (CSR) by filling up the fields below:
 1. **Organization:** Enter the name of your organization
 2. **Organization Unit:** Enter the name of the division of your organization that handles the certificate
 3. **Locality:** Enter the name of the city where the organization is located.
 4. **State:** Enter the name of the state where the organization is located.
 5. **Country:** Enter the name of the country where the organization is located.
 6. **Email Address:** Enter the email id of your organization.
 7. **Modulus:** Enter the length of the RSA key (in bits) for both private and public keys.
 8. Click **Create CSR**.
- Download the created CSR and use it to obtain a signed SSL certificate from the CA.
- Navigate to the **Apply Certificate** tab, once you have the signed certificate.
- Browse and upload the signed certificate.
- Click **Apply Certificate**.

The certificate will get applied to the IMM Transition Tool.



Note To generate a Certificate Signing Request (CSR) successfully:

1. Ensure that the virtual machine (VM) has a valid Fully Qualified Domain Name (FQDN).
 2. Set the FQDN using the following command:

```
sudo hostname --fqdn <fqdn>
```
 3. Replace <fqdn> with the desired FQDN for the VM.
-

Renewing Certificate

Perform the following steps to reset or renew the SSL certificate:

- Click **Certificate Settings** present under the gear icon on the top-right corner.

- Create a CSR using the steps mentioned in the Creating and Uploading Certificate section.
- Get the SSL certificate signed from the Certificate Authority (CA)



Note If you want to renew the self-signed certificate, follow the CLI commands as mentioned in [Appendix A : Management Operations Using CLI](#)

- Navigate to the **Apply Certificate** tab, once you have the CA-signed certificate.
- Browse and upload the signed certificate.
- Click **Apply Certificate**.



CHAPTER 11

Conversion Assumptions

- [Converting UCS Manager/Central Configuration, on page 57](#)

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**.



CHAPTER 12

Supported Features

- [Supported Features for Conversion, on page 61](#)
- [Supported Features for Cloning, on page 66](#)

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 1: (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
	Reserved VLAN Range * ₁₁	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 Policy	BIOS Policy
	Boot Policy	Boot Policy iSCSI Static Target Policy
	Disk Group Policy	Storage Policy
	IPMI Access Profile	IPMI over LAN Policy
	iSCSI Adapter Policy	iSCSI Adapter Policy
	iSCSI Boot Policy	iSCSI Boot Policy
	KVM Management Policy	Virtual KVM Policy
	Local Disk Config Policy * ₆	Storage Policy, SD Card Policy
	QoS Policy	Ethernet QoS Policy/ FC QoS Policy
	Serial over LAN Policy	Serial over LAN Policy
	Service Profile	Server Profile
	Service Profile Template * ₇	Server Profile Template
	Storage Profile	Storage Policy
	Storage Profile - Security Policy * ₁₁	Drive Security
	vMedia Policy	Virtual Media Policy
	vNIC/vHBA Placement Policy * ₈	LAN Connectivity Policy/SAN Connectivity Policy
	Ethernet Adapter Policy	Ethernet Adapter Policy
	Flow Control Policy	Flow Control Policy
	LACP Policy	Link Aggregation Policy
	LAN Connectivity Policy	LAN Connectivity Policy
	VMQ Connection Policy	VMQ * ₁₂
	usNIC Connection Policy	usNIC * ₁₂
	SRIOV HPN Connection Policy	SR-IOV * ₁₂
	Link Protocol Policy	Switch Control Policy
	Multicast Policy	Multicast Policy
	Network Control Policy	Ethernet Network Control Policy
Fibre Channel Adapter Policy	Fibre Channel Adapter Policy	

UCS Manager/UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
	SAN Connectivity Policy	SAN Connectivity Policy
	Storage Connection Policy	FC Zoning Policy
	Power Control Policy Power Restore BIOS setting	Power Policy
Pools	IP Pool	IP Pool
	IQN Suffix Pool	IQN Pool
	MAC Pools	MAC Pool
	WWNN Pool	WWNN Pool
	WWPN Pool	WWPN Pool
	Server Pool * ₉	Resource Pool

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

Table 2: (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 VLAN	VLAN Policy
	QoS System Class	System QoS Policy
	VLAN Group* ₁₃	Ethernet Network Group Policy
	VLAN	VLAN Policy
	VSAN	VSAN Policy
	Storage VSAN * ₉	VSAN Policy
	LAN/SAN Pin Group * ₁₀	LAN/SAN Pin Group
Fabric Policies * ₂	Appliance Network Control Policy	Ethernet Network Control Policy
	UDLD Link Policy	Link Control Policy

UCS Manager Feature Category	Source UCS Manager Feature Name	Equivalent IMM Policy
Port Roles	Appliance Port	Port Policy
	Appliance Port-Channel	Port Policy
	FCoE Uplink Port	Port Policy
	FCoE Uplink Port-Channel	Port Policy
	LAN Uplink Port	Port Policy
	LAN Uplink Port-Channel	Port Policy
	SAN Unified Port	Port Policy
	SAN Uplink Port	Port Policy
	SAN Uplink Port-Channel	Port Policy
	Server Port	Port Policy
	FC Storage Port *9	Port Policy
	SAN Storage Port *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 mapping is static, but can be adjusted in the Transition Settings. For more details, see B. Transition Settings for Conversion section in [Default Settings](#).

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

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



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

*11 - Supported in IMM Transition Tool, Release 4.0.1 and later.

*12 - Part of LAN Connectivity policy

*13 - IMM Transition Tool, Release 4.1.2 supports VIC QinQ Tunneling

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 3: 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).

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 4: Supported Features for Cloning an Intersight Account

Feature Category	Supported Feature
UCS Server Policy	Adapter Configuration
	BIOS
	Boot Order
	Certificate Management
	Device Connector
	Drive Security *2
	Ethernet Adapter
	Ethernet Network
	Ethernet Network Control
	Ethernet Network Group
	Ethernet QoS
	FC Zoning
	Fibre Channel Adapter
	Fibre Channel Network
	Fibre Channel QoS
	Firmware *2
	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	

Feature Category	Supported Feature
	SMTP
	SNMP
	SSH
	Storage
	Syslog
	Virtual KVM
	Virtual Media
UCS Domain Policy	Flow Control
	Link Aggregation
	Link Control
	Multicast
	Port
	Switch Control
	System QoS
	VLAN
	VSAN
	SNMP
UCS Chassis Policy	Thermal
	SNMP
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.
- *₂ - Supported from IMM Transition Tool, Release 4.0.1 onwards.



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 **A**

Appendix

- [Appendix A : Management Operations Using CLI , on page 71](#)
- [Appendix B: Download Logs/Technical Support, on page 73](#)
- [Appendix C: Providing Feedback, on page 73](#)

Appendix A : Management Operations Using CLI

(I) Edit the /etc/hosts File

You can edit the `/etc/hosts` file using the `sudo hosts` 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
```

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

Perform the following steps to change the IP address of the VM:

1. SSH to the VM.
2. Edit `/etc/netplan/00-installer-config.yaml` file using the below command:

```
$ sudoedit /etc/netplan/00-installer-config.yaml
```
3. Change the IP, Netmask, Gateway, and DNS fields as per your requirement.
4. Edit netplan configuration using following doc: <https://netplan.readthedocs.io/en/latest/examples/>
5. Save the file.
6. Reboot the VM using the below command:

```
sudo reboot
```

(III) Change the Hostname/Domain name of the IMM Transition Tool VM

Perform the following steps to change the hostname of the VM:

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

```
sudo hostnamectl <hostname>
```

Perform the following steps to change the domain name of the VM:

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

```
sudo hostname --fqdn <FQDN>
```

(IV) Change the NTP of the IMM Transition Tool VM

Perform the following steps to change the NTP of the VM:

1. SSH to the VM.
2. Edit `/etc/systemd/timesyncd.conf` file using the below command:

```
$ sudoedit /etc/systemd/timesyncd.conf
```

3. Uncomment and change the value of 'NTP=' field.
4. Save the file.
5. Reboot the VM using the below command:

```
sudo reboot
```

(V) 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.

(VI) Self-sign or Renew the SSL Certificates

Perform the following steps to self-sign or renew/reset the HTTPS SSL certificates:

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

```
ssl_cert
```

- `ssl_cert show`: Display information about the SSL certificate currently in use.
- `ssl_cert renew`: Renew self-signed SSL certificate with a validity of one year.

- `ssl_cert reset` : Remove SSL certificate files from the `/etc/data/certificates/` directory

Appendix B: Download Logs/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 C: Providing Feedback

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

