



Cisco Intersight Managed Mode Transition Tool User Guide, 5.x

First Published: 2025-01-10

Last Modified: 2026-04-08

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)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

[Full Cisco Trademarks with Software License](#) ?

PREFACE

[Communications, Services, Bias-free Language, and Additional Information](#) vii

CHAPTER 1

[New and Changed Information](#) 1

[New and Changed Information](#) 1

CHAPTER 2

[Overview](#) 11

[Overview](#) 11

CHAPTER 3

[Prerequisites](#) 15

[Prerequisites](#) 15

CHAPTER 4

[Installing Cisco Intersight Managed Mode Transition Tool](#) 17

[Installing Cisco Intersight Managed Mode Transition Tool](#) 17

CHAPTER 5

[Upgrading Cisco Intersight Managed Mode Transition Tool](#) 23

[Upgrading Cisco Intersight Managed Mode Transition Tool](#) 23

CHAPTER 6

[Accessing the Intersight Managed Mode Transition Tool](#) 25

[Accessing the Intersight Managed Mode Transition Tool](#) 25

CHAPTER 7

[Transition](#) 27

[Adding an IMM Transition for Conversion](#) 27

[Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device](#) 34

[Adding an IMM Transition for Cloning](#) 42

Adding an IMM Transition to Push the Uploaded Configuration 47
 Transition Management 50
 Interpreting Transition Readiness Report 51

CHAPTER 8 **Device Management** 53
 Adding Devices 53
 Claiming Devices 55
 Uploading Custom Device File 56
 Clearing an Intersight Account 56
 Viewing Clear Intersight Report 58

CHAPTER 9 **Software Repository** 59
 Overview 59
 Creating Folders and Uploading Files 59
 Managing Folders 62
 Managing Files 64
 Syncing File to Intersight 67
 Creating vMedia Policy 67

CHAPTER 10 **Settings** 69
 Default Settings 69
 Proxy Settings 77
 Backup/Restore 77
 Certificate Settings 78

CHAPTER 11 **Conversion Assumptions** 81
 Converting UCS Manager/Central Configuration 81

CHAPTER 12 **Supported Features** 85
 Supported Features for Conversion 85
 Supported Features for Cloning 94

APPENDIX A **Appendix** 99
 Appendix A: Management Operations Using CLI 99

Appendix B: Download Logs/Technical Support **100**

Appendix C: Known Behavior and Limitations **101**

Appendix D: Providing Feedback **101**



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 5.1.4

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.1.4

Feature	Description	Documentation
Support for Cisco UCS X410c M8 compute node	IMM Transition Tool, Release 5.1.4 supports the conversion for Cisco UCS X410c M8 compute node.	
Support for Unified Edge policies, profiles, and templates in cloning transitions	With the IMM Transition Tool, Release 5.1.4, you can fetch and push the Unified Edge policies, profiles, and templates during cloning transitions.	Supported Features for Cloning
Ability to clear the Asset Tags, User Labels, and Path Tags from an Intersight account during a clear Intersight configuration operation	With the IMM Transition Tool, Release 5.1.4, you can clear the Asset Tags, User Labels, and Path Tags associated with resources such as servers, chassis, Fabric Interconnects from an Intersight account during a clear Intersight configuration operation.	Device Management
Support for Fabric Interconnect Audit Logs conversion from UCS Manager to an AuditD policy	With the IMM Transition Tool, Release 5.1.4, you can convert Fabric Interconnect Audit Logs from Cisco UCS Manager into an AuditD policy in IMM. You can also fetch and push the AuditD policy during cloning transitions.	Supported Features for Conversion Supported Features for Cloning

Feature	Description	Documentation
Support for ID Range Access Control policy conversion from UCS Central to an ID Mapping policy	With the IMM Transition Tool, Release 5.1.4, you can convert an ID Range Access Control policy from Cisco UCS Central into an ID Mapping policy in IMM. You can also fetch and push the ID Mapping policy during cloning transitions.	Supported Features for Conversion Default Settings
Support for PCIe connectivity policy in cloning transitions	With the IMM Transition Tool, Release 5.1.4, you can fetch and push the PCIe Connectivity policy during cloning transitions.	Supported Features for Cloning
Miscellaneous support	The IMM Transition Tool, release 5.1.4, includes these enhancements: <ul style="list-style-type: none"> • You can fetch and push path tags during cloning transitions. • You can fetch and push IPMI user account types in the Local User Policy during cloning transitions. • You can filter profiles based on type (Server, Chassis, Domain, Unified Edge) on the Select Server Profiles and Templates page in cloning transition. 	

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.1.3

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.1.3

Feature	Description	Documentation
Added an optional step to push equipment-specific configurations to Intersight after devices are claimed	With Release 5.1.3, the IMM Transition Tool has added an optional step to all transitions, except for the Generate Readiness Report transition. This step allows you to push equipment-specific configuration items (User Labels & Tags for chassis/servers, SPAN sessions) to Intersight after devices have been properly claimed and discovered in the destination Intersight account. You can skip this step if devices are not yet claimed.	Adding an IMM Transition for Conversion Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device Adding an IMM Transition for Cloning Adding an IMM Transition to Push the Uploaded Configuration
Ability to automatically rename duplicate policies during a cloning transition	IMM Transition Tool, Release 5.1.3 provides ability to automatically rename duplicate policies from different source organizations when mapped to a single destination organization, preventing naming conflicts during a cloning transition.	Adding an IMM Transition for Cloning
Support for conversion of Host Firmware Package Policy from UCSM/UCS Central	With the IMM Transition Tool, Release 5.1.3, you can convert a Host Firmware Package policy from UCS Manager or UCS Central to a Firmware Policy in IMM.	Supported Features for Conversion
Support for Selective TLS Protocol Control	The IMM Transition Tool, Release 5.1.3, supports a new TLS CTL script that allows you to selectively enable or disable specific TLS protocols (e.g., TLS 1.2 and 1.3) on Apache web servers.	

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.1.2

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.1.2

Feature	Description	Documentation
Support for Cisco UCS 6664 Fabric Interconnects	The IMM Transition Tool, Release 5.1.2, supports the conversion of Cisco UCS 6664 Fabric Interconnects in the following transition types: In-Place migrations and cloning transitions.	

Feature	Description	Documentation
Support for automated network configuration for VIC Adapters	Starting with Release 5.1.2, the IMM Transition Tool simplifies vNICs/vHBAs conversion by automatically configuring Use vCon placement info for vNIC/vHBA order and Use Host Port info for vNIC/vHBA order settings and generating vCon-to-PCI slot mappings based on the server's hardware inventory. This automation is managed through two new settings in the Transition Settings page: Automatic vCon mapping and Allow Template Unbind . You can still utilize existing manual settings if automatic mapping fails.	Default Settings
Support for conversion of multiple Ethernet Network Group Policies (ENGP) from UCSM/UCS Central	IMM Transition Tool, Release 5.1.2 supports the conversion of multiple Ethernet Network Group Policies (ENGP) from UCSM/UCS Central. It allows for the attachment of up to 8 ENGP per vNIC in LAN Connectivity Policies/vNIC Templates and up to 50 ENGP for uplink ports/port-channels in Port Policies, with optimization logic applied for VLAN group consolidation based on these limits and native VLAN configurations.	
Support for conversion of User Labels on Fabric Interconnects physical interfaces	IMM Transition Tool, Release 5.1.2 supports the conversion of User Labels on Fabric Interconnects physical interfaces (ports and port channels) from UCSM to IMM and in cloning transitions as well.	
Support for conversion of User Label & Asset Tag of FI, FEX, chassis, blade servers, and rack servers from UCSM to IMM	IMM Transition Tool, Release 5.1.2 supports the conversion of User Label & Asset Tag of FI, FEX, chassis, blade servers, and rack servers from UCSM to IMM and in cloning transitions.	

Feature	Description	Documentation
Miscellaneous support	<p>With IMM Transition Tool, Release 5.1.2, the following miscellaneous enhancements have been added:</p> <ul style="list-style-type: none"> • Support for conversion of Forward Error Correction (FEC) attribute (RS Cons 16, RS 1eee, Off FEC options) from UCSM to IMM. It is supported in cloning transitions as well. • Support for the conversion of iSCSI Boot Policy with IPv6 configurations from UCSM to IMM. • Support for the conversion of new Fan Control Mode, Maximum Cooling, in the Thermal Policy from UCSM to IMM. 	

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.1.1

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.1.1

Feature	Description	Documentation
Support for Organization Mapping during Clone Intersight transition	The IMM Transition Tool, Release 5.1.1, now enables you to map organizations during a Clone Intersight transition from a source Intersight account to a destination Intersight account, allowing greater flexibility and supporting one-to-one or many-to-one organization mapping.	Adding an IMM Transition for Cloning
Support for Cisco UCS X210c M8, C220 M8, and C240 M8 servers	IMM Transition Tool, Release 5.1.1 supports the conversion for Cisco UCS X210c M8, C220 M8, and C240 M8 servers.	
Support for conversion of MACsec policy	With IMM Transition Tool, Release 5.1.1, you can convert MACsec policy from UCS Manager to IMM.	Supported Features for Conversion Default Settings

Feature	Description	Documentation
Support for conversion of UCS Manager/Central LDAP Authentication Domain to Intersight LDAP Policy or Intersight Appliance Authentication Domain	Starting with Release 5.1.1, the IMM Transition Tool enables the conversion of LDAP/AD Authentication Settings from UCS Manager/Central to an LDAP Policy attached to the converted UCS Domain Profile, as well as to the target Intersight Appliance device LDAP settings.	Supported Features for Conversion Default Settings
Miscellaneous support	With IMM Transition Tool, Release 5.1.1, the following miscellaneous enhancements have been added: <ul style="list-style-type: none"> • Support for UCS Manager 4.3(6) release. • Support for UCS Central 2.1(1) release. • Support for the conversion of Package Power Limit of UCSM's Power Control Policy to IMM. • Support for the conversion of SRIOV HPN Connection Policy from UCSC to IMM. 	

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.0.3

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.0.3

Feature	Description	Documentation
Support for Change Mode option during in-place migration of UCS Manager Devices	IMM Transition Tool, Release 5.0.3 introduces the option to select Change Mode during the Erase Configuration step of in-place migration for UCSM devices on version 4.3(5c) and above. This feature allows you to migrate your device from UCSM mode to IMM mode without requiring an initial setup, thus avoiding any manual operation using a console port or requiring a DHCP environment. Please note that this new option still requires a full domain downtime when performing the conversion.	Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device

Feature	Description	Documentation
Support for conversion of Scrub Policy, Memory policy, and Server Pool Qualification policy	With the IMM Transition Tool, Release 5.0.3, you can convert Scrub and Server Pool Qualification policies from UCS Manager/Central to IMM, and Memory policy from UCS Manager to IMM.	Supported Features for Conversion
Support for cloning in-place domain migrations	From Release 5.0.3 onward, the IMM Transition Tool allows for the cloning of in-place domain migration transitions. This operation is only possible if the transition is not complete, and the Erase Configuration operation has not yet been performed.	Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device
Ability to push only the configuration, the equipment-specific configuration items (SPAN sessions, User Labels and Tags assigned to hardware), or both to Intersight while cloning the transitions	From Release 5.0.3 onward, the IMM Transition Tool allows you to push only the configuration, the equipment-specific configuration items (SPAN sessions, User Labels and Tags assigned to hardware), or both to Intersight while cloning the transitions.	Adding an IMM Transition for Cloning Adding an IMM Transition to Push the Uploaded Configuration

Feature	Description	Documentation
Miscellaneous support for various policies	<p>With IMM Transition Tool, Release 5.0.3, following miscellaneous support has been added:</p> <ul style="list-style-type: none"> • EtherChannel Pinning in the Ethernet Adapter Policy (in conversion & cloning transitions). • Multiple Ethernet Network Group Policies attached to a vNIC in LAN Connectivity Policy/vNIC Template and to an uplink port/port-channel in Port Policy (in cloning transition only). • Forward Error Correction (FEC) for breakout ports in the Ethernet Uplink Port Channel, FCoE Uplink Port Channel, and Appliance Port Channel roles in the Port Policy (in conversion transitions from UCSM and cloning transitions). • Default Package Power Limit (PPL) in Power Policy for Cisco UCS C225 and C245 M8 servers (in cloning transitions). • Root CA certificates in Certificate Management Policy (in cloning transitions). • LDAP Policy attachment support for UCS domain profiles (in cloning transitions). 	

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.0.2

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.0.2

Feature	Description	Documentation
Support for adding and claiming IMM Domain devices in Device Management	IMM Transition Tool, Release 5.0.2 provides the ability to add and claim IMM Domain devices from the Device Management page.	Device Management

New Features and Changed Behavior in Intersight Managed Mode Transition Tool, Release 5.0.1

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 5.0.1

Feature	Description	Documentation
Ability to perform an automated in-place migration of UCS Manager Devices using the Transition Tool	IMM Transition Tool, Release 5.0.1 introduces a new transition type: In-Place UCS Domain Migration . This new type allows to perform an automated in-place migration of UCS Manager Devices to Intersight Managed Mode. IMM Transition Tool will fetch the UCS Manager domain configuration, convert it to Intersight, take a backup, and delete the configuration so that the domain is in a proper state to be reconfigured in Intersight Managed Mode. It will also perform the Initial Setup of the domain in Intersight mode (either manually or automatically via DHCP). The converted Domain Profile is then assigned and deployed automatically. The Server Profiles are automatically assigned to servers once they are successfully discovered. However, deployment is not automated; you need to manually power on each server and deploy the profile to complete the process for all server profiles.	Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device, on page 34
Change in the Operating System	The underlying operating system of the tool has changed from Ubuntu 22.04 to Ubuntu 24.04. Therefore, if you are an existing user using IMM Transition Tool, Release 4.X, 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.	-

Feature	Description	Documentation
Support for conversion of SPAN configurations from UCSM to IMM in Upload Configuration + Push to Intersight and Clone Intersight Transitions	The IMM Transition Tool, Release 5.0.1, allows conversion of UCSM SPAN local sessions into Intersight traffic mirroring sessions. However, these sessions are only pushed to Intersight during the Upload Configuration + Push to Intersight and Clone Intersight transitions, controlled by the Push Equipment toggle button.	Adding an IMM Transition to Push the Uploaded Configuration, on page 47 Adding an IMM Transition for Cloning, on page 42



CHAPTER 2

Overview

- [Overview, on page 11](#)

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.

With IMM Transition Tool, Release 5.0.1 onwards, you can perform an automated in-place migration of UCS Manager Devices to Intersight Managed Mode using the IMM Transition Tool.

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. For more information on firmware version equivalency between Cisco Intersight, Cisco IMC, and Cisco UCS Manager, see [Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager](#).

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.

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.

9. Performing an automated in-place migration of the UCS Manager device to Intersight

IMM Transition Tool, Release 5.0.1 introduces a new transition type: **In-Place UCS Domain Migration**. This new type allows to perform an automated in-place migration of UCS Manager Devices to Intersight Managed Mode. IMM Transition Tool will fetch the UCS Manager domain configuration, convert it to Intersight, take a backup, and delete the configuration so that the domain is in a proper state to be reconfigured in Intersight Managed Mode. It will also perform the Initial Setup of the domain in Intersight mode (either manually or automatically via DHCP). The converted Domain Profile is then assigned and deployed automatically. The Server Profiles are automatically assigned to servers once they are successfully discovered. However, deployment is not automated; you need to manually power on each server and deploy the profile to complete the process for all server profiles.



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 15](#)

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)



Note For **In-Place UCS Domain Migration**, TCP port 443 (HTTPS) and TCP port 22 (SSH) need to be open to the individual IP addresses of the Fabric Interconnects. This is required for erase, setup, and claim operations.

- 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 17](#)

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.

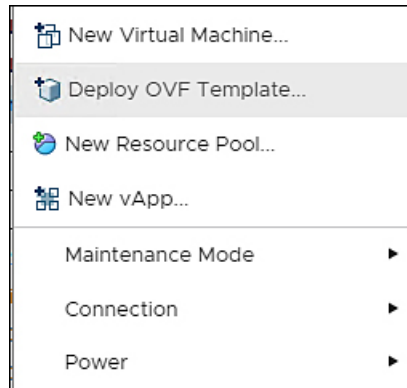
An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco Intersight Managed Mode Transition Tool OVA has a preinstalled operating system and includes application functionality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



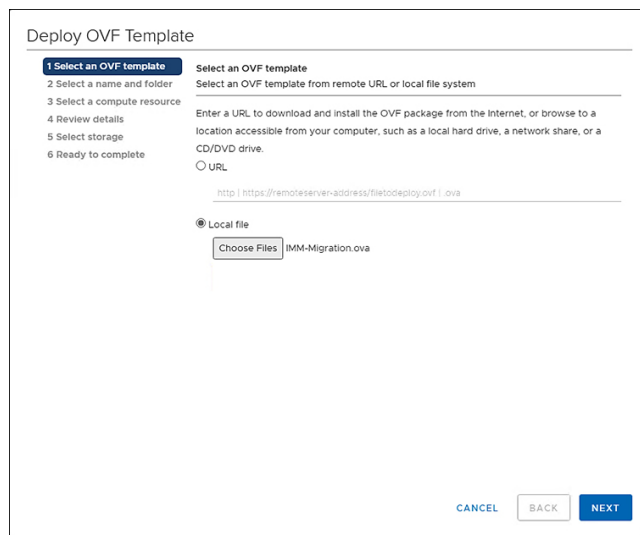
Note Deployment of the IMM Transition Tool OVA must be performed using VMware vCenter (vSphere Web Client). Direct deployment from an ESXi host is not supported and may result in deployment failures.

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](#).

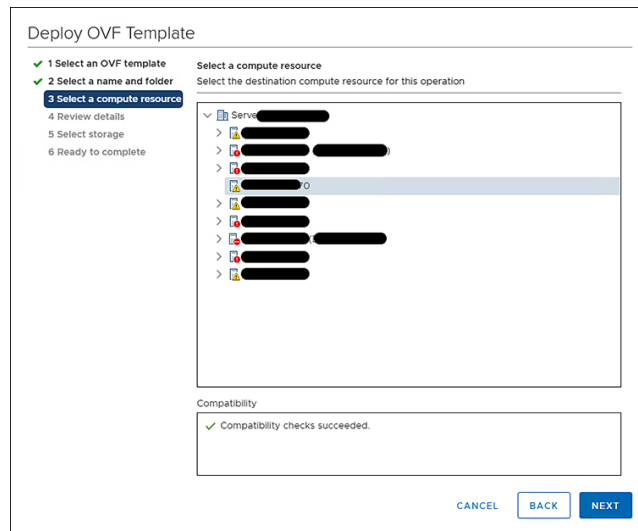
1. Log into the HTML5 vSphere Web Client and go to the **VMs** tab.
2. Right-click the host or cluster on which you want to deploy the IMM Transition Tool, and choose **Deploy OVF Template**.



3. On the **Select an OVF template** page:

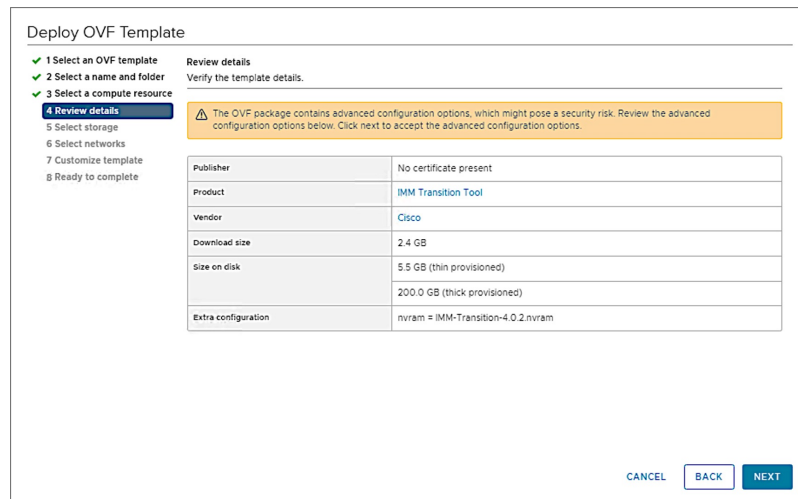


- a. Click the **Local file** radio button, click **Choose Files**, and then browse to the downloaded OVA file.
 - b. Click **Next**.
4. On the **Select a name and folder** page:
- a. Select the location where you want to deploy the virtual appliance.
 - b. Click **Next**.
5. On the **Select a compute resource** page:



- Select the resource you want to use to run the virtual appliance.
- Click **Next**.

6. On the **Review details** page:



- Review the package details, that contain advanced configuration options.
- Click **Next** to accept these options.

7. On the **Select storage** page:

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
[Redacted]	92.5 GB	973 MB	91.55 GB	VM
[Redacted]	1.5 TB	1 TB	509.62 GB	VM
[Redacted]	1.5 TB	1.28 TB	264.34 GB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

- a. Select the desired storage location from the list of datastores.
- b. Click **Next**.

8. On the **Select networks** page:

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

- a. Select a destination network from the dropdown list for each source network.
- b. Click **Next**.

9. On the **Customize template** page:

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

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

- b. Click **Next**.

10. On the **Ready to complete** page:

Deploy OVF Template	
✓ 1 Select an OVF template	Provisioning type: Deploy from template
✓ 2 Select a name and folder	Name: IMM-Transition-4.0.2-sampleee
✓ 3 Select a compute resource	Template name: IMM-Transition-4.0.2
✓ 4 Review details	Download size: 2.4 GB
✓ 5 Select storage	Size on disk: 200.0 GB
✓ 6 Select networks	Folder: ucs507-dc
✓ 7 Customize template	Resource: [REDACTED]
8 Ready to complete	Storage mapping: 1
	All disks: Datastore: 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 =

- a. Review the configuration data.

b. Click **FINISH**.

The system will import and deploy the file.

11. Click the **Refresh** button to update the system.

The VM will be visible in the center windowpane.

12. Select the VM and click **Power On**.

13. 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 Transition Tool

- [Upgrading Cisco Intersight Managed Mode Transition Tool, on page 23](#)

Upgrading Cisco Intersight Managed Mode Transition Tool

Before you begin:

From the UCS Tools page, download the IMM Transition Tool Upgrade package file to your computer in a location that is easy to find when you upgrade the IMM Transition Tool VM.

Upgrading 5.x Releases

Use one of the following options to upgrade the tool across 5.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 4.x to 5.x Releases** section.

Upgrading from 4.x to 5.x Releases

Perform the following steps to upgrade the tool from 4.x to 5.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 25](#)

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.

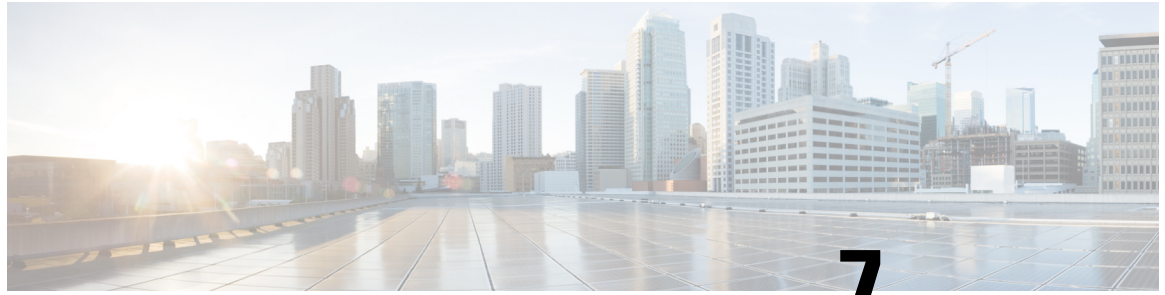


Note User name: admin
Password: Enter the password set on the Customize template page during installation.

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 27](#)
- [Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device, on page 34](#)
- [Adding an IMM Transition for Cloning, on page 42](#)
- [Adding an IMM Transition to Push the Uploaded Configuration, on page 47](#)
- [Transition Management, on page 50](#)
- [Interpreting Transition Readiness Report, on page 51](#)

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, see [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 **In-Place UCS Domain Migration** if you want to migrate a UCS Manager device from UCSM mode to Intersight Managed mode. For the detailed procedure, see [Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device](#).
 - (c) Select **Clone Intersight** if you want to migrate from one Intersight account to another by cloning the configurations. For the detailed procedure, see [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, see [Adding an IMM Transition to Push the Uploaded Configuration](#).

In IMM Transition Tool, Release 5.0.1 and later, a guided tour containing the summary of the selected transition type appears. This helps you to understand all the steps involved in the selected transition. You can check **Do not show this page again** check box if you don't want to get this information again.

Currently, this overview summary is available only for the following transitions:

- Generate Readiness Report
- Generate Readiness Report + Push Config to Intersight
- In-Place UCS Domain Migration

4. Click **Next**.
5. Select the Source UCS 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, see [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 12.
 - (b) Select **Add new account** option if you want to migrate the configuration to a new **Intersight SaaS** or a new **Intersight Appliance VM** account. Go to Step 10.



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**.

- (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 12.
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 settings that you want for the transition.
 - For details on each of the Transition Settings field, see **B. Transition Settings for Conversion** in [Default Settings](#).
 - For defining a default set of configurations for every new transition that you create, see **A. Default Transition Settings for Conversions** in [Default Settings](#).

14. Click **Next**.
15. Select the Service Profiles/Templates to convert.

View the state and physical server association details next to each profile name.

Use the search bar to find a specific profile or template.

You can apply a filter to view the **All** or **Templates** in the **Show** drop-down list, located beside the search bar.



Note Ensure that profiles are in a valid state. A warning appears for invalid states, such as a pending reboot or configuration failure, to prevent misconfiguration

16. Click **Next**.
17. Configure the mapping of converted objects from UCSM to Intersight from **Organization Mapping** page. You can choose either **Advanced Mapping** or **Default Mapping**.

The **Advanced Mapping** option helps in mapping a single UCS organization or multiple UCS organizations to an Intersight organization. Whereas, the **Default Mapping** option maps each UCS organization to an Intersight organization with the same name in Intersight.

- Proceed with the below steps, if you select **Advanced 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.

- Proceed with the below steps, if you select **Default Mapping**:
 - a. To manually enter the name of the Destination Intersight Org, enter a **Root Org name**.



Note

- When using the default mapping, ensure that the **Root Org** name on this page and the **Target Org Name for Fabric Policies** on the **Transition Settings** page are different. If these values are the same, a **Mapping Confirmation** dialog box will appear. Click **Cancel** and modify the **Root Org** name.

- When the selected **Target Org Name for Fabric Policies** on the **Transition Settings** page exists and is shared in the destination Intersight account, a **Mapping Confirmation** dialog box will appear on the **Organization Mapping** page. To avoid conflicts during the transition, click **Cancel** and enter a different **Target Org Name for Fabric Policies**.
-

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.

d. Go to step 19.

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 **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**.

If **Advanced Mapping** is selected, the **Next** button will appear enabled only when 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, see [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 converted configuration 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.

25. Click **Next** to proceed to the **Push Equipment Configuration (Optional)** page.

26. [Optional] On the **Push Equipment Configuration (Optional)** page, choose one of the following actions:

- To push the equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions) to your destination Intersight account, click **Next**.
- To skip this step if this configuration is not required, click **Skip**.
- To download the equipment configuration, click **Download**.

**Note**

- The IMM Transition Tool, Release 5.1.3 and later, supports this optional step.
- Ensure equipment is properly claimed and discovered in your destination Intersight account before pushing equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions).
- You can skip this step if the configuration is not required. This step will be automatically skipped if there are no equipment-specific configurations to push.

-
27. Click **View Equipment Push Summary** to view the push status of each equipment configuration (if applicable).

Adding an IMM Transition for an Automated In-Place Migration of UCS Manager Device

IMM Transition Tool, release 5.0.1 allows you to migrate a UCS Manager device from UCSM mode to Intersight Managed mode. Perform the following steps to add a transition for an automated in-place migration of a UCS Manager device:

1. Click **Add IMM Transition**.
2. Enter a name for the Transition.
3. Select **In-Place UCS Domain Migration** and click **Next**.

A guided tour containing the **Summary of In-Place UCS Domain Migration** appears. This helps you to understand all the steps involved in this transition. You can check **Do not show this page again** check box if you don't want to get this information again.

4. Click **Start**.
5. On the **Select Source UCS device** page, select the source UCS Manager device.





Note If the UCS Manager device is managed by UCS Central, UCS Central must be converted separately.

6. Enter the selected device details.
 - (a). Choose the **Select Existing UCS Manager** option, if you want to migrate the configuration of an existing device.
 - (b). Choose the **Add New UCS Manager** option, if you want to add a new UCS Manager configuration.
7. Enter the Domain IP/FQDN, Username, Password, and User Label for the device, in case you are adding a new UCS Manager device.



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, in case you want to deploy the configuration to an existing Intersight account and then go to step 12.
 - (b). Select **Add new account** option, in case you want to deploy the configuration to a new Intersight SaaS or a new Intersight Appliance VM account.
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.
 - User Label: Enter the User Label for the device for easy identification.
 - Intersight Appliance VM FQDN: Enter the FQDN if you have selected Intersight Appliance VM.

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, see [Proxy Settings](#).

12. Click **Next**.
13. On the **Transition Settings** page, configure the settings that you want for the transition. For more information, see [Default Settings](#).
14. Click **Next**.
15. On the **Select Service Profiles/Templates** page, select the profiles or templates that need to be converted. By default, all profiles on this page are selected.

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

You can apply a filter to view the **All** or **Templates** 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.
 - The system displays a warning when you attempt to push more than 100 service profiles.
-

16. Click **Next**.
17. On **Organization Mapping** page, configure the mapping of converted objects from UCSM to Intersight. You can choose either **Advanced Mapping** or **Default Mapping**.

The **Advanced Mapping** option helps in mapping a single UCS organization or multiple UCS organizations to an Intersight organization. Whereas, the **Default Mapping** option maps each UCS organization to an Intersight organization with the same name in Intersight.

- Proceed with the below steps, if you select **Advanced 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.

- Proceed with the below steps, if you select **Default Mapping**:
 - a. To manually enter the name of the Destination Intersight Org, enter a **Root Org name**.

**Note**

- When using the default mapping, ensure that the **Root Org** name on this page and the **Target Org Name for Fabric Policies** on the **Transition Settings** page are different. If these values are the same, a **Mapping Confirmation** dialog box will appear. Click **Cancel** and modify the **Root Org** name.
- When the selected **Target Org Name for Fabric Policies** on the **Transition Settings** page exists and is shared in the destination Intersight account, a **Mapping Confirmation** dialog box will appear on the **Organization Mapping** page. To avoid conflicts during the transition, click **Cancel** and enter a different **Target Org Name for Fabric Policies**.

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.

- d. Go to step 19.

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 **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.

If **Advanced Mapping** is selected, the **Next** button will appear enabled only when 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, converted to IMM, and the resultant report is generated.



Note Depending on the size of UCS Manager 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.



Note The **Errors and Warnings Overview** section displays issues related to the transition process. You cannot proceed if there are errors in this section. Resolve the errors manually, then attempt the transition again.

For details on interpreting the report, see [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**.

If you are proceeding with warnings on the readiness report, a **Readiness Report Confirmation** dialog box appears.

22. Check **I Acknowledge** check box and click **OK**.

Push converted configuration 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**.

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

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

24. 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 device, then the same device cannot be used by other transitions until the previous task on the device completes.
 - Reset the default password for the converted polices if those have been pushed to Intersight.
-

25. 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.

26. Click **Next**. If any errors occur in the push summary, the system will display a **Push Summary Confirmation** pop-up window. Click **OK** to proceed.
27. The **Backup** page appears.

A full-state backup of the UCSM setup will be taken before proceeding to ensure that a rollback is possible if needed. For more information on how to perform a rollback, see [Cisco UCS Manager Administration Management Guide 4.3 - Backup and Restore \[Cisco UCS Manager\] - Cisco](#).



Note Cisco UCS Manager release 4.2(3d) and later do not allow you to create backup configuration files or import backup configuration files without setting the Password Encryption Key. For more information, see [Cisco UCS Manager Administration Management Guide, 4.3](#).

28. Click **Download** if you wish to download the backup configuration file or click **Next**.
29. On the **Erase Configuration** page, select one of the following options:
 - **Erase Configuration** - Fabric Interconnects are reset to factory defaults and then reconfigured in Intersight mode. Initial Setup can be performed automatically via DHCP or manually using the Console ports on the devices.
 - **Change Mode** - Fabric Interconnects are automatically switched to Intersight Managed mode without requiring an Initial Setup. This option removes the requirement for a DHCP server, or for performing any manual operation.



Note To use the **Change Mode** option, the devices running in UCSM mode must have firmware version 4.3(5c) or later in the Fabric Interconnects. **Change Mode** is only available starting with IMM Transition Tool 5.0.3.

On the **Erase Configuration** page, mandatory validation will be performed before erasing the existing configuration or change mode operation. After validation is complete and no errors are found, the **Erase Configuration** or **Change Mode** button, depending on your selection, will be enabled. If there are errors, you can retry the validation check by clicking **Retry** button.



-
- Note** The following checks are performed on your existing UCS environment:
- a. Ensure all servers are in a **Powered off** state before continuing with the migration. This ensures they are in a clean state before reconfiguring the domain in IMM. If any server is not powered off, shut it down cleanly and retry the validations.
 - b. The existing UCS Manager domain should not be claimed by the destination Intersight account, as this prevents the pre-assignment of Server Profiles to the server serial numbers from working properly. To proceed, unclaim your UCS Manager domain from Intersight first.
 - c. Both HTTPS and SSH access must be open between the IMM Transition Tool and the IPs of both Fabric Interconnects in your UCS domain. These protocols are necessary for performing the erase, setup, and claim steps.
-

30. Click **Erase Configuration** or **Change Mode**.

- If you choose the **Erase Configuration**, enter the device password in the **Erase Confirmation** dialog box to confirm the erasure of all configurations, then click **Continue**. This action will delete all configurations and domain information from your device.

Alternatively, click **Skip** to manually erase the configuration if the automated operation fails.



-
- Note** If you click **Skip** to manually erase the configuration, you cannot make any changes to the erase configuration step. To proceed, you must manually erase the configurations.
-

- If you choose the **Change Mode**, both Fabric Interconnects (FIs) will automatically switch to Intersight Managed Mode on reboot. This operation can take up to 30 minutes. The **Next** button will be enabled once change mode operation is complete. Click **Next** and proceed to step 34 for further instructions.



-
- Note** Selecting **Skip** for the Change Mode option bypasses the initial setup, requiring you to manually complete the change-mode operation.
-

31. Click **Next**. The **Initial Setup** page appears.

32. Choose one of the following options:

- If you have DHCP servers, click **Yes** and enter the IP details for both Fabric Interconnect A and Fabric Interconnect B. The Transition Tool will then automatically complete the initial setup.
- If you do not have a DHCP server, click **No**. The Transition Tool will display all necessary values on your screen. Connect a console cable to each of your Fabric Interconnects and complete the initial setup manually. For more information, see [Setting Up Fabric Interconnects](#).



-
- Note**
- Make sure to enter the UCSM Device's admin password in the required field.
 - A DHCP server is the server on the network to which your Fabric Interconnects' management interfaces are connected.
-

33. Click **Next**.



-
- Note** If a DHCP server was not available in the previous step, the **Manual Initial Setup in IMM Mode Confirmation** dialog box will appear. After completing the manual initial setup, click **OK**.
-

The **Claim To Intersight** page appears.

34. Turn on the **Configure Proxy** toggle button to configure the Fabric Interconnects Device Connector to use a proxy to connect to Intersight.
- a. Enter the **Proxy Hostname** or **IP**.
 - b. Enter the **Proxy Port** number.
 - c. If your proxy settings require authentication, toggle **Authentication** to turn it on, else go to step e.
 - d. Enter the **Username** and the **Password**.
 - e. Click **Save**.

Alternatively, click **Skip** to proceed and manually perform the claim operation if the automated process fails.

35. Click **Next**.

36. Verify the details on the **Assign and Deploy - Domain Profile** page, then click **Next** to start assigning and deploying the domain profile to the Fabric Interconnects. Once the deployment is complete, click **OK**.



-
- Note**
- IMM Transition Tool, Release 5.0.1, does not support cloning of In-place domain migration transition.
 - From Release 5.0.3 onward, the IMM Transition Tool allows for the cloning of in-place domain migration transitions. This operation is only possible if the transition is not complete, and the **Erase Configuration** operation has not yet been performed.
-

37. Click **Next** to proceed to the **Push Equipment Configuration (Optional)** page.

38. [Optional] On the **Push Equipment Configuration (Optional)** page, choose one of the following actions:

- To push the equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions) to your destination Intersight account, click **Next**.
- To skip this step if this configuration is not required, click **Skip**.

- To download the equipment configuration, click **Download**.

**Note**

- The IMM Transition Tool, Release 5.1.3 and later, supports this optional step.
- Ensure equipment is properly claimed and discovered in your destination Intersight account before pushing equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions).
- You can skip this step if the configuration is not required. This step will be automatically skipped if there are no equipment-specific configurations to push.

39. Click **View Equipment Push Summary** to view the push status of each equipment configuration (if applicable).

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 **Intersight SaaS** or a new **Intersight Appliance VM** account. Refer step 9 and 10 for API Key ID and Secret key details and then go to step 7. 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. Click **Refresh** to retrieve the latest configuration from the existing Intersight account and then go to step 11.

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

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

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

7. Click **Next**.
8. 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 11.
 - (b) Select **Add new account** option, in case you want to migrate the configuration to a new **Intersight SaaS** or a new **Intersight Appliance VM** account. 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 **Intersight SaaS** account, you can also select the region to which the account belongs: **US** or **EU**.

9. 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.

10. 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.
11. Click **Next**.
12. Configure the settings 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](#).
13. Click **Next**.
14. You can choose either **Selective Cloning** or **Full Cloning** from this page.
 - Select **Selective Cloning** to choose the Organizations, Server Profiles/Templates, Chassis Profiles/Templates, or Domain Profiles/Templates that need to be cloned.
 - 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.
 - Select **Full Cloning** to clone all Organizations, Server Profiles/Templates, Chassis Profiles/Templates, or Domain Profiles/Templates and their associated policies.

**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.

15. Click **Next**.
16. Configure the mapping of cloned organization from source Intersight account to destination Intersight account from **Organization Mapping** page. You can choose either **Advanced Mapping** or **Default Mapping**.

The **Advanced Mapping** option helps in mapping a single source Intersight organization or multiple source Intersight organizations to a destination Intersight organization.

 - a. Proceed with the below steps, if you select **Advanced Mapping**:
 1. To add a new Destination Intersight Org, click **Add New**.

2. From the list of source Intersight Orgs, select one or more source Intersight Orgs and map it to a Destination Org in Intersight and click **Map Now**. Repeat this step until all the mapping is complete.
3. To configure a Destination Org as a Shared Org, click on ellipse (...) next to the Destination Org name and select the **Share with other orgs** option.

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



Note**• For Advanced Mapping:**

- The **Next** button becomes active only after you select and map all source Intersight organizations to their respective destination Intersight organizations.
- In IMM Transition Tool, Release 5.1.3 and later, if multiple policies from different source organizations have the same name and mapped to a single destination organization, a pop-up message appears once you proceed to the next step. This message provides an option to enable the **Rename Policies** toggle button.
 - **Enable Rename Policies:** If you enable this toggle, the tool automatically renames all conflicting policies by appending the source organization name to their original name.
 - **Do Not Enable Rename Policies:** If you do not enable the toggle, the tool converts only the first policy encountered with a conflicting name and skips all other policies with that same name during the cloning configuration.
- The IMM Transition Tool, Release 5.1.1 and later, supports Organization Mapping for Clone Intersight transition.
- If the selected source Intersight organization does not comply with the organization sharing rules, the tool will blur or disable access to that organization to prevent the mapping.
- **Organization Sharing Rules**
 - A shared org cannot be mapped concurrently with orgs that contain profiles.
 - A shared source org cannot be mapped to a destination org that is already a recipient of another shared org, and vice versa — An Intersight org that is already a recipient of a shared destination org cannot be mapped with a shared source org.
 - If the total resource groups from all mapped source organizations exceed the limit of 10 per organization, the mapping operation fails with an error message.
 - A shared organization cannot be mapped to a destination organization that already contains associated resource groups. To allow this, enable the **delete_existing_resource_group_memberships_for_intersight_shared_orgs** setting.
 - A source organization that has resource groups cannot be mapped to a shared destination organization — resource groups are not supported in shared organizations.

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 **Organization Mapping** page, by choosing **Destination Intersight Organization Name**.

You can use the **Un-Map All** option to unmap the existing Source Org to Destination Org mapping within a selected Intersight account. Alternatively, to unmap a single entity, navigate to the mapping section, select the specific mapped entity, click the three-dot menu next to it, and choose the **Un-map** option.

- b. Select **Default Mapping** option to map each source Intersight organization to a destination Intersight organization with the same name in Intersight.

17. Click **Next**.

If **Advanced Mapping** is selected in the previous step, the **Next** button will be enabled only when the all the source Intersight orgs have been selected and mapped to the respective destination Intersight org.

18. Click **Next**.

Push cloned configuration to Intersight page appears.



Note

- With IMM Transition Tool, Release 5.0.1, you can push the converted SPAN configurations by enabling the **Push Equipment** toggle button. However, it requires all the inventory to be fully discovered and all profiles to be assigned and deployed.
- With IMM Transition Tool Release 5.0.3, you can enable the **Push Equipment Configuration** toggle to choose between two options:
 - a. **Push Config + Equipment**: Push configuration along with the equipment-related configuration elements such as User Labels, Tags and SPAN sessions.
 - b. **Push Equipment Only**: Push only the equipment-related configuration elements (SPAN sessions, User Labels & Tags assigned to hardware).

However, it requires all the inventory to be fully discovered and all profiles to be assigned and deployed.
- With IMM Transition Tool Release 5.1.3, you can push equipment-specific configuration items to Intersight as an optional step after you claim and discover devices in the destination Intersight account. For more information, go to step 23.
- 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**.

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

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

20. Click **Next**.

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

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

22. Click **Next** to proceed to the **Push Equipment Configuration (Optional)** page.
23. [Optional] On the **Push Equipment Configuration (Optional)** page, choose one of the following actions:
 - To push the equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions) to your destination Intersight account, click **Next**.
 - To skip this step if this configuration is not required, click **Skip**.
 - To download the equipment configuration, click **Download**.



Note

- The IMM Transition Tool, Release 5.1.3 and later, supports this optional step.
 - Ensure equipment is properly claimed and discovered in your destination Intersight account before pushing equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions).
 - You can skip this step if the configuration is not required. This step will be automatically skipped if there are no equipment-specific configurations to push.
-

24. Click **View Equipment Push Summary** to view the push status of each equipment configuration (if applicable).

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 **Intersight SaaS** 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 configuration to Intersight page appears.

**Note**

- With IMM Transition Tool, Release 5.0.1, you can push the converted SPAN configurations by enabling the **Push Equipment** toggle button. However, it requires all the inventory to be fully discovered and all profiles to be assigned and deployed.
- With IMM Transition Tool Release 5.0.3, you can enable the **Push Equipment Configuration** toggle to choose between two options:
 - a. **Push Config + Equipment**: Push configuration along with the equipment-related configuration elements such as User Labels, Tags and SPAN sessions.
 - b. **Push Equipment Only**: Push only the equipment-related configuration elements (SPAN sessions, User Labels & Tags assigned to hardware).

However, it requires all the inventory to be fully discovered and all profiles to be assigned and deployed.
- With IMM Transition Tool Release 5.1.3, you can push equipment-specific configuration items to Intersight as an optional step after you claim and discover devices in the destination Intersight account. For more information, go to step 14.
- 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-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 on the three dots present next to the object status to know the reason for push failure.

13. Click **Next** to proceed to the **Push Equipment Configuration (Optional)** page.

14. [Optional] On the **Push Equipment Configuration (Optional)** page, choose one of the following actions:

- To push the equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions) to your destination Intersight account, click **Next**.

- To skip this step if this configuration is not required, click **Skip**.
- To download the equipment configuration, click **Download**.

**Note**

- The IMM Transition Tool, Release 5.1.3 and later, supports this optional step.
- Ensure equipment is properly claimed and discovered in your destination Intersight account before pushing equipment configuration (User Labels & Tags for chassis/servers, SPAN sessions).
- You can skip this step if the configuration is not required. This step will be automatically skipped if there are no equipment-specific configurations to push.

15. Click **View Equipment Push Summary** to view the push status of each equipment configuration (if applicable).

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 53](#)
- [Claiming Devices, on page 55](#)
- [Uploading Custom Device File, on page 56](#)
- [Clearing an Intersight Account , on page 56](#)
- [Viewing Clear Intersight Report, on page 58](#)

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.



Note Starting with IMM Transition Tool 5.0.2, you can add IMM Domain devices as well, using the **Add Device** option or by uploading a CSV file.

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 selected **Device Type** in Step 2b is **Cisco IMC**, **UCS Manager**, **UCS Central**, or **IMM Domain**, enter the **Username** for the device. Otherwise, proceed to Step 2f.
 - e. Enter the **Password** for the device and go to Step 2g.
 - f. If the Device Type selected in Step 2b 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. Enter a **User Label** for this device. The user label helps in identification of devices.



Note The **User Label** option is available only in IMM Transition Tool, 4.2.1 and above.

- h. Turn on the **Use Proxy** toggle button to enable proxy settings.
For more details on proxy settings, see [Proxy Settings](#).



Note For IMM Transition Tool, Release 5.0.1 and later, **Use Proxy** option is available for Intersight Devices only.

- i. 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 add multiple devices in bulk:

- 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	10.xxx.xx.xxx	admin	Paxxxxxx4
ucsc	10.xxx.xx.xxx	admin	Paxxxxxx5
cimc	10.xxx.xx.xxx	admin	Paxxxxxx6
imm_domain	10.xxx.xx.xxx	admin	Paxxxxxx7

- 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

Perform the following steps 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**, **UCS Manager**, or **IMM Domain** devices that you want to claim. If you want to add a new device, follow the steps in the **Adding Devices** section.



Note Starting with IMM Transition Tool 5.0.2, you can claim IMM Domain devices too.

- 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**.
- 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**.



Note In IMM Transition Tool 5.0.1 and later, you can enable the **Force Custom** toggle button. This allows the tool to ignore errors and proceed with uploading the edited configuration and inventory files.

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.

Clearing an Intersight Account

To reset an Intersight account to its default configuration, you can clear the account by removing its configuration objects and settings. You can delete the configuration objects (pools, policies, profiles, and templates), resource groups, users, and organizations from an Intersight account.



Note The **Clear Intersight Config** option is available only for Intersight devices and in IMM Transition Tool, 4.2.1 and above.

To clear an Intersight account:

1. Navigate to **Device Management**.

2. Click the three-dot menu (...) of the desired Intersight device, then select **Clear Intersight Config**.
3. Do one of the following:
 - Click **Clear Everything** to delete all the configuration objects (pools, policies, profiles, and templates), resource groups, users, and organizations from the selected Intersight account.
 - Check the **Clear Intersight Settings** check box if you want to delete the Intersight settings such as Local User Policy, Local Users and Custom Roles from the Intersight account.
 - Check the **Clear Asset tags and User Labels** check box to delete the asset tags and user labels associated with resources such as servers, chassis, Fabric Interconnects.
 - Check the **Clear Path Tags** check box to delete all path tag definitions are maintained in a centralized repository of an Intersight account.





Note **Clear Asset tags and User Labels** and **Clear Path Tags** options are available from Transition Tool, Release 5.1.4 onwards.

- Click **Clear Organizations** to select and delete one or more organizations, along with their associated configuration objects (pools, policies, profiles, and templates), from the Intersight account.



Note

- **Clear Organizations** action will only delete configuration objects in the selected organizations, and will not affect any other organization, settings or resource groups.
- The icon  represents that the Organization has one or more associated Resource Groups.
- The icon  represents that the Organization is shared with other Organizations.

4. To proceed with the clearing operation despite errors, you can enable the **Force Clear** toggle button. Failed objects will be skipped, which may result in an incomplete clearing.
5. Click **Clear Intersight** to start the clearing operation.
6. Click **View Delete Summary** to view the operation summary once the clearing is complete. This summary provides the delete status for each object.



Note You can also view the operation summary later from the **Clear Intersight Report** option.

Viewing Clear Intersight Report

The Clear Intersight Report is a detailed operation summary available after the **Clear Intersight Config** is performed. This report provides detailed information on the total number of objects, objects successfully deleted, objects skipped from deletion, and objects that failed to delete.

To view Clear Intersight Report:

1. Navigate to **Device Management**.
2. Click the three-dot menu (...) of the Intersight device on which **Clear Intersight Config** was performed, then select **Clear Intersight Report**. The clear summary page appears.
3. Click the three-dot menu (...) next to the object status to know the reason for skipped and failed statuses.



CHAPTER 9

Software Repository

- [Overview, on page 59](#)
- [Creating Folders and Uploading Files, on page 59](#)
- [Managing Folders, on page 62](#)
- [Managing Files, on page 64](#)

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:

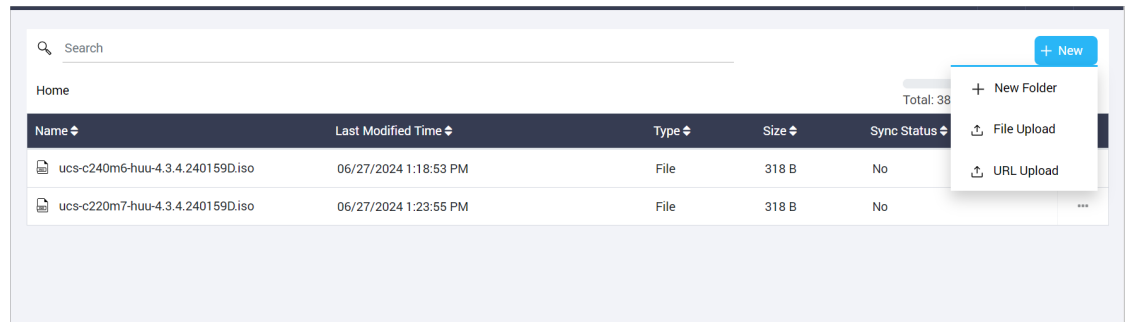
- [Creating Folders and Uploading Files, on page 59](#)
- [Managing Folders, on page 62](#)
- [Managing Files, on page 64](#)

Creating Folders and Uploading Files

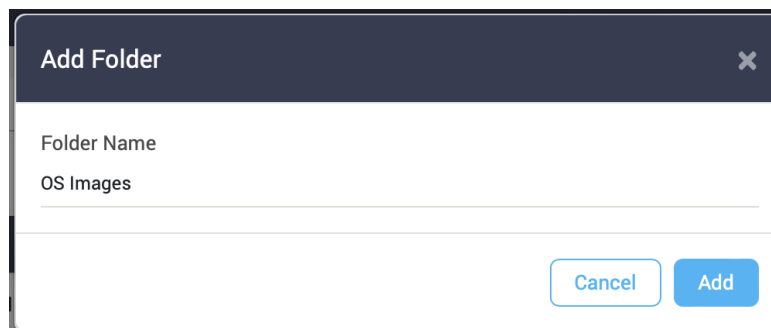
Adding Folder

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**.



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



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

Uploading File

You can upload an ISO file in the software repository either from your local machine or from an external URL.

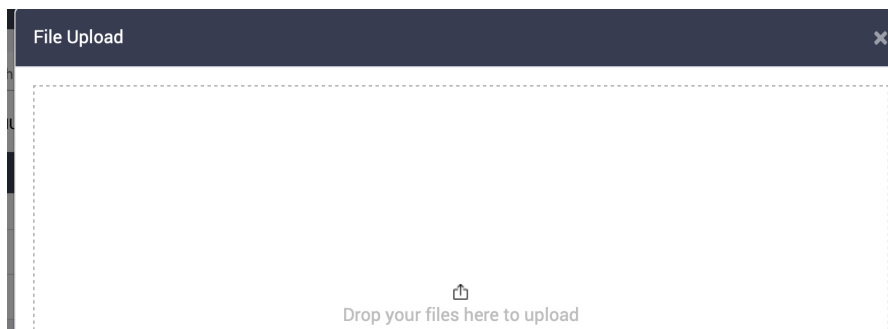


Note Uploading an ISO file from an external URL, is available only in IMM Transition Tool, 4.2.1 and above.

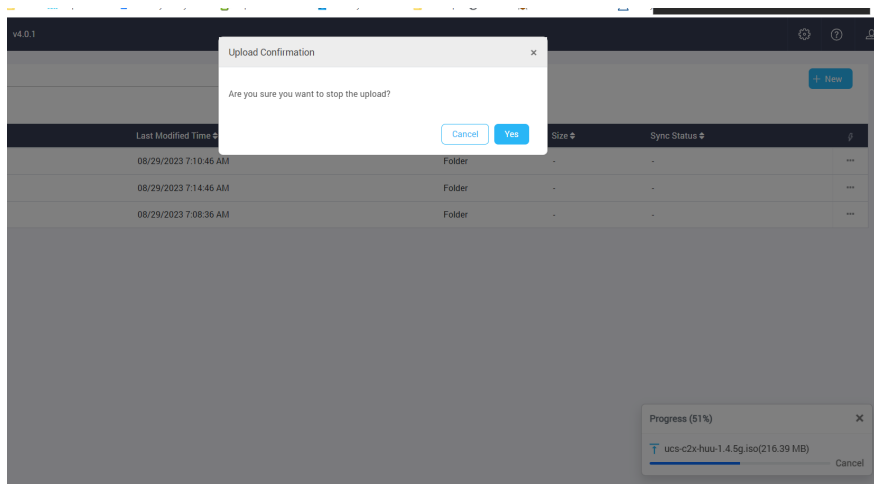
Perform the following steps to upload an ISO file in the software repository from your local machine:

1. Navigate to **Software Repository**.
2. Click **New**.
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 To cancel the upload operation, click **Cancel** and then click **Yes** in the confirmation dialog box.

IMM Transition Tool, Release 4.2.1 and above allows you to upload an ISO file in the software repository from an external URL.

Perform the following steps to upload an ISO file in the software repository from an external URL:

1. Navigate to **Software Repository**.
2. Click **New**.
3. Click **URL Upload**.

URL Upload dialog box appears.

4. Enter the URL from which you want to upload the ISO file.
5. Uncheck the **Verify SSL** check box if it is not required. By default, this option is checked.



Note Enabling the **Verify SSL** option ensures the validity and trustworthiness of the SSL/TLS certificate for the server hosting the file. We recommend that you enable this option as it safeguards both security and data integrity during the upload process.

6. Check the **Use Proxy** check box to enable proxy settings. For more details on proxy settings, see [Proxy Settings](#).
7. Click **Add**.
File gets uploaded to the software repository.



Note To cancel the upload operation, click **Cancel** and then click **Yes** in the confirmation dialog box.

Managing Folders

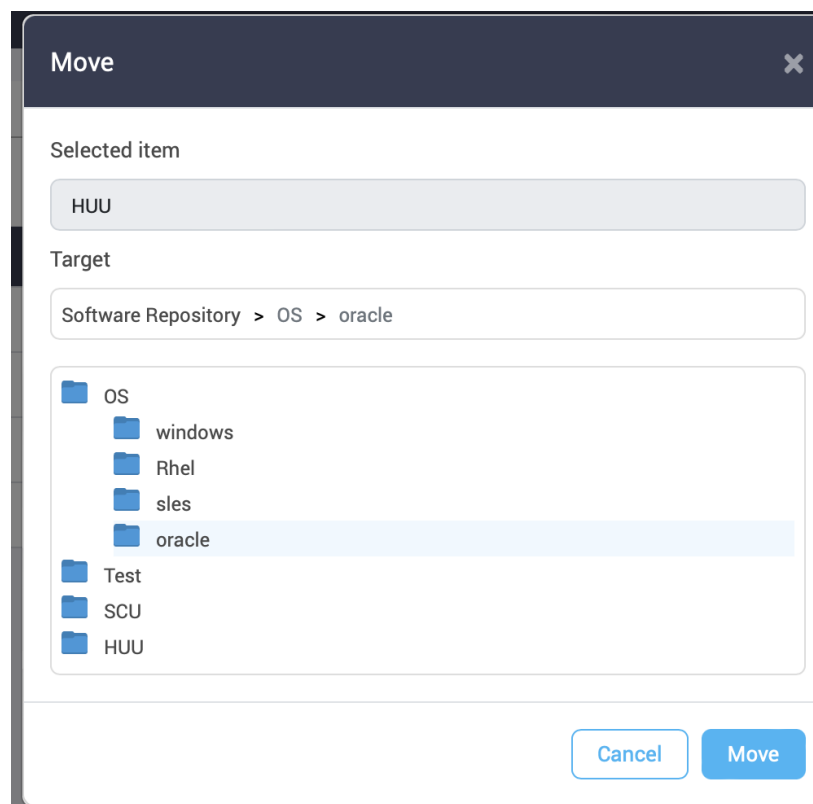
The listing page on the **Software Repository** tab displays the list of folders and files that do not belong to any folder. You can manage the folders by renaming, moving, or deleting folder.

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



3. 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.

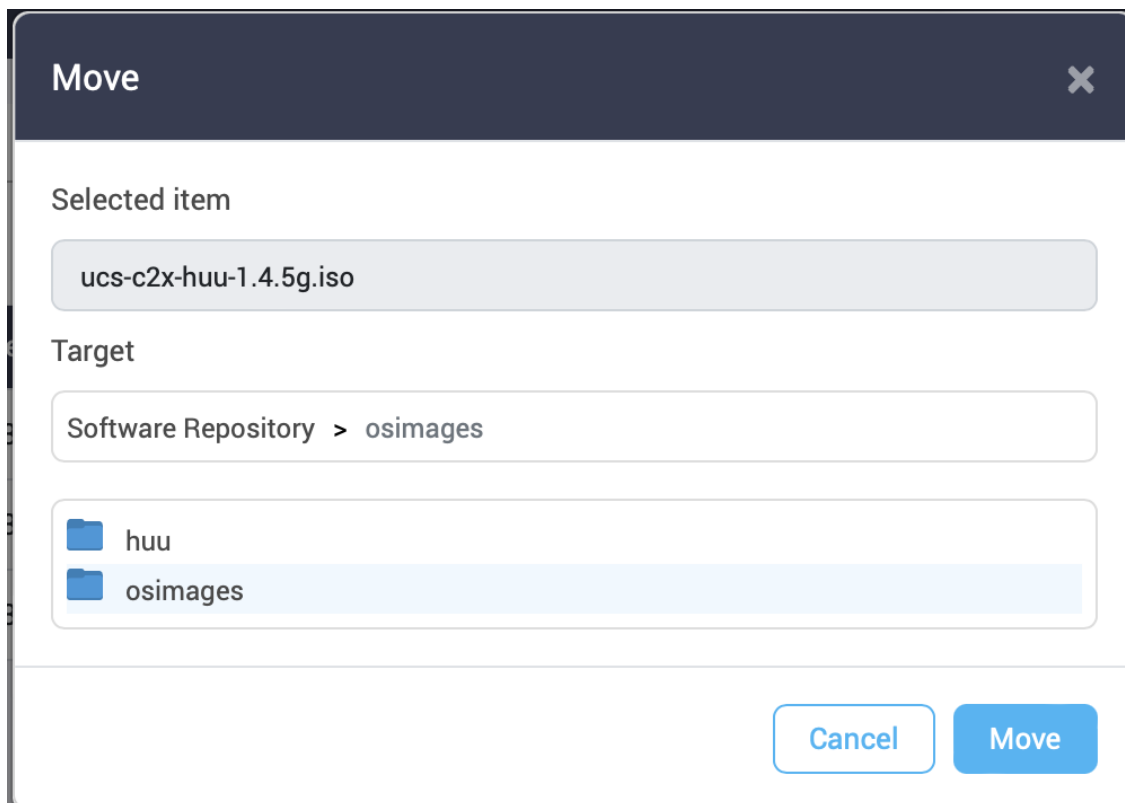
1. Navigate to the folder where the file is present.
2. Click ... present at the end of the file record that you want to manage.

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 69](#)
- [Proxy Settings, on page 77](#)
- [Backup/Restore , on page 77](#)
- [Certificate Settings, on page 78](#)

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**

- For an in-place migration of a UCSM device introduced in IMM Transition Tool version 5.0.1, the **Fabric Policies Conversion** option is always enabled. You cannot disable this setting.
- 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.

**Note**

For an in-place migration of a UCSM device introduced in IMM Transition Tool version 5.0.1, the **Preserve Chassis/Rack Server IDs** option is always enabled. You cannot disable this setting.

g. Create Chassis Profile Template

- This option is enabled by default.

- When enabled, a chassis profile template is created that includes the converted power and thermal policies from the UCS Manager's global policies section.



Note For an in-place migration of a UCSM device introduced in IMM Transition Tool version 5.0.1, the **Create Chassis Profile Template** option is always enabled. You cannot disable this setting.

h. Convert and attach LDAP to domain profile

- This option is enabled by default.
- When enabled, the UCSM LDAP configuration is converted into an Intersight LDAP Policy, which can then be attached to a Domain Profile.



Note If multiple UCSM LDAP Authentication Domains exist, the tool selects the first valid policy in which all groups have the 'admin' role, or a policy without groups. This is because Intersight supports attaching only one LDAP policy to a Domain Profile.

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



Note The IMM Transition Tool version 5.0.1 release removes the deprecated **Service Profiles Conversion** setting for all types of transitions.

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, and WWNN are preserved during the conversion of service profiles from UCS to IMM.

d. Preserve Service Profile Associations

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

e. Share "root" with all sub organizations

- This option is enabled by default.
- When enabled, then the converted root organization will be shared with all other organizations.

f. 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.

g. 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.

h. Automatic vCon mapping

- This option is enabled by default.
- When enabled, it will automatically determine the vCon to PCIe slot mapping based on the assigned server inventory.

i. 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.

j. Allow Template Unbind

- This option is disabled by default.
- When enabled, the converted Server Profiles lose their binding to the Template if the source Service Profiles bound to a common Service Profile Template are associated with servers that have different VIC characteristics (i.e., number of VIC adapters or varying VIC generations).

k. 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.

l. 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.

m. 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.



Note The IMM Transition Tool version 5.0.1 release removes the deprecated **Convert Power Policies** setting for all types of transitions.

n. 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.
-

o. 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.
-

p. Domain Group Conversion (for ID Range Access Control Policy)

- This option is enabled by default.
- When enabled, domain groups linked with ID Range Access Control policies are converted into Resource Groups with membership set to **All**. After the domains are claimed in Intersight, membership must be manually modified as needed.



-
- Note** This conversion applies only for UCS Central and is supported starting with IMM Transition Tool release 5.1.4.
-

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. Create Intersight appliance LDAP config

- This option is enabled by default.
- When enabled, an Intersight Appliance Authentication Domain will be created from the UCSM/UCSC LDAP configuration to support LDAP/AD login on the Intersight appliance.



Note The IMM Transition Tool supports the **Create Intersight Appliance LDAP Config** option starting with Release 5.1.1.

7. 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.

8. 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**.

9. Default AES 128 MACsec key

This default AES-128 MACsec key replaces any existing 128-bit secret key in a MACsec policy during the conversion of a UCS Manager MACsec Policy.



Note

- This password should be reset by the user after the converted policies are pushed to Intersight.
- When MACsec is assigned to a domain profile, AES encryption is automatically enabled. If the default password matches the encryption key, it will be used; otherwise, a random password will be generated to fill the required field.
- The IMM Transition Tool supports the **Default AES 128 MACsec key** option starting with Release 5.1.1.

10. Default AES 256 MACsec key

This default AES-256 MACsec key replaces any existing 256-bit secret key in a MACsec policy during the conversion of a UCS Manager MACsec Policy.



Note

- This password should be reset by the user after the converted policies are pushed to Intersight.
 - When MACsec is assigned to a domain profile, AES encryption is automatically enabled. If the default password matches the encryption key, it will be used; otherwise, a random password will be generated to fill the required field.
 - The IMM Transition Tool supports the **Default AES 256 MACsec key** option starting with Release 5.1.1.
-

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.

5. Delete Existing Resource Group Memberships for Intersight Shared Orgs

- This option is enabled by default.
- When enabled, it automatically deletes all existing Resource Group memberships from an Intersight organization that is set as shared.

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.

From IMM Transition Tool, 4.1.3 onwards, you can upload and add a trusted Certificate Authority (CA) certificate to trust a proxy SSL certificate when connecting to devices behind that proxy.

Adding Trusted Certificate

Perform the following steps to upload a trusted CA certificate:

1. Click **Certificate Settings** present under the gear icon on the top-right corner.
2. Go to **Trusted** tab.
3. Click **Add Certificate**.
4. Click **Browse**.
5. Select the CA certificate to be added.
6. Click **Save**.

The trusted certificate gets added.

Adding SSL 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.
- Go to **SSL** tab.
- 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 by clicking **Download 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.

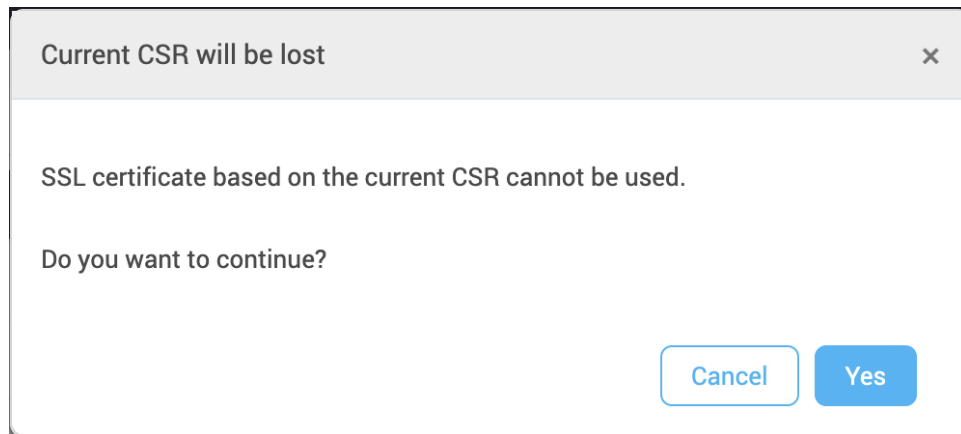
Creating a New CSR

You can regenerate the current CSR details by using the **New CSR** option. In this case, the existing or the current CSR will be lost and you will have to upload a new SSL certificate.

Perform the following steps to create a new CSR.

1. Click **Certificate Settings** present under the gear icon on the top-right corner.
2. Go to **SSL** tab.
3. Fill up the details as mentioned in the **Creating and Uploading Certificate** section.
4. Click **New CSR**.

A confirmation window, as shown below, appears with the message that the existing SSL certificate cannot be used.



5. Click **Yes** to proceed.
A new CSR gets created.

Renewing SSL Certificate

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

1. Click **Certificate Settings** present under the gear icon on the top-right corner.
2. Create a CSR using the steps mentioned in the Creating and Uploading Certificate section.
3. 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](#)

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



CHAPTER 11

Conversion Assumptions

- [Converting UCS Manager/Central Configuration, on page 81](#)

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**.

16. Memory Policy -

Starting with IMM Transition Tool Release 5.0.3, the default memory policy of UCSM will be converted during the transition if the **Blacklisting** option is disabled. If the **Blacklisting** option is enabled in UCSM, a converted memory policy will not be created.



CHAPTER 12

Supported Features

- [Supported Features for Conversion, on page 85](#)
- [Supported Features for Cloning, on page 94](#)

Supported Features for Conversion

A. Supported Features for Conversion from UCS Manager/Central 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 Manager/Central and Intersight Features

UCS Manager/UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Admin	Communication Services <i>Note: Sessions/HTTP settings are defined in Intersight Settings. Telnet/SSH settings are not supported.</i>	SNMP Policy
	Organizations	Intersight Organizations
	Syslog <i>Note: Only supports up to two remote destination servers</i>	Syslog Policy
	Time zone Management	NTP Policy
	MAC Address Table Aging	Switch Control Policy
	VLAN Port Count Optimization	Switch Control Policy
	Reserved VLAN Range <i>Note: Supported in IMM Transition Tool, Release 4.0.1 and later.</i>	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 <i>Note: In UCS Manager, it is found under Admin > Communication Management > DNS Management</i>	Network Connectivity Policy
LDAP Authentication Domain <i>Note: Supported in IMM Transition Tool, Release 5.1.1 and later.</i>		

UCS Manager/UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
		<p>Intersight LDAP Policy and/or Intersight Appliance Authentication Domain</p> <p>Note</p> <ul style="list-style-type: none"> • If the destination Intersight device is SaaS, the system creates and attaches an LDAP policy to the Domain Profile. For an Appliance device, it creates both the Intersight LDAP policy and the Intersight Appliance Authentication Domain from UCSM LDAP to enable LDAP/AD login on the appliance depending on the default settings during the conversion. • When converting from UCS Central, tool enables the conversion of LDAP/AD Authentication from UCS Central (UCSC) to the target Intersight appliance device.

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 <i>Note: Replaced by Storage Policy. Local Disk Configuration policy supports only Manual creation not the Automatic policy option.</i>	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 <i>Note: Only Updating Templates - no support for Initial Templates (though cloning can be achieved)</i>	Server Profile Template
	Storage Profile	Storage Policy
	Storage Profile - Security Policy <i>Note: Supported in IMM Transition Tool, Release 4.0.1 and later.</i>	Drive Security
	vMedia Policy	Virtual Media Policy
	LAN Connectivity Policy/SAN Connectivity Policy	

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
	vNIC/vHBA Placement Policy <i>Note: The placement is statically mapped to PCIe slots, with the following mapping:</i> <ul style="list-style-type: none"> • vCon 1: Slot MLOM • vCon 2: Slot PCIe1 • vCon 3: Slot PCIe2 • vCon 4: Slot PCIe3 <i>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.</i>	
	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
	usNIC Connection Policy	usNIC <i>Note: Part of LAN Connectivity policy</i>
	SRIOV HPN Connection Policy	SR-IOV
	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
	SAN Connectivity Policy	SAN Connectivity Policy
	Storage Connection Policy	FC Zoning Policy
	Power Control Policy Power Restore BIOS setting	Power Policy
	vNIC Template	vNIC Template

UCS Manager/UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
	vHBA Template	vHBA Template
	—	Chassis Profile Template <i>Note: Chassis Profile Template is created by using converted power and thermal policies from the global policies section of the UCS Manager.</i>
	Memory Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>	Memory Policy
	Scrub Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>	Scrub Policy
	Server Pool Qualification Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>	Server Pool Qualification Policy
	MACsec Policy <i>Note: Supported in IMM Transition Tool, Release 5.1.1 and later.</i>	MACsec Policy
	Host Firmware Package Policy <i>Note: Supported in IMM Transition Tool, Release 5.1.3 and later.</i>	Firmware Policy
	ID Range Access Control Policy Note <i>Conversion support is available only from UCS Central to IMM and is supported in the IMM Transition Tool, Release 5.1.4 and later.</i>	ID Mapping Policy

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM 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 <i>Note: Supported in IMM Transition Tool, Release 1.0.2 and later.</i>	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 Note: Merged with regular VLANs	Appliance VLAN	VLAN Policy
	QoS System Class	System QoS Policy
	VLAN Group <i>Note: IMM Transition Tool, Release 4.1.2 supports VIC QinQ Tunneling</i>	Ethernet Network Group Policy
	VLAN	VLAN Policy
	VSAN	VSAN Policy
	Storage VSAN <i>Note: Supported in IMM Transition Tool, Release 1.0.2 and later.</i>	VSAN Policy
	LAN/SAN Pin Group Note: <ul style="list-style-type: none"> • Supported in IMM Transition Tool, Release 3.0.1 and later. • Table containing aliases for aliased VLANs/VSANs are not supported for conversion. 	LAN/SAN Pin Group
Fabric Policies Note: Merged with regular Network Control Policies	Appliance Network Control Policy	Ethernet Network Control Policy
	UDLD Link Policy	Link Control Policy
	Fabric Interconnect Audit Logs Note <i>Supported in IMM Transition Tool, Release 5.1.4 and later.</i>	AuditD 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 <i>Note: Supported in IMM Transition Tool, Release 1.0.2 and later.</i>	Port Policy
	SAN Storage Port <i>Note: Supported in IMM Transition Tool, Release 1.0.2 and later.</i>	Port Policy
	Breakout Port <i>Note:</i> <ul style="list-style-type: none"> • Supported in IMM Transition Tool, Release 3.0.1 and later. • Table containing aliases for aliased VLANs/VSANs are not supported for conversion. 	Port Policy

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-6664	Cisco UCS-FI-6664 <i>Note: Supported in IMM Transition Tool, Release 5.1.2 and later.</i>

UCSM FI	Equivalent IMM FI
Cisco UCSX-S9108-100G	Cisco UCSX-S9108-100G <i>Note: Supported in IMM Transition Tool, Release 4.2.2 and later.</i>
Cisco UCS-FI-6536	Cisco UCS-FI-6536
Cisco UCS-FI-64108	Cisco UCS-FI-64108
Cisco UCS-FI-6454	Cisco UCS-FI-6454
Cisco UCS-FI-6332-16UP	Cisco UCS-FI-6536
Cisco UCS-FI-6332	Cisco UCS-FI-6536
UCS-FI-M-6324	Cisco UCS-FI-6454 <i>Note: Supported in IMM Transition Tool, Release 4.2.1 and earlier.</i>
	Cisco UCSX-S9108-100G <i>Note: Supported in IMM Transition Tool, Release 4.2.2 and later.</i>
Cisco UCS-FI-6296UP	Cisco UCS-FI-64108
Cisco UCS-FI-6248UP	Cisco UCS-FI-6454

**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
	<i>Note: Supported from IMM Transition Tool, Release 4.0.1 onwards.</i>
	Ethernet Adapter
	Ethernet Network
	Ethernet Network Control
	Ethernet Network Group
	Ethernet QoS
	FC Zoning
	Fibre Channel Adapter
	Fibre Channel Network
	Fibre Channel QoS
	Firmware
	<i>Note: Supported from IMM Transition Tool, Release 4.0.1 onwards.</i>
	IMC Access
	IPMI over LAN
	iSCSI Adapter
	iSCSI Boot
	iSCSI Static Target
	LAN Connectivity
	LDAP
	Local User
Network Connectivity	

Feature Category	Supported Feature
	NTP
	Persistent Memory
	Power
	SAN Connectivity
	SD Card
	Serial over LAN
	SMTP
	SNMP
	SSH
	Storage
	Syslog
	Virtual KVM
	Virtual Media
	Memory Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>
	Scrub Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>
	Server Pool Qualification Policy <i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>
	PCIe Connectivity Policy <i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>
	ID Mapping Policy <i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>

Feature Category	Supported Feature
UCS Domain Policy	Flow Control
	Link Aggregation
	Link Control
	Multicast
	Port
	Switch Control
	System QoS
	VLAN
	VSAN
	SNMP
	LDAP
	<i>Note: Supported in IMM Transition Tool, Release 5.0.3 and later.</i>
UCS Chassis Policy	AuditD Policy
	<i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>
UCS Chassis Policy	Thermal
	SNMP
Pools	IP
	IQN
	MAC
	Resource
	UUID
	WWNN
	WWPN
Profiles	UCS Server Profile
	UCS Chassis Profile
	UCS Domain Profile
	Unified Edge Profile
	<i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>

Feature Category	Supported Feature
Templates	UCS Server Profile Template
	UCS Domain Profile Template <i>Note: Supported in IMM Transition Tool, Release 4.2.1 and later.</i>
	UCS Chassis Profile Template <i>Note: Supported in IMM Transition Tool, Release 4.2.1 and later.</i>
	vNIC/vHBA Template <i>Note: Supported in IMM Transition Tool, Release 4.2.1 and later.</i>
	Unified Edge Template <i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>
Access and Permissions Settings	Users <i>Note: Cloned only when the "Trim Intersight Settings" option is not set. By default, the object is not cloned.</i>
	Groups <i>Note: Cloned only when the "Trim Intersight Settings" option is not set. By default, the object is not cloned.</i>
	Roles <i>Note: Cloned only when the "Trim Intersight Settings" option is not set. By default, the object is not cloned.</i>
	Organizations
	Resource Groups <i>Note: To include the entire domain or individual servers in the resource group, the target must be claimed first. Otherwise, an empty resource group with "custom" membership is created.</i>
System	Path Tags <i>Note: Supported in IMM Transition Tool, Release 5.1.4 and later.</i>

**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 99
- [Appendix B: Download Logs/Technical Support](#), on page 100
- [Appendix C: Known Behavior and Limitations](#), on page 101
- [Appendix D: Providing Feedback](#), on page 101

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/50-cloud-init.yaml` file using the below command:

```
$ sudoedit /etc/netplan/50-cloud-init.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.

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: Known Behavior and Limitations

For more information on known behavior and limitations, see the [Release Notes for Cisco Intersight Managed Mode Transition Tool](#).

Appendix D: Providing Feedback

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

