Appendix

Appendix A: Supported Features for Conversion

A. Supported Features for Conversion from UCS to IMM

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

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

Table 1: (I) Conversion Mapping between UCS and Intersight Features

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

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

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

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

Table 2: (II) Conversion Mapping between UCS Manager and Intersight Features

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

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

*1 - Merged with regular VLANs

*2 - Merged with regular Network Control Policies

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

*4 - Only supports up to two remote destination servers

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

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

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

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

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

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

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

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

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

B. Fabric Interconnect (FI) Mapping for Conversion

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

Table 3: Mapping between UCSM FI and IMM FI for Port Policy Conversion

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

Note

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

Appendix B: Supported Features for Cloning

Supported Features for Cloning an Intersight account

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

Note

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

Table 4: Supported Features for Cloning an Intersight Account

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

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

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

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

Note

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

Appendix C: Transition Settings

(I) Transition Settings for Conversion

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

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

Note Fabric policy conversion is supported for UCSM only.

a. **Fabric Policies Name**

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

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

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

c. **Always create separate VLAN Policies**

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

d. **Always create separate VSAN Policies**

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

e. **Always create separate Port Policies**

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

2. **Server Policies Conversion**

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

a. **Service Profiles Conversion**

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

b. **Global Service Profiles Conversion**

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

Note This conversion is applicable only for UCSM.

c. **Preserve Identities**

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

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

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

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

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

f. **UCS Central Tags Conversion**

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

Note

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

g. **UCS Central Tags Prefix**

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

Note This conversion is applicable only for UCS Central.

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

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

5. **Default Password for Converted Policies**

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

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

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

(II) Transition Settings for Cloning

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

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

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

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

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

(III) Default Transition Settings for Conversion

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

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

Appendix D: Proxy Settings

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

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

Perform the following steps to configure the proxy settings.

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

   The proxy settings get saved.

Note

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

Appendix E : Backup/Restore

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

Perform the following steps to backup and restore the data.

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

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

   The data present in the file gets restored.

Note

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

Appendix F : Management Operations Using CLI

(I) Edit the Advanced Configuration Settings

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

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

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

(II) Edit the /etc/hosts File

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

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

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

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

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

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

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

   ```
   sudo reboot
   ```

(IV) Change the Admin Password

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

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

   ```
   sudo passwd admin
   ```

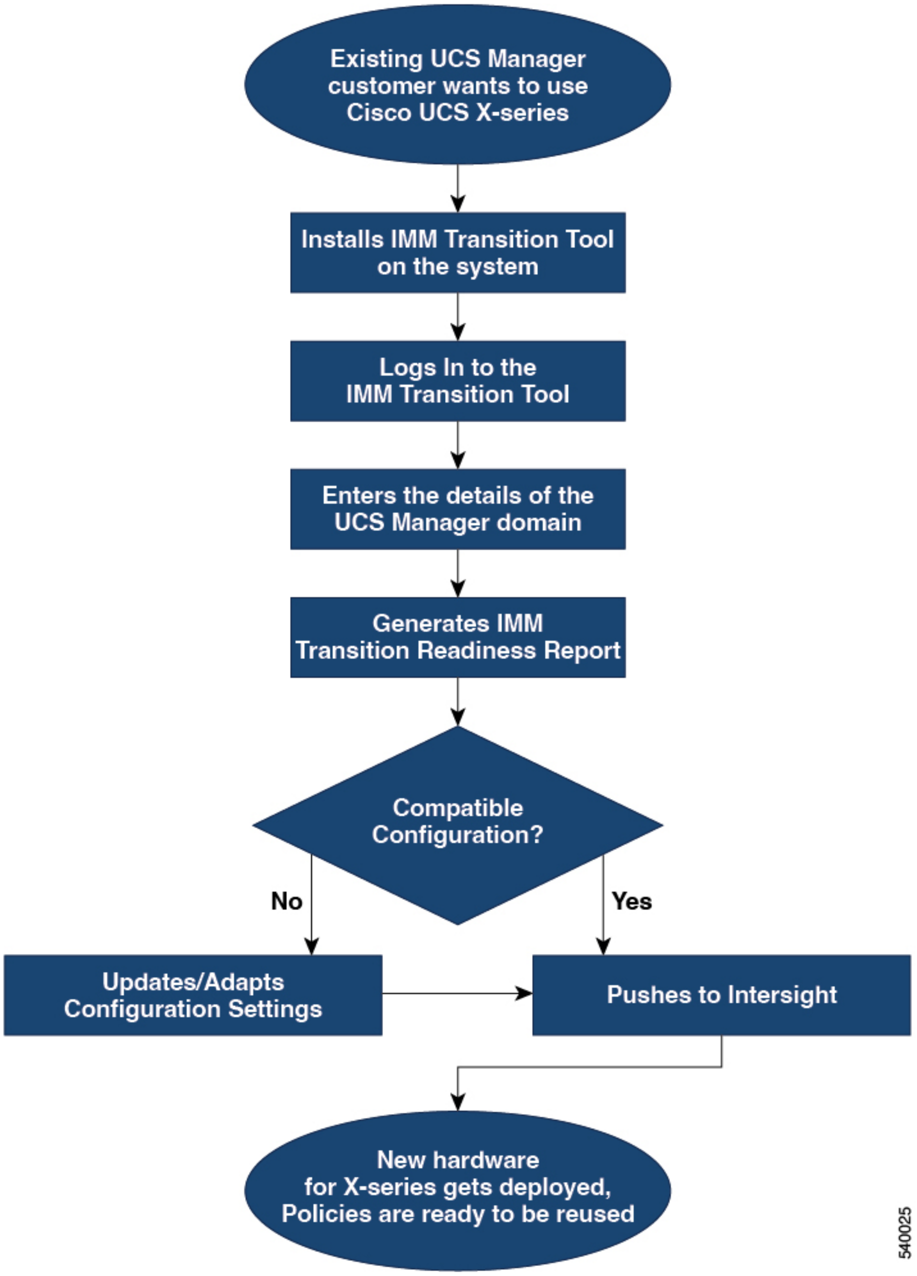
3. Enter the new password.

Appendix G: Sample Use Cases

(I) Accelerate deployments of UCS X-Series

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

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


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

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

Before you begin

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

Step 1 Install Cisco IMM Transition Tool in your system.

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

Step 2 Log into the IMM Transition Tool.

Step 3 Enter the details of the UCS Manager domain.

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

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

What to do next

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

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

(II) Moving Profiles from UCSM to IMM

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

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

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

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

Before you begin

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

Step 1 Install Cisco IMM Transition Tool in your system.

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

Step 2 Log into the IMM Transition Tool.

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

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

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

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

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

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

What to do next

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

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

Appendix H: Technical Support

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

Perform the following steps to send your query:

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

Appendix I: Providing Feedback

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