Appendix

- Appendix A: Supported IMM Features/Policies, on page 1
- Appendix B: Transition Settings, on page 5
- Appendix C: Proxy Settings, on page 8
- Appendix D: Sample Use Cases, on page 9
- Appendix E: Providing Feedback, on page 11
- Appendix F: Technical Support, on page 11

Appendix A: Supported IMM Features/Policies

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. Carefully review the resulting configuration to make sure it is appropriate.

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Admin	Communication Services *4	SNMP Policy
	Organizations	Intersight Organizations
	Syslog *5	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 *6	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 *7	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 *8	Server Profile Template
	Storage Profiles	Storage Policy
	vMedia Policies	Virtual Media Policy
	vNIC/vHBA Placement Policies *9	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 Policy	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

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 *10	Resource Pool

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

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 *2	VLAN Policy
	VSANs	VSAN Policy
	Storage VSANs *10	VSAN Policy
Fabric Policies *3	Appliance Network Control Policies	Ethernet Network Control Policy
	UDLD Link Policies	Link Control 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 *10	Port Policy
	SAN Storage Ports *10	Port Policy

*1 - Merged with regular VLANs

*2 - No support for PVLAN

*3 - Merged with regular Network Control Policies

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

*5 - Only supports up to two remote destination servers

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

*7 - Replaced by Storage Policy

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

*9 - 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.

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

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

Appendix B: Transition Settings

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 disabled by default.
- When the conversion of Service Profiles is enabled, user can select which Profiles will 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. UCS Central templates get converted by default.

c. Root Org Name

It is the name of the Intersight organization to which the UCS root organization gets mapped.

d. Keep source Org path in Intersight Org name

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

Note "root/PROD/WINDOWS" and "root/NONPROD/WINDOWS" would get converted to the same "WINDO organization in Intersight if option is disabled. This could cause conflicts if policies/pools/profiles/tem objects are named the same in both source UCS orgs.

e. 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".

f. 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.

3. Automatically tag converted objects

- This option is enabled by default.
- When enabled, Intersight objects are tagged with "imm_transition_version": "2.0.1", "imm_transition_name": "transition_name" .

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.

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**.

Appendix C: Proxy Settings

The IMM Transition Tool provides the option of enabling or disabling proxy settings while establishing a connection with the UCS device and with Intersight. You can change the proxy settings depending on your requirement scenario.

Scenario 1: Proxy Settings only for UCS device Connection

When you are on **Add UCS** page, perform the following steps if you need to enable Proxy Settings only for connecting to the UCS device.

1. Click **Settings** present under the Gear icon on the top-right corner.
2. Toggle **Enable Proxy** to turn it on.
3. Enter the Proxy Hostname or IP.
4. Enter the Proxy Port number.
5. If your proxy settings require authentication, toggle **Authentication** to turn it on, else go to step 8.
6. Enter the Username.
7. Enter the Password.
8. Click **Save**.

   The Proxy Settings get saved.
9. Generate the readiness report as per the steps mentioned in Working with Cisco Intersight Managed Mode Transition Tool
10. Go to the **Settings** section and toggle **Enable Proxy** to turn if off.
11. Push the converted objects to Intersight as per the steps mentioned in Working with Cisco Intersight Managed Mode Transition Tool

Scenario 2: Proxy Settings only for Intersight Connection

When you are on **Push to Intersight** page, perform the following steps if you need to enable Proxy Settings only for connecting to Intersight.

1. Click **Settings** present under the Gear icon on the top-right corner.
2. Toggle **Enable Proxy** to turn it on.
3. Enter the Proxy Hostname or IP.
4. Enter the Proxy Port number.
5. If your proxy settings require authentication, toggle **Authentication** to turn it on, else go to step 8.
6. Enter the Username.
7. Enter the Password.
8. Click **Save**.

   The Proxy Settings get saved.
9. Click **Next**.
10. Connect to Intersight and Push the converted objects to Intersight as per the steps mentioned in Working with Cisco Intersight Managed Mode Transition Tool
11. Go to the **Settings** section and toggle **Enable Proxy** to turn if off.

Scenario 3: Proxy Settings for UCS device and Intersight Connection

When you log into the IMM Transition Tool, perform the following steps to enable Proxy Settings.

1. Click **Settings** present under the Gear icon on top-right corner.
2. Toggle **Enable Proxy** to turn it on.
3. Enter the Proxy Hostname or IP.
4. Enter the Proxy Port number.
5. If your proxy settings require authentication, toggle **Authentication** to turn it on, else go to step 8.
6. Enter the Username.
7. Enter the Password.
8. Click **Save**.

   The Proxy Settings get saved.

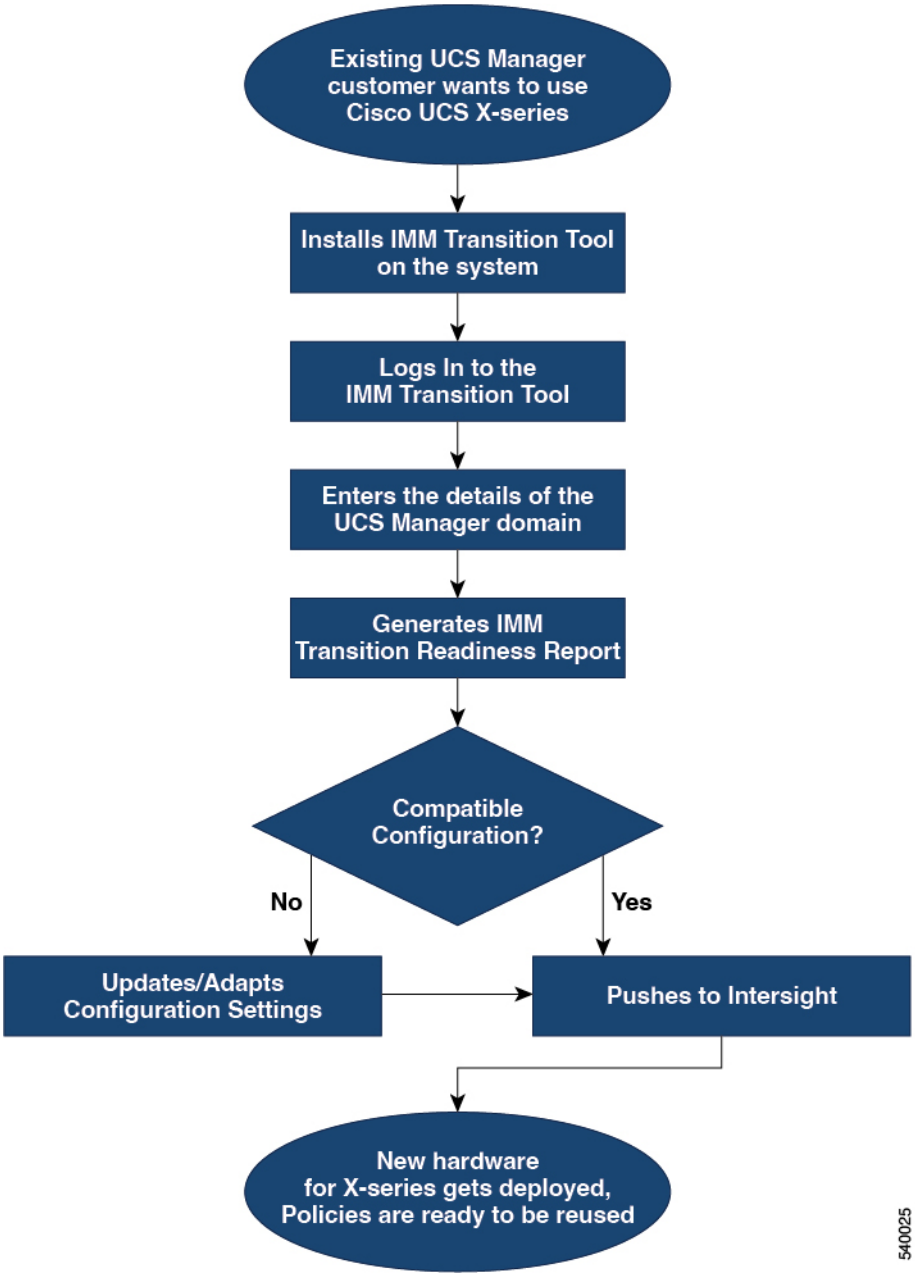
Appendix D: Sample Use Cases

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.



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.

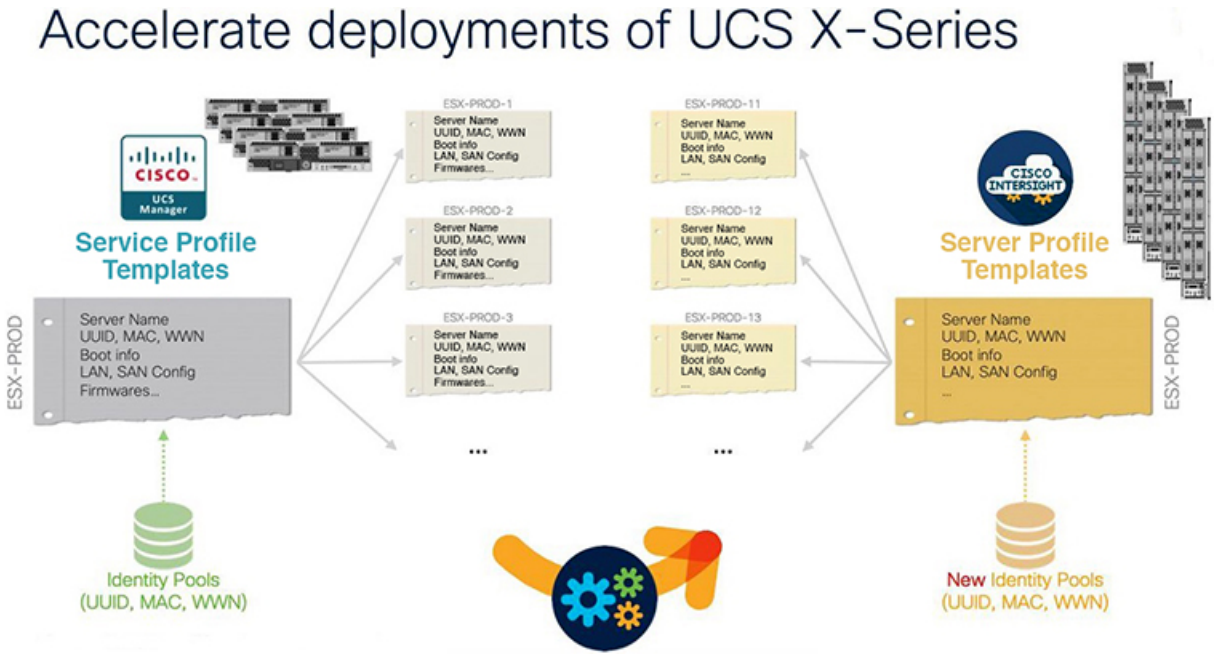
Step 3 Enter the details of the UCS Manager domain.

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 Working with Cisco Intersight Managed Mode Transition Tool

Appendix E: Providing Feedback

Use the **Feedback** icon located at the top-right corner to provide feedback about the tool or provide information about missing features.

Appendix F: 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.