Working with Cisco Intersight Managed Mode Transition Tool

Working with Cisco Intersight Managed Mode Transition Tool

Transition

Perform the following steps to start with the IMM transition:

Step 1 Click **Add IMM Transition**.

Step 2 Enter a name for the Transition.

Step 3 Select a Transition Type.

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

(b) Select **Transition Config to Intersight** if you want to view the readiness report and push the converted configuration to Intersight.

Step 4 Click **Next**.

Step 5 Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer Appendix C: Proxy Settings

Step 6 Enter the UCS Manager device details.

(a) Choose the **Select Existing UCSM Device** option, in case you want to migrate the configuration of the existing device. You can download the Configuration JSON file and Inventory JSON file for the current device using **Download** option.

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

Inventory JSON file contains the detailed information of the hardware inventory present in the existing UCS Manager domain.

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

(b) Choose the **Add New UCSM Device** option if you want to add a new UCS Manager domain configuration. Enter the Device IP/FQDN, Username, and Password for the device.

Step 7 Click **Next**.

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

Step 8 Click **View Report** to view the report or download the report using the **Download** option. The report can be generated for the latest config using the **Re-generate** option.

Step 9 If you have selected (b) in step 3, Click **Next**.

Step 10 Select the radio button for the Intersight Account. Valid options are Intersight SaaS or Intersight Appliance VM.

Step 11 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 3**.

Note OpenAPI schema version 2 is not supported in the IMM Transition Tool.

f. Click **Generate**.

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

Step 12 Complete the following fields:

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

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

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

Step 13

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

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

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

Note When a transition is being pushed to Intersight in an Intersight device or is fetching a UCSM config/inventory from a UCSM device, then the same device cannot be used by other transitions until the previous task on the device completes.

Device Management

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

Perform the following steps to add and manage a device.

Step 1 Navigate to **Device Management**.

Step 2 Click **Add Device**.

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

Step 4 Enter the Target IP/FQDN.

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

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

Step 7 If the Device Type selected in Step 3 is **Intersight**, enter the **API Key**.

Step 8 Enter the **Secret Key**.

Step 9 Click **Save**.
The device details get displayed on the Device Management listing page.

The added device 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.

Interpreting Transition Readiness Reports

The IMM transition readiness report gives a summary of the compatibility of the hardware inventory and software configuration of the UCS Manager domain for transition into IMM.

The Readiness Report is divided into sections as follows:

1. **Conversion Score**- This section shows score meters for Hardware Compatibility, Fabric Configuration, 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, 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.
   - **Intersight Managed Mode Config Conversion Summary** - This section shows the mapping tables for the UCS Manager 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. 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 UCS Manager domain. 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 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.

Converting UCS Domain Configuration

When you add a UCS manager 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 UCS manager domain is compatible with IMM.

It connects to the UCS manager 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.

Note If an object with the same name as the converted object already exists in Intersight, then it gets overwritten by the converted object.

Assumptions for Conversion

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

- **Ethernet Network Control Policy** - Ethernet Network Control Policy of Intersight can be created using two different sources of information of UCS manager.
  - Server vNICs - Maps to Network Control Policy of UCS manager
  - 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, name of the Ethernet Network Control Policy of Intersight will be same as Network Control Policy of UCS manager.

  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.
- **Ethernet Network Group Policy** - There is no Ethernet Network Group Policy equivalent in UCS manager. 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.
- **Ethernet QoS Policy** - QoS Policy of UCS manager is split into Ethernet and FC QoS Policies in Intersight.
- **Fibre Channel Network Policy** - There is no Fibre Channel Network Policy equivalent in UCS manager. 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.
- **Fibre Channel QoS Policy** - QoS Policy of UCS manager is split into Ethernet and FC QoS Policies in Intersight.
- **IMC Access Policy** - Creation of IMC Access Policy for a Service Profile in UCS manager 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. 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, 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 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.

- **IPMI Over LAN Policy** - IPMI Over LAN Policy of Intersight is mapped to IPMI Access Profiles in UCS manager. IPMI User-related information in IPMI Access Profile is moved to Local User Policy in Intersight.
- **iSCSI Boot Policy** - There is no iSCSI Boot Policy equivalent in UCS manager. 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, 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, 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, you have to provide CHAP Password as an input to the Tool. Otherwise Default Password will be considered during Policy creation.
- **iSCSI Static Target Policy** - There is no iSCSI Static Target Policy equivalent in UCS manager. 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.
- **LAN Connectivity Policy** - In UCSM, vNIC can be configured in multiple ways:

  1. Inline vNIC
     - Using Standalone vNIC
     - Using vNIC Templates
  2. LAN Connectivity Policy
     - Using Standalone vNIC
     - Using vNIC Templates

In UCSM, 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.

- **Power Policy** - In UCSM the Power Policy of Intersight is translated as Power Policy section of Global Policies.
- **SD Card Policy** - There is no SD Card Policy equivalent in UCS manager. This policy can be created by reading the information from Local Disk Configuration Policy of UCS manager. If there is Flexflash configured in Local Disk Configuration Policy of UCS manager, then an equivalent SD Card Policy will be created in Intersight.
- **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 UCSM 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 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 which has Specific Storage Profile and Generic Storage Profile should be merged to form a Single Storage Profile in Intersight.
- **VLAN Policy** -

  vLAN Policy of Intersight maps to vLAN Section in UCS manager. In case of 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**.
- **VSAN Policy** -

  vSAN Policy of Intersight maps to vSAN Section in UCS manager. In case of 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**.

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` as per your preference.

Note To know the various conversion options available in the IMM Transition tool, refer Appendix B: Conversion Options.

3. With the updated *convert_option.json* file,
   - you can create a new report for a new configuration.
   - you can regenerate a report for an existing configuration by navigating to **Readiness Report** page.

Note In the Config file, the passwords are stored in encrypted format. If you want to edit the password field then you have to replace the **encrypted_password** field with the **password** field.