Working with Cisco Intersight Managed Mode Transition Tool

Adding an IMM Transition for Conversion

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

Perform the following steps to start with the IMM transition:

Before you begin

You can set the default settings for the transition that will get applied for the current running and all the subsequent transitions. You can also change the default settings during the **Add Transition** process. For details, refer **Default Transition Settings for Conversion** section in Appendix C: Transition Settings.

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 the UCS Manager hardware and configuration or the compatibility of the UCS Central configuration.

(b) Select **Generate Readiness Report** + **Push Config to Intersight** if you want to view the readiness report and push the converted configuration to Intersight.

(c) Select **Clone Intersight** if you want to migrate from one Intersight account to another by cloning the configurations. For the detailed procedure, refer Adding an IMM Transition for Cloning.

Step 4   Click **Next**.

Step 5   Select the Source Device - UCS Manager or UCS Central.

Step 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 Device IP/FQDN, Username, and Password for the device. If required, enable the proxy for the newly added device by turning on the **Use Proxy** toggle button. Add proxy settings details in the **Proxy Settings** interface. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings

Step 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.

Step 8   Click **Next**.

Step 9   Select the destination Intersight Account.

(a) Select **Choose from existing account** option if you want to migrate the configuration to an existing Intersight account. Go to Step 13.

(b) Select **Add new account** option if you want to migrate the configuration to a new **SaaS Intersight** or a new **Intersight Appliance VM** account. Go to Step 11.

(c) Select **Proceed without Intersight device** option if you want to generate the conversion readiness report without adding the details of the destination Intersight account. Go to Step 13.

Step 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.

Step 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.

Step 12   Click **Next**.

Step 13   Configure the conversion options that you want for the transition.

> • For details on each of the Transition Settings field, refer Appendix C: Transition Settings.
>
> • For defining a default set of configurations for every new transition that you create, refer **Default Transition Settings** in Appendix C: Transition Settings.

Step 14   Click **Next**.

Step 15   Select the Service Profiles/Templates that need to be converted.

Next to the profile name, association details with the physical server can be viewed. Hover the mouse pointer over the service profile name to view the description of the Service Profile or Template.

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

You can apply a filter to only display the Service Profile Templates, or both the Service Profiles and Templates in the **Show** drop-down list, located beside the search bar.

Step 16   Click **Next**.

Step 17   Keep **Advanced Organization Mapping** turned on if you want the selected source org(s) to be converted to the mapped destination Intersight org. To manually enter the name of the destination Intersight org, turn off the toggle button, and enter a Root Org name and go to Step 20. You can also retain the source UCS org name in the destination Intersight org by enabling the **Keep source Org path in Intersight Org name** option.

> • This option gives the flexibility to control the mapping of converted objects from UCSM to Intersight. Unlike the same name mapping behavior, customized mapping avoids creating multiple Intersight orgs for an account. The **Advanced Organization Mapping** option can help map single or multiple UCS org(s) to an Intersight org.
>
> • You can also add a new destination Intersight org with the **Add New** option.
>
> • **Note**   If **Keep source Org path in Intersight Org name** option 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.

Step 18   Select the source UCS org, destination Intersight org, and click **Map Now**.
The source org and the destination org get mapped. Once mapped, you will see "Mapped" tag appearing next to the destination Intersight org name. You can also view the mapped source orgs in the mapping section present at the bottom of the **Advanced Organization Mapping** page.

Use the **Un-Map All** option to unmap all 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 on the three dots against it, and selecting the unmap option.

Step 19   Click **Next**.

Next will appear enabled only when the all the source UCS orgs have been selected and mapped to the respective destination Intersight org.

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

Note	Depending on the size of UCS Manager/Central Configurations and number of servers connected, some operations may take a significant amount of time to complete (more than an hour).

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

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.

Step 21 Click **Next**.
Push to Intersight page appears.

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**.

Step 22 Click **Advanced Options**, browse to the edited file, and click **Upload**.
The uploaded file is used for pushing the configuration to Intersight.

Step 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 polices if those have been pushed to Intersight.

Step 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 on the three dots (...) next to each object status displays the detailed commits performed by the IMM Transition Tool in order to push the object to Intersight. The status can be any one of the following:

- Success - The converted object has been pushed successfully to Intersight.

- Skipped - The converted object already exists in the destination Intersight account and has been skipped in the push operation.

- Failed - The converted object could not be pushed to Intersight.

  Click on the three dots present next to the object status to know the reason for push failure.

Adding an IMM Transition for Cloning

Cloning an account in Intersight

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

Step 1 Click **Add IMM Transition**.
Step 2 Enter a name for the Transition.

Step 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 Appendix B: Supported Features for Cloning.

Step 4   Click **Next**.

Step 5   Select the source Intersight account.

(a) Select **Choose from existing account** option, in case you want to migrate the configuration of an existing Intersight account.

(b) Select **Add new account** option, in case you want to migrate the configuration of a new **SaaS Intersight** or a new **Intersight Appliance VM** account. Refer Step 8 and 9 for API Key ID and Secret key details. Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings.

Step 6   Select the destination Intersight Account.

(a) Select **Choose from existing account** option, in case you want to migrate the configuration to an existing Intersight account and then go to step 8.

(b) Select **Add new account** option, in case you want to migrate the configuration to a new **SaaS Intersight** or a new **Intersight Appliance VM** account and then go to step 9. Enable Proxy Settings, if required. To know about the procedure to enable Proxy Settings, refer Appendix D: Proxy Settings.

Step 7   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.

Step 8   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.

Step 9   Complete the following fields:

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

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

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

Step 10   Click **Next**.

Step 11 Configure the conversion options that you want for the transition.

- From IMM Transition Tool, 3.1.1 onwards, you can preserve the assigned IDs on all the UCS server profiles while cloning an account. For more details, refer the **Transition Settings for Cloning** section in Appendix C: Transition Settings.

Step 12 Click **Next**.
Push to Intersight page appears.

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**.

Step 13 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.

Step 15 Click **View Push Summary** to view the push status of each of the converted object.

This summary lets you know the push status for each of the object. Clicking on the three dots (...) next to each object status displays the detailed commits performed by the IMM Transition Tool in order to push the object to Intersight. The status can be any one of the following:

- Success - The converted object has been pushed successfully to Intersight.

- Skipped - The converted object already exists in the destination Intersight account and has been skipped in the push operation.

- Failed - The converted object could not be pushed to Intersight.

  Click on the three dots present next to the object status to know the reason for push failure.

Transition Management

All the transitions that have been initiated by the user are listed on the **Transition** listing page. The page shows the name of the transition, the current status of the transition (Cancelled, Failed, Incomplete, In progress, Completed), type (Generate Readiness Report, Transition Config to Intersight, Clone Intersight), time of last modification.

Click **...** located against each transition record to perform the required action.

Step 1 Click **Report** to view the readiness report for the transition.

This option is not available for cancelled and failed transitions.

Step 2 Click **Edit** to change the transition name.

Step 3 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.

Step 4   Click **Clone** to copy the existing transition config.

4(a) Provide a name for the transition. It appears in the listing page with status as *Incomplete*.

4(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**.

Step 5   Click **Download Logs** to download the conversion logs to a file.

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 Manager** or **UCS Central**, 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 SaaS**, enter the API key/ Secret key. If the Device Type selected in Step 3 is **Intersight Appliance VM**, enter the Target/ API Key/Secret Key.

Step 8   Turn on the **Use Proxy** toggle button to enable proxy settings.

For more details on proxy settings, see Appendix D: Proxy Settings

Step 9   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.

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.

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.
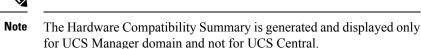
The Readiness Report is divided into sections as follows:

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.

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**.