Transition

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, refer 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 **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.

   (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, refer Adding an IMM Transition to Push the Uploaded Configuration.

4. Click **Next**.

5. Select the Source 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, refer 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 ((o)) , 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 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 10.

   Note From release 4.0.1 onwards, If you select **SaaS Intersight** 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 13.

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 conversion options that you want for the transition.

    • For details on each of the Transition Settings field, refer **B.Transition Settings for Conversion** section in Default Settings.

    • For defining a default set of configurations for every new transition that you create, refer **A. Default Transition Settings for Conversions** section in Default Settings .

14. Click **Next**.

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

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

    You can search for a specific service 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.

    ✎

    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.

16. Click **Next**.

17. Configure the mapping of converted objects from UCSM to Intersight.

The **Advanced Organization Mapping** option can help map single or multiple UCS org(s) to an Intersight Org. Do one of the following:

- Turn on **Advanced Organization 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.

- Turn off **Advanced Organization Mapping**

  a. To manually enter the name of the Destination Intersight Org, enter a Root Org name and go to Step 21.

  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.

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 **Advanced 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**.

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).

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, refer 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 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 polices 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.

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 **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 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. 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 10.

   (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 8. 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 **SaaS Intersight** account, you can also select the region to which the account belongs: **US** or **EU**.

7. Click **Refresh** to retrieve the latest configuration from the existing Intersight account and then go to step 10.

   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.

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.

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.

10. Click **Next**.

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 **C. Transition Settings for Cloning** section in Default Settings.

12. Click **Next**.

13. Select the Server Profiles/Templates, Chassis Profile, or Domain Profile that need to be converted.

- 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.

- If you disable the button, all the Server Profiles, Templates, and their associated policies get cloned.

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.

14. Click **Next**.

Push 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**.

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

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

16. Click **Next**.

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

17. 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 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 **SaaS Intersight** 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 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.

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 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.

   • 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.