Settings

- Default Settings, on page 1
- Proxy Settings, on page 6
- Backup/Restore , on page 7
- Certificate Settings, on page 8

Default Settings

A. Default Transition Settings

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

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

For details on each of the settings field, refer the **Transition Settings for Conversion** and **Transition Settings for Cloning** sections below.

B. Transition Settings for Conversion

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

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

Note Fabric policy conversion is supported for UCSM only.

a. **Fabric Policies Name**

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

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

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

c. **Always create separate VLAN Policies**

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

d. **Always create separate VSAN Policies**

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

e. **Always create separate Port Policies**

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

f. **Preserve Chassis/Rack Server IDs**

- This option is disabled by default.
- When enabled, the chassis/rack server IDs are preserved to the same server ports after transition as the one used in UCSM/Central.

2. **Server Policies Conversion**

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

a. **Service Profiles Conversion**

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

- IQN
- UUID
- WWN

b. Global Service Profiles Conversion

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

Note This conversion is applicable only for UCSM.

c. Preserve Identities

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

d. Root Org Name

- You can manually enter the name of the Intersight Organization to which the UCS Org will get mapped.
- or opt for the default UCS Domain name for the destination Intersight Organization.

e. Keep source Org path in Intersight Org name

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

f. 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".
- You can manually map the vCons to the PCIe slots by providing inputs and overwriting the dafult mapping.

  The supported range for vCon slot value is : 1-15.

- When disabled, the vNICs/vHBAs are configured with Auto PCIe Slot, which will resolve to the first VIC adapter.

g. Use Host Port info for vNIC/vHBA order (use only for VIC1300):

- This option is disabled by default.
- When enabled, vNICs/vHBAs are placed on two PCI Links corresponding to the source Admin Host Port values. This should only be used if the converted profile are assigned to a server with a VIC 1300 model.
- When disabled, all vNICs/vHBAs are mapped to a single PCI Link.

h. 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.

i. Convert Power Policies (Disable it for C-series server)

- This option is disabled by default.
- Power Policy is now supported on Cisco UCS B-Series and Cisco UCS X-Series servers but remains unsupported on Cisco UCS C-Series servers. Enable this option only when converting profiles assigned to Cisco UCS B-Series and Cisco UCS X-Series servers.

j. UCS Central Tags Conversion

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

Note

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

k. UCS Central Tags Prefix

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

Note This conversion is applicable only for UCS Central.

l. Preserve Service Profile Associations

- This option is disabled by default.
- When enabled, Server Profiles are pre-assigned to the same server serial number after transition as the one used in UCSM/Central.

3. **Automatically tag converted objects**
   - This option is enabled by default.
   - When enabled, Intersight objects are tagged with "imm_migration_version": "4.0.1" and "imm_transition_name": "_imm_transition_name_".
   - New tags can be added by clicking on **+ Add new** button and entering the **key-value** pair.
   - Existing tags can be modified and deleted.
   - Tags with keys "imm_migration_version" and "imm_transition_name" cannot be modified but can be deleted.
   - Every tag should have an unique key whereas values can be duplicated.
   - Duplicate tags with same **key-value** pairs are not allowed.
4. **Overwrite existing Intersight objects**
   - This option is disabled by default.
   - When enabled, existing Intersight objects are overwritten if objects with same name and type already exist in the organization. When disabled, any existing object is not changed.
5. **Delete Resource Group Memberships For Shared Orgs**
   - This option is disabled by default.

     Conversion and cloning of shared organizations is now supported.
   - Resource group membership to shared organizations is not supported.
   - When enabled, existing resource group memberships of an organization in Intersight are deleted if the same organization becomes a shared organization after conversion. Disabling this option will result in failures during pushing of the shared organization because Intersight does not support resource group mapping with a shared organization.
6. **Default Password for Converted Policies**

   The default password is used as a replacement for any existing password in UCS Manager/Central policies that are converted, such as Virtual Media, iSCSI Boot, IPMI over LAN. This password gets auto-generated during tool installation. This password should be reset by the user after the converted policies are pushed to Intersight.
7. **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**.

C. Transition Settings for Cloning

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

1. **Overwrite existing Intersight objects**
   - This option is disabled by default.
   - When enabled, existing objects in the destination Intersight will be overwritten, if objects with the same name and type already exist in the source org.
2. **Trim Intersight Settings**
   - This option is enabled by default.
   - When enabled, some of the Intersight settings get trimmed during cloning, such as user groups, users, and roles.
3. **Preserve Identities**
   - This option is enabled by default.
   - When enabled, you can clone an Intersight account while preserving the assigned IDs on all the UCS server profiles.
4. **Preserve Server Profile Associations**
   - This option is disabled by default.
   - When enabled, the Server Profiles associations are preserved while cloning.

Proxy Settings

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

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

Perform the following steps to configure the proxy settings.

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

   The proxy settings get saved.

Note

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

Backup/Restore

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

Perform the following steps to backup and restore the data.

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

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

   The data present in the file gets restored.

Note

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

Certificate Settings

IMM Transition Tool, Release 4.1.2 allows you to authenticate your secure connection to the tool. You can now create and upload Certificate Authority (CA)-signed secure sockets layer (SSL) certificate for the web server. You can also reset or renew this certificate.

Creating and Uploading Certificate

Perform the following steps to create and upload a CA-signed SSL certificate:

- Click **Certificate Settings** present under the gear icon on the top-right corner.
- Create a certificate signing request (CSR) by filling up the fields below:
  1. **Organization**: Enter the name of your organization
  2. **Organization Unit**: Enter the name of the division of your organization that handles the certificate
  3. **Locality**: Enter the name of the city where the organization is located.
  4. **State**: Enter the name of the state where the organization is located.
  5. **Country**: Enter the name of the country where the organization is located.
  6. **Email Address**: Enter the email id of your organization.
  7. **Modulus**: Enter the length of the RSA key (in bits) for both private and public keys.
  8. Click **Create CSR**.
- Download the created CSR and use it to obtain a signed SSL certificate from the CA.
- Navigate to the **Apply Certificate** tab, once you have the signed certificate.
- Browse and upload the signed certificate.
- Click **Apply Certificate**.

The certificate will get applied to the IMM Transition Tool.

Note To generate a Certificate Signing Request (CSR) successfully:

1. Ensure that the virtual machine (VM) has a valid Fully Qualified Domain Name (FQDN).
2. Set the FQDN using the following command:

   ```
   sudo hostname --fqdn <fqdn>
   ```
3. Replace <fqdn> with the desired FQDN for the VM.

Renewing Certificate

Perform the following steps to reset or renew the SSL certificate:

- Click **Certificate Settings** present under the gear icon on the top-right corner.

- Create a CSR using the steps mentioned in the Creating and Uploading Certificate section.
- Get the SSL certificate signed from the Certificate Authority (CA)

Note If you want to renew the self-signed certificate, follow the CLI commands as mentioned in Appendix A : Management Operations Using CLI

- Navigate to the **Apply Certificate** tab, once you have the CA-signed certificate.
- Browse and upload the signed certificate.
- Click **Apply Certificate**.