Cisco Intersight Managed Mode Transition Tool User Guide, 2.0

First Published: 2022-04-29

Last Modified: 2022-05-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

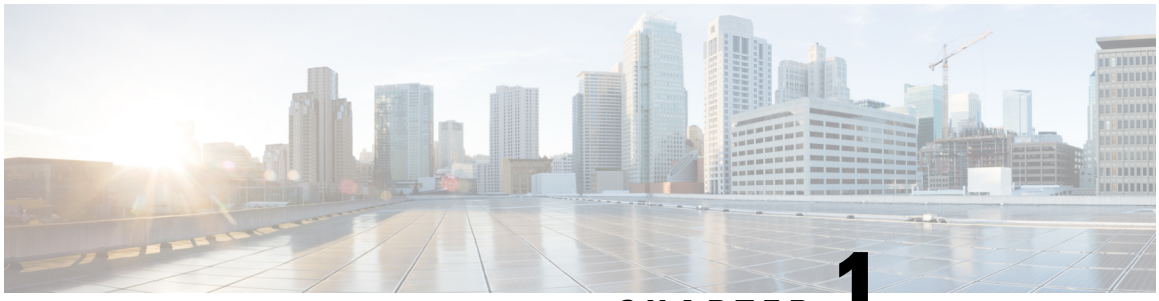
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Communications, Services, Bias-free Language, and Additional Information



CHAPTER 1

New and Changed Information

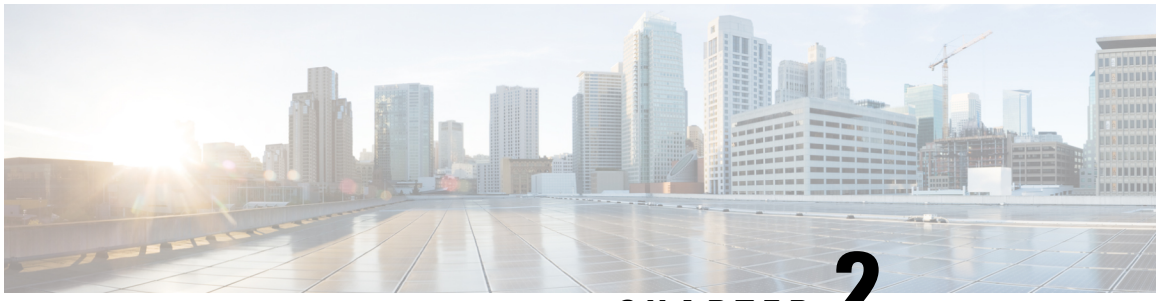
New and Changed Information

This section provides information on new features and changed behavior in Cisco Intersight Managed Mode Transition Tool, Release 2.0.

Table 1: New Features and Changed Behavior in Intersight Managed Mode Tool, Release 2.0.1

Feature	Description	Where Documented
Support for UCS Central	Cisco Intersight Managed Mode (IMM) Transition Tool, Release 2.0.1, introduces the ability to transition the Service Profile Templates from UCS Central to Intersight.	Overview
Service Profile/Template-based conversion	IMM Transition Tool, Release 2.0.1 converts only the policies that are attached to the selected Template(s).	Working with Cisco Intersight Managed Mode Tool
Selective conversion of Service Profile Templates	In IMM Transition Tool, Release 2.0.1, you can selectively convert Service Profile Template(s) to Intersight.	Working with Cisco Intersight Managed Mode Tool
Cloning of Transition	IMM Transition Tool, Release 2.0.1, allows you to clone any existing transition, edit the cloned configuration, and generate readiness report.	Transition Management in Working with Cisco Intersight Managed Mode Tool

Feature	Description	Where Documented
Transition Settings	With IMM Transition Tool, Release 2.0.1, you can set the conversion options to control the behavior of the transition.	Appendix B: Transition Settings



CHAPTER 2

Overview

Overview

Cisco Intersight Managed Mode (IMM) Transition Tool helps bootstrap new IMM deployments by replicating the configuration attributes of the existing Cisco UCS Manager (UCSM) and Cisco UCS Central infrastructure, and by converting the existing Service Profile Templates to IMM Server Profile Templates to accelerate deployment of new servers in IMM.

IMM Transition Tool offers the following functionality:

- Ability to validate hardware compatibility for Cisco UCS Manager domain.
- Fetching entire configuration from running UCS Manager domain or UCS Central instance.
- Ability to validate what part of the configuration is available in Intersight.
- Performing conversion of the UCS Manager or UCS Central configuration attributes to IMM.
    - Conversion of the running configuration of the UCS Manager domain is primarily done in two parts (you can selectively enable/disable each section for config conversion):
        - Convert the fabric configuration of the UCS Manager domain including VLANs/VLAN Groups/VSANs, Port roles, QoS, and administrative settings (NTP/DNS/SNMP/SYSLOG).
        - Convert the Service Profile Templates from the UCS Manager domain and all the attached policies to the best extent possible.
    - Conversion of the running configuration of the UCS Central instance is primarily done as follows (you can selectively enable/disable each section for config conversion):
        - Convert the Service Profile Templates from the UCS Central instance and all the policies attached to the template to the best extent possible.

Note Fabric configuration conversion for UCS Central can be achieved by performing a fabric conversion of the corresponding UCS Manager domain(s).

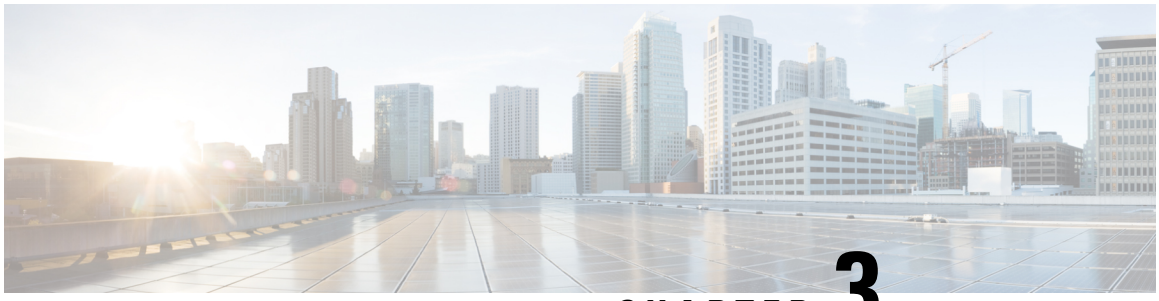
- Generation of IMM readiness report that can be used to get an overview of the compatibility of the hardware and configuration when the domain is converted from UCS Manager or UCS Central to IMM.

Note As Cisco UCS Central can be registered with multiple UCS Manager domains, the Hardware Compatibility is only available for a UCS Manager domain and not for the UCS Central instance itself.

The IMM readiness report provides:

- A conversion score and overall summary showing an overview of readiness of the UCS Manager or UCS Central device for migration into IMM.
- The detailed information for each configuration, such as converted objects and the objects that the tool could not convert.

Note If your UCSM domain has any HyperFlex cluster deployed, do not migrate to IMM. HyperFlex servers are not currently supported in IMM.



CHAPTER 3

Getting Started with Cisco Intersight Managed Mode Transition Tool

Prerequisites

This section covers the minimum requirements for installing Cisco Intersight Managed Mode Transition Tool:

- Supported version of Cisco UCS Manager: 3.2(1d) or above.
- Supported version of Cisco UCS Central: 2.0(1a) or above.
- Supported ESX version - ESXi 6.0 and above.
- Minimum VM requirement - 2 vCPUs, 8 GB RAM, 100 GB storage.
- Virtual Hardware Version used by the OVA - 11
- Network Connectivity Requirements:
  - TCP Port 443(HTTPS) (from IMM Transition Tool, Release 1.0.2 onwards)
  - TCP Port 22 (SSH) for troubleshooting or advanced configuration.
  - Access to the following is required:
    - DNS (using TCP/UDP Port 53)
    - NTP (using UDP Port 123)
    - UCS Manager/UCS Central devices (using TCP Port 443 [HTTPS] only)
    - Intersight devices (using TCP Port 443 [HTTPS] only)
    - Connection to the proxy server settings (if any)
  - Pushing Config to Intersight requires HTTPS connectivity to the Intersight instance.
    - For SaaS, the URL is https://www.intersight.com

- For Appliance, the URL is provided by the user.

Installing Cisco Intersight Managed Mode Transition Tool

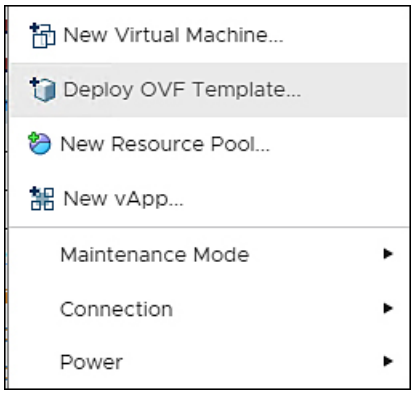
An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco Intersight Managed Mode Transition Tool OVA has a preinstalled operating system and includes application functionality that is necessary for the IMM Transition Tool functionality. The IMM Transition Tool as an OVA can be deployed on a VMWare Vsphere infrastructure.

Before you begin

- From the UCS Tools page, download the IMM Transition Tool .ova file to your computer in a place that is easy to find when you start to deploy the OVF template.

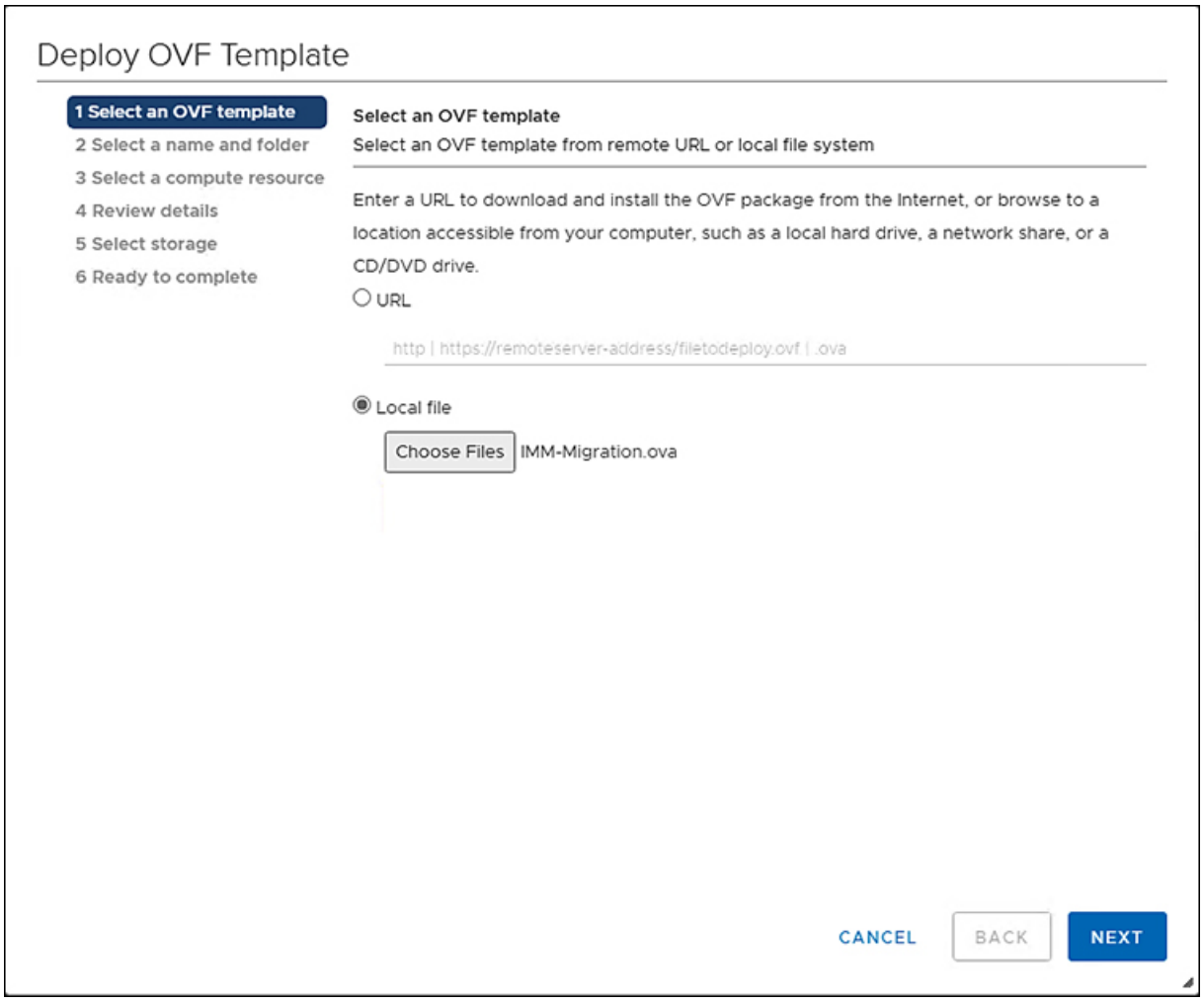
Step 1 Log into the HTML5 vSphere Web Client and go to the **VMs** tab.

Step 2 Add the **Deploy OVF Template** action button via the *Actions* dropdown list.



Step 3 Click the added **Deploy OVF Template** button.

A new window appears, asking to select a template.

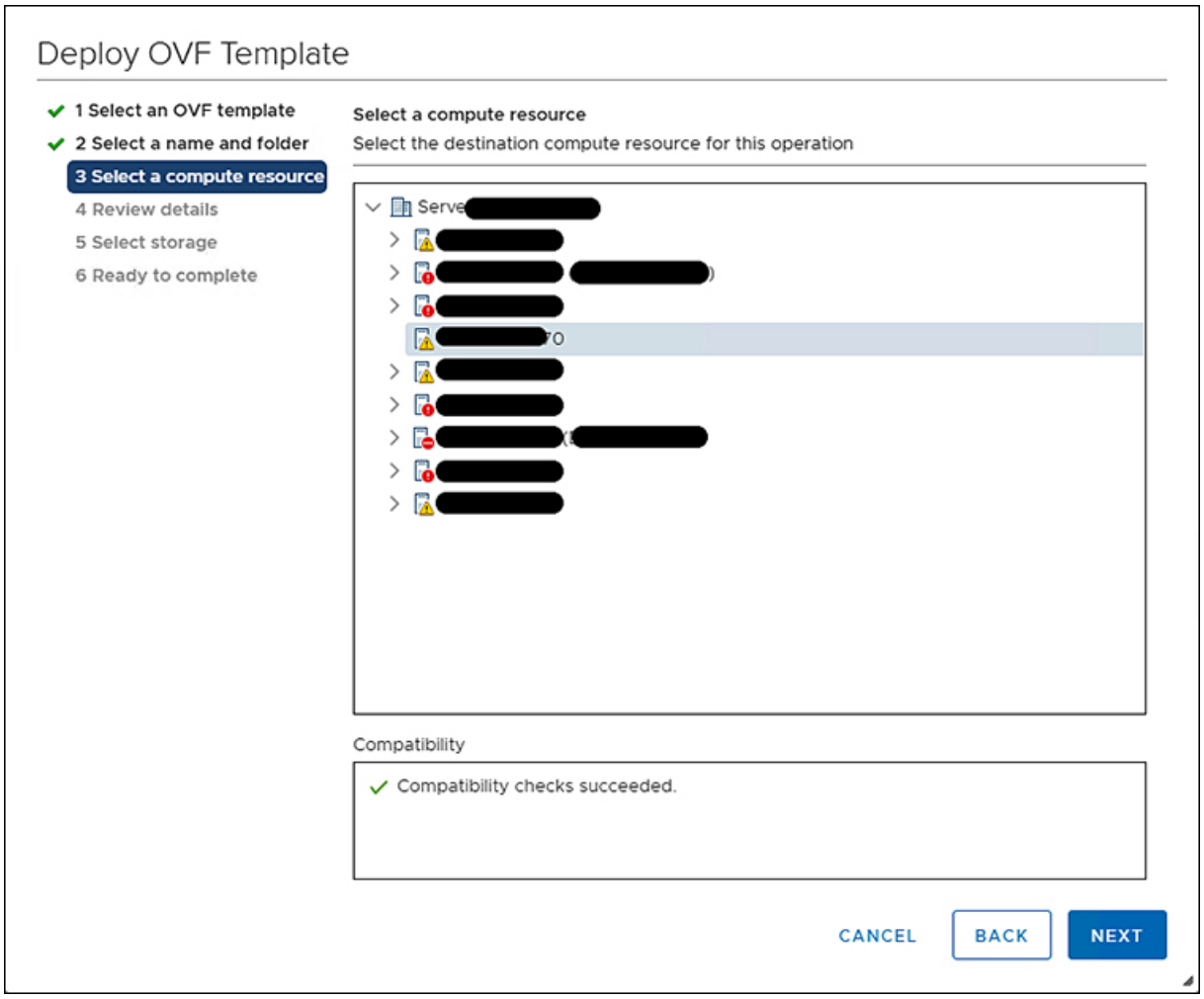


Step 4 Click the **Choose Files** button and select the downloaded OVA file.

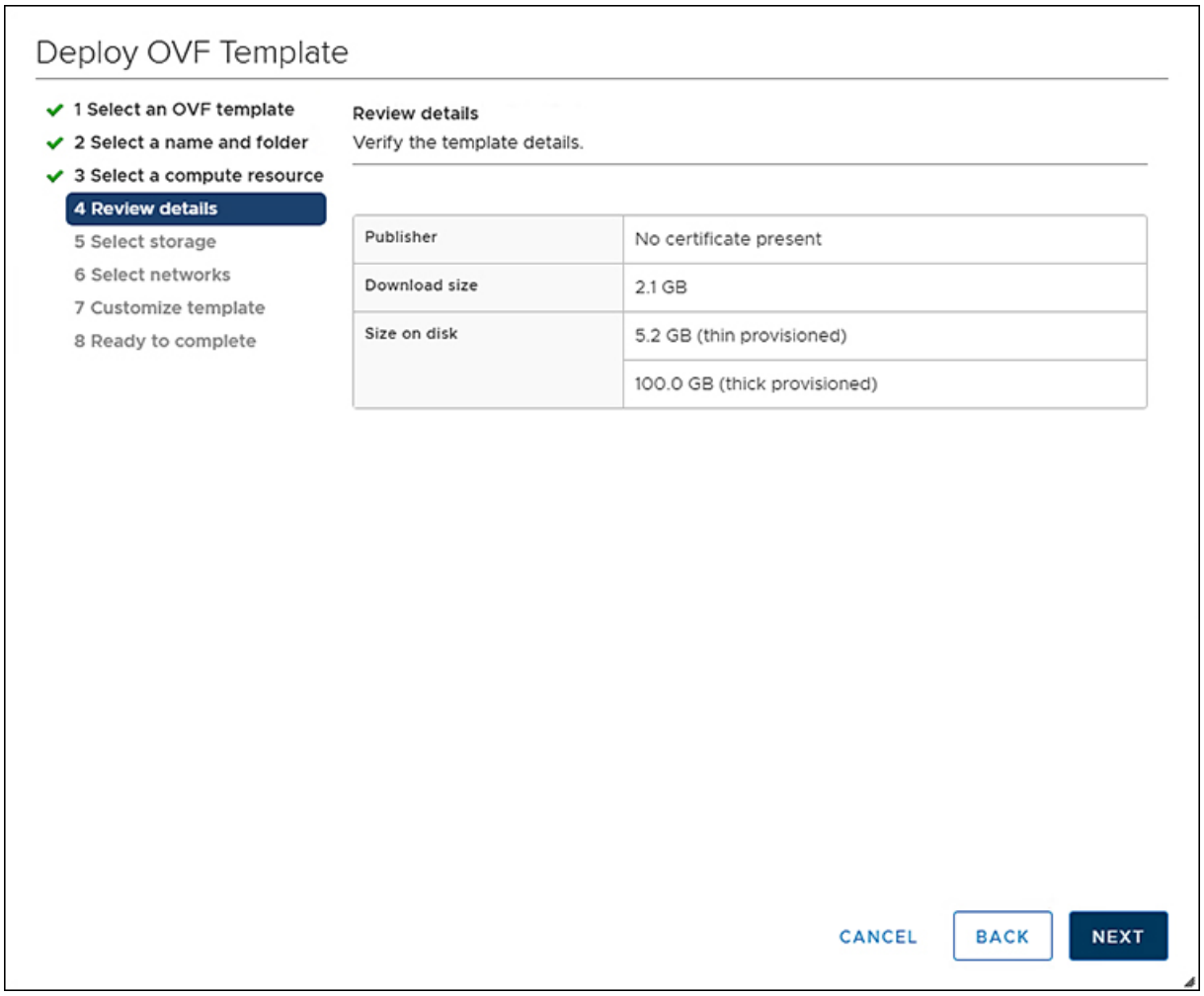
Step 5 Click **Next**.

Step 6 Select the location where you want to deploy the virtual appliance, then click **Next**.

Step 7 Select the resource you want to use to run the virtual appliance, click **Next** .

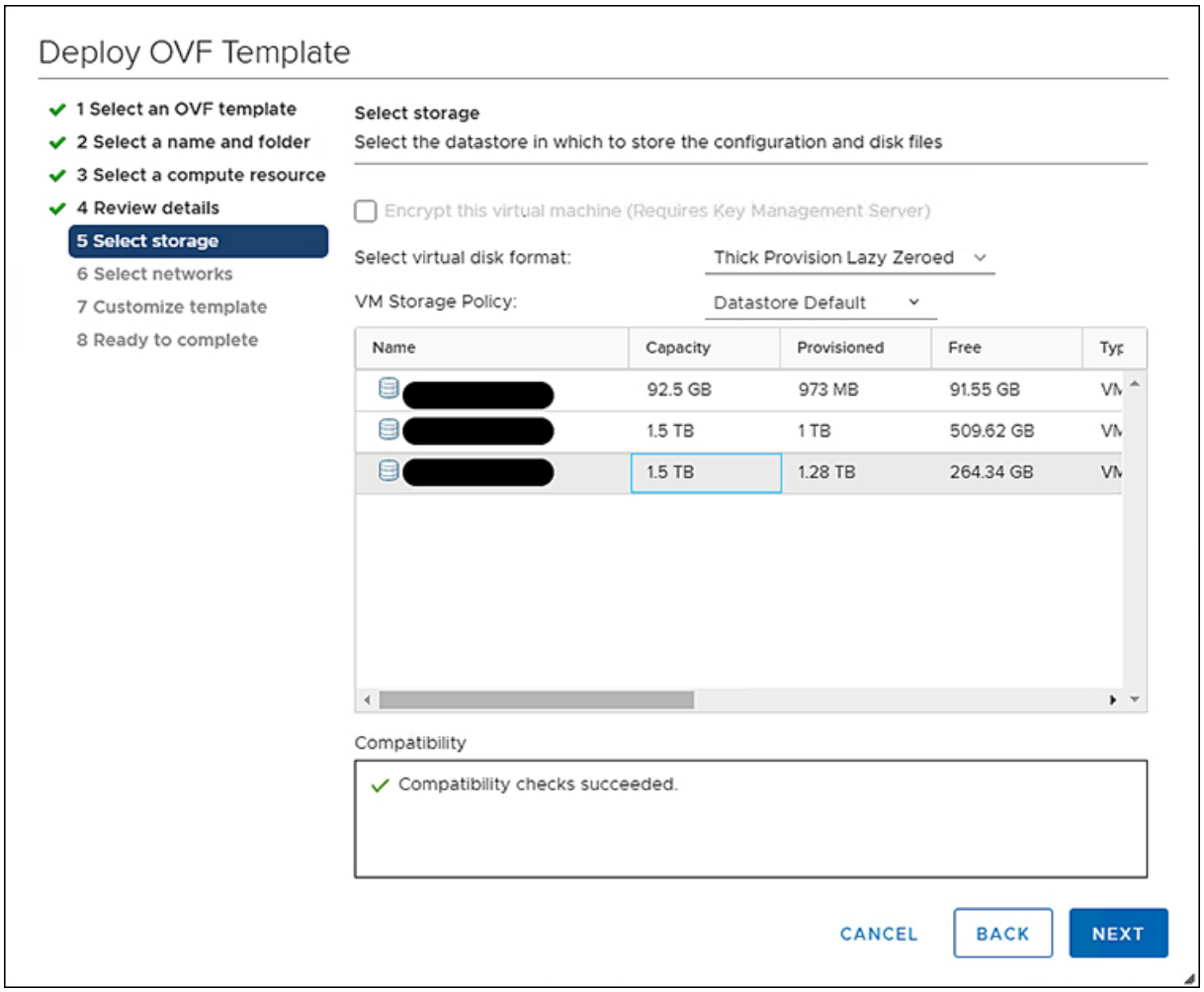


Review the package details, that contain advanced configuration options.

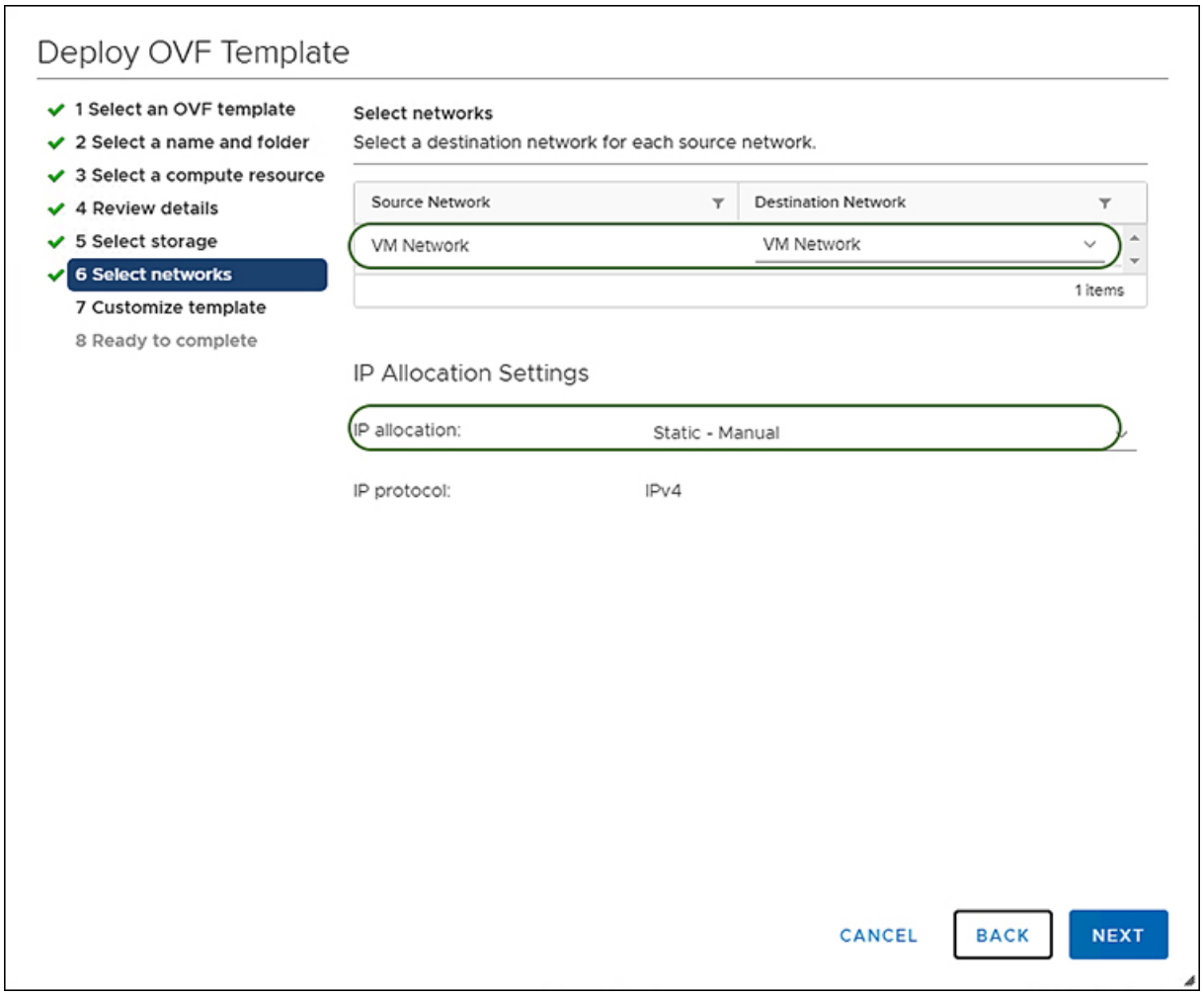


Step 8 Click **Next** to accept these options.

Step 9 Select the desired storage location from the list of datastores, then click **Next**.

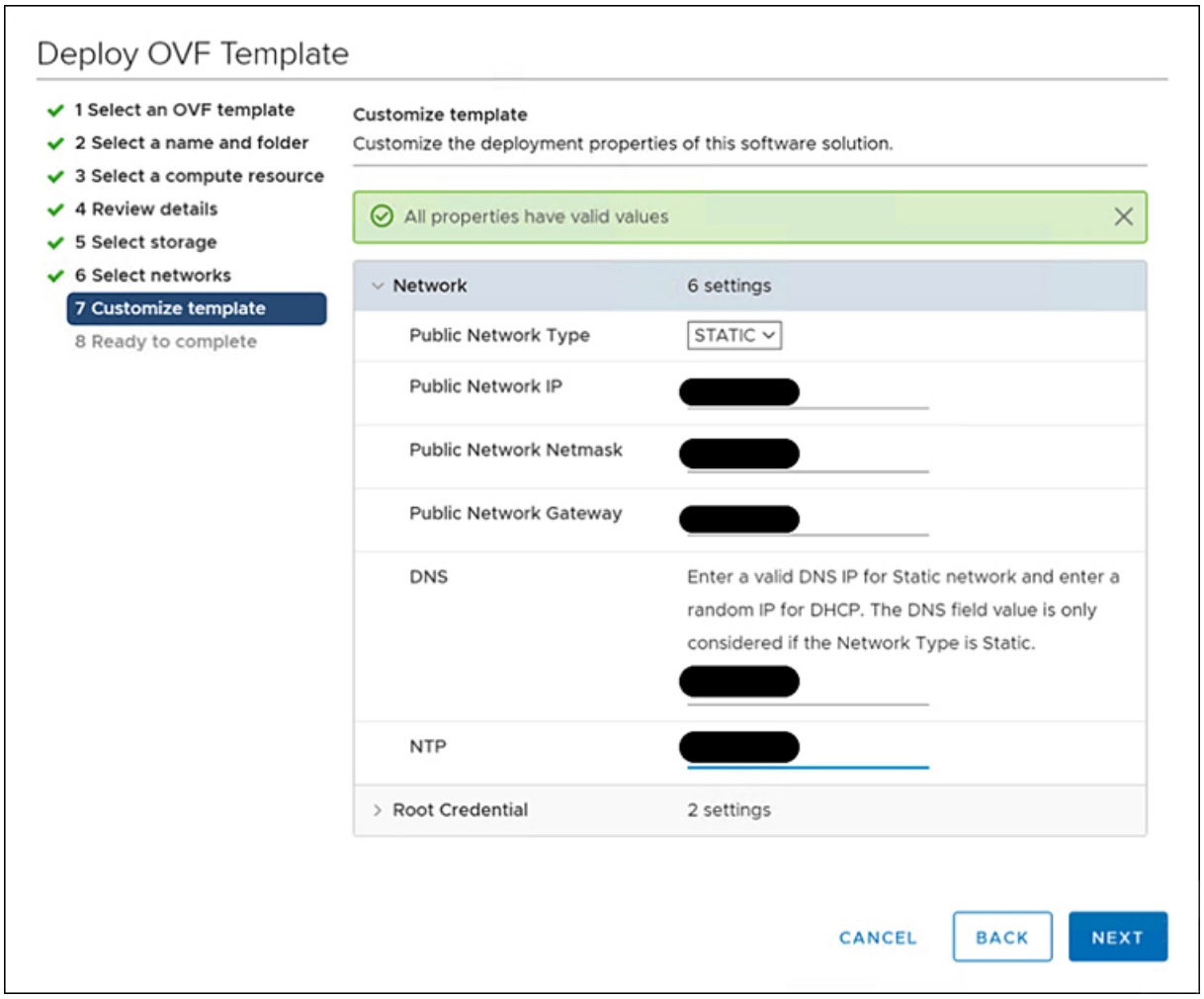


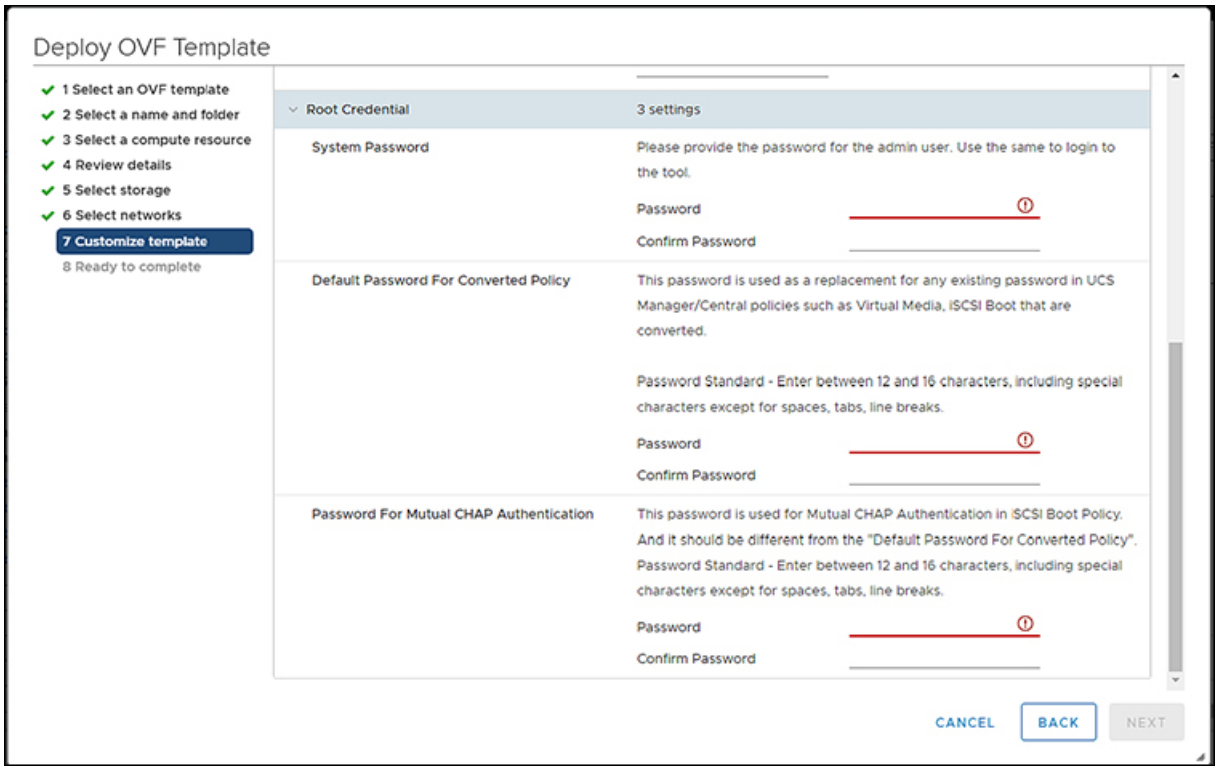
Step 10 Select a destination network from the dropdown list for each source network, click **Next**.



Step 11 Customize the template by entering the **Network** settings values and setting up **System Password**, a **Default Password For Converted Policy**, and a **Password For Mutual CHAP Authentication**.

The **Default Password For Converted Policy** is used as a replacement for any existing password in UCS Manager/UCS Central policies such as Virtual Media, iSCSI Boot that are converted. It should be between 12 to 16 characters, including special characters except for spaces, tabs, line breaks. The **Password For Mutual CHAP Authentication** is used for Mutual CHAP Authentication in iSCSI Boot Policy. It should be different from the **Default Password For Converted Policy**. It should be between 12 to 16 characters, including special characters except for spaces, tabs, line breaks.


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Network
6 settings
Public Network Type
STATIC
Public Network IP
Public Network Netmask
Public Network Gateway
DNS
Enter a valid DNS IP for Static network and enter a random IP for DHCP. The DNS field value is only considered if the Network Type is Static.
NTP
Root Credential
2 settings
CANCEL
BACK
NEXT



Step 12 Click **Next**.

Review the configuration data.

Step 13 Click the **Refresh** button to update the system.
The VM will be visible in the center windowpane.

Step 14 Select the VM and click **Power On**.

Step 15 Once the VM is powered on, click the **Open Console** icon to open the VM console in a new window.

You have successfully deployed the OVA template and powered on the VM.

Accessing Cisco Intersight Managed Mode Transition Tool using the Graphical User Interface

You can access the user interface of the Cisco IMM Transition Tool through browser window, to generate transition readiness report, and convert UCS domain into IMM configuration.

Step 1 Launch a Web browser window.

Step 2 Enter `http://<VM IP address>` or `https://<VM IP address>`. VM IP address is the IP address of the VM where you have deployed Cisco IMM Transition Tool OVA.

IMM Transition Tool, Release 1.0.2 and above, provides HTTPS support. All the `http` URLs get redirected to `https`.

Step 3 In the Login dialog box, enter the user name and password.

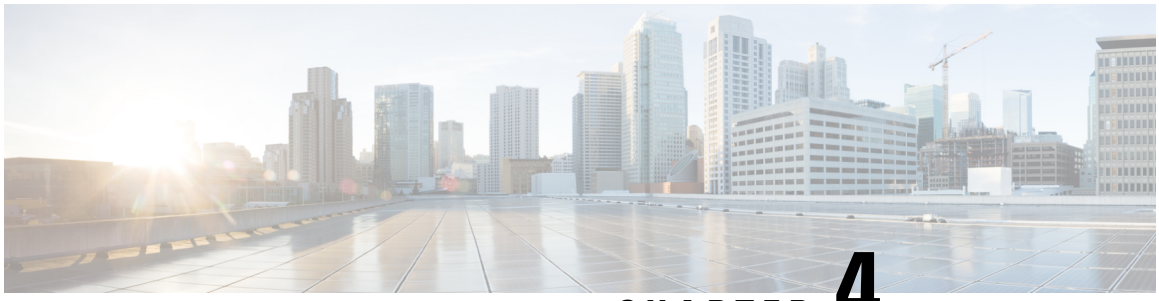
User name: admin

Password: Enter the password set on the **Customize template** page during installation.

Step 4 Click **Sign In**.

To end the user session, click **Log Out** from the user settings in the top-right corner.

Note **Session Timeout**—In IMM Transition Tool, Release 1.0.2 onwards, if you remain inactive for 30 min, you are automatically logged out of the session. You have to relogin to use the application again.



CHAPTER 4

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 the UCS Manager hardware and configuration or the compatibility of the UCS Central 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 Select the Source Device - UCS Manager or UCS Central.

Step 7 Enter the selected device details.

(a) Choose the **Select Existing UCS Manager/ Select Existing UCS Central** option, in case you want to migrate the configuration of the 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.

Step 8 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 9 Click **Next**.

Step 10 Configure the conversion options that you want for the transition.

For details on each of the Transition Settings field, refer Appendix B: Transition Settings.

Step 11 Click **Next**.

Step 12 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 13 Click **Next**.

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 14

Note 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.

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

Step 15 If you have selected (b) in step 3, Click **Next**.

Step 16 Select the radio button for the Intersight Account. Valid options are Intersight SaaS or Intersight Appliance VM.

Step 17 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 18 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 19 **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 20 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.

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), 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.

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.

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 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 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.

Converting UCS Manager/Central Configuration

When you add a UCS Manager/Central 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:

- **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.
- **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.
- **Ethernet QoS Policy** - QoS Policy of UCS Manager/Central 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/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.
- **Fibre Channel QoS Policy** - QoS Policy of UCS Manager/Central 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/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.
- **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.
- **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, 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/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.
- **LAN Connectivity Policy** - In UCS Manager/Central, 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

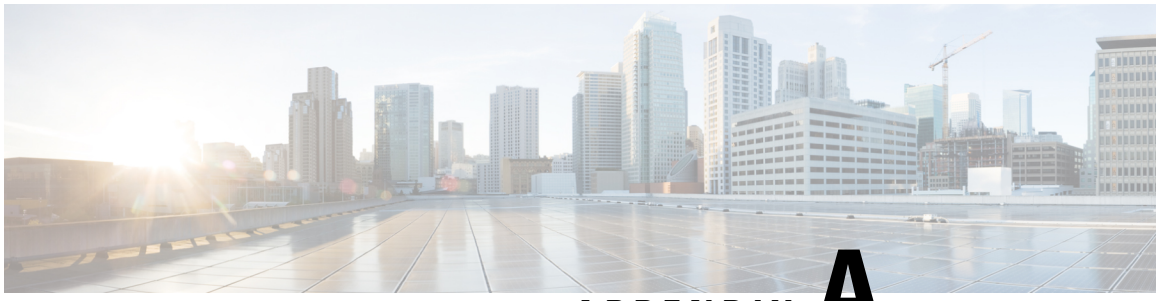
In UCS Manager/Central, it can be either a LAN/SAN Connectivity Policy, or inline vNIC/vHBA that can be using vNIC/vHBA Templates or not. All possible combinations are considered and accordingly converted into LAN/SAN Connectivity Policies in Intersight, as it is the only way to configure connectivity.

- **Power Policy** - In UCS Manager, the Power-related section of Global Policies is translated as a Power Policy in Intersight.
- **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.
- **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 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 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 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**.



APPENDIX A

Appendix

Appendix A: Supported IMM Features/Policies

This section provides a list of features that are supported for conversion in the IMM Transition Tool and a policy mapping between Cisco UCS Manager/Central and Intersight.

Note If the UCS Central configuration contains VLAN/VSAN aliasing, the IMM Transition Tool will automatically select one of the aliases when performing the conversion of the vNICs/vHBAs. Carefully review the resulting configuration to make sure it is appropriate.

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Admin	Communication Services *4	SNMP Policy
	Organizations	Intersight Organizations
	Syslog *5	Syslog Policy
	Time zone Management	NTP Policy
	MAC Address Table Aging	Switch Control Policy
	VLAN Port Count Optimization	Switch Control Policy
	Inband Profile VLAN Group	Ethernet Network Group Policy
	Inband Profile Network	IMC Access Policy
	Inband Profile IP Pool Name	IMC Access Policy
	FC Uplink Trunking	VSAN Policy
	DNS *6	Network Connectivity Policy

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Server Policies and Chassis Policies	BIOS Policies	BIOS Policy
	Boot Policies	Boot Policy iSCSI Static Target Policy
	Disk Group Policies	Storage Policy
	IPMI Access Profiles	IPMI over LAN Policy
	iSCSI Adapter Policies	iSCSI Adapter Policy
	iSCSI Boot Policies	iSCSI Boot Policy
	KVM Management Policies	Virtual KVM Policy
	Local Disk Config Policies *7	Storage Policy, SD Card Policy
	QoS Policies	Ethernet QoS Policy/ FC QoS Policy
	Serial over LAN Policies	Serial over LAN Policy
	Service Profiles	Server Profile
	Service Profile Templates *8	Server Profile Template
	Storage Profiles	Storage Policy
	vMedia Policies	Virtual Media Policy
	vNIC/vHBA Placement Policies *9	LAN Connectivity Policy/SAN Connectivity Policy
	Ethernet Adapter Policies	Ethernet Adapter Policy
	Flow Control Policies	Flow Control Policy
	LACP Policies	Link Aggregation Policy
	LAN Connectivity Policies	LAN Connectivity Policy
	Link Protocol Policy	Switch Control Policy
	Multicast Policies	Multicast Policy
	Network Control Policies	Ethernet Network Control Policy
	Fibre Channel Adapter Policies	Fibre Channel Adapter Policy
	SAN Connectivity Policies	SAN Connectivity Policy

UCS Manager/ UCS Central Feature Category	Source UCS Manager/UCS Central Feature Name	Equivalent IMM Policy
Pools	IP Pools	IP Pool
	IQN Suffix Pools	IQN Pool
	MAC Pools	MAC Pool
	WWNN Pools	WWNN Pool
	WWPN Pools	WWPN Pool
	Server Pools *10	Resource Pool

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

UCS Manager Feature Category	Source UCS Manager Feature Name	Equivalent IMM Policy
Fabric Config *1	Appliance VLANs	VLAN Policy
	QoS System Class	System QoS Policy
	VLAN Groups	Ethernet Network Group Policy
	VLANs *2	VLAN Policy
	VSANs	VSAN Policy
	Storage VSANs *10	VSAN Policy
Fabric Policies *3	Appliance Network Control Policies	Ethernet Network Control Policy
	UDLD Link Policies	Link Control Policy
Port Roles	Appliance Ports	Port Policy
	Appliance Port-Channels	Port Policy
	FCoE Uplink Ports	Port Policy
	FCoE Uplink Port-Channels	Port Policy
	LAN Uplink Ports	Port Policy
	LAN Uplink Port-Channels	Port Policy
	SAN Unified Ports	Port Policy
	SAN Uplink Ports	Port Policy
	SAN Uplink Port-Channels	Port Policy
	Server Ports	Port Policy
	FC Storage Ports *10	Port Policy
	SAN Storage Ports *10	Port Policy

*1 - Merged with regular VLANs

*2 - No support for PVLAN

*3 - Merged with regular Network Control Policies

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

*5 - Only supports up to two remote destination servers

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

*7 - Replaced by Storage Policy

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

*9 - The placement is statically mapped to PCIe slots, with the following mapping:

- vCon 1: Slot MLOM
- vCon 2: Slot PCIe1
- vCon 3: Slot PCIe2
- vCon 4: Slot PCIe3

This placement can be manually adjusted as needed after conversion is performed.

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

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

Appendix B: Transition Settings

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

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

Note Fabric policy conversion is supported for UCSM only.

    a. **Fabric Policies Name**

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

b. Target Org Name for Fabric Policies

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

c. Always create separate VLAN Policies

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

d. Always create separate VSAN Policies

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

e. Always create separate Port Policies

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

2. Server Policies Conversion

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

a. Service Profiles Conversion

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

b. Global Service Profiles Conversion

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

Note This conversion is applicable only for UCSM. UCS Central templates get converted by default.

c. Root Org Name

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

d. Keep source Org path in Intersight Org name

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

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

e. Use vCon placement info for vNIC/vHBA order

- This option is disabled by default.
- When enabled, vNICs/vHBAs get statically mapped to different PCIe slots depending on their source vCon.
- vCon any, 1: "PCIe MLOM", vCon2: "PCIe slot 1", vCon3: "PCIe slot 2" and vCon4: "PCIe slot 3".
- When disabled, all vNICs/vHBAs get mapped to PCIe slot "MLOM".

f. Automatically change long org names (>17 chars)

- This option is disabled by default.
- If enabled, the organization names that are longer than 17 characters are changed to automatically generated names. This prevents errors when the combined length of the organization name and QoS policies exceeds 40 characters.

3. Automatically tag converted objects

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

4. Overwrite existing Intersight objects

- This option is disabled by default.
- When enabled, existing Intersight objects are overwritten if objects with same name and type already exist in the organization. When disabled, any existing object is not changed.

5. **Default Password for Converted Policies**

   The default password is used as a replacement for any existing password in UCS Manager/Central policies that are converted, such as Virtual Media, iSCSI Boot, IPMI over LAN.

6. **Password for iSCSI Mutual Chap Authentication**

   This password is used for Mutual CHAP Authentication in iSCSI Boot Policy. It must be different from the **Default Password for Converted Policies**.

Appendix C: Proxy Settings

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

Scenario 1: Proxy Settings only for UCS device Connection

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

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

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

Scenario 2: Proxy Settings only for Intersight Connection

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

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

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

Scenario 3: Proxy Settings for UCS device and Intersight Connection

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

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

   The Proxy Settings get saved.

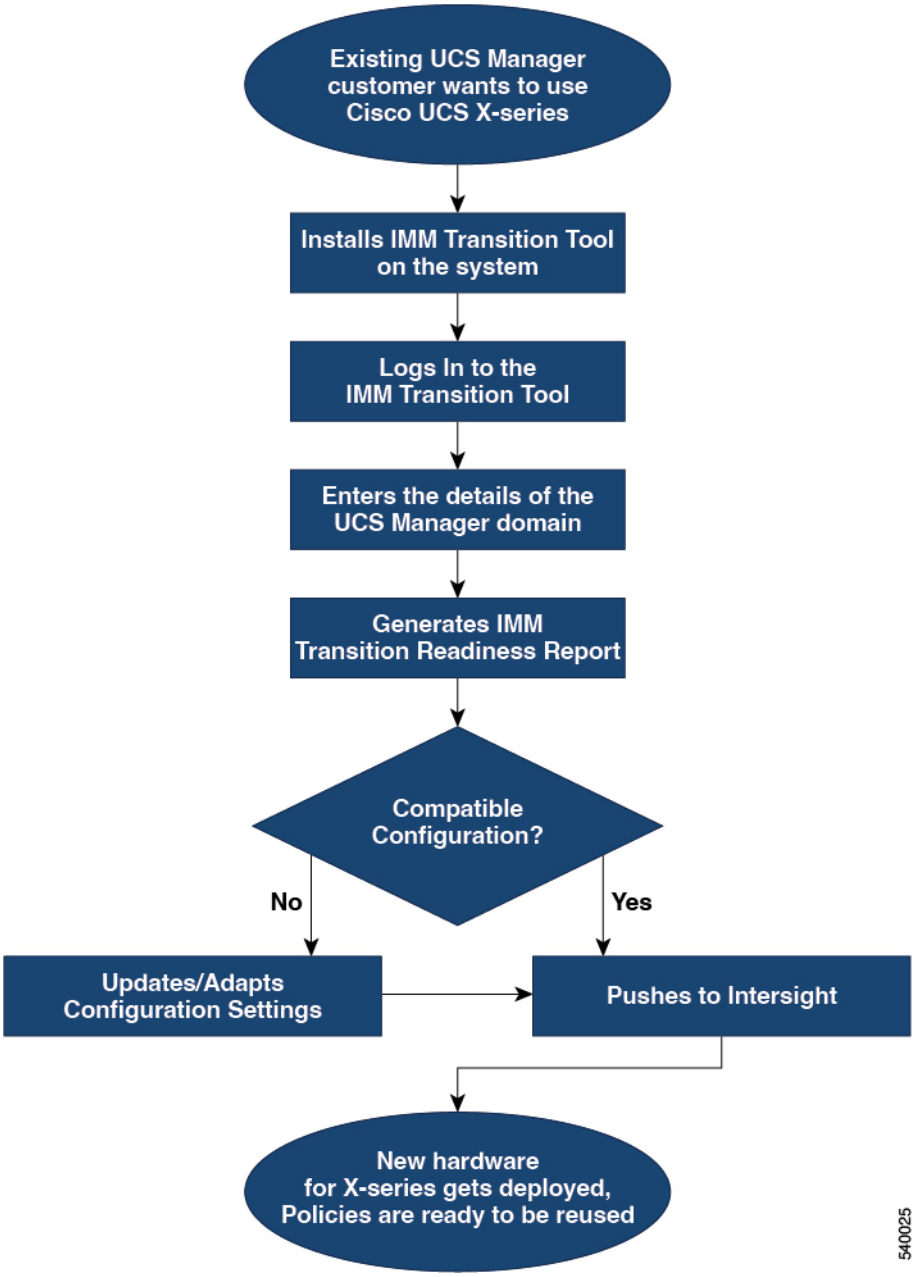
Appendix D: Sample Use Cases

Accelerate deployments of UCS X-Series

When supporting the UCS X-Series, the fabric interconnects run in Intersight Managed Mode. If you are using Cisco UCS Manager and want to use UCS X-series, then you have to transition to IMM. This transition

- Extends existing Service Profile Templates to Intersight.
- Automatically converts related server policies such as Boot, BIOS, LAN/SAN connectivity.

• Converts fabric configuration such as VLANs/VSANs, port configuration.



Perform following steps to convert the existing UCS Manager domain objects to Intersight objects.

Before you begin

Your system must meet the prerequisites mentioned in the Prerequisites section.

Step 1 Install Cisco IMM Transition Tool in your system.

Follow the Installation procedure mentioned in Installing Cisco Intersight Managed Mode Transition Tool

Step 2 Log into the IMM Transition Tool.

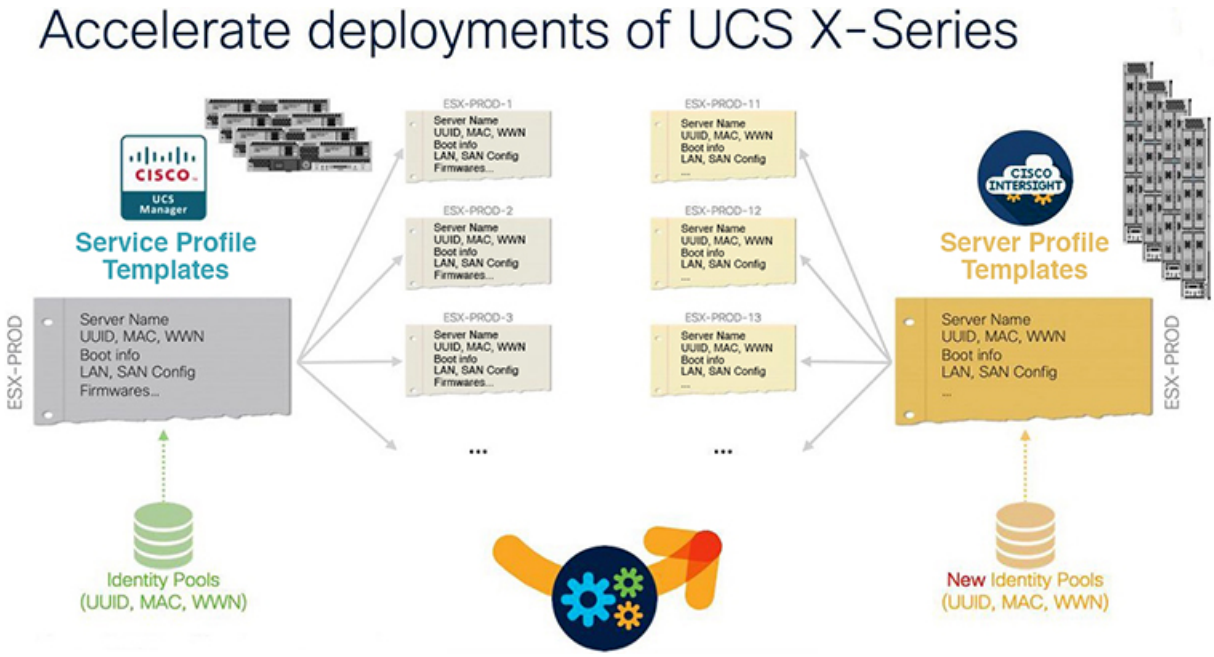
Step 3 Enter the details of the UCS Manager domain.

Step 4 Generate the readiness report to check the compatibility for transition.

Step 5
a) If incompatible, update configuration settings.
b) When compatible, push the converted configuration to Intersight.

What to do next

The new hardware gets deployed. The software configuration of the UCS Manager domain, and the existing policies are ready to be reused. You can now monitor the Cisco UCS X-Series systems from anywhere and perform Policy-based management across the servers.



For the steps on performing this transition, see Working with Cisco Intersight Managed Mode Transition Tool

Appendix E: Providing Feedback

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

Appendix F: Technical Support

In case you need any assistance, you can share the logs file with the technical team.

Perform the following steps to send your query:

1. Go to the list view displaying all the transition records.

2. Scroll down to the transition record for which you need technical assistance.
3. Click **…** present against the record.
4. Click **Download Logs**.
5. Save the logs file in your computer.
6. Attach the saved logs file to the email and send the email with your queries/feedback to the imm-transition-feedback@cisco.com group.