Cisco Intersight Management

Intersight Management Mode

Intersight Managed Mode (IMM) is a new set of features introduced in Cisco Intersight to configure, deploy, and manage a Server Profile for B-Series blade and FI-managed C-Series servers. IMM introduces a new implementation of concepts first introduced with Cisco UCS Manager and moves ownership of the policy model into Cisco Intersight. Hence, policies, VLANs, and VSANs are created in advance and built into a Server Profile. Then, the Server Profile is assigned and deployed to a Cisco Intersight discovered B-Series blade or managed C-Series servers.

To enable IMM in a fourth generation Fabric Interconnect (FI), perform a normal upgrade to Cisco UCS Infrastructure and server firmware (FW) (4.1(2)) and then reset the FI after successful upgrade. After FI reset, in the setup prompt, choose Intersight as the management mode. You can setup one of the FI's in the IMM mode and then join the second to the cluster. Subsequently, claim the IMM domain to Cisco Intersight. In IMM, all configurations and operations for the UCS domain is driven from Cisco Intersight. With IMM, configure and deploy a UCS Domain Profile to program the FIs for FI-A and FI-B with unified ports (Ethernet and FC) and port roles (uplink and server). The new UCS Domain Profile ensures a quick on-board of a new UCS domain in Cisco Intersight.

Note Cisco UCS Infrastructure and Server FW version 4.1(2) enables an opt-in to technical preview for IMM; a policy driven configuration platform for FIs and attached servers. When IMM is enabled, the entire UCS domain is reset to factory defaults and this will cause a disruption for workloads running on servers in the domain. While this feature is in technical preview, it is not recommended for production workloads or applications.

For more information, see https://intersight.com/help/resources#intersight_managed_mode.

Device Connector

Device connector connects Cisco UCS Manager to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Manager to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Connect Cisco UCS Manager with Cisco Intersight by configuring the device connector proxy settings, if they are required.
2. Use the device serial number and security code to validate your access to the device from Cisco Intersight and claim the device.

Enabling or Disabling Cisco Intersight Management

When you enable Cisco Intersight management, it establishes a bidirectional communication between the Intersight Cloud application and the device.

Before you begin

You must be an administrator to configure the device connector.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **Device Connector**.

The **Device Connector** tab displays the connection status and the set access mode. The device ID and claim code displayed in the **Device Connector** tab is used in Cisco Intersight to claim Cisco UCS Manager.

Step 3 Click **Settings**.

Step 4 In the **Settings** wizard, click **General**.

Step 5 Enable the **Device Connector** slider to enable Intersight management or disable the **Device Connector** slider to disable Intersight management.

By default, the Cisco Intersight Management state is **Enabled**.

Step 6 Select the **Access Mode** as **Read-only** or **Allow Control**.

You cannot configure the device through Cisco Intersight when the **Read-only** access mode is selected. Therefore, any configuration that comes to the device connector through the cloud is rejected with an error code.

You have full control to configure the device through Cisco Intersight when the **Allow Control** mode is selected.

Step 7 To disable the Intersight management, disable the **Device Connector** slider.

When you disable the Intersight management, the **Device Connector** page displays the connection status as **Administratively Disabled**.

Step 8 Click **Save**.

Viewing Intersight Device Connector Properties

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **Device Connector**.

The **Device Connector** tab displays the connection status and the set access mode. The device ID and claim code displayed in the **Device Connector** tab is used in Cisco Intersight to claim Cisco UCS Manager.

Step 3 Click **Settings**.

Step 4 In the **Settings** wizard, review the following information:

Name	Description
General tab	The state of the connection between Cisco UCS Manager and Cisco Intersight. **Device Connector** slider— Allows you to enable or disable the Cisco Intersight management. You can do one of the following: • Turn on **Device Connector** slider—To enable Cisco Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. This is the default connection status. • Turn off **Device Connector** slider—To disable Cisco Intersight management. No communication will be allowed with Cisco Intersight. **Access Mode**—Configure access as **Read-only** or **Allow Control**. • **Read-only**—When the **Read-only** access mode is selected, you cannot configure the device through Intersight. • **Allow Control**—When the**Allow Control** access mode is selected, you have full control to configure the device through Intersight.
DNS Configuration tab	Configure the DNS Settings • **Domain name** field—Add a domain name. • **DNS Server** field—Configure at least one DNS server to enable DNS name resolution. The Intersight Device Connector must be able to successfully resolve DNS records. **Note** When the DNS settings is managed by a global policy in Cisco UCS Central, the DNS settings will be grayed. In such cases, update the DNS settings from Cisco UCS Central.

Name	Description
NTP Configuration tab	Configure the NTP Settings. Cisco strongly recommends configuring at least one NTP Server for time synchronization. If the system clock time is not synchronized with the Internet time, the Intersight device connector may be able to communicate with the Intersight service, as long as the time offset is not too large. If the time offset is outside the validity period of the Intersight X.509 Certificate, the device connector will not be able to communicate with the Intersight service. • **NTP Server** field—Configure at least one NTP server. **Note** When the NTP settings is managed by a global policy in Cisco UCS Central, the NTP settings will be grayed. In such cases, update the NTP settings from Cisco UCS Central.
Proxy Configuration tab	Whether HTTPS proxy settings are disabled or manually configured. This can be one of the following: • Turn off **Enable Proxy**—To disable the HTTPS proxy settings configuration. • Turn on**Enable Proxy**—To enable the HTTPS proxy settings configuration. • **Proxy Hostname/IP**—Enter the proxy hostname or IP address. • **Proxy Port**— Enter the proxy port number. • **Authentication**—Enable this option to authenticate access to the proxy server. Enter the **Username** and **Password** to authenticate access. **Note** The device connector does not mandate the format of the login credentials, they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.

Name	Description
Certificate Manager tab	Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Import**—Allows you to select and import a CA signed certificate. **Important** The imported certificate must be in the *.pem (base64 encoded) format. • You can view the list of certificates with the following information: • **Name**—Common name of the CA certificate • **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server • **Issued By**—The issuing authority for the certificate • **Expires**—The expiry date of the certificate **Note** You cannot delete bundled certificates.

Step 5 Click **Close**.

Updating Device Connector

When you upgrade Cisco UCS Manager, the device connector is automatically updated to the image integrated with the Cisco UCS Manager version. The device connector does not get downgraded when you downgrade the Cisco UCS Manager version.

You can update the device connector through the Cisco Intersight GUI. You can also update the device connector through the local management shell in Cisco UCS Manager CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **copy** [*from-filesystem*:] [*from-path*] *filename to-path* [*dest-filename*]	Copies the device connector image file from a remote server to a local destination by using the specified file transfer protocol. You need to copy the file to one fabric interconnect only. • *from-filesystem*—The remote file system containing the file to be copied. This file system can be specified by using one of the following options: • **ftp:** [// [*username@*] *server*]

	Command or Action	Purpose
		• **scp:** [// [*username@*] *server*] • **sftp:** [// [*username@*] *server*] • **tftp:** [//*server* [:*port*]] If the file system is not specified, the current working file system is assumed. If a remote protocol is specified with no server name, you are prompted to enter the server name. • *from-path*—Absolute or relative path to the file to be copied. If no path is specified, the current working directory is assumed. • *filename*—The name of the source file to be copied. • *to-path*—Absolute or relative path to the copied file. If no path is specified, the current working directory is assumed. The path includes the local file system to contain the copied file. This file system can be specified from one of the following options: • **volatile:** • **workspace:** • *dest-filename*—The new name for the copied file. If a dest-filename is specified, the copied file is renamed at the destination location. **Note** You cannot download the device connector image file through Cisco UCS Manager GUI.
Step 3	UCS-A(local-mgmt)# **update-device-connector workspace:** | **volatile:**/*filename* [**skip-upgrade-on-peer**]	Updates the device connector image on the peer fabric interconnect and then the local fabric interconnect. Using the **skip-upgrade-on-peer** option skips update on the peer fabric interconnect.

Example

The following example updates the device connector on both fabric interconnects:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on peer Fabric interconnect
Successfully updated device connector on peer Fabric interconnect
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

The following example updates the device connector on the local fabric interconnect only:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin skip-upgrade-on-peer
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```