Cisco UCS Director Release Notes for Cisco IMC Connector Pack, Release 6.6.x.x

First Published: 2018-09-06

Cisco UCS Director Release Notes for Cisco IMC Connector Pack Release 6.6.x.x

Cisco UCS Director

Cisco UCS Director delivers unified, highly secure management for supported compute, network, storage, and virtualization platforms and for the industry's leading converged infrastructure solutions, which are based on the Cisco Unified Computing System (Cisco UCS) and Cisco Nexus platforms. Cisco UCS Director extends the unification of computing and network layers through Cisco UCS to provide data center administrators with comprehensive visibility and management capabilities for compute, network, storage, and virtualization. For more information, see Cisco UCS Director on Cisco.com.

Revision History

Release	Date	Description
6.6.0.1	September 6, 2018	Created for Release 6.6.0.1.

Connector Packs

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors and without having to upgrade the entire software version. After claiming Cisco UCS Director in Cisco Intersight, as a system administrator, you can view information on new versions of connector packs that are available for upgrade. The top header pane of the user interface displays a Download icon indicating that new connector pack versions are available. You can select and upgrade the connector packs in Cisco UCS Director.

Cisco IMC Connector Pack

The Cisco IMC connector pack enables you to orchestrate and automate some of the steps required to configure and maintain rack servers (Cisco UCS C-Series Rack-Mount Servers, Cisco UCS S-Series and Cisco UCS E-Series servers). You must add these rack servers as a Rack account to Cisco UCS Director, after which Cisco UCS Director provides you with complete visibility into the rack server configuration. In addition, you can use Cisco UCS Director to manage and configure the rack-mount server.

Upgrading Connector Packs

Before you begin

- You must have system administrator privileges in Cisco UCS Director and Cisco Intersight.
- Cisco UCS Director has been claimed in Cisco Intersight. For information on claiming a device, see the integrated guided walkthrough titled *Learn How to Claim a Device* available within the **Online Help** menu in the Cisco Intersight user interface.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- Take a snapshot of Cisco UCS Director before you initiate the upgrade.

Procedure

Step 1 On the header, click **Available Connector Packs for Upgrade**.

The **Available Connector Packs for Upgrade** screen appears that displays a list of available connector packs for upgrade along with the version information. Clicking **Yes** in the pop-up message that appeared immediately after you logged in to the user interface will display this screen.

Note The **Available Connector Packs for Upgrade** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the check box of a connector pack from the list.

You can check the check boxes of multiple connector packs.

Step 3 Click **Upgrade**.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes**.

After you confirm that the connector version must be upgraded, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **Connector Pack Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled. Proceed to step 5.

Following are some of the possible outcomes of the validation and upgrade process:

- If the validation process fails due to issues in the connector pack, the **Connector Pack Validation** screen is displayed with error details and corrective measures.

  Review the information and click **Close**.

- If the connector pack upgrade process fails, click **Logout**.

  Note If any of the connector pack upgrade fails, the connector pack is rolled back to the earlier version.

- The validation process fails if other users have logged in to the system or if workflows are in progress. An upgrade failure error message with appropriate corrective action is displayed.

  Review the corrective action, and click **Force Upgrade** to proceed with the connector pack upgrade.

The **Connector Pack Upgrade Status** screen is displayed with current status for the connector pack upgrade request. The other users are automatically logged out of the system with a system broadcast message about the upgrade and are redirected to the login page.

Note When a connector pack upgrade is in progress, and if another user with system administrator privileges logs in to the system, the **Connector Pack Upgrade Status** screen is displayed with the status of the upgrade process. When a connector pack upgrade is in progress, and if an end user logs in to the system, the system startup page is displayed.

Step 5 Click **Logout**.
You can login to Cisco UCS Director after the upgrade process is complete.

What to do next

You can view the upgrade reports by choosing **Administration** > **System** > **Connector Pack Upgrades**. From this screen, you can double-click on a report, and view additional details on the upgrade process. For more information, see Viewing Connector Pack Upgrade Information.

Viewing Connector Pack Upgrade Information

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Connector Pack Upgrades**.
Information such as upgrade request ID, user that initiated the upgrade, upgrade start time and end time, and the upgrade status are displayed.

Step 3 Select a connector pack and choose **View Details** to view details such as connector pack name, upgraded version, and prior version.

Step 4 Click **State History** to view the various states of the connector pack upgrade process. For example, upgrade request received, upgrade process initiated or upgrade process completed.

Step 5 Click **Stages** to view the entire lifecycle of the connector pack upgrade request.

New and Changed Features in Release 6.6.0.1

Enhancements to Host Image Mapping on E-series Servers

Host Image Mapping allows you to download a firmware file to Cisco UCS Director, and upgrade the firmware on E-series servers. Using Cisco UCS Director, you can create a host image mapping profile to download and upgrade either one of the following:

- ISO firmware image
- CIMC image or
- BIOS image

Using Cisco UCS Director, you can download the firmware image on Cisco IMC in one of the following methods:

- Provide a location on the network (an FTP, FTPS, HTTP or HTTPS server) where the firmware file is currently available.
- Choose the firmware file from a location on your system.
- Download the firmware image from www.cisco.com.

Important To perform these tasks, Cisco IMC version 3.2.4 must be installed on the E-series servers. This feature does not work with prior versions of Cisco IMC.

Host image mapping profiles created in prior versions of Cisco UCS Director will no longer work after you upgrade to the Cisco IMC Connector Pack release 6.6.0.1. You must delete these profiles and create it again after upgrading to this connector pack version.

For more information, see the knowledge base article titled Host Image Mapping with Cisco UCS Director IMC Connector Pack, Release 6.6.0.1.

Introduction of Power Restore Policy for E-series Servers

This release introduces a Power Restore policy that allows you to change the value set for the power restore policy on an E-series server without logging into the Cisco IMC of that server.

Support for Configuring Graceful Timeout on UCS C-series Servers

This release introduces support for configuring a timeout for host systems to shut down before a firmware upgrade process is initiated.

While uploading a firmware image from a local server, or while uploading a firmware image from a network server, you can now specify a timeout period, in minutes, within which the host system must gracefully shut down. You can also enable the host system to forcibly shutdown before the firmware upgrade process is initiated. The new fields introduced to enable configuring graceful timeout and force shut down are available on the **Add Firmware Image - Local** screen and **Add Firmware Image - Network** screen.

Note You can configure graceful timeout for systems running Cisco IMC version 3.1(3a) or higher.

Support for Cisco UCS VIC 1425 Series Adapter

This release introduces support for Cisco UCS VIC 1425 adapter.

Introduction of new REST APIs

This release introduces REST APIs for the following features:

- Host Image Mapping
  - CREATE_HOST_IMAGE_PROFILE
  - APPLY_HOST_IMAGE_PROFILE

- CCO_IMAGE_CREATE
- DELETE_HOST_IMAGE_PROFILE
- CCO_IMAGE_DOWNLOAD
- CCO_IMAGE_FIND
- DELETE_HOST_IMAGE_PROFILE

- Policy and Profile Related APIs
  - Deriving a Hardware Profile
  - Reading Hardware Policy Apply Status
  - Reading Hardware Profile Apply Status
  - Reading Power Restore Policy

- Graceful Timeout
  - Creating a Firmware Local Image
  - Creating a Firmware Network Image

Open Defects in Release 6.6.0.1

Following are the defects that are open in this release:

Defect ID	Description
CSCve35368	Cannot apply BIOS policy to ENCS/e-series servers
CSCvk55765	ULTRA M C series servers support by IMC Supervisor
CSCvj64814	CCO download for firmware versions 3.1(3a) and 3.1(3b) are failing in IMCS.
CSCvk50197	Failing validation when trying to perform FW update via IMC supervisor

Resolved Defects in Release 6.6.0.1

Following are the resolved defects in Release 6.6.0.1:

Defect ID	Description
CSCvj22809	CSV import does not escape out commas in fields enclosed with double quotes

Defect ID	Description
CSCvh22704	UCSD 6.6.0.0: NPE is displayed for Server health if no server is added under IMCS
CSCvh54491	UCSD 6.6.0.0: Firmware Management and Server diagnostics showing errors When tried with local option.
CSCvh61151	Valid file path example should be placed in Add Host Image mapping profile
CSCvd89755	Incorrect message is returned from CIMC when user deletes already added invalid image
CSCvj47971	IPV6 getting enabled even with v6extEnabled="no" in network config policy.
CSCvh12408	Tech Support operation is already in progress is showing when there is no operation in progress.
CSCvh59274	Host Image Upgrade status message should be appropriate
CSCvj60483	Available images from CCO are not displaying for EHWIC
CSCvh68103	In IMCS 2.2.0.+ the firmware graph does not display the version information as a label.
CSCvj52330	Firmware selection for S3260 needs further verification step
CSCvh89470	AD accounts used to connect IMCS to E-Series CIMC servers getting locked out
CSCvj60319	Power restore policy option text should be same as in CIMC
CSCvi88977	Upgrade status is empty when xml parsing error occurs
CSCvj82892	Creating multiple VDs with same DG policy when PDs in JBOD state results in error
CSCvh61216	HIU: Warning message to be updated in Run upgrade
CSCvi74807	IMCS 2.2.0.2 unable to apply Write policy "Write Back Good BBU" to S3260.
CSCvh19265	Error message is displayed when importing the server using csv file.
CSCvh61157	Map and delete image option to be placed in Upload HIM

Defect ID	Description
CSCvh59727	Apply profile should allow user to select respective servers alone
CSCvh13025	Cisco IMC Web Administrative Console cleartext passwords returned in server response
CSCvh13018	Cisco IMC Supervisor and UCS Director Third Party Library Upgrades
CSCvh57708	UCSE: Host image upgrade status show empty
CSCve93104	Issues while applying VIC policy with default iSCSI and usNIC properties
CSCvh57428	UCS-E - Multiple issues observed after HIM implementation in IMCS
CSCvj31145	When a local user password is about to expire, user getting blank email warnings
CSCvj31625	Add Advanced Filter and click on column heading to sort, lose filter
CSCvh13038	Cisco UCS Director and Cisco IMC Supervisor restrict unnecessary ports.
CSCvh59257	IMCS HIM profile - Need to add option to unmap current image
CSCvh56478	IMCS Web UI - Clear text passwords returned in server response for Credential Policies
CSCvh13048	Cisco IMC Web Administrative Console server information disclosure

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.