Cisco UCS Director Release Notes for Cisco IMC Connector Pack, Release 6.7

First Published: 2019-11-12

Last Modified: 2020-06-18

Cisco UCS Director Release Notes for Cisco IMC Connector Pack

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
6.7.3.1	November 12, 2019	Created release notes for release 6.7.3.1.
6.7.4.1	June 18, 2020	Created release notes for release 6.7.4.1

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.
- 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 **New Upgrades Available**.

The **Available System Upgrades** screen appears and will display all available connector packs for upgrade along with version information. Upon login, if you clicked **Yes** to the pop-up message, then the very same upgrade screen appears.

Note The **New Upgrades Available** 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 **System Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled.

Step 5 Click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking **Logout**, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director .

What to do next

You can view the upgrade reports by choosing **Administration** > **System** > **System Updates**. 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 **System Updates**.
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 6.7.3.1

Enabling Faster Download of Firmware Images

Starting with this connector pack release, you can enable faster download of firmware images if you configure a proxy server in Cisco UCS Director. To configure a proxy server, choose **Administration** > **System** > **Proxy Configuration**.

Enhancements to Zoning Policy

Starting with this connector pack release, you can use the zoning policy to assign physical drives to a specific controller slot on servers that support dual controllers such as Cisco UCS S3260 Dual Raid Controller (UCS-S3260-DRAID). However, choosing a specific controller slot is not mandatory. If you do not choose a specific controller slot, then the ownership of the physical drives is assigned to the first controller slot that is available on the server that you selected.

Enhancements to RAID Policy

Following are the enhancements introduced in this connector pack release to for confguring a RAID policy:

- **Deriving the Policy**
  - **Drive Security**

    Drive security for the RAID policy is retrieved only if the security properties, such as the security Key ID, are common for all controller slots associated with the server. If the security Key ID is not common across all controller slots in the server, deriving the policy will fail.
  - **Virtual Drive Configuration**
    - While creating a RAID policy based on an existing server configuration, virtual drives from all controller slots in the server are retrieved and listed in the **Virtual Drives Configuration** screen of the RAID policy. In addition, all related disk group policies are also created.

- **Applying the policy**

  While applying the policy, the Drive Security configuration is applied commonly to all controllers that are associated with the server.

  Applying the policy to virtual drives is determined by the disk group policy associated with the virtual drives. If a disk group includes slots from multiple controllers in the server, then the **Apply Policy** action fails. But a single RAID policy can include virtual drives with disk groups that belong to different controllers.

  The **Enable JBOD/UnConfigured Good** configuration is applied to unused disks that belong to all the controllers associated with the server.

Visual Representation of Device Claim Status

Starting with this connector pack release, the **Rack Server Summary** screen displays the claim status of the rack server in Cisco Intersight. A new field label titled **Intersight Claim Status** is displayed with one of the following values:

- **Yes**—when the rack server is claimed in Cisco Intersight.
- **No**—when the rack server is not claimed in Cisco Intersight.
- **Not Applicable**—when the firmware version running on the rack server is prior to version 4.0(2a) or if the server is Cisco UCS S3260.

In addition, the response output for the **GetConnector** API has been enhanced to display the claim status of the rack server, and the serial number of the claimed rack server. For Cisco UCS S3260 servers, the **Serial Number** attribute in the response output displays the chassis serial number. For all other servers, the server serial number is displayed as the value for the **Serial Number** attribute.

New and Changed Features in Release 6.7.4.1

Introduction of SFTP User Configuration

Starting with this release, you will need to configure a password for an SFTP user in Cisco UCS Director. This user configuration is used in server diagnostics and tech support processes to transfer files to Cisco UCS Director using SFTP. This SFTP user configuration replaces the previously available SCP user configuration functionality. After installing or upgrading to this release, you must configure the password for the SFTP user. To do so, choose **Administration** > **Users and Groups** > **SFTP User Configuration** and enter a password.

If you upgrade to version 6.7.4.1 of the Cisco UCS Director Base Platform Connector Pack, then you must also upgrade to version 6.7.4.1 of the Cisco UCS Director IMC Connector Pack to use the Server Diagnostics and Tech Support features with the SFTP user configuration.

Changes to Launching KVM Console for a Rack Server

Starting with this release, the process to launch the KVM console for a rack server is different based on the Cisco IMC version running on the server. If the Cisco IMC version installed on the server is prior to version 4.1(1.c), then clicking **Submit** in the **Launch KVM Console** screen will download a kvm.jnlp file. Double-click this file to launch the KVM Console. If the Cisco IMC version installed on the server is version 4.1(1.c) and above, then clicking **Submit** in the **Launch KVM Console** screen will display a new tab with a link. Click this link to enter the KVM console credentials and login.

Enhancements to VIC Adapter Policy

Starting with this release, for a VIC adapter policy, you can configure the Admin Forward Error Correction (FEC) mode for the following adapters:

- Cisco VIC 1455
- Cisco VIC 1457
- Cisco VIC 1495
- Cisco VIC 1497

By default, four ports are configured for these adapters and you cannot delete them. However, the number of ports configured with the Admin FEC mode varies depending on the adapter you have selected. For example, for a Cisco VIC 1497 adapter, there are only two ports. So, the Admin FEC mode is configured only on the first two ports (port 0 and port1), ignoring the remaining ports (port 2 and port 3). For the existing policies, this field is set to **Auto**. But you can change this value to **cl91**, **cl74**, and **Off**.

Note The **cl74** option is not supported for Cisco VIC 1495 and Cisco VIC 1497 adapters.

In addition to the default vNICs and vHBAs configured on these adapters, you can create additional vNICs and vHBAs based on the selected port channel state.

Note When you modify the port channel configuration for an adapter, all previously configured vNICs and vHBAs are deleted and the configuration is restored to the factory default settings.

Open Defects in Release 6.7.3.1

Following are the open defects in this release.

Bug ID	Headline
CSCvr69031	VIC Policy Issue when the policy is created from a template.

Open Defects in Release 6.7.4.1

Following are the open defects for this release.

Bug ID	Description
CSCvu46039	Tech Support and Server Diagnostics require IMC connector 6.7.4.1 upgrade after the Base Platform connector pack upgrade to version 6.7.4.1.
CSCvu65224	IMC Connector firmware upgrade issues

Resolved Defects in Release 6.7.3.1

Following are the resolved defects for this release.

Bug ID	Headline
CSCvr49351	Configure Rack Server task fails when Precision Boot Order Policy is selected as policy type
CSCvq79458	Unable to unassign a POD after Rack Group is renamed
CSCvp86377	HTTP Proxy settings in the user interface does not work.
CSCvq68812	Values for BIOS Policy set to 'platform-default' after creation
CSCvo83023	CIMC: Upgrading firmware on multiple UCS Rack Servers: Failed with Error

Resolved Defects in Release 6.7.4.1

Following are the defects resolved in this release:

Bug ID	Headline
CSCvt18846	Error occurred while launching KVM console

Communications, Services, 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.

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.