Cisco UCS Director Release Notes for Cisco Base Platform Connector Pack, Release 6.7.x.x

First Published: 2019-11-12

Last Modified: 2020-11-13

Cisco UCS Director Release Notes for Cisco Base Platform 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 for Release 6.7.3.1 for the Base Platform connector pack and System Update Manager connector pack releases.
6.7.3.2	January 9, 2020	Updated the release notes for release 6.7.3.2 of the Base Platform connector pack. See New and Changed Features in Release 6.7.3.2, on page 8.
6.7.4.1	June 18, 2020	Updated the release notes for release 6.7.4.1 of the Base Platform connector pack. This version is no longer available. All features released as part of 6.7.4.1 are available in 6.7.4.2.

Release	Date	Description
6.7.4.2	July 2, 2020	Updated the release notes for version 6.7.4.2 . See New and Changed Features in Release 6.7.4.2, on page 9
6.7.4.3	November 13, 2020	Updated the release notes for release 6.7.4.3 of the Base Platform connector pack. See #unique_6.

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.

Base Platform And System Update Manager Connector Packs

The base platform connector pack includes basic infrastructure components such as platform service enhancements, user interface changes, Shell Admin console changes and updated online help system. The System Update Manager includes the framework that helps you upgrade all connector packs and the base platform pack.

In an optimized multi-node setup, prior to installing or upgrading the base platform pack, you must configure passwordless authentication between the primary node and the database node. For more information, see Setting Up Passwordless Authentication, on page 2.

Setting Up Passwordless Authentication

In an optimized multi-node setup, prior to installing or upgrading the base platform pack to version 6.7.3.1 and later or to Cisco UCS Director 6.7(4.0) and later, you must first configure passwordless authentication between the primary node and the database node. You need to configure this form of authentication only once and need not repeat it before upgrading to later versions.

Procedure

Step 1 Login to the primary node.

Step 2 Run the following command on the primary node: **cd /opt/scalability**.

Step 3 Run the **./multiNodeConfig.sh script** command to start the passwordless authentication setup.

Step 4 When prompted, enter **2** to access the database node.

Step 5 When prompted, enter the database node IP address.

Step 6 When prompted, enter **root** as the username for the database node.

Step 7 When prompted, enter **y** to generate the key.

Step 8 At the confirmation prompt, enter **yes**.

Step 9 If you are installing a new version of Cisco UCS Director using the OVA, and if the default **root** user password of the database node is not reset already, you are prompted to change the password.

Step 10 When prompted, enter the password for the **root** user of the database node.

A confirmation message stating that passwordless authentication for the **root** user on the database node is displayed.

Step 11 Run the **chmod 600 ~/.ssh/id_rsa** command.
This completes the passwordless authentication setup.

Step 12 (Optional) Run the **sudo ssh <<username>>@<<db nodeIp>>** command to verify the completion of the setup.

If you are logged in to the database node after running this command, then passwordless authentication is successfully configured.

Step 13 (Optional) If you cannot login to the database node without a password, login to the primary node and delete the entry of the database node from the `~/.ssh/id_rsa/known_hosts` file and repeat this procedure.

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

Support for Upgrading the Bare Metal Agent (BMA) using a Connector Pack

The Base Platform connector pack and System Update Manager release 6.7.3.1 introduces support for upgrading the Bare Metal Agent (BMA) with a connector pack. You must install both, the Base Platform pack version 6.7.3.1 and System Update Manager version 6.7.3.1 to upgrade BMA with a connector pack.

After installing the System Update Manager connector pack, the **System Updates** screen is refreshed and it displays the status of the recent updates that were performed on the system. A new screen titled **BMA System Updates**, accessible from **Administration** > **System** menu, has been introduced. This screen displays the status of the recent updates made to the BMA. Also, a new system task called **BMA Update System Task** has been introduced. This system task is disabled by default. This system task is enabled only after you install the BMA connector pack, and it is set to run every 4 hours.

Support for Syncronizing Users from Cisco Identity Services Engine (Cisco ISE)

Starting with this connector pack release, you can sychronize and retrieve user accounts created in Cisco Identity Services Engine (Cisco ISE) by integrating a Cisco ISE server with Cisco UCS Director.

Note You can integrate a Cisco ISE server that is running release version 2.6.0.156 or later.

Following are the prerequisites to configuring a Cisco ISE server in Cisco UCS Director:

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE is required to configure the server in Cisco UCS Director.

- Specify an authentication protocol in Cisco ISE.

  It can either be Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director when you add the Cisco ISE server.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

Introduction of Email Notification for Rollback Service Requests

Starting with this connector pack release, when you initiate a rollback of a service request, an email notification is sent to the users configured as recipients in the email notification policy for the initial service request. In earlier releases, email notifications were sent to users configured in the email notification policy only for the initial service request.

Introduction of Additional Options for Rollback on Failure of Service Requests

Starting with this connector pack release, while creating a workflow, you can configure rollback options for the workflow. The user interface includes the following new options:

- **Rollback Workflow on Failure**
- **Abort Rollback on Failure** (displayed only if you check the **Rollback Workflow on Failure**)

Selecting the **Rollback Workflow on Failure** option ensures that the service request is automatically rolled back when the service request fails. In this scenario, a rollback service request is initiated. Selecting the **Abort Rollback on Failure** check box terminates the rollback of a service request if the execution of any task within the rollback service request fails.

Support for Auto-populating User Input Details for Workflows

Starting with this connector pack release, while mapping a user input for a workflow task, the **Input Label** field and the **Input Description** field are automatically populated, based on the input type. You can edit these values as well. However, you cannot create multiple user input names with the same value.

Introduction of a new API to Halt a Rollback SR on Task Failure

This connector pack introduces a new API **userAPIRollbackServiceRequest**. You can use this API to rollback a service request and set it to continue with the rollback in the event of a failure of a task execution. To use this API, you must provide the service request ID as a value for the API. If any task in the rollback service request fails, by default, the service request skips the task and continues to execute. If you set the value of the API to false, then if any task fails, the rollback service request halts.

Support for New Actions in Tabular Reports for Orchestration Workflows

Starting with this connector pack release, while working with tabular forms with orchestration workflows, you can now choose multiple entries and perform actions such as deleting entries, or reordering entries within the table.

Workflow Optimization

Starting with this connector pack release, the switching time between tasks is optimized such that the entire workflow completes faster.

Introduction of Quick Export for Workflows

This connector pack release introduces a new option called **Quick Export** on the **Workflows** page, using which you can select workflows and export them to your machine. After you select workflows and choose **Quick Export**, the subsequent screen lists the following information for the selected workflows:

- Script modules
- Workflow
- Custom tasks
- Activities
- Open APIs

You must provide a file name and choose **Export Workflow**.

Note The **Quick Export** option is also available from the right-click menu.

Support for Processing Header Response

Generic API task allows you to fetch specific values from the output of header response when the value of **Header Response** is set as **True** in the **Output Definition** table of a Generic API task. If the value of **Header Response** is set as **False** in the **Output Definition** table, you can fetch the output response values using JSON or XML.

For more information on processing header response, refer Working with Generic API Task of Cisco UCS Director.

Support for Generating a Task Using an OpenAPI Specification File

The OpenAPI specification file from connectors such as NetApp, VMware, defines all APIs of connectors in the JSON or YAML format. Starting with this connector pack release, Cisco UCS Director has the provision

to upload the OpenAPI specification file to Cisco UCS Director and make use of the connector specific API for creating a task. You can use the task created based on a OpenAPI specification file, in Cisco UCS Director workflow to perform a specific operation on the connector account.

You can also reset an API to their original form by clicking **Reset** after choosing the API that needs to be reset. Before initiating the reset process, ensure that the task created based on the API are deleted and workflows that use the API task are deleted from Workflow designer.

For more information on generating a task using an OpenAPI specification file, refer Cisco UCS Director Orchestration Guide.

Changes to Cisco UCS Director SDK Bundle

Starting with this connector pack release, the Cisco UCS Director SDK bundle uses the `http-client-4.4.jar` files. The SDK bundles of prior releases of Cisco UCS Director used the `commons-httpclient-3.1.jar` files. As a result of this change, if your customized programs use classes from the `commons-httpclient-3.1.jar`, you must update your code to use the new http-client classes.

Introduction of New Generic Tasks

Generic tasks allow you to automate certain operations on input parameter and deliver the processed output to next task. In the **Workflow Designer**, you can find the generic tasks under the **Cloupia Tasks** > **General Tasks** folder.

This release introduces the following generic tasks:

- **Process Text**

  You can add the **Process Text** task to any workflow to manipulate the defined inputs as per the operations and deliver the manipulated text as an output to next task. In the **Process Text** task, you must define the following parameters:

  1. Input List—You can add a list of input names as task inputs that can be mapped with values on which the operation must be performed.
  2. Operations—You can provide a name for the operation, and then choose an operation type and input parameter on which the operation has to be performed.
  3. Output List—You can define an output name and associate the output name with one of the operation outputs displayed based on defined operation names. These outputs can be mapped as inputs for other task.
  4. Check this option for script mode—You can enable this check box to enter the script for manipulating the text.

  For more information on the **Process Text** task, refer the Generic Tasks of Cisco UCS Director Base Platform Connector Pack.

- **Convert Type**

  You can use the **Convert Type** task to convert the given input value to any desired output type as required for a task. For example, you can convert the generic text into an email ID format and input the email ID as input for another task.

  You can define multiple input labels and an output type for each input label. So that, the **Convert Type** task converts each input value into defined output type.

- **Register LOV**

  The **Register LOV** task registers given key value pairs as an LOV in the workflow task input, which can be used by other tasks or workflows after registration. During LOV registration, you can define LOV name and LOV pairs in the JSON format as text or upload as a file:

  ```
  {"LOVName1" : {"LOVLabel":"LOVValue","LOVLabel":"LOVValue","LOVLabel":"LOVValue"},
  "LOVName2": {"LOVLabel":"LOVValue","LOVLabel":"LOVValue","LOVLabel":"LOVValue"}}
  ```

  You can also define the type of variables that you want to regsiter. You have the provision to enable overriding of LOV pairs when there is an LOV with the same name.

- **Get Data From Tabular Report**

  You can use the **Get Data From Tabular Report** task to retrieve specific data from a tabular report. To retrieve a report data, you have to provide report name, choose columns that you need in the output, and specify filter criteria to filter the data in the report.

- **Process Time**

  You can use the **Process Time** task to perform action such as converting time format, get system time and so on. To process time, define the input in a specific time format or define normal time value without following any format. Then, choose one or more operations such as **Convert Time Format**, to be performed on input time, and define the output format in which the processed time has to be output for each operation.

  The supported operations are: **Convert Time Format**, **Get System Time**, **Get Time Difference**, **Get Time Component**, **Get Prior or After Time**, and **Get Time from NTP server**.

  For the **Get Prior or After Time** operation type, you have to input two values: Date in any format and a generic number. Based on set prior or after action and time component, the output will be processed. For example, if you have set input as **16/07/2019** and **2**, chosen **Before** and **Date** in the **Select Prior or After** and **Select Time Component** drop-down lists, then the processed time output is **14**.

  For **Get Time from NTP server** operation type, you have to provide the IP address of the NTP server or DNS name.

- **Read File**

  Starting this connector pack release, you can use the **Read File** task to read the content of a specific file and generate an output with either the entire content of the file or the content in a specific line.

  You can also provide a regular expression pattern to read the lines matching the given pattern.

New and Changed Features in Release 6.7.3.2

Infrastructure Changes to Upgrade to Subsequent Patches

This release of the Base Platform connector pack includes infrastructure changes to support upgrades to subsequent Cisco UCS Director patches.

New and Changed Features in Release 6.7.4.2

Changes to Workflow Tasks and Validation

This connector pack release introduces the following changes to workflow tasks and validation:

- The stale data of the compound workflows will be removed during the upgrade. The execution of service requests will be started or resumed only after completion of this removal process. The time taken to complete this process depends on the number of compound workflows in the system.
- Nested macros are resolved only up to 25 levels.
- Workflow validation has been enhanced to determine if loop tasks, such as startloop and endloop, are accurately aligned in the workflow. If these loop tasks are not aligned accurately, both the workflow validation and workflow execution will fail.
- Due to security updates, workflow validation fails for tasks with Generic Text input mapping for Password input type. If workflows are invalid, then, you must manually edit these workflows and resolve the issues.

Note Although workflow validation fails for workflows with loop tasks or task with Generic text input mapping for Password input, you can continue to execute them.

Support for Bulk Archival of Service Requests

Starting with this release, you can archive a large number of service requests at a time using the bulk archival option. You can archive service requests based on the Range, Date, or Status.

To archive multiple service requests simultaneously, on the **Service Request** page, click the **Bulk Archive** option. On the **Bulk Archive** page, select the required option from the **Bulk Archive** drop-down list. Based on the option selection, the input field is displayed. The options include:

- Range: Specify the service request IDs separated by a comma, in one of the following formats:
  - Individual SR IDs: For example, 8, 9, 15, 77
  - Range of SR IDs: For example, 44-68, 108-332
  - Combination of a range and individual SR IDs: For example, 23-44, 55-90, 66, 8
- Date: All the services requests triggered before the selected date are archived.
- Status: Service requests are archived based on the status selected. You can select any of the following status:
  - Completed Service Requests
  - Failed Service Requests
  - Canceled Service Requests

A message screen, that shows the total number of service requests to be archived, appears.

Click **Archive**. A confirmation message that the service requests are archived successfully appears on top of the screen.

After service requests are archived, they are no longer displayed on the **Service Requests** page. You can view these archived service requests on the **Archived Service Request** page. You can use the **Unarchive** option on the **Archive Service Request** page if you want to reinstate a service request. You can also perform actions such as Purge Request, View Details, Delete Request and Report Metadata for a service request in the **Archived Service Request** page.

Enforcing of More Stringent Role-Based Access for REST APIs

Starting with this release, service end users and group administrator users can only use REST APIs for actions that they can perform in the user interface. These users cannot use REST APIs for actions that they cannot perform in the user interface. REST APIs for read operations for these actions continue to remain restricted for these users.

Introduction of Database Disk Usage Alerts

Starting with this release, administrator users receive alerts on database disk usage in the **Diagnostic System Messages** screen. You can view the database disk usage details such as disk capacity, used space, and free space in the **System Disk** pane on the **System Information** page.

Notification is sent to administrator users when usage exceeds the configured threshold. For example, administrator users get the following type of alert messages, if the database disk has been used greater than:

- 70 percent: message shows ‘notice’
- 80 percent: message shows ‘warning’.
- 90 percent: message shows ‘critical’.

For information on resolving database disk related issues, see the Cisco UCS Director Troubleshooting Guide

Enhancement to Get Data from Tabular Report Task

Starting with this release, the Get Data from Tabular Report task has been enhanced to retrieve data from the reports for a specific context by specifying a context value. To retrieve context-specific report data, you have to provide report name, context value, choose columns that you need in the output, and specify filter criteria to filter the data in the report.

Specifying the context value is mandatory for all reports, except for global reports. You can specify either a system-defined ID or a user-defined name specified for the resource in the **Context Value** field. You can determine the value for this field by choosing the Report Metadata option for the resource. You can enter value displayed for the ID in the **Context Value** field as input.

Enhancement to the OpenAPI Specification Integration

Starting with this release, OpenAPI Specification Integration has been enhanced with the following capabilities:

- Parser enhancements for faster OpenAPI Spec file processing
- Support for both JSON and YAML file formats
- Support for OpenAPI version 3.0
- Support for specifying an API key and a private authentication key of Cisco Intersight using a credential policy for Cisco Intersight API invocation in Cisco UCS Director.

You can use a credential policy to specify an API key and a private authentication key of Cisco Intersight for tasks imported through the OpenAPI specification files. These keys are mandatory for authentication with Cisco Intersight. You can create a credential policy using the **Credential Policy** tab or through a REST API call and associate this policy with a task when adding the task to the workflow.

To create a credential policy for setting up authentication with Cisco Intersight, select **HTTP API Signature Key** as the account type. Also, the API key and private key that you specify must be generated from Cisco Intersight. For information on generating these keys, see the *Cisco Intersight Help Center*. For more information on creating a credential policy in Cisco UCS Director, see Cisco UCS Director Administration Guide.

After creating this credential policy, you can associate it with an OpenAPI task. To do so, choose **Orchestration** > **OpenAPI Integration**. Expand the folder and choose any API task and select **Generate Task**. In the **Generate Task** screen, select **Use Credential Policy** check box to use the HTTP API Signature Key credential policy while running this task. When you use this task in a workflow, while specifying the task inputs, select the HTTP API Signature Key policy that you created.

Important

- The HTTP Signature has been implemented for authentication and authorization only for Cisco Intersight. Cisco Intersight implements the scheme RSA-SHA-256 of the RFC (see, https://tools.ietf.org/id/draft-richanna-http-message-signatures-00.html) and Cisco UCS Director implements the client algorithm of this scheme for authentication. Though the implementation is generic, currently, only Cisco Intersight is validated.
- You must configure the Network Time Protocol (NTP) for synchronization between Cisco UCS Director and Cisco Intersight. The system time for Cisco UCS Director and Cisco Intersight must be in sync for successful REST API authentication. You can enable proxy while creating the task if you observe connection timeout in the service request logs.
- You can associate the HTTP API Signature Key policy with any Cisco Intersight API task.

New and Changed Features in Release 6.7.4.3

Enhancement to the System Updates Report

Starting this release, the System Updates screen in Cisco UCS Director also displays the upgrade request and its status when a connector pack upgrade is triggered from Cisco Intersight.

Open Bugs in Release 6.7.3.1

The following table lists the open bugs for this release:

Bug ID	Headline
CSCvr66481	Workflow execution starts after 20 sec only when we resubmit the failed SR

Bug ID	Headline
CSCvr77976	Execute Generic API and OpenAPi Tasks Use Macros for rollback workflows password fields.

Open Bugs in Release 6.7.4.2

The following table lists the open bugs for this release:

Bug ID	Headline
CSCvu56678	Empty value is resolved as null when resolving the macro in task input.

Open Bugs in Release 6.7.4.3

There are no open bugs in this release.

Resolved Bugs in Release 6.7.3.1

The following table lists the resolved bugs in this release.

Bug ID	Headline
CSCvr35865	Upgrade vim-minimal library
CSCvq96746	Delivered messages count for deletion or termination are not reset when lease time of vm is extended

Resolved Bugs in Release 6.7.4.2

The following table lists the resolved bugs for this release:

Bug ID	Headline
CSCvt56483	In some situations, Powershell tasks are stuck and eventually times out with "Java heap space" error.
CSCvt56783	Service request takes input from another service request if they are running in parallel during the loop in workflow.
CSCvt83203	In parent workflow, the compound task password values are displayed in plain text.
CSCvu18137	Post upgrade: from 6.7.3.1 to 6.7.3.2: User login getting swapped during the workflow execution.

Bug ID	Headline
CSCvu23721	UCSD 6.7 : VM Action taking more time to load - bug for UI.
CSCvu21967	UCSD 6.7 : User report takes more time to load.
CSCvt61782	Slow page loading time when trying to re-run workflow from UCS Director.
CSCvu39393	UCS Director workflow User Group notification is blocking workflow.
CSCvt98179	In certain situations, the server selection screen will hang while applying a RAID policy.

Resolved Bugs in Release 6.7.4.3

The following table lists the resolved bugs for this release:

Bug ID	Headline
CSCvv72606	Intersight OpenAPI V3 is not working due to change in the basepath.
CSCvv03574	User interface is unavailable after upgrading to version 6.7.4.0 from 6.7.3.0.
CSCvu84152	Open API is importing the data check only for operation name due to which user unable to edit existing and imported API.
CSCvs11567	UCSD 6.7 - During approval phase, status workflow does not show user input details such as CPU, Memory requirements provided by requester during request phase.
CSCvu73362	Storage Tier Cost Models implementation fail.
CSCvv47766	Get WF service status API call in custom task returning null response.
CSCvv08780	When executing complex workflow with child and parent workflows including PowerShell scripts, in SR logs, credentials are echoed in clear text .
CSCvu56678	Empty value is resolved as null when resolving the macro in task input

Bug ID	Headline
CSCvu93814	During the SSL handshake process , the default "SSLSocketFactory" (from apache) is getting loaded at the JVM level overriding the "EasySSLProtocolSocketFactory" class and its configurations. This is causing the SSL certificate validation to happen and resulting in an SSL Certificate error.

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.