Cisco UCS Central Management Pack User Guide, Release 4.x For Microsoft System Center Operations Manager

First Published: 2016-05-03

Last Modified: 2021-09-02

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration

- Storage administration

- Network administration

- Network security

Conventions

This document uses the following conventions:

Conventions	Indication
bold font	Commands an keywords and user-entered text appear in bold font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.

Conventions	Indication
{ x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marts around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!,#	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take a note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem. The tips information might not be troubleshooting or even an action, buy could be useful information, similar to a Timesaver.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For more information, you can access the related documents from the following links:

- Cisco UCS Manager Management Pack User Guide, Release 4.x

- Cisco IMC Management Pack User Guide, Release 4.x

- Cisco UCS Central Management Pack User Guide, Release 4.x

- Cisco UCS Management Pack Suite Installation and Deployment Guide, Release 4.x

- Cisco UCS Documentation Roadmap

- Cisco UCS C-Series Documentation Roadmap

- Cisco UCS Central Configuration Guides

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL:https://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821 From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Overview

This chapter contains the following sections:

About the Cisco UCS Central Management Pack

A management pack is a definition file that contains predefined monitoring settings that enable an agent to monitor a specific service or application in Operations Manager. These predefined settings include discovery information that allows Operations Manager to automatically detect and begin monitoring services and applications. It also consists of a knowledge base that contains error and troubleshooting information, alerts, and reports to help you correct the problems detected in the environment.

The Cisco UCS Central Management Pack has rules to monitor global service profiles and organizations across multiple Cisco UCS Central. It provides visibility of health and alerts through familiar and easy-to-use interface.

System Requirements

The following system requirements are for Management Servers, Gateway Servers or Operations Manager Windows Agents (trusted or untrusted boundary) with Cisco UCS Monitoring Service running on them.

Verified versions of System Center Operations Manager are as follows:

- 2019 UR2
- 2019
- 1807
- 1801
- 2016
- 2012 R2
- 2012

Management and Gateway Servers

System requirement for Management Server and Gateway Server are as per the Microsoft recommendations mentioned, see https://docs.microsoft.com/en-us/system-center/scom/system-requirements

Operations Manager Windows Agents

The following are the System requirement for Windows agents, trusted or untrusted boundary running Cisco UCS Monitoring Service:

Hardware

- Processor Architecture—64-bit with Quad-core or higher

- Memory—8 GB or higher

- Free Disk Space — 50 MB or higher

- Network Connection — 1 MBps or faster

Operating System

Ensure that 64-bit version of the following operating systems are installed with the latest service packs:

- Windows Server 2019

- Windows Server 2016

- Windows Server 2012 R2

- Windows Server 2012

- Windows Server 2008 R2

Software

Install the following software components before installing the Cisco UCS monitoring service on management servers:

Cisco UCS MP Version	.NET Framework Version	Windows PowerShell Version
4.1.4 or higher	4.7.1 or higher	5.1 or higher
4.1.3 and earlier	4.6 or higher	3.0 or higher

Supported UCS Central Releases

Cisco UCS Central Management Pack for Microsoft System Center Operations Manager is compatible with the following Cisco Central Manager releases:

- Release 2.0

- Release 1.5

- Release 1.4

- Release 1.3

CHAPTER 3

Introduction

This chapter contains the following sections:

-

Key Features

The Cisco UCS Central Management Pack comprises the following key features. The subsequent chapters in this document elaborate these features further.

Rule(s) per UcsCentral Fault

This management pack implements one rule per Cisco UcsCentral domain fault. This provides improved power of customization at the fault level. You can override parameters, such as changing the priority and severity, enabling or disabling rules from the Operations Manager console interface. Apart from the console interface, all these customizations can also be applied using Operations Manager cmdlets. PowerShell scripts could be developed to operate on multiple rules at a time. The rules can be pre configured. You can either enable or disable these rules before adding any UcsCentral templates.

Modularized Management Pack Design

Added common modules and workflows in the Cisco UCS Core Library Management Pack to optimize the Cisco UCS Central Management Pack.

Additional Features

- Verified on System Center Operations Manager 2019 and 2019 UR2
- Support for System Center Operations Manager 1801 and 1807
- Support for System Center Operations Manager 2016
- Support for monitoring with IPv6 addresses
- Support for C3260/S3260 server

Configuring Cisco UCS Central Management Pack

This chapter contains the following sections:

Checklist for Configuring the Cisco UCS Central Management Pack

1. Ensure that the option **Allow this server to act as a proxy and discover managed objects on other computers** is enabled for the following server or computer hosting Cisco UCS Monitoring Service.

   - Agent Managed Computers (trusted boundary)

   - Management Server

   - Agent Managed Computers (Untrusted boundary)

   - Gateway Server

2. Ensure that all the Cisco UCS Monitoring Service are visible in **Operations Manager Console** > **Monitoring** > **Cisco UCS Monitoring** > **Cisco UCS Monitoring Service** > **Monitoring Service Dashboard**.

3. Ensure that all Cisco UCS Monitoring Service are discovered and in Healthy State in **Operations Manager Console** > **Administration** > **Device Management** > **(Management Server / Agent Managed)**.

4. Ensure that after adding UCS Central through Add Monitoring Wizard, appropriate Run As Account has been associated with correct Run As Profile.

5. Ensure, if Run As Account distribution is set to More Secure, the computer hosting Cisco UCS Monitoring Service must appear in the Selected Computers list and it must be same as selected for monitoring UCS Central.

6. If Cisco UCS Central is monitored via Gateway Server or agent managed computer (untrusted boundary), ensure that Cisco UCS Central is reachable from that machine.

7. Ensure that Operations Manager **Action Account** must have read and write privileges on TEMP (%SystemRoot%\Temp) folder.

Adding Cisco UCS Central to the Operations Manager

You can add Cisco UCS Central instance from all the Management servers in the Management Group using Operations Manager console or PowerShell cmdlets.

Step 1 Launch the **Operations Manager** console.

Step 2 Navigate to **Authoring** > **Cisco UCS Central**.

Step 3 From the **Tasks** pane, click **Add Monitoring Wizard**.

Step 4 On the **Monitoring Type** tab, click **Cisco UCS Central**.

Step 5 Click **Next**.

Step 6 On the **General Information** tab, review and complete the following:

In the **Connection** area, complete the following:

Name	Description
IP Address/Hostname field	Enter the IP address or the hostname of the UCS Central instance. You can use either the IPv6 or IPv4 address. **Note** For IPv6, enter the address in the `[2001:DB8::1]` format. You can add IPv6 addresses from Release 4.1(1).
Port Number field	Enter the port number specified in the HTTP or HTTPS during Cisco UCS Central configuration. By default, when a secure connection is established, the port number is set to 443.
Connection Mode check box	Establishes a secure HTTPS connection. By default, this option is checked, and you cannot uncheck it.

In the **Proxy Server** area, complete the following:

Name	Description
Enable Proxy Configuration check box	If checked, enables you to enter the proxy server details. Enter the following details: • **Host**—Enter the IP address of the proxy server • **Port**—Enter the port number which is used to connect to the proxy server

Name	Description
Enable Proxy Authentication check box	If checked, enables you to run authentication for the proxy server.
	Enter the following details:
	• **Username**—Enter the username configured on the proxy server
	• **Password**—Enter the password of the proxy server

In the **Cisco UCS Monitoring Service** area, complete the following:

Name	Description
Machine Type drop-down list	This can be one of the following:
	• Agent Managed Computer (Trusted Boundary)
	• Agent Managed Computer (Untrusted Boundary)
	• Management Server
	• Gateway Server
Service Machine drop-down list	Select the FQDN of the machine where Cisco UCS Monitoring Service is installed.

Step 7   To check Operations Manager connectivity to UCS Central, click **Test Connection**.

> **Note**   If the test connection fails, contact your network administrator.

> **Note**   For certification error, follow the instruction provided in the alert dialog box.

Step 8   In the **Authentication** dialog box, enter the username and password, and click **OK**.

If the UCS central instance is configured for domain authentication, enter the username in the <username@domainname> format. The <domainname> is the UCS Central authentication configured in **Administration** > **User Management** > **Authentication in UCS Central**.

> **Note**   When you select Management Server at the same active directory level as the Operations Manager console machine, the dialog box validates the state of Monitoring Service. You can start the Monitoring Service if it stops.
>
> You can add a UCS Central instance on the Management Server if you have local admin privileges . The local admin privileges are required to analyze the state of the Monitoring Service and remotely start the Monitoring Service.

Step 9   Click **Next**.

Step 10   On the **Instance Name** tab, complete the following:

Name	Description
Name field	A UCS Central instance name is set by default.

Name	Description
Description field	Enter a description for the UCS Central instance.

In the Configuration area, complete the following:

Name	Description
Org Discover level drop-down list	Sets the Org level up to which the Orgs can be discovered. By default, the value is set to 3.
Show Unassociated Profiles check box	whether unassociated service profiles are discovered or not. By default, this option is unchecked.
Discover Registered UCS Domains check box	Whether to monitor the registered UCS domains. By default, this option is checked. **Note** Once enabled, you cannot change the settings for these domains.

In the **Management Pack** area, you can continue with the default settings or use one of the following options:

Name	Description
Use Existing Management Pack or Create new check box	If checked, you can select an existing Management Pack to save this instance or to create a new Management Pack click **New**. **Note** We recommend not to select the default Management Pack from the drop-down list

Step 11 Click **Next**.

Step 12 On the **Run As Account** tab, click **Add**.

Step 13 If you want to associate a new run-as account to the UCS Central instance, click **New**.

> **Note** If you have read-only privileges in the UCS Central, you can collect inventory data and monitor faults of UCS Central.
>
> For privileges to perform actions, such as Acknowledge Fault and Launch KVM Console, see:
>
> https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-and-configuration-

Step 14 Click **Next**.

Step 15 On the Summary tab, review the configuration summary, and click Create.
The template for monitoring the UCS Central instance is created.

Creating an Account

Configure a Cisco UCS Central Instance account if you did not associate a Run-As Account with the UCS Central instance while adding the template in the **Add Monitoring Wizard** or if you want to modify the current account association for the UCS Central Instance.

To create an account for the Cisco UCS Central, create a Run-As Account with the Cisco UCS Central instance username and password which is used by the management pack. See, How to Create a Run As Account for detailed instruction.

Note   On the **General Properties** page, select **Simple Authentication** as the **Run-As Account Type**.

Note   If Cisco UCS Central is configured for domain authentication, enter the username in the *<username@domainname>* format. The *<domainname>* is the UCS Central authentication name, configured in **Administration** > **User Management** > **Authentication in Cisco UCS Central**. These credentials are used for all communication with the Cisco UCS Central.

Associating a Run As Account with a Profile

Once Run As Account is created, associate the account with the Cisco UCS Central Run-As Profile. A Run-As Profile is created with UCS Central name in the Operations Manager. See, https://docs.microsoft.com/en-us/system-center/scom/manage-security-create-runas-link-profile for detailed instructions on how to associate an account with a Run-As Profile.

Note   For inventory collection and fault monitoring of UCS Central, read-only privileges in the Cisco UCS Central is required.

To perform the actions, such as Acknowledge Fault and Launch KVM Console, see:

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-and-configuration-guides-list.html

CHAPTER 5

Configuring Fault Acknowledgment

This chapter contains the following sections:

Overview of Fault Acknowledgment

You can use the Operations Manager console to acknowledge the faults in a Cisco UCS Manager. This configuration helps to communicate with Cisco UCS for acknowledging alerts from the Operations Manager console. You can configure this from any management server in the same management group.

✎ **Note** If you have configured fault acknowledgment for UCS Manager Management Pack, then do not perform these tasks for UCS Central Management Pack.

Creating a Resolution State

See https://docs.microsoft.com/en-us/system-center/scom/manage-alert-set-resolution-states to create a resolution state.

✎ **Note** Provide a resolution state name which describes the resolution state. For example, *UCS Acknowledged*.

Creating a Channel

Step 1 In the **Operations Manager** console, click the **Go** tab in the menu bar.

Step 2 From the drop-down list, select **Administration** > **Notification**.

Step 3 Right-click **Channels**, and select **New Channel** > **Command**.

A **Command Notification Channel** dialog box is displayed.

Step 4 In the **Description** tab, enter a name and description for the channel.

Step 5 Click **Next**.

Step 6 On the Settings tab, complete the following:

Name	Description
Full path of the command file field	Enter the path to the command file. For example, *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*
Command line parameters field	Enter the command line parameters for the channel. For example, *-Command "& 'C:\ProgramData\Cisco\Scripts\AcknowledgeFault.ps1'" -instanceId '$Data[Default='Not Present']/Context/DataItem/Custom1$' -serviceMachineName '$Data[Default='Not Present']/Context/DataItem/Custom9$' -dn '$Data[Default='Not Present']/Context/DataItem/Custom10$' -faultCode '$Data[Default='Not Present']/Context/DataItem/Custom4$' -faultId '$Data[Default='Not Present']/Context/DataItem/Custom6$'* **Note** Configure the command line parameters correctly for acknowledging the UCS faults from the Operations Manager.
Startup folder for the command file field	Enter the startup folder name. For example, `C:\ProgramData\Cisco\Scripts` **Note** Before adding the folder, verify the path and the location of the scripts.

Step 7 Click **Finish**.

Creating a Subscriber and Subscription

To create a subscriber and subscription, see https://docs.microsoft.com/en-us/system-center/scom/manage-notifications-create-subscriptions.

Creating a Windows Firewall Inbound Rule

Create a Windows firewall inbound rule to open port 8732 in all the machine running Cisco UCS Monitoring service. This enables the Acknowledge Fault PowerShell script to communicate with the Cisco UCS Monitoring Service.

Customizing Cisco UCS Central Management Pack

This chapter contains the following sections:

Overview of Customizing Cisco UCS Central Management Pack

For each UCS Central added for monitoring in Operations Manager, a Management Pack Template is created in the Management Pack Templates tab of the Cisco Unified Computing System. It is important to understand the components of the Management Pack to perform any customization.

Cisco UCS Central Instance Object Discoveries

All the object discoveries are interval based and they can be periodically run to get the discovery data from monitoring service. To view the list of object discoveries in the pack, complete the following steps:

Step 1 In the **Operations Manager** console, click the **Go** tab in the menu bar.

Step 2 From the drop-down list, select **Authoring**.

Step 3 Select **Management Pack Templates** > **Cisco UCS Central**

Step 4 Select the template pack for which you want to view the object discoveries.

Step 5 Right click and select**View Management Pack Objects** > **Object Discoveries**.

Cisco UCS Central Root (Object Discovery)

This is the top level Object Discovery and the first discovery to run for an UCS Central. It discovers an instance of Cisco UCS Central into Operations Manager. This discovery runs to fetch the inventory and monitoring information from Cisco UCS Central using the Cisco UCS Monitoring Service. These discoveries can be overridden. The later sections shows how to override the object discoveries.

The following are the set of Overrides available for this Object Discovery:

- CacheClass–Defines the managed object for an inventory or monitoring information to be collected from the UCS Central

- Discovery Level–Defines the level up to which Organizations and Service Profiles from the UCS Central should be discovered in the Operations Manager

- Enabled–Defines the enabled state of the object discovery

- Interval Seconds–Defines the interval of execution

- ShowUnassociatedProfiles–Defines whether or not the associated or unassociated Service Profiles should be discovered in Operations Manager.

  The default value is **False** which means an unassociated service profile is not shown.

- Logging Level–Defines if the logging is enabled or disabled for this object discovery

- Timeout Seconds–Defines the timeout period for the discovery script to execute

Note   By default the Cisco UCS Central Root discovery is programmed to execute every two hours (7200 seconds) to get any modifications from the Cisco UCS Central.

Overriding Object Discoveries

Step 1   Go to **Object Discovery** page of the Cisco UCS Central instance.

Step 2   Select the object for which you want to override the properties.

Step 3   Right-click and select**Override** > **Override the Object Discovery** > **For All Objects of Class**.

Step 4   In the **Override Properties** dialog box, complete the following:

- Check the Override check box

- Modify the override values

- Click **OK** > **Apply**.

Note   When an object discovery is enabled using override, all its target class discoveries to the top level of Cisco UCS Central instance must be enabled. When disabled, the class discoveries targeted at this class to the leaf levels are not monitored.

Overriding Object Discoveries using PowerShell Cmdlets

You can disable or override object discoveries using PowerShell Cmdlets. For more details, see Retrieving, enabling, or disabling UCS Manager Object Discoveries.

Rules

Cisco UCS Core Library Management Pack has rule or rules for each UCS Central faults. The rules are inherited whenever the UCS Manager templates instance is create from **Add Monitoring Wizard**.

Note Rules are included for faults with Severity equal to Critical, Major, Minor, Warning, and Type, and not equal to FSM or Configuration.

Depending on the UCS Manager component on which a fault can occur, there can be one or multiple rules defined per UCS fault.

For example, F10000210 can occur on the following UCS Central components:

"org-[name]/ip-pool-[name]"

In the given example, parsing from the back side of the DN, Organization is the discovered components, so one rule is available that is

Fault Rule: Organization.F10000210

Now, consider the fault F10000195, which can occur of the following UCS Central components.

"extpol/reg/controllers/contro-[id]"

In the given example, parsing from the back side of the DNs, component are not discovered by the UCS Central Management Pack. So, a single rule is available whose target would be Cisco UCS Central Root Class and the fault name is:

Fault Rule: F10000195

Rules are event-based. Each rule can generate multiple alerts in the Operations Manager based on the event raised by the Cisco UCS Monitoring Service.

Note Currently, the Cisco UCS Manager Management Pack does not support display of informational faults from the Cisco UCS in Operations Manager.

Note UCS Central FSM faults are transient faults. So, the running version of the management pack does not support such faults.

For a complete list of FSM faults not supported in the Management Pack, see FSM Faults.

PreConfigure Rule

When all the Management Packs are imported, before Cisco UCS Central templates are created, configure (Enable/Disable) the rule from UI or Cmdlets. Once configured, you can import the templates and the configuration takes effect on all the templates which are added later. If you want to change the configuration of rules after the templates are imported, re-configure the rule. This automatically takes effect on the existing templates and for all the future templates they are to be added.

Enabling Rules using PowerShell Cmdlets

You can enable rules using PowerShell Cmdlets. For more details, see retrieving, enabling or disabling UCS Manager Fault Rules.

Severity Mapping

This section describes the mapping between the severity of faults in the UCS Central and the alert severity rules in Operations Manager console.

The following table shows the mapping of severity levels between the Cisco UCS Central and rules.

Severity Level	Cisco UCS (Severity)	Rules (Alert Severity)
2	Critical, Major	Critical
1	Minor, Warning	Warning

Note   All Rules are enabled by default.

Viewing List of Rules in the Management Pack

Step 1   From the Operations Manager menu bar, click **Go** and select **Authoring**.

Step 2   From the navigation pane, select **Management Pack Templates**.

Step 3   Select **Cisco UCS Central**.

Step 4   Right-click the Cisco UCS Central instance, and select **View Management Pack Objects** > **Rules**.

Overriding a Rule

Step 1   From Operations Manager menu bar, click **Go** and select **Authoring**.

Step 2   From the navigation pane, select **Management Pack Templates**.

Step 3   Select **Cisoc UCS Central**.

Step 4   Right-click the Cisco UCS Central instance, and select **View Management Pack Objects** > **Rules**.

Step 5   On the **Rules** page, select the rule which you want to override.

Step 6   Right-click the rule and click **Overrides** > **Override the Rule** > **For all objects of class**.

Step 7   On the **Override Properties** page, check the parameter you want to override and then modify the override value.

Step 8   Click **OK** to close the Override page.

Step 9   Close the **Rules** page.

Migrating the Cisco UCS Central to a Different Monitoring Service

In a deployment where multiple Operations Manager Management Servers and Agent Managed Computers are present, Cisco UCS Monitoring Service could be installed on more than one computer to monitor multiple Cisco UCS Central. This helps in sharing the load of monitoring multiple Cisco UCS Central among different Management Servers and Agent Managed Computers. While doing so, sometimes it may be required to assign the monitoring of Cisco UCS Central from one Cisco UCS Monitoring Service to another Monitoring Service.

Step 1   From the menu bar of the Operations Manager console, click the **Go** tab.

Step 2   From the drop-down menu, select **Authoring**.

Step 3   Select **Management Pack Templates**.

Step 4   Select **Cisco UCS Central**.

Step 5   Right-click one of the Cisco UCS Central instances and click **Properties**.

Step 6   From the drop-down list, Select a different machine type or service machine or both.

Step 7   Click **OK** > **Apply**.

Monitoring Cisco UCS Central Using Operations Manager

This chapter contains the following sections:

About the Monitoring Pane in Operations Manager

After you install and configure the Cisco UCS Central Management Pack, you can use the **Monitoring pane** in the Operations Manager to display a summary and components of monitored Cisco UCS Central. The Cisco UCS Monitoring tab, State, and Alert Dashboards in the Monitoring pane provide a complete view of the health of the UCS Central instances and its components.

Viewing List of Rules in the Management Pack

Step 1   From the Operations Manager menu bar, click **Go** and select **Authoring**.

Step 2   From the navigation pane, select **Management Pack Templates**.

Step 3   Select **Cisco UCS Central**.

Step 4   Right-click the Cisco UCS Central instance, and select **View Management Pack Objects** > **Rules**.

About the Cisco UCS Central Monitoring

The Cisco UCS Central Monitoring tab displays state and alert dashboards for all discovered Cisco UCS Central instances, and its components.

This folder contains the following subfolders related to Cisco UCS Central:

- Management Pack Events

- Cisco UCS Monitoring Service

- UCS Central Monitoring

Management Pack Events

This view shows any alert related to execution of monitoring scripts in Operations Manager, some of the common errors are listed in the table below:

Serial No.	Error Code	Error Description	What to check
1	19900	Service Connection Error	Verify the service machine entry in the **Add Monitoring Wizard**
2	19900	Service not found or not running	Check if the monitoring service is up and running on the service machine
3	19900	Error in Application	Verify whether the account is associated to the profile, and the account is authorized to make a connection to the UCS Central Instances

Cisco UCS Monitoring Service

The Cisco UCS Monitoring folder comprises **Monitoring Service Dashboard**, and **Monitoring Service Statistics**. The **Monitoring Service Dashboard** contains health state of all the machines connected in the **Management Group** and have the service installed.

The **Monitoring Service Statistics** contains several statistical graphs for thread count, IO Write Bytes/Sec, Elapsed Time, IO Read Bytes/Sec, % User Time, % Processor Time, and Page Faults/Sec.

Selecting a graph shows you the legends available in the bottom pane. Check or uncheck the instance depending on whether you want to see the statistical values in graphical form.

Start Service

If the Monitoring Service which is used to monitor the Cisco UCS Central is stopped, an alert is generated in the Alert View. Click the Start Service task to remotely start the Monitoring Service from the Operations Manager console.

Step 1   Launch Operations Manager console.

Step 2   From the menu bar, click the **Go** tab.

Step 3   From the drop-down menu, select **Monitoring**.

Step 4 Navigate to **Cisco UCS Monitoring** > **Cisco UCS Monitoring Service** > **Monitoring Service Dashboard**..

Step 5 Select the Monitoring Service.

Step 6 From the **Tasks** pane, click **State View**.

Step 7 Click **Start Service**.

Stop Service

If the Monitoring Service is no longer used to monitor Cisco UCS Central, then the Monitoring Service could be stopped from Operations Manager console.

Step 1 Launch Operations Manager console.

Step 2 From the menu bar, click the **Go** tab.

Step 3 From the drop-down menu, select **Monitoring**.

Step 4 Navigate to **Cisco UCS Monitoring** > **Cisco UCS Monitoring Service** > **Monitoring Service Dashboard**..

Step 5 Select the Monitoring Service.

Step 6 From the **Tasks** pane, click **State View**.

Step 7 Click **Stop Service**.

Note Ensure that all Cisco UCS Monitoring Services added in the Operations Manager are in healthy state. You can verify the health status in the alert dashboard.

Cisco UCS Central Monitoring Dashboards

The Cisco UCS Central Instance folder contains a sub-folder for each Cisco UCS Central instances monitored by Operations Manager. The UCS Central Monitoring folder contains the following sub-folders:

- **UCS Central Alert Dashboard**—Displays all alerts generated in the UCS Central. The alerts are further categorized into the following views:

   - Active Alerts

   - Acknowledge Alerts

   - Cleared Alerts

- **UCS Central Diagram**—Displays a graphical view of the relationship between different UCS Central components for all Instances. It also displays the hierarchal level of all UCS domains and its components, such as chassis, blade, and FI discovered through UCS Central.

- **UCS Central State Dashboard**—Display health state and other inventory information about Cisco UCS Central.

| Note | UCS Manager Management Pack is not required to discover and monitor UCS domains managed by UCS Central. |

| Note | UCS domain performance metrics is not collected by UCS Central Management Packs. |

Launching UCS Central GUI

In order to launch the UCS Central GUI, network connectivity should be available between the computer where the Operations Manager application is running and the Cisco UCS Central.

Step 1   In the Operations Manager console menu bar, click the Go tab.

Step 2   From the drop-down menu, select **Monitoring**.

Step 3   Navigate to **Cisco UCS Monitoring** > **UCS Central Monitoring** > **UCS Central State Dashboard**

Step 4   Select the target Cisco UCS Central on which the Cisco UCS Central must be launched.

Step 5   In the **Tasks** pane, click **Launch UCS Central GUI** to launch the web UI.

Loading the UCS Central Inventory Data

Step 1   In the **Monitoring** pane, expand **Cisco UCS Monitoring** > **UCS Central Monitoring** > **UCS Central State Dashboard**.

Step 2   Select the Cisco UCS Central target for which inventory data is to be loaded.

In the **Cisco UCS Central Instance Tasks** pane, select the **Load UCS Central Inventory Data**.

Step 3   Click **Load Cisco Central Inventory Data**.

A **Run Task- Load UCS Inventory Data** dialog box appears.

Step 4   Click **Run** to load the inventory data output.

Step 5   Click **Close** to exit the dialog box.

Ping UCS Central

Use **Ping** to check the connectivity between Operations Manager console and the Cisco UCS Central.

Step 1   On the menu bar of the Operations Manager, click the **Go** tab.

Step 2   From the drop-down menu, select **Monitoring**.

Step 3   Navigate to **Cisco UCS Monitoring** > **UCS Central Monitoring** > **UCS Central State Dshboard**.

Step 4   Select a UCS Central instance.

Step 5	On the **Tasks** pane, select **State View**.
Step 6	On the **Cisco UCS Tasks** pane, select **Ping UCS Central**.
Step 7	Review the output details, and click **Close**to exit.

Ping UCS Central Continuously

Use **Ping Continuously (ping-t)** to check the connectivity between Operations Manager console and the Cisco UCS Central.

Step 1	On the menu bar of the Operations Manager, click the **Go** tab.
Step 2	From the drop-down menu, select **Monitoring**.
Step 3	From the list, select a UCS Central.
Step 4	On the **Cisco UCS Tasks** pane, select **Ping UCS Manager Continuously (ping-t)**.
Step 5	Review the output details, and click **Close** to exit.

Logical Inventory

The logical inventory provides different views and insight to health state, inventory, fault information, and components of Cisco UCS Central.

The following dashboards can be viewed for each UCS components:

- Alert Dashboard

- Diagram View

- State Dashboard

Viewing Organization Details

Different views and folders in the Organization folder provides an insight to health state, inventory and fault information about various logical components of UCS Central. You can view the following views and subfolder:

- **Organization Alert Dashboard**—Displays all active, acknowledged and cleared alerts in different views for all organizations and its components. This Alert view also displays the alerts from objects which are not directly monitored by the management pack. The alerts are further categorized into the following views:

    - Active Alerts

    - Acknowledge Alerts

- **Organization State Dashboard**—Displays Health State of organization and other related information of Cisco UCS Central.

Note By default, the management pack discovers three levels of organization and its components (service profile). To discover more than three levels, override the Discovery level in Cisco UCS Central Instance Object Discovery.

Service Profile

You can view the following details related to the service profiles:

- **Service Profile Alert Dashboard**—Displays active, acknowledged and cleared alerts of all service profiles in different views.

- **Global Service Profile State Dashboard**—Displays Health State of all global service profiles and related information

- **Local Service Profile State Dashboard**—Displays all the local service profiles and related information

Note This dashboard only lists the Service Profiles of UCS Domain registered via UCS Central, and does not collect related faults. Therefore, the health state is always healthy.

Note UCS domains and its components, such as chassis, blade, and fabric interconnect, discovered through UCS Central are displayed under UCS Domain folder in the corresponding views.

Additional parameters like UCS Central name, description and so on, are added for UCS Central discovered components to distinguish them as UCS Central managed components.

Note UCS Manager Management Pack is not required to discover and monitor UCS domains managed by UCS Central.

UCS domain performance metrics are not collected by UCS Central Management Packs.

Alert Operations

Acknowledging the UCS Manager Faults

This operation could be performed on an Operation Manager alert created by the Management Pack due to a fault on Cisco UCS Central. Using this operation, user can acknowledge an Cisco UCS Central fault from the Operations Manager Console itself.

Step 1 Select an alert in Operations Manager which belongs to a Cisco UCS Central.

Step 2 Right click on the alert and choose **Set Resolution State**.

Step 3   Click UCS Acknowledged which is in configured resolution state.

Note   UCS domains which are monitored through Central, such domains faults are not acknowledged.

Viewing the Knowledge Article of Alerts

Knowledge Articles provide more information about an alert generated in Operations Manager. This Management Pack supports knowledge articles for every UCS fault generated as alert in Operations Manager. Knowledge articles will help the user to get additional information about the alert like Fault Cause, Explanations and Resolution steps. Resolution Steps should be followed to resolve the alerts.

Step 1   Select UCS Central alert in Operations Manager.

Step 2   Right click on the alert and select **Properties**.

Step 3   On the properties window, click the **Product Knowledge** tab.

Note   Local UCSM Organization and their faults are not displayed in UCS Central **Alert** dashboard.

Clearing of Alerts

When a fault or condition is cleared in Cisco UCS Central, the corresponding alert in operations manager is set to cleared state. There is no manual activity required to close an alert in the Operations Manager console.

By, default, for every 90 seconds interval all alerts are cleared. However, you can modify the interval period.

Rule Name: Cisco UCS Update and Close Alert Rule

Target: All Management Servers Resource Pool

Overridable Parameters:

- Enabled: This parameter can be used to enable or disable the rule (default value: true)

- EventQueryIntervalInSeconds : This parameter is used to set the desired time interval for which the events should be queries (default value : 120 seconds)

Note   If this parameter value is set to **0**, then the rule processes all the older events every time it runs. Hence, to avoid timeout and overlapping between consecutive runs of this rule, you should also set the parameters **Interval Seconds** and **Timeout Seconds** accordingly to higher values.

- Interval Seconds: This parameter is used to set the frequency to run the rule (default value : 90 seconds)

- Logging: set the logging (default value : false)

- Timeout Seconds: Set the time out interval for the rule (default value : 60 seconds)

PowerShell Cmdlets for Cisco UCS Central Management Pack

This chapter contains the following section:

Importing Cmdlets from the PowerShell Module

Step 1 On a Management Server open Operations Manager Shell.

The Cisco PowerShell module is shared across all the Management Servers in the Management Group.

Note The **CiscoUcsCentralScomPs** module is installed in `%PROGRAMDATA%\Cisco\Modules`.

Step 2 Import the CiscoUcsCentralScomPs module.

Step 3 To see all cmdlets in CiscoUcsCentralScomPs module, use the Get-Command -Module CiscoUcsCentralScomPs command in the PowerShell window.

Note If you are using another PowerShell session, import the OperationsManager module before importing the CiscoUcsCentralScomPs module.

Adding or Updating UCS Central Instances

Add-UcsCentralScomInstance

Provide either an existing management pack or name for new management pack to add this instance. If none is provided, a new management pack is created with the same name as that of instance.

```
Add-UcsCentralScomInstance -UcsIPAddress <string>
-MachineType <string> {Agent Managed Computer (Trusted Boundary)
| Agent Managed Computer (Untrusted Boundary) |
```

```
Management Server | Gateway Server} -MachineName <string>
-InstanceName <string> [-Port <int>]
[-ManagementPackName <string>] [-Description <string>]
[-ProxyHost <string>]
[-ProxyPort <int>] [-ProxyUsername <string>]
[-ProxyPassword <string>] [-ExistingRunAsAccount <string>]
[-OrgDiscoveryLevel <int>] [-ShowUnassociatedProfiles]
[-DisableUCSDomainsDiscovery]  [<CommonParameters>]

Add-UcsCentralScomInstance -UcsIPAddress <string>
-MachineType <string> {Agent Managed Computer (Trusted Boundary)
| Agent Managed Computer (Untrusted Boundary) |
Management Server | Gateway Server} -MachineName <string>
-InstanceName <string> -RunAsAccount <string>
-RunAsCredential <pscredential> [-Port <int>] [-ManagementPackName
<string>] [-Description <string>] [-ProxyHost
<string>] [-ProxyPort <int>] [-ProxyUsername <string>]
[-ProxyPassword <string>] [-OrgDiscoveryLevel
<int>] [-ShowUnassociatedProfiles] [-DisableUCSDomainsDiscovery]
[<CommonParameters>]

Add-UcsCentralScomInstance -UcsIPAddress <string>
-MachineType <string> {Agent Managed Computer (Trusted Boundary)
| Agent Managed Computer (Untrusted Boundary) |
Management Server | Gateway Server} -MachineName <string>
-InstanceName <string> -ExistingManagementPack
<ManagementPack> -Description <string> -RunAsAccount <string>
-RunAsCredential <pscredential> [-Port <int>]
[-ProxyHost <string>] [-ProxyPort <int>]
[-ProxyUsername <string>]
[-ProxyPassword <string>] [-OrgDiscoveryLevel
<int>] [-ShowUnassociatedProfiles] [-DisableUCSDomainsDiscovery]
[<CommonParameters>]

Add-UcsCentralScomInstance -UcsIPAddress
<string> -MachineType <string> {Agent Managed Computer (Trusted Boundary)
| Agent Managed Computer (Untrusted Boundary) |
Management Server | Gateway Server} -MachineName <string>
-InstanceName <string> -ExistingManagementPack
<ManagementPack> -Description <string> [-Port <int>] [-ProxyHost
<string>] [-ProxyPort <int>] [-ProxyUsername <string>]
[-ProxyPassword <string>] [-ExistingRunAsAccount <string>]
[-OrgDiscoveryLevel <int>] [-ShowUnassociatedProfiles]
[-DisableUCSDomainsDiscovery]  [<CommonParameters>]
```

Parameter	Description
UcsIPAddress	IP address or host name of the UCS Central to register
MachineType	Type of Operations Manager machine to register the UCS Central
MachineName	FQDN of the machine on which UCS Central is registered (all scripts related to this UCS Central MP will be run on this machine)
InstanceName	Name to be given to this UCS Central instance
Port	Port number

Parameter	Description
ManagementPackName	Name of the new management pack to be created (if not specified, InstacneName will be used for management pack)
Description	Optional description string for the UCS Central instance
NoSsl	Switch parameter to specify non-secure (http) connectivity with UCS Central
ProxyHost	IP address or hostname of proxy server to be used for communicating with UCS Central
ProxyPort	Proxy port number
ProxyUsername	Username for proxy server
ProxyPassword	Password for proxy server
ExistingRunAsAccount	Name of the existing Run-As account to be used for this instance
RunAsAccount	Name of new Run-As account to be created for this instance
RunAsCredential	UCS credentials for the new Run-As account to be created
ExistingManagementPack	Existing management pack object to which the instance is to be added

Example

```
$secureString =ConvertTo-SecureString "Nbv12#45" -AsPlainText –Force
$credentials = New-Object System.Management.Automation.PSCredential("admin", $secureString)
Add-UcsCentralScomInstance -UcsIPAddress "10.106.233.245" -MachineType 'Management Server'

-MachineName 'SCOM2016RTMMS.qatcslab.cisco.com' -InstanceName 'CISCO_UCS_Central_MS'
-RunAsAccount 'central245new'
-RunAsCredential $credentials  -Port '443' -ManagementPackName 'CISCO_UCSC_MP_NEW'
-Description "sampledescription"
-OrgDiscoveryLevel 4 -ShowUnassociatedProfiles  -DisableUCSDomainsDiscovery
```

Update-UcsCentralScomInstance

```
Update-UcsCentralScomInstance [-InstanceName] <string> [[-UcsIPAddress] <string>] [[-Port]
 <string>]
[[-MachineType] <string> {Agent Managed Computer (Trusted Boundary) | Agent Managed Computer

(Untrusted Boundary) | Management Server | Gateway Server}] [[-MachineName] <string>]
[[-Description]
<string>] [[-Secure] <bool>] [[-ProxyHost] <string>] [[-ProxyPort] <int>] [[-ProxyUsername]
 <string>] [[-ProxyPassword] <string>]
```

Parameter	Description
UcsIPAddress	IP address or host name of the UCS Central to register
MachineType	Type of Operations Manager machine to register the UCS Central
MachineName	FQDN of the machine on which UCS Central is registered (all scripts related to this UCS Central MP will be run on this machine)
Port	Port number
Description	Optional description string for the UCS Central instance
ProxyHost	IP address or hostname of proxy server to be used for communicating with UCS Central
ProxyPort	Proxy port number
ProxyUsername	Username for proxy server
ProxyPassword	Password for proxy server

Example

```
Update-UcsCentralScomInstance -InstanceName ' CISCO_UCS_Central_MS ' -UcsIPAddress
"10.106.233.245" -Port '443'
-MachineType  "Management Server"  -MachineName ' SCOM2016RTMMS.qatcslab.cisco.com '
-Description 'sample' -Secure $True -ProxyHost "10.65.183.85" -proxyport 808  -ProxyUsername
 'scom'
-ProxyPassword 'scom'  -OrgDiscoveryLevel 2
```

Get-UcsCentralScomAllInstances

```
Gets all existing UCS Central instances
[available in MP v4.1.5]
```

Get-UcsCentralScomDiscovery

```
Get-UcsCentralScomDiscovery -InstanceName <string> -ClassName <string[]>  [<CommonParameters>]
```

Example

```
Get-UcsCentralScomDiscovery -InstanceName "CISCO_UCS_Central_MS" -DiscoveryName "Organization
 Discovery"
```

Enable-UcsCentralScomDiscovery

```
Enable-UcsCentralScomDiscovery [-Discovery] <ManagementPackDiscovery[]>  [<CommonParameters>]
```

Example

```
$o = Get-UcsCentralScomDiscovery -InstanceName "CISCO_UCS_Central_MS" -ClassName 'Global
Service Profile'
Enable-UcsCentralScomDiscovery -Discovery $o
```

Disable-UcsCentralScomDiscovery

```
Disable-UcsCentralScomDiscovery [-Discovery] <ManagementPackDiscovery[]>  [<CommonParameters>]
```

Example

```
$o = Get-UcsCentralScomDiscovery -InstanceName "CISCO_UCS_Central_MS" -ClassName 'Global
Service Profile'
Disable-UcsCentralScomDiscovery -Discovery $o
```

Get-UcsCentralScomRule

```
Get-UcsCentralScomRule [[-Class] <string[]>] [[-FaultID] <string[]>]  [<CommonParameters>]
```

Example

```
Get-UcsCentralScomRule -class "Cisco UCs Central Instance"
```

Enable-UcsCentralScomRule

Provide a name of management pack to which the override is added.

```
Enable-UcsCentralScomRule [-Rule] <ManagementPackRule[]> [-ManagementPackName] <string>
[<CommonParameters>]
```

Example

```
Enable-UcsCentralScomRule -Rule (Get-UcscentralscomRule -FaultID "F10000374")
-ManagementPackName 'CISCO_UCSC_MP'
```

Disable-UcsCentralScomRule

Provide a name of management pack to which the override is added.

```
Disable-UcsCentralScomRule [-Rule] <ManagementPackRule[]> [-ManagementPackName] <string>
[<CommonParameters>]
```

Example

```
Disable-UcsCentralScomRule -Rule (Get-UcscentralscomRule -FaultID "F10000374")
-ManagementPackName "Cisco Ucs Central Management Pack"
```