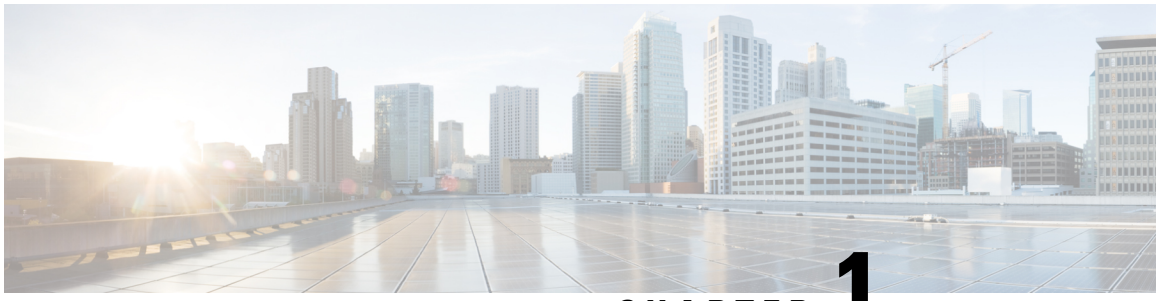
Cisco IMC Management Pack User Guide, Release 4.x For Microsoft System Center Operations Manager

First Published: 2016-05-04

Last Modified: 2021-09-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

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.
{ x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Conventions	Indication
[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

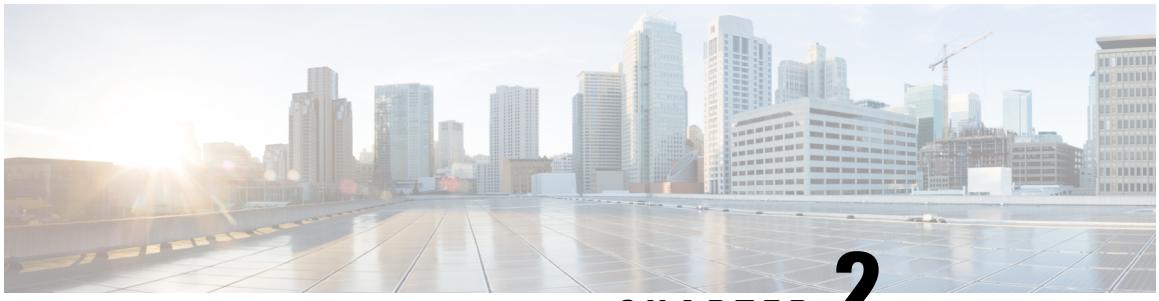
An ISO file containing all B and C-Series documents is available at the following URL:https://software.cisco.com/download/type.html?mdfid=283853163&flowid=25821 From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

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.



CHAPTER 2

Overview

This chapter contains the following sections:

About Cisco IMC Management Pack

Microsoft System Center Operations Manager (SCOM) provides infrastructure monitoring that's flexible and cost-effective, helps ensure the predictable performance and availability of vital applications, and offers comprehensive monitoring for your data center and cloud, both private and public.

The Cisco IMC Management Pack is a definition file that contains predefined monitoring settings. The plugin enables an agent to monitor a group of Cisco Integrated Management Controllers (IMC) of standalone servers. It contains object discoveries for discovering the IMC servers and contains rules to monitor the server health and raise alert for the faults occurring on these servers.

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.

The supported Windows server for System Center Operations Manager are 2012, 2016 and 2019.

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 Cisco IMC Release

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

- Release 4.1

Note Supported only for Cisco UCS Management Pack Suite version 4.1.4 or higher.

- Release 4.0

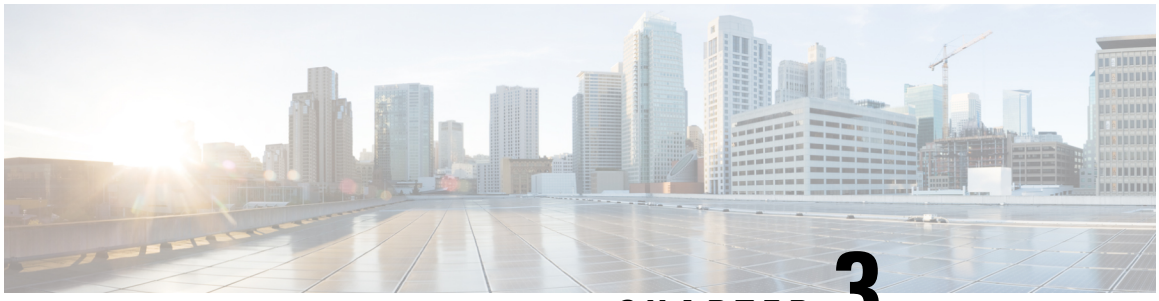
- Release 3.1

Note Supported only for Cisco UCS Management Pack Suite v4.1.1 or higher.

- Release 3.0

Note Supported only for Cisco UCS Management Pack Suite v4.1.1 or higher.

- Release 2.0(3) or higher



CHAPTER 3

Introduction

This chapter contains the following sections:

Key Features

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

Rule(s) per IMC Fault

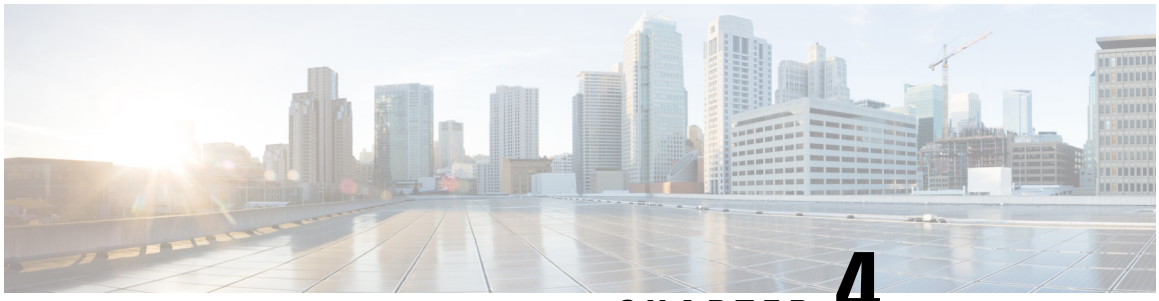
This management pack implements one rule per Cisco IMC domain fault. This provides improved power of customization at the fault level. You can override parameters, such as changing the priority and severity, enabling or disabling rules from the Operations Manager console interface. Apart from the console 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 IMC templates.

Modularized Management Pack Design

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



CHAPTER 4

Configuring the Cisco IMC Management Pack

This chapter contains the following sections:

Check list for Configuring the Cisco IMC 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 following server / computer hosting Cisco UCS Monitoring Service.
   - Agent Managed Computers (trusted boundary)
   - Management Server
   - Agent Managed Computers (Untrusted boundary)
   - Gateway Server
2. Ensure that all servers and system hosting 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 server(s) / computer(s) hosting 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 IMC Group through Add Monitoring Wizard, appropriate Run As Account has been associated with correct Run As Profile.
5. Ensure that if Run As Account distribution is set to More Secure, the computer hosting Cisco UCS Monitoring Service must appear in Selected Computers list and it must be same as selected for monitoring IMC Group.
6. If Cisco IMC Group is monitored via Gateway Server or agent managed computer (untrusted boundary), ensure that Cisco IMC is reachable from that machine.
7. Ensure that Operations Manager **Action Account** must have read and write privileges on TEMP (%SystemRoot%\Temp) folder.

Adding a Cisco IMC Group to the Operations Manager

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

Step 2 Navigate to **Authoring** > **Management Pack Templates** > **Cisco IMC**.

Step 3 In the Task pane, click **Add Monitoring Wizard**.

The **Add Monitoring Wizard** is displayed.

Step 4 Click **Next**.

Step 5 In the **Cisco IMC Discovery Method** tab, enter the following:

Name	Description
Select IP Address Type	You can set an IPv4 or IPv6 address of the server. For IPv6, enter the address in the `[2001:DB8:1]` format. By default, IPv4 address is selected. Adding IPv6 addresses is valid from Release 4.1(1).
Discover via IPv4 or IPv6 Combinations	Depending on the type of IP address selected, the corresponding IP address is displayed. Enter range of IP addresses separated by hyphen, and multiple single IP address separated by comma. You can add up to 254 IP addresses. For example, 10.105.210.15-10.105.210.129, 10.104.200.35, 10.104.100.133, 10.106.200.136-10.106.200.200. For IPv6, enter the address in the `[2001:DB8::1]` format.
Discover via IPv4 or IPv6 Range	Depending on the type of IP address selected, enter the corresponding IP address. Enter the first and the last IP addresses.
Discover via Subnet mask	Depending on the IP address selected, enter the network address and subnet mask.

Step 6 Click **Next**.

Step 7 In the **Discovery Results** tab, select the range of the IP addresses, then uncheck the IP addresses which you do not want to monitor.

Step 8 Click **Next**.

Step 9 In the **Connection Parameters** tab, review and complete the following:

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

Name	Description
Port Number field	Enter the port number specified in the HTTP or HTTPS during IMC configuration. By default, the port number is set to 80 for nonsecure connection, and 443 for secure connection.
Connection Mode check box	If checked, a secure HTTPS connection is established. If unchecked, a nonsecure HTTP connection is established. By default, the port is set to 80.

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
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 IMC Monitoring Service is installed.

Step 10 On the **Group Name** page, enter a name for the group of standalone Cisco IMC Servers. Optionally enter a description for the group.

Note In the **Management Pack** area, check the **Use existing management pack or create new** to use the existing management pack or click **New** to create a new management pack.

Step 11 To add an account, click **Run As Account**, and complete the following:

- From the drop-down list of the **Add Run As Account** dialog box, select **Run As Account** or click **New**.
- In the **Create Run As Account** dialog box, enter the following:
  - **Display Name**
  - **Description**
  - **Account Name**
  - **Password**
  - **Confirm Password**

Step 12 Click **Next**.

Step 13 Review your settings to configure the template in the **Summary** page. and click **Create**.

You can also add the Cisco IMC Group to Operations Manager using the PowerShell cmdlets, see Adding or Updating Cisco IMC Groups, on page 26.

Creating an Account

Configure Cisco IMC group account if you did not associate a Run-As Account with the IMC Group, or if you want to modify the current account association for the IMC group.

To create an account for the Cisco IMC group, create a Run-As Account with the Cisco IMC username and password, to be used by the management pack.

For more information on creating a Run-As account, see How to Create a Run As Account.

Important We recommend to select the more secure option while creating a Run As Account and select the machine from which the IMC group instance is monitored.

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

Note If the Cisco IMC is configured for domain authentication, enter the account name on the **Credentials** page in the <username@domainname> format, where domainname is the LDAP domain name configured in Cisco IMC.

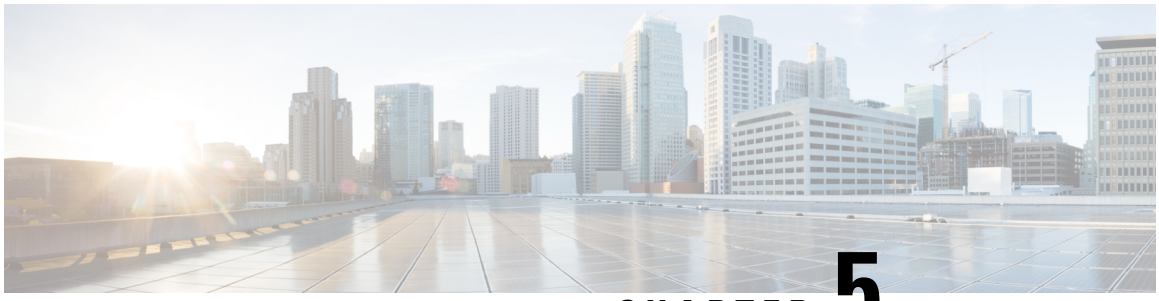
Note A Cisco IMC user account with read-only privileges can discover and monitor Cisco IMC from the Operations Manager console.

Associating an Account to a Run-As Profile

After you create an account, associate the account with the IMC Group's Run-As Profile. A Run-As Profile is created with the same name as the IMC Group name in the Operations Manager.

For more information on associating an account with a Run-As Profile, see https://docs.microsoft.com/en-us/system-center/scom/manage-security-create-runas-link-profile.

Note An account associated with the IMC Group Run-As Profile is used to establish a connection with all the Cisco IMC servers within the IMC Group.



CHAPTER 5

Monitoring Cisco IMC Using Operations Manager

This chapter contains the following sections:

Accessing the Cisco IMC Monitoring Pane

After installing and importing Cisco IMC management pack, you can use the **Monitoring** pane in the SCOM console to view the summary and the components of the Cisco IMC server.

Step 1 Go to **Operations Manager** console and click the **Go** tab.

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

Step 3 Expand **Cisco UCS Monitoring** > **IMC Monitoring**.

IMC Monitoring

The IMC Monitoring folder provides the following views:

- **IMC Group Diagram** — Displays the health and detailed information about the Cisco IMC servers. It also displays the hierarchical level of all Cisco IMC instances and its components discovered through Cisco IMC.

- **IMC Group State Dashboard** provides a consolidated view of all the groups of Cisco IMC monitored by this management pack. It also provides detail of the IMC groups, the health state and the monitoring server.

  The health status of the Cisco IMC group can be one of the following:

  - **Critical**—Indicates that the health of one or more Cisco IMC Servers within that group is critical.
  - **Warning**—Indicates that the health of one or more Cisco IMC servers within that group is unhealthy and requires attention.
  - **Healthy**—Indicates that all the Cisco IMC servers in that group are healthy.

- **Miscellaneous Alert View** — Displays all the alerts encountered during discovery of Cisco IMC servers in the group. The types of alerts are:

  - **Ping Failure**—Displays all the IPs for which the ping has failed.

    Note This feature is not applicable to Cisco IMC Management Pack, Release 1.2(1) and Cisco UCS Management Pack Suite, Release 4.0(1)

  - **Login Failure**—Displays all the IPs for which the login has failed.
  - **Unsupported IMC Server Model**—Displays all the Cisco IMC IP addresses whose model is not supported.
  - **Unsupported IMC Version**—Displays all the IPs which does not have the supported Cisco IMC version.

Manually Loading Cisco IMC Inventory Data

To collect the inventory data from all Cisco IMC servers in the group, follow these steps:

Step 1 In the **Monitoring** pane, navigate to **Cisco UCS Monitoring** > **IMC Monitoring** > **IMC Group State Dashboard**.

Step 2 From the list of available IMC server groups, select the IMC server group for which you want to load the inventory data.

Step 3 In the **Tasks** pane, click **Load Cisco IMC Inventory Data**.

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

Step 4 Click **Run**.

Step 5 Review the output data, and click **Close** to exit the dialog box.

Manually Loading Cisco IMC Fault Data

Step 1 In the **Monitoring** pane, navigate to **Cisco UCS Monitoring** > **IMC Monitoring** > **IMC Group State Dashboard**.

Step 2 From the list of available IMC server groups, select the IMC server group for which you want to load the Cisco IMC fault data.

Step 3 In the **Tasks** pane, click **Load Cisco IMC Fault Data**

A **Run Task - Load Cisco IMC Fault Data** dialog box appears.

Step 4 Click **Run**.

Step 5 Review the output data, and click **Close** to exit the dialog box.

IMC Chassis

The following views are available in the IMC Chassis folder:

- **IMC Chassis Alert View**—Displays the alerts related to all Cisco IMC chassis which are added. Various alert parameters such as the **Health State** icon, source, name, description, and custom fields provide more information about the fault.

Note The **Knowledge** section of the alert provides information about the resolution of the fault.

- **IMC Chassis State Dashboard**—Displays all the Cisco IMC chassis. The Details View pane displays the Cisco IMC chassis details, such as the model, serial number, available memory, IP address, and so on.

IMC Server(s)

The following views are available in the IMC Server(s) folder:

- **IMC Server Alert View** — Displays the alerts related to all Cisco IMC servers which are added. Various alert parameters such as the **Health State** icon, source, name, description, and custom fields provide more information about the fault.

Note The **Knowledge** section of the alert provides information about the resolution of the fault.

- **IMC Server State Dashboard** — Displays all the Cisco IMC servers. The Details View pane displays the Cisco IMC server details such as the model, serial number, available memory, IP address, and etc.

Launching Cisco IMC Web Interface Using Operations Manager Console

Step 1 In the **Monitoring** pane, navigate to **Cisco UCS Monitoring** > **IMC Monitoring** > **IMC Server(s)** > **IMC Server State Dashboard**.

Step 2 Select the target Cisco IMC server on which the Cisco IMC web interface must be launched.

Step 3 In the **Tasks** pane, click **Launch CIMC** to launch the CIMC web interface.

Launching the KVM Console of Cisco IMC Using Operations Manager Console

Note The KVM console requires Java Version 1.6 Update 45 or higher for Cisco IMC MP 4.1.3 or earlier versions.

Note To launch the KVM console, you must have valid Cisco IMC user credentials with administrator or user role privileges and must be associated with a group profile.

Step 1 In the **Monitoring** pane, navigate to **Cisco UCS Monitoring** > **IMC Monitoring** > **IMC Server(s)** > **IMC Server State Dashboard**.

Step 2 Select the target Cisco IMC server on which the KVM console must be launched.

Step 3 In the **Tasks** pane, click **Launch KVM** to launch the KVM console.

Step 4 Click **OK**.

Note When prompted, we recommend you to set the PowerShell execution policy to AllSigned or RemoteSigned. You can select either [R] Run once or [A] Always run option to set the execution policy.

Note The KVM console cannot be launched on a Cisco IMC server, if the connection to the Cisco IMC is established using a proxy server.

Adjusting the Object Discovery Interval

The discovery interval is the specified time interval for polling the details of Cisco IMC in a group. This section describes the steps required to change the polling intervals for the objects.

Lists details of the default discovery interval for the various Cisco IMC objects.

Table 1: Default Discovery Interval for Cisco IMC Objects

Serial Number	Object Name	Default Discovery Interval (in seconds)
1	IMC Server (Group) Discovery	14400
2	IMC Server Discovery	21600
3	IMC Chassis Discovery	21600
4	IMC Server Node Discovery	21600

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

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

Step 3 Navigate to **Authoring** > **Management Pack Templates** > **Cisco IMC**.

Step 4 In **Tasks** Pane of the **Management Pack Templates**, click **View Management Pack Objects** > **Object Discoveries**.

Step 5 Click **View Management Pack Objects** > **Object Discoveries**.

Step 6 On the **Object Discovery** page, right-click the object you want to modify.

Step 7 Select **Overrides** > **Override the Object Discovery** > **For all objects of class**.

Step 8 On the **Override Properties** page, do the following:

a) Check the **Override** check box in the Interval seconds parameter option.

b) Modify the **Override value**.

c) Click **Apply** and **OK**.

Note The IMC Server Discovery and IMC server Group (<Group Name>) Discovery interval values can be modified to any value. However, it is not recommended to have the interval values lower than 720 and 600 seconds for the IMC Server Discovery and IMC Group (<Group Name>) Discovery objects respectively.

Adjusting the Fault Polling Interval

The fault polling interval is used to poll the faults from the Cisco IMC.

The following table shows the default polling interval setting:

Rule Name	Polling Interval
Load Fault	720 seconds

Step 1 Go to the **Operations Manager** console, and click the**Go** tab.
Step 2 From the drop-down list, select **Authoring**.
Step 3 In the **Authoring** column, select **Authoring** > **Management Pack template** > **Cisco IMC**.
Step 4 Right-click the template pack and select **View Management Pack Objects** > **Rules**.
Step 5 On the **Rules** page, select the **Load Fault Rule**, and select **Overrides** > **Override the Rule** > **For All Objects of Class**.
Step 6 On the **Override Properties** page, do the following:

- Check the **Override** check box.
- Modify the value in the **Override Value** column.
- Click **OK**.

Viewing List of Rules in the Cisco IMC 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 IMC**.
Step 4 Right-click the Cisco IMC Group instance, and select **View Management Pack Objects** > **Rules**.

Remapping the Severity

This section describes how to modify the fault rule properties in the Cisco IMC.

The following table shows the default severity mapping between Cisco IMC and Operations Manager:

Cisco IMC	Operations Manager
Critical, Major	Critical
Minor, Warning	Warning

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 Cisco IMC.
Step 4 Right-click the Cisco IMC 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.

PreConfigure Rule

When all the Management Packs are imported, before Cisco IMC 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.

Clearing the Alerts

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

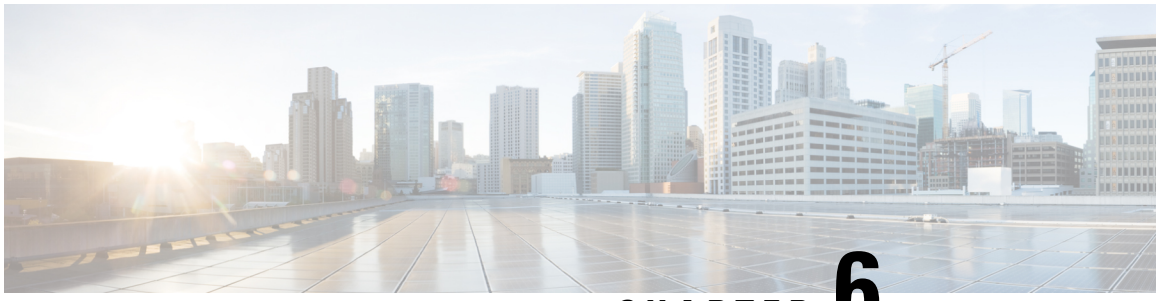
By, default, for every 90 seconds interval all alerts are cleared. However, you can modify the interval period.

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 queried. The default value is 120 seconds
- 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)



CHAPTER 6

PowerShell Cmdlets for Cisco IMC Management Pack

This chapter contains the following sections:

Overview of Cisco IMC PowerShell Cmdlets

Cisco IMC management pack supports the use of cmdlets which can be imported from a PowerShell module. These cmdlets are used to perform actions, such as adding a new Cisco IMC server group to the operations manager management group. Also, for updating an existing group or modifying existing rules for a Cisco IMC server group.

Importing Cmdlets from the PowerShell Module

Step 1 On the management server, go to **Windows PowerShell** > **Operations Manager Shell**.

Step 2 Run the **Import-Module CiscoImcScomPs** cmdlet to import the available cmdlets.

Step 3 You can view the list of available cmdlets by using the **Get-Command -Module CiscoImcScomPs** command.

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

Example

This example shows how to import and view the available cmdlets for Cisco IMC:

```
PS C:\Users\Administrator.MSCOM> import-module ciscoimcscomps
PS C:\Users\Administrator.MSCOM> get-command -module ciscoimcscomps
CommandType     Name                                               ModuleName
```

```
-----------     ----                                                ----------
Function        Add-ImcScomGroup                                    ciscoimcscomps
Function        Disable-ImcScomRule                                 ciscoimcscomps
Function        Enable-ImcScomRule                                  ciscoimcscomps
Function        Get-ImcScomRule                                     ciscoimcscomps
Function        Update-ImcScomGroup                                 ciscoimcscomps
Function        Update-ImcGroupScomAllInstances                     ciscoimcscomps
Function        Get-ImcGroupScomAllInstances                        ciscoimcscomps
PS C:\Users\Administrator.MSCOM>
```

Adding or Updating Cisco IMC Groups

Import the cmdlets available for the Cisco IMC management pack.

Cisco IMC group can have multiple IMC IP addresses using IP address range, subnet mask, or comma-separated values. You may specify the proxy details used to connect to the IMC. If the port is not specified, the default port 80 or 443 is used. You need not specify the Run-As-Account details if you want to manually create or assign it later.

1. On the management server, go to **the Windows PowerShell** console.
2. View the list of cmdlets that are available for use by using **Get-Command** . The cmdlet for viewing the available cmdlets for Cisco IMC is **Get- Command Add-ImcScomGroup**.
3. Enter the **Add-ImcScomGroup** cmdlet.
4. Get the parameters of the **Add-ImcScomGroup** cmdlet using the **Get-Help** command.

Syntax

```
Add-ImcScomGroup -GroupName <string>
-NetworkAddress <string> -SubnetMask <string>
-MachineType <string> {Agent Managed Computer
(Trusted Boundary) | Agent Managed Computer
(Untrusted Boundary) | Management Server |
Gateway Server} -MachineName <string>
-Run As Account <string> -RunAsCredential <pscredential>
[-GroupDescription <string>] [-NoSsl] [-Port <int>]
[-ExistingManagementPack <ManagementPack>]
[-ProxyHost <string>] [-ProxyPort <int>]
[-ProxyUsername <string>] [-ProxyPassword <string>]

Add-ImcScomGroup -GroupName <string>
-NetworkAddress <string> -SubnetMask <string>
-MachineType <string> {Agent Managed Computer
(Trusted Boundary) | Agent Managed Computer
(Untrusted Boundary) | Management Server |
Gateway Server} -MachineName <string>
[-GroupDescription <string>] [-NoSsl]
[-Port <int>] [-ExistingManagementPack
<ManagementPack>] [-ProxyHost <string>]
[-ProxyPort <int>] [-ProxyUsername <string>]
[-ProxyPassword <string>] [-ExistingRun As Account <string>]

Add-ImcScomGroup -GroupName <string>
-IpRangeStartAddress <string>
-IpRangeEndAddress <string> -MachineType <string>
{Agent Managed  Computer (Trusted Boundary) |
```

```
Agent Managed Computer (Untrusted Boundary) |
Management Server | Gateway Server}
-MachineName <string>  -Run As Account <string>
-RunAsCredential <pscredential>
[-GroupDescription <string>] [-ExcludeIpList <string>]
[-NoSsl] [-Port <int>]
 [-ExistingManagementPack <ManagementPack>]
[-ProxyHost <string>] [-ProxyPort <int>]
[-ProxyUsername <string>] [-ProxyPassword <string>]


 Add-ImcScomGroup -GroupName <string>
-IpRangeStartAddress <string> -IpRangeEndAddress
<string> -MachineType <string> {Agent Managed Computer
(Trusted Boundary) | Agent Managed Computer
(Untrusted Boundary) | Management Server |
Gateway Server} -MachineName <string>
[-GroupDescription <string>] [-ExcludeIpList <string>]
[-NoSsl] [-Port <int>] [-ExistingManagementPack
<ManagementPack>] [-ProxyHost <string>]
[-ProxyPort <int>] [-ProxyUsername <string>]
[-ProxyPassword <string>] [-ExistingRun As Account <string>]

Add-ImcScomGroup -GroupName <string>
-MultiIpAddressRange <string> -MachineType
<string> {Agent Managed Computer (Trusted Boundary) |
Agent Managed Computer (Untrusted Boundary) |
Management Server | Gateway Server} -MachineName <string>
-Run As Account <string> -RunAsCredential <pscredential>
[-GroupDescription <string>] [-ExcludeIpList <string>]
 [-NoSsl] [-Port <int>] [-ExistingManagementPack
<ManagementPack>] [-ProxyHost <string>] [-ProxyPort <int>]
 [-ProxyUsername <string>] [-ProxyPassword <string>]

 Add-ImcScomGroup -GroupName <string>
-MultiIpAddressRange <string>
-MachineType <string> {Agent Managed Computer
(Trusted Boundary) | Agent Managed Computer
(Untrusted Boundary) | Management Server |
Gateway Server} -MachineName <string>
[-GroupDescription <string>] [-ExcludeIpList
<string>] [-NoSsl] [-Port <int>]
[-ExistingManagementPack <ManagementPack>]
[-ProxyHost <string>] [-ProxyPort <int>]
[-ProxyUsername <string>] [-ProxyPassword <string>]
[-ExistingRun As Account <string>]
```

Enter the following parameters:

- GroupName – Name of the IMC Group
- MachineName – FQDN of the machine on which the IMC group is registered

  All scripts related to the IMC group management pack run on this machine.
- (Optional) GroupDescription – Description of the IMC group management pack
- NetworkAddress – Network address to be used with the subnet mask
- SubnetMask – Subnet mask specifying the IMC servers to consider. For example, 255.255.255.128
- IpRangeStartAddress – The first IP address in the IMC server block
- IpRangeEndAddress – The last IP address in the IMC server block

- ExcludeIpList – Comma-separated list of IP addresses to be excluded
- MultiIpAddressRange – Comma-separated list of IP addresses or IP address ranges. For example, 192.168.1.1,192.168.1.10 to 192.168.1.30,192.168.1.45
- NoSsI – Switch parameter to specify nonsecure (HTTP) connectivity with IMC
- Port – Optional port to connect to Cisco IMC. If not specified, default port (80/443) is used
- ProxyHost – IP address or hostname of the proxy server to be used for communicating to IMC
- ProxyPort – Port for the proxy server
- ProxyUsername – Proxy server username
- ProxyPassword – Proxy server password
- ExistingRunAsAccount – Name of the existing RunAs account for the IMC group
- RunAsAccount – Name of the new RunAs account for the IMC group
- RunAsCredential – Credentials for IMC to create a new RunAs account

Update-ImcScomGroup

Update-ImcScomGroup cmdlet, updates the required properties for an existing IMC group. You can specify the new values for any parameter or parameters you want to modify. For the parameters which are not specified, existing values are used.

Syntax

```
Update-ImcScomGroup -GroupName <string>
[-GroupDescription <string>] [-ExcludeIpList <string>] [-Secure <bool>] [-Port
<int>][-MachineType <string>
{Agent Managed Computer (Trusted Boundary) | Agent Managed Computer (Untrusted Boundary) |

Management Server |Gateway Server}]
[-MachineName <string>] [-ProxyHost
<string>] [-ProxyPort <int>] [-ProxyUsername <string>]
 [-ProxyPassword <string>]

Update-ImcScomGroup -GroupName <string>
-NetworkAddress <string> -SubnetMask <string>
[-GroupDescription <string>] [-ExcludeIpList<string>]
[-Secure <bool>] [-Port <int>] [-MachineType <string>
{Agent Managed Computer (Trusted Boundary) |
Agent Managed Computer(Untrusted Boundary) |
Management Server | Gateway Server}] [-MachineName <string>]
 [-ProxyHost <string>] [-ProxyPort <int>]
[-ProxyUsername <string>] [-ProxyPassword <string>]


Update-ImcScomGroup -GroupName <string>
-IpRangeStartAddress <string> -IpRangeEndAddress <string>
[-GroupDescription <string>][-ExcludeIpList <string>]
[-Secure <bool>] [-Port <int>] [-MachineType <string>
 {Agent Managed Computer (Trusted Boundary) |
AgentManaged Computer (Untrusted Boundary) | Management Server |
Gateway Server}] [-MachineName <string>] [-ProxyHost <string>]
 [-ProxyPort<int>] [-ProxyUsername <string>] [-ProxyPassword <string>]
```

```
Update-ImcScomGroup -GroupName <string>
-MultiIpAddressRange <string> [-GroupDescription
<string>] [-ExcludeIpList <string>] [-Secure<bool>]
[-Port <int>] [-MachineType <string>
{Agent Managed Computer (Trusted Boundary) |
Agent Managed Computer (Untrusted Boundary)|
Management Server | Gateway Server}]
[-MachineName <string>] [-ProxyHost <string>]
[-ProxyPort <int>] [-ProxyUsername <string>][-ProxyPassword <string>]
```

Enter the following parameters:

- GroupName – Name of the IMC group to be updated
- MachineName – FQDN of new machine, all scripts related to this IMC Group MP runs on this machine)
- GroupDescription – New description string for this IMC Group MP
- NetworkAddress – Network address to be used with the subnet mask
- SubnetMask – Subnet mask specifying the IMC servers to consider. For example, 255.255.255.128
- IpRangeStartAddress – First IP address from the IP address range for IMC servers
- IpRangeEndAddress – Last IP address from IP address range for IMC servers
- ExcludeIpList – Comma-separated list of IP addresses not to be included
- MultiIpAddressRange – Comma-separated list of IP addresses or IP address ranges. For example,192.168.1.1,192.168.1.10-192.168.1.30,192.168.1.45
- Secure – Boolean value to either set or reset the secure connection option
- Port – New port number to be used.
- ProxyHost – IP address or hostname of the new proxy server to be used for communicating with IMC
- ProxyPort – New port number for the proxy server
- ProxyUsername – New username for the Proxy server
- ProxyPassword – New password for the Proxy server

Get-ImcScomRule

```
Get-ImcScomRule [[-Class] <string[]>] [[-FaultCode] <string[]>]  [<CommonParameters>]
```

Get-ImcGroupScomAllInstances

```
Get-ImcGroupScomAllInstances
[available in MP v4.1.5]
```

Update-ImcGroupScomAllInstances

```
Update-ImcGroupScomAllInstances
```

Enable-ImcScomRule

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

```
Enable-ImcScomRule [-Rule] <ManagementPackRule[]>
 [-ManagementPackName] <string>
```

Disable-ImcScomRule

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

```
Disable-ImcScomRule [-Rule] <ManagementPackRule[]>
 [-ManagementPackName] <string>
```