Cisco Integrated Management Controller (IMC) Integration Pack User Guide, Release 1.1

For Microsoft System Center 2012, Configuration Manager
March 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

Cisco Integrated Management Controller (IMC) Integration Pack User Guide, Release 1.1

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:

Convention	Indication
bold font	Commands and 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.
[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 marks 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 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, but 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

Cisco UCS Communities

Cisco UCS Communities is a platform to discuss, share and learn about the Cisco UCS products and technologies. For blogs, discussion forums and documents related to UCS integrations with partner ecosystem, visit https://communities.cisco.com/ucsintegrations.

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: Cisco UCS B-Series Servers Documentation Roadmap

For a complete list of all C-Series documentation, see the *Cisco IMC Servers Documentation Roadmap* available at the following URL: *Cisco UCS C-Series and Cisco C880 Series Documentation Roadmap*.

For a complete list of all E-Series documentation, see the *Cisco IMC Servers Documentation Roadmap* available at the following URL: Documentation Guide for Cisco UCS E-Series Servers

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163andflowid=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

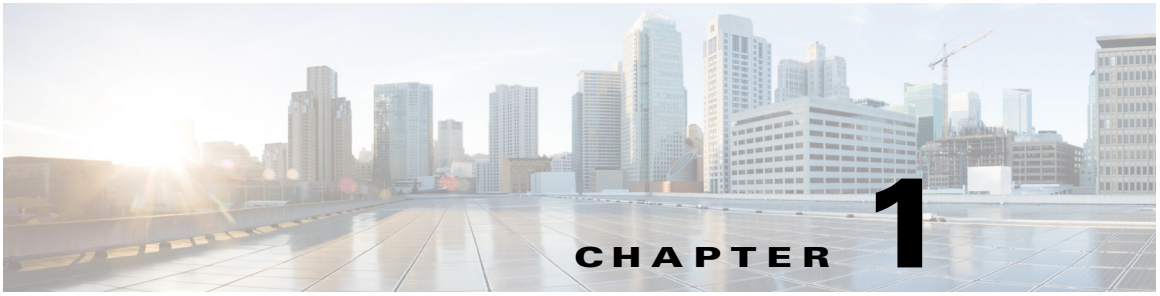
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

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: http://www.cisco.com/en/US/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.

CONTENTS



Overview

This chapter includes the following sections:

About the Cisco IMC Integration Pack

The **Cisco IMC Integration Pack** installs as a plug-in to System Center 2012 Configuration Manager. The plugin, simplifies the server management task like hardware configuration, firmware update, OS installation, and driver management process of Cisco Integrated Management Controller (IMC) for Cisco UCS C-series and E-series servers. With the **Cisco IMC Integration Pack** installed, you can do the following:

- Power Policy Configuration—Configures multiple power profiles for power capping feature
- Import Cisco IMC servers based on Cisco IMC IPs into Configuration Manager.
- Download drivers and create driver packages for the Cisco IMC servers that are required for OS deployment from the **Configuration Manager Console**.
- See an overview of hardware inventory, including CPUs, memory, power supplies, and storage.
- Configure RAID using the Array Builder wizard.
- BIOS configuration—Configures BIOS attributes and boot order settings of the server in both legacy and precision boot order mode.
- Cisco IMC Configuration—Ability to configure Cisco IMC Admin settings like Network, SNMP, local users, LDAP, and communication settings.
- page Configuration—Ability to configure page settings like vNICs, vHBAs, VMFEX.

Note page Configuration is supported only on C-series servers.

- Configuration Pools—Ability to create, edit, and delete configuration pools for MAC, IP, WWPN, and WWNN addresses.
- Download and perform firmware updates using the Host Upgrade Utility (HUU).

- Automatic boot to Preboot Execution Environment (PXE) or network boot using ISO mapping.
- Launch KVM Console—The KVM Console of the server.
- Launch the Cisco IMC web user interface (UI).

Components of the Cisco IMC Integration Pack

The Cisco IMC Integration Pack includes the following utilities:

- Launch the KVM console
- Launch the Cisco Integrated Management Controller web UI
- Import IMC Servers Wizard—Imports Cisco IMC Servers into Configuration Manager.
- Create Cisco UCS C-Series Server Driver Package Wizard—Imports the necessary driver packages that are required during the operating system deployment.
- Cisco IMC Configuration Profile Manager—Creates server configuration profiles such as RAID configuration, BIOS configuration, Cisco IMC admin configuration, page configuration, and firmware update profiles.
- Cisco IMC Server Configuration Manager—Performs server configuration and management tasks, such as Firmware Update, RAID Configuration, BIOS Configuration, page Configuration, Cisco IMC Admin Configuration, Operating System Deployment, and Viewing Hardware Inventory on a single server or a group of servers.
- Cisco IMC Task Manager—Allows you to view the status of the tasks and perform actions on it.

End to End Scenario

Atypical deployment scenario includes importing a server, driver packages, updating firmware, configuring hardware, and deploying an operating system on the server. This sample scenario includes the following tasks:

1. Installing the **Installing Cisco UCS Integration Pack Suite.** For more information, see Installing Cisco UCS Integration Pack Suite.
2. Importing driver packages in the **Configuration Manager Console** and assigning the servers to a collection. For more information, see Importing Driver packages.
3. Importing driver packages of the Cisco IMC servers into the **Configuration Manager Console**.
4. Creating a custom task sequence or editing an existing task sequence to support the deployment of operating systems. For more information, see Creating and Editing Task Sequences.
5. Update Firmware, Configure Hardware and Install an Operating System on th server through Task Sequence. For more information, see Cisco IMC Configuration Profile Manager, page 2-6 and Cisco IMC Configuration Manager, page 2-20.

Software Requirements

- .NET Framework 4.5 or higher
- Java Version 1.6 Update 45 or higher

- Following version of System Center 2012 Configuration Manager Primary Site or Admin Console Installations:
  - System Center 2012 Configuration Manager
  - System Center 2012 Configuration Manager SP1
  - System Center 2012 R2 Configuration Manager
  - System Center 2012 R2 SP1 Configuration Manager
  - System Center 2012 Configuration Manager SP2

Supported Operating Systems and Versions

The **Cisco IMC Integration Pack** supports the following operating systems:

- Microsoft Windows Server 2012 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)

Note Install the latest patch of the operating systems.

Supported Hardware Platforms

The **Cisco IMC Integration Pack** is supported on the following hardware platforms:

Supported C-Series Servers

- Cisco UCS C220 M4 Server
- Cisco UCS C240 M4 Server
- Cisco UCS C460 M4 Server
- Cisco UCS C22 M3 Server
- Cisco UCS C24 M3 Server
- Cisco UCS C220 M3 Series Server
- Cisco UCS C240 M3 Series Server
- Cisco UCS C260 M2 Server
- Cisco UCS C420 M3 Server
- Cisco UCS C460 M2 Server

Supported E-Series Servers

- Cisco UCS E160D-M1/K9
- Cisco UCS E160DP-M1/K9
- Cisco UCS E140D-M1/K9
- Cisco UCS E140S-M1/K9

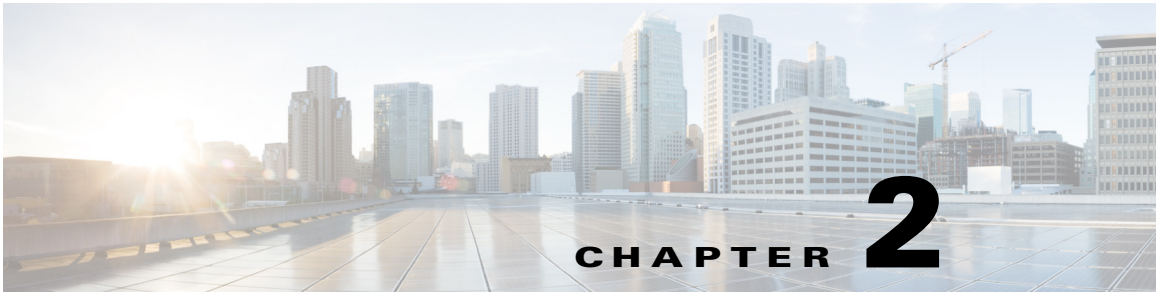
Supported Cisco IMC Version

The Cisco IMC Integration Pack is compatible with Cisco Integrated Management Controller (IMC) 1.5(2) or higher for C-Series servers and 2.3(x) and higher for E-Series servers.

Cisco IMC 1.5(1) supports the following features:

- Import Cisco Servers
- Import Driver Packages
- RAID Configuration
- OS Deployment

Note Configuring BIOS on Cisco UCS C-series servers requires Cisco IMC version of 1.5(4) or higher.



Working with Configuration Manager Console

This chapter includes the following sections:

Importing IMC Servers

Note The icon links on the ribbon bar of **Microsoft Configuration Manager Console** are product sensitive. It displays when a particular pack is installed. For example, you can see the **Cisco IMC Configuration** icon link when the **Cisco IMC Integration Pack** is successfully installed.

Step 1 Navigate to **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console** to launch **Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 Select **Assets and Compliance > Overview > Devices**.

The installed servers are displayed in the content pane.

Step 3 Right-click **Devices**, select **Cisco IMC Configuration > Import Cisco IMC Servers**.

The **Import Cisco IMC Servers Wizard** displays which allows you to import Cisco IMC servers only in the **Microsoft Configuration Manager Console**.

Step 4 In the **Enter Cisco IMC Address Input**, you can import the servers by selecting one of the following options:

- **IP Address combination** — Specify multiple hyphen separated IP addresses for range, and multiple single IP Address. Use comma to separate all the IP addresses. For example, 10.105.219.15-10.105.219.129,10.104.200.35,10.104.100.133,10.106.233.136-10.106.233.200.
- **IP Address range** — Specify the range of Cisco IMC IP address in the **Start** and **End** fields.

- **Select an IP Address CSV file** — Click **Browse**, and navigate to the network path where the CSV file is located. The CSV file must contain IP addresses separated by a comma. For example, 10.106.233.167,10.106.233.165, 10.104.255.248, 10.104.255.242,10.104.255.228.
- **Subnet mask** — Specify the network address and subnet mask.

Step 5 In the **CIMC connection parameters**, enter a valid username and password for Cisco IMC.

Step 6 Click **Next**.

In the **CIMC Authentication Progress**, the username and password is verified for the IP addresses provided.

Monitor the **Status Message** column.

Step 7 Click **Next**.

The list of servers that can be imported are displayed in **Select Servers**.

Step 8 Check the servers you want to import. Or, you can check the **Select All** check box to import all the servers.

Step 9 Click **Import Servers**.

Step 10 Once teh server import is successful, a confirmation message appears.

Step 11 You can verify whether the servers are imported successfully in the **Microsoft Configuration Manager Console** using one of the following ways:

a. Navigate to **Assets and Compliance > Overview > Devices**.

The **Device catalog** is refreshed and the imported servers are shown in the content pane.

b. Navigate to **Assets and Compliance > Overview > Devices Collections**.

The **Device Collections** catalog is refreshed. The *Cisco Collections* groups are automatically created, and are shown in the **Content Pane**. The groups created are:

- All Cisco IMC Servers.
- All Cisco UCS <*model*> Servers, where <*model*> is the type of Cisco IMC servers. For example, C240, C260 and so on.

c. To view all the devices listed in each device collection group, right-click the device collection group and select **Update Membership**.

Note When you select **Update Membership** on **All Cisco IMC Servers**, and then on the **Model Specific** groups refresh process is fastened.

The device collection group refreshes and displays the devices which are part of the device collection group.

Step 12 To view the properties of each device, follow these steps:

a. Right-click the device in the **Name column** and select **Properties.**

The **Device Properties** page displays.

b. Click the **Cisco IMC Information** tab to view the properties of the selected device.

Creating and Editing Task Sequences

You create task sequences to support the deployment of operating systems. Add or edit the following task sequence steps to a task sequence while creating a custom task sequence or while editing an existing task sequence to help ease the deployment of operating systems:

- Format and Partition Disk
- Apply Operating System Image
- Apply Network Settings
- Apply Windows Settings
- Apply Driver package
- Setup Windows and ConfigMgr

Creating a Custom Task Sequence

Step 1 From the left pane of the **Configuration Manager** console, select **Software Library > Overview > Operating Systems > Task Sequence** catalog.

Step 2 Right-click on the **Task Sequence** catalog and select **Create Task Sequence**.

The **Create Task Sequence Wizard** displays.

Step 3 In the **Create Task Sequence Wizard**, select **Create a new custom task sequence**, and click **Next**.

Step 4 In the **Specify task Sequence information**, complete the following fields:

- **Task sequence name**—Enter a name for the task sequence
- **Description**—Enter a brief description about the task sequence
- **Boot image**—Click **Browse**, to select the boot image from the **Select a Boot Image** screen and click **OK**.

Step 5 Click **Next**.

Step 6 In **Summary**, review the settings and click **Next.**

If you want to modify the settings, click **Previous**.

Step 7 Once the task sequence is created, click **Close** to exit the **Create Task Sequence** wizard.

You can view the task sequence in the **Name** column of the content pane.

Editing a Task Sequence

Step 1 From the left pane of **Microsoft Configuration Manager Console**, select **Software Library > Overview > Operating Systems > Task Sequences** catalog.

The task sequences are listed in the content pane.

Step 2 Right-click the task sequence, and select **Edit**.

The **Task Sequence Editor** page displays.

Step 3 From the drop-down list, select **Add > Disks > Format and Partition Disk**.

The **Format and Partition Disk** item is flagged with the a red X check mark.

Step 4 On the **Properties** tab, complete the following fields:

- **Name**—Enter a name for the task to be performed
- **Description**—Enter brief description for the task to be performed
- **Volume**—Create a new partition.

  To create a new partition, follow these steps:

  a. In the **Volume** area, click the  icon.

  The **Partition Properties** page displays.

  b. Enter a name for the partition and check the **Make this the boot partition** check box.

  c. Check the **Quick format** check box.
- **Variable**—Enter a name for the environment variable for the logical drive. For example, OSDRIVE.

Step 5 Click **OK**.

The **Format and Partition Disk** task sequence is now flagged with a green check mark.

Step 6 From the drop-down list of the **Task Sequence Editor**, select **Add> Images > Apply Operating System Image**.

The **Apply Operating System Image** item is flagged with the a red X check mark.

Step 7 In the left pane of the **Task Sequence Editor**, click on **Apply Operating System Image** which is flagged with a red X check mark.

Step 8 On the **Properties** tab, complete the following fields:

- **Name**—Enter a name for the task to be performed
- **Description**—Enter a description for the task to be performed
- **Apply operating system from a captured image**—Click **Browse** to open the **Select an Operating System Image** dialog box. Select the existing image package you want to install.

  If multiple images are associated with the specified **Image package**, use the drop-down list to specify the associated image to be used for this deployment.
- From the **Destination** drop-down list, select **Logical drive letter stores in a variable** and enter the variable name created in the **Format and Partition Disk** step. For example, OSDRIVE.

Note See, Technet documentation for importing **Operating System Images into Configuration Manager**.

Step 9 Click **OK**.

The **Apply Operating System Image** task sequence is now flagged with a green check mark.

Step 10 From the drop-down list of the **Task Sequence Editor**, select **Add> Settings > Apply Network Settings**.

The **Apply Network Settings** item is flagged with the a red X check mark.

Step 11 Click **Apply Network Settings** which is flagged with a red X check mark.

Step 12 On the **Properties** tab, complete the following fields:

- **Name**—Enter a name for the task to be performed
- **Description**—Enter a description for the task to be performed

- **Join a workgroup**—Select this option to join the destination computer with the specified workgroup. Enter the name in the **Workgroup** field. This value can be overridden by the value that in the Capture Network Settings task sequence step.
- **Join a domain** — Select this option to have the destination computer join the specified domain.
- **Account** — Click **Set** to specify an account with the necessary permissions to join the computer to the domain.
- **Adapter settings** — Specify network configurations for each network adapter in the computer. Click **New** to open the **Network Settings** dialog box, and then specify the network settings.

Step 13 Click **OK**.

The **Apply Network Settings** task sequence is now flagged with a green check mark.

Step 14 In the left pane of **Task Sequence Editor**, select **Add> Settings > Apply Windows Settings**.

The **Apply Windows Settings** item is flagged with the a red X check mark.

Step 15 In the left pane of the **Task Sequence Editor**, click on **Apply Windows Settings** which is flagged with a red X check mark.

Step 16 In the right pane of the **Task Sequence Editor**, under **Properties,** enter information for the following:

- **Name** — Enter short user defined name that describes the action taken in this step.
- **Description** — Enter a more detailed information about the action taken in this step.
- **User name** — Specify the registered user name that is associated with the destination computer.
- **Organization name** — Specify the registered organization name that is associated with the destination computer.
- **Product key** — Specify the product key that is used for the Windows installation on the destination computer.
- Select the radio button for **Enable the account and specify the local administrator password**. This lets you to have an alternate account for logging in with the local administrator password.
- **Time Zone** — Specify the time zone to configure on the destination computer.

Step 17 Click **OK**.

The **Apply Windows Settings** task sequence is now flagged with a green check mark.

Step 18 In the left pane of **Task Sequence Editor**, select **Add> Drivers > Apply Driver Package**.

The **Apply Driver Package** item is flagged with the a red X check mark.

Step 19 In the left pane of the **Task Sequence Editor**, click on **Apply Driver Package** which is flagged with a red X check mark.

Step 20 In the right pane of the **Task Sequence Editor**, under **Properties**, click **Browse** next to the **Driver Package** box and select the driver package that was created using the **Create UCS C-Series Driver Package Wizard**.

Step 21 Click **OK**.

The **Apply Driver Package** task sequence is now flagged with a green check mark.

Note The package contains all the drivers to be made available during operating system deployment.

Step 22 In the left pane of **Task Sequence Editor**, select **Add> Images > Setup Windows and ConfigMgr**.

The **Setup Windows and ConfigMgr** item is flagged with the a red X check mark.

Step 23 In the left pane of the **Task Sequence Editor**, click on **Setup Windows and ConfigMgr** which is flagged with a red X check mark.

Step 24 In the right pane of the **Task Sequence Editor**, under **Properties**, click **Browse** next to the **Package** box.

The **Select the Deployment Package** page displays.

Step 25 In the **Select the Deployment Package** page, under **Deployment packages**, select the required deployment package.

Note Refer to **Microsoft Technet** documentation on details for **Creating a Deployment Package**.

Step 26 Click **OK**.

The **Setup Windows and ConfigMgr** task sequence is now flagged with a green check mark.

Step 27 Click **Apply**.

Cisco IMC Configuration Profile Manager

Cisco IMC Configuration Profile Manager helps user in creating various configuration profiles such as BIOS, RAID, Firmware Update, Cisco IMC Admin, VIC Adapter. You can launch the Profile Manager by selecting a valid Cisco IMC server discovered in the Configuration Manager. You can either create a profile newly from scratch or get the settings from the system and use it. Creation of profile from a reference system is supported only for BIOS, IMC Admin and VIC Adapter configuration profiles.

Creating a RAID Profile Using Array Builder

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**. The **Cisco IMC Configuration Profiles Manager** window displays.

Step 2 Click the  icon to launch the new profile dialog box.

The **Create new profile** dialog box displays.

Step 3 From the **Profile Type** drop-down list, select **RAID**.

Step 4 Click **OK**.

A default embedded controller is created.

Step 5 Enter the configuration rule name in the **Configuration rule** name field.

Step 6 Select the **Error handling rule** from the drop-down menu. You can choose from:

- **Fail the task if any controller does not match a configuration rule** — Reports a failure if any of the detected controllers are not able to be configured by a rule.
- **Fail the task only if the first controller does not match a configuration rule** — Reports a failure if the first controller detected (usually the embedded controller) cannot be configured by a rule.
- **Fail the task only if none of the array controllers match a configuration rule** — Reports a failure only if all of the controllers in the system fail to match a rule; in other words, none of the controllers are configured. This rule also fails if a controller does not have sufficient disks to configure a RAID.

Step 7 You can:

a. Add new controllers and define rules for them, or edit the default controller and define the rules. For more information, see Controllers, page 2-7.

b. Add or edit variable conditions for the default controller or the controller that you add. For more information, see Variable Conditions, page 2-8.

c. Create new arrays from a variable condition, if required. For more information, see Arrays, page 2-9.

Step 8 Click **Save** to save the RAID profile.

Using the Array Builder

The Array Builder allows you to define arrays and disk sets with all available RAID settings, logical drives or virtual disks of varying sizes or use all available space, and assign hot spares to individual arrays or assign global hot spares to the controller.

When you run the task sequence on a target server, the array configuration utility detects the existing controllers in the system as well as the disks attached to each controller. The custom action then tries to match the physical configurations it detected to the logical configurations you defined in the configuration rules. These array configuration rules are defined using a graphical, logical layout that helps you visualize how your array controllers are configured. Rules are processed in the order displayed in the tree, so you know exactly which rules have priority.

Defining Rules With Array Builder

You can define rules to match configurations based on the following:

- Detected slot number that the controller is in or just the embedded controller, if any.
- Number of disks that are attached to the controller.
- Apply a blanket configuration to any controller that Array Builder finds.

Note You can define different configuration to different servers even if the detected hardware is identical by applying configuration rules based on the RAID profiles detected on the server.

Array Builder elements and associated rules

Controllers

When a controller is created, a default variable condition, array and disk(s) are created to ensure a valid configuration. You can choose to leave the controller un-configured with disks set to non-RAID, or you can add arrays or perform other actions.

Controller elements contain variable condition elements. Controllers can be one of several configuration types:

- The embedded controller
- A controller in slot “X”

- Any controller with “X” disks
- Any controller with “X” disks or more
- All remaining controllers

Adding A Controller

Step 1 Select a controller from the list, or select an embedded controller. The **Controllers** drop-down menu is enabled.

Step 2 Click **Controllers > New Controller**. The **Controller Configuration** window displays.

Step 3 Under **Controller Selection Criteria**, select from the following options:

- Select the controller located in slot — Enter the slot number of the controller.
- Select any controller with <exactly, atleast> <number of> disks attached — Set a rule to select any controller which matches exactly, or at least the number of disks you have selected.
- Select all remaining controllers in the system regardless of configuration

Step 4 Under **Variable Matching Criteria**, you can set a rule to apply this configuration only if it matches certain criteria that you select. Select **Apply this configuration** only when the variable to enable the rule matches certain criteria that you select.

Step 5 Click **OK**.

Editing A Controller

Select the controller and click **Controllers > Edit Controller**. The **Controller Configuration** window displays where you can make changes to the controller.

Deleting A Controller

Step 1 Select the controller and click **Controllers > Delete Controller**. A warning informing that all the attached arrays and disks will be deleted displays.

Step 2 Click **Yes** to delete or **No** to cancel.

Note At least one controller is required on the server. If there is only one controller and you delete it, a message that the default controller was inserted because the last controller was deleted displays.

Variable Conditions

To provide the ability to use the same RAID configuration in multiple logical configurations, variable evaluation is provided so that a different configuration for arrays and logical drives can be applied to different situations. To provide the ability to use the same hardware configuration in multiple logical configurations, variable evaluation is provided so that a different configuration for arrays and logical drives can be applied to different situations. Variable condition elements contain arrays and global hot spares, and are of two types:

- No variables defined: This is the default configuration inserted with every controller, and cannot be removed or moved from last in the order.

- Variables defined: This is where any variable is compared to a value using one of the pre-defined operators.

Adding A New Variable Condition

Step 1 Under an embedded controller, expand **Embedded Controller**, and choose **[No variable conditions defined]**.

Step 2 Click **Variables > New Variable Condition**. The **Variable Condition Configuration** window displays.

Step 3 Under **Variable Matching Criteria**, you can set a rule to apply this variable only if it matches certain criteria that you select.

Step 4 Click **OK** to apply the variable condition, or **Cancel** to return to the **Array Builder**.

Note If you define a variable condition, then the same condition has to be defined on the particular server to enable and apply the variable condition. This can be done by right-clicking the server and defining the variable from the variables tab.

Editing A Variable Condition

Step 1 Select the variable condition and click **Variables > Edit Variable Condition**. The **Variable Condition Configuration** window displays, where you can make changes to your variable condition.

Step 2 Click **OK** to apply the variable condition, or **Cancel** to return to **Array Builder**.

Deleting a Variable Condition

Step 1 Select the variable condition and click **Variables > Delete Variable Condition**. A message that all the attached arrays and disks will be deleted displays.

Step 2 Click **Yes** to delete or **No** to cancel.

Arrays

Array nodes include both RAID arrays and non-RAID disk groups that are indicated by the different icons. By default, a non-RAID disk group is created when a controller is created. If the controller configuration specifies the number of disks required, the same number of disks is added to the non-RAID group.

Arrays can be added, modified, or deleted depending on the controller configuration and number of disks available. Array elements contain logical drives and physical disks.

Adding A New Array

Step 1 Under a variable condition, select a variable condition and click **Arrays > New Array**. The **Array Settings** window displays.

Step 2 Set the required RAID level from the **Desired RAID Level** drop-down list.

Step 3 To set the **Boot Drive** check the given check-box.

Step 4 Click **OK** to apply the array, or **Cancel** to return to **Array Builder**.

Editing An Array

Step 1 Select the array and click **Arrays > Edit Array**. The **Array Settings** window displays. You can edit the array by selecting a different RAID level for the array.

Step 2 Click **OK** to apply the changes, or **Cancel** to return to **Array Builder**.

Deleting An Array

Step 1 Select the array and click **Arrays > Delete Array**. A message that all the attached disks will be deleted displays.

Step 2 Click **Yes** to delete or **No** to cancel.

Firmware Update Profile

You can perform firmware update on single systems or group of systems by creating a firmware update profile. Host Upgrade Utility (HUU) is used to perform firmware update on the system. You have an option to download the HUU image from either cisco.com from the utility or if you have already downloaded the HUU you can provide the same details as part of firmware update profile.

Creating a Firmware Update Profile Using Configuration Profile Manager

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**. The **Cisco IMC Configuration Profile Manager** window displays.

Step 2 Click the  icon to create a new firmware update profile.

The **Create new profile** dialog box displays.

Step 3 From the **Profile Type** drop-down list, select **Firmware Update**.

Step 4 Click **OK**.

The **Select Host Update Utility** screen displays.

Step 5 Under **Select Host Update Utility**, create a firmware update profile by selecting one of the following radio buttons:

a. **Specify HUU source** — Select **Download HUU from Cisco.com** radio button if you want to download the ISO from Cisco.com

Note For M4 servers, download the HUU manually from Cisco.com and then go to option **b**.

- Click **Download Details**.

  The **Download Details** screen displays.
- Enter the following download details:
  - Under **Select a platform**, select the server.
  - Under the **Credentials for Cisco.com**, enter your Cisco.com username and password in the respective fields.

Note Provide the proxy server details only if you have a proxy connection setup to access the server.

  - Under the **Proxy Server**, select **Enable Proxy Configuration** and **Enable Proxy Authentication**.
  - Enter the proxy configuration details and the proxy authentication details in the respective sections.
  - Click **OK**.

  If the credentials are valid the UI will display all the available HUU versions for download. Select a HUU version from the drop down list.
  - In the **Path** field, click **Browse** and navigate to the path where HUU must be downloaded to a network location and not local path.
  - In the **Username** filed, enter the username of the share in the username@domainname format.
  - In the **Password** filed, enter the password of the share.
- Click **Next** to save the firmware update profile.

  If **Download** option is selected it will start the download process and displays the progress. After the download is complete click **Customize** option to update the firmware from the given list. Cisco recommends that you update all the firmware that are supported by the server. To update all the firmware, click **Select All**. Enter a name for the profile and click **Save Profile** option to save the profile.

Note You cannot update BIOS and Cisco IMC independently, and they must be on the same version.

b. **Select HUU from local share** — Select this radio button, if you have already downloaded the HUU and it is available in a share

- Click **Browse** and navigate to the path where the HUU is present.
- Select the HUU and click **OK**.
- In the **Path** filed, click **Browse** and navigate to the path where HUU is present.
- In the **Username** filed, enter the username of the share. Username is provided in the format username@domainname, for example Administrator@SCCM.cisco.com
- In the **Password** filed, enter the password of the share.
- Click **Next**.
- Enter name for the profile.

- Click **Customize** to select the firmware to be updated.

Note It is recommended that you select **All** components for update.

Note Cisco IMC and BIOS cannot be update independently. They should always be on the same version.

- Click **Save Profile** to save the firmware update profile.

Configuring BIOS Profile

You can use BIOS configuration profile to apply the BIOS settings to a single system or to a group of systems. You have the option to configure BIOS settings connected to Processor, Memory, Serial configuration, PCI and LOM settings, Server Management, Onboard Storage, USB configurations and Boot order related settings from the BIOS profile. As part of the Hardware Provisioning and OS Deployment Workflow, you can select the BIOS Profiles and the same settings are applied. Also you can apply BIOS configuration separately.

Creating a BIOS Profile Using Profile Manager

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**. The **Cisco IMC Configuration Profiles Manager** window displays.

Step 2 Click the icon to create a new BIOS Profile.

Step 3 **Create new profile** dialog box displays. From the **Profile Type** drop-down list, select **BIOS**.

Step 4 You can create a new BIOS profile by choosing **Create new profile** or **Create profile from the current configuration of the server** option.

Note If you choose the Create profile from the current configuration of server option, the application retrieves the current settings from the server. This might take a while.

Step 5 Click **OK**.

Step 6 In the **Profile Name** field, enter a name for the profile.

Step 7 In the **IMC Server Configuration Profile Manager** window, update the following areas:

- Main
- Processor Configuration
- Memory and Serial Configuration
- LOM and PCC Configuration
- Server Management
- Boot Order

To configure the boot order, follow these steps:

a. Select **Legacy Boot Order** or **Precision Boot Order**.

Note You can choose precision boot order only for C-Series servers with version 2.0(1) and above. You can also apply legacy boot order to the servers on versions 2.0(1) and above, however you cannot apply precision boot order to servers on any version prior to 2.0(1).

b. If you have chosen **Legacy Boot Order,** from the **Device Order** area, select the device that you want to configure.

c. If you have chosen **Precision Boot Order,** from the **Add Boot Device** area, click on a boot device from the list and populate the field in the add device pop-up window.

d. Click **Add** button. The device gets listed in the **Configure Boot Order** area.

e. Follow **Step 1** and **Step 2** to add other devices.

Note To remove the device from the list, select **Remove** button. Also, you can change the order of the devices by selecting **Move Up** or **Move Down** button. You also can modify the device details by clicking the **Modify** button.

Note To update these areas, see BIOS Parameters by Server Model for the C-Series servers, and E-Series documentation for the E-Series servers.

Step 8 Click **Save Profile** to save the profile in the database.

If you select **Reset to Defaults,** by default **platform-default** is set for all the parameters.

Configuring Cisco IMC Admin Profile

You can use Cisco IMC Admin profile to apply the Cisco IMC settings to a single system or to a group of systems. You have the option to configure Cisco IMC Admin settings like network, SNMP, local users, LDAP and communication settings. As part of the hardware provisioning and OS deployment workflow, you can select the Cisco IMC Admin profile and the same settings are applied. Also you can apply Cisco IMC Admin profile separately.

You can launch the Profile Manager by selecting a valid Cisco IMC discovered in the Configuration Manager.It is used to configure Cisco IMC Settings like Network Settings, Communication Services, SNMP Settings, adding Local Cisco IMC Users, LDAP Settings and Logging controls.

Creating Cisco IMC Profile Admin Profile

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**. The **Cisco IMC Configuration Profiles Manager** window displays.

Step 2 Click the icon to create a new Cisco IMC Profile.

Step 3 The **Create new profile** dialog box displays.From the **Profile Type** drop-down list, select **Cisco IMC Admin Configuration**.

Step 4 You can create a new profile by using either **Create a new profile** or **Create profile from current configuration of the server** option. Choose the option through which you want to create a new Cisco IMC profile.

Step 5 Click **OK**.

Step 6 In the **Profile Name** field, enter a name for the profile.

Step 7 In the **Cisco IMC Server Configuration Profile Manager** window, update the following areas:

Note To modify the properties of the following configuration settings, you must enable the parameter that you want to edit.

- **Network Settings**

  For more information, see:

  - Connecting to a Port Profile
  - Configuring NTP Settings
  - Configuring Network Security
    - Configure IP Address
- **Communication Service**

  For more information, see:

  - Configuring SSH
  - Configuring IPMI over LAN
  - Configuring the Virtual KVM
- **SNMP Setting**

  For more information, see Configuring SNMP Properties
- **Local Users**

  For more information, see Configuring Local User

  Note When you create a profile by using **Current configuration of the server** option, passwords are not retrieved. If you want to successfully apply this profile settings on different server, you need to enter the password manually. This is applicable for Local Users, SNMP user with passwords.
- **LDAP**
- **LDAP Group Authorization**

  For more information, see LDAP Servers

- **Logging Controls**

  For more information, see Logging Controls

Step 8 Click **Save Profile** to save the profile in the database.

If you select **Reset to Defaults,** the parameters are set to the initial values.

Configuring VIC Adapter Profile

You can use VIC Adapter profile to apply the Cisco VIC adapter settings to a single system or to a group of systems. You have the option to configure the VIC adapter settings such as creating vNICs, vHBAs, and VMFEX interfaces from the VIC configuration profile. You can define settings for the VIC adapter based on the PCI slot it is present or Any Slot. When you apply the profile the VIC Adapter Configuration task will inventory the system and based on that it performs a match based on the PCI slot. All the settings defined for that PCI slot is applied to the VIC adapter.

As part of the Hardware Provisioning and OS Deployment Workflow, you can select the VIC Adapter Configuration profile and the same settings are applied. Also you can apply VIC Adapter Configuration profile separately.

Creating VIC Adapter Profile Using Profile Manager

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**. The **Cisco IMC Configuration Profiles Manager** window displays.

Step 2 Click the icon to create a new VIC Adapter Profile.

Step 3 The **Create new profile** dialog box displays. From the **Profile Type** drop-down list, select **VIC Adapter Configuration**.

Step 4 You can create a new profile by using either **Create a new profile** or choose **Create profile from current configuration of the server**.

Step 5 Click **OK**.

Step 6 In the **Profile Name** field, enter a name for the profile.

Step 7 In the **Cisco IMC Server Configuration Profile Manager** window, click an adapter in the table to display its properties.

Step 8 In **Adapter Cards** area, update the following properties:

Name	Description
Add button	Add the adapter card in the PCI slot. The range is between 1 and 509.
Remove button	Removes the selected adapter card from the PCI slot.
Modify button	Modifies the PCI Slot of the adapter card.
PCI Slot column	The PCI slot in which the adapter is installed.
Product Name column	The product name for the adapter.

Step 9 In the tabbed menu below the **Adapter Card** area, click the **General** tab.

Step 10 In the **Modify Adapter Properties** area, review the following information for the adapter:

Name	Description
Description field	The user-defined description for the adapter, if any.
Enable FIP Mode check box	Whether FCoE Initialization Protocol (FIP) mode is enabled. FIP mode ensures that the adapter is compatible with current FCoE standards.
Enable VNTAG Mode check box	Whether virtual network tag (VNTAG) is enabled. If VNTAG mode is enabled: • vNICs and vHBAs can be assigned to a specific channel • vNICs and vHBAs can be associated with a port profile • vNICs can fail over to another vNIC if there are communication problems
Number of VM FEX interf field.	The number of VM FEX.

Step 11 In the **Pool Properties** area, you can define pools for MAC, WWPN, and WWNN address for vNICs and vHBAs.

Step 12 In the tabbed menu below the **Adapter Card** area, click the **vNICs tab.**

Step 13 In the Host Ethernet Interfaces area, select a vNIC from the table.

Step 14 Click **Properties** to open the **vNIC Properties** dialog box. Review and update the properties for the selected vNIC. For more information on vNIC properties, see Modifying vNIC Properties, and Managing vNICs for detailed information on managing vNICs.

Step 15 For reviewing and updating VM FEXs, click the VM FEXs tab in the tabbed menu below the Adapter Cards area. For more information on the VM FEX properties, see Managing VM FEX.

Step 16 For reviewing and updating vHBAs, click the vHBAs tab in the tabbed menu below the Adapter Cards area. For more information on the vHBAs properties, see Managing vHBAs.

Step 17 Click **Save Profile** to save the profile in the database.

If you select **Reset to Defaults,** by default **platform-default** is set for all the parameters.

Configuring Power Policies

Note The power cap configuration, and power restore policies features are available on all Cisco UCS M4 servers which supports Cisco IMC 2.0(2c) or higher. These features are not supported on Cisco UCS E-Series servers.

Creating Power Policy Configuration

Step 1 Launch the **Cisco IMC Configuration Profile Manager Utility**.

The **Cisco IMC Configuration Profiles Manager** window displays.

Step 2 Click the create new profile icon.

The **Create new profile** dialog box displays.

Step 3 From the **Profile Type** drop-down list, select Power Policy Configuration.

You can create a new profile by using either create a new profile or by selecting create profile from the current configuration of the server.

Step 4 Click **OK**.

Step 5 In the **Profile Name** field, enter a name for the profile.

Step 6 See, Power Profiles to configure the power policies.

Note **Run Power Characterization, Reset Profiles To Default, Recommended Power Cap, and Fan Policy Configuration** options are not available.

Configuration Pools

Creating a Configuration Pool

Step 1 From the left pane of the **Configuration Manager Console**, select **Assets and Compliance** > **Overview> Devices**.

A list of all devices that are currently installed are displayed in the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**.

Step 2 Right-click Devices, select Cisco IMC Server Configuration > Manage Cisco IMC Configuration Pools.

The Manage Cisco IMC Configuration Pools Wizard displays which allows you to add, edit and delete pools using this utility.

Step 3 Click the icon to create a new configuration pool.

Step 4 The **Create New Configuration Pool** dialog box displays. From the **Pool Type** drop-down list, select the configuration pool type that you want to create. This can be any of the following:

- IP Pool
- MAC Pool
- World Wide Node Name (WWNN) Pool
- World Wide Port Name (WWPN) Pool

Following sections shows how to configure each pool type:

IP Pools Configuration

a. From the **Pool Type** drop-down list, select IP Pool.

b. In the **Add IP Blocks** area, enter a name and a description for the pool.

c. Click **Add** button.

d. In the **Create Block of IP Address area**, review and update the following parameters:

- **From**—The IP address of the server from which the servers are assigned to the server pool.
- **Subnet Masks**—The subnet mask for the server pool.
- **Primary DNS**—The primary DNS server address.
- **Size**—The size of the server pool that you want to create.
- **Default Gateway**—The default gateway.
- **Secondary DNS**—The secondary DNS server address.

e. Click **Add**.

f. In the **Add IP Blocks** dialog box, click **Save**.

Mac Pool Configuration

a. From the **Pool Type** drop-down list, select MAC Pool.

b. In the **Add MAC Address Blocks** area, enter name and description for the pool.

c. Click **Add** button.

d. In the **Create MAC Address Block** area of the **Create Pool Block** dialog box, review and update the following parameters:

- **From**—The MAC address of the server from which the servers are assigned to the server pool. By default, the MAC address is set to 00:25:B5:00:00:00.
- **Size**—The size of the server pool that you want to create.

e. Click **Add**.

f. In the **Add MAC Address Blocks** dialog box, click **Save**.

World Wide Node Name (WWNN) Configuration

a. From the **Pool Type** drop-down list, select **World Wide Node Name (WWNN)**.

b. In the **Create WWN Pool Block** area enter the name and description for the pool.

c. Click **Add** button.

d. In the **Create WWN Block** area of the **Create Pool Block**, review and update the following parameters:

- **From**—The WWNN address of the server from which the servers are assigned to the server pool. By default, the WWNN address is set to 20:00:00:25:B5:00:00:00.
- **Size**—The size of the server pool that you want to create.

e. Click **Add**.

f. In the **Create WWN Pool Block** dialog box, click **Save**.

World Wide Port Name (WWPN) Configuration

a. From the **Pool Type** drop-down list, select **World Wide Node Name (WWNN)**.

b. In the **Create WWP Pool Block** area enter the name and description for the pool.

c. In the **Description** field, add a description for the pool.

d. Click **Add** button.

e. In the **Create WWP Block** area, review and update the following parameters:

   – **From**—The WWPN address of the server from which the servers are assigned to the server pool. By default, the WWNN address is set to 20:00:00:25:B5:00:00:00.

   – **Size**—The size of the server pool that you want to create.

f. Click **Add**.

In the **Create WWP Pool Block** dialog box, click **Save**.

Cisco IMC Task Manager

Using the Cisco IMC Task Manager, you can view the status of the tasks and perform actions on it.

Launching the Cisco IMC Task Manager

Step 1 Launch **Configuration Manager** by clicking **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 From the left pane of the **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Devices**.

A list of all devices that are currently installed are displayed in the **Name** column of the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**.

Step 3 Right-click **Devices**, select **Cisco IMC Configuration > Cisco IMC Task Manager**.

The **Cisco IMC Task Manager** window appears displaying the all the tasks that are initiated.

You can perform the following tasks on the **IMC Task Manager** window:

- Click **In Progress** to view all the tasks that are in progress.
- Click **Completed** to view all the tasks that are completed.
- Click **Failed** to view all the tasks that have failed.

You can also perform the following actions on particular tasks from the **IMC Task Manager** window:

- Select a task and click **Launch KVM Console** to launch the KVM console for the task.
- Select a task and click **Launch Cisco IMC Web UI** to launch the Cisco IMC Web UI for the task.
- Select a task and click **Delete** to delete it.

Cisco IMC Configuration Manager

Cisco IMC Configuration Manager is used to configure Hardware configuration settings like BIOS, RAID, VIC Adapter and Cisco IMC Admin Configuration. You can also view the hardware inventory of a single or a group of servers based on how the IMC Configuration Manager is launched. You can also initiate a single workflow involving Firmware Update, RAID, BIOS, IMC Admin, VIC Adapter configuration and start the OS deployment process.

Hardware Provisioning and OS Deployment

To deploy an operating system using the **Cisco IMC Integration Pack**:

Step 1 From the left pane of **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Device Collections** catalog.

Step 2 Right-click **Device Collection** and select any **Cisco IMC Server collection**. On selecting the collection all the Cisco Servers on the content pane are displayed. You can either right click on a server or launch the **Server configuration Manager** from the top ribbon.

The **IMC Server Configuration Manager** displays.

Step 3 Click **Hardware Provisioning & OS Deployment**.

Step 4 Under **Select Firmware Update and RAID Configuration Profiles** in the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**, select the **Update Firmware** check-box.

Note Only if you want to update the firmware as part of the OS Deployment check the **Update Firmware** check-box and follow the steps for updating.

The **Firmware Update Profile** drop-down list is enabled.

Step 5 From the **Firmware Update Profile** drop-down list select the firmware update profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Note **The Profile Details** section is updated based on the selection from **Select Firmware Update Profile** drop-down list.

Note If you want to configure RAID profile, select the **Apply RAID Configuration** check box and follow the steps for updating.

Step 6 From the **RAID Configuration Profile** drop-down list, select the RAID configuration profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Step 7 Click **Next** to configure BIOS, VIC Adapter profile, Cisco IMC Admin, and Power Policies Configuration.

Step 8 To configure BIOS profile select **Apply BIOS Configuration** check box.

Step 9 From the **BIOS Configuration Profile** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Step 10 To configure Cisco IMC admin profile check the **Apply Cisco IMC Admin Configuration** check box.

Step 11 From the **Cisco IMC Admin Configuration** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Step 12 To configure Cisco VIC adapter profile check the **Apply Cisco VIC Adapter Configuration** check box.

Step 13 From the **Cisco VIC Adapter Configuration Profile** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Step 14 To configure Power Policies, check the **Apply Power Policies Configuration** check box.

Step 15 Click **Next**.

Step 16 Under **Select Operating System Deployment Method**, select either:

- **PXE Boot** radio button. If you select **PXE Boot** radio button, it initiates operating system deployments from computers whose network interface card is configured to allow PXE boot requests.

Note Configure **PXE** options from **Administration** workspace before deploying OS. For more details, refer to **Microsoft Technet Configuration Manager** documentation.

- **Network ISO Boot (Select Task Sequence Media)** radio button. If you select the **Network ISO Boot (Select Task Sequence Media)** radio button, enter information for the following:
  - **Path** — Specify the location of the shared ISO boot image. This has to be on network location and the format for specifying the location is through IP address only and not hostname, for example \10.a.b.c.d\test.iso.
  - **Domain\Username** — Specify a valid user name in form of **username@domain name**, for example **adminstrator@sccm.cisco.com**.
  - **Password** — Specify a valid password.

Step 17 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 18 Click **Select all** to choose all the servers on the list, or if you want perform this task only for specific servers then select them.

Step 19 Click **Finish**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 20 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

Viewing Hardware Inventory

You can use the **Cisco IMC Integration Pack** to view the hardware inventory details of all the IMC servers under the **Devices** or **Device Collections** catalog in the left pane of the **Configuration Manager Console**.

Hardware inventory data gives you system information (such as available memory, which is Memory information, CPU, Power Supply, PCI Adapter, Network Adapter and Storage Adapter, processor type memory, number of CPUs and operating system) about each device.

Viewing Hardware Inventory

Step 1 Launch **Configuration Manager** by clicking **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 From the left pane of the **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Device Collections** catalog.

A list of all devices (including groups) that are currently installed displays in the **Name** column of the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**.

Step 3 In the **Name** column of the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**, right-click **All Cisco IMC Servers**, or any other device and choose **Cisco IMC Configuration > Launch Cisco IMC Configuration Manager**.

The **IMC Server Configuration Manager** displays.

Step 4 Click on **Hardware Inventory**.

The hardware inventory list based on the devices or groups selected are refreshed and displayed under **Hardware Inventory** in the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**.

Step 5 Under **Hardware Inventory**, the following information displays:

- **Select Server** drop-down list — populates the serial numbers of all the devices that are imported.
- **CPU** tab — displays information about the number of CPUs present. A more detailed description displays in the **CPU** tab table.
- **Memory** tab — displays information about memory components, such as total memory, available speed, and available memory. A more detailed description displays in the **Memory** tab table.
- **Power Supply** tab — displays information about the power supply components. A more detailed description displays in the **Power Supply** tab table.
- **PCI Adapter** tab — displays information about the available PCI adapters. A more detailed description displays in the **PCI Adapter** tab table.
- **Network Adapter** tab — displays information about the available network adapters. A more detailed description displays in the **Network Adapter** tab table.
- **Storage Adapter** tab — displays information about the available storage adapters. A more detailed description displays in the **Storage Adapter** tab table.

Note The information displayed in each tab is based on the value selected in the **Select Server** drop-down list.

Step 6 To view the updated information of the hardware inventory components, login to **Cisco IMC** and choose **Server > Inventory** in the left pane of **Cisco IMC**.

The corresponding hardware inventory information displays in the right pane of **Cisco IMC**.

Updating Firmware

Note To update the firmware you must create a profile using the **Launch Cisco IMC Configuration Profile Manager**. For more information, see Creating a Firmware Update Profile Using Configuration Profile Manager, page 2-10.

Step 1 Launch **Configuration Manager** by clicking **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 From the left pane of the **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Device Collections** catalog.

A list of all devices (including groups) that are currently installed displays in the **Name** column of the **Content Pane** on the right side of the **Microsoft Configuration Manager Console**.

Step 3 If you select **All Cisco IMC Servers** and try to launch the **Server Configuration Manager**, the **Firmware Update** option is disabled in the **Hardware Provisioning & OS Deployment** and **Firmware Update** tab is not available. This happens if **All Cisco IMC Servers** has more than one server. Select a model specific device collection, for example, All Cisco UCS C460 Servers, right-click and choose **Cisco IMC Configuration > Launch Cisco IMC Configuration Manager**.

The **IMC Server Configuration Manager** displays.

Step 4 Go to **Firmware Update** tab in the **Cisco IMC Server Configuration Manager.**

The **Select Firmware Update Profile** drop-down list is enabled.

Step 5 From the **Select Firmware Update Profile** drop-down list select the required profile.

Note **The Profile Details** section is updated based on the selection from **Select Firmware Update Profile** drop-down list.

Step 6 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 7 Click **Select all** to choose all the servers on the list, or if you want perform this task only for specific servers then select them.

Step 8 Click **Update**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 9 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

Applying a BIOS Profile Using Server Configuration Manager

Before You Begin

For the C-Series servers, you must have Cisco IMC version 1.5(4) to apply the BIOS settings successfully.

Step 1 From the left pane of Configuration Manager Console, select **Assets and Compliance > Overview >Device Collections** catalog.

Step 2 From the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**, right-click a device in the **Name** column.

Step 3 Choose **Cisco IMC Configuration > Launch Cisco IMC Server Configuration Server Manager**.

Step 4 In the left Pane, select BIOS Configuration.

Step 5 In the **Select BIOS Configuration** window, select **Apply BIOS Configuration**.

Step 6 From the BIOS Configuration Profile drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**. See, Creating a BIOS Profile Using Profile Manager, page 2-12.

Step 7 Select **Reboot Host Immediately** option if you want to reboot the server immediately. Else, ignore this option.

Step 8 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 9 Click **Select all** to choose all the servers on the list, or if you want perform this task only for specific servers then select them.

Step 10 Click **Apply**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 11 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

Cisco IMC Admin Configuration

Applying Cisco IMC Using Server Configuration Manager

Step 1 From the left pane of Configuration Manager Console, select **Assets and Compliance > Overview >Device Collections** catalog.

Step 2 From the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**, right-click a device in the **Name** column.

Step 3 Choose **Cisco IMC Configuration > Launch Cisco IMC Configuration Manager**.

Step 4 In the left Pane, select **Cisco IMC Admin Configuration**.

Step 5 In the **Select Cisco IMC Configuration** window, select **Apply Cisco IMC Configuration**.

Step 6 From the **Cisco IMC Admin Configuration Profile** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**. See, Creating Cisco IMC Profile Admin Profile, page 2-14.

Step 7 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 8 Click **Select all** to choose all the servers on the list, or if you want perform this task only for specific servers then select them.

Step 9 Click **Apply**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 10 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

VIC Adapter Configuration

Applying VIC Adapter Using Server Configuration Manager

Step 1 From the left pane of Configuration Manager Console, select **Assets and Compliance > Overview >Device Collections** catalog.

Step 2 From the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**, right-click a device in the **Name** column.

Step 3 Choose **Cisco IMC Configuration > Launch Cisco IMC Server Configuration Server Manager**.

Step 4 In the left Pane, select **VIC Adapter Configuration**.

Step 5 In the **Select VIC Adapter Configuration** window, select **Apply VIC Adapter Configuration**.

Step 6 From the **VIC Adapter Configuration** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**. See, Creating a VIC Adapter Using Profile Manager.

Step 7 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 8 Click **Select all** to choose all the servers on the list, or if you want perform this task only for specific servers then select them.

Step 9 Click **Apply**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 10 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

Power Policy Configuration

Applying Power Policy Configuration

Step 1 From the left pane of Configuration Manager Console, select **Assets and Compliance > Overview >Device Collections** catalog.

Step 2 From the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**, right-click a device in the **Name** column.

Step 3 Choose **Cisco IMC Configuration** > **Launch Cisco IMC Server Configuration Server Manager**.

Step 4 In the left Pane, select **Power Policy Configuration**.

Step 5 From the **Power Policies Configuration Profile** drop-down list, select the Profile created using the **Launch Cisco IMC Configuration Profile Manager**.

Step 6 Click **Next**.

If you are launching from a device collection a list of servers appear or if it launched from a device the server details appears.

Step 7 Click **Select all** to choose all the servers on the list, or if you want to perform this task for specific servers, then select them.

Step 8 Click **Apply**.

Cisco IMC Configuration confirmation pop-up window appears. Indicating that the task has been submitted to the service and if you want to launch the task manager to view the progress of the task.

Step 9 Click **Yes**.

Cisco IMC Task Manager window appears. For details on Cisco IMC Task Manager, see Cisco IMC Task Manager.

Launching the Cisco IMC Web Interface

Step 1 Launch **Configuration Manager** by clicking **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 From the left pane of the **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Device Collection** catalog.

Select any **Cisco IMC Collection**. On selecting the collection you will see all the **Cisco Servers** on the **Content Pane** then you can either right-click on a server or launch it from the top ribbon.

Step 3 In the **Name** column of the **Content Pane** on the right side of the **Configuration Manager Console**, right-click **All Cisco IMC Servers**, or any other device and choose **Cisco IMC Configuration** > **Launch Cisco Integrated Management Controller Web UI**. The Cisco Integrated

The **Cisco Integrated Management Controller Web UI** displays.

Launching the KVM Console

Note The KVM console requires Java Version 1.6 Update (14) or higher and Cisco IMC version 1.5(2) or higher.

Note To launch the KVM console, you must have valid Cisco IMC user credentials with admin or user role privileges.

Step 1 Launch **Configuration Manager** by clicking **Start > All Programs > Microsoft System Center> Configuration Manager > Microsoft Configuration Manager Console**.

The **Configuration Manager Console** screen displays.

Step 2 From the left pane of the **Microsoft Configuration Manager Console**, select **Assets and Compliance > Overview > Device Collection** catalog.

Select any **Cisco IMC Collection**. On selecting the collection you will see all the **Cisco Servers** on the **Content Pane** then you can either right-click on a server or launch it from the top ribbon.

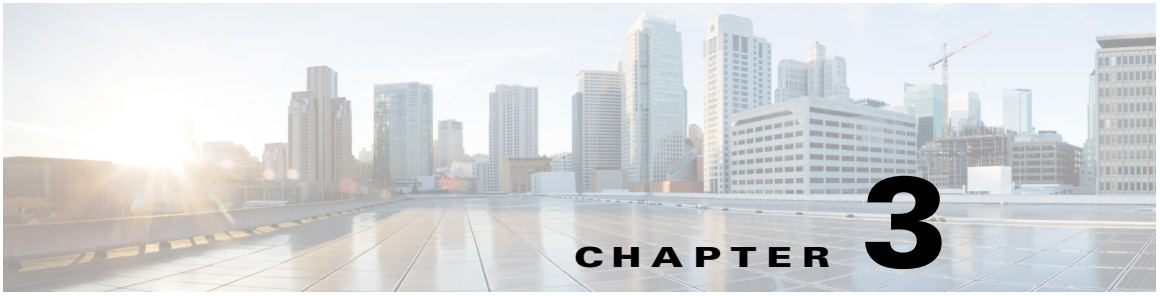
Step 3 You can launch the server from the top ribbon or double-click **Device Collection**.

Step 4 Right-click the server through which you want launch the KVM console and choose **Launch Cisco IMC> Launch KVM Console**.

The **KVM Console** displays.

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

Note If you are unable to launch KVM Console when Window like Configuration Manager or Profile Manager is open then launch KVM Console first and then open other windows.



Troubleshooting

This chapter includes the following sections:

Tip For troubleshooting issues with Configuration Manager, see the knowledge base articles available from Support for Microsoft System Center 2012.

Unable to login to Cisco IMC

Problem When you import servers using the Import IMC Servers Wizard utility, an error occurs during the authentication process of the user credentials provided to login to Cisco IMC.

Solution The table below gives the reasons as to why this error occurs and also the possible action to be taken to correct the error.

Reason	Action
There is no free XMLAPI sessions available in Cisco IMC.	Terminate unused session from Cisco IMC Web GUI
Either the username or password entered is not valid	Enter valid credentials.
Redirect HTTP to HTTPS Enabled check box is checked in the communication settings of Cisco IMC	Uncheck the Redirect HTTP to HTTPS Enabled check box
Unsupported server model is selected when importing servers	See the list of supported servers in the Overview chapter and select
Proxy is enabled when it is not required to access the servers.	Disable the proxy server
Under Communication Services, XML API Properties, XML API Enabled check box is disabled.	Enable the check-box for XML API under Communication Properties in the Cisco IMC Web GUI.

OS Deployment

Problem Windows Server 2008 R2, Windows 2012, and Windows 2012 R2 virtual machines reboot repeatedly. This issue occurs when an invalid License Key is entered in the Task Sequence.

Solution Provide the correct License Key in the Task Sequence.

Problem Reply has no message header marker and cannot recognize client identity. The problem is caused by the incorrect date and time or both being set in the BIOS.

Solution Correct the date and time in the Cisco IMC Server.

Problem Fails to stage WinPE.

Solution Correct the date and time of the Configuration Manager Server.

Firmware Update Profile

Problem When Cisco UCS M4 server is imported using Cisco IMC integration pack 1.0.1, firmware update profiles are not listed for this server in 1.0.2 version.

Solution To resolve this issue, follow these steps:

Step 1 Save the resource ID of the server for which the issue occurs.

Step 2 Delete the server from the **Configuration Manager Admin** console.

Step 3 Open **WBEMTEST.exe** on the configuration manager site server.

Step 4 Connect to the configuration manager WMI namespace, root\sms\site_<SITECODE>. Where SITECODE is the configuration manager site code.

Step 5 Once the connection is successful, open the query and enter the following:

Select * from SMS_R_CIMC Where ServerID=<ResourceID>. The resource ID is same as saved in **Step 1**.

Step 6 Delete the object shown in the query result window.

Step 7 Re-import the server using the **Import Cisco IMC** wizard.