Managing Rack Server Policies and Profiles

This chapter contains the following topics:

- Rack Server Policies, page 1
- Rack Server Profiles, page 22

Rack Server Policies

Rack server policies are a primary mechanism for defining configuration of various attributes on rack servers in Cisco UCS Director. These policies help ensure consistency and repeatability of configurations across rack servers. Defining and using a comprehensive set of policies enables greater consistency, control, predictability, and automation as similar configurations are applied across many rack servers.

The following workflow indicates how you can work with server policies in Cisco UCS Director:

1. Create a server policy such as BIOS policy or an NTP policy. You can create a policy in one of the following methods:
   a. Create a new policy. For more information about the various policy types and creating a new policy, see Creating Server Policies, on page 2.
   b. Create a policy from the configuration existing on a server. For more information about creating a policy from the configuration existing on a server, see Creating a Policy from an Existing Configuration, on page 3.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 21.
3. Perform any of the following optional tasks on the policy:
   a. View the list of servers that are mapped to a specific policy. For more information on performing these tasks, see Common Tasks for Server Policies, on page 4.
   b. Edit a policy to modify values.
   c. Delete a policy when it is no longer needed
   d. Clone a policy to use similar values

e Group multiple policies into a server profile. For more information about applying profiles, see Applying a Policy, on page 21.

Creating Server Policies

Perform this procedure when you want to create a new server policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add**.

Step 4 In the **Add Policy** dialog box, choose a policy type from the drop-down list.
For more information about creating a policy based on the policy type, select the policy type listed in the table below. The various properties required to configure these policies are available in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide. The respective sections in this guide are listed against each policy type.

Policy	Procedure Documented in this Guide	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy	Creating a BIOS Policy, on page 5	*Configuring BIOS Settings*
Disk Group Policy	Creating a Disk Group Policy, on page 6	*Managing Storage Adapters*
FlexFlash Policy	FlexFlash Policy, on page 7	*Managing the Flexible Flash Controller*
IPMI over LAN Policy	Creating an IPMI Over LAN Policy, on page 10	*Configuring IPMI*
LDAP Policy	Creating an LDAP Policy, on page 11	*Configuring the LDAP Server*
Legacy Boot Order Policy	Creating a Legacy Boot Order Policy, on page 12	*Server Boot Order*
Network Security Policy	Creating a Network Security Policy, on page 12	*Network Security Configuration*
Network Time Protocol Policy	Creating an NTP Policy, on page 13	*Configuring Network Time Protocol Settings*
Precision Boot Order Policy	Creating a Precision Boot Order Policy, on page 14	*Configuring the Precision Boot Order*

Policy	Procedure Documented in this Guide	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
RAID Policy	Creating a RAID Policy, on page 15	*Managing Storage Adapters*
Serial Over LAN Policy	Creating a Serial Over LAN Policy, on page 16	*Configuring Serial Over LAN*
SNMP Policy	Creating an SNMP Policy, on page 16	*Configuring SNMP*
SSH Policy	Creating an SSH Policy, on page 17	*Configuring SSH*
User Policy	Creating a User Policy, on page 18	*Configuring Local Users*
VIC Adapter Policy	Creating a VIC Adapter Policy, on page 19	*Viewing VIC Adapter Properties*
Virtual KVM Policy	Creating a Virtual KVM Policy, on page 20	*Configuring the Virtual KVM*
vMedia Policy	Creating a vMedia Policy, on page 21	*Configuring Virtual Media*

What to Do Next

Apply the policy to a server. For more information about applying a policy, see Applying a Policy, on page 21.

Creating a Policy from an Existing Configuration

You can choose to create a policy using a server that you have previously configured. By re-using the existing configuration on a server, you can reduce the time and effort involved in creating similar configurations.

Note When you create a policy from current configuration of a server, the password fields are not retrieved from the server.

Perform the following procedure when you want to create a policy from current configuration of a server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose a policy from the drop-down list and click **Submit**.

Step 5 In the dialog box that appears, check the **Create policy from current configuration of the server** check box and click **Next**.

Step 6 In the **Server Details** dialog box, check the **Create policy from current configuration of the server** check box. You can use the server details in the following two methods:

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the IP address in the **Server IP** field.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.
3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.
6. Enter the port number associated with the selected protocol in the **Port** field.

b) Click **Select** and choose a server from where you can retrieve the configurations.

Step 7 Click **Next**.
You will return to the **Main** dialog box. Continue with creating a policy following the prompts in the wizard. The fields for each policy vary depending on the policy you are creating in the system.

Common Tasks for Server Policies

Perform the following procedure when you want to edit, delete, clone, or view server mapping details of an existing policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Policies** tab.

Step 3 Expand a policy from the left pane and select a policy.

Step 4 To apply a policy to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Policy, on page 21.

Step 5 (Optional) Click **View Details** to view the details of a selected policy such as the status of the policy you have applied, the server details to which you have applied the policy and so on. If the policy is not successfully applied for example, an error message is displayed in the **Status Message** column.

Step 6 (Optional) To modify a policy, click **Properties** and modify the required properties.
When you modify a policy name, ensure that you do not specify a name which already exists.

Step 7 (Optional) To clone a policy, click **Clone** to copy the details of a selected policy to a new policy.

Step 8 (Optional) To delete a policy, click **Delete**. In the **Delete Policy** dialog box, click **Select** and select the policies you want to delete. Click **Select** and **Submit**.
You can delete one or more selected policies even if you have associated the policy with a server. If you try to delete a policy which is associated to a profile, an error occurs.

Step 9 Click **Submit** and/or **Close** if applicable.

Creating a BIOS Policy

A BIOS policy automates the configuration of BIOS settings on servers. You can create one or more BIOS policies which contain a specific grouping of BIOS settings that match the needs of a server or a set of servers. If you do not specify a BIOS policy for a server, the BIOS settings will remain as they are, either a default set of values for a brand new bare metal server or a set of values which were configured using Cisco IMC. If a BIOS policy is specified, the values specified in the policy replace any previously configured values on the server.

For details about configuring the various BIOS properties, see section *Configuring BIOS Settings* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a BIOS policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **BIOS Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Note If some properties or attributes in Cisco UCS Director are not applicable to a server running a specific Cisco IMC version, they are not applied. If the properties are not available on the Cisco IMC server, they are displayed as **Platform-Default** in the property fields.

Step 6 In the **Main** dialog box, select values for the main BIOS properties such as **Boot Option Retry**, **Post Error Pause**, and **TPM Support** drop-down lists.

Step 7 In the **Advanced** dialog box, choose the BIOS property values from the drop-down lists and click **Next**.

Step 8 In the **Server Management** dialog box, choose the server property values from the drop-down lists and click **Submit**.

Step 9 In the **Submit Result** dialog box, click **OK**.

Creating a Disk Group Policy

Using a Disk Group policy, you can select the physical disks used for Virtual Drives and also configure various attributes associated with a virtual drive.

A disk group policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the virtual drive. You can use a disk group policy to manage multiple disk groups. A single Disk Group policy can be associated with multiple virtual drives. If so, the virtual drives share the same Virtual Drive group space. Disk Group policies associated with different virtual drives in a RAID policy do not have any physical disk repeated across different Disk Group policies. For more information about RAID policy, see Creating a RAID Policy, on page 15.

For details about configuring the various disk group properties, see section *Managing Storage Adapters* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Disk Group policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Disk Group Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.

Step 6 In the **Virtual Drive Configuration** dialog box, choose the virtual drive properties and click **Next**.

Step 7 In the **Local Disk Configuration** dialog box, click + to add an entry to reference a local disk configuration and click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Step 9 Click **Submit** in the **Main** dialog box.

Step 10 In the **Submit Result** dialog box, click **OK**.

Note
- You cannot create a Disk Group policy from current configuration of the server.
- When a RAID policy is created from current configuration of the server, the Disk Group policy is also created automatically from the server configuration.

FlexFlash Policy

A FlexFlash policy allows you to configure and enable the SD card.

For details about configuring the various properties, see section *Managing the Flexible Flash Controller* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Note The minimum Cisco Integrated Management Controller firmware version for FlexFlash support is 2.0(2c).

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 In the **Add** dialog box, choose **FlexFlash Policy** from the drop-down list and click **Submit**.

Step 4 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 5 In the **Configure Cards** dialog box, complete the following fields:

Field	Description
Firmware Mode pane	Choose any of the following firmware operating modes: • **Mirror Mode** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util Mode** - In this mode one card with four partitions and one card with a single partition is created. This mode is available only for C220 M4 and C240 M4 servers. • **Not Applicable** - No firmware operating modes are selected. Go to step 5 if you select **Not Applicable**. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Partition Name field	The name of the partition.

Field	Description
Non Util Card Partition Name field	The name that you want to assign to the single partition on the second card, if it exists. **Note** This option is available only for util mode.
Select Primary Card (available for mirror mode) or **Select Util Card** (available for Util mode) drop-down list	Select the slots **Slot 1** or **Slot 2** where the SD cards are present or select **None** if only one SD card is present on the server. **Note** **None** is available only for **Select Util Card** option.
Auto Sync check box	Automatically synchronizes the SD card available in the selected slot. **Note** This option is available only for mirror mode.
Slot-1 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Slot-1 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 1 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
Slot-2 Read Error Threshold field	The number of read errors that are permitted while accessing Slot 2 of the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero). **Note** This option is available only for util mode. In case of mirror mode, the slot-1 Read/Write threshold will be applied to Slot-2 as well.

Field	Description
Slot-2 Write Error Threshold field	The number of write errors that are permitted while accessing Slot 2 of the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy. To specify a write error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero). **Note** This option is available only for util mode. In case of mirror mode, the slot-1 Read/Write threshold will be applied to Slot-2 as well.

Step 6 If you selected **Not Applicable** in the **Details** pane in step 4, complete the following fields:

Field	Description
Virtual Drive Enable drop-down list	The virtual drives that can be made available to the server as a USB-style drive.
RAID Primary Member drop-down list	The slot in which the primary RAID member resides.
RAID Secondary Role drop-down list	The role of the secondary RAID.
I/O Read Error Threshold field	The number of read errors that are permitted while accessing the Cisco FlexFlash card. If the number of read errors exceeds this threshold on a card, the card is marked unhealthy. To specify a read error threshold, enter an integer between 1 and 255. To specify that the card should never be disabled regardless of the number of errors encountered, enter 0 (zero).
I/O Write Error Threshold field	The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy The number of write errors that are permitted while accessing the Cisco FlexFlash card. If the number of write errors exceeds this threshold on a card, the card is marked unhealthy.
Clear Errors check box	If checked, the read/write errors are cleared when you click **Submit**.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
You can also select an existing FlexFlash policy from the **Hardware Policies** table and delete, edit, clone, apply or view the apply status by selecting the respective options in the user interface.

Note Applying a FlexFlash policy is a two step process as follows:

1. The settings on the server will be set to default.
2. The new settings on the policy will be applied. If there is any failure in this step, you will lose the existing settings prior to applying the policy.

Creating an IPMI Over LAN Policy

Configure an IPMI over LAN policy when you want to manage Cisco IMC with IPMI messages.

For details about configuring the various properties, see section *Configuring IPMI* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create an IPMI Over LAN policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **IPMI Over LAN Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, complete the following fields.

Field	Description
Enable IPMI Over LAN check box	Check this check box to configure the IPMI properties.
Privilege Level Limitdrop-down list	Choose a privilege level from the drop-down list.
Encryption Key field	Enter a key in the field.

Note Encryption key must contain even number of hexadecimal characters, not exceeding 40 characters in total length. If less than 40 characters are specified, the key will be padded with zeros to the length of 40.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Creating an LDAP Policy

Cisco UCS Director supports the LDAP configuration settings on the servers using an LDAP policy. You can create one or more LDAP policies which contain a specific grouping of LDAP settings that match the needs of a server or a set of servers.

For details about configuring the various LDAP properties, see section *Configuring LDAP Server* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a LDAP policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **LDAP Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, fill in the LDAP properties.

Step 7 Click **Next**.

Step 8 In the **LDAP Servers** dialog box, fill in the LDAP server details.

Step 9 Click **Next**.

Step 10 In the **Group Authorization** dialog box, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 11 In the **Add Entry to LDAP Groups** dialog box, fill in the group details.

Step 12 Click **Submit**.

Step 13 In the **Submit Result** dialog box, click **OK**.

Step 14 Click **Submit** in the **Group Authorization** dialog box.

Step 15 In the **Submit Result** dialog box, click **OK**.

Note
- Any existing LDAP Role Groups configured previously on the rack server are removed and replaced with the role groups that you configured in the policy. If you have not added any role groups into the policy, then the existing role groups on the server are removed, but not replaced.
- **Nested Group Search Depth** is applicable only to Cisco IMC versions 2.0(4c) and above. This value cannot be applied using the policy on a server that is running Cisco IMC versions prior to 2.0(4c).

Creating a Legacy Boot Order Policy

A Legacy Boot Order Policy automates the configuration of boot order settings of a rack server. You can create one or more Legacy Boot Order policies which contain a specific grouping of boot order settings that match the needs of a server or a set of servers. Using Cisco UCS Director, you can configure the order in which the rack server attempts to boot from available boot device types. You can also configure the precision boot order which allows linear ordering of the devices. For more information about precision boot order, see Creating a Precision Boot Order Policy, on page 14.

For details about configuring the various server boot order properties, see section *Server Boot Order* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a Legacy Boot Order policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Legacy Boot Order Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, click + and select the device type from the drop-down list. The table lists the devices you have added.
In the **Select Devices** table, select an existing device and click **x** to delete a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

You cannot add the same device type again.

Step 7 Click **Submit** in the **Add Entry to Select Devices** dialog box.

Step 8 In the **Submit Result** dialog box, click **OK**.

Step 9 Click **Submit** in the **Main** dialog box.

Step 10 In the **Submit Result** dialog box, click **OK**.

Note This policy is applicable only for Cisco IMC versions prior to 2.0. An error message is displayed if the policy is applied to a server running higher Cisco IMC versions. For servers running versions higher than 2.0, you must use the Precision Boot Order policy instead.

Creating a Network Security Policy

Cisco UCS Director uses IP blocking as network security. IP blocking prevents the connection between a server or a website and certain IP addresses or a range of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers. You can create one or more Network Security policies which contain a specific grouping of IP properties that match the needs of a server or a set of servers.

For details about configuring the various network security properties, see section *Network Security Configuration* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a Network Security policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Network Security** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Creating an NTP Policy

With an NTP service, you can configure a server managed by Cisco UCS Director to synchronize the time with an NTP server. By default, the NTP server does not run in Cisco UCS Director. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco UCS Director synchronizes the time on the managed server with the configured NTP server.

For details about configuring the various NTP properties, see section *Configuring Network Time Protocol Settings* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a NTP policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **NTP Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check **Enable NTP** check box to enable alternate servers and specify up to 4 NTP servers.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Note This policy is not applicable to E-series server models.

Creating a Precision Boot Order Policy

Configuring the precision boot order allows linear ordering of the devices. In Cisco UCS Director you can change the boot order and boot mode, add multiple devices under each device types, re-arrange the boot order, and set parameters for each device type.
For details about configuring the various boot order properties, see section *Configuring the Precision Boot Order* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

You can create this policy for servers that are running Cisco IMC version 2.x and above. For servers that are running versions prior to 2.x, you must configure the Legacy Boot Order policy instead.

Perform the following procedure to create a Precision Boot Order policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Precision Boot Order Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check the **UEFI Secure Boot** check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 7 Click + and select or enter device details. The table lists the devices you have added.
You can also select an existing device in the **Select Devices** table and click **x** to delete or click edit icon to edit a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

Step 8 Click **Submit** in the **Add Entry to Select Devices** dialog box.

Step 9 In the **Submit Result** dialog box, click **OK**.

Step 10 Click **Submit** in the **Main** dialog box.

Step 11 In the **Submit Result** dialog box, click **OK**.

Creating a RAID Policy

You can use a RAID policy to create virtual drives on a server. You can also configure the storage capacity of a virtual drive. Each virtual drive in a RAID policy is associated with a disk group policy. Using a disk group policy you can select and configure the disks to be used for a particular virtual drive.

RAID policy is supported only on the following:

- Storage controllers that support RAID configurations.
- Cisco IMC firmware version 2.0(4c) and above.
- Servers containing single storage controllers. On servers containing multiple storage controllers, the RAID policy will be applied only on the storage controller in the first slot.

For details about configuring the various properties, see section *Managing Storage Adapters* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a RAID policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **RAID Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 7 In the **Add Entry to Virtual Drives** dialog box, enter or select the virtual drive details.
You can either select an existing Disk Group policy from the drop-down list and edit or add a new Disk Group policy to specify local disks. To create a Disk Group policy, refer Disk Group Policy.

Note If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.

Step 8 Click **Submit** in the **Add Entry** dialog box.

Step 9 In the **Submit Result** dialog box, click **OK**.

Step 10 Check the **Erase existing Virtual Drives** check box to delete all existing virtual drives on the server.
If you select this check box, all existing virtual drives on the server will be deleted when the policy is applied. This results in loss of existing data.

Step 11 Check the **Configure remaining disks as JBOD** check box to configure the remaining disks as JBOD.
This option is applicable only on storage controllers that support JBOD. The disks that are not used for virtual drives or hotspares are configured as JBOD.

Step 12 Click **Submit** in the **Main** dialog box.

Step 13 In the **Submit Result** dialog box, click **OK**.

Creating a Serial Over LAN Policy

Serial over LAN enables the input and output of the serial port of a managed system to be redirected over IP. Configure and use a serial over LAN on your server when you want to reach the host console with Cisco UCS Director. You can create one or more Serial over LAN policies which contain a specific grouping of Serial Over LAN attributes that match the needs of a server or a set of servers.

For details about configuring the various Serial Over LAN properties, see section *Configuring Serial Over LAN* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a Serial Over LAN policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Serial Over LAN Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check the **Enable SoL** check box and select the **CoM Port** and **Baud Rate** values from the drop-down list or use the existing values.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Creating an SNMP Policy

Cisco UCS Director supports configuration of the Simple Network Management Protocol (SNMP) settings and for sending fault and alert information by SNMP traps from the managed server.

For details about configuring the various SNMP properties, see section *Configuring SNMP* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a SNMP policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **SNMP Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **SNMP Users** dialog box, click + to add a SNMP user and fill in the user details. You can use the + icon to add up to 15 SNMP Users.
Select an existing SNMP entry to edit or delete an entry from the table.

Step 7 Click **Next**.

Step 8 In the **SNMP Traps** dialog box, click + to add a SNMP trap and fill in the trap details. You can use the + icon to add up to 15 SNMP Traps.
Select an existing SNMP entry to edit or delete an entry from the table.

Step 9 Click **Next**.

Step 10 In the **SNMP Settings** dialog box, configure the SNMP properties.

Step 11 Click **Submit**.

Step 12 In the **Submit Result** dialog box, click **OK**.

Note
- Any existing **SNMP Users** or **SNMP Traps** configured previously on the server are removed and replaced with users or traps that you configured in the policy. If you have not added any users or traps into the policy, the existing users or traps on the server are removed but not replaced.
- The **SNMP Port** cannot be configured on a server that is running Cisco IMC versions prior to 2.x; it must be excluded for such servers using the check box.

Creating an SSH Policy

The SSH server enables an SSH client to make a secure, encrypted connection and the SSH client is an application running over the SSH protocol to provide device authentication and encryption. You can create one or more SSH policies which contain a specific grouping of SSH properties that match the needs of a server or a set of servers.

For details about configuring the various SSH properties, see section *Configuring SSH* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create an SSH policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **SSH Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check the **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.

Creating a User Policy

A User policy automates the configuration of local user settings. You can create one or more user policies which contain a list of local users that need to be configured on a server or a group of servers.

For details about configuring the various properties, see section *Configuring Local Users* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a User policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **User Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, you can add users that need to be configured on the server to the **Users** list.

Step 7 Click + to add a user.

Step 8 In the **Add Entry to Users** dialog box, complete the following fields:

Field	Description
Username field	Enter a name for the user in the field.

Field	Description
Role drop-down list	Choose a role for the user such as read-only, admin and so on from the drop-down list.
Enabled check box	Check this check box to activate the user.
New Password field	Enter a password associated with the username.
Confirm New Password field	Repeat the password from the previous field.

Step 9 Click **Submit**.

Step 10 In the **Submit Result** dialog box, click **OK**.
You can also select an existing user from the **Users** table in the **Main** dialog box and click **Edit** or **Delete** icons to edit or delete a user.

Note
- The first user in the **Users** table is the admin user. You cannot delete this admin user but you can change the password.
- When you apply a user policy, the user entries in Cisco UCS Director are replaced with the user entries you created. Blank entries in Cisco UCS Director are replaced with default users from Cisco UCS Director. The default user role is always read-only and the user is disabled.
- Ensure that the account used to manage the Cisco UCS Director is not deleted from the user list in the policy. If deleted, the Cisco UCS Director will lose connection to the server being managed.

Creating a VIC Adapter Policy

For details about configuring the various properties, see section *Viewing VIC Adapter Properties* in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Perform the following procedure to create a VIC Adapter policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **VIC Adapter Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, click + to add a VIC adapter entry in the table.

Step 7 In the **Add Entry to VIC Adapters** dialog box, enter or select the adapter details.

- **vNIC** - default properties are eth0 and eth1. You can only edit these properties and cannot delete them. These properties are also available for usNIC properties.
- **vHBA** - default properties are fc0 and fc1. You can only edit these properties and cannot delete them.

Step 8 Click **Submit**.

Step 9 In the **Submit Result** dialog box, click **OK**.

Step 10 Click **Submit** in the **Main** dialog box.

Step 11 In the **Submit Result** dialog box, click **OK**.

Creating a Virtual KVM Policy

The KVM console is an interface accessible from Cisco UCS Director that emulates a direct keyboard, video, and mouse (KVM) connection to the server. The KVM console allows you to connect to the server from a remote location. You can create one or more KVM policies which contain a specific grouping of virtual KVM properties that match the needs of a server or a set of servers.

For details about configuring the various KVM properties, see section *Configuring the Virtual KVM* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform this procedure when you want to create a Virtual KVM policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **Virtual KVM Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 Check the **Enable vKVM** check box.

Step 7 In the **Max Sessions** drop-down list, choose a number to indicate the maximum number of KVM sessions.

Step 8 In the **Remote Port** field, specify the port number.

Step 9 Check the **Enable Video Encryption** check box.

Step 10 Check the **Enable Local Server Video** check box.

Step 11 Click **Submit**.

Step 12 In the **Submit Result** dialog box, click **OK**.

Creating a vMedia Policy

You can use Cisco UCS Director to install an OS on the server using the KVM console and VMedia. You can create one or more vMedia policies which contain vMedia mappings for different OS images that match the needs of a server or a set of servers. You can configure upto two vMedia mappings in Cisco UCS Director - one for ISO files (through CDD) and the other for IMG files (through HDD).

For details about configuring the various vMedia properties, see section *Configuring Virtual Media* in the *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*.

Perform the following procedure to create a VMedia policy.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose **Hardware Policies** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add** dialog box, choose **vMedia Policy** from the drop-down list and click **Submit**.

Step 5 Enter a name in the **Policy Name** field and click **Next**.
You can also check the **Create policy from current configuration of the server** check box and click **Next**. This takes you to the **Server Details** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Main** dialog box, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 7 Click **Next**.

Step 8 Check the **Add CDD vMedia Mapping** check box and complete the CDD mapping details.

Step 9 Click **Next**.

Step 10 Check the Add **HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 11 Click **Submit**.

Step 12 In the **Submit Result** dialog box, click **OK**.

Note
- **Low Power USB State** cannot be configured currently in Cisco UCS Director.
- Applying a vMedia policy removes any existing vMedia mappings previously configured on the server, even if the policy does not contain any vMedia mappings.

Applying a Policy

Perform this procedure when you want to apply an existing policy to a server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 Choose the **Hardware Policies** tab.
Step 3 Select a policy you want to apply from the left pane.
Step 4 Click **Apply** from the options available at the top.
Step 5 In the **Apply Policy** dialog box, choose the server or server group from the drop-down list based on whether you want to apply the policy to individual servers or an entire rack server group.
Step 6 Click **Select** to select the server groups or servers to which you want to apply the policy.
Step 7 Click **Submit**.
Step 8 In the **Submit Result** dialog box, click **OK**.
The process of applying the policy to the specified set of servers begins. This process can take a few minutes depending on the policy type and network connectivity to servers to which the policy is being applied.

What to Do Next

You can also perform the following policy-related tasks:

- Click **Clone** to copy the details of a selected policy to a new policy.
- Click **View Apply Status** to see the list of the servers that the policy is associated to.
- Click **Delete** to delete policies from the system.

Deleting a Policy

You cannot delete a policy if it is associated with or applied to a server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 Choose the **Hardware Policies** tab.
Step 3 Click **Delete**.
Step 4 In the **Delete Policy** dialog box, click **Select** to check the check boxes of the policies you want to delete.
Step 5 Click **Submit**.

Rack Server Profiles

Multiple policies combined together form a server profile. For example, you can apply configuration details of a rack server profile to multiple rack-mount servers. You can associate this server profile to specific rack-mount servers. This helps ensure consistency and repeatability of configurations across servers. Defining

and using a profile enables greater consistency, control, predictability, and automation as similar configurations are applied across many servers.

The following workflow indicates how you can work with a server profile in Cisco UCS Director:

1 Create a server profile. You can create a policy in one of the following methods:

   a Create a new profile. For more information about creating a new profile, see Creating a Server Profile, on page 23.

   b Create a profile from the configuration existing on a server. For more information about creating a profile from the configuration existing on a server, see Creating a Profile from an Existing Configuration, on page 24.

2 Apply the profile on a server. For more information about applying a profile, see Applying a Server Profile, on page 25.

3 Perform any of the following optional tasks on the profile.

   a Edit

   b Delete

   c Clone

   You can also view the list of servers that are mapped to a specific profile and view details of policies tied to this profile. For more information on performing these tasks, see Common Tasks Under Server Profiles, on page 25.

Creating a Server Profile

Perform this procedure when you want to create a server profile.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Profiles** tab.

Step 3 Click **Add**.

Step 4 In the **Create Hardware Profile** dialog box, enter a name for the profile you want to create in the **Profile Name** field.

Step 5 Click **Next** or check **Create profile from current configuration of the server** check box and click **Next**. To perform the tasks in the **Server Details** pane, see Creating a Profile from an Existing Configuration, on page 24.

Step 6 In the **Profile Entities** dialog box, click + to add a profile entry.
You can also click the edit and delete icons to edit and delete the existing entries.

Step 7 In the **Add Entry to Profile Name** dialog box, choose the **Policy Type**.

Step 8 Select the policy name from the **Policy Name** drop-down list which lists the names of policies you have already created.
You can click the + next to **Policy Name** to create a new policy based on the policy type you have selected earlier. For more information about creating policies, see Creating Server Policies, on page 2.

Step 9 Click **Submit**.

Step 10 In the **Submit Result** confirmation dialog box, click **OK**.

Step 11 Click **Submit** in the **Profile Entities** dialog box.

Step 12 In the **Submit Result** confirmation dialog box, click **OK**.

What to Do Next

You can also edit, delete, clone a profile and also view the server mapped to a selected profile. For performing these tasks, see Common Tasks Under Server Profiles, on page 25

Creating a Profile from an Existing Configuration

You can choose to create a profile using a server that you have previously configured. By re-using the existing configuration on a server, you can reduce the time and effort involved in creating similar configurations.

Note When you create a profile from current configuration of a server, the password fields are not retrieved from the server.

Perform the following procedure when you want to create a profile from current configuration of a server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Profiles** tab.

Step 3 Click **Add**.

Step 4 Enter a name for the profile in the **Profile Name** field.

Step 5 Check the **Create profile from current configuration of the server** check box. You can use the server details in the following methods:

a) Check the **Enter Server Details Manually** check box and fill in the following fields:

1. Enter the IP address in the **Server IP** field.
2. Check the **Use Credential Policy** check box to select an existing policy and select a policy from the **Credential Policy** drop-down list or click+ next to the **Credential Policy** drop-down list and enter the details to create a new policy in the **Credential Policy Add Form** dialog box.
3. Enter the server login name in the **User Name** field.
4. Enter the server login password in the **Password** field.
5. Select http or https from the **Protocol** drop-down list.
6. Enter the port number associated with the selected protocol in the **Port** field.
7. Click **Select**, select the policies, and click **Select**.

b) Click **Select** and choose a server from where you can retrieve the configurations.

c) Click **Select**, choose the policies, and click **Select**.

Step 6 Click **Next**.

Step 7 In the **Profile Entities** dialog box, click + to add an entry to the profile name.
Click **x** to delete an existing entry from the **Profile Name** table.

Step 8 Click **Submit**.

Step 9 In the **Submit Result** dialog box, click **OK**.

Common Tasks Under Server Profiles

Perform the following procedure when you want to edit, delete, clone, or view server mapping details of an existing profile.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Profiles** tab.

Step 3 Expand the Hardware Profile in the left pane and select a profile.

Step 4 (Optional) To delete a profile, click **Delete** and complete the following steps:

a) Click **Select** in the **Delete Profile** dialog box.
b) Select one or more profiles.
c) Click **Select**.
d) Click **Submit**.

You cannot delete a profile which is associated to a server. You must associate a different profile to the server before deleting it.

Step 5 (Optional) To modify a profile, select a profile, click **Edit** and modify the required properties.
When you modify a profile name, ensure that you do not specify a name which already exists.

Step 6 (Optional) To copy the details of an existing profile to a new profile, click **Clone**.

Step 7 (Optional) To apply a profile to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Server Profile, on page 25.

Step 8 Click **View Details** to view the details of a selected profile such as the status of the profile you have applied, the server details to which you have applied the profile and so on. If the profile is not successfully applied for example, an error message is displayed in the **Status Message** column.

Step 9 Click **Submit** or **Close** if applicable.

Applying a Server Profile

Perform this procedure when you want to apply a server profile to a rack server.

Procedure

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 Choose the **Hardware Profiles** tab.

Step 3 Select an existing server profile and click **Apply**.

Step 4 In the **Apply Profile** dialog box, choose the server or server group from the drop-down list, based on whether you want to apply the profile to individual servers or an entire rack server group.

Step 5 Click **Select** to select the server groups or servers to which you want to apply the profile.

Step 6 Click **Submit**.

Step 7 In the **Submit Result** confirmation dialog box, click **OK**.
The process of applying a profile to the specified set of servers begins. This process can take a few minutes depending on the profile type and network connectivity to server(s) to which the profile is being applied.