Managing Rack Server Policies and Profiles

This chapter contains the following topics:

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 35.
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 5.
   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 35.

Creating Server Policies

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, 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 7	*Managing Storage Adapters*
FlexFlash Policy	FlexFlash Policy, on page 8	*Managing the Flexible Flash Controller*
IPMI over LAN Policy	Creating an IPMI Over LAN Policy, on page 11	*Configuring IPMI*
LDAP Policy	Creating an LDAP Policy, on page 12	*Configuring the LDAP Server*
Legacy Boot Order Policy	Creating a Legacy Boot Order Policy, on page 15	*Server Boot Order*
Network Configuration Policy	Creating a Network Configuration Policy, on page 16	*Configuring Network-Related Settings*
Network Security Policy	Creating a Network Security Policy, on page 18	*Network Security Configuration*
Network Time Protocol Policy	Creating an NTP Policy, on page 19	*Configuring Network Time Protocol Settings*

Policy	Procedure Documented in this Guide	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
Password Expiration Policy	Creating a Password Expiration Policy, on page 21	*Password Expiry*
Precision Boot Order Policy	Creating a Precision Boot Order Policy, on page 22	*Configuring the Precision Boot Order*
RAID Policy	Creating a RAID Policy, on page 23	*Managing Storage Adapters*
Serial Over LAN Policy	Creating a Serial Over LAN Policy, on page 25	*Configuring Serial Over LAN*
SNMP Policy	Creating an SNMP Policy, on page 26	*Configuring SNMP*
SSH Policy	Creating an SSH Policy, on page 28	*Configuring SSH*
User Policy	Creating a User Policy, on page 29	*Configuring Local Users*
VIC Adapter Policy	Creating a VIC Adapter Policy, on page 30	*Viewing VIC Adapter Properties*
Virtual KVM Policy	Creating a Virtual KVM Policy, on page 31	*Configuring the Virtual KVM*
vMedia Policy	Creating a vMedia Policy, on page 32	*Configuring Virtual Media*
Zoning Policy	Creating a Zoning Policy, on page 34	*Dynamic Storage* in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers.

Step 5 Click **Submit**.

What to Do Next

Apply the policy to a server. For more information about applying a policy, see Applying a Policy, on page 35.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

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

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

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Server Details** pane, you can use the server details in the following two methods:

a) Check **Enter Server Details Manually** and complete the required fields, including the following:

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 8 Click **Next**.

You will return to the **Main** pane for creating the policy. Continue with creating a policy using the prompts in the wizard. The fields for each policy vary depending on the policy you are creating in the system.

Step 9 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Expand a policy folder 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 35.

Step 5 (Optional) Click **View Apply Status** 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** screen, expand **Select Policy(s)** and check the policies you want to delete, and click **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**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

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 Click **Next**.

Step 7 In the **Main** pane, select values for the main BIOS properties such as **CDN Control**, **POST Error Pause**, and **TPM Support** drop-down lists.

Step 8 Click **Next**.

Step 9 In the **Advanced** pane, choose the BIOS property values from the drop-down lists and click **Next**.

Step 10 In the **Boot Options** pane, choose the appropriate setting for the drop-down lists.
The **Power ON Password Support** drop-down list allows you to enable or disable power on password support. You can also choose the default platform setting. Enabling this option prevents you from making any changes to the server, including configuration changes and entering the BIOS setup. Prior to enabling this option, ensure that a BIOS password is set in the BIOS Configuration screen using the Cisco IMC user interface.

Step 11 In the **Server Management** pane, choose the server property values from the drop-down lists.

Step 12 Click **Submit**.

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 23.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create Disk Group Policy** screen, enter a name in the **Policy Name** field and click **Next**.

Step 6 In the **Virtual Drive Configuration** pane, choose the RAID level and click **Next**.

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

Step 8 In the **Add Entry to Local Disk Configuration Reference** pane, complete the required fields, including the following:

Name	Description
Slot Number field	Enter the slot number of the disk.
Role drop-down list	Choose a role. It be can one of the following: • Normal • Dedicated Hot Spare • Global Hot Spare

Step 9 Click **Submit**.

Step 10 In the **Local Disk Configuration** pane, select a local disk from the table and click **Submit**.

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).

You cannot create a FlexFlash policy for Cisco UCS S3260 rack servers.

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **FlexFlash 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** pane. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 3.

Step 6 In the **Configure Cards** pane, complete the required fields, including the following:

Field	Description
Firmware Mode options	Choose any of the following firmware operating modes: • **Mirror** - This mode is a mirror configuration and is available only for C220 M4 and C240 M4 servers. • **Util** - 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. This mode is available only for C220 M3, C240 M3, C22, C24, and C460 M4 servers.
Mirror radio button	Check **Enable Virtual Drive** to enable the Hypervisor virtual drive or **check Erase Virtual Drive** to erase it.

Field	Description
Util radio button	Check **Enable Virtual Drive** to enable virtual drives such as SCU, Hypervisor, Drivers, HUU, and User Partition or check **Erase Virtual Drive** to erase them. **Note** You can select multiple virtual drives.
Not Applicable radio button	Check **Enable Virtual Drive** to enable virtual drives such as SCU, HV, Drivers, and HUU. **Note** You can select multiple virtual drives. The **Erase Virtual Drive** check box is not available.
Partition Name field	The name of the partition.
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).

Field	Description
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.
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 7 If you selected **Not Applicable** as the firmware mode, complete the required fields, including the following:

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).

Field	Description
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 8 Click **Submit**.
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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 On the **Rack Server** page, click **Hardware Policies**.
Step 3 Click **Add**.
Step 4 In the **Add** screen, choose **IPMI Over LAN Policy** from the drop-down list and click **Submit**.
Step 5 In the **Create IPMI Over LAN Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.

Name	Description
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** page, complete the required fields, including the following:

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. 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 automatically added with zeros to the length of 40.

Step 8 Click **Next**.

Step 9 In the **Confirm** page, click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create LDAP Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable LDAP check box	Check the check box to enable LDAP on the server.
Base DN field	The Base DN for the server. The Base DN refers to the point from where the server begins the search for users.
Domain field	The LDAP domain name.
Timeout drop-down list	Choose a timeout interval.
Enable Encryption check box	Check this check box to enable encryption.
Binding Parameters	
Method drop-down list	Choose a binding method from the drop-down list.

Name	Description
Binding DN field	Specify the binding DN for the LDAP server. The Binding DN consists of the user and the location of the user in the LDAP tree.
Password field	The password.
Search Parameters	
Filter Attribute field	Specify the filtering attribute.
Group Attribute field	Specify the group attribute.
Attribute field	Specify the attribute.

Step 8 Click **Next**.

Step 9 In the **Configure LDAP Servers** pane, complete the required fields, including the following:

Name	Description
Use DNS to Configure LDAP Servers check box	Check this check box to specify DNS parameters.
Source drop-down list	Choose a source method for DNS. It can be Extracted, Configured or Configured-Extracted. If you select Extracted, then the remaining DNS parameters are not displayed.
Domain to Search field	Specify the domains that must be searched.
Forest to Search field	Specify the forests that must be searched.
Server 1 field	The IP address or the host name of the LDAP server.
Port field	The port number. You can enter details for about 6 servers. **Note** These fields are not displayed if you have enabled DNS to configure LDAP servers.

Step 10 Click **Next**.

Step 11 In the **Group Authorization** pane, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 12 In the **Add Entry to LDAP Groups** screen, fill in the group details.

Step 13 Click **Submit**.

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 22.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers. For this policy, this check box is disabled.

Step 6 In the **Main** pane, click + to create a device type entry to the table. and select the device type from the drop-down list. The table lists the devices you have added.

Step 7 In the **Add Entry to Select Devices** pane, choose a device type, and click **Submit**.
You cannot add a device type multiple times.

In the **Device Type** table, select an existing device and 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**.

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 Configuration Policy

With a Network Configuration policy, you can specify the following network settings on a server:

- DNS Domain
- DNS Server for IPv4 and IPv6
- VLAN configuration

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

Perform the following procedure to create a Network Configuration policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Network Configuration Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.

Name	Description
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, see Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the following fields:

Field	Description
Common Properties	
Use Dynamic DNS check box	Check the check box to indicate use of Dynamic DNS. Dynamic DNS is used to add or update the resource records on the DNS server from Cisco UCS Director.
If you check **Use Dynamic DNS** check box	
Dynamic DNS Update Domain field	You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of Cisco UCS Director for the DDNS update.
IPv4 Properties	
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco UCS Director retrieves the DNS server addresses from DHCP.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
IPv6 Properties	
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco UCS Director retrieves the DNS server addresses from DHCP.
If you do not check **Obtain DNS Server Addresses from DHCP** check box	

Field	Description
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.
VLAN Properties	
Enable VLAN check box	If checked, is connected to a virtual LAN.
If you check **Enable VLAN** check box	
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 8 If you checked the **Cisco UCS S3260** check box in the **General** pane, then you must complete the following steps:

a) In the **CMC Settings** pane, specify the hostname and IPv4 address, and click **Next**.
b) In the **BMC Settings** pane, specify the hostname and IPv4 address, and click **Next**.

Step 9 In the **Confirm** pane, click **Submit**.

Caution To prevent breaking the communication between Cisco UCS Director and the rack server which depends on the DHCP settings in your network, exercise caution when using the following setting.

If you choose to use DHCP for obtaining the DNS IP addresses, the system will also configure the rack server (where this policy is applied) to use DHCP for the Management IP Address of the server.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **IP Blocking** pane, check the **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 8 Click **Next**.

Step 9 In the **IP Filtering** pane, check the **Enable IP Filtering** checkbox to enter IP addresses or a range of IP addresses.

Step 10 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable NTP check box	Check this check box to enable NTP and to configure a maximum of 4 servers.
NTP Server 1 field	Enter the IP address of the NTP server. You can enter the IP addresses of a maximum of 4 servers.

Step 8 Click **Submit**.

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

Creating a Password Expiration Policy

You can set a shelf life for a password, after which the password expires and is no longer valid for use. As an administrator, you can set this time in days. This configuration is common to all users. Users can set and derive the configuration as part of the user policy and create a password expiration policy.

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Password Expiration Policy** from the drop-down list and click **Submit**.

Step 5 In the **General** page, enter a name for the policy and click **Next**.

Step 6 In the **Main** page, complete the required fields, including the following:

Field	Description
Enable Password Expiry check box	Check this check box to enable a specified password expiry duration. You must set the number of days after which the password will expire. Choose a number from the **Password Expiry Duration** drop-down list.
Password History field	Set the number of occurrences that will be displayed when you view the password history.
Notification Period field	Set the number of days before which you will be notified about the password expiry.
Grace Period field	Set the grace period after which the password will expire.

Step 7 Click **Submit**.

- You can also select an existing policy and click Properties or Delete to edit or delete a policy from the More Actions drop-down list.
- This policy must be applied along with the User policy. You cannot apply a Password Expiration policy individually.
- E-Series servers do not suppport Password Expiration policy.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create Precision Boot Order Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 In the **Main** pane, complete the required fields, including the following:

Name	Description
UEFI Secure Boot check box	Check the check box to enable UEFI secure boot. If you check this check box, then you cannot configure a boot mode.

Name	Description
Configure Boot Mode drop-down list	Choose a boot mode from the drop-down list. You can choose a boot mode only if you have not checked **UEFI Secure Boot**.
Select Devices list	Expand the list, and click + and select or enter device details. To enter the device details, you must specify the following fields: • Device Type • Device Name • State • Slot

Step 7 In the **Add Entry to Select Devices** screen, click **Submit**.
The devices that you have added are listed in the table. 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**.

Step 9 Check **Configure One Time Boot Device** to set the device from which the server must boot once.

Important This check box is not applicable for Cisco IMC versions older than 3.0(1c).

Step 10 Select the device from the **One Time Boot Device** drop-down list.

Step 11 Check **Reboot On Update** to reboot the selected server after the one time boot device has been updated in the server.

Step 12 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create RAID Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 8 In the **Add Entry to Virtual Drives** screen, complete the required fields, including the following:

Name	Description
Virtual Drive Name field	Enter a unique name for the virtual drive.
Virtual Drive Size (MB) field	The size of the virtual drive.
Disk Group Policy drop-down list	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, see Creating a Disk Group Policy, on page 7. **Note** If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.

Name	Description
Access Policy drop-down list	Choose an access policy for the virtual drive.
Read Policy drop-down list	Choose a read policy for the virtual drive.
Write Policy drop-down list	Choose a Write for the virtual drive.
IO Policy drop-down list	Choose an IO for the virtual drive.
Drive Cache drop-down list	Select the status of the drive cache.
Expand to available check box	Check the check box to expand the virtual drive.
Boot drive check box	Check the check box to indicate this virtual drive as a boot drive.
Set disks in JBOD state to Unconifigured Good check box	Disks which are in JBOD state will be set to Unconfigured Good state before being used for the Virtual Drive creation

Step 9 In the **Add Entry to Virtual Drives** screen, click **Submit**.

Step 10 Check **Delete existing Virtual Drives** 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 **Configure Unused Disks** to configure the remaining disks.
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.

a) Check either of the following options:

- **Unconfigured Good**
- **JBOD**

Step 12 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create SoL Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, 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 8 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create SNMP Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **SNMP Users** pane, 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 8 Click **Next**.

Step 9 In the **SNMP Traps** pane, 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 10 Click **Next**.

Step 11 In the **SNMP Settings** pane, configure the SNMP properties.

Step 12 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create SSH Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, complete the required fields, including the following:

Name	Description
Enable SSH check box	Check the check box to enable SSH and configure the SSH properties.
SSH Port field	By default, the port number of 22 is displayed. Use the arrows to increase or decrease the number.

Name	Description
SSH Session Timeout (seconds) field	The idle time, in seconds, after which an SSH session is timed out. By default, it is set to 60 seconds. Use the arrows to increase or decrease the number.

Step 8 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create User Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, check **Enforce Strong Password**.
Checking this check box implies that users selected for this policy must create a strong password.

Step 8 Click + to add users that need to be configured on the server to the **Users** list.
You can also select an existing user from the **Users** table and click **Edit** or **Delete** icons to edit or delete a user.

Step 9 In the **Add Entry to Users** screen, complete the required fields, including the following:

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

Step 10 Click **Submit**.

Step 11 In the **Main** pane, check **Add Password Expiration Policy**, and you can either choose a password expiration policy that you have previously created, or you can create a new policy.
To use a password expiration policy, Cisco IMC version 3.0(1c) or later is required.

Step 12 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create VIC Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** pane, click + to add a VIC adapter entry in the table.

Step 8 In the **Add Entry to VIC Adapters** screen, 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 9 Click **Submit**.

Step 10 In the **Main** pane, click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create vKVM Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 Check **Enable vKVM**.

Step 8 In the **Max Sessions** drop-down list, choose a number to indicate the maximum number of KVM sessions.

Step 9 In the **Remote Port** field, specify the port number.

Step 10 Check the **Enable Video Encryption** check box.

Step 11 Check the **Enable Local Server Video** check box.

Step 12 Click **Submit**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

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

Step 5 In the **Create vMedia Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	Check this check box to create this policy for Cisco UCS S3260 servers.

Step 6 Click **Next**.

Step 7 In the **Main** screen, complete the required fields, including the following:

Name	Description
Enable vMedia check box	Check the check box to enable vMedia.
Enable Virtual Media Encryption check box	Check the check box for enabling vMedia encryption. This field is editable only after you check **Enable vMedia**.
Enable Low Power USB check box	Check this check box to enable low power USB on the server.
Maximum Sessions drop-down list	Select the maximum number of sessions allowed on the server.

Step 8 Click **Next**.

Step 9 Check **Add CDD vMedia Mapping** and complete the CDD mapping details.

Step 10 Click **Next**.

Step 11 Check **Add HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 12 Click **Submit**.

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.

Creating a Zoning Policy

A Zoning policy is used to assign physical drives to server. The Cisco UCS C-Series rack-mount servers support dynamic storage of Serial Attached SCSI (SAS) drives in the Cisco Management Controller (CMC). This dynamic storage support is provided by the SAS fabric manager located in the CMC. Dynamic storage supports the following options:

- Assigning physical disks to server 1 and server 2
- Chassis Wide Hot Spare (supported only on RAID controllers)
- Shared mode (supported only in HBAs)
- Un-assigning physical disks
- Viewing SAS expander properties
- Assigning physical drives to servers
- Moving physical drives as Chassis Wide Hot Spare
- Un-assigning physical drives

For details about configuring the various disk group properties, see section *Dynamic Storage* in the Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers.

Perform the following procedure to create a Zoning policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 In the **Add** screen, choose **Zoning Policy** from the drop-down list and click **Submit**.

Step 5 In the **Create Zoning Policy** screen, in the **General** pane, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.

Name	Description
Policy Type field	The type of policy that you are creating. You cannot edit this field.
Create policy from current configuration of the server check box	Check this check box to create the policy from an existing configuration of the server. If you check this check box, an additional **Server Details** pane is displayed. For information on performing tasks in this pane, refer Creating a Policy from an Existing Configuration, on page 3.
Cisco UCS S3260 check box	A Zoning Policy is only applicable to Cisco UCS S3260 Rack Server. So, the **Cisco UCS S3260** check box is checked by default.

Step 6 Click **Next**.
Step 7 In the **Zoning** screen, click + to add local disks that you want to configure on the server.
Step 8 In the **Add Entry to Local Disks** screen, enter the **Slot Number** where the local disk is present.
Step 9 Select the local disk details such as the **Ownership** assigning the ownership of the local disk.
Step 10 Check **Force** when assigning disks owned by one server to another server.
Step 11 Click **Submit**.
Step 12 Check **Modify Physical Drive Power Policy** to set the policy.
Step 13 Select the power state from the **Physical Drive Power State** drop-down list.
Step 14 Click **Submit**.

Applying a Policy

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 On the **Rack Server** page, click **Hardware Policies**.
Step 3 Expand the folders, and select a policy you want to apply.
Step 4 Click **Apply** from the options available at the top.
Step 5 In the **Apply Policy** screen, choose the servers on which you want to apply this policy.
Step 6 Check **Schedule Later** to apply the policy at a later time.
You will have to select a schedule from the **Schedule** drop-down list, or create a new schedule.
Step 7 Click **Submit**.

The process of applying the policy to the specified set of servers is initiated. 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 mapped to a hardware profile.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 On the **Rack Server** page, click **Hardware Policies**.
Step 3 Click **Delete**.
Step 4 In the **Delete Policy** screen, 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 37.

   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 37.

2 Apply the profile on a server. For more information about applying a profile, see Applying a Server Profile, on page 39.

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 38.

Creating a Server Profile

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

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 In the **Create Hardware Profile** screen, in the **General** pane, 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 37.

Step 6 In the **Profile Entities** screen, 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** screen, 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 **Profile Entities** screen, click **Submit**.

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 38

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Click **Add**.

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

Step 5 Check **Create profile from current configuration of the server**. 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** screen, 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**.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

Step 3 Expand the list of hardware profiles 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** screen.

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 39.

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 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Hardware Profiles**.

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

Step 4 In the **Apply Profile** screen, 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**.
The process of applying a profile to the specified set of servers is initiated. 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.

Host Image Mapping for E-series Servers

Host Image Mapping is a commonly used feature for E-Series servers. Using this feature, you can upload an ISO file before installing it on the server running Cisco IMC. To use this feature, you must first create a host image mapping profile within Cisco UCS Director. After creating a mapping profile, you can either edit or delete the profiles from the system.

Creating a Host Image Mapping Profile

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.

Step 2 On the **Rack Server** page, click **Host Image Mapping**.

Step 3 Click **Add**.

Step 4 In the **Add Host Image Mapping Profile** page, complete the require fields, including the following:

Field	Description
Profile Name field	A descriptive name for the profile.
Download Image From drop-down list	Select any of the FTP, SFTP, HTTP, or HTTPS servers to download image.
Server IP Address field	IP address of the server.
File Path field	The path of the file.
User name field	The user name. This field is applicable only for FTP and SFTP servers.
Password field	The password. This field is applicable only for FTP and SFTP servers.
Map After Download check box	Check this check box to map the downloaded image. If you check this check box, you can view if the image is downloaded successfully and if the downloaded image is mapped to the server. This information is displayed when you click **View Status Details** on the **Host Image Mapping** page.
Delete All Images check box	Deletes all the downloaded images from the server where you apply this profile.

Step 5 Click **Submit**.

What to Do Next

Apply the profile to a server.

Applying a Host Image Mapping Profile

Before You Begin

You have created a host image mapping profile.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Rack Server**.
Step 2 On the **Rack Server** page, click **Host Image Mapping**.
Step 3 Choose a profile from the list and click **Apply**.
Step 4 In the **Apply Profile** page, expand the server list and select the servers you want to apply the profile to.
Step 5 Click **Submit**.