Managing Policies and Profiles

This chapter contains the following topics:

Credential Policies

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco IMC Supervisor. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application.

The **Credential Policies** page displays the following details:

Field	Description
Policy Name	User defined name of the policy.
Description	User defined brief description of the policy.
Username	Cisco user name.
Protocol	Protocol followed by the policy.
Port	Port for the policy.

You can perform various tasks such as adding, editing, and deleting policies from this page. For information about creating a credential policy, see Creating a Credential Policy, on page 2.

Creating a Credential Policy

Perform this procedure to create a credential policy.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Credential Policies**.

Step 3 Click **Add**.

Step 4 On the **Add Credential Policy** screen, complete the following fields:

Field	Description
Policy Name field	A descriptive name for the policy.
Description field	(Optional) A description of the policy.
User Name field	Cisco IMC user name or the rack mount server user name.
Password field	Cisco IMC password or the rack mount server password.
Protocol drop-down list	Choose a protocol from the drop-down list.
Port field	Enter a port number for the policy.

Step 5 Click **Submit**.

Note You can edit, clone, delete, view, apply and view server mappings of the credential policy you have created.

Hardware Policies

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

Use Case: As an administrator, you may have identified a "Golden Server" which contains the required configurations including the right Networking, BIOS, RAID configurations and so on. You can replicate these configurations across other servers which are out of compliance. You can retain this configuration within Cisco IMC for any new servers that you may need to add in future and roll-out the configured server. You have the flexibility of changing the configuration on the fly before applying the same. For example, a component may need an update, ntp ip address, baud rate and so on. You may have forgotten the configuration on the "Golden Server" and may want to verify it before applying to other servers.

Individual policies are processed one after the other. Policies bundled into profiles are multi-threaded and helps starting a bunch of processes at the same time.

The following workflow indicates how you can work with hardware policies in Cisco IMC Supervisor:

1 Create a hardware 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 Hardware Policies, on page 3.

   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 29.

2 Apply the policy on a server. For more information about applying a policy, see Applying a Hardware Policy, on page 30.

3 Perform any of the following optional tasks on the policy:

   a Edit

   b Delete

   c Clone

   d You can also view the list of servers that are mapped to a specific policy. For more information on performing these tasks, see General Tasks Under Hardware Policies, on page 31.

   e You can apply profiles to servers after creating various policies and grouping them into profiles. For more information about applying profiles, see Applying a Hardware Profile, on page 34.

Creating Hardware Policies

Perform this procedure to create hardware policies.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Policies**.

Step 3 Click **Add**.

Step 4 On 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.

Note A check box is introduced to select the Cisco UCS S3260 platform for creating policy. This option is disabled by default. If you need to create a policy for Cisco UCS S3260, you must check the check box and enable the same.

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy, on page 5	*Configuring BIOS Settings*
Disk Group Policy, on page 6	*Managing Storage Adapters*
FlexFlash Policy, on page 6	*Managing the Flexible Flash Controller*
IPMI Over LAN Policy, on page 10	*Configuring IPMI*
LDAP Policy, on page 11	*Configuring the LDAP Server*
Legacy Boot Order Policy, on page 12	*Server Boot Order*
Network Configuration Policy, on page 13	*Configuring Network-Related Settings*
Network Security Policy, on page 17	*Network Security Configuration*
NTP Policy, on page 17	*Configuring Network Time Protocol Settings*
Password Expiration Policy, on page 18	*Password Expiry*
Precision Boot Order Policy, on page 19	*Configuring the Precision Boot Order*
RAID Policy, on page 20	*Managing Storage Adapters*
Serial Over LAN Policy, on page 22	*Configuring Serial Over LAN*
SNMP Policy, on page 23	*Configuring SNMP*
SSH Policy, on page 24	*Configuring SSH*
User Policy, on page 24	*Configuring Local Users*
VIC Adapter Policy, on page 26	*Viewing VIC Adapter Properties*
Virtual KVM Policy, on page 26	*Configuring the Virtual KVM*
vMedia Policy, on page 27	*Configuring Virtual Media*
Zoning Policy, on page 28	*Dynamic Storage* in the *Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Storage Servers*

What to Do Next

Apply the policy to a server. See Applying a Hardware Policy, on page 30.

BIOS Policy

A BIOS policy automates the configuration of BIOS settings on servers. You can create one or more BIOS policies that contain a specific grouping of BIOS settings, matching 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 default to set of values for a brand new baremetal server or to a set of values previously configured using Cisco IMC. If a BIOS policy is specified, its values replace any previously configured values on the server.

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

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **BIOS Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, select values for the main BIOS properties, such as **Boot Option Retry**, **Post Error Pause**, and entries in **TPM Support** drop-down list. 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 prevents you from making any changes to the server, including configuration changes and entering the BIOS setup.

Note Ensure that a BIOS password is set in the BIOS Configuration screen using the CIMC UI.

Step 6 On the **Advanced** screen, choose the BIOS property values from the drop-down lists and click **Next**.

Step 7 On the **Server Management** screen, choose the server property values from the drop-down lists and click **Submit**.

Note BIOS policy displays tokens for all the available platforms.

- If an attribute is not valid for a particular server platform it is ignored. For example, Power On Password Support BIOS token is applicable only for servers running a 3.x firmware. If this token is applied on a server running firmware below 3.x, it is ignored.
- If an attribute is present for the target platform and the value is not applicable, an error occurs. For example, Extended APIC BIOS token has values Enabled and Disabled which is applicable only for platform A based server models. However, if this token is applied on platform B server models, you will get an xml parsing error.

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 group of physical disks used for creating a virtual drive is called a Disk Group.

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 .

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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Disk Group Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field and click **Next**.

Step 4 On the **Virtual Drive Configuration** screen, choose the RAID level from the **RAID Level** drop-down list and click **Next**.

Step 5 On the **Local Disk Configuration** screen, click + to add an entry to reference a local disk configuration 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).
- Flex Flash policies are not available for Cisco UCS S3260 Rack Server.

Perform the following procedure to create a FlexFlash policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **FlexFlash Policy** from the drop-down list and click **Submit**.

Step 3 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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 On the **Configure Cards** page, 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.
Mirror radio button	Check **Enable Virtual Drive** to enable the **Hypervisor** virtual drive or check **Erase Virtual Drive** to erase it.
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. • **Erase Virtual Drive** check box is not available.

Field	Description
Partition Name field (available only for **Mirror** and **Util** mode	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 5 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).

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 6 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. Hence, if there is any failure in this step, you will lose the existing settings prior to applying the policy.

IPMI Over LAN Policy

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus. 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **IPMI Over LAN Policy** from the drop-down list and click **Submit**.

Step 3 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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 If you are creating this policy for a rack-mount server, then complete the following steps:

a) In the **Main** dialog box, complete the following fields.

Option	Description
Enable IPMI Over LAN	Check this check box to configure the IPMI properties.
Privilege Level Limit	Choose a privilege level from the drop-down list.
Encryption Key	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.

b) Click **Next**.

c) On the **Confirm** screen, click **Submit**.
You can see the rack-mount server listed in the **Server Platform** column under **Hardware Policies**.

Step 5 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **CMC Settings** screen, check the **Enable IPMI Over LAN** checkbox for both CMC 1 and CMC 2 if required.

Step 7 Click **Next**.

Step 8 On the **BMC Settings** screen, check the **Enable IPMI Over LAN** checkbox for both BMC 1 and BMC 2 if required.

Step 9 On the **Confirm** screen, click **Submit**.
You can see the Cisco UCS S3260 Dense Storage Rack Server listed in the Server Platform column in the Hardware Policies page.

LDAP Policy

Cisco C-series and E-series servers support LDAP. Cisco IMC Supervisor supports the LDAP configuration settings on the servers using an LDAP policy. You can create one or more LDAP policies that contain a specific grouping of LDAP settings, matching the needs of a server or a set of servers.

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

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **LDAP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, enter the LDAP properties and click **Next**

Step 6 On the **Configure LDAP Servers** screen, enter the LDAP server details and click **Next**

Step 7 On the **Group Authorization** screen, enter the group authorization details and click + to add an LDAP group entry to the table.

Step 8 On the **Add Entry to LDAP Groups** screen, fill in the group details and click **Submit**.

Note
- Any existing LDAP Role Groups configured previously on the server are removed and replaced with the role groups that you configured in the policy. If you have not added any role groups to the policy, then the existing role groups on the server are simply removed.
- **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).

Legacy Boot Order Policy

A Legacy Boot Order Policy automates the configuration of boot order settings. 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 IMC Supervisor, you can configure the order in which the server attempts to boot from available boot device types. You can also configure the precision boot order which allows linear ordering of the devices. See .

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.

Note Legacy Boot Order policies are not available for Cisco UCS S3260 Rack Server.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Legacy Boot Order Policy** from the drop-down list and click **Submit**.

Step 3 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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 On the **Main** screen, 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 5 Click **Submit** in the **Add Entry to Select Devices** screen.

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. Use Precision Boot Order policy instead.

Network Configuration Policy

Cisco IMC Supervisor allows you to create a Network Configuration policy which 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 In the **Add** dialog box, choose **Network Configuration Policy** from the drop-down list and click **Submit**.

Step 3 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** window. See Creating a Policy from an Existing Configuration, on page 29

Step 4 If you are creating this policy for a rack-mount server, complete the following steps:

a) On the **Main** screen, complete the following fields:

Field	Description
Common Properties	
Use Dynamic DNS check box	Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor
If you check **Use Dynamic DNS** check box	

Field	Description
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 IMC Supervisor for the DDNS update.
IPv4 Properties	
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC Supervisor 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 IMC Supervisor 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.
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.

b) Click **Next**.
c) On the **Confirm** xreen, click **Submit**.
You can see the rack-mount server listed in the Server Platform column in the Hardware Policies page.

Step 5 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **Main** screen, complete the following fields:

Field	Description
Common Properties	

Field	Description
Use Dynamic DNS check box	Dynamic DNS is used to add or update the resource records on the DNS server from Cisco IMC Supervisor
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 IMC Supervisor for the DDNS update.
IPv4 Properties	
Use DHCP check box	If checked, the **Obtain DNS Server Addresses from DHCP** check box is displayed.
Obtain DNS Server Addresses from DHCP check box	If checked, enables DHCP for DNS.
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	
Enable IPv6 check box	If checked, the **Use DHCP** check box is displayed.
Use DHCP check box	If checked, the **Obtain DNS Server Addresses from DHCP** check box is displayed.
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC Supervisor retrieves the DNS server addresses from DHCP.
If you do not check **Use DHCP** check box	
Management IP Address field	Enter the Management IP address.
Prefix Length field	Enter the number of characters for the prefix length.
Gateway field	Enter the Gateway IP address.
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.

Field	Description
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 7 Click **Next**.

Step 8 On the **CMC Settings** screen, enter the following fields for both CMC 1 and CMC 2 if required:

Field	Description
Hostname field	The hostname of the server.
IPv4 Address field	The IPv4 IP address.
IPv6 Address field	The IPv6 IP address.

Step 9 Click **Next**.

Step 10 On the **BMC Settings** screen, enter the following fields for both BMC 1 and BMC 2 if required:

Field	Description
Hostname field	The hostname of the server.
IPv4 Address field	The IPv4 IP address.
IPv6 Address field	The IPv6 IP address.

Step 11 Click **Next**.

Step 12 On the **Confirm** screen, click **Submit**.

Caution To prevent breaking the communication between Cisco IMC Supervisor 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.

Network Security Policy

Cisco IMC Supervisor 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.

You can set four IP filtering properties while creating the Network Security policy. IP Filtering allows a selected set of IPs to access the servers. You can either input a single IP address or a range of IP Addresses separated by hyphen in any of the four filter fields. An IP address can either be a IPv4 or IPv6 address.

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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Network Security** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **IP Blocking** window, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 6 Click **Next**.

Step 7 On the **IP Filtering** screen, check **Enable IP Filtering** checkbox to enable the IP, and enter either single or a range of IP addresses.

Note Filter 1 displays the IP address of Cisco IMC Supervisor by default.

Step 8 Click **Submit**.

NTP Policy

With an NTP service, you can configure a server managed by Cisco IMC Supervisor to synchronize the time with an NTP server. By default, the NTP server does not run in Cisco IMC Supervisor. 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 IMC Supervisor 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **NTP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, check **Enable NTP** check box to enable alternate servers and specify up to 4 NTP servers.

Step 6 Click **Submit**.

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

Password Expiration Policy

You can set a shelf life for a password, after which it expires. 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 User policy and create 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*.

Perform the following procedure to create a Password Expiration policy.

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Password Expiration Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

Step 4 On the **Main** screen, complete the following:

Field	Description
Enable Password Expiry check box	Check this check box to enable a specified password expiry duration and complete the following: **Password Expiry Duration** - Set the number of days for the password to expire.
Password History field	Set the number of occurrences that will be displayed when you view the password history.

Field	Description
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 5 Click **Submit**.

Note
- 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.

Precision Boot Order Policy

Configuring the precision boot order allows linear ordering of the devices. In Cisco IMC Supervisor you can change the boot order and boot mode, add multiple devices under each device types, rearrange 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **Precision Boot Order Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check UEFI Secure Boot check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 6 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 7 On the **Add Entry to Select Devices** page, click **Submit**.

Step 8 Check **Configure One Time Boot Device** check box to set the device from which the server must boot once.

Step 9 Select the device from the **One Time Boot Device** drop-down list.

Note **Configure One Time Boot Device** is not applicable for CIMC versions older than 3.0(1c).

Step 10 Check **Reboot On Update** check box to reboot the selected server after the one time boot device has been updated in the server.

Step 11 Click **Submit**.

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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **RAID Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Drive Security** window, check the **Configure Drive Security** check box to configure the security for the drive.

Step 6 Select the **Enable Drive Security** or **Disable Drive Security** radio buttons to enable or disable the security for the drive.

Note Enabling drive security will allow you to enter the security key details.

Step 7 Select **Enable Drive Security** and complete the following fields:

Field	Description
Local Key Management check box	This check box is selected by default.
Security Key field	Enter a security key.
Security Key Identifier field	Enter a security key identifier.
Confirm Security Key field	Confirm the previously entered security key.
Current Security Key field	Enter the key only when modifying the security key.

Note When Cisco IMC Supervisor exports a RAID policy with security keys, the security key parameters are left empty so that Cisco IMC Supervisor does not expose the security key. You must manually key in the values.

Step 8 On the **Virtual Drive Configuration** window, click + to add virtual drives that you want to configure on the server.

Step 9 Click + to add an entry to the virtual drives table. On the **Add Entry to Virtual Drives** page, complete the following:

Field	Description
Virtual Drive Name field	Check this check box to enable a specified password expiry duration and complete the following: **Password Expiry Duration** - Set the number of days for the password to expire.
Virtual Drive Size	
Disk Group Policy drop-down list	Select an existing Disk Group policy from the **Disk Group Policy** drop-down list or click + to add a new Disk Group policy to specify local disks. See . **Note** If two virtual drives are created and associated to the same Disk Group policy, they will share the same virtual drive group space.
Access Policy drop-down list	Select from the options listed.
Read Policy drop-down list	Select from the options listed.
Write Policy drop-down list	Select from the options listed.
IO Policy drop-down list	Select from the options listed.
Drive Cache drop-down list	Select from the options listed.

Field	Description
Expand to available check box	Expands the virtual drive size to use maximum capacity available on the disks.
Boot Drive check box	Sets the virtual drive you are creating as a boot drive. **Note** You cannot have more than one boot drive.
Set disks in JBOD state to Unconfigured Good check box	Sets the disks which are in JBOD state to unconfigured good state before they are used for virtual drive creation.
Enable Full Disk Encryption check box	Creates virtual drive from unused physical drives.

Step 10 Click **Submit**.
You can see the virtual drives you have created in the **Virtual Drives** table.

Step 11 Check the **Delete 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 may result in loss of existing data.

Step 12 Click **Next**.

Step 13 On the **Physical Drive Configuration** page, complete the following:

Step 14 Check **Configure Unused Disks** check box and select an option to configure the unused disks as either **Unconfigured Good** or **JBOD** state.

Note If you select **Unconfigured Good**, the **Clear Secure Drive** check box is displayed. If you select **JBOD**, the **Enable Secure Drive** check box is displayed.

Step 15 Check **Clear Secure Drive** to delete all data on the physical drive or check **Enable Secure Drive** to enable the secure drive.

Step 16 Click **Submit**.

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 IMC Supervisor. 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Serial Over LAN Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, 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 6 Click **Submit**.

SNMP Policy

Cisco IMC Supervisor 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **SNMP Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **SNMP Users** window, 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 6 Click **Next**.

Step 7 On the **SNMP Traps** window, 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 8 Click **Next**.

Step 9 On the **SNMP Settings** window, configure the SNMP properties.

Step 10 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 C-series server that is running Cisco IMC versions prior to 2.x; it must be excluded for such servers using the check box.
- The **SNMP Port** cannot be configured on a E-series server that is running Cisco IMC version 2.x; it must be excluded for such servers using the check box.

SSH Policy

The SSH server enables a 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **SSH Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 6 Click **Submit**.

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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **User Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, you can add users that need to be configured on the server to the **Users** list.

Step 6 Check **Enforce Strong Password** check box if you want to enforce strong password on users you will configure in the next step.
This feature is applicable only on servers running CIMC 2.0(9c) and above.

Step 7 Click + to add a user.

Step 8 On the **Add Entry to Users** window, complete the following fields:

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

Step 9 Click **Submit**.

Step 10 Check **Add Password Expiration Policy** check box to apply a Password Expiration policy.

Note You cannot apply a Password Expiration policy individually.

Step 11 Choose an existing Password Expiration policy from the drop-down list or click + to add a new Password Expiration policy. See Password Expiration Policy, on page 18.

Step 12 Click **Submit**.
You can also select an existing user from the **Users** table on the **Main** window 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 can change the password.
- For servers running CIMC older than version 2.0(8d), Cisco IMC Supervisor created dummy user entries on the server along with the ones defined in the policy. When you now apply the policy on servers running CIMC 2.0(8d) and higher, these blank user entries are no longer created. The previously existing dummy user entries (applied through an earlier policy) will now be cleared.
- Ensure that the account used to manage Cisco IMC Supervisor is not deleted from the user list in the policy. If deleted, Cisco IMC Supervisor loses connection to the server being managed.

Virtual KVM Policy

The KVM console is an interface accessible from Cisco IMC Supervisor 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** window, choose **Virtual KVM Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 Check the **Enable vKVM** check box.

Step 6 Choose or enter the virtual server properties or use the existing properties.

Step 7 Click **Submit**.

VIC Adapter Policy

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

Procedure

Step 1 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **VIC Adapter Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** screen. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** screen, click + to add a VIC adapter entry in the table.

Step 6 On the **Add Entry to VIC Adapters** screen and enter and 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 7 Click **Submit**.

vMedia Policy

You can use Cisco IMC Supervisor 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 IMC Supervisor - 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **vMedia Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.
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** window. See Creating a Policy from an Existing Configuration, on page 29.

Step 4 Check **Cisco UCS S3260** check box if the policy is for a Cisco UCS S3260 server and click **Next**.

Step 5 On the **Main** window, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 6 Click **Next**.

Step 7 Check the **Add CDD vMedia Mapping** check box and complete the CDD mapping details.

Step 8 Click **Next**.

Step 9 Check the Add **HDD vMedia Mapping** check box and complete the HDD mapping details.

Step 10 Click **Submit**.

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

Zoning Policy

Zoning policy is used to assign physical drives to a server. The Cisco UCS S3260 dense storage rack 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)
- Unassigning physical disks
- Viewing SAS expander properties
- Assigning physical drives to servers
- Moving physical drives as Chassis Wide Hot Spare
- Unassigning 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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 On the **Add** screen, choose **Zoning Policy** from the drop-down list and click **Submit**.

Step 3 Enter a name in the **Policy Name** field.

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** window. See Creating a Policy from an Existing Configuration, on page 29.

Note Zoning Policy is only applicable to Cisco UCS 3260 Rack Server. Hence, the **Cisco UCS S3260** check box in the UI is checked by default.

Step 4 On the **Zoning** window, click + to add local disks that you want to configure on the server.

Step 5 On the **Add Entry to Local Disks** window, enter **Slot Number** where the local disk is present .

Step 6 Select the local disk details such as the **Ownership** assigning the ownership of the local disk.

Step 7 Check the **Force** check box when assigning disks owned by one server to another server.

Step 8 Click **Submit**.

Step 9 Check the **Modify Physical Drive Power Policy** check box to set the policy.

Step 10 Select the power state from the **Physical Drive Power State** drop-down list.

Step 11 Click **Submit**.

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 Click **Add** after selecting **Hardware Policies**. For accessing this page, see Creating Hardware Policies, on page 81.

Step 2 Check **Create policy from current configuration of the server** check box and click **Next**.

Step 3 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. For Cisco UCS S3260 servers go to step 5.

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 on the **Credential Policy Add Form** screen.
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 4 Click **Next**.
You will go to the **Main** screen. Continue creating a policy.

Step 5 For Cisco UCS S3260 servers, check both the **Create policy from current configuration of the server** and **Cisco UCS S3260** check boxes and click **Next**.

Step 6 Check the **Enter Server Details Manually** check box in the **Server Details** screen and fill in the following fields or click **Select** to select a Cisco UCS S3260 server to apply the policy to.

1 Enter the Virtual Management IP address in the **Server IP** field for Cisco UCS S3260 platforms.

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.

Step 7 Select either Server Node 1or 2 radio buttons.

Step 8 Click **Next**.
You will go to the **Main** screen. Continue creating a policy.

Applying a Hardware Policy

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

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the Manage Policies and Profiles page, click **Hardware Policies**.

Step 3 Select a policy you want to apply.

Step 4 Click **Apply** from the options available at the top.
In the **Apply Policy** screen, you can either choose **Chassis** or **Server(s)** to which you want to apply the policy. These options are displayed based on either the User Administration or Compute Node policy you have selected.

Step 5 Click **Select** to select the chassis or servers to which you want to apply the policy.

Note For Cisco UCS 3260 type policies, chassis is shown as Administration policies and server is shown as Compute Node policies. See Policies and Profiles.

Step 6 Check the **Schedule Later** check box to schedule the apply policy task at a later time.

Step 7 Select an existing schedule from the **Schedule** drop-down list or click on + create a new schedule. See Creating Schedules.

Note You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.

Step 8 Click **Submit**.
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 server(s) to which the policy is being applied.

General Tasks Under Hardware 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** > **Manage Policies and Profiles**.

Step 2 On the Manage Policies and Profiles page, click **Hardware Policies**.

Step 3 Expand a policy from the left pane and select a policy in the **Hardware Policies** page. Perform the following optional steps:

a) (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 to a server. If you try to delete a policy which is associated to a profile, an error occurs.

b) (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.

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

d) (Optional) Click **View Details** to view the status of the policy you have applied and the server IP address to which you have applied the policy. If the policy is not successfully applied an error message is displayed in the **Status Message** column.

Step 4 To apply a policy to a server or server group, click **Apply**. For more information about applying a profile, see Applying a Hardware Policy, on page 30.

Step 5 Click **Submit** and/or **Close** if applicable.

Hardware Profiles

Multiple policies combined together form a hardware profile. You can apply configuration details of a rack hardware profile for example, to multiple rack-mount servers. You can associate this hardware 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 hardware profile in Cisco IMC Supervisor:

1. Create a hardware profile. You can create a profile in one of the following methods:
   a. Create a new profile. For more information about creating a new profile, see Creating a Hardware Profile, on page 32.
   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 33.
2. Apply the profile on a server. For more information about applying a profile, see Applying a Hardware Profile, on page 34.
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 General Tasks Under Hardware Profiles, on page 35.

Creating a Hardware Profile

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Hardware Profiles**.

Step 3 Click **Add**.

Step 4 In the **Hardware Profile** screen, enter a name for the profile that you want to create in the **Profile Name** field.
You can also check **Create profile from current configuration of the server** check box, if you want use the existing server configuration. This takes you to the **Server Details** screen. See Creating a Profile from an Existing Configuration.

Step 5 Check **Cisco UCS S3260** check box if the profile is for a Cisco UCS S3260 server and click **Next**.

Step 6 On the **Profile Entities** window, click + to add a profile entry.
You can also click the delete icon to delete existing entries.

Step 7 In the **Add Entry to Profile Name** window, choose **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 selected earlier. See Creating Hardware Policies, on page 3

Step 9 Select the servers to which you want to apply the policy to from the **Apply Policy To** drop-down list.

Step 10 Click **Submit**.

What to Do Next

You can also edit, delete or clone a profile, or view the server mapped to a selected profile. See General Tasks Under Hardware Profiles, on page 35

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 the current configuration of a server.

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the Manage Policies and Profiles page, click **Hardware Profiles**.

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. For Cisco UCS S3260 servers go to step 10.

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** window, 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 For Cisco UCS S3260 servers, check **Cisco UCS S3260** check box and click **Next**.

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

1. Enter the Virtual Management IP address in the **Server IP** field for Cisco UCS S3260 platforms.
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 you want to create from the servers, and click **Select**.

Step 10 Click **Next**.

Step 11 In the **Profile Entities** window, click + to add an entry to the profile name.
Click **x** to delete an existing entry from the **Profile Name** table.

Note For Cisco UCS S3260 profile type, only policies of platform type Cisco UCS S3260 can be added. If the policies are Compute Node type, you must specify the server node in the **Apply Policy To** field. For example, **Server-1**, **Server-2**, and **Both**. For Administration policies this field is not relevant.

Step 12 Click **Submit**.

Applying a Hardware Profile

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

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the Manage Policies and Profiles page, click **Hardware Profiles**.

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

On the **Apply Profile** screen, you can either choose **Chassis** (applicable for Cisco UCS S3260 type profiles) or **Server(s)** to which you want to apply the profile. These options are displayed based on the server platform you have selected.

Step 4 In the **Apply Profile** screen, click **Select** to select the chassis or servers to which you want to apply the profile.

Step 5 Check the **Schedule Later** check box to schedule the apply profile task at a later time.

Step 6 Select an existing schedule from the **Schedule** drop-down list or click on + create a new schedule. See Creating Schedules.

Note You can go to **Policies** > **Manage Schedules**, select a schedule and click **View Scheduled Tasks** to view the scheduled task or click **Remove Scheduled Tasks** to delete scheduled tasks.

Step 7 Click **Submit**.
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 servers to which the profile is being applied.

General Tasks Under Hardware 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** > **Manage Policies and Profiles**.

Step 2 On the Manage Policies and Profiles page, click **Hardware Profiles**.

Step 3 Expand the **Hardware Profile** and select a profile. Perform the following optional tasks:

a) (Optional) To delete a profile, click **Delete**. Click **Select** in the **Delete Profile** dialog box, select one or more profiles and click **Select**. Click **Submit** to delete a profile.
You can delete a profile even if it is associated to a server.

b) (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.

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

d) (Optional) To apply a profile to a server or server group, click **Apply**. See Applying a Hardware Profile, on page 34.

e) (Optional) Click **View Details** to view the status of the profile you have applied and the server IP address to which you have applied the profile. If the profile is not successfully applied an error message is displayed in the **Status Message** column.

Step 4 Click **Submit** and/or **Close** if applicable.

Host Image Mapping

Host Image Mapping is a commonly used feature for the E-Series servers. It allows customers to upload an ISO file before installing it. This feature provides an option to upload an iso file to the E-Series servers running CIMC.

You can perform various tasks such as adding, editing, and deleting mapped profiles from this page. See Adding Host Image Mapping Profile, on page 36.

Adding Host Image Mapping Profile

Procedure

Step 1 Choose **Policies** > **Manage Policies and Profiles**.

Step 2 On the **Manage Policies and Profiles** page, click **Host Image Mapping**.

Step 3 Click **Add**.

Step 4 On the Add Host Image Mapping Profile screen, complete 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 (only for FTP and SFTP servers)	The user name.
Password field (only for FTP and SFTP servers)	The user password.
Map After Download check box	Maps the downloaded image.
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

You can also edit, delete, or apply a profile. You can see if the image is downloaded successfully and if the downloaded images are mapped (if you have checked the **Map After Download** check box) successfully using the **View Status Details** option.

Tag Library

Tagging is when you assign a label to an object. As an administrator, you can decide to tag objects such as resource groups and user groups in Cisco IMC Supervisor. You can assign tags to a category such as a rack account. You can also apply a tag to a specific type of account in the selected category.

Tag Library has only one tab which displays the following details:

Field	Description
Name	User defined name of the tag library.
Description	User defined brief description of the tag library.
Type	String or an integer.
Possible Tag Values	User defined tag values.
Applies To	Rack mount servers or users.

Creating a Tag Library

Perform this procedure when you want to create a tag library.

Procedure

Step 1 Choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 In the **Create Tag** screen, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.
Description field	(Optional) A description of the tag.
Type drop-down list	Select String or Integer.
Possible Tag Values field	The possible values for the tag.

Step 4 Click **Next**.

Step 5 In the **Applicability Rules** pane, complete the following:

Name	Description
Taggable Entities field	Choose the entities on which the tag needs to be applied. To add an entity, do the following: **1** Click the + icon. **2** From the **Category** drop-down list, choose the category. It can be one of the following: • **Physical_Compute** • **Administration** **3** Choose the taggable entities from the table. **4** Click **Submit**. **Note** The tags are displayed under the respective category according to the set taggable entities.

Step 6 Click **Submit**.

Note You can perform various tasks such as cloning, editing, deleting, viewing tag and tag association details by clicking on the available options.

REST API and Orchestration

The **REST API Browser** screen lists all the APIs that are provided with Cisco IMC Supervisor that you can use. The APIs are categorized into the following groups:

- Firmware Management Tasks
- General Tasks
- Platform Tasks
- Policy Tasks
- Policy and Profile Tasks
- Server Tasks
- User and Group Tasks

You can use the controls on the screen to perform the following actions:

- Expand and collapse the entire list
- Add this screen to **Favorites**

- Use the **Search** or **Advanced Filter** options to locate a specific API
- Export the report
- Add servers to manage

For more information on how to use these APIs, see *Cisco IMC Supervisor REST API Cookbook* available at: http://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-programming-reference-guides-list.html.