Policies Menu

This chapter contains the following topics:

Policies Menu Options

The **Policies** menu contains the following menu options:

- Manage Policies and Profiles
- Tag Library

Managing Policies

The **Manage Policies and Profiles** menu displays the following tabs:

Tab	Description
Credential Policies	You can create a credential policy specifying a user name, password, protocol, and port. You can reuse the credentials specified in this policy for example, while creating a rack account. You can perform various tasks such as adding, editing, and deleting credential policies from this page. For information on performing these tasks, see Creating a Credential Policy.

Tab	Description
Manage Hardware Policies	A policy helps in categorically grouping and classifying the various characteristics of a server. You can create hardware policies by configuring various properties such as BIOS, LDAP, Users and so on. These policies can then be applied to a server or server groups. You can perform various tasks such as adding, editing, and deleting hardware policies from this page. For information on performing these tasks, see Hardware Policies.
Manage Hardware Profiles	A combination of existing set of policies make up a profile. You can apply configuration details of a rack hardware profile for example, to multiple servers. You can associate this hardware profile to specific servers. You can perform various tasks such as adding, editing, and deleting hardware profiles from this page. For information on performing these tasks, see Creating a Hardware Profile.

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.

Credential Policies

Creating a Credential Policy

Perform this procedure when you want to create a credential policy.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 Click **Add**.

Step 3 In the **Add Credential Policy** dialog box, 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 4 Click **Submit**.

Step 5 In the confirmation dialog box, click **OK**.

Note You can also perform the following policy tasks:

- Click **Edit** and modify a selected credential policy you created.
- Click **Clone** to copy the details of a selected credential policy to a new policy.
- Click **Delete** to delete a selected policy.
- Click **View** to view the credential policy details of a selected policy.
- Click **Apply** to apply a policy on a server or server group.
- Click **View Server Mappings** to see the list of the servers that the policy is associated to.

Editing a Credential Policy

Perform this procedure when you want to edit a credential policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to edit.

Step 3 Click **Edit**.

Note You cannot see the **Edit** button till you select the policy from the list.

Step 4 In the **Modify Credential Policy** dialog box, edit the following fields:

Field	Description
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.

Note You cannot change the name of the policy.

Step 5 Click **Submit**.

Step 6 In the confirmation dialog box, click **OK**.

Cloning a Credential Policy

Perform this procedure when you want to create a new credential policy based on another policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to clone.

Step 3 Click **Clone**.

Note You cannot see the **Clone** button till you select the policy from the list.

Step 4 In the **Clone Credential Policy** dialog box, 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**.

Step 6 In the confirmation dialog box, click **OK**.

Deleting a Credential Policy

Perform this procedure when you want to delete a credential policy.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to delete.

Step 3 Click **Delete**.

Note You cannot see the **Delete** button till you select the policy from the list.

Step 4 In the **Delete Credential Policy** dialog box, click **Delete**.

Step 5 In the confirmation dialog box, click **OK**.

Viewing a Credential Policy Details

Perform this procedure when you want to view a credential policy details.

Before You Begin

The policy has already been created under **Credential Policies**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies** > **Credential Policies**.

Step 2 From the list of policies, select the policy you want to view.

Step 3 Click **View**.

Note You cannot see the **View** button till you select the policy from the list.

Step 4 You can view the details in the **Credential Policy Details** dialog box.

Step 5 Click **Close** to go back to the previous screen.

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.

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 7.
   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 21.
2. Apply the policy on a server. For more information about applying a policy, see Applying a Policy, on page 21.
3. Perform any of the following optional tasks on the policy:
   a. Edit
   b. Delete
   c. Clone

   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 22.

   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 25.

Creating Hardware Policies

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

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

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

Step 3 Click **Add**.

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

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
BIOS Policy, on page 8	*Configuring BIOS Settings*
Disk Group Policy, on page 9	*Managing Storage Adapters*
IPMI Over LAN Policy, on page 9	*Configuring IPMI*
LDAP Policy, on page 10	*Configuring the LDAP Server*
Legacy Boot Order Policy, on page 11	*Server Boot Order*
Network Security Policy, on page 12	*Network Security Configuration*
NTP Policy, on page 13	*Configuring Network Time Protocol Settings*
Precision Boot Order Policy, on page 13	*Configuring the Precision Boot Order*
RAID Policy, on page 14	*Managing Storage Adapters*
Serial Over LAN Policy, on page 15	*Configuring Serial Over LAN*
SNMP Policy, on page 16	*Configuring SNMP*
SSH Policy, on page 17	*Configuring SSH*
User Policy, on page 17	*Configuring Local Users*
VIC Adapter Policy, on page 19	*Viewing VIC Adapter Properties*
Virtual KVM Policy, on page 19	*Configuring the Virtual KVM*

Policy Type	Sections in the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
vMedia Policy, on page 20	*Configuring Virtual Media*

What to Do Next

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

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 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **BIOS 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Note If some properties or attributes in Cisco IMC Supervisor 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 4 In the **Main** dialog box, select values for the main BIOS properties such as **Boot Option Retry**, **Post Error Pause**, and **TPM Support** drop-down lists.

Step 5 In the **Advanced** dialog box, choose the BIOS property values from the drop-down lists and click **Next**.

Step 6 In the **Server Management** dialog box, choose the server property values from the drop-down lists and click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

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 RAID Policy, on page 14.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, 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 In the **Virtual Drive Configuration** dialog box, choose the virtual drive properties and click **Next**.

Step 5 In the **Local Disk Configuration** dialog box, click + to add an entry to reference a local disk configuration and click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

Step 7 Click **Submit** in the **Main** dialog box.

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

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

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 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.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

LDAP Policy

Cisco C-series and E series servers support LDAP and Cisco IMC Supervisor 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 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **LDAP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, fill in the LDAP properties.

Step 5 Click **Next**.

Step 6 In the **LDAP Servers** dialog box, fill in the LDAP server details.

Step 7 Click **Next**.

Step 8 In the **Group Authorization** dialog box, fill in the group authorization details and click + to add an LDAP group entry to the table.

Step 9 In the **Add Entry to LDAP Groups** dialog box, fill in the group details.

Step 10 Click **Submit**.

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

Step 12 Click **Submit** in the **Group Authorization** dialog box.

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

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. removed and replaced with whatever role groups are 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).

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. For more information about precision boot order, see Precision Boot Order Policy, on page 13.

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 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, click + and select the device type from the drop-down list. The table lists the devices you have added.

In the **Select Devices** table, select an existing device and click **x** to delete a device. Use the up and down arrow icons to re-order the entries. The order of entries in the table determines the boot order.

You cannot add the same device type again.

Step 5 Click **Submit** in the **Add Entry to Select Devices** dialog box.

Step 6 In the **Submit Result** dialog box, click **OK**.

Step 7 Click **Submit** in the **Main** dialog box.

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

Note This policy is applicable only for Cisco IMC versions prior to 2.0. An error message is displayed if the policy is applied to a server running higher Cisco IMC versions. Use Precision Boot Order policy instead.

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.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **Network Security** 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, check **Enable IP Blocking** checkbox to block the IP, and enter attributes to set IP Blocking properties.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **NTP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

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

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **Precision 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, check UEFI Secure Boot check box or select the boot mode from the **Configure Boot Mode** drop-down list.

Step 5 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 6 Click **Submit** in the **Add Entry to Select Devices** dialog box.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Click **Submit** in the **Main** dialog box.

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

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **RAID 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, click + to add virtual drives that you want to configure on the server to the **Virtual Drives** list.

Step 5 In the **Add Entry to Virtual Drives** dialog box, enter or select the virtual drive details.
You can either select an existing Disk Group policy from the drop-down list and edit or add a new Disk Group policy to specify local disks. To create a Disk Group policy, refer Disk Group Policy, on page 9.

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

Step 6 Click **Submit** in the **Add Entry** dialog box.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Check the **Erase existing Virtual Drives** check box to delete all existing virtual drives on the server.
If you select this check box, all existing virtual drives on the server will be deleted when the policy is applied. This results in loss of existing data.

Step 9 Check the **Configure remaining disks as JBOD** check box to configure the remaining disks as JBOD.
This option is applicable only on storage controllers that support JBOD. The disks that are not used for virtual drives or hotspares are configured as JBOD.

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

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

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **Serial 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, check the **Enable SoL** check box and select the **CoM Port** and **Baud Rate** values from the drop-down list or use the existing values.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **SNMP 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **SNMP Users** dialog box, click + to add a SNMP user and fill in the user details. You can use the + icon to add up to 15 SNMP Users.
Select an existing SNMP entry to edit or delete an entry from the table.

Step 5 Click **Next**.

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

Step 7 Click **Next**.

Step 8 In the **SNMP Settings** dialog box, configure the SNMP properties.

Step 9 Click **Submit**.

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

Note
- Any existing **SNMP Users** or **SNMP Traps** configured previously on the server are removed and replaced with users or traps that you configured in the policy. If you have not added any users or traps into the policy, the existing users or traps on the server are removed but not replaced.
- The **SNMP Port** cannot be configured on a 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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **SSH 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, check **Enable SSH** check box, and enter SSH properties or use the existing properties.

Step 5 Click **Submit**.

Step 6 In the **Submit Result** dialog box, click **OK**.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **User 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, you can add users that need to be configured on the server to the **Users** list.

Step 5 Click + to add a user.

Step 6 In the **Add Entry to Users** dialog box, complete the following fields:

Option	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.
Enabled	Check this check box to activate the user.
NewPassword	Enter a password associated with the username.
Confirm New Password	Repeat the password from the previous field.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
You can also select an existing user from the **Users** table in the **Main** dialog box and click **Edit** or **Delete** icons to edit or delete a user.

Note
- The first user in the **Users** table is the admin user. You cannot delete this admin user but can change the password.
- When you apply a user policy, the user entries in Cisco IMC Supervisor are replaced with the user entries you created. Blank entries in Cisco IMC are replaced with default users from Cisco IMC Supervisor. The default user role is always read-only and the user is disabled.
- Ensure that the account used to manage the Cisco IMC Supervisor is not deleted from the user list in the policy. If deleted, the Cisco IMC Supervisor will lose 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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **Virtual KVM 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 Check the **Enable vKVM** check box.

Step 5 Choose or enter the virtual server properties or use the existing properties.

Step 6 Click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

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 Click **Add** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **VIC Adapter 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, click + to add a VIC adapter entry in the table.

Step 5 In the **Add Entry to VIC Adapters** dialog box and 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 6 Click **Submit**.

Step 7 In the **Submit Result** dialog box, click **OK**.

Step 8 Click **Submit** in the **Main** dialog box.

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

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

Step 2 In the **Add** dialog box, choose **vMedia 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** dialog box. For information on performing tasks in this dialog box, refer Creating a Policy from an Existing Configuration, on page 21.

Step 4 In the **Main** dialog box, check the **Enable vMedia** check box to enable vMedia and check the **Enable Virtual Media Encryption** for enabling vMedia encryption.

Step 5 Click **Next**.

Step 6 Check the **Add CDD vMedia Mapping** check box and complete the CDD mapping details.

Step 7 Click **Next**.

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

Step 9 Click **Submit**.

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

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.

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** in the **Manage Hardware Policies** page. For more information about how to go to this page, see Creating Hardware Policies, on page 7.

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:

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

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

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

Step 4 Click **Next**.
You will go to the **Main** dialog box. Continue creating a policy.

Applying a Policy

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

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies**.

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

Step 3 Select a policy you want to apply from the left pane.

Step 4 Click **Apply** from the options available at the top.

Step 5 In the **Apply Policy** dialog box, choose the server or server group from the drop-down list based on whether you want to apply the policy to individual servers or an entire rack server group.

Step 6 Click **Select** to select the server groups or servers to which you want to apply the policy.

Step 7 Click **Submit**.

Step 8 In the **Submit Result** dialog box, click **OK**.
The process of applying the policy to the specified set of servers begins. This process can take a few minutes depending on the policy type and network connectivity to 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 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

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

Step 3 Expand a policy from the left pane and select a policy in the **Manage 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 only if you have not associated the policy with a server. If you have associated a policy to a server, re-associate the server with a different policy or the same policy after modifying it.

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 Policy, on page 21.

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 policy 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 23.
   b. Create a profile from the configuration existing on a server. For more information about creating a profile from the configuration existing on a server, see Creating a Profile from an Existing Configuration, on page 24.
2. Apply the profile on a server. For more information about applying a profile, see Applying a Hardware Profile, on page 25.
3. Perform any of the following optional tasks on the profile.
   a. Edit
   b. Delete
   c. Clone

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

Creating a Hardware Profile

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

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

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

Step 3 Click **Add**.

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

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

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

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

Step 8 Select the policy name from the **Policy Name** drop-down list which lists the names of policies you have already created.
You can click the + next to **Policy Name** to create a new policy based on the policy type you have selected earlier. For more information about creating policies, see Creating Hardware Policies, on page 7

Step 9 Click **Submit**.

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

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

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

What to Do Next

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

Creating a Profile from an Existing Configuration

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

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

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

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

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

Step 3 Click **Add**.

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

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

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

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

6 Enter the port number associated with the selected protocol in the **Port** field.

7 Click **Select**, select the policies, and click **Select**.

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

Step 6 Click **Next**.

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

Step 8 Click **Submit**.

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

Applying a Hardware Profile

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

Procedure

Step 1 From the menu bar, choose **Policies** > **Manage Policies and Profiles**.

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

Step 3 Select an existing hardware profile and click **Apply** from the options listed above.

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

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

Step 6 Click **Submit**.

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

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 From the menu bar, choose **Policies** > **Manage Policies and Profiles** > **Manage Hardware Profiles**.

Step 2 Expand the Hardware Profile in the left pane and select a profile in the **Manage Hardware Profiles** page.
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 cannot delete a profile which is associated to a server. You must associate a different profile to the server before deleting it.

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**. For more information about applying a profile, see Applying a Hardware Profile, on page 25.

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 3 Click **Submit** and/or **Close** if applicable.

Tagging Task Under Tag Library

Creating a Tag Library

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

Before You Begin

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 In the **Create Tag** dialog box, 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** screen, 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 In the confirmation dialog box, click **OK**.

Step 7 In the **Create Tag** dialog box, click **Submit**.

Step 8 Click **OK**.

Cloning a Tag Library

Perform this procedure when you want to create a new tag library based on another tag library.

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to clone.

Step 3 Click **Clone**.

Note You cannot see the **Clone** button till you select the tag library from the list.

Step 4 In the **Clone Tag** dialog box, complete the following fields for **Tag Details**:

Field	Description
Name field	A descriptive name for the tag.

Field	Description
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 5 Click **Next**.

Step 6 In the **Applicability Rules** screen, 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 7 In the confirmation dialog box, click **OK**.

Step 8 Click **Submit**.

Step 9 Click **OK**.

Editing a Tag Library

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

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to edit.

Step 3 Click **Edit**.
You cannot see the **Edit** button till you select the tag library from the list.

Step 4 In the **Edit Tag** dialog box, 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 5 Click **Next**.

Step 6 In the **Applicability Rules** screen, 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 7 In the confirmation dialog box, click **OK**.

Step 8 Click **Submit**.

Step 9 Click **OK**.

Deleting a Tag Library

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

Before You Begin

The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to delete.

Step 3 Click **Delete**.

Note You cannot see the **Delete** button till you select the tag library from the list.

Step 4 In the **Tag** dialog box, click **Delete**.

Step 5 In the confirmation dialog box, click **OK**.

Viewing a Tag Details

Perform this procedure when you want to view a tag library details.

Before You Begin

- The tag library has already been created under **Tag Library**.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to view.

Step 3 Click **View**.

Note You cannot see the **View** button till you select the tag library from the list.

Step 4 You can view the details in the **Tag Details** dialog box.

Step 5 Click **Close** to go back to previous screen.

Viewing a Tag Association Details

Perform this procedure when you want to view a tag library association details.

Before You Begin

The tag library has already been created under **Tag Library** and has been associated with an entity.

Procedure

Step 1 From the menu bar, choose **Policies** > **Tag Library**.

Step 2 From the list of tag libraries, select the tag library you want to view.

Step 3 Double-click the tag library from the list or click the tag library from the list and click **View Details**.

Note You cannot see the **View Details** button till you select the tag library from the list.

You can view the following details in the **Tag Association** page:

Field	Description
Tag Name	The descriptive name for the tag.
Associated Resource Entity	The value of the entity.
Resource Entity Type	The resource type of the entity.
Tag Value	The value of the tag.

Step 4 Click **Close** to go back to previous screen.