Configuring Network-Related Settings

This chapter includes the following sections:

Server NIC Configuration

Server NICs

NIC Mode

The NIC mode setting determines which ports can reach the CIMC. The following network mode options are available, depending on your platform:

- **Dedicated**—The management port is used to access the CIMC.
- **Shared LOM**—Any LOM (LAN On Motherboard) port can be used to access the CIMC.
- **Shared LOM 10G**—Any 10G LOM port can be used to access the CIMC. This option is only available for some adapter cards.
- **Cisco Card**—Any port on the adapter card can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with Network Communications Services Interface protocol (NCSI) support.
- **Shared LOM Extended**—Any LOM port or adapter card port can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with NCSI support.

NIC Redundancy

The following NIC redundancy options are available, depending on the selected NIC mode and your platform:

- **none**—Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem.
- **active-active**—If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC.
- **active-standby**—If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode.

Note If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the *Hardware Installation Guide* (HIG) for the type of server you are using. The C-Series HIGs are available at the following URL: http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before You Begin

You must log in as a user with admin privileges to configure the NIC.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **NIC Properties** area, update the following properties:

Name	Description
NIC Mode drop-down list	Determines the ports that can be used to access the CIMC. This can be one of the following: • **Dedicated**—The management port is used to access the CIMC. • **Shared LOM**—Any LOM (LAN On Motherboard) port can be used to access the CIMC. • **Shared LOM 10G**—Any 10G LOM port can be used to access the CIMC. This option is only available for some adapter cards. • **Cisco Card**—Any port on the adapter card can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with Network Communications Services Interface protocol (NCSI) support. • **Shared LOM Extended**—Any LOM port or adapter card port can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with NCSI support. **Note** If you select any of the shared LOM options, make sure that all host ports belong to the same subnet.
NIC Redundancy drop-down list	The available NIC redundancy options depend on the selected NIC mode and the model of the server that you are using. If you do not see a particular option, then it is not available for the selected mode or server model. This can be one of the following: • **none**—Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem. • **active-active**—If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC. • **active-standby**—If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode. **Note** If you select this option, make sure all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.
MAC Address field	The MAC address of the CIMC network interface selected in the **NIC Mode** field.

Step 5 Click **Save Changes**.

Configuring Common Properties

Use common properties to describe your server.

Before You Begin

You must log in as a user with admin privileges to configure common properties.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **Hostname** field, enter the name of the host.
Step 5 Click **Save Changes**.

Configuring IPv4

Before You Begin

You must log in as a user with admin privileges to configure IPv4.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **IPv4 Properties** area, update the following properties:

Name	Description
Enable IPv4 check box	If checked, IPv4 is enabled.
Use DHCP check box	If checked, the CIMC uses DHCP.
IP Address field	The IP address for the CIMC.
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The gateway for the IP address.

Name	Description
Obtain DNS Server Addresses from DHCP check box	If checked, the CIMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 5 Click **Save Changes**.

Connecting to a VLAN

Before You Begin

You must be logged in as admin to connect to a VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **VLAN Properties** area, update the following properties:

Name	Description
Enable VLAN check box	If checked, the CIMC is connected to a virtual LAN. **Note** You can configure a VLAN or a port profile, but you cannot use both. If you want to use a port profile, make sure this check box is not checked.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 Click **Save Changes**.

Connecting to a Port Profile

Note You can configure a port profile or a VLAN, but you cannot use both. If you want to use a port profile, make sure the **Enable VLAN** check box in the **VLAN Properties** area is not checked.

Before You Begin

You must be logged in as admin to connect to a port profile.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **Port Profile** area, update the following properties:

Name	Description
Port Profile field	The port profile CIMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC1225 Virtual Interface Card. Enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. **Note** The port profile must be defined on the switch to which this server is connected.

Step 5 Click **Save Changes**.

Network Security Configuration

Network Security

The CIMC uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. CIMC bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before You Begin

You must log in as a user with admin privileges to configure network security.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Security** tab.

Step 4 In the **IP Blocking Properties** area, update the following properties:

Name	Description
Enable IP Blocking check box	Check this box to enable IP blocking.
IP Blocking Fail Count field	The number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the **IP Blocking Fail Window** field. Enter an integer between 3 and 10.
IP Blocking Fail Window field	The length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
IP Blocking Penalty Time field	The number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.

Step 5 Click **Save Changes**.