



Configuring Network-Related Settings

This chapter includes the following sections:

- [Server NIC Configuration, on page 1](#)
- [Common Properties Configuration, on page 5](#)
- [Configuring IPv4, on page 7](#)
- [Configuring IPv6, on page 7](#)
- [Connecting to a VLAN, on page 8](#)
- [Connecting to a Port Profile, on page 9](#)
- [Configuring Interface Properties, on page 10](#)
- [Network Security Configuration, on page 11](#)
- [Network Time Protocol Settings, on page 12](#)
- [Pinging an IP Address from the Web UI, on page 14](#)

Server NIC Configuration

Server NICs

NIC Mode

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

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



Note **Shared LOM Extended** and **Shared LOM 10G** are available only on some UCS C-Series servers.

NIC Redundancy

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

- **none**—Each port that is 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 that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC.



Note When using **active-active**, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using **active-standby**.

- **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode.



Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN 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 Cisco IMC
NIC Mode drop-down list	<p>The ports that can be used to access Cisco IMC. This can be one of the following:</p> <ul style="list-style-type: none"> • Dedicated—The management port that is used to access the Cisco IMC. • Shared LOM—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC. • Shared LOM 10G—Any 10G LOM port can be used to access the Cisco IMC. • Cisco Card—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI). • Shared LOM Extended—Any LOM port or Cisco adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support. <p>Note Shared LOM Extended and Shared LOM 10G are available only on some UCS C-Series servers.</p> <p>Note If you choose any of the shared LOM options, make sure that all host ports belong to the same subnet.</p>

Name	Description Cisco IMC
VIC Slot drop-down list	<p>The VIC slot that can be used for management functions in Cisco card mode. This can be one of the following:</p> <p>For C220 M4 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 1 is selected. • Riser 2— Slot 2 is selected. • FLEX LOM—Slot 3 (MLOM) is selected. <p>For C240 M4 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 2 is the primary slot, but you can also use slot 1. • Riser 2— Slot 5 is the primary slot, but you can also use slot 4. • FLEX LOM—Slot 7 (MLOM) is selected. <p>The following options are available only on some UCS C-Series servers:</p> <ul style="list-style-type: none"> • 4 • 5 • 9 • 10 <p>Note This option is available only on some UCS C-Series servers.</p>
SIOC Slot drop-down list	<p>Configures Cisco IMC network mode. Based on the card present in the System IO Controller (SIOC1), network mode can be changed to either Cisco card mode or Shared LOM mode.</p> <p>Note This option is available only on some UCS C-Series servers.</p>

Name	Description Cisco IMC
NIC Redundancy drop-down list	<p>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, it is not available for the selected mode or server model.</p> <p>This can be one of the following:</p> <ul style="list-style-type: none"> • none—Each port that is 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 that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to Cisco IMC. <p>Note When using active-active, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using active-standby.</p> <ul style="list-style-type: none"> • active-standby—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode. <p>Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same VLAN to ensure that traffic is secure regardless of which port is used.</p>
MAC Address field	The MAC address of the Cisco IMC network interface that is selected in the NIC Mode field.

Step 5 Click **Save Changes**.

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

The Dynamic Host Configuration Protocol (DHCP) enhancement is available with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname, which is now added to the options field of the DHCP packet, sent in the DHCP DISCOVER packet that was initially sent to the DHCP server.

The default hostname of the server is changed from ucs-c2XX to CXXX-YYYYYY, where XXX is the model number and YYYYYY is the serial number of the server. This unique string acts as a client identifier, allows

you to track and map the IP addresses that are leased out to Cisco IMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server from Cisco IMC. You can enable Dynamic DNS by using either the web UI or CLI. When you enable the DDNS option, the DDNS service records the current hostname, domain name, and the management IP address and updates the resource records in the DNS server from Cisco IMC.



Note

The DDNS server deletes the prior resource records (if any) and adds the new resource records to the DNS server if any one of the following DNS configuration is changed:

- Hostname
- Domain name in the LDAP settings
- When DDNS and DHCP are enabled, if the DHCP gets a new IP address or DNS IP or domain name due to a change in a network or a subnet.
- When DHCP is disabled and if you set the static IP address by using CLI or web UI.
- When you enter the **dns-use-dhcp** command.

Dynamic DNS Update Domain— 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 the Cisco IMC for the DDNS update.

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 Common Properties area, update the following properties:
 - a) In the **Hostname** field, enter the name of the host.

By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

Note If DHCP is enabled, the DHCP DISCOVER packet sent out will also carry the Cisco IMC hostname in it.

- b) Check the **Dynamic DNS** check box.
- c) In the **Dynamic DNS Update Domain** field, enter the domain name.

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, Cisco IMC uses DHCP.
IP Address field	The IP address for Cisco IMC.
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The gateway for the IP address.
Obtain DNS Server Addresses from DHCP check box	If checked, Cisco IMC 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**.

Configuring IPv6

Before you begin

You must log in as a user with admin privileges to configure IPv6.

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 **IPv6 Properties** area, update the following properties:

Name	Description
Enable IPv6 check box	If checked, IPv6 is enabled.
Use DHCP check box	If checked, the Cisco IMC uses DHCP. Note Only stateful DHCP is supported.
IP Address field	The IPv6 address for the Cisco IMC. Note Only global unicast addresses are supported.
Prefix Length field	The prefix length for the IPv6 address. Enter a value within the range 1 to 127. The default value is 64.
Gateway field	The gateway for the IPv6 address. Note Only global unicast addresses are supported.
Obtain DNS Server Addresses from DHCP check box	If checked, the Cisco IMC retrieves the DNS server addresses from DHCP. Note You can use this option only when the Use DHCP option is enabled.
Preferred DNS Server field	The IPv6 address of the primary DNS server.
Alternate DNS Server field	The IPv6 address of the secondary DNS server.
Link Local Address field	The link local address for the IPv6 address.
Stateless Address Auto Configuration field	The Stateless Address Auto Configuration (SLAAC) depends on the Router Advertisement (RA) of the network.

- 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 Cisco IMC 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 that 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	<p>The port profile that Cisco IMC uses to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC 1225 Virtual Interface Card.</p> <p>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.</p> <p>Note The port profile must be defined on the switch to which this server is connected.</p>

Step 5 Click **Save Changes**.

Configuring Interface Properties

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the Cisco IMC management port. Auto Negotiation mode can be set for dedicated mode only. When auto negotiation is enabled the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. When auto negotiation is disabled, you can configure the network port speed (10 Mbps, 100 Mbps, or 1 Gbps) and set the duplex value at either full or half.

Port Properties can be managed in the following two modes:

- **Admin Mode**—You can configure the network speed and duplex values by disabling the **Auto Negotiation** option. The default value of the network speed in the admin mode is 100 Mbps and the duplex mode is set to Full. Before changing the network speed ensure that the switch you connected to has the same port speed.
- **Operation Mode**—Displays the operation network port speed and duplex values. If you enabled auto negotiation mode, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed.

When you reset Cisco IMC 1.5(x), 2.0(1), and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default.

For C3160 servers, if you reset to factory defaults, **Dedicated** mode is configured to **Full** duplex mode with 100 Mbps speed by default.

Configuring Interface Properties

The settings on the switch must match with the Cisco IMC settings to avoid any speed or duplex mismatch.



Important

This action is available only on some UCS C-Series servers.

Procedure

- Step 1** Log in to Cisco IMC Web UI.
- Step 2** In the **Navigation** pane, click the **Admin** tab.
- Step 3** On the **Admin** tab, click **Network**.
- Step 4** In the **Network** pane, click the **Network Settings** tab.
- Step 5** In the **NIC Properties** area, select **Dedicated** mode from the **NIC Mode** drop down list.
NIC mode must be in dedicated to set any network configuration like net speed and duplex.
- Step 6** In the **Port Properties** area:
- If you check the **Auto Negotiation** check box, the setting for duplex will be ignored by the system. The Cisco IMC retains the speed at which the switch is configured.
 - If you uncheck the **Auto Negotiation** check box, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value.
- By default, the duplex mode is set to **Full**.
- Step 7** Click **Save Changes**.
-

Network Security Configuration

Network Security

The Cisco IMC 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. Cisco IMC 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 In the **IP Filtering** area, update the following properties:

Name	Description
Enable IP Filtering check box	Check this box to enable IP filtering.
IP Filter fields	To provide secure access to the server, you can now set a filter to allow only a selected set of IPs to access it. This option provides four slots for storing IP addresses (IP Filter 1, 2, 3, and 4). You can either assign a single IP address or a range of IP addresses while setting the IP filters. Once you set the IP filter, you would be unable to access the server using any other IP address.

Step 6 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

By default, when Cisco IMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure Cisco IMC to synchronize the time with an NTP server. The NTP server does not run in Cisco IMC by default. 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 or time source servers. When you enable the NTP service, Cisco IMC synchronizes the time with the configured NTP server. The NTP service can be modified only through Cisco IMC.



Note To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

Configuring Network Time Protocol Settings

Configuring NTP disables the IPMI Set SEL time command.

Before you begin

You must log in with admin privileges to perform this task.

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 **NTP Settings** tab.
- Step 4** In the **NTP Settings** area, update the following properties:

Name	Description
Enable NTP	Check this box to enable the NTP service.
Server 1	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 2	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 3	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Server 4	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Status message	Indicates whether or not the server is able to synchronize its time with the remote NTP server. This can be one of the following: <ul style="list-style-type: none">• synchronized to NTP server (RefID) at stratum 7— When the NTP service is enabled and multiple or individual IPv4 or IPv6 based NTP servers are added.• unsynchronized — When the NTP service is enabled and an unknown or unreachable server is added.• NTP service disabled — When the NTP service is disabled.

- Step 5** Click **Save Changes**.

Pinging an IP Address from the Web UI

Effective with this release, you can ping an IP address from the Cisco IMC web UI using a **Ping** button available on the toolbar. This would help validate the network connectivity to the IP address available in Cisco IMC. You can ping an IPv4, IPv6 or a host IP address using this button.

Before you begin

You must log in with user or admin privileges to perform this task.

Procedure

Step 1 In the toolbar above the work pane, click the **Ping** icon.

Step 2 In the **Ping Details** dialog box, update the following fields:

Name	Description
Hostname/IP Address column	Hostname or IP address you want to reach out to.
Number of Retries column	The maximum number of retries allowed to ping the IP address. The default value is 3. The valid range is from 1 to 10.
Timeout column	The maximum response time for a pinging activity. The default value is 10 seconds. The valid range is from 1 to 20 seconds.
Ping Status area	Displays results of the pinging activity.

Step 3 Click **Ping**.