



# Configuring Network-Related Settings

---

This chapter includes the following sections:

- [Server NIC Configuration, on page 1](#)
- [Common Properties Configuration, on page 7](#)
- [Configuring IPv4, on page 9](#)
- [Configuring IPv6, on page 10](#)
- [Connecting to a VLAN, on page 11](#)
- [Connecting to a Port Profile, on page 11](#)
- [Configuring Individual Settings, on page 13](#)
- [Network Security Configuration, on page 14](#)
- [Network Time Protocol Settings, on page 15](#)

## 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.
- **Cisco Card**—Any port on the adapter card that can be used to access the Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI).
- **Shared LOM**—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC.
- **Shared LOM Extended**—Any LOM port or 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** and **Shared LOM Extended** ports are available only on some C-series servers.

---



---

**Note** For other UCS C-Series M4 and M5 servers, the NIC mode is set to **Shared LOM Extended** by default.

---

#### Default NIC Mode Setting:

- For UCS C-Series C125 M5 servers and S3260 servers, the **NIC Mode** is set to **Cisco Card** by default.

#### NIC Redundancy

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

- **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 the Cisco IMC.
- **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 subnet to ensure that traffic is secure regardless of which port is used.

---

- **None**—In *Dedicated* mode, NIC redundancy is set to *None*.

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](http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html)

#### VIC Slots

The VIC slot that can be used for management functions in Cisco card mode.

For C125 M5, VIC slot option is **Riser 2**.

For C220 M4, C220 M5 and C240 M5 servers, VIC slot options are as follows:

- **Riser 1**—Slot 1 is selected.
- **Riser 2**—Slot 2 is selected.
- **FLEX LOM**—Slot 3 (MLOM) is selected.

For C240 M4 servers, VIC slot options are as follows:

- **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.

For C480 M5 ML servers, Cisco card mode slot is Slot 11 and Slot 12.

The following options are available only on some UCS C-Series servers:

- 4
- 5
- 9
- 10



**Note** This option is available only on some UCS C-Series servers.

## 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **NIC Properties** area, update the following properties:

Name	Description
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"> <li>• <b>Dedicated</b>—The management port that is used to access the Cisco IMC.</li> <li>• <b>Cisco Card</b>—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).</li> </ul> <p><b>Default NIC Mode Setting:</b></p> <ul style="list-style-type: none"> <li>• For UCS C-Series C125 M5 servers and S3260 servers, the <b>NIC Mode</b> is set to <b>Cisco Card</b> by default.</li> </ul>

Name	Description
VIC Slot drop-down list	

Name	Description
	<p>The VIC slot that can be used for management functions in Cisco card mode.</p> <p>For C220 M6, VIC slot options are as follows:</p> <p><b>Note</b> For C220 M6 , after resetting to factory default settings, the slot precedence is as follows:</p> <ul style="list-style-type: none"> <li>a. mLOM</li> <li>b. Riser 1 - Slot 1</li> <li>c. Riser 3 - Slot 3</li> </ul> <p>For C125 M5, VIC slot option is <b>Riser 2</b>.</p> <p>For C220 M4, C220 M5 and C240 M5 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Riser 1</b>—Slot 1 is selected.</li> <li>• <b>Riser 2</b>—Slot 2 is selected.</li> <li>• <b>FLEX LOM</b>—Slot 3 (MLOM) is selected.</li> </ul> <p>For C240 SD M5 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> <li>• For servers with PCIe Riser 1 and 2B combination: <ul style="list-style-type: none"> <li>• If you select Riser1, you must install the VIC in slot 2.</li> <li>• If you select Riser2, you must install the VIC in slot 5.</li> </ul> </li> <li>• For servers with PCIe Riser 1C and 2E combination: <ul style="list-style-type: none"> <li>• If you select Riser1, you must install the VIC in slot 1.</li> <li>• If you select Riser2, you must install the VIC in slot 2.</li> </ul> </li> <li>• If you select Flex-LOM, you must install an mLOM-style VIC in the mLOM slot.</li> </ul> <p>For C480 M5 ML servers, Cisco card mode slot is Slot 11 and Slot 12.</p> <p>The following options are available only on some UCS C-Series servers:</p> <ul style="list-style-type: none"> <li>• 4</li> <li>• 5</li> <li>• 9</li> <li>• 10</li> </ul> <p>For C240 M4 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Riser 1</b>—Slot 2 is the primary slot, but you can also use slot 1.</li> </ul>

Name	Description
	<ul style="list-style-type: none"> <li>• <b>Riser 2</b>—Slot 5 is the primary slot, but you can also use slot 4.</li> <li>• <b>FLEX LOM</b>—Slot 7 (MLOM) is selected.</li> </ul> <p><b>Note</b> This option is available only on some UCS C-Series servers.</p>
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"> <li>• <b>Riser 1</b>—Slot 1 is selected.</li> <li>• <b>Riser 2</b>— Slot 2 is selected.</li> <li>• <b>FLEX LOM</b>—Slot 3 (MLOM) is selected.</li> </ul> <p>For C240 M4 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Riser 1</b>—Slot 2 is the primary slot, but you can also use slot 1.</li> <li>• <b>Riser 2</b>— Slot 5 is the primary slot, but you can also use slot 4.</li> <li>• <b>FLEX LOM</b>—Slot 7 (MLOM) is selected.</li> </ul> <p>The following options are available only on some UCS C-Series servers:</p> <ul style="list-style-type: none"> <li>• 4</li> <li>• 5</li> <li>• 9</li> <li>• 10</li> </ul> <p><b>Note</b> 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 1 or 2.</p> <p><b>Note</b> This option is available only on some UCS S-Series servers.</p>

Name	Description
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"> <li>• <b>active-active</b>—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.</li> <li>• <b>active-standby</b>—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.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• When using <b>active-active</b>, do not configure a port-channel in the upstream switch for the member interfaces. A port-channel can be configured when using <b>active-standby</b>.</li> </ul> <ul style="list-style-type: none"> <li>• <b>None</b>—In <i>Dedicated</i> mode, NIC redundancy is set to <i>None</i>.</li> </ul>
MAC Address field	The MAC address of the Cisco IMC network interface that is selected in the <b>NIC Mode</b> field.

**Step 4** 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **Common Properties** area, update the following properties:

Name	Description
<b>Management Hostname</b> field	The user-defined management hostname of the system that manages the various components of Cisco IMC.
<b>Dynamic DNS</b> check box	If checked, updates the resource records to the DNS from Cisco IMC.
<b>Dynamic DNS Update Domain</b> field	The domain name that is appended to a hostname for a Dynamic DNS (DDNS) update. If left blank, only a hostname is sent to the DDNS update request.



Name	Description
<b>Dynamic DNS Refresh Interval</b> field	The time set to refresh the DNS. Set a value between 0 and 8736 hours. If set to 0, it is disabled.

**Step 4** 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** menu.

**Step 2** In the **Admin** menu, click **Networking**.

**Step 3** In the **IPv4 Properties** area, update the following properties:

Name	Description
<b>Enable IPv4</b> check box	If checked, IPv4 is enabled.
<b>Use DHCP</b> check box	If checked, Cisco IMC uses DHCP.
<b>Management IP Address</b> field	The management IP address. An external virtual IP address that helps manage the CMCs and BMCs.
<b>Subnet Mask</b> field	The subnet mask for the IP address.
<b>Gateway</b> field	The gateway for the IP address.
<b>Obtain DNS Server Addresses from DHCP</b> check box	If checked, Cisco IMC retrieves the DNS server addresses from DHCP.
<b>Preferred DNS Server</b> field	The IP address of the primary DNS server.
<b>Alternate DNS Server</b> field	The IP address of the secondary DNS server.

**Step 4** 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **IPv6 Properties** area, update the following properties:

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

- Step 4** 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **VLAN Properties** area, update the following properties:

Name	Description
<b>Enable VLAN</b> check box	If checked, the Cisco IMC is connected to a virtual LAN.  <b>Note</b> 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.
<b>VLAN ID</b> field	The VLAN ID.
<b>Priority</b> field	The priority of this system on the VLAN.

- Step 4** Click **Save Changes**.

## Connecting to a Port Profile

### 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **Port Properties** area, update the following properties:

Name	Description
<b>Port Profile</b> field	Details of the <b>Port Profile</b> field.

Name	Description
<b>Auto Negotiation</b> check box	<p>Using this option, you can either set the network port speed and duplex values for the switch, or allow the system to automatically derive the values from the switch. This option is available for dedicated mode only.</p> <ul style="list-style-type: none"> <li>• If checked, the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured.</li> <li>• If unchecked, you can configure the network port speed and duplex values.</li> </ul>
<b>Admin Mode Area</b>	<p><b>Network Port Speed</b> field</p> <p>The network speed of the port. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• 10 Mbps</li> <li>• 100 Mbps</li> <li>• 1 Gbps</li> </ul> <p>The default value is 100 Mbps. In the <b>Dedicated</b> mode, if you disable <b>Auto Negotiation</b>, you can configure the network speed and duplex values.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Before changing the port speed, ensure that the switch you connected to has the same port speed.</li> </ul> <p><b>Duplex</b> drop-down list</p> <p>The duplex mode for the Cisco IMC management port.</p> <p>This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Half</b></li> <li>• <b>Full</b></li> </ul> <p>By default, the duplex mode is set to <b>Full</b>.</p>

Name	Description
<b>Operation Mode Area</b>	Displays the operation network port speed and duplex values.  If you checked the <b>Auto Negotiation</b> check box, 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 <b>Admin Mode</b> are displayed.

**Step 4** Click **Save Changes**.

## Configuring Individual Settings

This functionality is applicable only for Cisco UCS S-Series servers.

### Before you begin

You must be logged in as admin to configure the settings.

### Procedure

- Step 1** In the **Navigation** pane, click the **Admin** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the Individual Settings area, review and update the following fields for **CMC 1**, **CMC 2**, **BMC 1** and **BMC 2** in their respective areas:

Name	Description
<b>Hostname</b> field	The user-defined hostname. By default, the hostname appears in CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.
<b>MAC Address</b> field	The MAC address of the component.
<b>IPv4 Address</b> field	The IPv4 address of the component.
<b>IPv6 Address</b> field	The IPv6 address of the component.
<b>Link Local Address</b> field	The link local address for the component's IPv6 address.

**Step 4** 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** menu.
- Step 2** In the **Networking** pane, click **Network Security**.
- Step 3** In the **IP Blocking Properties** area, update the following properties:

Name	Description
<b>Enable IP Blocking</b> check box	Check this box to enable IP blocking.
<b>IP Blocking Fail Count</b> 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 <b>IP Blocking Fail Window</b> field.  Enter an integer between 3 and 10.
<b>IP Blocking Fail Window</b> 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 280.
<b>IP Blocking Penalty Time</b> 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 4** In the **IP Filtering (Whitelisting)** area, update the following properties:

Name	Description
<b>Enable IP Filtering</b> check box	Check this box to enable IP filtering.
<b>IP Filter</b> 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 5** 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** menu.
- Step 2** In the **Admin** menu, click **Networking**.
- Step 3** In the **Networking** pane, click **NTP Setting**.
- Step 4** In the **NTP Properties** area, update the following properties:

Name	Description
<b>NTP Enabled</b> check box	Check this box to enable the NTP service.
<b>Server 1</b> field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
<b>Server 2</b> field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
<b>Server 3</b> field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
<b>Server 4</b> field	The IP/DNS address of one of the four servers that act as an NTP server or the time source server.
<b>Status</b> message	<p>Indicates whether or not the server is able to synchronize its time with the remote NTP server. It is an eight bit integer indicating the stratum level of the local clock. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• 0—Unspecified or invalid</li> <li>• 1—Primary server</li> <li>• 2-15—Secondary server (via NTP)</li> <li>• 16—Unsynchronized</li> <li>• 17-255—Reserved</li> </ul>

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

---