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 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.

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	The ports that can be used to access . This can be one of the following: • **Dedicated**—The management port that is used to access the . • **Shared LOM**—The LOM (LAN On Motherboard) ports are used to access the CIMC.
NIC Interface field	The network interface that is selected in the **NIC Mode** 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 EXXXX-YYYYYYYYYYY, where XXXX is the model number and YYYYYYYYYYY 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 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.

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:

a) In the **Management Hostname** field, enter the name of the host.

By default, the hostname appears in EXXXX-YYYYYYYYYYY format, where XXXX is the model number and YYYYYYYYYYY is the serial number of the server.

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

Step 4 Click **Save Changes**.

Network Security Configuration

Network Security

The 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. 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
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.

Name	Description
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 4 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.
[+] (button)	Click the [+] ("Plus" button) to add a new filter. You can configure upto 20 filters.

Note If the filters are removed from the middle, filters will be re-arranged automatically.

Step 5 Click **Save Changes**.

Network Time Protocol Settings

Network Time Protocol Service Setting

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

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 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: • **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**.