



Configuring Network-Related Settings

This chapter includes the following sections:

- [Server NIC Configuration, page 1](#)
- [Configuring Common Properties, page 3](#)
- [Configuring IPv4, page 3](#)
- [Configuring the Server VLAN, page 5](#)
- [Network Security Configuration, page 6](#)

Server NIC Configuration

Server NICs

You can configure NIC mode and NIC redundancy for the server NICs using the CIMC.

Set the NIC mode in the CIMC network command mode to determine which port you want to use to reach the CIMC:

- **Dedicated**—The management port is used to access the CIMC
- **Shared LOM**—The LOM (LAN On Motherboard) host ports 1 and 2 are used to access the CIMC
- **Shipping**—The out-of-the-box defaults will be used for all options



Note

The available NIC modes may vary depending on your platform.

Set the NIC redundancy mode in the CIMC network command mode to determine how NIC redundancy is handled:

- **None**—No redundancy
- **Active-Active**—Use both ports simultaneously
Active-Active provides a throughput improvement by utilizing both host ports simultaneously.

- Active-Standby—Fail one port over to another

**Note**

The available NIC redundancy modes may vary depending on your platform.

Configuring 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

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set mode {dedicated shared_lom}	<p>Sets the NIC mode to one of the following:</p> <ul style="list-style-type: none"> • Dedicated—The management port is used to access the CIMC. • Shared LOM—The LOM (LAN On Motherboard) ports are used to access the CIMC. <p>Note The available NIC modes may vary depending on your platform.</p>
Step 4	Server /cimc/network # set redundancy {none active-active active-standby}	<p>Sets the NIC redundancy for systems in which the NIC mode is Shared LOM. The redundancy type can be one of the following:</p> <ul style="list-style-type: none"> • none—The NICs operate independently and do not failover if there is a problem. • active-active—If supported, both NICs are utilized simultaneously. This increases throughput and provides multiple paths to the CIMC. <p>Note If you select this option for a server that does not support teaming, the system displays an error message when you save your changes.</p> <ul style="list-style-type: none"> • active-standby—If one NIC fails, traffic fails over to the other NIC. <p>Note If you select this option, make sure that both NICs are connected to the same subnet to ensure that the traffic is secure regardless of which NIC is used.</p> <p>Note The available NIC redundancy may vary depending on your platform.</p>

	Command or Action	Purpose
Step 5	Server /cimc/network # commit	Commits the transaction to the system configuration.

This example configures the server NIC:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
Server /cimc/network #
```

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

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set hostname <i>host-name</i>	Specifies the name of the host.
Step 4	Server /cimc/network # commit	Commits the transaction to the system configuration.

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Server /cimc/network *# commit
Server /cimc/network #
```

Configuring IPv4

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set dhcp-enabled {yes no}	Selects whether the CIMC uses DHCP.
Step 4	Server /cimc/network # set v4-addr <i>ipv4-address</i>	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # set v4-netmask <i>ipv4-netmask</i>	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # set v4-gateway <i>gateway-ipv4-address</i>	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # set dns-use-dhcp {yes no}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # set preferred-dns-server <i>dns1-ipv4-address</i>	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # set alternate-dns-server <i>dns2-ipv4-address</i>	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # show [detail]	(Optional) Displays the IPv4 network settings.

This example configures and displays the IPv4 network settings:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated

```

```
NIC Redundancy: none
Server /cimc/network #
```

Configuring the Server VLAN

Before You Begin

You must be logged in as admin to configure the server VLAN.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set vlan-enabled {yes no}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # set vlan-id id	Specifies the VLAN number.
Step 5	Server /cimc/network # set vlan-priority <i>priority</i>	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # show [detail]	(Optional) Displays the network settings.

This example configures the server VLAN:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: yes
  VLAN ID: 10
  VLAN Priority: 32
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated
  NIC Redundancy: none

Server /cimc/network #
```

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

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # scope ipblocking	Enters the IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # set enabled {yes no}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # set fail-count fail-count	Sets 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.
Step 6	Server /cimc/network/ipblocking # set fail-window fail-seconds	Sets 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.
Step 7	Server /cimc/network/ipblocking # set penalty-time penalty-seconds	Sets 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.

	Command or Action	Purpose
Step 8	Server /cimc/network/ipblocking # commit	Commits the transaction to the system configuration.

This example configures IP blocking:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

