# Configuring Communication Services

This chapter includes the following sections:



# Configuring HTTP

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope http** | Enters the HTTP command mode. |
| **Step 2** | Server /http # **set enabled** {**yes** \| **no**} | Enables or disables HTTP and HTTPS service on the CIMC. |
| **Step 3** | Server /http # **set http-port** *number* | Sets the port to use for HTTP communication. The default is 80. |
| **Step 4** | Server /http # **set https-port** *number* | Sets the port to use for HTTPS communication. The default is 443. |
| **Step 5** | Server /http # **set timeout** *seconds* | Sets the number of seconds to wait between HTTP requests before the CIMC times out and terminates the session.<br>Enter an integer between 60 and 10,800. The default is 1,800 seconds. |
| **Step 6** | Server /http # **commit** | Commits the transaction to the system configuration. |

This example configures HTTP for the CIMC:

```
Server# scope http
Server /http # set enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled
---------- ---------- -------- --------------- -------
80         443        1800     0               yes

Server /http #
```

# Configuring SSH

### Before You Begin

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope ssh** | Enters the SSH command mode. |
| **Step 2** | Server /ssh # **set enabled** {**yes** \| **no**} | Enables or disables SSH on the CIMC. |
| **Step 3** | Server /ssh # **set ssh-port** *number* | Sets the port to use for secure shell access. The default is 22. |
| **Step 4** | Server /ssh # **set timeout** *seconds* | Sets the number of seconds to wait before the system considers an SSH request to have timed out.<br>Enter an integer between 60 and 10,800. The default is 300 seconds. |
| **Step 5** | Server /ssh # **commit** | Commits the transaction to the system configuration. |
| **Step 6** | Server /ssh # **show** [**detail**] | (Optional) Displays the SSH configuration. |

This example configures SSH for the CIMC:

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show
SSH Port   Timeout  Active Sessions Enabled
---------- -------- --------------- -------
22         600      1               yes

Server /ssh #
```

# IPMI Over LAN Configuration

## IPMI Over LAN

IPMI defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC), and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

## Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the CIMC with IPMI messages.

### Before You Begin

You must log in as a user with admin privileges to configure IPMI over LAN.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Server# **scope ipmi** | Enters the IPMI command mode. |
| **Step 2** | Server /ipmi # **set enabled** {**yes** \| **no**} | Enables or disables IPMI access on this server. |
| **Step 3** | Server /ipmi # **set privilege-level** {**readonly** \| **user** \| **admin**} | Specifies the user role that must be assigned to users accessing the system though IPMI. The user roles are as follows:<br>• **readonly**—This user can view information but cannot make any changes.<br>• **user**—This user can do the following:<br>  • View all information<br>  • Manage the power control options such as power on, power cycle, and power off<br>  • Launch the KVM console and virtual media<br>  • Clear all logs<br>  • Toggle the locator LED<br>• **admin**—This user can perform all actions available through the GUI, CLI, and IPMI. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** The value of this field must match exactly the role assigned to the user attempting to log in. For example, if this field is set to readonly and a user with the admin role attempts to log in through IPMI, that login attempt will fail. |
| **Step 4** | Server /ipmi # **set encryption-key** *key* | Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers. |
| **Step 5** | Server /ipmi # **commit** | Commits the transaction to the system configuration. |

This example configures IPMI over LAN for the CIMC:

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /ipmi #
```