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

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communication Services**.

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

Name	Description
HTTP/S Enabled check box	Whether HTTP and HTTPS are enabled on the CIMC.
HTTP Port field	The port to use for HTTP communication. The default is 80.
HTTPS Port field	The port to use for HTTPS communication. The default is 443
Session Timeout field	The number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC.

Name	Description
	This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the CIMC.

Step 4 Click **Save Changes**.

Configuring SSH

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communication Services**.

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

Name	Description
SSH Enabled check box	Whether SSH is enabled on the CIMC.
SSH Port field	The port to use for secure shell access. The default is 22.
SSH Timeout field	The number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 300 seconds.
Max Sessions field	The maximum number of concurrent SSH sessions allowed on the CIMC. This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the CIMC.

Step 4 Click **Save Changes**.

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 IMPI over LAN

Configure IMPI 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 IMPI over LAN.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Communication Services**.

Step 3 In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IMPI access is allowed on this server.
Privilege Level Limit drop-down list	The user role that must be assigned to users accessing the system though IPMI. This can be: • **read-only**—This user can view information but cannot make any changes. • **user**—This user can: ◦ View all information ◦ Manage the power control options such as power on, power cycle, and power off ◦ Launch the KVM console and virtual media ◦ Clear all logs ◦ Toggle the locator LED

Name	Description
	• **admin**—This user can perform all actions available through the GUI, CLI, and IPMI. **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 **read-only** and a user with the admin role attempts to log in through IPMI, that login attempt will fail.
Encryption Key field	The IMPI encryption key to use for IMPI communications.

Step 4 Click **Save Changes**.