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 perform this task.

Procedure

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

Step 2 On the **Admin** tab, click **Communications 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.

Name	Description
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC. 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 **Communications 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 1,800 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**.

Configuring IPMI

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

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

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

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

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.
Privilege Level Limit drop-down list	The highest privilege level that can be assigned to an IPMI session on this server. This can be: • **read-only**—IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges. • **user**—IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server. • **admin**—IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.

Name	Description
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 4 Click **Save Changes**.

Configuring SNMP Properties

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Communications Services**.
Step 3 In the **Communications Services** pane, click the **SNMP** tab.
Step 4 In the **SNMP Properties** area, update the following properties:

Name	Description
Enabled check box	Whether this server sends SNMP traps to the designated host.
SNMP Port field	The port the server uses to communicate with the SNMP host. This value cannot be changed.
Access Community String field	The default SNMP v1 or v2c community name or SNMP v3 username CIMC includes on any trap messages it sends to the SNMP host. Enter a string up to 18 characters.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 254 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter a string up to 254 characters.

Step 5 Click **Save Changes**.

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings.