



Configuring Communication Services

This chapter includes the following sections:

- [Configuring HTTP, page 1](#)
- [Configuring SSH, page 3](#)
- [Configuring IPMI, page 4](#)
- [Configuring SNMP, page 6](#)

Configuring HTTP

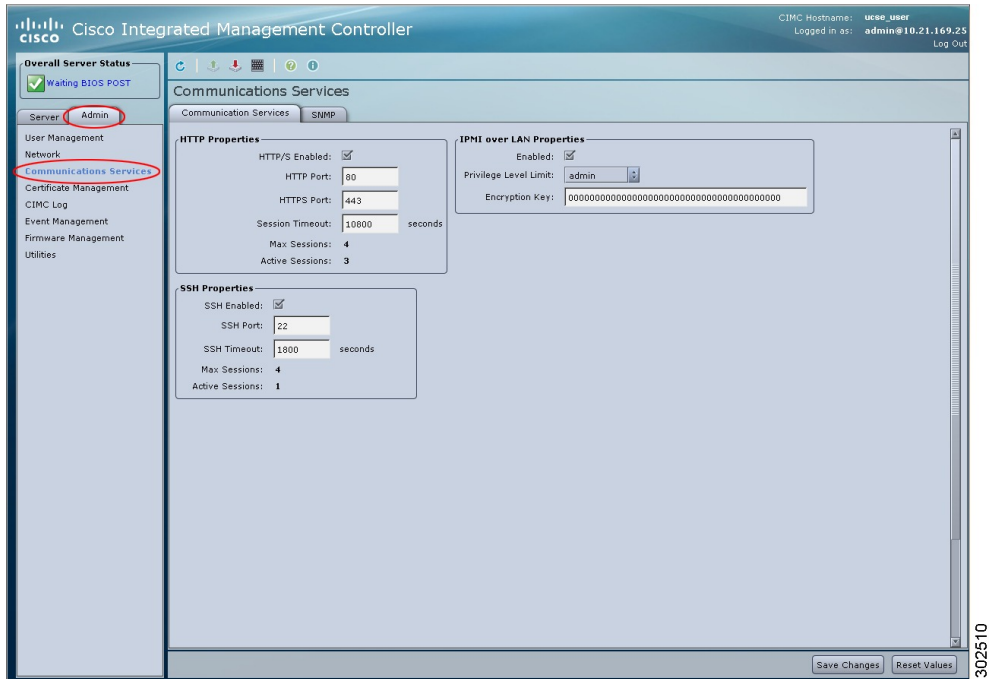
Before You Begin

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 **Communications Services** pane, click the **Communication Services** tab.

Figure 1: Communication Services Tab



- Step 4** 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 1800 seconds.
Max Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed on the CIMC. This value may not be changed.

Name	Description
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the CIMC.

Step 5 Click **Save Changes**.

Configuring SSH

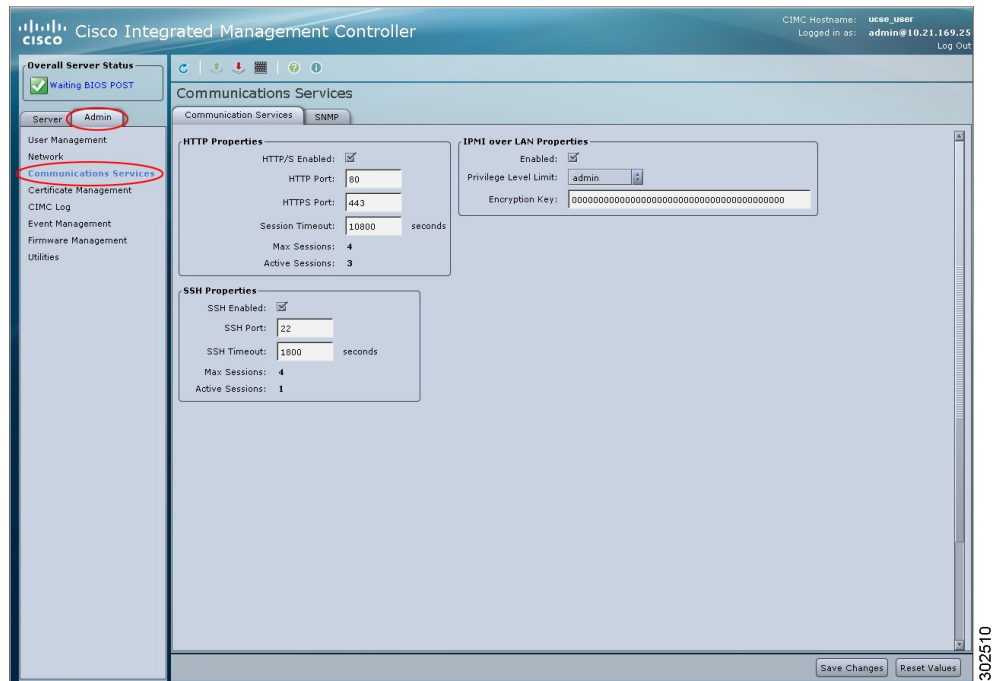
Before You Begin

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 **Communications Services** pane, click the **Communication Services** tab.

Figure 2: Communication Services Tab



Step 4 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 5 Click **Save Changes**.

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (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 the 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.

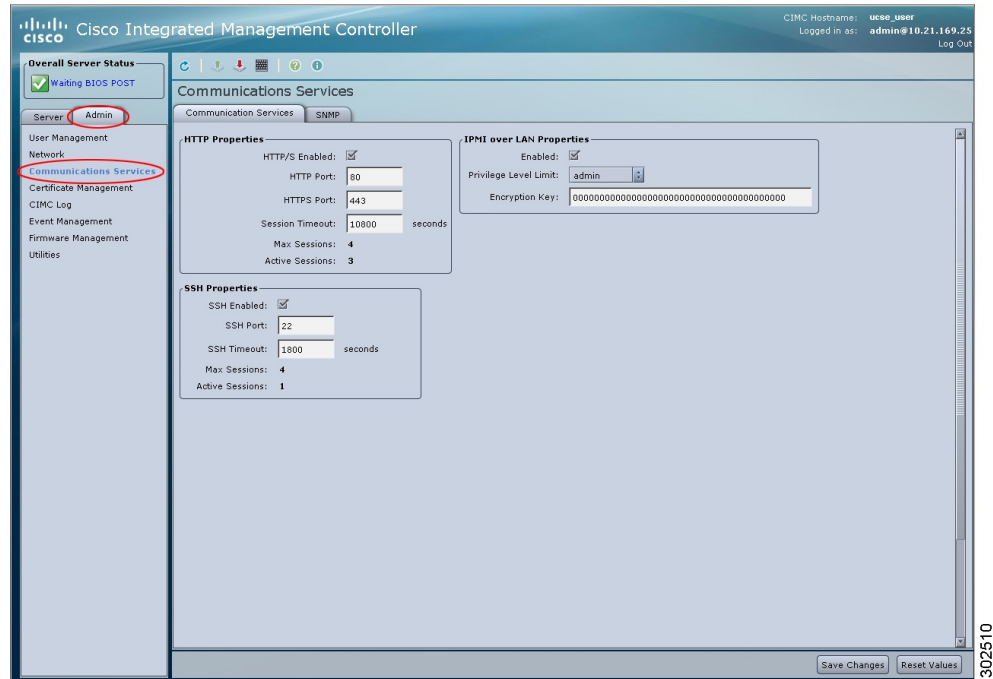
Before You Begin

You must log in as a user with admin privileges to 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 **Communication Services** tab.

Figure 3: Communication Services Tab



- Step 4** In the **IPMI over LAN Properties** area, update the following properties:

Name	Description
Enabled check box	Whether IPMI access is allowed on this server.

Name	Description
Privilege Level Limit drop-down list	<p>The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following:</p> <ul style="list-style-type: none"> • 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.
Encryption Key field	<p>The IPMI encryption key to use for IPMI communications.</p>

Step 5 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS E-Series Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps.

Configuring SNMP Properties

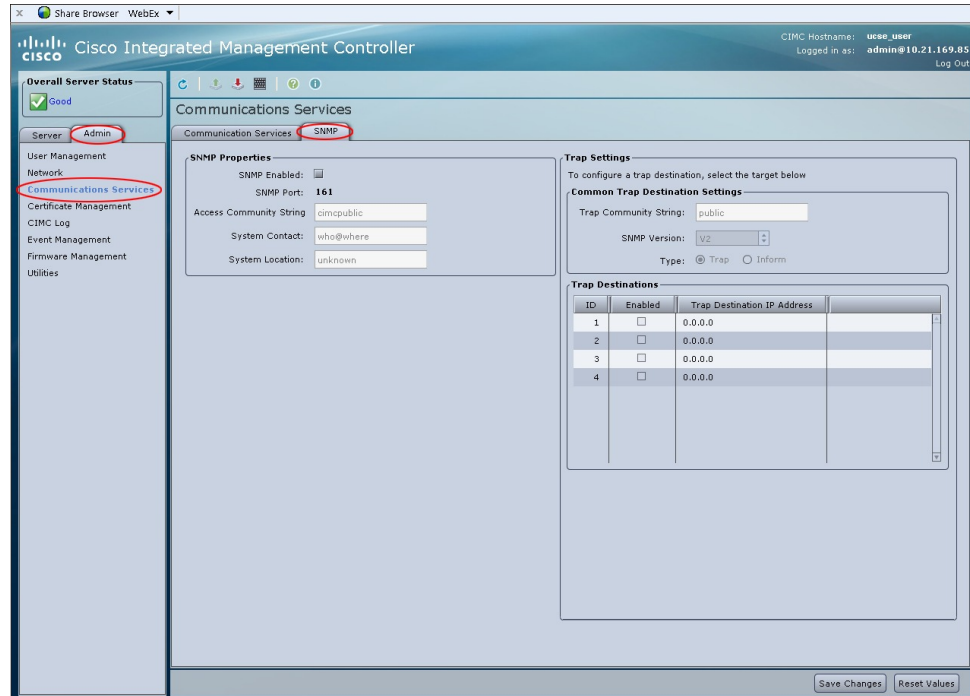
Before You Begin

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.

Figure 4: SNMP Tab



- Step 4** In the **SNMP Properties** area, update the following properties:

Name	Description
SNMP 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. 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.

Name	Description
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](#).

Configuring SNMP Trap Settings

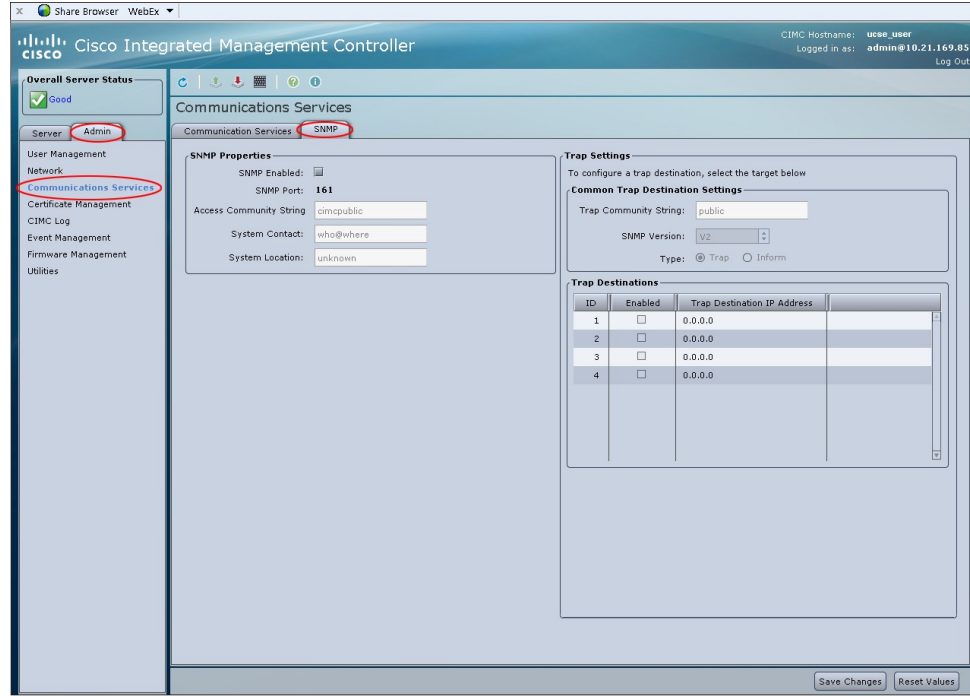
Before You Begin

You must log in as a user with admin privileges to disable platform event alerts.

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.

Figure 5: SNMP Tab



- Step 4** In the **Trap Community String** text box in the **Common Trap Destination Settings** area, enter the name of the SNMP community to which trap information should be sent.
- Step 5** In the **Trap Destinations** area, click the row of the desired SNMP trap destination. The **Traps Details** dialog box opens.
- Step 6** In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID column	The trap destination ID. This value cannot be modified.
Enabled column	For each SNMP trap destination that you want to use, check the associated check box in this column.
Trap Destination IP Address column	The IP address to which SNMP trap information is sent.

Step 7 Click **Save Changes**.

Sending a Test SNMP Trap Message

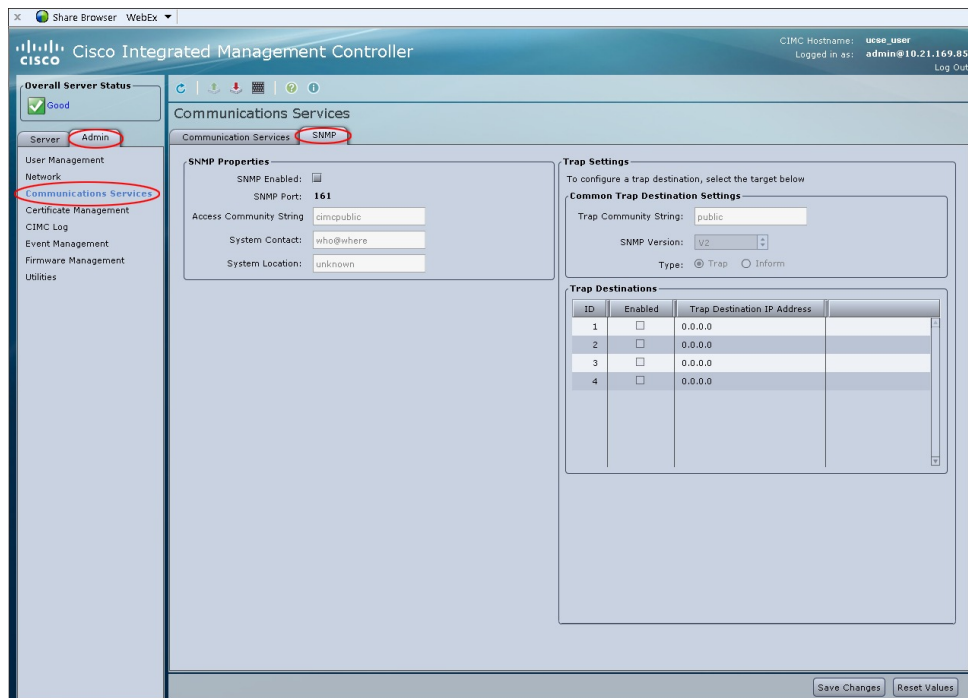
Before You Begin

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.

Figure 6: SNMP Tab



Step 4 In the **Trap Destinations** area, click the row of the desired SNMP trap destination. The **Traps Details** dialog box opens.

Step 5 Click **Send SNMP trap**. An SNMPv1 test trap message is sent to the trap destination.

Note The trap must be configured and enabled in order to send a test message.

