Managing Communication Services

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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

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

Name	Description
HTTPS Enabled check box	Check box to indicate whether HTTPS is enabled on the CIMC.
HTTP Enabled check box	Check box to indicate whether HTTP is enabled on the CIMC.
Redirect HTTP to HTTPS Enabled check box	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. It is recommended that you enable this option if you enable HTTP.
HTTP Port field	The port to use for HTTP communication. The default is 80.

Name	Description
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 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.
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 perform this task.

Procedure

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

Step 2 In the **Admin** menu, click **Communication Services**.

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

Name	Description
SSH Enabled check box	Check box to enable or disable SSH.
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 1800 seconds.

Name	Description
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 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 the Cisco Integrated Management Controller (CIMC), and resides on the server motherboard. The CIMC links to the main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating systemobtain 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 CIMC to increase fan speed or reduce processor speed to address the problem.

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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

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

Name	Description
Enabled check box	Check box to enable or disable IPMI access.

Name	Description
Privilege Level Limit drop down	The highest privilege level that can be assigned to an IPMI session on this server. This can be one of the following: • **read-only**—IPMI users can view information but cannot make any changes. If you choose 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 choose 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 choose this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.
Encryption Key field	The IPMI encryption key to use for IPMI communications.

Step 4 Click **Save Changes**.

Configuring XML API

The Cisco XML application programming interface (API) is a programmatic interface for the UCS E-Series M6 Server. The API accepts XML documents through HTTP or HTTPS.

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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

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

Name	Description
XML API Enabled check box	Check box to enable or disable API access.

Name	Description
Max Sessions field	The maximum number of concurrent API sessions allowed on the CIMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the CIMC.

Step 4 Click **Save Changes**.

Configuring Redfish

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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

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

Name	Description
Redfish Enabled check box	Check box enable or disable Redfish.
Max Sessions field	The maximum number of concurrent redfish sessions allowed on CIMC.
Active Sessions field	The number of Redfish sessions currently running on CIMC.

Step 4 Click **Save Changes**.

SNMP - Overview

The Cisco UCS E-Series M6 Servers support the Simple Network Management Protocol (SNMP) for viewing the 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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

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

Name	Description
SNMP Enabled check box	Check box to enable or disable sending SNMP traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP Port field	The port on which SNMP agent runs.
Access Community String field	The default SNMP v1 or v2c community name includes on any SNMP get operations. Enter a string up to 18 characters.
SNMP Community Access drop down	This can be one of the following: • **Disabled**—This option blocks access to the information in the inventory tables. • **Limited**—This option provides partial access to read the information in the inventory tables. • **Full**—This option provides full access to read the information in the inventory tables. **Note** SNMP Community Access is applicable only for SNMP v1 and v2c users.
Trap Community String field	The name of the SNMP community group used for sending SNMP trap to other devices. Enter a string up to 18 characters. **Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials.

Name	Description
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string up to 64 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 64 characters.
SNMP Input Engine ID field	User-defined unique identification of the static engine.
SNMP Engine ID field	Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the CIMC serial number.

Step 5 Click **Save Changes**.

Managing SNMP Users

Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

Procedure

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

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** area, click the **SNMP** tab.

Step 4 In the **v3 User Settings** area, update the following properties:

Name	Description
Add User button	Click an available row in the table then click this button to add a new SNMP user.
Modify User button	Select the user you want to change in the table then click this button to modify the selected SNMP user.
Delete User button	Select the user you want to delete in the table then click this button to delete the selected SNMP user.
ID column	The system-assigned identifier for the SNMP user.

Name	Description
Name column	The SNMP user name.
Auth Type column	The user authentication type.
Privacy Type column	The user privacy type.

Step 5 Click **Save Changes**.

Configuring SNMP Users

Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled.

Procedure

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

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

Step 4 In the **v3 User Settings** area, perform one of the following actions:

- Choose an existing user from the table and click **Modify User**.
- Choose a row in the **Users** area and click **Add User** to create a new user.

Step 5 In the **SNMP User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user. This field cannot be changed.
User Name field	The SNMP username. Enter between 1 and 31 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.

Name	Description
Security Level drop-down list	The security level for this user. This can be one of the following: • **no auth, no priv**—The user does not require an authorization or privacy password. • **auth, no priv**—The user requires an authorization password but not a privacy password. If you select this option, Cisco IMC enables the Auth fields described below. • **auth, priv**—The user requires both an authorization password and a privacy password. If you select this option, Cisco IMC enables the Auth and Privacy fields.
Auth Type drop-down	The authorization type. This can be one of the following: • **MD5** • **SHA**
Change Auth Password field	The authorization password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Auth Password field	The authorization password again for confirmation purposes.
Privacy Type drop down	The privacy type. This can be one of the following: • **DES** • **AES**
Privacy Password field	The privacy password for this SNMP user. Enter between 8 and 64 characters or spaces. **Note** Cisco IMC automatically trims leading or trailing spaces.
Confirm Privacy Password field	The authorization password again for confirmation purposes.

Step 6 Click **Save Changes**.

Step 7 If you want to delete a user, choose the user and click **Delete User**, and click **OK** in the delete confirmation prompt.

Configuring v2c 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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

Step 4 In the **v2c Properties** area, update the following properties:

Name	Description
SNMP v2c Enabled check box	Check box to enable or disable sending SNMP v2c traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
Access Community String field	The default SNMP v1 or v2c community name Cisco IMC includes on any SNMP get operations. Enter a string up to 18 characters.
SNMP Community Access drop down	This can be one of the following: • **Disabled** — This option blocks access to the information in the inventory tables. • **Limited** — This option provides partial access to read the information in the inventory tables. • **Full** — This option provides full access to read the information in the inventory tables. **Note** SNMP Community Access is applicable only for SNMP v1 and v2c users.
Trap Community String field	The name of the SNMP community group used for sending SNMP trap to other devices. Enter a string up to 18 characters. **Note** This field is visible only for SNMP v1 and v2c users. SNMP v3 users need to use SNMP v3 credentials.

Step 5 Click **Save Changes**.

Configuring v3c 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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

Step 4 In the **v3c Properties** area, update the following properties:

Name	Description
SNMP v3 Enabled check box	Check box to enable or disable sending SNMP v3c traps to the designated host. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP Engine ID field	Unique string to identify the device for administration purpose. This is generated from the SNMP Input Engine ID if it is already defined, else it is derived from the BMC serial number.
SNMP Input Engine ID field	User-defined unique identification of the static engine.

Step 5 Click **Save Changes**.

Configuring SNMP Trap Settings

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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

Step 4 In the **Trap Destinations** area, you can perform one of the following:

- Choose an existing user from the table and click **Modify Trap**.
- Click **Add Trap** to create a new trap.

Step 5 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID column	The trap destination ID. This value cannot be modified.

Name	Description
Enabled column	For each SNMP trap destination that you want to use, check the associated check box in this column.
Version column	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**
Type column	The type of trap to send. This can be one of the following: • **Trap**: If this option is chosen, the trap will be sent to the destination but you do not receive any notifications. • **Inform**: You can choose this option only for V2 users. If chosen, an acknowledgment is sent to the SNMP engine.
User column	Displays the user for each trap.
Community String column	Displays the community string for each trap.
Destination Address column	The IP address to which SNMP trap information is sent.
Port column	The port that the server uses to communicate with the trap destination. The port number can be 1 to 65535.

Step 6 Click **Save Changes**.

Step 7 If you want to delete a trap destination, choose the row and click **Delete Trap**, and then click **OK** in the delete confirmation prompt.

Step 8 Click **Save Changes**.

Sending an SNMP Test 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** menu.

Step 2 In the **Admin** menu, click **Communication Services**.

Step 3 In the **Communication Services** pane, click the **SNMP** tab.

Step 4 In the **Trap Destinations** area, choose the row of the desired SNMP trap destination.

Step 5 Click **Send SNMP Test Trap**.

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

An SNMP test trap message is sent to the trap destination.