Configuring Communication Services

This chapter includes the following sections:

Enabling or Disabling TLS v1.2

Beginning with release 4.2(2a), Cisco IMC supports disabling TLS v1.2 and also customize the cipher values for both v1.2 and v1.3.

Before you begin

If **CC** (Common Criteria) under **Security Configuration** is enabled, you cannot disable TLS v1.2. Ensure that **CC** is disabled before you disable TLS v1.2.

Enabling or disabling TLS v1.2, restarts vKVM, Webserver, XML API, and Redfish API sessions.

Procedure

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

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

Step 3 In the **TLS Configuration** area, update the following properties:

Name	Description
Enable TLS v1.2 check box	Whether TLS v1.2 is enabled on Cisco IMC. **Note** Enabling or disabling TLS v1.2, restarts vKVM, Webserver, XML API, and Redfish API sessions. **Note** If **CC** (Common Criteria) under **Security Configuration** is enabled, you cannot disable TLS v1.2.
Configured TLS Version field	TLS versions supported by Cisco IMC. This field is not user configurable. The value shown here depends on the value selected for **Enable TLS v1.2** check box.
TLS v1.2 Cipher Mode drop-down list	Allows you to select the desired cipher mode when TLS v1.2 is enabled. This can be one of the following: • **High** • **Medium** • **Low** **Note** If **FIPS** under **Security Configuration** is enabled, you cannot select **Low** mode. • **Custom**—You can enter custom cipher values. Refer https://www.openssl.org/docs/man1.0.2/man1/ciphers.html for OpenSSL equivalent cipher name for a specific cipher to be provided in custom cipher field. For example: To set **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, provide **ECDHE-RSA-AES256-GCM-SHA384** input in the cipher list as input.

Name	Description
TLS v1.2 Cipher List field	Displays the list of ciphers based on the value selected in **TLS v1.2 Cipher Mode** drop-down list. You can edit the cipher values if you choose **TLS v1.2 Cipher Mode** as **Custom**. **Note** When FIPS is enabled, you are not allowed to set FIPS unsupported ciphers. **Note** If the cipher value entered is invalid or unsupported, then while saving the configuration, Cisco IMC automatically changes the **TLS v1.2 Cipher Mode** value to **High** and saves the configuration. For example: If **DH-RSA-AES256-GCM-SHA384** is set, **TLS v1.2 Cipher Mode** sets to **High** automatically After saving the configuration, Cisco IMC disables the **TLS v1.2 Cipher List** field and when you hover the mouse over **TLS v1.2 Custom Cipher Status** icon, it displays an error message similar to the following: `TLS v1.2 Custom Cipher Status: Error: Configuring an invalid or unsupported TLS v1.2 Cipher List-'`*`Cipher_Name`*`'. Setting TLS v1.2 Cipher Mode to High.`
TLS v1.3 Cipher Suite field	Allows you to edit the cipher values for TLS v1.3 **Note** When FIPS is enabled, you are not allowed to set FIPS unsupported ciphers.

Configuring HTTP

Beginning with release 4.1(2b), Cisco IMC supports separate HTTPS and HTTP communication services. You can disable only HTTP services using this functionality.

This functionality is supported only on the following servers:

- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C480 M5
- Cisco UCS C480 ML M5
- Cisco UCS C240 SD M5
- Cisco UCS C125 M5

Note If **Redirect HTTP to HTTPS Enabled** was disabled in any release earlier than 4.1(2b), then after upgrading to release 4.1(2b) or later, **HTTP Enabled** value is set to **Disabled** by the system.

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	**Warning** Disabling this option terminates the exiting Cisco IMC Web GUI session. Disabling this option, disables both HTTP and HTTPS services to access Cisco IMC. This option enables only HTTPS services to access Cisco IMC.
HTTP Enabled check box	**Warning** To successfully save any changes for this option, Cisco IMC Web GUI is restarted automatically. Communication with the management controller is lost momentarily and you must log in again after the restart. This option enables only HTTP services to access Cisco IMC. **Note** If HTTPS is disabled, HTTP services to access Cisco IMC are also disabled.
Redirect HTTP to HTTPS Enabled check box	**Note** This option is applicable only when HTTP Enabled is checked. If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. We strongly recommend that you enable this option if you enable HTTP.
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 Cisco IMC 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 Cisco IMC. This value may not be changed.
Active Sessions field	The number of HTTP and HTTPS sessions currently running on the Cisco IMC.

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** 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	Whether SSH is enabled on the Cisco IMC.
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 Cisco IMC. This value may not be changed.
Active Sessions field	The number of SSH sessions currently running on the Cisco IMC.

Step 4 Click **Save Changes**.

Configuring XML API

XML API for Cisco IMC

The Cisco Cisco IMC XML application programming interface (API) is a programmatic interface to Cisco IMC for a C-Series Rack-Mount Server. The API accepts XML documents through HTTP or HTTPS.

For detailed information about the XML API, see *Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*.

Enabling the XML API

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	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the Cisco IMC.

Step 4 Click **Save Changes**.

Enabling Redfish

Before you begin

You must be logged in as admin to perform this action.

Procedure

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

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

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

Name	Description
XML API Enabled check box	Whether API access is allowed on this server.
Max Sessions field	The maximum number of concurrent API sessions allowed on the Cisco IMC. This value may not be changed.
Active Sessions field	The number of API sessions currently running on the Cisco IMC.

Step 4 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 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 Cisco IMC with IPMI messages.

Note

- If you would want to run IPMI commands without issuing an encryption key, set the **Encryption Key** field in Cisco IMC to any even number of zeroes and save. This allows you to issue IPMI commands without including an encryption key.
- You are only allowed a maximum of four concurrent IPMI sessions.

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 for BMC 1, BMC 2, CMC 1, or CMC 2:

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 one of the following: • **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	The IPMI encryption key to use for IPMI communications.
Randomize button	Enables you to change the IPMI encryption key to a random value.

Step 4 Click **Save Changes**.

Configuring SNMP

SNMP

The Cisco UCS C-Series Rack-Mount Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps. For information on Management Information Base (MIB) files supported by Cisco IMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html.

Beginning with release 4.1(3b), Cisco IMC introduces enhanced authentication protocol for SNMP v3 version. SNMP v3 users cannot be added with **DES** security protocol.

Cisco IMC GUI displays a warning when you select an existing v3 version with unsupported security level, authentication type, or privacy type. You may select and modify the user details.

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 **Communications Services** pane, click the **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. **Note** After you check this check box, you need to click **Save Changes** before you can configure SNMP users or traps.
SNMP v2c Enabled check box	Allows you to enable or disable SNMP v2c version.
SNMP v3 Enabled check box	Allows you to enable or disable SNMP v3 version.
SNMP Port field	The port on which Cisco IMC SNMP agent runs. Enter an SNMP port number within the range 1 to 65535. The default port number is 161. **Note** The port numbers that are reserved for system calls, such as 22,23,80,123,443,623,389,636,3268,3269 and 2068, cannot be used as an SNMP port.
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.

Name	Description
SNMP Community Access drop-down list	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 version need to use SNMP v3 credentials.
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.
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 BMC serial number.

Step 5 Click **Save Changes**.

What to do next

Configure SNMP trap settings.

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

Step 4 Click on **Trap Destinations** tab.

Step 5 In the **Trap Destinations** area, you can perform one of the following:

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

Note If the fields are not highlighted, select **Enabled**.

Step 6 In the **Trap Details** dialog box, complete the following fields:

Name	Description
ID field	The trap destination ID. This value cannot be modified.
Enabled check box	If checked, then this trap is active on the server.
Version drop-down list	The SNMP version and model used for the trap. This can be one of the following: • **V2** • **V3**
Trap Type radio button	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, you will receive a notification when a trap is received at the destination.
User drop-down list	The drop-down list displays all available users, select a user from the list. **Note** While Configuring SNMP v3 version, SNMP users with Encryption Method set as **DES** are not displayed in the drop-down list.
Trap Destination Address field	Address to which the SNMP trap information is sent. You can set an IPv4 or IPv6 address or a domain name as the trap destination.
Port	The port the server uses to communicate with the trap destination. Enter a trap destination port number within the range 1 to 65535.

Step 7 Click **Save Changes**.

Step 8 If you want to delete a trap destination, select the row and click **Delete**.

Click **OK** in the delete confirmation prompt.

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** menu.

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

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

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

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

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

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

Managing SNMP Users for Cisco UCS C-Series M7 and Later Servers

Procedure

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

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

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

Step 4 In the **v3 User Settings** area, click **CLICK HERE to change the Users configurations**

Refer Adding Local Users for Cisco UCS C-Series M7 and Later Servers to change user settings.

Configuring a Server to Send Email Alerts Using SMTP

The Cisco IMC supports email-based notification of server faults to recipients without relying on the SNMP. The system uses the Simple Mail Transfer Protocol (SMTP) to send server faults as email alerts to the configured SMTP server.

A maximum of four recipients is supported.

Configuring SMTP Server For Receiving Email Alerts

Configure the SMTP properties and add email recipients on the **Mail Alert** tab to receive email notifications for server faults.

Before you begin

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

Procedure

Step 1

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

Step 3 In the **Communications Services** pane, click the **Mail Alert** tab.

Step 4 In the **SMTP Properties** area, update the following properties.

Name	Description
SMTP Enabled check box	If checked, it enables the SMTP service.
SMTP Server Address field	Allows you to enter the SMTP server address.
SMTP Port field	Allows you to enter the SMTP port number. The default port number is 25.
SMTP From Address	Allows you to set the From address of the SMTP mail alerts that are sent. The email address that you enter in this field will be displayed as the from address (mail received from address) of all the SMTP mail alerts that you receive. **Note** This is an optional field. If you do not enter an email address in this field, by default the server hostname ID is displayed as the from address (mail received from address).

Step 5 In the **SMTP Recipients** area, do the following:

a) Click the **Add (+)** button to add the email recipients to whom notifications should be sent. Enter the email ID and click **Save**.

To delete an email recipient, select the email recipient and click the **Delete (X)** button.

b) **Minimum Severity to Report** drop-down list allows you to choose the minimum severity level for receiving the email alert. This can be one of the following:

- Condition
- Warning
- Minor
- Major
- Critical

If you choose a minimum severity level, the mail alerts are sent for that level and the other higher severity levels. For example, if you choose 'Minor' as the minimum severity level, you will receive email alerts for the minor, major, and critical fault events.

c) Click **Send Test Mail** to check whether the email recipient you added is reachable.
If the email address and the SMTP settings are valid, a confirmation pop-up window appears with the message that an email has been sent. If the settings are not valid, a confirmation pop-up window appears with the message that no email has been sent. The **Reachability** column indicates whether test mails have been sent successfully to the email recipient. The **Reachability** column has one of the following values:

- **Yes** (if the test mail has been sent successfully)
- **No** (if the test mail has not been sent successfully)
- **na** (if no test mail has been sent)

Step 6 Click **Save Changes**.

Troubleshooting

The following table describes troubleshooting suggestions for SMTP mail alert configuration issues (when the reachability status is **No**) that may appear in the Cisco IMC logs:

Issue	Suggested Solution
Timeout was reached	This could occur when you are not able to reach the configured SMTP IP address. Enter a valid IP address.
Couldn't resolve host name	This could occur when you are not able to reach the configured SMTP domain name. Enter a valid domain name.
Couldn't connect to server	This could occur when the SMTP IP or domain name or port number is/are incorrectly configured. Enter valid configuration details.
Failed sending data to the peer	This could occur when the an invalid recipient email ID is configured. Enter a valid email ID.

Adding SMTP Email Recipients

Add email recipients on the **Mail Alert** tab to receive email notifications for server faults.

Before you begin

- You must log in as a user with admin privileges to perform this task.
- Configure the SMTP server properties in the SMTP Properties area. See Configuring SMTP Server For Receiving Email Alerts, on page 13

Procedure

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

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

Step 3 In the **Communications Services** pane, click the **Mail Alert** tab.

Step 4 In the **SMTP Recipients** area, do the following:

a) Click the **Add (+)** button to add the email recipients to whom notifications should be sent. Enter the email ID and click **Save**.

b) **Minimum Severity to Report** drop-down list allows you to choose the minimum severity level for receiving the email alert. This can be one of the following:

- Condition
- Warning
- Minor
- Major
- Critical

If you choose a minimum severity level, the mail alerts are sent for that level and the other higher severity levels. For example, if you choose 'Minor' as the minimum severity level, you will receive email alerts for the minor, major, and critical fault events.

c) Click **Send Test Mail** to check whether the email recipient you added is reachable.
If the email address and the SMTP settings are valid, a confirmation pop-up window appears with the message that an email has been sent. If the settings are not valid, a confirmation pop-up window appears with the message that no email has been sent. The **Reachability** column indicates whether test mails have been sent successfully to the email recipient. The **Reachability** column has one of the following values:

- **Yes** (if the test mail has been sent successfully)
- **No** (if the test mail has not been sent successfully)
- **na** (if no test mail has been sent)