Configuring Communication Services

This chapter includes the following sections:

- Communication Services, page 1
- Configuring CIM-XML, page 2
- Configuring HTTP, page 3
- Configuring HTTPS, page 3
- Configuring SNMP, page 8
- Enabling Telnet, page 15
- Disabling Communication Services, page 15

Communication Services

You can use the following communication services to interface third-party applications with Cisco UCS:

Communication Service	Description
CIM XML	This service is disabled by default and is only available in read-only mode. The default port is 5988. This common information model is one of the standards defined by the Distributed Management Task Force.
HTTP	This service is enabled on port 80 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTP, all data is exchanged in clear text mode. For security purposes, we recommend that you enable HTTPS and disable HTTP. By default, Cisco UCS redirects any attempt to communicate via HTTP to the HTTPS equivalent. We recommend that you do not change this behavior. **Note** If you are upgrading to Cisco UCS, version 1.4(1), this does not happen by default. If you want to redirect any attempt to communicate via HTTP to an HTTPS equivalent, you should enable **Redirect HTTP to HTTPS** in Cisco UCS Manager.

Communication Service	Description
HTTPS	This service is enabled on port 443 by default. With HTTPS, all data is exchanged in encrypted mode through a secure server. For security purposes, we recommend that you only use HTTPS and either disable or redirect HTTP communications.
SMASH CLP	This service is enabled for read-only access and supports a limited subset of the protocols, such as the **show** command. You cannot disable it. This shell service is one of the standards defined by the Distributed Management Task Force.
SNMP	This service is disabled by default. If enabled, the default port is 161. You must configure the community and at least one SNMP trap. Enable this service only if your system includes integration with an SNMP server.
SSH	This service is enabled on port 22. You cannot disable it, nor can you change the default port. This service provides access to the Cisco UCS Manager CLI.
Telnet	This service is disabled by default. This service provides access to the Cisco UCS Manager CLI.

Configuring CIM-XML

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **CIM-XML** area, click the **enabled** radio button.
The **CIM-XML** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI will use for CIM-XML. The default port is 5988.

Step 6 Click **Save Changes**.

Configuring HTTP

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Click the **Communication Services** tab.

Step 4 In the **HTTP** area, click the **enabled** radio button.
The **HTTP** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTP.
The default port is 80.

Step 6 (Optional) In the **Redirect HTTP to HTTPS** field, click the **enabled** radio button.
You must also configure and enable HTTPS to enable redirection of HTTP logins to the HTTPS login. Once enabled, you cannot disable the redirection until you have disabled HTTPS.

Step 7 Click **Save Changes**.

Configuring HTTPS

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and Cisco UCS Manager.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Manager provides a default key ring with an initial 1024-bit key pair, and allows you to create additional key rings.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By

default, Cisco UCS Manager contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for Cisco UCS Manager, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through Cisco UCS Manager and submit the request to a trusted point.

Creating a Key Ring

Cisco UCS Manager supports a maximum of 8 key rings, including the default key ring.

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click **Key Management** and choose **Create Key Ring**.

Step 4 In the **Create Key Ring** dialog box, do the following:

a) In the **Name** field, enter a unique name for the key ring.

b) In the **Modulus** field, select one of the following radio buttons to specify the SSL key length in bits:

- **mod512**
- **mod1024**
- **mod1536**
- **mod2048**

c) Click **OK**.

What to Do Next

Create a certificate request for this key ring.

Creating a Certificate Request for a Key Ring

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Click the key ring for which you want to create a certificate request.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click **Create Certificate Request**.

Step 6 In the **Create Certificate Request** dialog box, complete the following fields:

Name	Description
Password field	An optional password for this request.
Confirm Password field	If you specified a password, enter it again for confirmation.
Subject field	The fully qualified domain name of the fabric interconnect.
IP Address field	The IP address of the fabric interconnect.

Step 7 Click **OK**.

Step 8 Copy the text of the certificate request out of the **Request** field and save in a file.

Step 9 Send the file with the certificate request to the trust anchor or certificate authority.

What to Do Next

Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click **Key Management** and choose **Create Trusted Point**.

Step 4 In the **Create Trusted Point** dialog box, complete the following fields:

Name	Description
Name field	The name of the trusted point.

Name	Description
	This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Certificate Chain field	The certificate information for this trusted point.

Step 5 Click **OK**.

What to Do Next

When you receive the certificate from the trust anchor or certificate authority, import it into the key ring.

Importing a Certificate into a Key Ring

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Click the key ring into which you want to import the certificate.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Certificate** area, complete the following fields:

a) From the **Trusted Point** drop-down list, select the trusted point for the trust anchor that granted this certificate.

b) In the **Certificate** field, paste the text from the certificate you received from the trust anchor or certificate authority.

Tip If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

Step 6 Click **Save Changes**.

What to Do Next

Configure your HTTPS service with the key ring.

Configuring HTTPS

Caution After you complete the HTTPS configuration, including changing the port and key ring to be used by HTTPS, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **HTTPS** area, click the **enabled** radio button.
The **HTTPS** area expands to display the available configuration options.

Step 5 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTPS.
The default port is 443.

Step 6 (Optional) From the **Key Ring** drop-down list, choose the key ring you created for HTTPS.

Step 7 Click **Save Changes**.

Deleting a Key Ring

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click the key ring you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Trusted Point

Before You Begin

Ensure that the trusted point is not used by a key ring.

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Key Management**.

Step 3 Right-click the trusted point you want to delete and choose **Delete**.

Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 5 Click **OK**.

Configuring SNMP

Information about SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS, the managed device, that maintains the data for Cisco UCS and reports the data, as needed, to the SNMP manager. Cisco UCS includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Manager.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS release 1.4(1) and higher support a larger number of MIBs than earlier releases.

Cisco UCS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Manager generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Manager cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the Cisco UCS Manager does not receive the PDU, it can send the inform request again.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Supported Combinations of SNMP Security Models and Levels

The following table identifies what the combinations of security models and levels mean.

Table 1: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code

Model	Level	Authentication	Encryption	What Happens
				(HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMPv3 Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support in Cisco UCS

Cisco UCS provides the following support for SNMP:

Support for MIBs

Cisco UCS supports read-only access to MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Quick Reference for Cisco UCS.

Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Enabling SNMP and Configuring SNMP Properties

SNMP messages from a Cisco UCS instance display the fabric interconnect name rather than the system name.

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP** area, click the **enabled** radio button.
The **SNMP** area expands to display the available configuration options. You cannot change the port on which Cisco UCS Manager communicates with the SNMP host.

Step 5 Complete the following fields:

Name	Description
Community/Username field	The default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS Manager includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string of up to 255 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.

Name	Description
	Enter an alphanumeric string up to 512 characters.

Step 6 Click **Save Changes**.

What to Do Next

Create SNMP traps and users.

Creating an SNMP Trap

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click +.

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

Name	Description
IP Address field	The IP address of the SNMP host to which Cisco UCS Manager should send the trap.
Community/Username field	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS Manager includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which Cisco UCS Manager communicates with the SNMP host for the trap. The default port is 162.
Version field	The SNMP version and model used for the trap. This can be: • **v1** • **v2c** • **v3**
Type field	If you select v2c or v3 for the version, the type of trap to send. This can be:

Name	Description
	• **traps** • **informs**
v3 Privilege field	If you select v3 for the version, the privilege associated with the trap. This can be: • **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMP Trap

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

Creating an SNMPv3 user

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click +.

Step 5 In the **Create SNMP User** dialog box, complete the following fields:

Name	Description
Name field	The username assigned to the SNMP user. An SNMP username cannot be the same as a local username. Choose an SNMP username that does not match a local username.
Auth Type field	The authorization type. This can be: • **MD5** • **SHA**
Use AES-128 check box	If checked, this user uses AES-128 encryption.
Password field	The password for this user.
Confirm Password field	The password again for confirmation purposes.
Privacy Password field	The privacy password for this user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMPv3 User

Procedure

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

Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save Changes**.

Enabling Telnet

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.
Step 3 Click the **Communication Services** tab.
Step 4 In the **Telnet** area, click the **enabled** radio button.
Step 5 Click **Save Changes**.

Disabling Communication Services

Note We recommend that you disable all communication services that are not required to interface with other network applications.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ Communication Management ➤ Communication Services**.
Step 3 On the **Communication Services** tab, click the **disable** radio button for each service that you want to disable.
Step 4 Click **Save Changes**.