Configuring Communication Services

This chapter includes the following sections:

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.
HTTPS	This service is enabled on port 443 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTPS, all data is exchanged in encrypted mode through a secure server.

Communication Service	Description
	For security purposes, we recommend that you enable HTTPS and disable HTTP.
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 In the **Admin** tab, expand **All ➤ 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 In the **Admin** tab, expand **All ➤ Communication Services**.

Step 3 Select 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 will use for HTTP.
The default port is 80.

Step 6 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

Procedure

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

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

Step 3 Right-click **Root** 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 ➤ Root**.

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 ➤ Root**.

Step 3 Right-click **Root** 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.
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 ➤ Root**.

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

Procedure

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

Step 2 In the **Admin** tab, expand **All ➤ 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 will use for HTTPS.
The default port is 443.

Step 6 (Optional) In the **Key Ring** field, enter the name of the key ring you created for HTTPS.

Caution If you update the **Key Ring** field, all current HTTP and HTTPS sessions will be closed without warning after you click **Save Changes**.

Step 7 Click **Save Changes**.

Step 8 Click **OK**.

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 ➤ Root**.
Step 3 Right-click the key ring you want to delete and select **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Deleting a Trusted Point

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All ➤ Key Management ➤ Root**.
Step 3 Right-click the trusted point you want to delete and select **Delete**.
Step 4 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 5 Click **OK**.

Configuring SNMP

Enabling SNMP and Configuring an SNMP Community

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 In the **Admin** tab, expand **All ➤ 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 In the **Community** field, enter the default community name that Cisco UCS Manager GUI should include with any trap messages it sends to the SNMP server.
The default community is public.

Step 6 Click **Save Changes**.

What to Do Next

Create SNMP trap hosts and users.

Creating an SNMP Trap Host

Procedure

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

Step 2 In the **Admin** tab, expand **All ➤ 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 the fabric interconnect should send the trap.
Community field	The community name the fabric interconnect includes when it sends the trap to the SNMP host. This must be the same community as you configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters.
Port field	The port on which the fabric interconnect communicates with the SNMP host. The default port is 162.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMP Trap Host

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 In the **Admin** tab, expand **All ➤ Communication Services**.
Step 3 Select the **Communication Services** tab.
Step 4 In the **SNMP Trap Hosts** 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 In the **Admin** tab, expand **All ➤ 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 user name cannot be the same as a local user name. Choose an SNMP user name that does not match a local user name.
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.

Name	Description
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 In the **Admin** tab, expand **All ➤ 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 In the **Admin** tab, expand **All ➤ 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 In the **Admin** tab, expand **All ➤ 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**.