UCS Manager Communication Services

Communication Protocols

Communication Services

You can use the communication services defined below to interface third-party applications with Cisco UCS.

Cisco UCS Manager supports IPv4 and IPv6 address access for the following services:

- CIM XML
- HTTP
- HTTPS
- SNMP
- SSH
- Telnet

Cisco UCS Manager supports out-of-band IPv4 address access to the **Cisco UCS KVM Direct** launch page from a web browser. To provide this access, you must enable the following service:

- CIMC Web Service

Communication Service	Description
CIM XML	The Common Information Model (CIM) XML) service is disabled by default and is only available in read-only mode. The default port is 5988. The CIM XML is a standards-based protocol for exchanging CIM information that the Distributed Management Task Force defines.

Communication Service	Description
CIMC Web Service	This service is disabled by default. When this service is enabled, users can directly access a server CIMC using one of the out-of-band management IP addresses assigned directly to the server, or associated with the server through a service profile. **Note** CIMC Web Service can only be enabled or disabled globally. You cannot configure KVM direct access for individual CIMC IP addresses.
HTTP	By default, HTTP is enabled on port 80. You can run the Cisco UCS Manager GUI in an HTTP or HTTPS browser. If you select HTTP, all data is exchanged in clear text mode. For a secure browser session, we recommend that you enable HTTPS and disable HTTP. By default, Cisco UCS implements a browser redirects to an HTTPS equivalent and recommends that you do not change this behavior. **Note** If you are upgrading to Cisco UCS, version 1.4(1), the browser redirect to a secure browser does not occur by default. To redirect the HTTP browser to an HTTPS equivalent, enable the **Redirect HTTP to HTTPS** in Cisco UCS Manager.
HTTPS	By default, HTTPS is enabled on port. With HTTPS, all data is exchanged in encrypted mode through a secure server. For a secure browser session, 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 that the Distributed Management Task Force defines.
SNMP	By default, this service is disabled. 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, and you cannot change the default port. This service provides access to the Cisco UCS Manager CLI.
Telnet	By default, this service is disabled. This service provides access to the Cisco UCS Manager CLI.

Non-Secure Communication Services

Web Session Limits for User Accounts

Cisco UCS Manager uses web session limits to restrict the number of web sessions (both GUI and XML) that a given user account is permitted to access at any one time.

Each Cisco UCS Manager domain supports a maximum of 32 concurrent web sessions per user and 256 total user sessions. By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32 per user, but this value can be configured up to the system maximum of 256.

Setting Web Session Limits

Procedure

Step 1 Navigate to **Admin** > **Communication Management** > **Communication Services**

Step 2 Under Web Session Limits, complete the following fields:

Name	Description
Maximum Sessions Per User	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.
Maximum Sessions	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.
Maximum Event Interval (in seconds)	The maximum time interval between two events. This tracks various types of event change notifications, such as responses to any user requests from the UI. If the interval expires, the UI session is terminated. Enter and integer between 120-3600

Step 3 Click **Save Changes**.

Setting Shell Session Limits

Procedure

Step 1 Navigate to **Admin** > **Communication Management** > **Communication Services**

Step 2 Under Shell Session Limits, complete the following fields:

Name	Description
Maximum Sessions Per User	The maximum number of concurrent shell sessions allowed per user. Enter an integer between 1-32.
Maximum Sessions	The maximum number of concurrent shell sessions allowed for all users within the system. Enter an integer between 1-32.

Step 3 Click **Save Changes**.

Configuring CIM-XML

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **CIM-XML** area, click the **Enabled** radio button.

The **CIM-XML** area expands to display the default **Port** number, 5988. You cannot change this port number.

Step 4 Click **Save Changes**.

Configuring HTTP

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **HTTP** area, click the **Enabled** radio button.

The **HTTP** area expands to display the available configuration options.

Step 4 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTP.

The default port is 80.

Step 5 (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.

Note If you redirect HTTP to HTTPS, you cannot use HTTP to access Cisco UCS Manager GUI. Redirection disables HTTP as it automatically redirects to HTTPS.

Step 6 Click **Save Changes**.

Secure Communication Services

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.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

This operation is only available in the UCS Manager CLI.

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.

You can change the self-signed KVM certificate on CIMC for UCS M7M6, M5 servers to a user-generated public certificate. However, a password protected X.509 certificate private key is not supported. provides detailed information about this process.

Important The certificate must be in Base64 encoded X.509 (CER) format.

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.

Related Topics

Changing the KVM Certificate, on page 8

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 **Admin**.

Step 2 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:

- **Mod2048**
- **Mod2560**
- **Mod3072**
- **Mod3584**
- **Mod4096**

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 **Admin**.

Step 2 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
DNS field	The Domain Name System (DNS) assigned to the network that corresponds to the Hostname, Fully Qualified Domain Name (FQDN), or IP Address. Enter the domain name. A maximum of three comma separated domain names can be entered in this field. For example, you can enter www.example1.com,www.example2.com,www.example3.com
Locality field	The city or town in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
State field	The state or province in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Country field	The country code corresponding to the country in which the company resides. Enter two alphabetic characters.
Organization Name field	The organization requesting the certificate. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Organization Unit Name field	The organizational unit. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Email field	The email address associated with the request.
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. **Note** Ensure this Subject name is not the same as the domain name specified in the DNS field.

Step 7 To assign IP addresses, click the **IPv4** or **IPv6** tab. The choice you make depends upon how the fabric interconnects were configured when you set up Cisco UCS Manager.

- Click the IPv4 tab, and complete the following fields:

Name	Description
IP Address field	The IPv4 address of the Cisco UCS domain.
FI-A IP field	The IPv4 address of fabric interconnect A.
FI-B IP field	The IPv4 address of fabric interconnect B.

- Click the IPv6 tab, and complete the following fields:

Name	Description
IP Address field	The IPv6 address of the Cisco UCS domain.
FI-A IP field	The IPv6 address of fabric interconnect A.
FI-B IP field	The IPv6 address of fabric interconnect B.

Step 8 Click **OK**.

Step 9 Copy the text of the certificate request from the **Request** field and save in a file.

Step 10 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.

Changing the KVM Certificate

You can use this procedure to change the KVM certificate to a user-generated public certificate.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to change the KVM certificate.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Change KVM Certificate**:

Step 7 In the **Change KVM Certificate** dialog box, complete the following fields:

Field	Description
Certificate field	A user-generated public certificate.

Field	Description
Key field	The corresponding user-generated private key. **Note** Password protected X.509 certificate private key is not supported.

Step 8 Click **OK**.

Step 9 If a confirmation dialog box appears, click **Yes**.

This operation will result in a reboot of the CIMC

Clearing the KVM Certificate

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to clear the KVM certificate.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Clear KVM Certificate**:

Step 7 In the **Clear KVM Certificate** dialog box, click **Yes**.

This operation will result in a reboot of the CIMC

Creating a Trusted Point

Procedure

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

Step 2 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. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Certificate Chain field	The certificate information for this trusted point. **Important** The certificate must be in Base64 encoded X.509 (CER) format. For windows 2012 server, using RSASSA-PSS returns the following error occurs: Trustpoint's cert-chain is invalid, reason: unknown. UCS Manager does not support this algorithm.

Step 5 Click **OK**.

What to do next

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

Importing a Certificate into a Key Ring

Procedure

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

Step 2 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.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Tip If the fields in an area do not display, 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 for the HTTPS to use, 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 **Admin**.

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **HTTPS** area, click the **Enabled** radio button.

The **HTTPS** area expands to display the available configuration options.

Step 4 Complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.
Port field	The port to use for HTTPS connections. Specify an integer between 1 and 65535. By default, HTTPS is enabled on port.
Operational Port field	The port Cisco UCS Manager requires for system-level HTTPS communication. You cannot change this port.
Key Ring drop-down list	The key ring for HTTPS connections.
Cipher Suite Mode field	The level of Cipher Suite security used by the Cisco UCS domain. This can be one of the following: • **High Strength** • **Medium Strength** • **Low Strength** • **Custom**—Allows you to specify a user-defined Cipher Suite specification string.

Name	Description
Cipher Suite field	If you select **Custom** in the **Cipher Suite Mode** field, specify the user-defined Cipher Suite specification string in this field. The Cipher Suite specification string can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). For details, see http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite. For example, the medium strength specification string Cisco UCS Manager uses as the default is: `ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`
Allowed SSL Protocols	Enables you to choose which SSL protocols can be used. Values are **Default (Allow all except SSLv2 and SSLv3)** and **Only TLSV1.2.** If you choose Only TSLV1.2, all web client connections trying to use less secure versions of TLS are blocked.

Step 5 Click **Save Changes**.

Deleting a Key Ring

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Key Management**.
Step 3 Right-click the key ring you want to delete and choose **Delete**.
Step 4 If a confirmation dialog box displays, 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 **Admin**.
Step 2 Expand **All** > **Key Management**.
Step 3 Right-click the trusted point you want to delete and choose **Delete**.
Step 4 If a confirmation dialog box displays, click **Yes**.

Step 5 Click **OK**.

Network-Related Communication Services

Enabling SNMP and Configuring SNMP Properties

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

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

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

Step 4 In the **SNMP** area, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** Enable this service only if your system includes integration with an SNMP server. If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.

Step 5 Click **Save Changes**.

What to do next

Create SNMP traps and users.

Enabling the CIMC Web Service

The CIMC web service is enabled by default. Follow the steps below to enable the service if it is disabled.

Note Access to Port Number 443 is blocked when the CIMC Web Service **Admin State** is in **Disabled** mode. To enable access, set CIMC Web Service **Admin State** to **Enabled** mode.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Communication Management** > **Communication Services**.
Step 3 Select the **Communication Services** tab.
Step 4 In the **CIMC Web Service** 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 **Admin**.
Step 2 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**.

Enabling Telnet

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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**.