UCS Manager Communication Services

- Communication Services, on page 1
- NonSecure Communication Services, on page 3
- Secure Communication Services, on page 8
- Network-Related Services, on page 24

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.

NonSecure Communication Services

Setting Web Session Limits

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system** .	Enters system mode.
Step 2	UCS-A /system # **scope services** .	Enters services mode.
Step 3	UCS-A /system/services # **scope web-session-limits** .	Enters webs session limits mode.
Step 4	UCS-A /system/services/web-session-limits # **set** {**maximum-event-interval** |**per-user** | **total**}*number* .	Enables you to set the following web session limits:
Step 5	UCS-A /system/services/web-session-limits # **commit-buffer** .	Commits the transaction to the system configuration.

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. 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

Example

The following example shows how to set the maximum-event-interval:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits # set maximum-event-interval 300
UCS-A /system/services/web-session-limits # commit buffer
```

Viewing Web Session Limits

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters services mode.
Step 3	/system/services # **show web-session-limits**	Shows the web session settings.

Example

The following example shows how to view web session limits:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # show web-session-limits
Web Sessions:
    Maximum logins for single user Maximum Sessions Maximum Event Interval (sec)
    ------------------------------ ---------------- ----------------------------
    32                             256              600
UCS-A /system/services #
```

Setting Shell Session Limits

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system** .	Enters system mode.
Step 2	UCS-A /system # **scope services** .	Enters services mode.
Step 3	UCS-A /system/services # **scope shell-session-limits**	
Step 4	UCS-A /system/services/shell-session-limits # **set** {**per-user** |**total**}*number*.	Enables you to set the following shell session limits:

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Maximum Sessions Per User</td><td>The maximum number of concurrent shell sessions allowed per user.
Enter an integer between 1-32.
Note
The maximum session per user can vary based on the specific Fabric Interconnect model. For more information, refer to the relevant release versions of Cisco UCS 6400, 6536, 6664, and UCSX-S9108-100G FI Configuration Limits for Cisco UCS Manager.</td></tr>
<tr><td>Maximum Sessions</td><td>The maximum number of concurrent shell sessions allowed for all users within the system.
Enter an integer between 1-32.</td></tr>
</table>
</td></tr>
<tr><td>Step 5</td><td>UCS-A /system/services/shell-session-limits # commit-buffer .</td><td>Commits the transaction to the system configuration.</td></tr>
</table>

Example

The following example shows how to set the maximum sessions:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope shell-session-limits
UCS-A /system/services/shell-session-limits # set maximum-sessions 20
UCS-A /system/services/shell-session-limits # commit buffer
```

Viewing Shell Session Limits

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters services mode.
Step 3	/system/services # **show shell-session-limits**	Shows the shell session settings.

Example

The following example shows how to view shell session limits:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # show shell-session-limits
Shell Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             32
UCS-A /system/services #
```

Configuring CIM XML

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **enable cimxml**	Enables the CIM XLM service.
Step 4	UCS-A /system/services # **set cimxml port** *port-num*	Specifies the port for the CIM XML connection.
Step 5	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables CIM XML, sets the port number to 5988, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable cimxml
UCS-A /system/services* # set cimxml port 5988
```

```
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Configuring HTTP

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **enable http**	Enables the HTTP service.
Step 4	UCS-A /system/services # **set http port** *port-num*	Specifies the port to be used for the HTTP connection.
Step 5	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables HTTP, sets the port number to 80, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http
UCS-A /system/services* # set http port 80
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Unconfiguring HTTP

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **disable http**	Disables the HTTP service.
Step 4	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disables HTTP and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable http
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Secure Communication Services

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

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **enable https**	Enables the HTTPS service.
Step 4	(Optional) UCS-A /system/services # **set https port** *port-num*	Specifies the port to be used for the HTTPS connection.
Step 5	(Optional) UCS-A /system/services # **set https keyring** *keyring-name*	Specifies the name of the key ring you created for HTTPS.
Step 6	(Optional) UCS-A /system/services # **set https cipher-suite-mode** *cipher-suite-mode*	The level of Cipher Suite security used by the Cisco UCS domain. *cipher-suite-mode* can be one of the following keywords: • **high-strength** • **medium-strength** • **low-strength** • **custom**—Allows you to specify a user-defined Cipher Suite specification string.

	Command or Action	Purpose
Step 7	(Optional) UCS-A /system/services # **set https cipher-suite** *cipher-suite-spec-string*	Specifies a custom level of Cipher Suite security for this Cisco UCS domain if **cipher-suite-mode** is set to **custom**. *cipher-suite-spec-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 **Note** This option is ignored if **cipher-suite-mode** is set to anything other than **custom**.
Step 8	(Optional) UCS-A /system/services # **set https ssl-protocol** *default|tls1-2|tls1-3*	Enables you to choose which SSL protocols can be used. This can be one of the following: • **Default (Allow all except SSLv2 and SSLv3)** • **Only TLSv1.2** **Note** If you choose Only TLSv1.2, all web client connections trying to use less secure versions of TLS are blocked. • **Only TLSv1.3** **Note** If you choose Only TLSv1.3, all web client connections trying to use less secure versions of TLS are blocked.
Step 9	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables HTTPS, sets the port number to 443, sets the key ring name to kring7984, sets the Cipher Suite security level to high, configures the web server to accept only connections using TLSv1.2, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable https
UCS-A /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # set https keyring kring7984
UCS-A /system/services* # set https cipher-suite-mode high
UCS-A /system/services* # set https ssl-protocol tls1-2
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Unconfiguring HTTPS

Before you begin

Disable HTTP to HTTPS redirection.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **disable https**	Disables the HTTPS service.
Step 4	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disables HTTPS and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable https
UCS-A /system/services* # commit-buffer
UCS-A /system/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 Cisco UCS servers to a user-generated public certificate. However, a password protected X.509 certificate private key is not supported. Changing the KVM Certificate, on page 19 Creating a KVM Certificate, on page 18 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 19

Creating an Untrusted CA-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a certificate, you can operate your own CA and sign your own certificates. To generate the certificate-key pair, you must generate a 2048 bit RSA key and an x.509 PEM certificate. This section shows commands for creating a CA and generating a certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see http://www.openssl.org.

Note These commands are to be entered on a Linux server with the OpenSSL package.

Before you begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out cert.private 2048`	This command generates an RSA private key that will be used by the CA. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key cert.private -out cert.pem`	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	(Optional) **openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** **Example:** `# openssl x509 -req -days 365 -in csr.txt -CA cert.pem -set_serial 04 -CAkey cert.private -out myserver05.crt -extfile openssl.conf`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

Example

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
# /usr/bin/openssl genrsa -out cert.private 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key cert.private -out cert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
```

```
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA cert.pem -set_serial 01
-CAkey cert.private -out server.crt -extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

Creating a Key Ring

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **create keyring** *keyring-name*	Creates and names the key ring.
Step 3	UCS-A /security/keyring # **set modulus** {**mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}	Sets the SSL key length in bits.
Step 4	UCS-A /security/keyring # **commit-buffer**	Commits the transaction.

Example

The following example creates a keyring with a key size of 1024 bits:

```
UCS-A# scope security
UCS-A /security # create keyring kr220
UCS-A /security/keyring* # set modulus 'modvalue'
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

What to do next

Create a certificate request for this key ring.

Regenerating the Default Key Ring

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope keyring default**	Enters key ring security mode for the default key ring.
Step 3	UCS-A /security/keyring # **set regenerate yes**	Regenerates the default key ring.
Step 4	UCS-A /security/keyring # **commit-buffer**	Commits the transaction.

Example

The following example regenerates the default key ring:

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring* # set regenerate yes
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

Creating a Certificate Request for a Key Ring with Basic Options

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope keyring** *keyring-name*	Enters configuration mode for the key ring.
Step 3	UCS-A /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}	Creates a certificate request using the IPv4 or IPv6 address specified, or the name of the fabric interconnect. You are prompted to enter a password for the certificate request.
Step 4	UCS-A /security/keyring/certreq # **commit-buffer**	Commits the transaction.
Step 5	UCS-A /security/keyring # **show certreq**	Displays the certificate request, which you can copy and send to a trust anchor or certificate authority.

Example

The following example creates and displays a certificate request with an IPv4 address for a key ring, with basic options:

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

UCS-A /security/keyring #
```

Creating a Certificate Request for a Key Ring with Advanced Options

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope keyring** *keyring-name*	Enters configuration mode for the key ring.
Step 3	UCS-A /security/keyring # **create certreq**	Creates a certificate request.
Step 4	UCS-A /security/keyring/certreq* # **set country** *country name*	Specifies the country code of the country in which the company resides.
Step 5	UCS-A /security/keyring/certreq* # **set dns** *DNS Name*	Specifies the Domain Name Server (DNS) address associated with the request. 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
Step 6	UCS-A /security/keyring/certreq* # **set e-mail** *E-mail name*	Specifies the email address associated with the certificate request.

	Command or Action	Purpose
Step 7	UCS-A /security/keyring/certreq* # **set ip** *certificate request ip-address* | **ipv6** *certificate request ipv6-address*	Specifies the IPv4 or IPv6 address of the Cisco UCS domain.
Step 8	UCS-A /security/keyring/certreq* # **set fi-a-ip** *certificate request FI A ip-address* | **fi-a-ipv6** *certificate request FI A ipv6-address*	The IPv4 or IPv6 address of fabric interconnect A.
Step 9	UCS-A /security/keyring/certreq* # **set fi-b-ip** *certificate request FI B ip-address* | **fi-b-ipv6** *certificate request FI B ipv6-address*	The IPv4 or IPv6 address of fabric interconnect B.
Step 10	UCS-A /security/keyring/certreq* # **set locality** *locality name (eg, city)*	Specifies the city or town in which the company requesting the certificate is headquartered.
Step 11	UCS-A /security/keyring/certreq* # **set org-name** *organization name*	Specifies the organization requesting the certificate.
Step 12	UCS-A /security/keyring/certreq* # **set org-unit-name** *organizational unit name*	Specifies the organizational unit.
Step 13	UCS-A /security/keyring/certreq* # **set password** *certificate request password*	Specifies an optional password for the certificate request.
Step 14	UCS-A /security/keyring/certreq* # **set state** *state, province or county*	Specifies the state or province in which the company requesting the certificate is headquartered.
Step 15	UCS-A /security/keyring/certreq* # **set subject-name** *certificate request name*	Specifies the fully qualified domain name of the Fabric Interconnect. **Note** Ensure the **subject-name** is not same as the **dns** name.
Step 16	UCS-A /security/keyring/certreq* # **commit-buffer**	Commits the transaction.
Step 17	UCS-A /security/keyring # **show certreq**	Displays the certificate request, which you can copy and send to a trust anchor or certificate authority.

Example

The following example creates and displays a certificate request with an IPv4 address for a key ring, with advanced options:

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq
UCS-A /security/keyring/certreq* # set ip 192.168.200.123
UCS-A /security/keyring/certreq* # set fi-a-ip 192.168.200.124
```

```
UCS-A /security/keyring/certreq* # set fi-b-ip 192.168.200.125
UCS-A /security/keyring/certreq* # set subject-name sjc04
UCS-A /security/keyring/certreq* # set country US
UCS-A /security/keyring/certreq* # set dns bg1-samc-15A,bg2-samc-15A,bg3-samc-15A
UCS-A /security/keyring/certreq* # set e-mail test@cisco.com
UCS-A /security/keyring/certreq* # set locality new york city
UCS-A /security/keyring/certreq* # set org-name "Cisco Systems"
UCS-A /security/keyring/certreq* # set org-unit-name Testing
UCS-A /security/keyring/certreq* # set state new york
UCS-A /security/keyring/certreq* # commit-buffer
UCS-A /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request FI A ip address: 192.168.200.124
Certificate request FI B ip address: 192.168.200.125
Certificate request e-mail name: test@cisco.com
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----
UCS-A /security/keyring/certreq #
```

What to do next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a KVM Certificate

You can use this procedure to create the KVM certificate. This operation will result in a reboot of the CIMC.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope cimc**	Enters chassis server CIMC mode.
Step 3	UCS-A /chassis/server/cimc # **create kvm-certificate**	Creates the KVM certificate.
Step 4	UCS-A /chassis/server/cimc/kvm-certificate* # set certificate	Sets the specified user-generated public certificate.
Step 5	UCS-A /chassis/server/cimc/kvm-certificate* # set key	Sets the corresponding user-generated private key. **Note** Password protected X.509 certificate private key is not supported.
Step 6	UCS-A /chassis/server/cimc/kvm-certificate* # **commit-buffer**	Commits the transaction to the system configuration. This operation will result in a reboot of the CIMC.

Example

The following example creates a KVM certificate and commits the transaction:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # create kvm-certificate
UCS-A /chassis/server/cimc/kvm-certificate* # set certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>
...

UCS-A /chassis/server/cimc/kvm-certificate* # set key
```

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Key:
>
...

UCS-A /chassis/server/cimc/kvm-certificate* # commit-buffer
UCS-A /chassis/server/cimc/kvm-certificate #
```

Clearing a KVM Certificate

This operation will result in a reboot of the CIMC.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / blade-id*	Enters chassis server mode for the specified server.
Step 2	UCS-A /chassis/server # **scope cimc**	Enters chassis server CIMC mode.
Step 3	UCS-A /chassis/server/cimc # **clear kvm-certificate**	Clears the KVM certificate.
Step 4	UCS-A /chassis/server/cimc* # **commit-buffer**	Commits the transaction to the system configuration. This operation will result in a reboot of the CIMC.

Example

The following example clears a KVM certificate and commits the transaction:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # clear kvm-certificate
Warning: When committed, this operation will result in CIMC reboot.
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

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.
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

Creating a Trusted Point

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **create trustpoint** *name*	Creates and names a trusted point.
Step 3	UCS-A /security/trustpoint # **set certchain** [*certchain*]	Specifies certificate information for this trusted point. If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trustpoints defining a certification path to the root certificate authority (CA). On the next line following your input, type ENDOFBUF to finish. **Important** The certificate must be in Base64 encoded X.509 (CER) format.
Step 4	UCS-A /security/trustpoint # **commit-buffer**	Commits the transaction.

Example

The following example creates a trusted point and provides a certificate for the trusted point:

```
UCS-A# scope security
UCS-A /security # create trustpoint tPoint10
UCS-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/trustpoint* # commit-buffer
UCS-A /security/trustpoint #
```

What to do next

Obtain a key ring certificate from the trust anchor or certificate authority and import it into the key ring.

Importing a Certificate into a Key Ring

Before you begin

- Configure a trusted point that contains the certificate chain for the key ring certificate.
- Obtain a key ring certificate from a trust anchor or certificate authority.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **scope keyring** *keyring-name*	Enters configuration mode for the key ring that will receive the certificate.

	Command or Action	Purpose
Step 3	UCS-A /security/keyring # **set trustpoint** *name*	Specifies the trusted point for the trust anchor or certificate authority from which the key ring certificate was obtained.
Step 4	UCS-A /security/keyring # **set cert**	Launches a dialog for entering and uploading the key ring certificate. At the prompt, paste the certificate text that you received from the trust anchor or certificate authority. On the next line following the certificate, type ENDOFBUF to complete the certificate input. **Important** The certificate must be in Base64 encoded X.509 (CER) format.
Step 5	UCS-A /security/keyring # **commit-buffer**	Commits the transaction.

Example

The following example specifies the trust point and imports a certificate into a key ring:

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # set trustpoint tPoint10
UCS-A /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

What to do next

Configure your HTTPS service with the key ring.

Deleting a Key Ring

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **delete keyring** *name*	Deletes the named key ring.
Step 3	UCS-A /security # **commit-buffer**	Commits the transaction.

Example

The following example deletes a key ring:

```
UCS-A# scope security
UCS-A /security # delete keyring key10
UCS-A /security* # commit-buffer
UCS-A /security #
```

Deleting a Trusted Point

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope security**	Enters security mode.
Step 2	UCS-A /security # **delete trustpoint** *name*	Deletes the named trusted point.
Step 3	UCS-A /security # **commit-buffer**	Commits the transaction.

Example

The following example deletes a trusted point:

```
UCS-A# scope security
UCS-A /security # delete trustpoint tPoint10
UCS-A /security* # commit-buffer
UCS-A /security #
```

Enabling HTTP Redirection to HTTPS

Before you begin

Enable both HTTP and HTTPS.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **enable http-redirect**	Enables the HTTP redirect service. If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. This option effectively disables HTTP access to this Cisco UCS domain.
Step 4	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables HTTP to HTTPS redirection and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http-redirect
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Network-Related Services

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 supports 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

Simple Network Management Protocol (SNMP) offers versions such as SNMPv1, SNMPv2c, and SNMPv3—each with its own 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 requires protection from disclosure or whether the message is authenticated. The supported security level depends on 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 the combinations of security models and levels.

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 (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 through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes only configured users to perform management operations 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 are not altered or destroyed in an unauthorized manner, and that data sequences are not altered beyond what can occur non-maliciously.
- Message origin authentication—Ensures that the identity of a message originator is verifiable.
- 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 http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html for B-series servers, and http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html C-series servers.

Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

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

Cisco UCS Manager Release 3.2(3) and later releases do not support MD5 authentication if SNMPv3 is in Federal Information Processing Standards (FIPS) mode. Hence, any existing or newly created SNMPv3 users with MD5 authentication will not be deployed with these releases and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: MD5 auth is not supported
```

To deploy such a user, modify the authentication type to **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.

Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without AES encryption. Hence, any existing or newly created SNMPv3 users without AES encryption will not be deployed with these releases, and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: AES is not enabled
```

To deploy such a user, enable **AES-128** encryption.

Enabling SNMP and Configuring SNMP Properties

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.

	Command or Action	Purpose
Step 2	UCS-A /monitoring # **enable snmp**	Enables SNMP.
Step 3	UCS-A /monitoring # **set snmp community**	Enters snmp community mode.
Step 4	UCS-A /monitoring # **Enter a snmp community:** *community-name*	Specifies SNMP community. Use the community name as a password. The community name can be any alphanumeric string up to 32 characters.
Step 5	UCS-A /monitoring # **set snmp syscontact** *system-contact-name*	Specifies the system contact person responsible for the SNMP. The system contact name can be any alphanumeric string up to 255 characters, such as an email address or name and telephone number.
Step 6	UCS-A /monitoring # **set snmp syslocation** *system-location-name*	Specifies the location of the host on which the SNMP agent (server) runs. The system location name can be any alphanumeric string up to 512 characters.
Step 7	UCS-A /monitoring # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables SNMP, configures an SNMP community named SnmpCommSystem2, configures a system contact named contactperson, configures a contact location named systemlocation, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community
UCS-A /monitoring* # Enter a snmp community: SnmpCommSystem2
UCS-A /monitoring* # set snmp syscontact contactperson1
UCS-A /monitoring* # set snmp syslocation systemlocation
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

What to do next

Create SNMP traps and users.

Creating an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.

	Command or Action	Purpose
Step 2	UCS-A /monitoring # **enable snmp**	Enables SNMP.
Step 3	UCS-A /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}	Creates an SNMP trap host with the specified host name, IPv4 address, or IPv6 address. The host name can be a fully qualified domain name of an IPv4 address.
Step 4	UCS-A /monitoring/snmp-trap # **set community** *community-name*	Specifies the SNMP community name to be used for the SNMP trap.
Step 5	UCS-A /monitoring/snmp-trap # **set port** *port-num*	Specifies the port to be used for the SNMP trap.
Step 6	UCS-A /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}	Specifies the SNMP version and model used for the trap.
Step 7	(Optional) UCS-A /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}	The type of trap to send. If you select v2c or v3 for the version, this can be: • **traps**—SNMP trap notifications • **informs**—SNMP inform notifications
Step 8	(Optional) UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** | **noauth** | **priv**}	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 9	UCS-A /monitoring/snmp-trap # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables SNMP, creates an SNMP trap using an IPv4 address, specifies that the trap will use the SnmpCommSystem2 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap 192.168.100.112
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

The following example enables SNMP, creates an SNMP trap using an IPv6 address, specifies that the trap will use the SnmpCommSystem3 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap  2001::1
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem3
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

Deleting an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}	Deletes the specified SNMP trap host with the specified hostname or IP address.
Step 3	UCS-A /monitoring # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes the SNMP trap at IP address 192.168.100.112 and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap 192.168.100.112
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Creating an SNMPv3 User

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **enable snmp**	Enables SNMP.
Step 3	UCS-A /monitoring # **create snmp-user** *user-name*	Creates the specified SNMPv3 user.

	Command or Action	Purpose
		An SNMP username cannot be the same as a local username. Choose an SNMP username that does not match a local username.
Step 4	UCS-A /monitoring/snmp-user # **set aes-128** {**no** | **yes**}	Enables or disables the use of AES-128 encryption.
Step 5	UCS-A /monitoring/snmp-user # **set auth** {**md5** | **sha**}	Specifies the use of MD5 or DHA authentication.
Step 6	UCS-A /monitoring/snmp-user # **set password**	Specifies the user password. After you enter the **set password** command, you are prompted to enter and confirm the password.
Step 7	UCS-A /monitoring/snmp-user # **set priv-password**	Specifies the user privacy password. After you enter the **set priv-password** command, you are prompted to enter and confirm the privacy password.
Step 8	UCS-A /monitoring/snmp-user # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables SNMP, creates an SNMPv3 user named snmp-user14, disables AES-128 encryption, specifies the use of MD5 authentication, sets the password and privacy password, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-user snmp-user14
UCS-A /monitoring/snmp-user* # set aes-128 no
UCS-A /monitoring/snmp-user* # set auth md5
UCS-A /monitoring/snmp-user* # set password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # commit-buffer
UCS-A /monitoring/snmp-user #
```

Deleting an SNMPv3 User

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.

	Command or Action	Purpose
Step 2	UCS-A /monitoring # **delete snmp-user** *user-name*	Deletes the specified SNMPv3 user.
Step 3	UCS-A /monitoring # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes the SNMPv3 user named snmp-user14 and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-user snmp-user14
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Enabling Telnet

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /services # **enable telnet-server**	Enables the Telnet service.
Step 4	UCS-A /services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example enables Telnet and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /services # enable telnet-server
UCS-A /services* # commit-buffer
UCS-A /services #
```

Enabling the CIMC Web Service

To enable the CIMC Web Service:

- You must be logged in with admin privileges.
- The CIMC web service must be disabled, as it is enabled by default.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system** /	Enters the system mode.
Step 2	UCS-A /system #**scope services**/	Enters the services mode for the system.
Step 3	UCS-A/system/services #**enable cimcwebsvc**/	Enable the CIMC web service.
Step 4	UCS-A/system/services *# **commit-buffer**/	Commits the transaction to the system configuration.

Example

The following example shows how to enable the CIMC web service and save the transaction:

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # enable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Enabled
```

Disabling the CIMC Web Service

To disable the CIMC Web Service:

- You must be logged in with admin privileges.
- The CIMC web service must be enabled.

Note The CIMC web service is enabled by default.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system** /	Enters the system mode.
Step 2	UCS-A /system #**scope services**/	Enters the services mode for the system.
Step 3	UCS-A/system/services #**disable cimcwebsvc**/	Disables the CIMC web service.
Step 4	UCS-A/system/services *# **commit-buffer**/	Commits the transaction to the system configuration.

Example

The following example shows how to disable the CIMC web service and save the transaction:

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # disable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Disabled
```

Disabling Communication Services

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope services**	Enters system services mode.
Step 3	UCS-A /system/services # **disable** *service-name*	Disables the specified service, where the *service-name* argument is one of the following keywords: • *cimxml* —Disables CIM XML service • **http** —Disables HTTP service • **https** —Disables HTTPS service • **telnet-server** —Disables Telnet service
Step 4	UCS-A /system/services # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disables CIM XML and commits the transaction:

```
UCS-A# scope system
UCS-A# scope services
UCS-A /system/services # disable cimxml
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```