



Configuring Communication Services

This chapter includes the following sections:

- [Communication Services, page 1](#)
- [Configuring CIM XML, page 2](#)
- [Configuring HTTP, page 3](#)
- [Configuring HTTPS, page 3](#)
- [Configuring SNMP, page 4](#)
- [Configuring Telnet, page 8](#)
- [Disabling Communication Services, page 8](#)

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. Only enable this service 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



Note

Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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 XML service.
Step 4	UCS-A /system/services # set cimxml port <i>port-num</i>	Specifies the port to be used for the CIM XML connection.
Step 5	UCS-A /system/services # commit-buffer	Commits the transaction to the system configuration.

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



Note Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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 <i>port-num</i>	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.

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

Configuring HTTPS



Note Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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.

	Command or Action	Purpose
Step 4	UCS-A /system/services # set https port <i>port-num</i>	Specifies the port to be used for the HTTPS connection.
Step 5	UCS-A /system/services # set https keyring <i>keyring-name</i>	Specifies the name for the HTTPS keyring. Caution When the HTTPS keyring is modified using the set https keyring command, all current HTTP and HTTPS sessions will be closed without any warning.
Step 6	UCS-A /system/services # commit-buffer	Commits the transaction to the system configuration.

The following example enables HTTPS, sets the port number to 443, sets the key ring name to kring7984, 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
UCS-A /system/services* # set https keyring kring7984
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Configuring SNMP

Configuring an SNMP Community



Note Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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 # set snmp community <i>community-name</i>	Specifies SNMP community. The community name can be any alphanumeric string up to 32 characters.
Step 4	UCS-A /monitoring # commit-buffer	Commits the transaction to the system configuration.

The following example enables SNMP, configures an SNMP community named `SnpCommSystem2`, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community SnpCommSystem2
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Configuring an SNMPv3 User



Note

Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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 <i>user-name</i>	Creates the specified SNMPv3 user.
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.

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.
Step 2	UCS-A /monitoring # delete snmp-user <i>user-name</i>	Deletes the specified SNMPv3 user.
Step 3	UCS-A /monitoring # commit-buffer	Commits the transaction to the system configuration.

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 #
```

Configuring an SNMP Trap



Note

Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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-trap <i>trap-name</i>	Creates the specified SNMP trap.
Step 4	UCS-A /monitoring/snmp-trap # set community <i>community-name</i>	Specifies the SNMP community name to be used for the SNMP trap.
Step 5	UCS-A /monitoring/snmp-trap # set port <i>port-num</i>	Specifies the port to be used for the SNMP trap.
Step 6	UCS-A /monitoring/snmp-trap # commit-buffer	Commits the transaction to the system configuration.

The following example enables SNMP, creates an SNMP trap named sys-trap2, specifies that the trap will use the SnmpCommSystem2 community on port 2, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap sys-trap2
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
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 <i>trap-name</i>	Deletes the specified SNMP trap.
Step 3	UCS-A /monitoring # commit-buffer	Commits the transaction to the system configuration.

The following example deletes the SNMP trap named sys-trap2 and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap sys-trap2
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Disabling SNMP

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope monitoring	Enters monitoring mode.
Step 2	UCS-A /monitoring # disable snmp	Disables the SNMP service.
Step 3	UCS-A //monitoring # commit-buffer	Commits the transaction to the system configuration.

The following example disables SNMP:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable snmp
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Configuring Telnet



Note Cisco recommends that you enable only the communication services that are required to interface with other network applications.

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.

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 #
```

Disabling Communication Services



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

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 <i>service-name</i>	Disables the specified service, where the <i>service-name</i> argument is one of the following keywords: <ul style="list-style-type: none"> • cimxml—Disables CIM XML service • http—Disables HTTP service • https—Disables HTTPS service • telnet-server—Disables Telnet service

	Command or Action	Purpose
Step 4	UCS-A /system/services # commit-buffer	Commits the transaction to the system configuration.

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 #
```

