Authentication Services

General Settings

You can configure and define policies in Cisco UCS Central at the organization level. Manage them in the infrastructure.

IPv6 Support

Cisco UCS Central supports IPv6 addressing. Cisco UCS Central operates on a dual mode where it enables both IPv4 and IPv6. This feature helps Cisco UCS Central and Cisco UCS Manager communicate with each other through an IPv6 address, primarily to share pools and policy related information.

Cisco UCS Central supports the creation and deletion of IPv4 and IPv6 blocks in the IP pools, and supports IPv6 addressing for the following policies:

- LDAP
- TACAS
- Radius
- NTP
- DNS

You can now register a Cisco UCS Manager domain using an IPv6 address or an IPv4 address.

You can configure an IPv6 address on the Cisco UCS Central through the GUI or CLI commands. This is also true for all the other areas where Cisco UCS Central uses IPv6 addresses.

You can now create a global service profile (GSP) and a local service profile (LSP) using an outband management IPv4 address and an inband IPv4 and/or IPv6 address.

Configuring IPv6 in Standalone Mode

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters system mode.
Step 2	UCSC /system # **scope network-interface a**	Enters network interface of node A.
Step 3	UCSC /network-interface # **scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC /network-interface/ipv6-config # **set net ipv6** *ipv6 address* **ipv6-gw** *IPv6 gateway* **ipv6-prefix** *prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 5	UCSC /network-interface/ipv6-config # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Configures IPv6 in standalone mode
- Commits the transaction.

```
UCSC #scope system
UCSC /system #scope network-interface a
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 ipv6 2001:db8:a::11 ipv6-gw  2001:db8:a::1
 ipv6-prefix  64
UCSC /network-interface/ipv6-config # commit-buffer
```

Configuring IPv6 in High Availability Mode

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters system mode.
Step 2	UCSC /system #**scope network-interface a**	Enters node A of the network interface, which is also the primary virtual machine.
Step 3	UCSC /network-interface #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC /network-interface/ipv6-config #**set net ipv6** *ipv6 address* **ipv6-gw** *ipv6 gateway* **ipv6-prefix** *prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 5	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.

	Command or Action	Purpose
Step 7	UCSC# **scope system**	Enters system mode.
Step 8	UCSC /system #**scope network-interface b**	Enters node B of the network interface, which is also the subordinate virtual machine.
Step 9	UCSC /network-interface/ipv6-config #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 10	UCSC /network-interface/ipv6-config #**set net ipv6***ipv6 address* **ipv6-gw***ipv6 gateway***ipv6-prefix***prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 11	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 12	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.
Step 13	UCSC # **scope system**	Enters system mode.
Step 14	UCSC /system # **set virtual ip ipv6***ipv6 address*	Configures a virtual IPv6 address.
Step 15	UCSC /system # **commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC /system # **top**	Returns to the top most directory.

The following example:

- Configures IPv6 in high availability mode
- Commits the transaction

```
UCSC #scope system
UCSC /system #scope network-interface a
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 2001:db8:a::11 ipv6-gw  2001:db8:a::1
ipv6-prefix  64
UCSC /network-interface/ipv6-config # commit-buffer
UCSC /network-interface/ipv6-config # top

UCSC #scope system
UCSC /system #scope network-interface b
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 2001:db8:a::12 ipv6-gw  2001:db8:a::1
ipv6-prefix  64
UCSC /network-interface/ipv6-config # commit-buffer
UCSC /network-interface/ipv6-config # top

UCSC # scope system
UCSC /system # set virtual-ip ipv6 2001:db8:a::10
UCSC /system # commit-buffer
UCSC /system # top
```

Disabling IPv6

You can disable IPv6 on the Cisco UCS Central by setting the IPv6 address (in both the standalone and HA mode) to null.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **scope system**	Enters system mode.
Step 2	UCSC /system #**scope network-interface a**	Enters node A of the network interface.
Step 3	UCSC /network-interface #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 5	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.
Step 7	UCSC # **scope system**	Enters system mode.
Step 8	UCSC /system #**set virtual-ip ipv6 ::**	Sets the IPv6 address to null, therefore disabling it.
Step 9	UCSC /system # **commit-buffer**	Commits the transaction to the system configuration.
Step 10	UCSC /system # **top**	Returns to the top most directory.
Step 11	UCSC # **scope system**	Enters system mode.
Step 12	UCSC /system # **scope network-interface a**	Enters node A of the network interface.
Step 13	UCSC /network-interface #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 14	UCSC /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 15	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.
Step 17	UCSC # **scope system**	Enters system mode.
Step 18	UCSC /system # **scope network-interface b**	Enters node B of the network interface.
Step 19	UCSC /network-interface #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 20	UCSC /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 21	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 22	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.

Setting the IPv6 value to null moves all of the affected IPv6 devices to a state of lost visibility. The following example:

- Disables IPv6 on Cisco UCS Central for the standalone and HA modes
- Commits the transaction

```
UCSC # scope system
UCSC /system # scope network-interface a
UCSC /network-interface# scope ipv6-config
UCSC /network-interface/ipv6-config #set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC /network-interface/ipv6-config #commit-buffer
UCSC /network-interface/ipv6-config #top
```

```
UCSC # scope system
UCSC /system # set virtual-ip ipv6 ::
UCSC /system # commit-buffer
UCSC /system # top
UCSC # scope system
UCSC /network-interface # scope network-interface a
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC /network-interface/ipv6-config # commit-buffer
UCSC /network-interface/ipv6-config # top
```

```
UCSC # scope system
UCSC /system #  scope network-interface b
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC /network-interface/ipv6-config # commit-buffer
UCSC /network-interface/ipv6-config # top
```

Configuring an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/snmp # **create snmp-trap** *snmp-trap-ip*	(Optional) If scoping into an organization previously created, it creates the SNMP trap IP address for that organization (in format 0.0.0.0), and enters SNMP trap configuration mode.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/snmp # **scope snmp-trap** *snmp-trap-ip*	(Optional) If scoping into organization previously created, it scopes the SNMP trap IP address for that organization (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string*	Enter the SNMP trap community string to configure the SNMP trap host.
Step 8	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set notificationtype traps**	Enter the notification type for the SNMP trap as SNMP trap notifications (traps).
Step 9	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set port** *port-number*	Enter the SNMP trap port number (1-65535).
Step 10	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set v3privilege auth** | **noauth** | **priv**	Enter a V3 privilege security level for the SNMP trap of authNoPriv security level (auth), noAuthNoPriv security level (noauth), or authPriv security level (priv).
Step 11	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set version v1** | **v2c** | **v3**	Enter a version for the SNMP trap of SNMP v1, v2c, or v3.
Step 12	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into an organization
- Scopes the SNMP policy
- Creates the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap01
- Sets the SNMP notification type to traps
- Sets the SNMP port to 1
- Sets the v3privilege to priv
- Sets the version to v1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
```

```
UCSC(policy-mgr) /org/device-profile # scope snmp
UCSC(policy-mgr) /org/device-profile/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # commit-buffer
```

Configuring an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/snmp # **create snmp-user** *snmp-user*	Enter a name for the SNMP user.
Step 6	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set aes-128 yes** | **no**	Use AES-128 for the SNMP user (yes or no).
Step 7	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set auth md5** | **sha**	Use MD5 or SHA authorization mode for the SNMP user.
Step 8	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set password**	Enter and confirm a password for the SNMP user.
Step 9	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set priv-password**	Enter and confirm a private password for the SNMP user.
Step 10	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into an organization
- Scopes the SNMP policy
- Scopes into the SNMP user named snmpuser01

- Sets aes-128 mode to enabled
- Sets authorization to sha mode
- Sets password to userpassword01
- Sets private password to userpassword02
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope snmp
UCSC(policy-mgr) /org/device-profile/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set auth sha
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set password
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set priv-password
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # commit-buffer
```

Configuring an NTP Server

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/timezone-ntp-config # **create ntp** server-name	Creates an NTP server instance.
Step 6	UCSC(policy-mgr) /org/device-profile/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into an organization
- Creates an NTP server instance named orgNTP01

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope timezone-ntp-config
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config # create ntp orgNTP01
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config #
```

Configuring a DNS Server

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope dns-config**	Enter an existing DNS policy's configuration mode from the organization.
Step 5	UCSC(policy-mgr) /org/device-profile/dns-config # **create dns** server-IP-address	Creates a DNS server instance.
Step 6	UCSC(policy-mgr) /org/device-profile/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Creates a DNS server instance named 0.0.0.0
- Commis\ts the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)/org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope dns-config
UCSC(policy-mgr) /org/device-profile # create dns 0.0.0.0
UCSC(policy-mgr) /org/device-profile* # commit-buffer
```

Configuring a Fault Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org # **scope fault policy**	(Optional) If scoping into the domain group root previously created, scopes the default fault policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /org/device-profile/policy* # **set ackaction delete-on-clear**	Sets the fault policy acknowledgment action to delete on clear (delete-on-clear) or reset to initial severity (reset-to-initial-severity).
Step 6	UCSC(policy-mgr) /org/device-profile/policy* # **set clearaction delete** | **retain**	Sets the fault policy clear action to delete or retain.
Step 7	UCSC(policy-mgr) /org/device-profile/policy* # **set clearinterval** *days* | *hours* | *minutes* | *seconds* | **retain**	Sets the fault policy clear interval to the number of days, hours, minutes, and seconds or retain.
Step 8	UCSC(policy-mgr) /org/device-profile/policy* # **set flapinterval** *flap-number-of-days*	Sets the fault policy flap interval to the number of days.
Step 9	UCSC(policy-mgr) /org/device-profile/policy* # **set retentioninterval** *days* | *hours* | *minutes* | *seconds* | **forever**	Sets the fault policy clear interval to the number of days, hours, minutes, and seconds or forever.
Step 10	UCSC(policy-mgr) /org/device-profile/policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Creates a global fault debug policy
- Enters the status settings

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope fault policy
UCSC(policy-mgr) /org/device-profile/policy* # set ackaction delete-on-clear
UCSC(policy-mgr) /org/device-profile/policy* # set clearaction delete
UCSC(policy-mgr) /org/device-profile/policy* # set clearinterval 15 30 60 90
UCSC(policy-mgr) /org/device-profile/policy* # set flapinterval 180
UCSC(policy-mgr) /org/device-profile/policy* # set retentioninterval 180 54 52 63
UCSC(policy-mgr) /org/device-profile/policy* # commit-buffer
UCSC(policy-mgr) /org/device-profile/policy #
```

Configuring a TFTP Core Export Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope tftp-core-export-config**	(Optional) Scopes an existing TFTP core export debug policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.
Step 6	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target path** *name-of-path*	Sets the TFTP core export policy target path.
Step 7	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target port** *port-number*	Sets the TFTP core export policy port number (1-65535).
Step 8	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target server-description** *port-number*	Sets the TFTP core export target policy server description. **Note** Do not use spaces in the server description unless the text is quoted (format examples: "Server description text" or Server_description_text).
Step 9	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target server-name** *server-name*	Sets the TFTP core export target policy server name.

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Scopes the TFTP Core Export Policy
- Configures the policy
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope tftp-core-export-config
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # enable core-export-target
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target path
 /target
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target port
 65535
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target
server-description "TFTP core export server 2"
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target
server-name TFTPcoreserver01
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # commit-buffer
```

Creating a Locally Authenticated User

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create local-user** *local-user-name*	Creates a user account for the specified local user and enters security local user mode.
Step 6	UCSC(policy-mgr) org/device-profile/security/local-user* # **set account-status** {**active** | **inactive**}	Specifies to enable or disable the local user account. The admin user account is always set to active. You cannot modify it.

	Command or Action	Purpose
		Note If you set the account status to inactive, Cisco UCS Central does not delete the configuration from the database. Cisco UCS Central prevents the user from logging into the system using their existing credentials.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set password** *password*	Sets the password for the user account.
Step 8	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	(Optional) Specifies the first name of the user.
Step 9	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	(Optional) Specifies the last name of the user.
Step 10	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month day-of-month year*	(Optional) Specifies the date that the user account expires. The *month* argument is the first three letters of the month name.
Step 11	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	(Optional) Specifies the user e-mail address.
Step 12	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** *phone-num*	(Optional) Specifies the user phone number.
Step 13	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	(Optional) Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

The following example:

- Scopes into the organization
- Creates the user account named eagle_eye
- Enables the user account
- Sets the password to eye5687
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
```

```
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user eagle_eye
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set password
Enter a password: eye5687
Confirm the password: eye5687
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

The following example:

- Scopes into the organization
- Creates the user account named lincey
- Enables the user account
- Sets an openSSH key for passwordless access
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user lincey
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawcljk8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

The following example:

- Scopes into the organization
- Creates the user account named jforlenz
- Enables the user account
- Sets an secure SSH key for passwordless access
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user jforlenz
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

Creating a Remote User Login Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **set remote-user default-role** {**assign-default-role** | **no-login**}	Specifies whether user access to Cisco UCS Central is restricted based on user roles.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Sets the role policy for remote users
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # set remote-user default-role
assign-default-role
UCSC(policy-mgr) /org/device-profile/security/auth-realm* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm #
```

Creating a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create role** *name*	Creates the user role and enters security role mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Creates the service-profile security-admin role
- Adds the service profile security to the role
- Adds service profile security policy privileges to the role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create role security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
```

Creating a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create locale** *name*	Creates the user role and enters security role mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale * # **create org-ref** *org-ref-name* **orgdn** *orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference, and the *orgdn-name* argument is the distinguished name of the organization referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates the finance organization for the western locale
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create locale western
UCSC(policy-mgr) /org/device-profile/security/locale* # create org-ref finance-ref orgdn
finance
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
```

Users and Authentication

Cisco UCS Central supports creating local and remote users to access the system. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user must have a unique username and password.

Creating an Authentication Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm mode.
Step 6	UCSC(policy-mgr) / org/device-profile/security/auth-realm # **create auth-domain** *domain-name*	Creates an authentication domain and enters authentication domain mode. The Radius related settings are applicable only for the Cisco UCS Central in the domain group root and sub-domain groups.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **create default-auth**	(Optional) Creates a default authentication for the specified authentication domain.
Step 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) Specifies the provider group for the specified authentication domain.
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	Specifies the realm for the specified authentication domain.
Step 10	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Creates an authentication domain called domain1
- Sets the web refresh period to 3600 seconds (1 hour)
- Sets the session timeout period to14400 seconds (4 hours)
- Configures domain1 to use the providers in ldapgroup1
- Sets the realm type to ldap

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org/# scope device-profile
UCSC(policy-mgr) /org/device-profile/ # scope security
UCSC(policy-mgr) /org/device-profile/security # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # create default-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
realm ldap
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth #
```

Creating an LDAP Provider

Create and configure LDAP remote users, and assign roles and locales from Cisco UCS Central, in the same manner as Cisco UCS Manager. Always create the LDAP provider from the Cisco UCS Central domain group root.

Before You Begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS. Give this account a non-expiring password.

In the LDAP server, perform one of the following configurations:

- Configure LDAP groups. LDAP groups contain user role and locale information.
- Configure users with the attribute that holds the user role and locale information for Cisco UCS Central. You can choose to extend the LDAP schema for this attribute. If you do not want to extend the schema, use an existing LDAP attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the CiscoAVPair attribute.

  The Cisco LDAP implementation requires a unicode type attribute.

  If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1
- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

If you want to use secure communications, create a trusted point containing the certificate of the root certificate authority (CA) of the LDAP server in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create server** *server-name*	• Creates an LDAP server instance • Enters LDAP security server mode **Note** • If SSL is enabled, the server-name must match a common name (CN) in the LDAP server's security certificate. • If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. • If the Cisco UCS domain is not registered with Cisco UCS Central, or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. • If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set attribute** *attribute*	(Optional) An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set basedn** *basedn-name*	The name in the LDAP hierarchy, where the server begins a search, when a remote user logs in. After log in, the system attempts to obtain the user's DN based on their username. You can set the length of the base DN to a maximum of 255 characters minus the length of CN=username. Where username identifies the remote user attempting to access Cisco UCS Central using LDAP authentication.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set binddn** *binddn-name*	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set filter** *filter-value*	Restricts the LDAP search to those user names that match the defined filter.
Step 11	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set password**	To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.
Step 12	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set order** *order-num*	The order in which Cisco UCS Central uses this provider to authenticate users.
Step 13	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set port** *port-num*	The port through which Cisco UCS Central communicates with the LDAP database. The standard port number is 389.
Step 14	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set ssl** {**yes** | **no**}	Enables or disables encryption when communicating with the LDAP server. The options are as follows: • **yes —**Encryption required. If Cisco UCS Central cannot negotiate encryption, the connection fails. • **no —**Encryption disabled. Authentication information sent as clear text.
Step 15	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set timeout** *timeout-num*	If the LDAP provider does not receive an LDAP response within the specified period, it aborts the read attempt.
Step 16	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad —**Specifies Microsoft Active Directory. • **openldap —**Specifies OpenLDAP server.
Step 17	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Creates an LDAP server instance named 10.193.169.246
- Configures the binddn
- Configures the password
- Configures the order
- Configures the port
- Configures the SSL settings

- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create server 10.193.169.246
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set password
Enter the password:
Confirm the password:
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set order 2
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set port 389
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set ssl yes
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/server #
```

Creating an LDAP Provider Group

Before You Begin

Create one or more LDAP providers.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create auth-server-group** *auth-server-group-name*	Creates an LDAP provider group and enters authentication server group security LDAP mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified LDAP provider to the LDAP provider group.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS Central uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is

	Command or Action	Purpose
		equivalent to giving that server reference the highest priority.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates an LDAP provider group called ldapgroup
- Adds two previously configured providers called ldap1 and ldap2 to the provider group
- Sets the order
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
ldap2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* #
commit-buffer
```

What to Do Next

Configure an authentication domain.

Creating an LDAP Group Map

Before You Begin

- Create an LDAP provider group.
- Configure the distinguished name for the LDAP group in the LDAP server.
- Create user locales in Cisco UCS Central (optional).
- Create user roles in Cisco UCS Central (optional).

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create ldap-group** *group-dn*	Creates an LDAP group map for the specified DN.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create locale** *locale-name*	Maps the LDAP group to the specified locale.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create role** *role-name*	Maps the LDAP group to the specified role.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Scopes into the organization
- Maps the LDAP group mapped to a DN
- Sets the locale to pacific
- Sets the role to admin
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create locale pacific
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create role admin
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group #
```

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes the LDAP server called ldap1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete server ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

Deleting an LDAP Provider Group

Before You Begin

Remove the provider group from an authentication configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete auth-server-group** *auth-server-group-name*	Deletes the LDAP provider group.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes an LDAP provider group called ldapgroup
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

Deleting an LDAP Group Map

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete ldap-group** *group-dn*	Deletes the LDAP group map for the specified DN.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Deletes an LDAP group map
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
```

Creating a Trusted Point

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**create trustpoint***trust point name*	Creates a trusted point. Provide a certificate name.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/trustpoint* #**set certchain***[certificate chain]*	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.

The following example:

- Creates a trusted point
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create trustpoint key01
UCSC(policy-mgr) /org/device-profile/security/trustpoint* # set certchain
>-----BEGIN CERTIFICATE-----
>MIIDgzCCAmugAwIBAgIQeXUhz+ZtnrpK4x65oJkQZzANBgkqhkiG9w0BAQUFADBU
>MSIwIAYDVQQDExlibHJxYXVjc2MtV0lOMjAxMi1JUFY2LUNBMB4XDTE0MDIyNjEy
>-----END CERTIFICATE-----
>ENDOFBUF
UCSC(policy-mgr) /org/device-profile/security/trustpoint* # commit-buffer
```

Deleting a Trusted Point

Before You Begin

Ensure that a key ring is not using the trusted point.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**delete trustpoint***trustpoint- name*	Deletes the trusted point.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security#**commit-buffer**	Commits the transaction.

The following example:

- Deletes a trusted point
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # delete trustpoint tp1
UCSC(policy-mgr) /org/device-profile/security* #commit-buffer
```

Creating a Key Ring

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create keyring** *keyring-name*	Creates and names the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring # **set modulus mod2048**	Sets the SSL key length in bits.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring* # **set trustpoint** *trustpoint-name*	Sets a trust point within the key ring.
Step 8	UCSC(policy-mgr) /org/device-profile/security/keyring* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Creates a key ring with a key size of 2048 bits
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create keyring kr126
UCSC(policy-mgr) /org/device-profile/security/keyring* # set modulus mod2048
UCSC(policy-mgr) /org/device-profile/security/keyring* # set trustpoint tp1
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

Deleting a Key Ring

Before You Begin

Ensure that the HTTPS service is not using the key ring.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**delete keyring***keyring name*	Deletes the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security#**commit-buffer**	Commits the transaction.

The following example:

- Scopes into the organization
- Deletes a key ring
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # delete keyring kr126
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

Creating a Certificate Request

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope keyring** *keyring-name*	Enters the configuration mode for the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring* # **create certreq**	Sets the SSL key length in bits.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set country** *country name*	Specifies the country code of the company.
Step 8	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set dns** *DNS name*	Specifies the Domain Name Server (DNS) address associated with the certificate request.
Step 9	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set e-mail** *E-mail address*	Specifies the e-mail address associated with the certificate request.
Step 10	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set ip** { *certificate request ipv4-address*}	Specifies the IP address of the fabric interconnect.
Step 11	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set locality** *locality name*	Specifies the city or town in which the company requesting the certificate is headquartered.
Step 12	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set org-name** *organization name*	Specifies the organization requesting the certificate.
Step 13	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set org-unit-name** *organizational unit name*	Specifies the organizational unit.
Step 14	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set password** *certificate request password*	Specifies an optional password for the certificate request.

	Command or Action	Purpose
Step 15	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set state** *state, province or country*	Specifies the state or province in which the company requesting the certificate is headquartered.
Step 16	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set subject-name** *certificate request name*	Specifies the fully qualified domain name of the Fabric Interconnect.
Step 17	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **commit-buffer**	Commits the transaction.

The following example:

- Creates a certificate request with an IPv4 address for a key ring
- Sets advanced options
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring
UCSC(policy-mgr) /org/device-profile/security # create certreq
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set ip 192.168.200.123
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set country US
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set dns bgl-samc-15A
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set e-mail test@gmail.com
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set locality san_francisco
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set org-name "xyz"
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set org-unit-name Testing
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set state california
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set subject-name abc01
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* #commit-buffer
```

Configuring an HTTPS Certificate

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope https**	Enters the HTTPS service mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/https # **set keyring** *keyring-name*	Creates and names the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/https* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Configures an HTTPS certificate
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope https
UCSC(policy-mgr) /org/device-profile/https # set keyring kr126
UCSC(policy-mgr) /org/device-profile/https* # commit-buffer
```

Regenerating the Default Key Ring

You must manually regenerate the default key ring certificate if the cluster name changes or the certificate expires.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope keyring default**	Enters key ring security mode for the default key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring # **set regenerate yes**	Regenerates the default key ring.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring* # **commit-buffer**	Commits the transaction to the system configuration.

The following example:

- Regenerates a default key ring
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring default
UCSC(policy-mgr) /org/device-profile/security/keyring* # set generate yes
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```