User Management

This chapter includes the following sections:

Cisco UCS Central User Accounts

Access the system with user accounts. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user account must have a unique username and password.

You can setup a user account with an SSH public key, in either of the two formats: OpenSSH or SECSH.

Admin Account

The Cisco UCS Central admin account is the default user account. You cannot modify or delete it. This account is the system administrator, or superuser account, and has full privileges. There is no default password assigned to the admin account. You must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user can login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database. Anyone with admin or aaa privileges can enable or disable it. Once you disable a local user account, the user cannot log in.

Note Cisco UCS Central does not delete configuration details for disabled local user accounts from the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domains support LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the user account reaches the expiration time, the account disables.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account to expire with the farthest expiration date available.

Guidelines for Creating Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS Central user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
    - Any alphabetic character
    - Any digit
    - _ (underscore)
    - - (dash)
    - . (dot)
- The login ID must be unique within Cisco UCS Central.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

You cannot use the following words when creating a local user account in Cisco UCS.

- root
- bin

- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Creating a Locally Authenticated User Account

At a minimum, Cisco recommends that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Before you begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services—Ensures that the users exist in the remote authentication server with the appropriate roles and privileges.
- Multitenancy with organizations—Creates one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication—Obtains the SSH key.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 whether the local user account is enabled or disabled. The admin user account is always set to active. It cannot be modified. **Note** If you set the account status to inactive, Cisco UCS Central does not delete the configuration from the database. It 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	Specifies the first name of the user.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	Specifies the last name of the user.

	Command or Action	Purpose
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month* *day-of-month* *year*	Specifies the date that the user account expires. The *month* argument is the first three letters of the month name. **Note** After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. However, you can configure the account to use the latest expiration date available.
Step 11	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	Specifies the user e-mail address.
Step 12	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** phone-num	Specifies the user phone number.
Step 13	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Creates the user account named kikipopo
- Enables the user account
- Sets the password to foo12345
- 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 kikipopo
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:
Confirm the password:
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

The following example:

- 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
AAAAB3NzaC1yc2EAAAA
BIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4
VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8="
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

The following example:

- Creates the user account named hpotter
- Enables the user account,
- Sets a 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 hpotter
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 #
```

Deleting a Locally Authenticated User Account

Procedure

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

	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 # **delete local-user** *local-user-name*	Deletes the local-user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the foo user account
- 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 local-user foo
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security #
```

Enabling the Password Strength Check for Locally Authenticated Users

You must have privileges to enable the password strength check. If enabled, does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 password-profile**.	Specifies whether the password strength check is enabled or disabled.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set enforce-strong-password** {**yes** | **no**}	Specifies whether the password strength check is enabled or disabled.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Enables the password strength check
- 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 password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set enforce-strong-password
 yes
UCSC(policy-mgr) /org/device-profile/security/password-profile # commit-buffer
```

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or org/device-profile-management privileges to change the password profile properties.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 local-user** *local-user-name*	Commits the transaction.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **scope password-profile**	Enters password profile security mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set history-count** 0	Setting the **History Count** field to 0 (the default setting) disables the history count and allows users to reuse previously used passwords at any time.
Step 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Clears the password history count for the user account named kikipopo
- 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 local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 0
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Enabling or Disabling a User Account

You must have privileges to enable or disable a local user account.

Before you begin

Create a local user account.

Procedure

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

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **set account-status** {**active** | **inactive**}	Specifies whether the local user account is enabled or disabled. The admin user account is always set to active. It cannot be modified. **Note** If you set the account status to inactive, the configuration is not deleted from the database. The user is prevented from logging into the system using their existing credentials.

Example

The following example:

- Enables a local user account called accounting
- 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 local-user accounting
UCSC(policy-mgr) /org/device-profile/security/local-user # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user # commit-buffer
```

Web Session Limits for User Accounts

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

Monitoring User Sessions

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters system mode.
Step 2	UCSC /system # **scope security**	Enters security mode.
Step 3	UCSC /security # **show user-sessions** {**local** | **remote**} [**detail**]	Displays session information for all users logged in to the system. An asterisk (*) next to the session ID denotes the current login session.

Example

The following example lists all of the local users logged in to the system. The asterisk indicates which session is the current login session.

```
UCSC# scope system
UCSC /system # scope security
UCSC /security # show user-sessions local
Session Id      User            Host                 Login Time
--------------- --------------- -------------------- ----------
pts_25_1_31264* steve           192.168.100.111      2012-05-09T14:06:59.000
ttyS0_1_3532    jeff            console              2012-05-02T15:11:08.000
web_25277_A     faye            192.168.100.112      2012-05-15T22:11:25.000
```

The following example displays detailed information on all local users logged in to the system:

```
UCSC# scope system
UCSC /system # scope security
UCSC /security # show user-sessions local detail
Session Id pts_25_1_31264:
    Fabric Id: A
    Term: pts/25
    User: steve
    Host: 64.101.53.93
    Pid: 31264
    Login Time: 2012-05-09T14:06:59.000

Session Id ttyS0_1_3532:
    Fabric Id: A
    Term: ttyS0
    User: jeff
    Host: console
    Pid: 3532
    Login Time: 2012-05-02T15:11:08.000

Session Id web_25277_A:
    Fabric Id: A
    Term: web_25277
    User: faye
    Host: 192.168.100.112
    Pid: 3518
    Login Time: 2012-05-15T22:11:25.000
```

Configuring Passwords

Guidelines for Creating Passwords

Each locally authenticated user account requires a password. Cisco recommends that each user have a strong password. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If you enabled the password strength check, each user must use a strong password.

Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.

- Must contain at least three of the following:
    - Lower case letters
    - Upper case letters
    - Digits
    - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. Meaning, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Password Profile for Locally Authenticated Users

The password profile contains the password history and the password change interval properties for all locally authenticated users of . You cannot specify a different password profile for locally authenticated users.

Password History Count

The password history count prevents locally authenticated users from reusing the same password. When you configure the password history count, stores up to a maximum of 15 previously used passwords. The password history count stores the passwords in reverse chronological order with the most recent password first. This ensures that the user can only reuse the oldest password when the history count reaches its threshold.

A user can create and use the number of passwords configured in the password history count before reusing a password. For example, if you set the password history count to 8, a user cannot reuse the first password until the ninth password expires.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously used passwords at any time.

You can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval restricts the number of password changes that a locally authenticated user can make within a specific number of hours. The following table describes the two interval configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	Does not allow changing passwords for locally authenticated user within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	To prevent the user from changing passwords within 48 hours after a password change: • Set **Change during interval** to disable • Set **No change interval** to 48
Password changes allowed within change interval	Specifies the maximum number of times that a locally authenticated user password change can occur within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of two password changes within a 48-hour interval.	To allow a password change for a maximum of one time within 24 hours after a password change: • Set **Change during interval** to enable • Set **Change count** to 1 • Set **Change interval** to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin, aaa, or org/device-profile-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set change-during-interval enable**	Restricts the number of password changes a locally authenticated user can make within a given number of hours.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **set change-count** *pass-change-num*	Specifies the maximum number of times a locally authenticated user can change his or her password during the Change Interval.

	Command or Action	Purpose
		This value can be anywhere from 0 to 10.
Step 8	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **set change-interval** *num-of-hours*	Specifies the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced. This value can be anywhere from 1 to 745 hours. For example, if this field is set to 48 and the **Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.
Step 9	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enables the change during interval property
- Sets the change count to 5
- Sets the change interval to 72 hours
- 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 password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 enable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-interval 72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring a No Change Interval for Passwords

You must have admin, aaa, or org/device-profile-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set change-during-interval disable**	Disables the change during interval feature.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **set no-change-interval** *min-num-hours*	Specifies the minimum number of hours that a locally authenticated user must wait before changing a newly created password. This value can be anywhere from 1 to 745 hours. This interval is ignored if the **Change During Interval** property is set to **Disable**.
Step 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Disables the change during interval property
- Sets the no change interval to 72 hours
- 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 password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 disable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set no-change-interval
72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set history-count** *num-of-passwords*	Specifies the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password This value can be anywhere from 0 to 15. By default, the **History Count** field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Configures the password history count
- 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 password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring User Roles

Role-Based Access Control Overview

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the engineering organization can update server configurations in the Engineering organization. They cannot, however, update server configurations in the Finance organization, unless the locales assigned to the user include the Finance organization.

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining system.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However, the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server-related operations. Read access to the remaining system.

Server Profile Administrator

Read-and-write access to logical server-related operations. Read access to the remaining system.

Server Security Administrator

Read-and-write access to server security-related operations. Read access to the remaining system.

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users, assigned to user roles, access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 1: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator

Privilege	Description	Default Role Assignment
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile endpoint access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

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 the organization root.
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 role security mode.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **add privilege** *privilege-name*	Adds one or more privileges to the role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role. You can also add privileges to the same role using multiple **add** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the service-profile-security-admin role
- Adds the service profile security to the role
- Adds the service profile security policy privileges to the role
- 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 role ls-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege service-profile-security

service-profile-security-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Deleting 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 the organization root.
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.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/security # **delete role** *name*	Deletes the user role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the service-profile-security-admin role
- 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 role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Adding Privileges to 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 the organization root.
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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **add privilege** *privilege-name*	Adds one or more privileges to the existing privileges of the user role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role. You can also add privileges to the same role using multiple **add privilege** commands.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Adds the server security to the service-profile-security-admin role
- Adds the server policy privileges to the service-profile-security-admin role
- 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 role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Replacing Privileges for 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 the organization root.
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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **set privilege** *privilege-name*	Replaces the existing privileges of the user role.

	Command or Action	Purpose
		Note You can specify more than one *privilege-name* on the same command line to replace the existing privilege with multiple privileges. After replacing the privileges, you can add privileges to the same role using the **add privilege** command.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Replaces the existing privileges for the service-profile-security-admin role with server security
- Replaces the existing privileges for the service-profile-security-admin role with server policy privileges
- 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 role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # set privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Removing Privileges from 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 the organization root.
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.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **remove privilege** *privilege-name*	Removes one or more privileges from the existing user role privileges. **Note** You can specify more than one *privilege-name* on the same command line to remove multiple privileges from the role. You can also remove privileges from the same role using multiple **remove privilege** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Removes the server security from the service-profile-security-admin role
- Removes the server policy privileges from the service-profile-security-admin role
- 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 role
UCSC(policy-mgr) /org/device-profile/security/role # remove privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/role #
```

Assigning a Role to a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

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

	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create role** *role-name*	Assigns the specified role to the user account. **Note** You can enter the **create role** command multiple times to assign more than one role to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the operations role to the kikipopo local user account
- 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 local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # create role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Removing a Role from a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

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

	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete role** *role-name*	Removes the specified role from the user account. **Note** You can enter the **delete role** command multiple times to remove more than one role from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the operations role from the kikipopo local user account
- Commits the transaction

```
CSC # 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 local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # delete role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Configuring User Locales

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

Users with admin or aaa privileges can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, a user assigned to that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization. However, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

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 the organization root.
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** org-root/org-*orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. 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.

Example

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
org-root/org-finance
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/locale #
```

Deleting 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 the organization root.
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 locale** *locale-name*	Deletes the locale.
Step 6	UCSC(policy-mgr) /org/device-profile/security # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes 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 # delete locale western
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security #
```

Assigning a Locale to a User Account

Note Do not assign locales to users with an admin role.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 /security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create locale** *locale-name*	Assigns the specified locale to the user account. **Note** You can enter the **create locale** command multiple times to assign more than one locale to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the western locale to the kikipopo local user account
- 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/local-user # create locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Removing a Locale from a User Account

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete locale** *locale-name*	Removes the specified locale from the user account. **Note** You can enter the **delete locale** command multiple times to remove more than one locale from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the western locale from the kikipopo local user account
- 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 local-user
UCSC(policy-mgr) /org/device-profile/security/local-user # delete locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Assigning an Organization to 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 the organization root.
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 locale** *locale-name*	Enters locale security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **create org-ref** *org-ref-name* **orgdn org-root/org-***orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. 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.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing organization to the locale
- Names the reference marketing-ref
- 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 locale western
UCSC(policy-mgr) /org/device-profile/security/locale # create org-ref marketing-ref orgdn
org-root/org-marketing
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/locale #
```

Deleting an Organization from 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 the organization root.
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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete org-ref** *org-ref-name*	Deletes the organization from the locale.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the finance organization from 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete org-ref finance-ref
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/locale #
```

Assigning a Domain Group to a User Locale

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) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /domain-group/security/locale # **create domain-group-ref** *domain-group-ref-name* **domain-group-dn** *domaingroup-root-name*	References (binds) a domain group to the locale. The *domain-group-ref-name* argument (1-16 characters) is the name used to identify the domain group reference. The *domain-group-dn-name* argument is the distinguished name of the domain group root referenced.
Step 7	UCSC(policy-mgr) /domain-group/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing domain group to the locale
- Names the reference marketdomain01-ref
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope locale western
UCSC(policy-mgr) /domain-group/security/locale # create domain-group-ref marketdomain01
domain-group-dn domaingroup-root/domaingroup-marketing
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Deleting a Domain Group from 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.
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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete domain-group-ref** *domain-group-ref-name*	Deletes references (unbinds) domain groups referenced to the locale. The *domaingroup-ref* argument (1-16 characters) is the name used to identify the domain group reference.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Deletes references (unbinds) the marketing domain group references from the locale marketdomain01
- 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 locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete domain-group-ref marketdomain01
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/locale #
```

Configuring User Domain Groups

Creating a User Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create domain-group** *name*	Creates the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the central-audit domain group
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create domain-group central-audit
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting a User Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **delete domain-group** *name*	Deletes the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the central-audit domain group
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # delete domain-group central-audit
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring User Organizations

User Organizations

A user can create one or more organizations. Each organization defines sub-organizations, faults, events, UUID suffix pools and blocks of UUIDs.

Cisco UCS organizations are hierarchically managed by users. A user that is assigned at the root level organization has automatic access to all organizations and domain groups under it.

Creating a User Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create org** *name*	Creates the organization.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the central-audit organization
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create org central-audit
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Deleting a User Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete org** *name*	Deletes the organization.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the central-audit organization
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete org central-audit
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Creating a User Sub-Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create org** *name*	Creates the sub-organization under the organization scoped.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the central-audit organization
- Creates the north-audit sub-organization
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org central-audit
UCSC(policy-mgr) /org # create org north-audit
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Deleting a User Sub-Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete org** *name*	Deletes the sub-organization under the organization scoped.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the central-audit organization
- Deletes the north-audit sub-organization
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org central-audit
UCSC(policy-mgr) /domain-group # delete org north-audit
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```