



# Configuring Role-Based Access Control

---

This chapter includes the following sections:

- [Role-Based Access Control](#), page 1
- [User Accounts for Cisco UCS Manager](#), page 1
- [User Roles](#), page 4
- [User Locales](#), page 8
- [Configuring User Roles](#), page 9
- [Configuring Locales](#), page 11
- [Configuring User Accounts](#), page 13
- [Monitoring User Sessions](#), page 20

## Role-Based Access Control

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 the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired 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 could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

## User Accounts for Cisco UCS Manager

User accounts are used to access the system. Up to 48 user accounts can be configured in each Cisco UCS instance. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

### Default User Account

Each Cisco UCS instance has a default user account, admin, which cannot be modified or deleted. 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.

### Local User Accounts

Local user accounts are authenticated directly through the fabric interconnect and can be enabled or disabled by anyone with admin or aaa privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

### Remote User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or 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

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

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 with the latest date available.

---

## Guidelines for Cisco UCS Manager Usernames

The username is also used as the login ID for Cisco UCS Manager. When you assign usernames to Cisco UCS Manager 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 unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.

- The unique username must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

## Reserved Words: Local User Accounts

The following words cannot be used when creating a local user account in Cisco UCS Manager.

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

## Guidelines for Cisco UCS Manager Passwords

A password is required for each locally authenticated user account. A user with admin or aaa privileges can configure Cisco UCS Manager to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 64 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. For example, 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.

## Web Session Limits for User Accounts

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

By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32; although this value can be configured up to the system maximum of 256.

## User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, users who are assigned to both Role1 and Role2 have storage and server related privileges.

A Cisco UCS instance can contain up to 48 user roles, including the default user roles.

All roles include read access to all configuration settings in the Cisco UCS instance. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

**Note**

---

If a local user account and a remote user account have the same username, any roles assigned to the remote user are overridden by those assigned to the local user.

---

## 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 rest of the system.

**Administrator**

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

**Facility Manager**

Read-and-write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.

**Network Administrator**

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

**Operations**

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

**Read-Only**

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

**Server Equipment Administrator**

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

**Server Profile Administrator**

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

**Server Security Administrator**

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

**Storage Administrator**

Read-and-write access to storage operations. Read access to the rest of the system.

## Reserved Words: User Roles

The following words cannot be used when creating custom roles in Cisco UCS Manager.

- 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.

**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

Privilege	Description	Default Role Assignment
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	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
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security 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 end point 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

Privilege	Description	Default Role Assignment
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

## User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS instance can contain up to 48 user locales.

Users with AAA privileges (AAA Administrator role) 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 then a user assigned 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
- operations

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under 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.

# Configuring User Roles

## Creating a User Role

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>create role</b> <i>name</i>	Creates the user role and enters security role mode.
<b>Step 3</b>	UCS-A /security/role # <b>add privilege</b> <i>privilege-name</i>	<p>Adds one or more privileges to the role.</p> <p><b>Note</b> You can specify more than one <i>privilege-name</i> on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple <b>add</b> commands.</p>
<b>Step 4</b>	UCS-A /security/role # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example creates the service-profile-security-admin role, adds the service profile security and service profile security policy privileges to the role, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create role ls-security-admin
UCS-A /security/role* # add privilege service-profile-security service-profile-security-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

## Adding Privileges to a User Role

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope role</b> <i>name</i>	Enters security role mode for the specified role.
<b>Step 3</b>	UCS-A /security/role # <b>add privilege</b> <i>privilege-name</i>	<p>Adds one or more privileges to the existing privileges of the user role.</p> <p><b>Note</b> You can specify more than one <i>privilege-name</i> on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple <b>add privilege</b> commands.</p>

	Command or Action	Purpose
<b>Step 4</b>	UCS-A /security/role # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example adds the server security and server policy privileges to the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # add privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

## Removing Privileges from a User Role

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope role name</b>	Enters security role mode for the specified role.
<b>Step 3</b>	UCS-A /security/role # <b>remove privilege privilege-name</b>	Removes one or more privileges from the existing user role privileges.  <b>Note</b> You can specify more than one <i>privilege-name</i> on the same command line to remove multiple privileges from the role, or you can remove privileges from the same role using multiple <b>remove privilege</b> commands.
<b>Step 4</b>	UCS-A /security/role # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example removes the server security and server policy privileges from the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # remove privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

## Deleting a User Role

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>delete role name</b>	Deletes the user role.
<b>Step 3</b>	UCS-A /security # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example deletes the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete role service-profile-security-admin
UCS-A /security* # commit-buffer
UCS-A /security #
```

## Configuring Locales

### Creating a Locale

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>create locale locale-name</b>	Creates a locale and enters security locale mode.
<b>Step 3</b>	UCS-A /security/locale # <b>create org-ref org-ref-name orgdn orgdn-name</b>	References (binds) an organization to the locale. The <i>org-ref-name</i> argument is the name used to identify the organization reference, and the <i>orgdn-name</i> argument is the distinguished name of the organization being referenced.
<b>Step 4</b>	UCS-A /security/locale # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example creates the western locale, references the finance organization to the locale, names the reference finance-ref, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create locale western
UCS-A /security/locale* # create org-ref finance-ref orgdn finance
```

```
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

## Adding an Organization to a Locale

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A# <b>scope locale</b> <i>locale-name</i>	Enters security locale mode.
<b>Step 3</b>	UCS-A /security/locale # <b>create org-ref</b> <i>org-ref-name</i> <b>orgdn</b> <i>orgdn-name</i>	References (binds) an organization to the locale. The <i>org-ref-name</i> argument is the name used to identify the organization reference, and the <i>orgdn-name</i> argument is the distinguished name of the organization being referenced.
<b>Step 4</b>	UCS-A /security/locale # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example enters the western locale, adds (references) the marketing organization to the locale, names the reference marketing-ref, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale* # create org-ref marketing-ref orgdn marketing
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

## Deleting an Organization from a Locale

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope locale</b> <i>locale-name</i>	Enters security locale mode.
<b>Step 3</b>	UCS-A /security/locale # <b>delete org-ref</b> <i>org-ref-name</i>	Deletes the organization from the locale.
<b>Step 4</b>	UCS-A /security/locale # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example deletes the finance organization from the western locale and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale # delete org-ref finance-ref
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

## Deleting a Locale

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>delete locale</b> <i>locale-name</i>	Deletes the locale.
<b>Step 3</b>	UCS-A /security # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example deletes the western locale and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete locale western
UCS-A /security* # commit-buffer
UCS-A /security #
```

## Configuring User Accounts

### Creating a User Account

At a minimum, we recommend 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, ensure the users exist in the remote authentication server with the appropriate roles and privileges.
- Multi-tenancy with organizations, create 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, obtain the SSH key.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>create local-user</b> <i>local-user-name</i>	Creates a user account for the specified local user and enters security local user mode.
<b>Step 3</b>	UCS-A /security/local-user # <b>set account-status</b> { <b>active</b>   <b>inactive</b> }	Specifies whether the local user account is enabled or disabled.  If the account status for a local user account is set to inactive, the user is prevented from logging into the system using their existing credentials.
<b>Step 4</b>	UCS-A /security/local-user # <b>set password</b> <i>password</i>	Sets the password for the user account
<b>Step 5</b>	UCS-A /security/local-user # <b>set firstname</b> <i>first-name</i>	(Optional) Specifies the first name of the user.
<b>Step 6</b>	UCS-A /security/local-user # <b>set lastname</b> <i>last-name</i>	(Optional) Specifies the last name of the user.
<b>Step 7</b>	UCS-A /security/local-user # <b>set expiration</b> <i>month day-of-month year</i>	(Optional) Specifies the date that the user account expires. The <i>month</i> argument is the first three letters of the month name.  <b>Note</b> After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest date available.
<b>Step 8</b>	UCS-A /security/local-user # <b>set email</b> <i>email-addr</i>	(Optional) Specifies the user e-mail address.
<b>Step 9</b>	UCS-A /security/local-user # <b>set phone</b> <i>phone-num</i>	(Optional) Specifies the user phone number.
<b>Step 10</b>	UCS-A /security/local-user # <b>set sshkey</b> <i>ssh-key</i>	(Optional) Specifies the SSH key used for passwordless access.
<b>Step 11</b>	UCS-A security/local-user # <b>commit-buffer</b>	Commits the transaction.

The following example creates the user account named kikipopo, enables the user account, sets the password to foo12345, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create local-user kikipopo
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* # set password
Enter a password:
```

```
Confirm the password:
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

The following example creates the user account named lincey, enables the user account, sets an OpenSSH key for passwordless access, and commits the transaction.

```
UCS-A# scope security
UCS-A /security # create local-user lincey
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* # set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30k1CWjnV31gdXMzO0WU15iPw851kdQqap+NFuNmHcb4K
iaQB8X/PDdmt1xQQcawclj+k8f4VcOelBx1sGk51uq51s1ob1VOIEwckEL/h51rdbN1I8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

The following example creates the user account named jforlenz, enables the user account, sets a Secure SSH key for passwordless access, and commits the transaction.

```
UCS-A# scope security
UCS-A /security # create local-user jforlenz
UCS-A /security/local-user* # set account-status active
UCS-A /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/S1f30k1CWjnV31gdXMzO0WU15iPw8
>51kdQqap+NFuNmHcb4KiaQB8X/PDdmt1xQQcawclj+k8f4VcOelBx1sGk51uq51s1ob1VO
>IEwckEL/h51rdbN1I8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

## Enabling or Disabling a Local User Account

You must be a user with admin or aaa privileges to enable or disable a local user account.

### Before You Begin

Create a local user account.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope local-user</b>	Enters local-user security mode.
<b>Step 3</b>	UCS-A /security/local-user # <b>set account-status {active   inactive}</b>	Specifies whether the local user account is enabled or disabled.  The admin user account is always set to active. It cannot be modified.  <b>Note</b> If you set the account status to inactive, the configuration is not deleted from the database.

The following example enables a local user account called accounting:

```
UCS-A# scope security
UCS-A /security # scope local-user accounting
UCS-A /security/local-user # set account-status active
```

## Enabling the Password Strength Check for Locally Authenticated Users

You must be a user with admin or aaa privileges to enable the password strength check. If the password strength check is enabled, Cisco UCS Manager does not permit a user to choose a password that does not meet the guidelines for a strong password.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>enforce-strong-password</b> {yes   no}	Specifies whether the password strength check is enabled or disabled.

The following example enables the password strength check:

```
UCS-A# scope security
UCS-A /security # set enforce-strong-password yes
UCS-A /security #
```

## Setting Web Session Limits for User Accounts

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope system</b>	Enters system mode.
<b>Step 2</b>	UCS-A /system # <b>scope services</b>	Enters system services mode.
<b>Step 3</b>	UCS-A /system/services # <b>scope</b> <b>web-session-limits</b>	Enters system services web session limits mode.
<b>Step 4</b>	UCS-A /system/services/web-session-limits # <b>set peruser</b> <i>num-of-logins-per-user</i>	Sets the maximum number of concurrent HTTP and HTTPS sessions allowed for each user.  Enter an integer between 1 and 256. By default, this value is set to 32.
<b>Step 5</b>	UCS-A /system/services/web-session-limits # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example sets the maximum number of HTTP and HTTPS sessions allowed by each user account to 60 and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits* # set peruser 60
UCS-A /system/services/web-session-limits* # commit-buffer
UCS-A /system/services/web-session-limits #
```

## 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
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope local-user</b> <i>local-user-name</i>	Enters security local user mode for the specified local user account.
<b>Step 3</b>	UCS-A /security/local-user # <b>create role</b> <i>role-name</i>	Assigns the specified role to the user account .  <b>Note</b> The <b>create role</b> command can be entered multiple times to assign more than one role to a user account.
<b>Step 4</b>	UCS-A security/local-user # <b>commit-buffer</b>	Commits the transaction.

The following example assigns the operations role to the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /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
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope local-user</b> <i>local-user-name</i>	Enters security local user mode for the specified local user account.
<b>Step 3</b>	UCS-A /security/local-user # <b>delete role</b> <i>role-name</i>	Removes the specified role from the user account .  <b>Note</b> The <b>delete role</b> command can be entered multiple times to remove more than one role from a user account.
<b>Step 4</b>	UCS-A security/local-user # <b>commit-buffer</b>	Commits the transaction.

The following example removes the operations role from the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

## Assigning a Locale to a User Account



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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope local-user</b> <i>local-user-name</i>	Enters security local user mode for the specified local user account.
<b>Step 3</b>	UCS-A /security/local-user # <b>create</b> <b>locale</b> <i>locale-name</i>	Assigns the specified locale to the user account.  <b>Note</b> The <b>create locale</b> command can be entered multiple times to assign more than one locale to a user account.
<b>Step 4</b>	UCS-A security/local-user # <b>commit-buffer</b>	Commits the transaction.

The following example assigns the western locale to the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

## Removing a Locale from a User Account

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>scope local-user</b> <i>local-user-name</i>	Enters security local user mode for the specified local user account.
<b>Step 3</b>	UCS-A /security/local-user # <b>delete</b> <b>locale</b> <i>locale-name</i>	Removes the specified locale from the user account.  <b>Note</b> The <b>delete locale</b> command can be entered multiple times to remove more than one locale from a user account.
<b>Step 4</b>	UCS-A security/local-user # <b>commit-buffer</b>	Commits the transaction.

The following example removes the western locale from the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

## Deleting a User Account

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>delete local-user</b> <i>local-user-name</i>	Deletes the local-user account.

	Command or Action	Purpose
<b>Step 3</b>	UCS-A /security # <b>commit-buffer</b>	Commits the transaction to the system configuration.

The following example deletes the foo user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete local-user foo
UCS-A /security* # commit-buffer
UCS-A /security #
```

## Monitoring User Sessions

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	UCS-A# <b>scope security</b>	Enters security mode.
<b>Step 2</b>	UCS-A /security # <b>show user-session</b> {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.

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

```
UCS-A# scope security
UCS-A /security # show user-session local
Session Id      User      Host      Login Time
-----
pts_25_1_31264*  steve    192.168.100.111  2009-05-09T14:06:59
ttyS0_1_3532    jeff     console    2009-05-02T15:11:08
web_25277_A     faye     192.168.100.112  2009-05-15T22:11:25
```

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

```
UCS-A# scope security
UCS-A /security # show user-session 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: 2009-05-09T14:06:59

Session Id ttyS0_1_3532:
  Fabric Id: A
  Term: ttyS0
  User: jeff
  Host: console
  Pid: 3532
  Login Time: 2009-05-02T15:11:08

Session Id web_25277_A:
  Fabric Id: A
```

```
Term: web_25277  
User: faye  
Host: 192.168.100.112  
Pid: 3518  
Login Time: 2009-05-15T22:11:25
```

