User Management

User Accounts

User accounts are used to access the system. You can configure up to 48 local user accounts. Each user account must have a unique username and password.

Admin Account

The admin account is a default user account and 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.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated directly through the chassis 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 reenable a disabled local user account, the account becomes active again with the existing configuration.

Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+. All remote users are initially assigned the **Read-Only** role by default.

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.

The fallback authentication method is to use the local database. This fallback method is not configurable.

Note When remote authentication is set as the default authentication method, you cannot log in to Firepower Chassis Manager with the local user account, even though, local authentication is set, by default, as the fallback authentication method in case the remote authentication server becomes unavailable. Thus, you cannot use local and remote user account interchangeably.

See the following topics for more information on guidelines for remote authentication, and how to configure and delete remote authentication providers:

- Guidelines for Remote Authentication, on page 4
- Configuring LDAP Providers
- Configuring RADIUS Providers
- Configuring TACACS+ Providers

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

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 expiration date available.

Guidelines for Usernames

The username is also used as the login ID for Firepower Chassis Manager and the FXOS CLI. When you assign login IDs to 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.
- 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.

Guidelines for Passwords

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

We recommend that each user have a strong password. If you enable the password strength check for locally authenticated users, the FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 127 characters.

Note You can optionally configure a minimum password length of 15 characters on the system, to comply with Common Criteria requirements. For more information, see Configure Minimum Password Length Check, on page 15.

- Must include at least one uppercase alphabetic character.
- Must include at least one lowercase alphabetic character.
- Must include at least one non-alphanumeric (special) character.
- Must not contain a space.
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.
- 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).

Note This restriction applies whether the password strength check is enabled or not.

- Must not be blank for local user and admin accounts.

Guidelines for Remote Authentication

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that the Firepower 4100/9300 chassis can communicate with the system. The following guidelines impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in the Firepower 4100/9300 chassis or in the remote authentication server.

You can view the temporary sessions for users who log in through remote authentication services from the Firepower Chassis Manager or the FXOS CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in the Firepower 4100/9300 chassis and that the names of those roles match the names used in FXOS. Based on the role policy, a user might not be allowed to log in, or is granted only read-only privileges.

User Attributes in Remote Authentication Providers

For RADIUS and TACACS+ configurations, you must configure a user attribute for the Firepower 4100/9300 chassis in each remote authentication provider through which users log in to Firepower Chassis Manager or the FXOS CLI. This user attribute holds the roles and locales assigned to each user.

When a user logs in, FXOS does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by FXOS:

Authenication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	You can choose to do one of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	The Cisco LDAP implementation requires a unicode type attribute. If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1 A sample OID is provided in the following section.
RADIUS	Optional	You can choose to do one of the following: • Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

User Roles

The system contains the following user roles:

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.

Read-Only

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

Operations

Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.

AAA Administrator

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

Password Profile for Locally Authenticated Users

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

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, the Firepower chassis stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

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

If necessary, 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 enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed 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.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed 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 2 password changes within a 48 hour interval.	For example, to allow a password to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Select the Default Authentication Service

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter default authorization security mode:

Firepower-chassis /security # **scope default-auth**

Step 3 Specify the default authentication:

Firepower-chassis /security/default-auth # **set realm** *auth-type*

where *auth-type* is one of the following keywords:

- **ldap**—Specifies LDAP authentication
- **local**—Specifies local authentication
- **none**—Allows local users to log on without specifying a password
- **radius**—Specifies RADIUS authentication
- **tacacs**—Specifies TACACS+ authentication

Note If Default Authentication and Console Authentication are both set to use the same remote authentication protocol (RADIUS, TACACS+, or LDAP), you cannot change certain aspects of that server's configuration (for example, deleting that server, or changing its order of assignment) without updating these user settings.

Step 4 (Optional) Specify the associated provider group, if any:

Firepower-chassis /security/default-auth # **set auth-server-group** *auth-serv-group-name*

Step 5 (Optional) Specify the maximum amount of time allowed between refresh requests for a user in this domain:

Firepower-chassis /security/default-auth # **set refresh-period** *seconds*

Specify an integer between 0 and 600. The default is 600 seconds.

If this time limit is exceeded, FXOS considers the web session to be inactive, but it does not terminate the session.

Step 6 (Optional) Specify the maximum amount of time that can elapse after the last refresh request before FXOS considers a web session to have ended:

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

Specify an integer between 0 and 600. The default is 600 seconds.

Note If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the **session-refresh** and **session-timeout** periods so that remote users do not have to reauthenticate too frequently.

Step 7 (Optional) Set the authentication method to two-factor authentication for the realm:

Firepower-chassis /security/default-auth # **set use-2-factor yes**

Note Two-factor authentication applies only to the RADIUS and TACACS+ realms.

Step 8 Commit the transaction to the system configuration:

commit-buffer

Example

The following example sets the default authentication to RADIUS, the default authentication provider group to provider1, enables two-factor authentications, sets the refresh period to 300 seconds (5 minutes), the session timeout period to 540 seconds (9 minutes), and enables two-factor authentication. It then commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 300
Firepower-chassis /security/default-auth* # set session-timeout 540
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

Configuring the Session Timeout

You can use the FXOS CLI to specify the amount of time that can pass without user activity before the Firepower 4100/9300 chassis closes user sessions. You can configure different settings for console sessions and for HTTPS, SSH, and Telnet sessions.

You can set a timeout value up to 3600 seconds (60 minutes). The default value is 600 seconds. To disable this setting, set the session timeout value to 0.

Note If the refresh-period is not set to zero while setting the session timeout value to 0, an error message `Update failed:[For Default Authentication, Refresh Period cannot be greater than Session Timeout]` will be displayed. This is because you must first set refresh-period to 0 and then the session-timeout to 0.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter default authorization security mode:

Firepower-chassis /security # **scope default-auth**

Step 3 Set the idle timeout for HTTPS, SSH, and Telnet sessions:

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

Step 4 (Optional) Set the idle timeout for console sessions:

Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /security/default-auth # **commit-buffer**

Step 6 (Optional) View the session and absolute session timeout settings:

Firepower-chassis /security/default-auth # **show detail**

Example:

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

Configuring the Absolute Session Timeout

The Firepower 4100/9300 chassis has an absolute session timeout setting that closes user sessions after the absolute session timeout period has passed, regardless of session use. This absolute timeout functionality is global across all forms of access including serial console, SSH, and HTTPS.

You can separately configure the absolute session timeout for serial console sessions. This allows for disabling the serial console absolute session timeout for debugging needs while maintaining the timeout for other forms of access.

The absolute timeout value defaults to 3600 seconds (60 minutes) and can be changed using the FXOS CLI. To disable this setting, set the absolute session timeout value to 0.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter default authorization security mode:

Firepower-chassis /security # **scope default-auth**

Step 3 Set the absolute session timeout:

Firepower-chassis /security/default-auth # **set absolute-session-timeout** *seconds*

Step 4 (Optional) Set a separate console absolute session timeout:

Firepower-chassis /security/default-auth # **set con-absolute-session-timeout** *seconds*

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /security/default-auth # **commit-buffer**

Step 6 (Optional) View the session and absolute session timeout settings:

Firepower-chassis /security/default-auth # **show detail**

Example:

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

Configuring the Role Policy for Remote Users

By default, read-only access is granted to all users logging in to Firepower Chassis Manager or the FXOS CLI from a remote server using the LDAP, RADIUS, or TACACS+ protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role.

You can configure the role policy for remote users in the following ways:

assign-default-role

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, the user is allowed to log in with a read-only user role.

This is the default behavior.

no-login

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, access is denied.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Specify whether user access to Firepower Chassis Manager and the FXOS CLI should be restricted based on user roles:

Firepower-chassis /security # **set remote-user default-role** {**assign-default-role** | **no-login**}

Step 3 Commit the transaction to the system configuration:

Firepower-chassis /security # **commit-buffer**

Example

The following example sets the role policy for remote users and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # set remote-user default-role no-login
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Enabling Password Strength Check for Locally Authenticated Users

If the password strength check is enabled, the FXOS does not permit a user to choose a password that does not meet the guidelines for a strong password (see Guidelines for Passwords, on page 3).

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Specify whether the password strength check is enabled or disabled:

Firepower-chassis /security # **set enforce-strong-password** {**yes** | **no**}

Example

The following example enables the password strength check:

```
Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Set the Maximum Number of Login Attempts

You can configure the maximum number of failed login attempts allowed before a user is locked out of the Firepower 4100/9300 chassis for a specified amount of time. If a user exceeds the set maximum number of login attempts, the user is locked out of the system. No notification appears indicating that the user is locked out. In this event, the user must wait the specified amount of time before attempting to log in.

Perform these steps to configure the maximum number of login attempts.

Note

- All types of user accounts (including admin) are locked out of the system after exceeding the maximum number of login attempts.
- The default maximum number of unsuccessful login attempts is 0. The default amount of time the user is locked out of the system after exceeding the maximum number of login attemps is 30 minutes (1800 seconds).
- For steps to view a user's lockout status and to clear the user's locked out state, see View and Clear User Lockout Status, on page 13.

This option is one of a number offered for achieving Common Criteria certification compliance on your system. For more information, see Security Certifications Compliance.

Procedure

Step 1 From the FXOS CLI, enter security mode:

scope security

Step 2 Set the maximum number of unsuccessful login attempts.

set max-login-attempts *num_attempts*

The *num_attempts* value is any integer from 0-10.

Step 3 Specify the amount of time (in seconds) the user should remain locked out of the system after reaching the maximum number of login attempts:

set user-account-unlock-time

unlock_time

Step 4 Commit the configuration:

commit-buffer

View and Clear User Lockout Status

Admin users can view and clear the locked out status of users that have been locked out of the Firepower 4100/9300 chassis after exceeding the maximum number of failed login attempts specified in the Maximum Number of Login Attempts CLI setting. For more information, see Set the Maximum Number of Login Attempts, on page 12.

Procedure

Step 1 From the FXOS CLI, enter security mode:

scope security

Step 2 Display the user information (including lockout status) of the user in question:

Firepower-chassis /security # **show local-user** *user* **detail**

Example:

```
Local User user:
 First Name:
 Last Name:
 Email:
 Phone:
 Expiration: Never
 Password:
 User lock status: Locked
 Account status: Active
 User Roles:
 Name: read-only
 User SSH public key:
```

Step 3 (Optional) Clear the user's lock out status:

Firepower-chassis /security # **scope local-user** *user*

Firepower-chassis /security/local-user # **clear lock-status**

Configuring the Maximum Number of Password Changes for a Change Interval

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter password profile security mode:

Firepower-chassis /security # **scope password-profile**

Step 3 Restrict the number of password changes a locally authenticated user can make within a given number of hours:

Firepower-chassis /security/password-profile # **set change-during-interval enable**

Step 4 Specify the maximum number of times a locally authenticated user can change his or her password during the Change Interval:

Firepower-chassis /security/password-profile # **set change-count** *pass-change-num*

This value can be anywhere from 0 to 10.

Step 5 Specify the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced:

Firepower-chassis /security/password-profile # **set change-interval** *num-of-hours*

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 6 Commit the transaction to the system configuration:

Firepower-chassis /security/password-profile # **commit-buffer**

Example

The following example enables the change during interval option, sets the change count to 5, sets the change interval to 72 hours, and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Firepower-chassis /security/password-profile* # set change-count 5
Firepower-chassis /security/password-profile* # set change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Configure Minimum Password Length Check

If you enable minimum password length check, you must create passwords with the specified minimum number of characters. For example, if the *min_length* option is set to 15, you must create passwords using 15 characters or more. This option is one of a number that allow for Common Criteria certification compliance on your system. For more information, see Security Certifications Compliance.

Perform these steps to configure the minimum password length check.

Procedure

Step 1 From the FXOS CLI, enter security mode:

scope security

Step 2 Specify the minimum password length:

set min-password-length *min_length*

Step 3 Commit the configuration:

commit-buffer

Configuring a No Change Interval for Passwords

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter password profile security mode:

Firepower-chassis /security # **scope password-profile**

Step 3 Disable the change during interval feature:

Firepower-chassis /security/password-profile # **set change-during-interval disable**

Step 4 Specify the minimum number of hours that a locally authenticated user must wait before changing a newly created password:

Firepower-chassis /security/password-profile # **set no-change-interval** *min-num-hours*

This value can be anywhere from 1 to 745 hours.

This interval is ignored if the **Change During Interval** property is not set to **Disable**.

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /security/password-profile # **commit-buffer**

Example

The following example disables the change during interval option, sets the no change interval to 72 hours, and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Configuring the Password History Count

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter password profile security mode:

Firepower-chassis /security # **scope password-profile**

Step 3 Specify the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password:

Firepower-chassis /security/password-profile # **set history-count** *num-of-passwords*

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 4 Commit the transaction to the system configuration:

Firepower-chassis /security/password-profile # **commit-buffer**

Example

The following example configures the password history count and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set history-count 5
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Creating a Local User Account

Procedure

Step 1 Enter security mode:

Firepower-chassis# **scope security**

Step 2 Create the user account:

Firepower-chassis /security # **create local-user** *local-user-name*

where *local-user-name* is the account name to be used when logging into this account. This name must be unique and meet the guidelines and restrictions for user account names (see Guidelines for Usernames, on page 2).

After you create the user, the login ID cannot be changed. You must delete the user account and create a new one.

Step 3 Specify whether the local user account is enabled or disabled:

Firepower-chassis /security/local-user # **set account-status** {**active**| **inactive**}

Step 4 Set the password for the user account:

Firepower-chassis /security/local-user # **set password**

Enter a password: *password*

Confirm the password: *password*

If password strength check is enabled, a user's password must be strong and the FXOS rejects any password that does not meet the strength check requirements (see Guidelines for Passwords, on page 3).

Note Passwords must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). This restriction applies whether the password strength check is enabled or not.

Step 5 (Optional) Specify the first name of the user:

Firepower-chassis /security/local-user # **set firstname** *first-name*

Step 6 (Optional) Specify the last name of the user:

Firepower-chassis /security/local-user # **set lastname** *last-name*

Step 7 (Optional) Specify the date that the user account expires. The *month* argument is the first three letters of the month name.

Firepower-chassis /security/local-user # **set expiration** *month day-of-month year*

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 expiration date available.

Step 8 (Optional) Specify the user e-mail address.

Firepower-chassis /security/local-user # **set email** *email-addr*

Step 9 (Optional) Specify the user phone number.

Firepower-chassis /security/local-user # **set phone** *phone-num*

Step 10 (Optional) Specify the SSH key used for passwordless access.

Firepower-chassis /security/local-user # **set sshkey** *ssh-key*

Step 11 All users are assigned the *read-only* role by default and this role cannot be removed. For each additional role that you want to assign to the user:

Firepower-chassis /security/local-user # **create role** *role-name*

where *role-name* is the role that represents the privileges you want to assign to the user account (see User Roles, on page 6).

Note 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.

Step 12 To remove an assigned role from the user:

Firepower-chassis /security/local-user # **delete role** *role-name*

All users are assigned the *read-only* role by default and this role cannot be removed.

Note When you delete a user role, current session IDs for the user are revoked, meaning all of the user's active sessions (both CLI and Web) are immediately terminated.

Step 13 Commit the transaction.

Firepower-chassis security/local-user # **commit-buffer**

Example

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

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # create role admin
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

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

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
Firepower-chassis /security/local-user* # create role aaa
Firepower-chassis /security/local-user* # create role operations
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /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.

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /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
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

Deleting a Local User Account

Procedure

Step 1 Enter security mode:

Firepower-chassis# **scope security**

Step 2 Delete the local-user account:

Firepower-chassis /security # **delete local-user** *local-user-name*

Step 3 Commit the transaction to the system configuration:

Firepower-chassis /security # **commit-buffer**

Example

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

```
Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Activating or Deactivating a Local User Account

You must be a user with admin or AAA privileges to activate or deactivate a local user account.

Procedure

Step 1 Enter security mode:

Firepower-chassis# **scope security**

Step 2 Enter local-user security mode for the user you want to activate or deactivate:

Firepower-chassis /security # **scope local-user** *local-user-name*

Step 3 Specify whether the local user account is active or inactive:

Firepower-chassis /security/local-user # **set account-status** {**active** | **inactive**}

Note The admin user account is always set to active. It cannot be modified.

Step 4 Commit the transaction to the system configuration:

Firepower-chassis /security/local-user # **commit-buffer**

Example

The following example enables a local user account called accounting:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope local-user accounting
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Clearing the Password History for a Locally Authenticated User

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter local user security mode for the specified user account:

Firepower-chassis /security # **scope local-user** *user-name*

Step 3 Clear the password history for the specified user account:

Firepower-chassis /security/local-user # **clear password-history**

Step 4 Commit the transaction to the system configuration:

Firepower-chassis /security/local-user # **commit-buffer**

Example

The following example clears the password history and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```