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; however, the account password must be reset.

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 14.

- 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.

Authenication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
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

Configuring User Settings

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Settings** tab.

Step 3 Complete the following fields with the required information:

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.

Name	Description
Default Authentication field	The default method by which a user is authenticated during remote login. This can be one of the following: • **Local**—The user account must be defined locally on the chassis. • **Radius**—The user account must be defined on the RADIUS server specified for the chassis. • **TACACS**—The user account must be defined on the TACACS+ server specified for the chassis. • **LDAP**—The user account must be defined on the LDAP/MS-AD server specified for the chassis. • **None**—If the user account is local to the chassis, no password is required when the user logs in remotely. **Note** All **Radius**, **TACACS**, and **LDAP** settings must be configured under Platform Settings. For more information, see About AAA in the Platform Settings chapter.
Console Authentication field	The method by which a user is authenticated when connecting to the FXOS CLI via the console port. This can be one of the following: • **Local**—The user account must be defined locally on the chassis. • **Radius**—The user account must be defined on the RADIUS server specified for the chassis. • **TACACS**—The user account must be defined on the TACACS+ server specified for the chassis. • **LDAP**—The user account must be defined on the LDAP/MS-AD server specified for the chassis. • **None**—If the user account is local to the chassis, no password is required when the user connects to the FXOS CLI using the console port.
Remote User Settings	
Remote User Role Policy	Controls what happens when a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information: • **Assign Default Role**—The user is allowed to log in with a read-only user role. • **No-Login**—The user is not allowed to log in to the system, even if the username and password are correct.
Local User Settings	

Name	Description
Password Strength Check check box	If checked, all local user passwords must conform to the guidelines for a strong password (see Guidelines for Passwords, on page 3). The strong password check is enabled by default.
History Count field	The number of unique passwords a user must create before the user can reuse a previously used password. The history count is in reverse chronological order with the most recent password first to ensure that only the oldest password can be reused when the history count threshold is reached. This value can be anywhere from 0 to 15. You can set the **History Count** field to 0 to disable the history count and allow users to reuse previously used passwords at any time.
Change During Interval field	Controls when a locally authenticated user can change his or her password. This can be: • **Enable**—Locally authenticated users can change their passwords based on the settings for Change Interval and Change Count. • **Disable**—Locally authenticated users cannot change their passwords for the period of time specified for No Change Interval.
Change Interval field	The 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.
Change Count field	The maximum number of times a locally authenticated user can change his or her password during the Change Interval. This value can be anywhere from 0 to 10.
No Change Interval field	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 not set to **Disable**.
Passphrase Expiration Days field	Set the expiration between 1 and 9999 days. By default, expiration is disabled.
Passphrase Expiration Warning Period field	Set the number of days before expiration to warn the user about their password expiration at each login, between 0 and 9999. The default is 14 days.
Expiration Grace Period field	Set the number of days a user has to change their password after expiration, between 0 and 9999. The default is 3 days.

Name	Description
Password Reuse Interval field	Set the number of days before you can reuse a password, between 1 and 365. The default is 15 days. If you enable both the **History Count** and the **Password Reuse Interval**, then both requirements must be met. For example, if you set the history count to 3, and the reuse interval to 10 days, then you can change your password only after 10 days have passed, and you have changed your password 3 times.

Step 4 Click **Save**.

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
```

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**

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

Creating a Local User Account

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 Click **Add User** to open the **Add User** dialog box.

Step 4 Complete the following fields with the required information about the user:

Name	Description
User Name field	The account name that is 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 save the user, the login ID cannot be changed. You must delete the user account and create a new one.
First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address for the user.

Name	Description
Phone Number field	The telephone number for the user.
Password field	The password associated with this account. 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.
Confirm Password field	The password a second time for confirmation purposes.
Account Status field	If the status is set to **Active**, a user can log into Firepower Chassis Manager and the FXOS CLI with this login ID and password.
User Role list	The role that represents the privileges you want to assign to the user account (see User Roles, on page 6). All users are assigned the Read-Only role by default and this role cannot be deselected. To assign multiple roles, hold down **Ctrl** and click the desired roles. **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.
Account Expires check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field. **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.
Expiry Date field	The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 5 Click **Add**.

Deleting a Local User Account

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 In the row for the user account that you want to delete, click **Delete**.

Step 4 In the **Confirm** dialog box, click **Yes**.

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 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 In the row for the user account that you want to activate or deactivate, click **Edit (pencil icon)**.

Step 4 In the **Edit User** dialog box, do one of the following:

- To activate a user account, click the **Active** radio button in the **Account Status** field. Note that when you reactivate a user account, the account password must be reset.
- To deactivate a user account, click the **Inactive** radio button in the **Account Status** field.

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

Step 5 Click **Save**.

Step 6 Commit the transaction to the system configuration:

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

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 #
```