Secure Role-Based Access Control

User roles are assigned privileges that define what that user can do on the system. 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.

Using the FXOS Chassis Manager web interface or FXOS CLI, you can configure the following settings for each user account on the system:

- User Role - the role that represents the privileges you want to assign to the user account.

  All users are assigned the Read-Only role by default and this role cannot be deselected. To assign multiple roles, hold down **Ctrl**+ click the desired roles.

- Account Expiration Date
- Account Status - if the status is set to **Active**, the user can log into Firepower Chassis Manager and the FXOS CLI with their login ID and password.

For maximum security on locally-authenticaed accounts, configure SSH for encrypted sessions.

- Password Management, on page 2
- Harden Locally Authenticated User Accounts, on page 2
- Harden Remotely Authenticated User Accounts, on page 2

Password Management

Passwords control access to resources or devices, and administrators define passwords to authenticate requests. When FXOS recieves a request for access to a resource or device, the request is challenged for verification of the password and identity, and access is granted, denied, or limited based on the result. Security best practices dictate that passwords should be managed with an LDAP, TACACS+ or RADIUS authentication server. However, a locally configured password for access is still required in the event that LDAP, TACACS+ or RADIUS services fail. A device can also have other password information present within its configuration, such as an NTP key, or a SNMP community string.

Harden Locally Authenticated User Accounts

When configuring individual internal user roles, admin account users can use the following settings to harden the system against attacks through web interface login mechanisms:

- Set 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 (**set max-login-attempts**)
- Set the amount of time the user should remain locked out of the system after exceeding the maximum number of login attempts (**set user-account-unlock-time**)
- Enforce a minimum password length (**set min-password-length**)
- Specify the minimum number of hours that a locally authenticated user must wait before changing a newly created password (**set no-change-interval**)
- Set the number of days local user accounts are valid (**set expiration**)
- Require strong passwords (**set enforce-strong-password yes**)
- Assign user access privileges appropriate only to the type of access the user requires (**create role**)

Harden Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+. Remote authentication allows for a maximum of 16 TACACS+ servers, 16 RADIUS servers, and 16 LDAP providers for a total of 48 providers.

AAA is a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. These processes are considered important for effective network management and security.

Note that 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.

TACACS+ is an authentication protocol that the FXOS chassis can use to authenticate management users against a remote AAA server. These management users can access the FXOS chassis via SSH, HTTPS, telnet, or HTTP. We recommend SSH for maximum security when accessing the FXOS chassis. Numerous authentication methods provide enhanced security.

TACACS+ authentication, or more generally AAA authentication, provides the ability to use individual user accounts for each network administrator. When you do not depend on a single shared password, the security of the network is improved and your accountability is strengthened.

RADIUS is a protocol similar in purpose to TACACS+; however, it encrypts only the password sent across the network. In contrast, TACACS+ encrypts the entire TCP payload, which includes both the username and password. For this reason, we recommend that you use TACACS+ in preference to RADIUS when TACACS+ is supported by the AAA server.

LDAP is a client-server protocol for accessing directory services, such as Microsoft Active Directory. LDAP does not require any security between the client and server. However, through the use of SSL, LDAP can encrypt user sessions between the client and server. This keeps all information transferred in LDAP transactions over the network secure. For this reason, we strongly recommend that you use LDAP in preference to TLS.

For more information and detailed procedures on how to configure RADIUS, TACAS+, and LDAP on your FXOS chassis, see the Configuring AAA section in the Platform Settings chapter of the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.