Firepower 4100/9300 FXOS Local User Password Recovery via TACACS Administrative Access

Contents

Issue

The local admin password for FXOS on Firepower 4100/9300 appliances was unknown and needed to be reset to reg

All existing TACACS users were only assigned the Read-
Only role, which restricted them from performing administrative tasks on the FXOS chassis.

Note: Remotely authenticated user accounts (LDAP, RADIUS, TACACS+, SSO) are assigned the Read-
Only role by default.

Environment

- Cisco Firepower 4100/9300 running ASA/FTD
- FXOS default authentication set to remote (Cisco ISE); local authentication configured as fallback.

Resolution

Create an Administrative TACACS User

On Cisco ISE (or your TACACS server), create a new TACACS user (for example, **fxosadmin**) and assign administ

FXOS Chassis Authentication/Authorization for remote management with ISE using TACACS+.

1. Create the Identity groups and Users
2. Create the Shell Profile for each User Role (For 'admin' role, use cisco-av-pair=shell:roles="admin")
3. Create the TACACS Authorization Policy

Log In Using the New TACACS Admin User

Use the newly created **fxosadmin** account to log in to the FXOS GUI and CLI. This account now has full administra

Reset the Local Admin Password

Access the FXOS CLI and execute these commands:

```
FP4100# scope security
FP4100 /security # show local-user
User Name       First Name      Last name
--------------- --------------- ---------
admin
FP4100 /security # enter local-user admin
FP4100 /security/local-user # set password
```

```
Enter a password:
Confirm the password:
FP4100 /security/local-user* # commit-buffer
FP4100 /security/local-user #
```

Notes and Considerations

- When remote authentication (TACACS, RADIUS, LDAP, SSO) is the default method, you cannot log in to th
- Local and remote user accounts cannot be used interchangeably when remote authentication is active.
- In the scenario, if the console port authentication method is set to 'LOCAL', it allows verification of the new a

Cause

- The local admin password for the FXOS chassis was lost or unknown, preventing direct administrative access
- All existing TACACS user accounts were configured with Read-
  Only privileges, which restricted the ability to perform necessary administrative tasks, such as chassis reboot,
- The situation created a risk of being unable to manage or recover the device if further changes or troubleshooti
- This necessitated an admin password reset to proceed with planned maintenance activities.

Related Content

- FXOS User Management
- Password Recovery Procedure For Firepower 9300/4100 Series Appliances