

# Secure Firewall FTD Password Reset After Password Loss

## Issue

Firewall Threat Defense (FTD) became inaccessible via CLI due to a lost local admin password. The affected node could not be accessed for administrative purposes. The initial assumption was that the admin password had been changed from the default and was unknown, leading to concerns that a complete factory reset (reimage) would be required to restore access and default credentials. Specific questions arose regarding the proper procedure for handling this situation:

## Environment

- Cisco Secure Firewall 1000, 2100, and 3100 FTD managed Firepower Management Center

## Resolution

The resolution involved attempting to access the affected FTD device using the default admin credentials before proceeding with the more complex reimage procedure.

1: Before beginning, attempt to log into the affected FTD device using the factory default admin credentials.

Username: admin  
Password: Admin123

This step is to be performed first as it could eliminate the need for more disruptive recovery procedures.

2: If default credentials are ruled out, reset the admin password to a new, known value through the standard FTD CLI password change procedure.

Reimage Process: [Cisco Secure Firewall ASA and Threat Defense Reimage Guide](#)

- Perform complete reimage of the affected FTD device, adhering to the steps in the Cisco documentation.
- Restore factory default credentials through the reimage process.

## Cause

The root cause was that the admin password on the affected FTD device had never been changed from the factory default during initial deployment. The loss of access was due to the incorrect assumption that the password was unknown, rather than an actual credential loss. The device remained accessible using the default admin credentials throughout the incident.

## Related Content

- [Replace Faulty Unit in Secure Firewall Threat Defense of High Availability](#)
- [Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense: Image Management](#)
- [Cisco Secure Firewall ASA and Threat Defense Reimage Guide](#)
- [Configure, Verify, and Troubleshoot Firepower Device Registration](#)
- [Configure FTD High Availability on Firepower Appliances](#)
- [Cisco Technical Support & Downloads](#)