Reset the Password of the Admin User on a Firepower System

Contents

Introduction

Background Information

Firepower Threat Defense: Reset the Admin Password

ASA Firepower Services Module: Reset the Admin Password

- Reset the Admin Password on the ASA 5512-X through ASA 5555-X and ASA 5506-X through ASA 5516-X (Software ASA Firepower Module) and ISA 3000 Devices
- Reset the Admin Password on the ASA 5585-X Series Devices (Hardware ASA Firepower Module)

Change the CLI or Shell Admin Password for FMCs and NGIPSv

Change the Web Interface Admin Password for FMCs or the Web Interface Admin and CLI Admin Password for 7000 and 8000 Series Devices

Reset a Lost CLI or Shell Admin Password for FMCs or NGIPSv, or Reset a Lost Web Interface or CLI Password for 7000 and 8000 Series Devices

- Option 1. Safely Reboot the Device and Enter Single User Mode at Boot to Reset the Password
- Option 2. Use External Authentication to Gain Access to the CLI to Reset the Password for a Firepower Management Center

Reset a Lost Web Interface Admin Password for Firepower Management Centers

Introduction

This document describes the instructions to reset the Firepower system admin account password.

Note: Log in to the Firepower system using the default credentials Admin/admin123 to verify the password reset was successful.

Background Information

The Firepower Management Center (FMC) maintains separate admin accounts and passwords for the CLI shell and web interfaces. Managed devices, such as Firepower and Adaptive Security Appliance (ASA) Firepower Services, use a single admin account for CLI, shell, and web interface access.

Note: References to the Firepower Management Center CLI apply only to Versions 6.3+ and the 7000 and 8000 Series devices are supported through Version 6.4.

Firepower Threat Defense: Reset the Admin Password

To reset a lost admin password for a Firepower Threat Defense (FTD) logical device on Firepower 9300 and 4100 platforms, perform the instructions in the Change or Recover Password for FTD through FXOS Chassis Manager guide.

For FTD devices running on Firepower 1000/2100/3100, you must reimage the device. Review the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense for the Reimage Procedure on these platforms.

For FTD devices running on ASA 5500-X and Integrated Security Appliance (ISA) 3000 models, you must reimage the device. Review the Cisco ASA and Firepower Threat Defense Device Reimage Guide for instructions.

For virtual FTD devices, you must replace the device with a new deployment.

Reimaging of a physical device erases its configuration and resets the admin password to **Admin123**.

With the exception of FTDvs that use Firepower 7.0+ on Amazon Web Services (AWS), a new FTDv deployment has no configurations, and the admin password is **Admin123**. For FTDvs that use Firepower 7.0+ on AWS, a new deployment has no configuration and there is no default password; you supply an admin password at deployment time.

- If you reimage an FTD device managed with Firepower Device Manager:
  - If you have a recent, externally stored backup, you can restore the back-up configurations after you reimage. For more information, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version.
  - If you do not have a backup, you must recreate the device configuration manually, which includes interfaces, routing policies, and DHCP and Dynamic Domain Name System (DDNS) settings.
- If you reimage an FTD device managed with the Firepower Management Center, and the FMC and the device that runs Version 6.3+, you can use the FMC web interface to back-up the device configuration before you reimage, and restore the back-up after you reimage. For more information, see the Firepower Management Center Configuration Guide for your version.

Note: If you run v6.0.1 - 6.2.3, you cannot back-up the FTD configuration. If you run v6.3.0 - 6.6.0, and back-up and restore from the FMC web interface, it is not supported for FTD container instances. Although you can apply shared policies from the Firepower Management Center after you reimage, you must manually configure anything device-specific, such as interface, routing policies, DHCP and DDNS settings.

ASA Firepower Services Module: Reset the Admin Password

You can reset the admin password for the ASA Firepower module CLI with the session command of the ASA General Operations CLI. If you have lost the password for the ASA CLI, you can recover them as

described in the CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide for your ASA version.

Reset the Admin Password on the ASA 5512-X through ASA 5555-X and ASA 5506-X through ASA 5516-X (Software ASA Firepower Module) and ISA 3000 Devices

To reset the admin user of the ASA Firepower software module or the ISA 3000 device to the default password, enter this command at the ASA prompt: **session sfr do password-reset**

For more information, review the Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide for your ASA version.

Reset the Admin Password on the ASA 5585-X Series Devices (Hardware ASA Firepower Module)

To reset the admin user of the ASA Firepower hardware module to the default password enter this command at the ASA prompt: **session 1 do password-reset**

For more information, review the Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide for your ASA version.

Change the CLI or Shell Admin Password for FMCs and NGIPSv

Use these instructions to reset a known password for these admin accounts:

- Firepower Management Center: Admin password used to access the CLI or the shell.
- Next Generation Information Preservation System Virtual (NGIPSv: Admin password used to access CLI.

Procedure:

1. Log into the Appliance Admin account by SSH or the console.
    - For the Firepower Management Center:
        - If your Firepower Management Center runs Firepower v6.2 or lower, the log in provides you with direct access to the Linux shell.
        - If your Firepower Management Center runs Firepower v6.3 or 6.4 and the Firepower Management Center CLI is not enabled, the log in provides you with direct access to the Linux shell.
        - If your Firepower Management Center runs Firepower v6.3 or 6.4 and the Firepower Management CLI is enabled, log in provides you with direct access to the Firepower Management Center CLI. Enter the expert command to access the Linux shell.
        - If your Firepower Management Center runs Firepower v6.5+, the log in provides you

with direct access to the Firepower Management Center CLI. Enter the expert command to access the Linux shell.
    - For managed devices, the log in provides you with access to the CLI. Enter the expert command to access the Linux shell.
2. At the shell prompt, enter this command: **sudo passwd admin**.
3. When prompted, enter the current admin password to elevate root access privileges.
4. In response to prompts, enter the new admin password twice.

Note: If the system displays a BAD PASSWORD message, this is informational only. The system applies the password you supply even if this message appears. However, Cisco recommends you use a more complex password for security reasons.

---

1. Type **exit** to exit the shell.
2. On a managed device, or on a Firepower Management Center with CLI enabled, type **exit** to exit the CLI.

Change the Web Interface Admin Password for FMCs or the Web Interface Admin and CLI Admin Password for 7000 and 8000 Series Devices

Use these instructions to reset a known password for these admin accounts:

- Firepower Management Center: admin password used to access the web interface.
- 7000 and 8000 Series devices: admin password used to access the web interface, as well as the CLI.

Procedure:

1. Log into the web interface for the appliance as a user with Administrator access.
2. Choose **System** > **Users** and click the **Edit** icon for the admin user.
3. Enter values for the **Password** and **Confirm Password** fields.
   The values must be the same and must conform with the password options set for the user.
4. Click **Save**.

Reset a Lost CLI or Shell Admin Password for FMCs or NGIPSv, or Reset a Lost Web Interface or CLI Password for 7000 and 8000 Series Devices

Use these instructions to reset a lost password for these admin accounts:

- Firepower Management Center: Admin password used to access the CLI or shell.
- 7000 and 8000 Series devices: Admin password used to access the web interface, as well as CLI.
- NGIPSv: Admin password used to access the CLI.

Note: To reset a lost password for these admin accounts, you must establish a console or SSH connection with the appliance (in the case of a Firepower Management Center with external users configured, you can use an SSH connection). You must also reboot the appliance whose admin credentials you have lost. You can initiate the reboot in different ways, depending on what type of device access you have available:
• For the Firepower Management Center, you must have log in credentials for a web interface user with Administrator access, or the log in credentials for an externally authenticated user with CLI/shell access.
• For 7000 or 8000 Series devices, you must have log in credentials for a web interface user with Administrator access, a CLI user with Configuration access, or a user with Administrator access on the managed Firepower Management Center.
• For NGIPSv, you must have log in credentials for a CLI user with Configuration access, or a user with Administrator access on the managed Firepower Management Center.
• For the Firepower Management Center, 7000 and 8000 Series devices and NGIPSv devices, if you have a console connection (physical or remote), you can perform this task without log in credentials.

If you cannot access the device with one of these methods, you cannot reset the admin password with these instructions; please contact Cisco TAC.

Option 1. Safely Reboot the Device and Enter Single User Mode at Boot to Reset the Password

1. Open a connection to the appliance console for the device whose admin password you have lost:
   • For 7000/8000 Series devices and Firepower Management Centers, use a keyboard/monitor or serial connection.
   • For virtual appliances, use the console provided by the virtual platform. Review the Cisco Firepower Management Center Virtual Getting Started Guide or the Cisco Firepower NGIPSv Quick Start Guide for VMware for more information.
   • Alternatively, for Firepower Management Centers, 7000/8000 Series and virtual appliances, if you have a console connection established with the appliance through use of the remote Keyboard Video/Mouse (KVM), you can access that interface.
2. Reboot the device whose admin password you have lost and you have these choices:
   • For the Firepower Management Center:
   a. Log into the web interface for the Firepower Management Center as a user with Administrator access.
   b. Reboot the Firepower Management Center as described in the Firepower Management Center Configuration Guide for your version.

   • For 7000 or 8000 Series devices or NGIPSv, if you have credentials for a web interface user with Administrator access on the managed Firepower Management Center:
   a. Log in to the web interface for the managed Firepower Management Center as a user with Administrator access.
   b. Shut down and restart the managed device as described in the Firepower Management Center Configuration Guide for your version.

   • For 7000 or 8000 Series devices, if you have credentials for a web interface user with Administrator access:
   a. Log in to the web interface for the device as a user with Administrator access.
   b. Reboot the device as described in the Firepower Management Center Configuration Guide for your version.

• For 7000 or 8000 Series devices or NGIPSv, if you have credentials for a CLI user with Configuration access:
a. Log in to the appliance with shell through a user name with the CLI Configuration access.
b. At the prompt, enter the system reboot command.

• For Firepower Management Centers, 7000 and 8000 Series and virtual appliances with a console, press CTRL-ALT-DEL (if you use a remote KVM, the KVM interface provides a way to send **CTRL-ALT-DEL** to the device without interference with the KVM itself).



Note: When you reboot your Firepower Management Center or managed device, this logs you out of your appliance and the system runs a database check that can take up to an hour to complete.



Caution: Do not shut down appliances with the power button or unplug the power cable; it can corrupt the system database. Shut down appliances completely by use of the web interface.

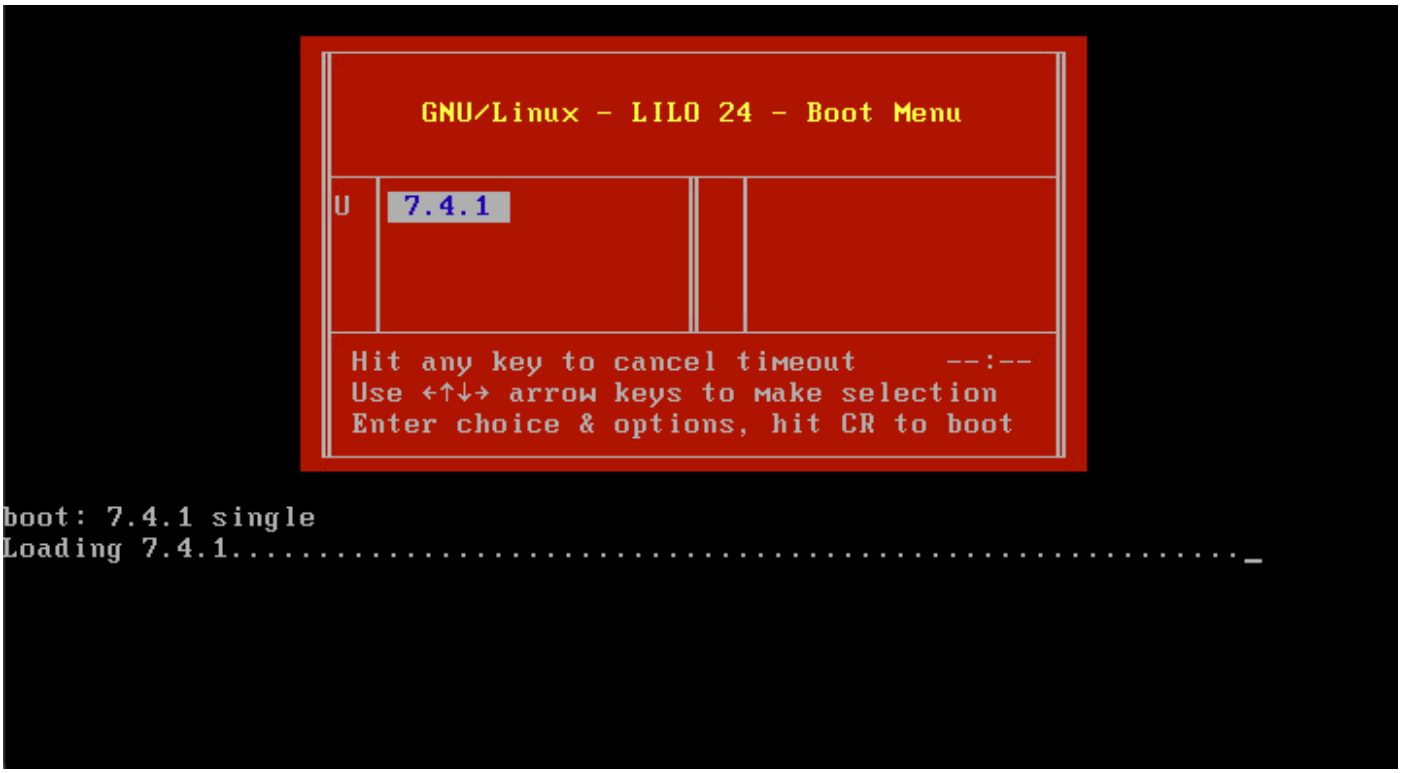
---

3. At the appliance console display, observe the reboot process and proceed dependent on the type of appliance that is rebooted:



Note: If the system is in the process of a database check, you can see the message: "**The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish.**"

• For Firepower Management Centers models 750, 1500, 2000, 3500, or 4000, or for Firepower 7000 or 8000 Series devices or NGIPSv, interrupt the reboot process:
a. Once the appliance begins to boot up, press any key on your keyboard to cancel the countdown at the LILO Boot Menu.
b. The version number displayed in the LILO Boot Menu. In this example, the version number is 7.4.1



c. At the **boot** prompt, type the "**command_version single**" where the version is the version number (for example "**7.4.1 single**"). If the system has United Capabilities Approved Products List (UCAPL) compliance enabled, you are prompted for a password; enter the password **Sourcefire**.

- For Firepower Management Centers models 1000, 1600, 2500, 2600, 4500, or 4600:

- When the boot menu appears, select **Option 4, Cisco Firepower Management Console Password Restore Mode**.

4. Assign a new admin password; use the instructions appropriate to your device:
   - For a new CLI and shell admin password for the Firepower Management Center or NGIPSv:

     a. When the system displays an OS prompt that ends with a pound sign (#), enter this command: **passwd admin**.

     b. Enter the new admin password when prompted to do so (twice).

     Note: If the system displays a BAD PASSWORD message, this is informational only. The system applies the password you supply even if this message appears. However, it is recommended that you use a more complex password for security reasons.

- For a new Web and CLI admin password for the 7000 and 8000 Series devices:

- At the OS prompt that ends with the pound sign (#), enter this command:

usertool.pl -p 'admin password'

- Where a password is the new admin password.

5. If the admin account has been locked down due to too many failed log in attempts, you must unlock the account. Use the instructions appropriate to your device:

• To unlock the CLI and shell admin accounts on a Firepower Management Center or NGIPSv, enter this command at the OS prompt that ends with the pound sign (#):

pam_tally --user admin --reset

• To unlock both the Web and CLI admin accounts on 7000 and 8000 Series devices, enter this command at the OS prompt that ends with a pound sign (#):

usertool.pl -u admin

6. At the OS prompt that ends with the pound sign (#), enter the **reboot** command.

7. Allow the reboot process to complete.

Option 2. Use External Authentication to Gain Access to the CLI to Reset the Password for a Firepower Management Center

If you are in a situation where you still have access to the FMC Web Interface with an account with Administrator access, you can use the **External Authentication** feature to gain access to the CLI. This method allows you to log into the CLI of an FMC, access the Linux shell, elevate to root, and reset the CLI/shell admin password manually. This option does not require a reboot or console access. This option requires you to have properly configured External Authentication (with SSH access) on the Firepower Management Center where you want to reset the admin password (review the Firepower Management Center Configuration Guide for your version for instructions). Once this is configured, complete these steps:

1. Log in to the Firepower Management Center with an externally authenticated account that has CLI/shell access with the use of SSH or the console:
   - If your FMC runs v6.2 or lower, this provides you with direct access to the Linux shell.
   - If your FMC runs v6.3 or 6.4 and FMC CLI is not enabled, this provides you with direct access to the Linux shell.
   - If your FMC runs v6.3 or 6.4 and the Firepower Management Center CLI is enabled, this provides you with access to the Firepower Management Center CLI. Enter the **expert** command to access the

Linux shell.
• If your FMC runs v6.5+, this provides you with access to the Firepower Management Center CLI. Enter the **expert** command to access the Linux shell.
2. At the shell prompt with a dollar sign ($), run this command to reset the CLI password for the admin user:
sudo passwd admin
3. At the **Password** prompt, enter the password for the username you are currently logged in as.
4. Enter the new admin password when prompted to do so (twice).

Note: If the system displays a **BAD PASSWORD** message, this is informational only. The system applies the password you supply, even if this message appears. However, Cisco recommends that you use a more complex password for security reasons.

---

1. If the **admin** account has been locked out due to too many failed log in attempts, you must unlock the account, run the **pam_tally** command and enter your password when prompted:
sudo pam_tally --user --reset
2. Type **exit** to leave shell.
3. On a Firepower Management Center with the CLI enabled, type **exit** to leave the CLI.

Reset a Lost Web Interface Admin Password for Firepower Management Centers

Use these instructions to change the password for the admin account used to access the Firepower Management Center web interface.

Procedure:

1. Log in to the appliance with the CLI admin account with SSH or the console.
2. Access the Linux shell:
• If your FMC runs 6.2 or lower, logging in provides you with direct access to the Linux shell.
• If your FMC runs 6.3 or 6.4 and the Firepower Management Center CLI is not enabled, logging in provides you with direct access to the Linux shell.
• If your FMC runs 6.3 or 6.4 and the Firepower Management Center CLI is enabled, logging provides you with access to the Firepower Management Center CLI. Run the **expert** command to access the Linux shell.
• If your FMC runs 6.5+, the log in provides you with access to the Firepower Management Center CLI. Run the **expert** command to access the Linux shell.
3. At the shell prompt, run this command to reset the password for the web interface admin user:
sudo usertool.pl -p 'admin password'
Where **password** is the new password for the web interface admin user.
4. At the **Password** prompt, enter the password for the username you are currently logged in.
5. If the Web admin account has been locked out due to too many failed log in attempts, you must unlock the account. Run the **usertool** command, enter your CLI admin password when prompted:
sudo usertool.pl -u admin
6. Type **exit** to leave shell.
7. On a Firepower Management Center with the CLI enabled, type **exit** to leave the CLI.