Reset the Password of the Admin User on a Cisco Firepower System

Contents

Introduction

This document provides instructions for resetting the password of the `admin` account on FireSIGHT, Firepower, and ASA FirePOWER Services appliances, including in situations where that password has been lost. The Defense Center and Firepower Management Center provide different `admin` accounts (with separate passwords) for Command Line Interface (CLI)/shell access and web interface access (when available). The `admin` account on managed devices is the same for CLI access, shell access, and web interface access (when available.)

These instructions cite the Firepower Management Center; the same instructions apply to the Defense Center.

Note: References to the Firepower Management Center CLI apply only to Versions 6.3+.

Firepower Threat Defense: Resetting the admin password

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

For FTD devices running on Firepower 2100, you must reimage the device. See the Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense for the Reimage Procedure on this platform.

For FTD devices running on ASA5500-X and ISA 3000 models, you must reimage the device. See the Cisco ASA and Firepower Threat Defense Device Reimage Guide for instructions.

Reimaging a device erases its configuration and resets the `admin` password to `Admin123.`

- If you reimage an FTD device managed with Firepower Device Manager: If you have a recent, externally stored backup, you can restore the backed up configurations after you reimage. For more information see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager* for your version (https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html).If you have no backup you must recreate the device configuration manually, including interfaces, routing policies, and DHCP and DDNS settings.
- If you reimage an FTD device managed with the Firepower Management Center: If the FMC and the device are running Version 6.3+, you can use the FMC web interface to back up the device configuration before you reimage, and restore the backup after you reimage. For more information, see the Firepower Management Center Configuration Guide for your version. **Note**: Backup and restore from the FMC web interface is not supported for FTD container instances.If you are running an earlier version, you cannot back up the device configuration. Although you can apply shared policies from the Firepower Management Center after you reimage, you must manually configure anything device-specific, such as interfaces, routing policies, and DHCP and DDNS settings.

ASA FirePOWER Services Module: Resetting the admin

You can reset the admin password of the ASA FirePOWER module CLI using the `session` command of the ASA General Operations CLI. If you have lost the passwords for the ASA CLI, you can recover them as described in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide for your ASA version.

Resetting the admin Password on the ASA 5512-X through ASA 5555-X and ASA 5506-X through ASA 5516-X Devices (Software Module)

To reset the `admin` user of the ASA FirePOWER software module to the default password enter this command at the ASA prompt:

```
session sfr do password-reset
```

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

Resetting the admin Password on the ASA 5585-X Series Devices (Hardware 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, see the Cisco ASA Series CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide for your ASA version.

Changing the CLI or Shell admin Password for FMCs, 7000 and 8000 Series Devices, and NGIPSv

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

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

Procedure:

1. Log into the appliance via SSH using the `admin` account.
   • For the Firepower Management Center, by default this gives you access to the shell. If the Firepower Management Center CLI is enabled, this give you access to the CLI.
   • For managed devices this gives you access to the device CLI.

2. For managed devices, or for a Firepower Management Center with the CLI enabled, enter the `expert` command to access the shell.

3. At the shell prompt enter the following command:
   ```
   sudo passwd admin
   ```

4. When prompted, enter the current `admin` password to elevate privilege to root access.

5. 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 that you use a more complex password for security reasons.
6. Type `exit` to exit the shell.

7. On a managed device, or on a Firepower Management Center with the CLI enabled, type `exit` to exit the CLI.

Changing the Web Interface admin Password for FMCs and 7000 and 8000 Series Devices

Use these instructions to reset a known password for the following `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 appliance via SSH using the `admin` account.

• For the Firepower Management Center by default this gives you access to the shell. If the Firepower Management Center CLI is enabled, this gives you access to the CLI.
• For managed devices this gives you access to the device CLI.

2. For managed devices, or for a Firepower Management Center with the CLI enabled, enter the `expert` command to access the shell.

3. At the shell prompt enter the following command:
   `sudo usertool.pl -p 'admin` *`password`*`'`
   Where *`password`* is the desired new password.

4. Type `exit` to exit the shell.

5. On a managed device, or on a Firepower Management Center with the CLI enabled, type `exit` to exit the CLI.
6. In some cases you may have to reload the FMC to user the new web interface password

Resetting a Lost CLI or Shell admin Password for FMCs, 7000 and 8000 Series Devices, and NGIPSv

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

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

> **Note**: To reset a lost password for these `admin` accounts you need to establish a console connection with the appliance. You also need to 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 need the login credentials for a web interface user with Administrator access.
> • For 7000 or 8000 Series devices you need the login credentials for one of the following means of access: a web interface user with Administrator access, a CLI user with Configuration access, or a user with Administrator access on the managing Firepower Management Center.
> • For NGIPSv you need login credentials for a CLI user with Configuration access, or a user with Administrator access on the managing Firepower Management Center.
>
> If you cannot access the device with one of those methods, you cannot reset the `admin` password with these instructions; contact Cisco TAC.

Option 1 - Safely reboot the device and enter single 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 Series devices, 8000 Series devices, and Firepower Management Centers use a keyboard/monitor connection, specifying the host name of the device or the IP address of the management interface for the appliance.
- For virtual appliances use the VMware console. See the Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide for more information.

2. Reboot the device whose `admin` password you have lost. You have the following choices:

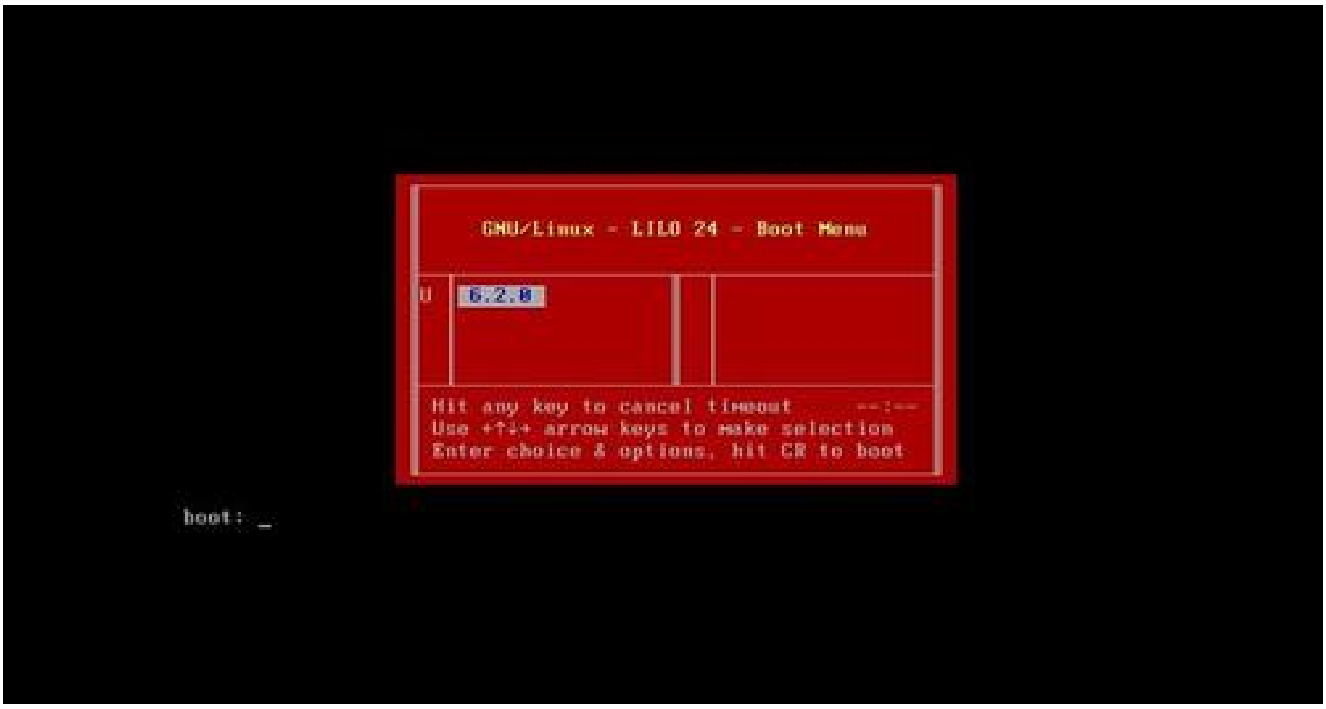
   - For the Firepower Management Center:
   A. Log into the web interface for the Firepower Management Center as a user with Administrator access.
   B. Reboot the Firepower Management Center as described in the Firepower Management Center Configuration Guide for your version.

   - For 7000 or 8000 Series devices or NGIPSv, if you have credentials for a web interface user with Administrator access on the managing Firepower Management Center:
   A. Log into the web interface for the managing 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 into the appliance via the shell using a user name with the CLI Configuration access.
   B. At the prompt, enter the `system reboot` command.
   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 off appliances using the power button, or by unplugging the power cable; it may corrupt the system database. Shut down appliances completely using the web interface.

3. At the appliance console display, observe the reboot process and proceed depending on the type of appliance being rebooted:
   Note: If the system is performing a database check, you may see the following message: `The system is not operational yet. Checking and repairing database are 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. Note the version number displayed in the LILO Boot Menu. In the example below the version number is `6.2.0`.



```
GNU/Linux - LILO 24 - Boot Menu

6.2.0

Hit any key to cancel timeout      --:--
Use ←↑↓→ arrow keys to make selection
Enter choice & options, hit CR to boot

boot: _
```

C. At the `boot:` prompt, type the command *`version`* `single` where *`version`* is the version number (for example `6.2.0 single)`.

• For Firepower Management Centers models 1000, 2500, or 4500:
When the boot menu appears, select Option 4, Cisco Firepower Management Console Password Restore Mode.

4. When the system displays an OS prompt ending with a pound sign (`#), enter the command` `passwd admin`.

5. 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.
6. At the OS prompt ending 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

If you are in a situation where you still have access to the FMC Web Interface, you can leverage the "External Authentication" feature to gain access to the CLI. Using this method will allow you to log into the CLI of a device, elevate to root, and reset the admin password manually. This option does **not** require a reboot or console access. This option requires that you have properly configured External Authentication (with SSH access) on the device that you wish to reset the admin password for. Once this is configured, follow the steps below:

1. Open a connection to the appliance to access the shell login prompt.

2. At the `login as:` command prompt, enter the username of the external authentication account that has shell access.

3. At the `Password:` prompt, enter the password for the external authentication account.

4. For managed devices or for a Firepower Management Center with the CLI enabled, at the CLI prompt, enter the `expert` command to exit the CLI and access the shell.

5. At the shell prompt with a dollar sign (`$), enter the following command to reset the CLI password for the admin` user:
   ```
   sudo passwd admin
   ```

6. At the `Password:` prompt, enter the password for the username with which you are currently logged in.
7. 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.
8. Type `exit` to exit the shell.

9. On a managed device or on a Firepower Management Center with the CLI enabled, type `exit` to exit the CLI.

Resetting a Lost Web Interface admin Password for FMCs and 7000 and 8000 Series Devices

Use these instructions to change the passwords for the following `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 shell

Procedure:

1. Open a connection to the appliance to access the shell login prompt:
   - For 7000 Series devices, 8000 Series devices, and Firepower Management Centers, use a keyboard/monitor or serial connection, specifying the hostname of the device or the IP address of the management interface for the appliance.
   - For virtual Firepower Management Centers use the VMware console. See the Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide for more information.

2. At the `login as:` command prompt, enter a user name.
   - For Firepower Management Centers, enter `admin.`
   - For 7000 and 8000 Series devices, enter a user name with CLI Configuration access.

3. At the `Password:` prompt, enter the password.

4. For managed devices or for a Firepower Management Center with the CLI enabled, at the CLI prompt, enter the `expert` command to exit the CLI and access the shell.

5. At the shell prompt, enter the following command to reset the password for the web interface `admin` user:
   ```
   sudo usertool.pl -p 'admin password'
   ```
   Where *`password`* is the new password.

6. At the `Password:` prompt, enter the password for the username with which you are currently logged in.

7. Type `exit` to exit the shell.

8. On a managed device or on a Firepower Management Center with the CLI enabled, type `exit` to exit the CLI.