Getting Started

- Task Flow, on page 1
- Initial Configuration Using Console Port, on page 1
- Accessing the FXOS CLI, on page 4

Task Flow

The following procedure shows the basic tasks that should be completed when configuring your Firepower 9300 chassis.

Procedure

Step 1	Configure the Firepower 9300 chassis hardware (see the *Cisco Firepower Security Appliance Hardware Installation Guide*).
Step 2	Complete the initial configuration (see Initial Configuration Using Console Port, on page 1).
Step 3	Set the Date and Time (see Setting the Date and Time).
Step 4	Configure a DNS server (see Configuring DNS Servers).
Step 5	Register your product license (see License Management for the ASA).
Step 6	Configure users (see User Management).
Step 7	Perform software updates as required (see Image Management).
Step 8	Configure additional platform settings (see Platform Settings).
Step 9	Configure interfaces (see Interface Management).
Step 10	Create logical devices (see Logical Devices).

Initial Configuration Using Console Port

Before you can use Firepower Chassis Manager or the FXOS CLI to configure and manage your system, you must perform some initial configuration tasks using the FXOS CLI accessed through the console port.Use the following procedure to perform initial configuration using the FXOS CLI accessed through the console port.

The first time that you access the Firepower 9300 chassis using the FXOS CLI, you will encounter a setup wizard that you can use to configure the system.

Note To repeat the initial setup, you need to erase any existing configuration using the following commands:

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

You can choose to either restore the system configuration from an existing backup file, or manually set up the system by going through the Setup wizard. If you choose to restore the system, the backup file must be reachable from the management network.

You must specify only one IPv4 address, gateway, and subnet mask, or only one IPv6 address, gateway, and network prefix for the single management port on the Firepower 9300 chassis. You can configure either an IPv4 or an IPv6 address for the management port IP address.

Before you begin

1. Verify the following physical connections on the Firepower 9300 chassis:
   - The console port is physically connected to a computer terminal or console server.
   - The 1 Gbps Ethernet management port is connected to an external hub, switch, or router.

   For more information, refer to the *Cisco Firepower Security Appliance Hardware Installation Guide*.
2. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
   - 9600 baud
   - 8 data bits
   - No parity
   - 1 stop bit
3. Gather the following information for use with the setup script:
   - New admin password
   - Management IP address and subnet mask
   - Gateway IP address
   - Hostname and domain name
   - DNS server IP address

Procedure

Step 1 Power on the chassis.

Step 2 Connect to the serial console port using a terminal emulator.

The Firepower includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection. Use the following serial parameters:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Step 3 Complete the system configuration as prompted.

Example:

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (yes/no) [y]: n
Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300
Physical Switch Mgmt0 IP address : 10.80.6.12
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.80.6.1
Configure the DNS Server IP address? (yes/no) [n]: y
  DNS IP address : 10.164.47.13
Configure the default domain name? (yes/no) [n]: y
  Default domain name : cisco.com

Following configurations will be applied:
  Switch Fabric=A
  System Name=firepower-9300
  Enforced Strong Password=no
  Physical Switch Mgmt0 IP Address=10.89.5.14
  Physical Switch Mgmt0 IP Netmask=255.255.255.192
  Default Gateway=10.89.5.1
  IPv6 value=0
  DNS Server=72.163.47.11
  Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

Accessing the FXOS CLI

You can connect to the FXOS CLI using a terminal plugged into the console port. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You can also connect to the FXOS CLI using SSH and Telnet. The Firepower eXtensible Operating System supports up to eight simultaneous SSH connections. To connect with SSH, you need to know the hostname or IP address of the Firepower 9300 chassis.

Use one of the following syntax examples to log in with SSH, Telnet, or Putty:

Note SSH log in is case-sensitive.

From a Linux terminal using SSH:

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

From a Linux terminal using Telnet:

Note Telnet is disabled by default. See Configuring Telnet for instructions on enabling Telnet.

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

```
Login as: ucs-example\jsmith
```

Note If the default authentication is set to local, and the console authentication is set to LDAP, you can log in to the fabric interconnect from a Putty client using **ucs-local\admin**, where admin is the name of the local account.