Getting Started

Task Flow

The following procedure shows the basic tasks that should be completed when configuring your Firepower 4100/9300 chassis.

Procedure

Step 1	Configure the Firepower 4100/9300 chassis hardware (see the *Cisco Firepower Security Appliance Hardware Installation Guide*).
Step 2	Complete the initial configuration (see Initial Configuration, on page 1).
Step 3	Log in to the Firepower Chassis Manager (see Log In or Out of the Firepower Chassis Manager, on page 8).
Step 4	Set the Date and Time (see Setting the Date and Time).
Step 5	Configure a DNS server (see Configuring DNS Servers).
Step 6	Register your product license (see License Management for the ASA).
Step 7	Configure users (see User Management).
Step 8	Perform software updates as required (see Image Management).
Step 9	Configure additional platform settings (see Platform Settings).
Step 10	Configure interfaces (see Interface Management).
Step 11	Create logical devices (see Logical Devices).

Initial Configuration

Before you can use Firepower Chassis Manager or the FXOS CLI to configure and manage your system, you must perform some initial configuration tasks. You can perform the initial configuration using the FXOS CLI

accessed through the console port or using SSH, HTTPS, or REST API accessed through the management port (this procedure is also referred to as low-touch provisioning).

Initial Configuration Using Console Port

The first time that you access the Firepower 4100/9300 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 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 4100/9300 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 4100/9300 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 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
   - Subnets from which you want to allow HTTPS and SSH access (you are prompted for "IP block" addresses)
   - 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 4100/9300 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.

Note You can optionally enter the debug menu at any time during initial configuration to debug any setup issues or abort configurations and reboot the system. To enter the debug menu, press Ctrl-C. To exit the debug menu, press Ctrl-D twice. Note that anything you type in the interim between pressing Ctrl-D the first time and pressing it a second time will run after the second time Ctrl-D is pressed.

Example:

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): 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

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

Do you want to configure IP block for ssh access? (yes/no) [y]: y

SSH IP block address : 10.0.0.0

SSH IPv4 block netmask : 255.0.0.0
```

```
  Do you want to configure IP block for https access? (yes/no) [y]: y

  HTTPS IP block address : 10.0.0.0

  HTTPS IPv4 block netmask : 255.0.0.0

  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
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    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#
```

Low-Touch Provisioning Using Management Port

When your Firepower 4100/9300 chassis boots up, if it does not find the startup configuration, the device enters the Low-Touch Provisioning mode in which the device locates a Dynamic Host Control Protocol (DHCP) server and then bootstraps itself with its management interface IP address. You can then connect through the management interface to configure the system using SSH, HTTPS, or the FXOS REST API.

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 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 4100/9300 chassis. You can configure either an IPv4 or an IPv6 address for the management port IP address.

Before you begin

Gather the following information for use with the setup script:

- New admin password
- Management IP address and subnet mask
- Gateway IP address
- Subnets from which you want to allow HTTPS and SSH access (you are prompted for "IP block" addresses)
- Hostname and domain name
- DNS server IP address

Procedure

Step 1 Configure your DHCP server to assign an IP address to management port of the Firepower 4100/9300 chassis.

The DHCP client request from the Firepower 4100/9300 chassis will contain the following:

- The management interface's MAC address.
- DHCP option 60 (vendor-class-identifier)—Set to "FPR9300" or "FPR4100".
- DHCP option 61 (dhcp-client-identifier)—Set to the Firepower 4100/9300 chassis serial number. This serial number can be found on a pull-out tab on the chassis.

Step 2 Power on the Firepower 4100/9300 chassis.
If the startup configuration is not found when the chassis boots up, the device enters the Low-Touch Provisioning mode.

Step 3 To configure your system using HTTPS:

a) Using a supported browser, enter the following URL in the address bar:

https://<*ip_address*>/api

where <*ip_address*> is the IP address of the management port on the Firepower 4100/9300 chassis that was assigned by your DHCP server.

Note For information on supported browsers, refer to the release notes for the version you are using (see http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htm

b) When prompted, log in with the username **install** and the password <*chassis_serial_number*>.

The <*chassis_serial_number*> can be obtained by inspecting a tag on the chassis.

c) Complete the system configuration as prompted.

- Strong password enforcement policy (for strong password guidelines, see User Accounts) .
- Password for the admin account.
- System name
- Supervisor Management IPv4 address and subnet mask, or IPv6 address and prefix.
- Default gateway IPv4 or IPv6 address.
- Host/network address and netmask/prefix from which SSH access is allowed.
- Host/network address and netmask/prefix from which HTTPS access is allowed.
- DNS Server IPv4 or IPv6 address.
- Default domain name.

d) Click **Submit**.

Step 4 To configure your system using SSH:

a) Connect to the management port using the following command:

```
ssh install@<ip_address>
```

where <*ip_address*> is the IP address of the management port on the Firepower 4100/9300 chassis that was assigned by your DHCP server.

b) When prompted, log in with the password **Admin123**.

c) Complete the system configuration as prompted.

Note You can optionally enter the debug menu at any time during initial configuration to debug any setup issues or abort configurations and reboot the system. To enter the debug menu, press Ctrl-C. To exit the debug menu, press Ctrl-D twice. Note that anything you type in the interim between pressing Ctrl-D the first time and pressing it a second time will run after the second time Ctrl-D is pressed.

Example:

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): 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

  Supervisor Mgmt IP address : 10.80.6.12

  Supervisor Mgmt IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 10.80.6.1

  Do you want to configure IP block for ssh access? (yes/no) [y]: y

  SSH IP block address : 10.0.0.0

  SSH IPv4 block netmask : 255.0.0.0

  Do you want to configure IP block for https access? (yes/no) [y]: y

  HTTPS IP block address : 10.0.0.0

  HTTPS IPv4 block netmask : 255.0.0.0

  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
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    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
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.
```

Step 5 To configure your system using the FXOS REST API:

Use the following examples for configuring the system using the REST API. For more information, see https://developer.cisco.com/site/ssp/firepower/.

Note The attributes dns, domain_name, https_net, https_mask, ssh_net, and ssh_mask are optional. All other attributes are mandatory for REST API configuration.

```
IPv4 REST API example:

{
    "fxosBootstrap": {
        "dns": "1.1.1.1",
        "domain_name": "cisco.com",
        "mgmt_gw": "192.168.0.1",
        "mgmt_ip": "192.168.93.3",
        "mgmt_mask": "255.255.0.0",
        "password1": "admin123",
        "password2": "admin123",
        "strong_password": "yes",
        "system_name": "firepower-9300",
        "https_mask": "2",
        "https_net": "::",
        "ssh_mask": "0",
        "ssh_net": "::"
    }
}


IPV6 REST API example

{
    "fxosBootstrap": {
        "dns": "2001::3434:4343",
        "domain_name": "cisco.com",
        "https_mask": "2",
        "https_net": "::",
        "mgmt_gw": "2001::1",
        "mgmt_ip": "2001::2001",
        "mgmt_mask": "64",
        "password1": "admin123",
        "password2": "admin123",
        "ssh_mask": "0",
        "ssh_net": "::",
        "strong_password": "yes",
        "system_name": "firepower-9300"
    }
}
```

Log In or Out of the Firepower Chassis Manager

Before you can configure your Firepower 4100/9300 chassis using Firepower Chassis Manager, you must log in using a valid user account. For more information on user accounts, see User Management.

You are automatically logged out of the system if a certain period of time passes without any activity. By default, the system will log you out after 10 minutes of inactivity. To configure this timeout setting, see Configuring the Session Timeout. You can also configure an absolute timeout setting that will log users out of the system after a certain period of time even if the session is active. To configure the absolute timeout setting, see Configuring the Absolute Session Timeout.

For a list of all system changes that cause you to be automatically logged out of Firepower Chassis Manager, see System Changes that Cause Firepower Chassis Manager Sessions to be Closed.

Note You can optionally configure your Firepower Chassis Manager to allow only a certain number of unsuccessful login attempts before the user is locked out of the system for a specified amount of time. For more information, see Set the Maximum Number of Login Attempts.

Procedure

Step 1 To log in to the Firepower Chassis Manager:

a) Using a supported browser, enter the following URL in the address bar:

```
https://<chassis_mgmt_ip_address>
```

where <*chassis_mgmt_ip_address*> is the IP address or host name of the Firepower 4100/9300 chassis that you entered during initial configuration.

Note For information on supported browsers, refer to the release notes for the version you are using (see http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htm

b) Enter your username and password.

c) Click **Login**.

You are logged in and the Firepower Chassis Manager opens to show the Overview page.

Step 2 To log out of the Firepower Chassis Manager, point at your username in the navigation bar and then select **Logout**.

You are logged out of the Firepower Chassis Manager and are returned to the login screen.

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 FXOS supports up to eight simultaneous SSH connections. To connect with SSH, you need to know the hostname or IP address of the Firepower 4100/9300 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.