



使用する前に

- タスク フロー (1 ページ)
- 初期設定 (2 ページ)
- Firepower Chassis Manager のログイン/ログアウト (9 ページ)
- FXOS CLIへのアクセス (10 ページ)

タスク フロー

次に、Firepower4100/9300 シャーシを設定する際に実行する必要がある基本的なタスクの手順を示します。

手順

- ステップ1** Firepower 4100/9300 シャーシハードウェアを設定します (『Cisco Firepower Security Appliance Hardware Installation Guide』を参照)。
- ステップ2** 初期設定を完了します (初期設定 (2 ページ) を参照)。
- ステップ3** Firepower Chassis Manager にログインします (Firepower Chassis Manager のログイン/ログアウト (9 ページ) を参照)。
- ステップ4** 日付と時刻を設定します (日時の設定を参照)。
- ステップ5** DNS サーバを設定します (DNS サーバの設定を参照)。
- ステップ6** 製品ライセンスを登録します (ASA のライセンス管理を参照)。
- ステップ7** ユーザを設定します (User Managementを参照)。
- ステップ8** 必要に応じてソフトウェア アップデートを実行します (イメージ管理を参照)。
- ステップ9** 追加のプラットフォーム設定を行います (プラットフォーム設定を参照)。
- ステップ10** インターフェイスを設定します (インターフェイス管理を参照)。
- ステップ11** 論理デバイスを作成します (論理デバイスを参照)。
-

初期設定

システムの設定と管理に Firepower Chassis Manager または FXOS CLI を使用するには、初めにいくつかの初期設定タスクを実行する必要があります。初期設定を実行するには、コンソールポートを介してアクセスする FXOS CLI を使用するか、管理ポートを介してアクセスする SSH、HTTPS、または REST API を使用します（この手順は、ロータッチプロビジョニングとも呼ばれます）。

コンソールポートを使用した初期設定

FXOS CLI を使用して Firepower 4100/9300 シャーシに初めてアクセスすると、システムの設定に使用できるセットアップ ウィザードが表示されます。



(注) 初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

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

Firepower 4100/9300 シャーシの単一の管理ポートには、1つのみの IPv4 アドレス、ゲートウェイ、サブネットマスク、または1つのみの IPv6 アドレス、ゲートウェイ、ネットワークプレフィックスを指定する必要があります。管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

始める前に

1. Firepower 4100/9300 シャーシの次の物理接続を確認します。

- コンソールポートがコンピュータ端末またはコンソールサーバに物理的に接続されている。
- 1 Gbps イーサネット管理ポートが外部ハブ、スイッチ、またはルータに接続されている。

詳細については、『*Cisco Firepower Security Appliance Hardware Installation Guide*』を参照してください。

2. コンソールポートに接続しているコンピュータ端末（またはコンソールサーバ）でコンソールポートパラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データビット
- パリティなし

- 1 ストップ ビット

3. セットアップスクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネットマスク
- ゲートウェイ IP アドレス
- HTTPS および SSH アクセスを許可するサブネット（「IP ブロック」アドレスの入力を求められます）
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ1 シャーシの電源を入れます。

ステップ2 ターミナルエミュレータを使用して、シリアルコンソールポートに接続します。

Firepower には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。次のシリアルパラメータを使用します。

- 9600 ポー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ステップ3 プロンプトに従ってシステム設定を行います。

(注) 必要に応じて、初期設定時に随时デバッグメニューに移動し、セットアップ問題のデバッグ、設定の中止、およびシステムの再起動を行うことができます。デバッグメニューに移動するには、Ctrl+C を押します。デバッグメニューを終了するには、Ctrl + D を2回押します。Ctrl+D を押す1回目と2回目の間に入力したものがある場合、2回目の Ctrl+D を押した後に実行されます。

例：

```
---- 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
```

■ コンソールポートを使用した初期設定

```
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#

```

管理ポートを使用したロータッチ プロビジョニング

Firepower 4100/9300 シャーシの起動時にスタートアップ コンフィギュレーションが見つからない場合、デバイスはロータッチプロビジョニングモードに入り、Dynamic Host Control Protocol (DHCP) サーバを検出して、その管理インターフェイス IP を使用して自身のブートストラップを実行します。その後、管理インターフェイスを介して接続して、SSH、HTTPS、または FXOS REST API を使用してシステムを設定できます。



(注)

初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

```

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

```

Firepower 4100/9300 シャーシの単一の管理ポートには、1つのみの IPv4 アドレス、ゲートウェイ、サブネットマスク、または1つのみの IPv6 アドレス、ゲートウェイ、ネットワークプレフィックスを指定する必要があります。管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネットマスク
- ゲートウェイ IP アドレス
- HTTPS および SSH アクセスを許可するサブネット（「IP ブロック」アドレスの入力を求められます）
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ1 DHCP サーバを設定して、Firepower 4100/9300 シャーシの管理ポートに IP アドレスを割り当てます。

Firepower 4100/9300 シャーシからの DHCP クライアント要求には、次のものが含まれます。

- 管理インターフェイスの MAC アドレス。
- DHCP オプション 60 (vendor-class-identifier) : 「FPR9300」または「FPR4100」に設定します。
- DHCP オプション 61 (dhcp-client-identifier) : Firepower 4100/9300 シャーシのシリアル番号に設定します。このシリアル番号は、シャーシの引き出しタブで確認できます。

ステップ2 Firepower 4100/9300 シャーシの電源を入れます。

シャーシの起動時にスタートアップコンフィギュレーションが見つからない場合、デバイスはロータッチ プロビジョニング モードに入ります。

ステップ3 HTTPS を使用してシステムを設定するには、次の手順を実行します。

- サポートされているブラウザを使用して、アドレスバーに次の URL を入力します。

https://<ip_address>/api

ここで、<ip_address> は、DHCP サーバによって割り当てられた Firepower 4100/9300 シャーシの管理ポートの IP アドレスです。

(注) サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください

(<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htm> を参照)。

- ユーザ名とパスワードの入力を求められたら、それぞれ **install** と <chassis_serial_number> を入力してログインします。

<chassis_serial_number> は、シャーシのタグを調べると確認できます。

- プロンプトに従ってシステム設定を行います。

- 強力なパスワードの適用ポリシー (強力なパスワードのガイドラインについては、[ユーザアカウント](#) を参照)。
- admin アカウントのパスワード。
- システム名
- スーパーバイザ管理の IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。

- SSH アクセスが許可されているホスト/ネットワーク アドレスおよびネットマスク/プレフィックス。
 - HTTPS アクセスが許可されるホスト/ネットワークアドレスとネットマスク/プレフィックス。
 - DNS サーバの IPv4 または IPv6 アドレス。
 - デフォルト ドメイン名。
- d) [送信 (Submit)] をクリックします。

ステップ4 SSH を使用してシステムを設定するには、次の手順を実行します。

- a) 次のコマンドを使用して、管理ポートに接続します。

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

ここで <ip_address> は、DHCP サーバによって割り当てられた Firepower 4100/9300 シャーシの管理ポートの IP アドレスです。

- b) パスワードの入力を求められたら、**Admin123** を入力してログインします。
 c) プロンプトに従ってシステム設定を行います。

(注) 必要に応じて、初期設定時に随时デバッグメニューに移動し、セットアップ問題のデバッグ、設定の中止、およびシステムの再起動を行うことができます。デバッグメニューに移動するには、Ctrl+C を押します。デバッグメニューを終了するには、Ctrl+D を 2 回押します。Ctrl+D を押す 1 回目と 2 回目の間に入力したものがある場合、2 回目の Ctrl+D を押した後に実行されます。

例：

```
---- 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
```

■ 管理ポートを使用したロータッチ プロビジョニング

```

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.

```

ステップ5 FXOS REST API を使用してシステムを設定するには、次の手順を実行します。

REST API を使用してシステムを設定するには、次の例を使用します。詳細については、<https://developer.cisco.com/site/ssp/firepower/>を参照してください。

(注) dns、domain_name、https_net、https_mask、ssh_net、ssh_mask の各属性はオプションです。REST API 設定の場合、他のすべての属性は必須です。

IPv4 REST API example:

```
{
  "fxosBootstrap": {
    "dns": "1.1.1.1",
    "domain_name": "cisco.com",
    "mgmt_gw": "192.168.0.1",
    "mgmt_ip": "192.168.0.100",
    "mgmt_ipmask": "255.255.255.0",
    "mgmt_net": "192.168.0.0",
    "mgmt_subnet": "255.255.255.0"
  }
}
```

```

        "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"
    }
}

```

Firepower Chassis Manager のログイン/ログアウト

Firepower Chassis Manager を使用して Firepower 4100/9300 シャーシを設定するには、その前に、有効なユーザ アカウントを使用してログオンする必要があります。ユーザ アカウントの詳細については、[User Management](#)を参照してください。

一定期間にわたって操作がない場合は、自動的にシステムからログアウトされます。デフォルトでは、10分間にわたり操作を行わないと自動的にログアウトします。このタイムアウト設定を変更するには、[セッションタイムアウトの設定](#)を参照してください。また、セッションがアクティブな場合でも、一定時間の経過後にユーザをシステムからログオフさせるように絶対タイムアウトを設定することもできます。絶対タイムアウトを設定するには、[絶対セッションタイムアウトの設定](#)を参照してください。

システムを変更した結果、Firepower Chassis Manager から自動的にログアウトされる場合の一覧については、[セッション変更により Firepower Chassis Manager セッションが閉じる場合](#)を参照してください。



(注) 指定した時間でユーザがシステムからロックアウトされる前に、ログイン試行の失敗を特定の数だけ許可するように Firepower Chassis Manager を任意で設定できます。詳細については、[ログイン試行の最大回数の設定](#)を参照してください。

手順

ステップ1 Firepower Chassis Manager にログインするには、次の手順を実行します。

- サポートされているブラウザを使用して、アドレスバーに次の URL を入力します。

https://<chassis_mgmt_ip_address>

ここで、<chassis_mgmt_ip_address> は、初期設定時に入力した Firepower 4100/9300 シャーシの IP アドレスまたはホスト名です。

(注) サポートされるブラウザの詳細については、使用しているバージョンのリリースノートを参照してください
(<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.htm> を参照)。

- ユーザ名とパスワードを入力します。

- [ログイン (Login)] をクリックします。

ログインすると Firepower Chassis Manager が開き、[概要 (Overview)] ページが表示されます。

ステップ2 Firepower Chassis Manager からログアウトするには、ナビゲーションバーに表示されている自分のユーザ名をポイントし、[ログアウト (Logout)] を選択します。

Firepower Chassis Manager からログアウトすると、ログイン画面に戻ります。

FXOS CLIへのアクセス

FXOS CLIには、コンソールポートに繋いだ端末を使って接続します。コンソールポートに接続しているコンピュータ端末（またはコンソールサーバ）でコンソールポートパラメータが次のとおりであることを確認します。

- 9600 ポー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

SSH と Telnet を使用しても FXOS CLI に接続できます。Firepower eXtensible Operating System は最大 8 つの SSH 接続を同時にサポートできます。SSH で接続するには、Firepower 4100/9300 シャーシのホスト名または IP アドレスが必要になります。

次のいずれかの構文例を使用して SSH、Telnet または Putty でログインします。



(注)

SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **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| UCMS-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 | UCMS-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 | UCMS-ipv6-address}**
`ssh ucs-ldap23\\jsmith@192.0.20.11`
`ssh ucs-ldap23\\jsmith@2001::1`

Linux 端末からは以下の Telnet を使用します。



(注)

Telnet はデフォルトでディセーブルです。Telnet を有効化する手順については、[Telnet の設定](#)を参照してください。

- **telnet ucs-UCSM-host-name ucs-auth-domain\\username**
`telnet ucs-qa-10`
`login: ucs-ldap23\blradmin`
- **telnet ucs-{UCSM-ip-address | UCMS-ipv6-address}ucs-auth-domain\\username**
`telnet 10.106.19.12 2052`
`ucs-qa-10-A login: ucs-ldap23\blradmin`

Putty クライアントから：

- **ucs-auth-domain\\username** でログインします。
`Login as: ucs-example\\jsmith`



(注)

デフォルトの認証がローカルに設定され、コンソール認証がLDAPに設定されている場合は、**ucs-local\admin** (adminはローカルアカウント名) を使用して Putty クライアントからファブリック インターコネクトにログインできます。