



## **Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 2.3(1) コンフィギュレーションガイド**

初版：2017年12月4日

最終更新：2018年9月27日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2018 Cisco Systems, Inc. All rights reserved.



## 目次

---

第 1 章	<b>Firepower セキュリティ アプライアンスの概要 1</b>
	Firepower セキュリティ アプライアンスについて 1
	Firepower Chassis Manager の概要 1
	シャーシステータスのモニタリング 2

---

第 2 章	<b>使用する前に 5</b>
	タスク フロー 5
	初期設定 6
	Firepower Chassis Manager のログイン/ログアウト 9
	FXOS CLIへのアクセス 10

---

第 3 章	<b>ASA のライセンス管理 13</b>
	スマート ソフトウェア ライセンスについて 13
	ASA のスマート ソフトウェア ライセンシング 14
	Smart Software Manager とアカウント 14
	オフライン管理 14
	パーマネント ライセンスの予約 14
	サテライト サーバ 15
	仮想アカウントごとに管理されるライセンスとデバイス 15
	評価ライセンス 15
	Smart Software Manager 通信 16
	デバイスの登録とトークン 16
	License Authority との定期通信 16
	非適合状態 16

Smart Call Home インフラストラクチャ	17
スマート ソフトウェア ライセンスの前提条件	17
スマート ソフトウェア ライセンスのガイドライン	18
スマート ソフトウェア ライセンスのデフォルト	18
通常スマート ソフトウェア ライセンシングの設定	18
(任意) HTTP プロキシの設定	18
(任意) Call Home URL の削除	19
Firepower セキュリティ アプライアンスの License Authority への登録	19
Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定	20
パーマネント ライセンス予約の設定	22
パーマネント ライセンスのインストール	22
(任意) パーマネント ライセンスの返却	23
スマート ソフトウェア ライセンスの履歴	24

## 第 4 章

**User Management 25**

ユーザ アカウント	25
ユーザ名に関するガイドライン	26
パスワードに関するガイドライン	27
リモート認証のガイドライン	28
ユーザ ロール	31
ローカル認証されたユーザのパスワード プロファイル	31
ユーザ設定	32
セッション タイムアウトの設定	35
絶対セッション タイムアウトの設定	36
ログイン試行の最大回数の設定	37
ユーザ ロックアウト ステータスの表示およびクリア	38
最小パスワード長チェックの設定	39
ローカル ユーザ アカウントの作成	40
ローカル ユーザ アカウントの削除	41
ローカル ユーザ アカウントのアクティブ化または非アクティブ化	42
ローカル認証されたユーザのパスワード履歴のクリア	42

## 第 5 章

## イメージ管理 45

イメージ管理について 45

Cisco.com からのイメージのダウンロード 46

Firepower セキュリティ アプライアンスへのイメージのアップロード 46

イメージの整合性の確認 47

Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード 47

論理デバイスのイメージバージョンの更新 48

Firmware アップグレード 50

## 第 6 章

## セキュリティ認定準拠 53

セキュリティ認定準拠 53

SSH ホスト キーの生成 54

IPSec セキュア チャネルの設定 55

トラストポイントのスタティック CRL の設定 60

証明書失効リストのチェックについて 61

CRL 定期ダウンロードの設定 66

LDAP キー リング証明書の設定 68

クライアント証明書認証の有効化 69

## 第 7 章

## システム管理 71

セッション変更により Firepower Chassis Manager セッションが閉じる場合 71

管理 IP アドレスの変更 72

アプリケーション管理 IP の変更 74

Firepower 4100/9300 シャーシ名の変更 77

ログイン前バナー 78

ログイン前バナーの作成 78

ログイン前バナーの変更 79

ログイン前バナーの削除 80

Firepower 4100/9300 シャーシの再起動 81

Firepower 4100/9300 シャーシの電源オフ 81

工場出荷時のデフォルト設定の復元 81

トラスト ID 証明書のインストール 82

---

第 8 章

**Platform Settings 89**

NTP サーバ認証の有効化 89

日時の設定 90

設定された日付と時刻の表示 91

タイムゾーンの設定 91

NTP を使用した日付と時刻の設定 91

NTP サーバの削除 92

手動での日付と時刻の設定 92

SSH の設定 93

TLS の設定 94

Telnet の設定 96

SNMP の設定 97

SNMP の概要 97

SNMP 通知 98

SNMP セキュリティ レベルおよび権限 98

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ 99

SNMPv3 セキュリティ機能 99

SNMP サポート 100

SNMP のイネーブル化および SNMP プロパティの設定 100

SNMP トラップの作成 101

SNMP トラップの削除 103

SNMPv3 ユーザの作成 103

SNMPv3 ユーザの削除 105

HTTPS の設定 106

証明書、キーリング、トラストポイント 106

キーリングの作成 107

デフォルト キーリングの再生成 108

キーリングの証明書要求の作成 108

基本オプション付きのキーリングの証明書要求の作成	108
詳細オプション付きのキーリングの証明書要求の作成	110
トラストポイントの作成	112
キーリングへの証明書のインポート	113
HTTPS の設定	114
HTTPS ポートの変更	116
キーリングの削除	116
トラストポイントの削除	117
HTTPS の無効化	118
AAA の設定	118
AAA について	118
LDAP プロバイダーの設定	120
LDAP プロバイダーのプロパティの設定	120
LDAP プロバイダーの作成	121
LDAP プロバイダーの削除	124
RADIUS プロバイダーの設定	124
RADIUS プロバイダーのプロパティの設定	124
RADIUS プロバイダーの作成	125
RADIUS プロバイダーの削除	126
TACACS+ プロバイダーの設定	126
TACACS+ プロバイダーのプロパティの設定	126
TACACS+ プロバイダーの作成	127
TACACS+ プロバイダーの削除	128
Syslog の設定	128
DNS サーバの設定	131
FIPS モードの有効化	132
コモンクライテリアモードの有効化	133
IP アクセスリストの設定	133

## 第 9 章

インターフェイス管理	135
Firepower インターフェイスについて	135

シャーシ管理インターフェイス	135
インターフェイス タイプ	136
ハードウェア バイパス ペア	136
ジャンボ フレーム サポート	137
Firepower Threat Defense のインラインセット リンク ステートの伝達	138
Firepower インターフェイスに関する注意事項と制約事項	138
インターフェイスの設定	139
インターフェイスの有効化または無効化	139
物理インターフェイスの設定	140
EtherChannel (ポート チャンネル) の追加	140
ブレイクアウト ケーブルの設定	142
モニタリング インターフェイス	143
インターフェイスの履歴	144

## 第 10 章

## 論理デバイス 147

論理デバイスについて	147
スタンドアロン論理デバイスとクラスタ化論理デバイス	148
論理デバイスの要件と前提条件	148
クラスタリングの要件と前提条件	148
論理デバイスに関する注意事項と制約事項	150
一般的なガイドラインと制限事項	150
クラスタリング ガイドラインと制限事項	151
スタンドアロン論理デバイスの追加	156
スタンドアロン ASA の追加	156
スタンドアロン Firepower Threat Defense の追加	158
ハイ アベイラビリティ ペアの追加	160
クラスタの追加	161
Firepower 4100/9300 シャーシでのクラスタリングについて	161
標準出荷単位とセカンダリ単位の役割	162
クラスタ制御リンク	162
管理ネットワーク	164

管理インターフェイス	164
スパンド EtherChannel	165
サイト間クラスタリング	166
ASA クラスタの追加	167
ASA クラスタの作成	167
クラスタ メンバの追加	170
Firepower Threat Defense Cluster の追加	171
Firepower Threat Defense クラスタの作成	172
クラスタ メンバの追加	176
Radware DefensePro の設定	177
Radware DefensePro について	177
Radware DefensePro の前提条件	178
サービス チェーンのガイドライン	178
スタンドアロンの論理デバイスでの Radware DefensePro の設定	179
シャーシ内クラスタの Radware DefensePro の設定	180
UDP/TCP ポートのオープンと vDP Web サービスの有効化	182
論理デバイスの管理	183
アプリケーションのコンソールへの接続	183
論理デバイスの削除	185
論理デバイスに関連付けられていないアプリケーションインスタンスの削除	185
ASA のトランスペアレント ファイアウォール モードへの変更	185
Firepower Threat Defense 論理デバイスのインターフェイスの変更	187
ASA 論理デバイスのインターフェイスの変更	188
論理デバイスのブートストラップ設定の変更または回復	190
[Logical Devices] ページ	190
サイト間クラスタリングの例	193
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例	193
スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例	194
論理デバイスの履歴	196

FXOS セキュリティ モジュール/セキュリティ エンジンについて	199
セキュリティ モジュールの使用停止/再稼働	201
セキュリティ モジュール/エンジンの確認応答	202
セキュリティ モジュール/エンジンのリセット	202
セキュリティ モジュール/エンジンの再初期化	203
ネットワーク モジュールのオフラインまたはオンラインの切り替え	204
インストールされているモジュール/エンジンの電源オン/オフ	205

## 第 12 章

コンフィギュレーションのインポート/エクスポート	207
コンフィギュレーションのインポート/エクスポートについて	207
FXOS コンフィギュレーション ファイルのエクスポート	208
自動設定エクスポートのスケジューリング	209
設定エクスポート リマインダの設定	210
コンフィギュレーション ファイルのインポート	211

## 第 13 章

トラブルシューティング	213
パケット キャプチャ	213
バックプレーン ポート マッピング	213
パケット キャプチャの注意事項および制限事項	214
パケット キャプチャ セッションの作成または編集	214
パケット キャプチャのためのフィルタの設定	216
パケット キャプチャ セッションの開始または停止	217
パケット キャプチャ ファイルのダウンロード	218
パケット キャプチャ セッションの削除	218
ネットワーク接続のテスト	219
ポート チャネル ステータスの確認	221
ソフトウェア障害からの回復	223
破損ファイル システムの回復	228
Firepower Threat Defense のクラスター メンバのディザスタ リカバリ	238



# 第 1 章

## Firepower セキュリティ アプライアンスの概要

- [Firepower セキュリティ アプライアンスについて \(1 ページ\)](#)
- [Firepower Chassis Manager の概要 \(1 ページ\)](#)
- [シャーシ ステータスのモニタリング \(2 ページ\)](#)

## Firepower セキュリティ アプライアンスについて

Cisco Firepower 4100/9300 シャーシは、ネットワークおよびコンテンツセキュリティソリューションの次世代プラットフォームです。Firepower 4100/9300 シャーシはシスコアプリケーションセントリック インフラストラクチャ (ACI) セキュリティソリューションの一部であり、拡張性、一貫性のある制御、シンプルな管理を実現するために構築された、俊敏でオープン、かつセキュアなプラットフォームを提供します。

Firepower 4100/9300 シャーシ は次の機能を提供します。

- モジュラ シャーシ ベースのセキュリティ システム：高性能で柔軟な入出力構成と、優れた拡張性が提供されます。
- Firepower Chassis Manager：グラフィカルユーザインターフェイスによって、現在のシャーシ ステータスが効率良く視覚的に表示され、シャーシの機能は簡単に設定できます。
- FXOS CLI：機能の設定、シャーシ ステータスのモニタリング、および高度なトラブルシューティング機能へのアクセスを行うコマンドベースのインターフェイスを提供します。
- FXOS REST API：ユーザがシャーシをプログラムを使用して設定し、管理できます。

## Firepower Chassis Manager の概要

Firepower eXtensible Operating System は、プラットフォーム設定やインターフェイスの構成、デバイスのプロビジョニング、およびシステム ステータスのモニタリングを簡単にする Web

インターフェイスを提供します。ユーザ インターフェイスの上部にあるナビゲーションバーを使用して以下にアクセスできます。

- **Overview** : [Overview] ページから Firepower シャーシのステータスを簡単にモニタできます。詳細については、[シャーシステータスのモニタリング \(2 ページ\)](#) を参照してください。
- **Interfaces** : [Interfaces] ページから、シャーシにインストールされたインターフェイスのステータスの表示、インターフェイスプロパティの編集、インターフェイスの有効化とディセーブル化、ポートチャンネルの作成が可能です。詳細については、[インターフェイス管理 \(135 ページ\)](#) を参照してください。
- **Logical Devices** : [Logical Devices] ページから、論理デバイスを作成、編集、削除できます。既存の論理デバイスの現在のステータスを表示することもできます。詳細については、[論理デバイス \(147 ページ\)](#) を参照してください。
- **セキュリティモジュール/セキュリティエンジン** : [セキュリティモジュール/セキュリティエンジン (Security Modules/Security Engine) ] ページから、セキュリティモジュール/エンジンのステータスを表示し、電源の再投入、再初期化、確認応答、解放などのさまざまな機能を実行できます。詳細については、[セキュリティモジュール/エンジン管理 \(199 ページ\)](#) を参照してください。
- **Platform Settings** : [Platform Settings] ページから、シャーシの設定（日時、SSH、SNMP、HTTPS、AAA、Syslog、DNS）を行えます。詳細については、[Platform Settings \(89 ページ\)](#) を参照してください。
- **System Settings** : [System] メニューで次の設定を管理できます。
  - **Licensing** : [Licensing] ページから、Smart Call Home の設定、Firepower シャーシの Licensing Authority への登録が可能です。詳細については、[ASA のライセンス管理 \(13 ページ\)](#) を参照してください。
  - **Updates** : [Updates] ページから、プラットフォーム バンドルおよびアプリケーション イメージを Firepower シャーシにアップロードできます。詳細については、[イメージ管理 \(45 ページ\)](#) を参照してください。
  - **ユーザ管理** : [ユーザ管理 (User Management) ] ページでは、ユーザ設定を行ったり、Firepower 4100/9300 シャーシのユーザアカウントを定義したりできます。詳細については、[User Management \(25 ページ\)](#) を参照してください。

## シャーシステータスのモニタリング

[Overview] ページから、Firepower 4100/9300 シャーシのステータスを簡単にモニタできます。[Overview] ページには次の要素が表示されます。

- **[Device Information]** : [Overview] ページの上部には、Firepower 4100/9300 シャーシについての次の情報が表示されます。

- [Chassis name] : 初期設定時にシャーシに割り当てられた名前を表示します。
- [IP address] : 初期設定時にシャーシに割り当てられた IP アドレスを表示します。
- [Model] : Firepower 4100/9300 シャーシ のモデルを表示します。
- [Version] : シャーシ上で実行されている FXOS のバージョンを示します。
- [Operational State] : シャーシの動作可能ステータスを示します。
- [Chassis uptime] : システムが最後に再起動されてからの経過時間を表示します。
- [Shutdown] ボタン : Firepower 4100/9300 シャーシをグレースフルシャットダウンします ([Firepower 4100/9300 シャーシの電源オフ \(81 ページ\)](#) を参照)。



---

(注) [Security Modules/Security Engine] ページからセキュリティ モジュール/エンジンの電源をオン/オフできます ([インストールされているモジュール/エンジンの電源オン/オフ \(205 ページ\)](#) を参照)。

---

- [Reboot] ボタン : Firepower 4100/9300 シャーシをグレースフルシャットダウンします ([Firepower 4100/9300 シャーシの再起動 \(81 ページ\)](#) を参照)。



---

(注) [Security Modules/Security Engine] ページからセキュリティ モジュール/エンジンの電源をリセットできます ([セキュリティ モジュール/エンジンのリセット \(202 ページ\)](#) を参照)。

---

- [Uptime Information] アイコン : アイコンにカーソルを合わせると、シャーシおよびインストールされているセキュリティ モジュール/エンジンの稼働時間を表示します。
- [Visual Status Display] : [Device Information] セクションの下にはシャーシが視覚的に表示されて、搭載されているコンポーネントとそれらの全般ステータスを示します。[Visual Status Display] に表示されるポートにカーソルを合わせると、インターフェイス名、速度、タイプ、管理状態、動作状態などの追加情報が表示されます。複数のセキュリティモジュール搭載モデルでは、[Visual Status Display] に表示されるポートにカーソルを合わせると、デバイス名、テンプレートタイプ、管理状態、動作状態などの追加情報が表示されます。当該セキュリティモジュールに論理デバイスがインストールされている場合は、管理 IP アドレス、ソフトウェアバージョン、論理デバイス モードも表示されます。
- [Detailed Status Information] : [Visual Status Display] の下に表示されるテーブルで、シャーシの詳細なステータス情報を含みます。ステータス情報は、[Faults]、[Interfaces]、[Devices]、[License]、[Inventory] の 5 つのセクションに分かれています。これらの各セクションの概要をテーブルの上に表示できます。さらに確認する情報の概要エリアをクリックするとそれぞれの詳細を表示できます。

システムは、シャーシに関する次の詳細なステータス情報を表示します。

- **[Faults]** : システムで発生した障害をリスト表示します。障害は **[Critical]**、**[Major]**、**[Minor]**、**[Warning]**、**[Info]** という重大度でソートされます。リストされた各障害について、重大度、障害の説明、原因、発生回数、最後の発生日時を確認できます。障害が確認済みかどうかもわかります。

いずれかの障害をクリックして、詳細を表示したり、その障害を確認済みにしたりすることができます。



(注) 障害の根本原因が解消されると、その障害は次のポーリング間隔中にリストから自動的にクリアされます。特定の障害に対処する場合、現在処理中であることが他のユーザにわかるように、その障害を確認済みにすることができます。

- **[Interfaces]** : システムにインストールされているインターフェイスが表示されます。**[All Interfaces]** タブにインターフェイス名、動作状態、管理状態、受信したバイト数、送信したバイト数が表示されます。**[ハードウェア バイパス]** タブには、FTD アプリケーションのハードウェア バイパス機能でサポートされるインターフェイス ペアだけが表示されます。各ペアについて、動作状態が表示されます (**disabled** : このペアでハードウェア バイパスは構成されていない、**standby** : ハードウェア バイパスは構成されているが、現在アクティブではない、**bypass** : ハードウェア バイパスでアクティブ)。
- **[Devices & Network]** : システムに設定されている論理デバイスを表示し、各論理デバイスに次の詳細情報を提供します。デバイス名、ステータス、イメージバージョン、管理 IP アドレス。
- **[License]** : (ASA 論理デバイスの場合) スマートライセンスが有効化になっているかどうかを表示し、Firepower ライセンスの現在の登録ステータスおよびシャーシのライセンス認可情報を示します。
- **[Inventory]** : シャーシに搭載されているコンポーネントをリスト表示し、それらのコンポーネントの関連情報 (コンポーネント名、コアの数、設置場所、動作ステータス、運用性、キャパシティ、電源、温度、シリアル番号、モデル番号、製品番号、ベンダー) を示します。



## 第 2 章

### 使用する前に

---

- [タスク フロー \(5 ページ\)](#)
- [初期設定 \(6 ページ\)](#)
- [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、Firepower 4100/9300 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 \(6 ページ\)](#) 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 \(90 ページ\)](#) 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 \(131 ページ\)](#) 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 \(13 ページ\)](#) を参照)。
  - ステップ 7 ユーザを設定します ([User Management \(25 ページ\)](#) 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 \(45 ページ\)](#) 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 ([Platform Settings \(89 ページ\)](#) 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 \(135 ページ\)](#) 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 \(147 ページ\)](#) 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、まず、コンソールポートを介してアクセスした FXOS CLI を使用して初期設定タスクを実行する必要があります。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。

システム設定を既存のバックアップファイルから復元するか、セットアップ ウィザードを実行してシステムを手動でセットアップするか、選択できます。システムを復元する場合は、バックアップファイルが、管理ネットワークから到達可能な場所に存在する必要があります。

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

## 手順

---

**ステップ 1** コンソールポートに接続します。

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

Firepower 4100/9300 シャーシが起動すると、電源投入時セルフテストメッセージが表示されます。

**ステップ3** 未設定のシステムが起動すると、セットアップウィザードでシステム設定に必要な次の情報の入力を求められます。

- セットアップ モード（フルシステムバックアップからの復元または初期セットアップ）
- 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、[ユーザーアカウント（25 ページ）](#) を参照）
- admin パスワード
- システム名
- 管理ポートの 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
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- SSH アクセス用 IP ブロック アドレス
- SSH アクセス用 IPv4 または IPv6 ブロック ネットマスク
- HTTPS アクセス用 IP ブロック アドレス
- HTTPS アクセス用 IPv4 または IPv6 ブロック ネットマスク
- DNS サーバの IPv4 または IPv6 アドレス
- デフォルトのドメイン名

**ステップ4** 設定の要約を確認し、設定を保存および適用する場合は **yes** を入力し、セットアップウィザードをやり直して設定を変更する場合は **no** を入力します。

セットアップウィザードのやり直しを選択した場合は、以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

## 例

次の例では、IPv4 管理アドレスを使用して設定します。

```
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? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv4 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv4 block netmask: 0.0.0.0
Configure the DNS Server IP address (yes/no) [n]:y
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: y
```

```

Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Enforce Strong Password=no
Physical Switch Mgmt0 IP Address=192.168.10.10
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
IPv6 value=0
SSH Access Configured=yes
  SSH IP Address=0.0.0.0
  SSH IP Netmask=0.0.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=0.0.0.0
  HTTPS IP Netmask=0.0.0.0
DNS Server=20.10.20.10
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

次の例では、IPv6 管理アドレスを使用して設定します。

```

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? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address : 2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv6 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv6 block netmask: 0.0.0.0
Configure the DNS Server IPv6 address? (yes/no) [n]: y
  DNS IP address: 2001::101
Configure the DNS Server IP address (yes/no) [n]:
Configure the default domain name? (yes/no) [n]: y
  Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Enforced Strong Password=no
Physical Switch Mgmt0 IPv6 Address=2001::107
Physical Switch Mgmt0 IPv6 Prefix=64
Default Gateway=2001::1
Ipv6 value=1
SSH Access Configured=yes
  SSH IP Address=0.0.0.0
  SSH IP Netmask=0.0.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=0.0.0.0
  HTTPS IP Netmask=0.0.0.0
DNS Server=2001::101
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

# 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 \(25 ページ\)](#) 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 \(35 ページ\)](#) 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 \(36 ページ\)](#) 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 \(71 ページ\)](#) 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 \(37 ページ\)](#) 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。

- a) 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 <http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list> を参照してください。

- b) ユーザ名とパスワードを入力します。  
c) [Login] をクリックします。

ログインすると Firepower Chassis Manager が開き、[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、[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 ボー
- 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* | *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
```

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 \(96 ページ\)](#) 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\bladmin
```

- **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\bladmin
```

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 インターコネクタにログインできます。

---





## 第 3 章

# ASA のライセンス管理

シスコスマートソフトウェアライセンスによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。各ユニットのライセンスキーを管理しなくても、簡単にデバイスを導入したり導入を終了したりできます。スマートソフトウェアライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。



(注) このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

- [スマートソフトウェアライセンスについて \(13 ページ\)](#)
- [スマートソフトウェアライセンスの前提条件 \(17 ページ\)](#)
- [スマートソフトウェアライセンスのガイドライン \(18 ページ\)](#)
- [スマートソフトウェアライセンスのデフォルト \(18 ページ\)](#)
- [通常スマートソフトウェアライセンシングの設定 \(18 ページ\)](#)
- [Firepower 4100/9300 シャーシのスマートライセンス サテライト サーバの設定 \(20 ページ\)](#)
- [パーマネントライセンス予約の設定 \(22 ページ\)](#)
- [スマートソフトウェアライセンスの履歴 \(24 ページ\)](#)

## スマートソフトウェアライセンスについて

ここでは、スマートソフトウェアライセンスの仕組みについて説明します。



(注) このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

## ASA のスマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ上の ASA アプリケーションの場合、スマート ソフトウェア ライセンス設定は Firepower 4100/9300 シャーシ スーパーバイザとアプリケーションの間で分割されます。

- Firepower 4100/9300 シャーシ：ライセンス認証局との通信を行うためのパラメータを含めて、スーパーバイザにすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。



(注) シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：アプリケーションのすべてのライセンスの権限付与を設定します。

## Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

<https://software.cisco.com/#module/SmartLicensing>

Smart Software Manager では、組織のマスター アカウントを作成できます。



(注) まだアカウントをお持ちでない場合は、リンクをクリックして**新しいアカウントを設定**してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトで、ライセンスはマスターアカウントの下のデフォルト仮想アカウントに割り当てられます。アカウント管理者であれば、任意で追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社のアカウントを作成できます。複数の仮想アカウントを使用すると、大量のライセンスおよびデバイスをより簡単に管理できます。

## オフライン管理

デバイスにインターネットアクセスがなく、License Authority に登録できない場合は、オフラインライセンスを設定できます。

## パーマネント ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、License Authority への定期的なアクセスは必要ありません。PAK ライセンスのように、ライセンスを購入し、ASA のライ

センス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

すべての機能、すなわちモデルの正しい最大スループットを備えた標準ティアおよびキャリア ライセンスを有効にするライセンスを取得できます。ライセンスは Firepower 4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

## サテライト サーバ

デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン (VM) としてローカル Smart Software Manager サテライトサーバをインストールできます。サテライト (衛星) は、Smart Software Manager 機能のサブセットを提供し、これによりすべてのローカル デバイスに重要なライセンス サービスが提供可能になります。ライセンス使用を同期するために、定期的に衛星だけが License Authority と同期する必要があります。スケジュールに沿って同期するか、または手動で同期できます。

サテライトアプリケーションをダウンロードして導入したら、インターネットを使用して Cisco SSM にデータを送信しなくても、以下の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、[Smart Account Manager satellite](#)にあるスマート ソフトウェア マネージャ サテライトのインストール ガイドおよびコンフィギュレーション ガイドを参照してください。

## 仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。アカウントに割り当てられたライセンスを使用できるのは、その仮想アカウントのデバイスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシのみがデバイスとして登録され、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3つのセキュリティモジュールを搭載した Firepower 9300 シャーシでは、全シャーシが1つのデバイスとして登録されますが、各モジュールは合計3つのライセンスを別個に使用します。

## 評価ライセンス

Firepower 4100/9300 シャーシは、次の2種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード : Firepower 4100/9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間 (合計使用期間) 動作します。このモードでは、ASA

は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。

- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシが Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。



(注) 高度暗号化 (3DES/AES) の評価ライセンスは取得できません。永続ライセンスのみがこの権限をサポートします。

## Smart Software Manager 通信

このセクションでは、デバイスの Smart Software Manager に対する通信方法について説明します。

### デバイスの登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各シャーシを導入するとき、または既存のシャーシを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

導入した後、または既存のシャーシでこれらのパラメータを手動で設定した後、そのシャーシを起動するとシスコのライセンス認証局に登録されます。シャーシがトークンで登録される時、ライセンス認証局はシャーシとそのライセンス認証局との間で通信を行うために ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

### License Authority との定期通信

デバイスは 30 日ごとに License Authority と通信します。Smart Software Manager に変更を行う場合、デバイスの認証を更新して変更をすぐに反映させることができます。またはスケジューリング設定されたデバイスの通信を待つこともできます。

必要に応じて、HTTP プロキシを設定できます。

Firepower 4100/9300 シャーシでは、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネット アクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

### 非適合状態

デバイスは、次の状況においてコンプライアンス違反になる可能性があります。

- 使用率超過：デバイスが使用不可のライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、Firepower4100/9300 シャーシで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反の場合、特別なライセンスが必要な機能への設定変更はできなくなりますが、その他の動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

## Smart Call Home インフラストラクチャ

デフォルトで、Smart Call Home のプロファイルは、ライセンス認証局の URL を指定する FXOS 設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの唯一の設定可能なオプションが License Authority の宛先アドレス URL であることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

# スマート ソフトウェア ライセンスの前提条件

- この章は、Firepower4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。
- Cisco Smart Software Manager でマスター アカウントを作成します。  
<https://software.cisco.com/#module/SmartLicensing>  
まだアカウントをお持ちでない場合は、このリンクをクリックして[新しいアカウントをセットアップ](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- [Cisco Commerce Workspace](#) から 1 つ以上のライセンスを購入します。ホームページの [Find Products and Solutions] フィールドで、該当するプラットフォームを検索します。一部のライセンスは無料ですが、スマート ソフトウェア ライセンス アカウントにそれらを追加する必要があります。
- シャーシがライセンス機関と通信できるように、シャーシからのインターネットアクセスまたは HTTP プロキシアクセスを確保します。
- シャーシがライセンス機関の名前を解決できるように、DNS サーバを設定します。
- シャーシのための時間を設定します。
- ASA ライセンス資格を設定する前に、Firepower4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

# スマートソフトウェアライセンスのガイドライン

## フェイルオーバークラスタリングのための ASA ガイドライン

各 Firepower 4100/9300 シャーシは、License Authority またはサテライト サーバに登録される必要があります。セカンダリ ユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。

# スマートソフトウェアライセンスのデフォルト

Firepower 4100/9300 シャーシのデフォルト設定には、ライセンス認証局の URL を指定する「SLProf」という Smart Call Home のプロファイルが含まれています。

# 通常スマートソフトウェアライセンシングの設定

Cisco License Authority と通信するため、必要に応じて HTTP プロキシを設定できます。License Authority に登録するには、スマートソフトウェアライセンスアカウントから取得した Firepower 4100/9300 シャーシの登録トークン ID を入力する必要があります。

## 手順

- 
- ステップ 1 (任意) [HTTP プロキシの設定 \(18 ページ\)](#)。
  - ステップ 2 [Firepower セキュリティアプライアンスの License Authority への登録 \(19 ページ\)](#)。
- 

## (任意) HTTP プロキシの設定

ネットワークでインターネットアクセスに HTTP プロキシを使用する場合、スマートソフトウェアライセンスのプロキシアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。



---

(注) 認証を使用する HTTP プロキシはサポートされません。

---

## 手順

- 
- ステップ 1 `[System] > [Licensing] > [Call Home]` を選択します。

[Call Home] ページには、License Authority の宛先アドレス URL を設定するフィールド、および HTTP プロキシを設定するフィールドが表示されます。

(注) Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

- ステップ 2 [Server Enable] ドロップダウン リストで [on] を選択します。
- ステップ 3 [Server URL] および [Server Port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバのポート 443 を入力します。
- ステップ 4 [Save] をクリックします。

## (任意) Call Home URL の削除

以前に設定された Call Home URL を削除するには、次の手順を実行します。

### 手順

- ステップ 1 [System] > [Licensing] > [Call Home] を選択します。
- ステップ 2 [Call home Configuration] 領域で、[Delete] を選択します。

## Firepower セキュリティ アプライアンスの License Authority への登録

Firepower 4100/9300 シャーシを登録すると、ライセンス認証局によって Firepower 4100/9300 シャーシとライセンス認証局との間の通信に使用される ID 証明書が発行されます。また、Firepower 4100/9300 シャーシが該当する仮想アカウントに割り当てられます。通常、この手順は 1 回で済みます。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、Firepower 4100/9300 シャーシの再登録が必要になります。

### 手順

- ステップ 1 Smart Software Manager または Smart Software Manager Satellite で、この Firepower 4100/9300 シャーシの追加先となるバーチャルアカウントの登録トークンを要求してコピーします。  
スマートソフトウェアマネージャサテライトを使用して登録トークンを要求する方法について詳しくは、『Cisco Smart Software Manager Satellite User Guide』（[http://www.cisco.com/web/software/286285517/138897/Smart\\_Software\\_Manager\\_satellite\\_4.1.0\\_User\\_Guide.pdf](http://www.cisco.com/web/software/286285517/138897/Smart_Software_Manager_satellite_4.1.0_User_Guide.pdf)）を参照してください。
- ステップ 2 Firepower Chassis Manager で、[System] > [Licensing] > [Smart License] の順に選択します。
- ステップ 3 [Enter Product Instance Registration Token] フィールドに登録トークンを入力します。
- ステップ 4 [Register] をクリックします。

Firepower 4100/9300 シャーシがライセンス認証局への登録を試行します。

デバイスの登録を解除するには、[Unregister] をクリックします。

Firepower 4100/9300 シャーシの登録を解除すると、アカウントからデバイスが削除されます。デバイスのすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい Firepower 4100/9300 シャーシに利用することもできます。あるいは、Smart Software Manager からデバイスを削除できます。

---

## Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定

スマート ライセンス サテライト サーバを使用するように Firepower 4100/9300 シャーシを設定するには、次の手順に従います。

### 始める前に

- [スマート ソフトウェア ライセンスの前提条件 \(17 ページ\)](#) に記載のすべての前提条件を満たす必要があります。
- [スマート ライセンス サテライト OVA ファイルを Cisco.com からダウンロードし、VMwareESXi サーバにインストールおよび設定します。](#) 詳細については、『[Smart Software Manager satellite Install Guide](#)』を参照してください。
- 証明書チェーンがまだない場合、次の手順を使用してそれを要求します。
  - キー リングを作成します ([キー リングの作成 \(107 ページ\)](#)) 。
  - そのキー リングの証明書要求を作成します ([基本オプション付きのキー リングの証明書要求の作成 \(108 ページ\)](#)) 。
  - キーリングの証明書チェーンを取得するために、この証明書要求をトラストアンカーまたは認証局に送信します。

詳細については、[証明書、キーリング、トラストポイント \(106 ページ\)](#) を参照してください。

### 手順

---

**ステップ 1** [System] > [Licensing] > [Call Home] を選択します。

**ステップ 2** [Call home Configuration] 領域で、[Address] フィールドのデフォルト URL を、サテライト URL [https://ip\\_address/Transportgateway/services/DeviceRequestHandler](https://ip_address/Transportgateway/services/DeviceRequestHandler) に置き換えます。

**ステップ 3** 新しいトラストポイントを作成します。新しいトラストポイントを作成するには、FXOS CLI を使用する必要があります。



# パーマネントライセンス予約の設定

Firepower 4100/9300 シャーシにパーマネントライセンスを割り当てることができます。このユニバーサル予約では、デバイスで無制限の数の使用権を使用できるようになります。



- (注) Smart Software Manager で使用できるように、開始前にパーマネントライセンスを購入する必要があります。すべてのアカウントがパーマネントライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

## パーマネントライセンスのインストール

以下の手順は、Firepower 4100/9300 シャーシにパーマネント（永続）ライセンスを割り当てる方法を示しています。

### 手順

- ステップ 1 **System > Licensing > Permanent License** を選択します。
- ステップ 2 **Generate** をクリックして、予約要求コードを生成します。予約要求コードをクリップボードにコピーします。
- ステップ 3 Cisco Smart Software Manager ポータルの [Smart Software Manager] インベントリ画面に移動して、**Licenses** タブをクリックします。  
<https://software.cisco.com/#SmartLicensing-Inventory>  
**Licenses** タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。
- ステップ 4 **License Reservation** をクリックして、生成された予約リクエストコードをボックスにペーストします。
- ステップ 5 **Reserve License** をクリックします。  
Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。  
**License Reservation** ボタンが表示されない場合、お使いのアカウントにはパーマネントライセンスの予約が許可されていません。この場合、パーマネントライセンスの予約を無効にして標準のスマートライセンス コマンドを再入力する必要があります。
- ステップ 6 Firepower Chassis Manager で、生成された承認コードを **Authorization Code** テキストボックスに入力します。
- ステップ 7 **Install** をクリックします。

Firepower 4100/9300 シャーシが PLR で完全にライセンス付与されたら、[Permanenet License] ページにライセンス ステータスが表示され、パーマネント ライセンスを返却するためのオプションが示されます。

- ステップ 8** ASA 論理デバイスで機能のライセンス資格を有効にします。ライセンス資格を有効にするには、[ASA ライセンス](#)の章を参照してください。

## (任意) パーマネント ライセンスの返却

パーマネント ライセンスが不要になった場合、この手順で Smart Software Manager に正式に返却する必要があります。すべてのステップに従わないと、ライセンスが使用状態のままになり、別の場所で使用できません。

### 手順

- ステップ 1** **System > Licensing > Permanent License** を選択します。
- ステップ 2** **Return** をクリックして、戻りコードを生成します。戻りコードをクリップボードにコピーします。
- ただちに Firepower 4100/9300 シャーシ のライセンスがなくなり、評価状態に移行します。
- ステップ 3** Smart Software Manager インベントリ画面に移動して、**Product Instances** タブをクリックします。
- <https://software.cisco.com/#SmartLicensing-Inventory>
- ステップ 4** ユニバーサルデバイス識別子 (UDI) を使用して Firepower 4100/9300 シャーシを検索します。
- ステップ 5** **Actions > Remove** の順に選択して、生成された戻りコードをボックスに貼り付けます。
- ステップ 6** **Remove Product Instance** をクリックします。
- パーマネント ライセンスが使用可能なライセンスのプールに戻されます。
- ステップ 7** システムをリブートします。Firepower 4100/9300 シャーシの再起動の方法については、[Firepower 4100/9300 シャーシの再起動 \(81 ページ\)](#) を参照してください。

## スマートソフトウェアライセンスの履歴

機能名	プラットフォーム リリース	説明
Firepower 4100/9300 シャーシ向けシステムスマートソフトウェアライセンスング	1.1(1)	<p>スマートソフトウェアライセンスによって、ライセンスを購入し、ライセンスのプールを管理することができます。スマートライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単にデバイスを導入したり導入を終了したりできます。スマートソフトウェアライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。スマートソフトウェアライセンスの設定は、Firepower 4100/9300 シャーシスーパーバイザとセキュリティモジュール間で分割されます。</p> <p>次の画面が導入されました。</p> <p><b>[System] &gt; [Licensing] &gt; [Call Home]</b>  <b>[System] &gt; [Licensing] &gt; [Smart License]</b></p>



## 第 4 章

# User Management

- ユーザアカウント (25 ページ)
- ユーザ名に関するガイドライン (26 ページ)
- パスワードに関するガイドライン (27 ページ)
- リモート認証のガイドライン (28 ページ)
- ユーザロール (31 ページ)
- ローカル認証されたユーザのパスワードプロファイル (31 ページ)
- ユーザ設定 (32 ページ)
- セッションタイムアウトの設定 (35 ページ)
- 絶対セッションタイムアウトの設定 (36 ページ)
- ログイン試行の最大回数の設定 (37 ページ)
- ユーザロックアウトステータスの表示およびクリア (38 ページ)
- 最小パスワード長チェックの設定 (39 ページ)
- ローカルユーザアカウントの作成 (40 ページ)
- ローカルユーザアカウントの削除 (41 ページ)
- ローカルユーザアカウントのアクティブ化または非アクティブ化 (42 ページ)
- ローカル認証されたユーザのパスワード履歴のクリア (42 ページ)

## ユーザアカウント

ユーザアカウントは、システムにアクセスするために使用されます。最大 48 のローカルユーザアカウントを設定できます。各ユーザアカウントには、一意のユーザ名とパスワードが必要です。

### 管理者アカウント

管理者アカウントはデフォルトユーザアカウントであり、変更や削除はできません。このアカウントは、システム管理者またはスーパーユーザアカウントであり、すべての権限が与えられています。admin アカウントには、デフォルトのパスワードは割り当てられません。初期システムセットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定できません。

### ローカル認証されたユーザアカウント

ローカル認証されたユーザアカウントは、シャージによって直接認証され、admin 権限か AAA 権限を持つユーザが有効または無効にできます。ローカルユーザアカウントを無効にすると、ユーザはログインできません。データベースは無効化されたローカルユーザアカウントの設定の詳細を削除しません。無効ローカルユーザアカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存の設定で再びアクティブになります。

### リモート認証されたユーザアカウント

リモート認証されたユーザアカウントとは、LDAP、RADIUS、または TACACS+ で認証されたユーザアカウントです。

ユーザがローカルユーザアカウントとリモートユーザアカウントを同時に保持する場合、ローカルユーザアカウントで定義されたロールがリモートユーザアカウントに保持された値を上書きします。

リモート認証のガイドラインの詳細や、リモート認証プロバイダーの設定および削除方法については、次のトピックを参照してください。

- [リモート認証のガイドライン](#) (28 ページ)
- [LDAP プロバイダーの設定](#) (120 ページ)
- [RADIUS プロバイダーの設定](#) (124 ページ)
- [TACACS+ プロバイダーの設定](#) (126 ページ)

### ユーザアカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。有効期限の時間になると、ユーザアカウントは無効になります。

デフォルトでは、ユーザアカウントの有効期限はありません。

ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、アカウントの有効期限を使用可能な最も遅い日付に設定することは可能です。

## ユーザ名に関するガイドライン

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID としても使用されます。ユーザアカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1～32 の文字を含めることができます。
  - 任意の英字

- 任意の数字
  - \_ (アンダースコア)
  - - (ダッシュ)
  - . (ドット)
- ログイン ID は一意である必要があります。
  - ログイン ID は、英文字で開始する必要があります。アンダースコアなどの特殊文字や数字から始めることはできません。
  - ログイン ID では、大文字と小文字が区別されます。
  - すべてが数字のログイン ID は作成できません。
  - ユーザアカウントの作成後は、ログイン ID を変更できません。ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。

## パスワードに関するガイドライン

ローカル認証された各ユーザアカウントにパスワードが必要です。admin 権限または AAA 権限を持つユーザは、ユーザパスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証されたユーザのパスワード強度チェックを有効にすると、Firepower eXtensible Operating System は次の要件を満たしていないパスワードを拒否します。

- 8 ~ 80 文字の長さであること。



---

(注) コモンクライテリア要件に準拠するために、オプションでシステムの最小文字数 15 文字の長さのパスワードを設定できます。詳細については、[最小パスワード長チェックの設定 \(39 ページ\)](#) を参照してください。

---

- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字 (特殊文字) を少なくとも 1 文字含む。
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。

- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワードディクショナリチェックに合格する。たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。\$（ドル記号）、?（疑問符）、=（等号）。
- ローカルユーザアカウントおよび admin アカウントの場合は空白にしない。

## リモート認証のガイドライン

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Firepower 4100/9300 シャーシがそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

### リモート認証サービスのユーザアカウント

ユーザアカウントは、Firepower 4100/9300 シャーシにローカルに存在するか、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションを、Firepower Chassis Manager または FXOS CLI から表示できます。

### リモート認証サービスのユーザロール

リモート認証サーバでユーザアカウントを作成する場合は、ユーザが Firepower 4100/9300 シャーシで作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を FXOS で使用される名前と一致させることが必要です。ロールポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

### リモート認証プロバイダーのユーザ属性

RADIUS および TACAS+ 構成では、ユーザが Firepower Chassis Manager または FXOS CLI へのログインに使用する各リモート認証プロバイダーで Firepower 4100/9300 シャーシ用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

ユーザがログインすると、FXOS は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表は、FXOS でサポートしているリモート認証プロバイダーのユーザ属性要件を比較したものです。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	任意	<p>次のいずれかを実行するように選択できます。</p> <ul style="list-style-type: none"> <li>• LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。</li> <li>• LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。</li> </ul>	<p>シスコの LDAP の実装では、Unicode タイプの属性が必要です。</p> <p>CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します</p> <p>次の項で、サンプル OID を示します。</p>
RADIUS	任意	<p>次のいずれかを実行するよう選択できます。</p> <ul style="list-style-type: none"> <li>• RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用します。</li> <li>• RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成します。</li> </ul>	<p>シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。</p> <p>次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザーロールとロケールを指定する方法を示しています。</p> <pre>shell:roles="admin,aaa" shell:locales="L1,abc"</pre> <p>複数の値を区切るには、区切り文字としてカンマ「,」を使用します。</p>

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
TACAS	必須	スキーマを拡張し、 <b>cisco-av-pair</b> という名前前のカスタム属性を作成する必要があります。	<p><b>cisco-av-pair</b> 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。</p> <p>次の構文例は、<b>cisco-av-pair</b> 属性を作成するときに複数のユーザロールとロケールを指定する方法を示しています。</p> <pre>cisco-av-pair=shell:roles=admin aaa" shell:locales*"L1 abc"</pre> <p><b>cisco-av-pair</b> 属性構文でアスタリスク (*) を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。</p>

### LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
LDAPDisplayName: CiscoAVPair
```

```
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

## ユーザ ロール

システムには、次のユーザ ロールが用意されています。

### 管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトの `admin` アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

### Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

### 操作

NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ (syslog サーバとエラーを含む) に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

### AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

## ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、ローカル認証されたすべてのユーザのパスワード履歴やパスワード変更間隔プロパティが含まれます。ローカル認証されたユーザのそれぞれに異なるパスワード プロファイルを指定することはできません。

### パスワード履歴のカウント

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。このプロパティが設定されている場合、Firepower シャーシは、ローカル認証されたユーザが以前に使用したパスワードを最大 15 個まで保存します。パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になるまでに、ユーザはパスワード履歴カウントで設定された数だけパスワードを作成して使用する必要があります。たとえば、パスワード履歴カウントを 8 に設定した場合、ローカル認証されたユーザは、9 番目のパスワードが期限切れになるまで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。この値によって履歴カウントが無効化されるため、ユーザはいつでも以前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザのパスワード履歴カウントをクリアし、以前のパスワードの再利用を有効にできます。

### パスワード変更間隔

パスワード変更間隔によって、ローカル認証されたユーザが特定の時間内に実施できるパスワード変更の回数を制限することができます。次の表は、パスワード変更間隔の2つの設定オプションを示しています。

間隔の設定	説明	例
No password change allowed	このオプションを設定すると、ローカル認証されたユーザは、パスワードを変更してから特定の時間内はパスワードを変更できなくなります。  1 ~ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが 48 時間以内にパスワードを変更できないようにするには、次のように設定します。  <ul style="list-style-type: none"> <li>• [Change During Interval] を無効に設定</li> <li>• [No Change Interval] を 48 に設定</li> </ul>
変更間隔内のパスワード変更許可	このオプションでは、事前に定義した時間内にローカル認証ユーザがパスワードを変更できる最大回数を指定します。  変更間隔を 1 ~ 745 時間で、パスワード変更の最大回数を 0 ~ 10 で指定できます。デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に 1 回まで変更できるようにする場合、次のように設定します。  <ul style="list-style-type: none"> <li>• [間隔中の変更 (Change During Interval)] を有効にする</li> <li>• [Change Count] を 1 に設定</li> <li>• [Change Interval] を 24 に設定</li> </ul>

## ユーザ設定

### 手順

- ステップ 1 [System] > [User Management] を選択します。
- ステップ 2 [Settings] タブをクリックします。
- ステップ 3 次のフィールドに必要な情報を入力します。

名前	説明
[Default Authentication] フィールド	<p>リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Local] : ユーザアカウントは、Firepower シャーシでローカルに定義する必要があります。</li> <li>• [Radius] : ユーザアカウントは、Firepower シャーシに指定された RADIUS サーバで定義する必要があります。</li> <li>• [TACACS] : ユーザアカウントは、Firepower シャーシに指定された TACACS+サーバで定義する必要があります。</li> <li>• [LDAP] : ユーザアカウントは、Firepower シャーシに指定された LDAP/MS-AD サーバで定義する必要があります。</li> <li>• [None] : ユーザアカウントが Firepower シャーシに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。</li> </ul>
[Console Authentication] フィールド	<p>コンソールポート経由で FXOS CLI に接続するときにユーザが認証される方法。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Local] : ユーザアカウントは、Firepower シャーシでローカルに定義する必要があります。</li> <li>• [Radius] : ユーザアカウントは、Firepower シャーシに指定された RADIUS サーバで定義する必要があります。</li> <li>• [TACACS] : ユーザアカウントは、Firepower シャーシに指定された TACACS+サーバで定義する必要があります。</li> <li>• [LDAP] : ユーザアカウントは、Firepower シャーシに指定された LDAP/MS-AD サーバで定義する必要があります。</li> <li>• [None] : ユーザアカウントが Firepower シャーシにローカルである場合、ユーザがコンソールポートを使用して FXOS CLI に接続するときにはパスワードは不要です。</li> </ul>
リモート ユーザの設定	

名前	説明
[Remote User Role Policy]	<p>ユーザがログインを試みたときに、リモート認証プロバイダーが認証情報を含むユーザ ロールを提供しない場合の動作を制御します。</p> <ul style="list-style-type: none"> <li>• [Assign Default Role] : ユーザは、読み取り専用ユーザ ロールでログインできます。</li> <li>• [No-Login] : ユーザ名とパスワードが正しくても、ユーザはシステムにログインできません。</li> </ul>
<b>ローカル ユーザ設定</b>	
[パスワード強度チェック (Password Strength Check) ] チェックボックス	<p>オンにすると、すべてのローカルユーザパスワードは、強力なパスワードのガイドラインに準拠しなければなりません (パスワードに関するガイドライン (27 ページ) を参照)。</p>
[History Count] フィールド	<p>以前に使用したパスワードが再使用可能になるまでにユーザが作成する必要がある、一意のパスワードの数。履歴カウントは、最も新しいパスワードを先頭に時系列とは逆の順番で表示され、履歴カウントのしきい値に到達すると、最も古いパスワードのみが使用可能になります。</p> <p>この値は、0 ~ 15 から自由に設定できます。</p> <p>[History Count] フィールドを 0 に設定して履歴カウントをディセーブルにすると、ユーザは以前のパスワードをいつでも再使用できます。</p>
[Change During Interval] フィールド	<p>ローカル認証されたユーザがパスワードを変更できるタイミングを制御します。ここに表示される値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• [Enable] : ローカル認証されたユーザは、[Change Interval] および [Change Count] の設定に基づいて、パスワードを変更できます。</li> <li>• [Disable] : ローカル認証されたユーザは、[No Change Interval] に指定された期間はパスワードを変更できません。</li> </ul>

名前	説明
[Change Interval] フィールド	<p>[Change Count] フィールドで指定したパスワード変更回数が適用される時間数。</p> <p>この値は、1 ~ 745 時間から自由に設定できます。</p> <p>たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。</p>
[Change Count] フィールド	<p>ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数。</p> <p>この値は、0 ~ 10 から自由に設定できます。</p>
[No Change Interval] フィールド	<p>ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。</p> <p>この値は、1 ~ 745 時間の範囲で自由に設定できます。</p> <p>この間隔は、[間隔中の変更 (Change During Interval)] プロパティが [無効 (Disable)] に設定されていない場合は無視されます。</p>

ステップ 4 [Save] をクリックします。

## セッションタイムアウトの設定

FXOS CLI を使用することにより、ユーザアクティビティなしで経過可能な時間を指定できます。この時間が経過した後、Firepower 4100/9300 シャーシはユーザセッションを閉じます。コンソールセッションと、HTTPS、SSH、および Telnet セッションとで、異なる設定を行うことができます。

タイムアウトとして 3600 秒 (60 分) 以下の値を設定できます。デフォルト値は 600 秒です。この設定を無効にするには、セッションタイムアウト値を 0 に設定します。

### 手順

ステップ 1 セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

ステップ 2 デフォルト認証セキュリティ モードを開始します。

```
Firepower-chassis /security # scope default-auth
```

**ステップ 3** HTTPS、SSH、および Telnet セッションのアイドル タイムアウトを設定します。

```
Firepower-chassis /security/default-auth # set session-timeout seconds
```

**ステップ 4** (任意) コンソールセッションのアイドル タイムアウトを設定します。

```
Firepower-chassis /security/default-auth # set con-session-timeout seconds
```

**ステップ 5** (任意) セッションおよび絶対セッションタイムアウトの設定を表示します。

```
Firepower-chassis /security/default-auth # show detail
```

例 :

```
Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Session timeout(in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

## 絶対セッションタイムアウトの設定

Firepower 4100/9300 シャーシには絶対セッションタイムアウト設定があり、セッションの使用状況に関係なく、絶対セッションタイムアウト期間が経過するとユーザセッションは閉じられます。この絶対タイムアウト機能は、シリアルコンソール、SSH、HTTPS を含むすべての形式のアクセスに対してグローバルに適用されます。

シリアルコンソールセッションの絶対セッションタイムアウトを個別に設定できます。これにより、デバッグニーズに応えるシリアルコンソール絶対セッションタイムアウトは無効にしながら、他の形式のアクセスのタイムアウトは維持することができます。

絶対タイムアウト値のデフォルトは 3600 秒 (60 分) であり、FXOS CLI を使用して変更できます。この設定を無効にするには、絶対セッションタイムアウト値を 0 に設定します。

### 手順

**ステップ 1** セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

**ステップ 2** デフォルト認証セキュリティ モードを開始します。

```
Firepower-chassis /security # scope default-auth
```

**ステップ 3** 絶対セッションタイムアウトを設定します。

```
Firepower-chassis /security/default-auth # set absolute-session-timeout seconds
```

**ステップ 4** (任意) 別個のコンソールセッションタイムアウトを設定します。

```
Firepower-chassis /security/default-auth # set con-absolute-session-timeout seconds
```

**ステップ 5** (任意) セッションおよび絶対セッションタイムアウトの設定を表示します。

```
Firepower-chassis /security/default-auth # show detail
```

例 :

```
Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Session timeout(in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

## ログイン試行の最大回数の設定

ロックアウト前にユーザに許可されるログイン試行の最大回数を指定します。この回数を超えると、指定した時間だけ Firepower 4100/9300 シャーシからロックアウトされることとなります。ユーザは、設定した最大回数を超過してログインを試行すると、システムからロックされません。ユーザがロックアウトされたことを示す通知は表示されません。これが起きると、ユーザは次にログインを試行できるようになるまで、指定された時間だけ待機する必要があります。

ログイン試行の最大数を設定するには、次の手順を実行します。



- (注)
- どのタイプのユーザアカウントであっても (管理者を含む)、ログイン試行の最大数を超過してログインを試行すると、システムからロックアウトされます。
  - 失敗できるログイン試行のデフォルトの最大回数は0です。ユーザがログイン試行の最大数を超過したときにシステムからロックアウトされるデフォルトの時間は、30分 (1800秒) です。
  - ユーザのロックアウトのステータスを表示し、ユーザのロックアウト状態をクリアする手順については、[ユーザロックアウトステータスの表示およびクリア \(38 ページ\)](#) を参照してください。

このオプションは、システムのコモンライテリア認定への準拠を取得するさまざまなサービスの1つです。詳細については、[セキュリティ認定準拠 \(53 ページ\)](#) を参照してください。

## 手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

```
scope system
```

```
scope security
```

ステップ 2 失敗できるログイン試行の最高回数を設定します。

```
set max-login-attempts
```

```
max_login
```

*max\_login* の値は、0 ~ 10 の範囲内の任意の整数です。

ステップ 3 ログイン試行の最高回数に達した後、ユーザがシステムからロックアウトされる時間（秒単位）を指定します。

```
set user-account-unlock-time
```

```
unlock_time
```

ステップ 4 設定をコミットします。

```
commit-buffer
```

## ユーザ ロックアウト ステータスの表示およびクリア

管理者ユーザは、失敗の回数が [Maximum Number of Login Attempts] CLI 設定で指定されたログイン最大試行回数を超えたら、Firepower 4100/9300 シャーシからロックアウトされているユーザのロックアウトステータスを表示およびクリアできます。詳細については、[ログイン試行の最大回数の設定（37 ページ）](#) を参照してください。

## 手順

ステップ 1 FXOS CLI から、セキュリティ モードに入ります。

```
scope system
```

```
scope security
```

ステップ 2 該当するユーザのユーザ情報（ロックアウトステータスを含む）を次のように表示します。

```
Firepower-chassis /security # show local-user user detail
```

例：

```
Local User user:
First Name:
Last Name:
```

```
Email:  
Phone:  
Expiration: Never  
Password:  
User lock status: Locked  
Account status: Active  
User Roles:  
Name: read-only  
User SSH public key:
```

**ステップ 3** (任意) ユーザのロックアウト ステータスをクリアします。

```
Firepower-chassis /security # scope local-user user
```

```
Firepower-chassis /security/local-user # clear lock-status
```

## 最小パスワード長チェックの設定

最小パスワード長チェックを有効にした場合は、指定した最小文字を使用するパスワードを作成する必要があります。たとえば、*min\_length* オプションを 15 に設定した場合、パスワードは 15 文字以上を使用して作成する必要があります。このオプションは、システムのコモンクライテリア認定への準拠のための数の 1 つです。詳細については、[セキュリティ認定準拠 \(53 ページ\)](#) を参照してください。

最小パスワード長チェックを設定するには、次の手順を実行します。

### 手順

**ステップ 1** FXOS CLI から、セキュリティ モードに入ります。

```
scope system
```

```
scope security
```

**ステップ 2** パスワードの最小の長さを指定します。

```
set min-password-length min_length
```

**ステップ 3** 設定をコミットします。

```
commit-buffer
```

# ローカル ユーザ アカウントの作成

## 手順

- ステップ 1** [System] > [User Management] を選択します。
- ステップ 2** [Local Users] タブをクリックします。
- ステップ 3** [Add User] をクリックして [Add User] ダイアログボックスを開きます。
- ステップ 4** ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明
[User Name] フィールド	このアカウントにログインするときに使用されるアカウント名。この名前は、固有であり、ユーザアカウント名のガイドラインと制限を満たしている必要があります ( <a href="#">ユーザ名に関するガイドライン (26 ページ)</a> を参照)。  ユーザを保存した後は、ログインIDを変更できません。ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メールアドレス。
[Phone Number] フィールド	ユーザの電話番号。
[Password] フィールド	このアカウントに関連付けられているパスワード。パスワード強度チェックを有効にした場合は、ユーザパスワードを強固なものにする必要があります。Firepower eXtensible Operating System は強度チェック要件を満たしていないパスワードを拒否します ( <a href="#">パスワードに関するガイドライン (27 ページ)</a> を参照)。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Status] フィールド	ステータスが [Active] に設定されている場合、ユーザはこのログインIDとパスワードを使用して Firepower Chassis Manager と FXOS CLI にログインできます。

名前	説明
[User Role] リスト	<p>ユーザアカウントに割り当てる権限を表すロール (<a href="#">ユーザロール (31 ページ)</a>) を参照)。</p> <p>すべてのユーザはデフォルトでは読み取り専用ロールが割り当てられます。このロールは選択解除できません。複数のロールを割り当てるには、<b>Ctrl</b>を押したまま、目的のロールをクリックします。</p> <p>(注) ユーザロールおよび権限の変更は次回のユーザログイン時に有効になります。ユーザアカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。</p>
[Account Expires] チェックボックス	<p>オンにすると、このアカウントは [Expiration Date] フィールドで指定した日付に期限切れになり、それ以降は使用できなくなります。</p> <p>(注) ユーザアカウントに有効期限を設定した後、有効期限なしに再設定することはできません。ただし、アカウントの有効期限を使用可能な最も遅い日付に設定することは可能です。</p>
[Expiry Date] フィールド	<p>アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。</p> <p>このフィールドの終端にあるカレンダーアイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。</p>

ステップ 5 [Add] をクリックします。

## ローカル ユーザ アカウントの削除

### 手順

- ステップ 1 [System] > [User Management] を選択します。
- ステップ 2 [Local Users] タブをクリックします。
- ステップ 3 削除するユーザアカウントの行で、[Delete] をクリックします。

ステップ 4 [Confirm] ダイアログボックスで、[Yes] をクリックします。

---

## ローカルユーザアカウントのアクティブ化または非アクティブ化

ローカルユーザアカウントをアクティブ化または非アクティブ化できるのは、admin 権限または AAA 権限を持つユーザのみです。

### 手順

---

ステップ 1 [System] > [User Management] を選択します。

ステップ 2 [Local Users] タブをクリックします。

ステップ 3 アクティブ化または非アクティブ化するユーザ アカウントの行で、[Edit] (鉛筆アイコン) をクリックします。

ステップ 4 [Edit User] ダイアログボックスで、次のいずれかを実行します。

- ユーザ アカウントをアクティブ化するには、[Account Status] フィールドの [Active] オプション ボタンをクリックします。
- ユーザ アカウントを非アクティブ化するには、[Account Status] フィールドの [Inactive] オプション ボタンをクリックします。

admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。

ステップ 5 [Save] をクリックします。

---

## ローカル認証されたユーザのパスワード履歴のクリア

### 手順

---

ステップ 1 セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

ステップ 2 指定したユーザ アカウントに対してローカル ユーザ セキュリティ モードを開始します。

```
Firepower-chassis /security # scope local-user user-name
```

ステップ 3 指定したユーザ アカウントのパスワード履歴をクリアします。

```
Firepower-chassis /security/local-user # clear password-history
```

**ステップ 4** トランザクションをシステム設定にコミットします。

```
Firepower-chassis /security/local-user # commit-buffer
```

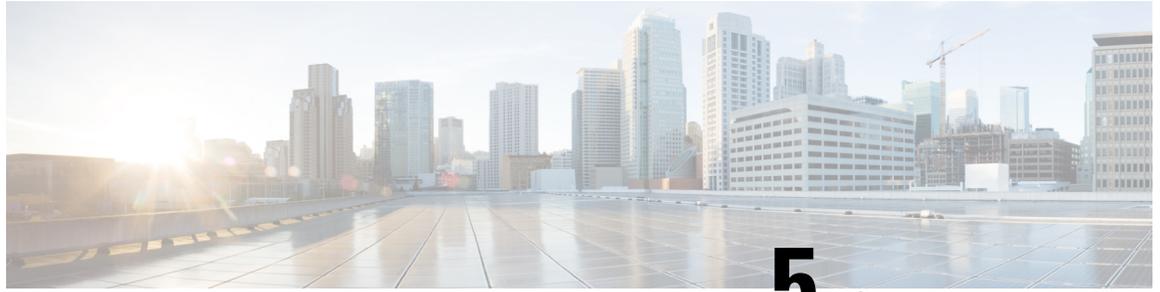
---

### 例

次に、パスワード履歴を消去し、トランザクションを確定する例を示します。

```
Firepower-chassis # scope security  
Firepower-chassis /security # scope local-user admin  
Firepower-chassis /security/local-user # clear password-history  
Firepower-chassis /security/local-user* # commit-buffer  
Firepower-chassis /security/local-user #
```

ローカル認証されたユーザのパスワード履歴のクリア



## 第 5 章

# イメージ管理

- [イメージ管理について](#) (45 ページ)
- [Cisco.com](#) からのイメージのダウンロード (46 ページ)
- [Firepower セキュリティ アプライアンスへのイメージのアップロード](#) (46 ページ)
- [イメージの整合性の確認](#) (47 ページ)
- [Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード](#) (47 ページ)
- [論理デバイスのイメージ バージョンの更新](#) (48 ページ)
- [Firmware アップグレード](#) (50 ページ)

## イメージ管理について

Firepower 4100/9300 シャーシ では 2 つの基本タイプのイメージを使用します。



(注) すべてのイメージに対して、セキュアブートによるデジタル署名と検証が行われます。どのような場合も、イメージを変更しないでください。変更すると、検証エラーになります。

- **プラットフォームバンドル**：Firepowerプラットフォームバンドルは、Firepower Supervisor およびFirepowerセキュリティモジュール/エンジンで動作する、複数の独立したイメージの集まりです。プラットフォームバンドルは、Firepower eXtensible Operating System のソフトウェアパッケージです。
- **アプリケーション**：アプリケーションイメージは、Firepower 4100/9300 シャーシのセキュリティモジュール/エンジンに導入するソフトウェアイメージです。アプリケーションイメージは、Cisco Secure Package ファイル (CSP) として提供されます。これは、論理デバイス作成時にセキュリティモジュール/エンジンに展開されるまで（または以降の論理デバイス作成に備えて）スーパーバイザに保存されます。同じアプリケーションイメージタイプの複数の異なるバージョンを Firepower Supervisor に保存できます。



- (注) プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

## Cisco.com からのイメージのダウンロード

Cisco.com から FXOS およびアプリケーション イメージをダウンロードし、Firepower シャーシにアップロードすることができます。

### 始める前に

Cisco.com アカウントが必要です。

### 手順

- ステップ 1** Web ブラウザを使用して、<http://www.cisco.com/go/firepower9300-software> または <http://www.cisco.com/go/firepower4100-software> にアクセスします。  
Firepower 4100/9300 シャーシのソフトウェア ダウンロード ページがブラウザに表示されます。
- ステップ 2** 該当するソフトウェア イメージを見つけて、ローカル コンピュータにダウンロードします。

## Firepower セキュリティ アプライアンスへのイメージのアップロード

FXOS およびアプリケーション イメージをシャーシにアップロードできます。

### 始める前に

アップロードするイメージがローカル コンピュータで使用可能であることを確認してください。

### 手順

- ステップ 1** **[System] > [Updates]** を選択します。  
**[Available Updates]** ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ 2** **[Upload Image]** をクリックして、**[Upload Image]** ダイアログボックスを開きます。

- ステップ3** [Choose File] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
- ステップ4** [Upload] をクリックします。  
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
- ステップ5** 特定のソフトウェア イメージの場合、イメージのアップロード後にエンドユーザー ライセンス 契約書が表示されます。システム プロンプトに従って、エンドユーザー ライセンス契約書に同意します。
- 

## イメージの整合性の確認

イメージの整合性は、新しいイメージが Firepower 4100/9300 シャーシに追加されると自動的に確認されます。必要な場合に、手動でイメージの整合性を確認するには、次の手順を実行できます。

### 手順

---

- ステップ1** [System] > [Updates] を選択します。  
[Available Updates] ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。
- ステップ2** 確認するイメージの [Verify] (チェックマーク アイコン) をクリックします。  
システムはイメージの整合性を確認し、[Image Integrity] フィールドにステータスを表示します。
- 

## Firepower eXtensible Operating System プラットフォームバンドルのアップグレード

### 始める前に

プラットフォーム バンドルのソフトウェア イメージを Cisco.com からダウンロードして ([Cisco.comからのイメージのダウンロード \(46ページ\)](#) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepowerセキュリティアプライアンスへのイメージのアップロード \(46ページ\)](#) を参照)。



(注) アップグレードプロセスには通常 20 ～ 30 分かかります。

スタンドアロン論理デバイスを実行中の Firepower 9300 または Firepower 4100 シリーズセキュリティ アプライアンスをアップグレードしている場合、または シャーシ内クラスタを実行中の Firepower 9300 セキュリティ アプライアンスをアップグレードしている場合、アップグレード中にデバイスを介してトラフィックは通過しません。

シャーシ間クラスタに属する Firepower 9300 または Firepower 4100 シリーズセキュリティ アプライアンスをアップグレードしている場合、アップグレード中にアップグレードされたデバイスを介してトラフィックは通過しません。ただし、クラスタ内の他のデバイスではトラフィックは通過し続けます。

## 手順

**ステップ 1** **[System] > [Updates]** を選択します。

**[Available Updates]** ページに、シャーシで使用可能な Firepower eXtensible Operating System プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

**ステップ 2** アップグレードする FXOS プラットフォーム バンドルの **[Upgrade]** をクリックします。

システムは、まずインストールするソフトウェアパッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**ステップ 3** インストールの続行を確定するには **[Yes]** を、インストールをキャンセルするには **[No]** をクリックします。

Firepower eXtensible Operating System がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

## 論理デバイスのイメージバージョンの更新

この手順を使用して、新しいバージョンに ASA アプリケーション イメージをアップグレードするか、Firepower Threat Defense アプリケーション イメージをディザスタリカバリ シナリオで使用される新しいスタートアップバージョンに設定します。

Firepower Chassis Manager または FXOS CLI を使用して Firepower Threat Defense 論理デバイスでスタートアップバージョンを変更しても、アプリケーションはすぐに新しいバージョンにアップグレードされません。論理デバイス スタートアップバージョンは、Firepower Threat Defense がディザスタリカバリ シナリオで再インストールされるバージョンです。詳細については、[Firepower Threat Defense のクラスタ メンバのディザスタリカバリ \(238 ページ\)](#) を参照してください。FTD 論理デバイスの初期作成後には、FTD 論理デバイスを、Firepower Chassis

Manager または FXOS CLI を使用してアップグレードすることはありません。FTD 論理デバイスをアップグレードするには、Firepower Management Center を使用する必要があります。詳細については、次のサイトにある FirePOWER システムのリリース ノートを参照してください。  
<http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>

さらに、FTD 論理デバイスへの更新は、Firepower Chassis Manager の **[Logical Devices]** > **[Edit]** ページおよび **[System]** > **[Updates]** ページには反映されないことに注意してください。これらのページで、表示されるバージョンは、FTD 論理デバイスを作成するために使用されたソフトウェア バージョン (CSP イメージ) を示します。

ASA 論理デバイスでスタートアップ バージョンを変更すると、ASA はこのバージョンにアップグレードされ、すべての設定が復元されます。設定に応じて ASA スタートアップ バージョンを変更するには、次のワークフローを使用します。

ASA ハイ アベイラビリティ :

1. スタンバイ ユニットで論理デバイス イメージ バージョンを変更します。
2. スタンバイ ユニートをアクティブにします。
3. 他のユニットでアプリケーション バージョンを変更します。

ASA シャーシ間クラスタ :

1. スレーブ ユニットでスタートアップ バージョンを変更します。
2. スレーブ ユニートをマスター ユニットに変更します。
3. 元のマスターユニット (ここではスレーブ) でスタートアップバージョンを変更します。

### 始める前に

論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロード \(46 ページ\)](#) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード \(46 ページ\)](#) を参照)。

プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

### 手順

- 
- ステップ 1** **[Logical Devices]** を選択して **[Logical Devices]** ページを開きます。  
**[Logical Devices]** ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
  - ステップ 2** 更新する論理デバイスの **[Update Version]** をクリックして、**[Update Image Version]** ダイアログ ボックスを開きます。
  - ステップ 3** **[New Version]** では、ソフトウェア バージョンを選択します。

ステップ4 [OK] をクリックします。

## Firmware アップグレード

次の手順を使用して、Firepower 4100/9300 シャーシのファームウェアをアップグレードします。

### 手順

- ステップ1 Web ブラウザを使用して、<http://www.cisco.com/go/firepower9300-software> または <http://www.cisco.com/go/firepower4100-software> にアクセスします。Firepower 4100/9300 シャーシのソフトウェアダウンロードページがブラウザに表示されます。
- ステップ2 Cisco.com で適切なファームウェア パッケージを見つけ、Firepower 4100/9300 シャーシからアクセス可能なサーバにダウンロードします。
- ステップ3 Firepower 4100/9300 シャーシで、ファームウェア モードに入ります。  
Firepower-chassis # **scope firmware**
- ステップ4 FXOS ファームウェア イメージを Firepower 4100/9300 シャーシへダウンロードします。  
Firepower-chassis /firmware # **download image URL**  
次のいずれかの構文を使用してインポートされるファイルの URL を指定します。
- **ftp:// username@hostname / path**
  - **scp:// username@hostname / path**
  - **sftp://username@hostname/path**
  - **tftp:// hostname : port-num / path**
- ステップ5 ダウンロードプロセスをモニタする場合：  
Firepower-chassis /firmware # **show download-task image\_name detail**
- ステップ6 ダウンロードが完了したら、次のコマンドを入力してファームウェアパッケージの内容を表示できます。  
Firepower-chassis /firmware # **show package image\_name expand**
- ステップ7 次のコマンドを入力してファームウェア パッケージのバージョン番号を表示できます。  
Firepower-chassis /firmware # **show package**  
このバージョン番号は、以下のステップでファームウェアパッケージをインストールするときに使用されます。
- ステップ8 ファームウェア パッケージをインストールする場合：

- a) firmware-install モードに入ります。  
Firepower-chassis /firmware # **scope firmware-install**
- b) ファームウェア パッケージをインストールします。  
Firepower-chassis /firmware/firmware-install # **install firmware pack-version version\_number**  
システムでファームウェアパッケージが確認され、確認プロセスが完了するまでに数分か  
かることがあると通知されます。
- c) **yes** と入力し、確認を続行します。  
ファームウェア パッケージの確認後、インストール プロセスが完了するまで数分か  
かる可能性があることと、システムが更新プロセス中にリブートされることが通知されま  
す。
- d) **yes** と入力し、インストールを続行します。アップグレードプロセス中に Firepower 4100/9300  
シャーシの電源を再投入しないでください。

**ステップ 9** アップグレードプロセスをモニタするには、次の手順を実行します。

```
Firepower-chassis /firmware/firmware-install # show detail
```

**ステップ 10** インストールが完了したら、現在のファームウェアバージョンを表示するために、次のコマン  
ドを入力することもできます。

```
Firepower-chassis /firmware/firmware-install # top
```

```
Firepower-chassis # scope chassis 1
```

```
Firepower-chassis /firmware # show sup version
```

## 例

次の例では、ファームウェアをバージョン 1.0.10 にアップグレードします。

```
Firepower-chassis# scope firmware  
Firepower-chassis /firmware # download image  
tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA  
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail
```

```
Download task:  
File Name: fxos-k9-fpr9k-firmware.1.0.10.SPA  
Protocol: Tftp  
Server: 10.10.10.1  
Port: 0  
Userid:  
Path:  
Downloaded Image Size (KB): 2104  
Time stamp: 2015-12-04T23:51:57.846  
State: Downloading  
Transfer Rate (KB/s): 263.000000  
Current Task: unpacking image fxos-k9-fpr9k-firmware.1.0.10.SPA on primary(  
FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)
```

```
Firepower-chassis /firmware # show package fxos-k9-fpr9k-firmware.1.0.10.SPA expand
```

```
Package fxos-k9-fpr9k-firmware.1.0.10.SPA:  
Images:
```

```
fxos-k9-fpr9k-fpga.1.0.5.bin
fxos-k9-fpr9k-rommon.1.0.10.bin
```

```
Firepower-chassis /firmware # show package
```

```
Name                                     Version
-----
fxos-k9-fpr9k-firmware.1.0.10.SPA       1.0.10
```

```
Firepower-chassis /firmware # scope firmware-install
```

```
Firepower-chassis /firmware/firmware-install # install firmware pack-version 1.0.10
```

```
Verifying FXOS firmware package 1.0.10. Verification could take several minutes.
Do you want to proceed? (yes/no):yes
```

```
FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA : Upgrade from 1.04 to 1.05
```

```
This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup
```

```
Attention:
```

```
The system will be reboot to upgrade the SUP firmware.
The upgrade operation will take several minutes to complete.
PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
```

```
Do you want to proceed? (yes/no):yes
```

```
Upgrading FXOS SUP firmware software package version 1.0.10
```

```
command executed
```



## 第 6 章

# セキュリティ認定準拠

- [セキュリティ認定準拠](#) (53 ページ)
- [SSH ホスト キーの生成](#) (54 ページ)
- [IPSec セキュア チャンネルの設定](#) (55 ページ)
- [トラストポイントのスタティック CRL の設定](#) (60 ページ)
- [証明書失効リストのチェックについて](#) (61 ページ)
- [CRL 定期ダウンロードの設定](#) (66 ページ)
- [LDAP キー リング証明書の設定](#) (68 ページ)
- [クライアント証明書認証の有効化](#) (69 ページ)

## セキュリティ認定準拠

米国連邦政府機関は、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。Firepower 4100/9300 シャーシは、これらのセキュリティ認証基準のいくつかに準拠しています。

これらの基準に準拠する機能を有効にするステップについては、次のトピックを参照してください。

- [FIPS モードの有効化](#) (132 ページ)
- [コモンクライテリア モードの有効化](#) (133 ページ)
- [IPSec セキュア チャンネルの設定](#) (55 ページ)
- [トラストポイントのスタティック CRL の設定](#) (60 ページ)
- [証明書失効リストのチェックについて](#) (61 ページ)
- [CRL 定期ダウンロードの設定](#) (66 ページ)
- [NTP サーバ認証の有効化](#) (89 ページ)
- [LDAP キー リング証明書の設定](#) (68 ページ)
- [IP アクセス リストの設定](#) (133 ページ)

- [クライアント証明書認証の有効化 \(69 ページ\)](#)
- [最小パスワード長チェックの設定 \(39 ページ\)](#)
- [ログイン試行の最大回数の設定 \(37 ページ\)](#)



(注) これらのトピックは Firepower 4100/9300 シャーシにおける認定準拠の有効化についてのみ説明していることに注意してください。Firepower 4100/9300 シャーシで認定準拠を有効にしても、接続された論理デバイスにまでそのコンプライアンスは自動的に伝搬されません。

## SSH ホスト キーの生成

FXOS リリース 2.0.1 より以前は、デバイスの初期設定時に作成した既存の SSH ホスト キーが 1024 ビットにハードコードされていました。FIPS およびコモンクライテリア認定に準拠するには、この古いホスト キーを破棄して新しいホスト キーを生成する必要があります。詳細については、[FIPS モードの有効化 \(132 ページ\)](#) または [コモンクライテリアモードの有効化 \(133 ページ\)](#) を参照してください。

古い SSH ホスト キーを破壊し、新しい証明書準拠キーを生成するには、次の手順を実行します。

### 手順

**ステップ 1** FXOS CLI から、サービス モードに入ります。

```
scope system
```

```
scope services
```

**ステップ 2** SSH ホスト キーを削除します。

```
delete ssh-server host-key
```

**ステップ 3** 設定をコミットします。

```
commit-buffer
```

**ステップ 4** SSH ホスト キーのサイズを 2048 ビットに設定します。

```
set ssh-server host-key rsa 2048
```

**ステップ 5** 設定をコミットします。

```
commit-buffer
```

**ステップ 6** 新しい SSH ホスト キーを作成します。

```
create ssh-server host-key
```

**commit-buffer**

**ステップ 7** 新しいホスト キーのサイズを確認します。

```
show ssh-server host-key
```

```
ホスト キー サイズ : 2048
```

## IPSec セキュア チャネルの設定

Firepower 4100/9300 シャーシ上で IPSec を設定して、エンドツーエンドのデータ暗号化や、パブリック ネットワーク内を移動するデータ パケットに対する認証サービスを提供できます。このオプションは、システムのコモンクライテリア認定への準拠を取得するさまざまなサービスの 1 つです。詳細については、[セキュリティ認定準拠 \(53 ページ\)](#) を参照してください。



(注) IKE 接続と SA 接続の間で一致する暗号キー強度の適用を設定する場合は、次のようにします (次の手順で `sa-strength-enforcement` を `yes` に設定します)。

SA の適用を有効にする場合	<p>IKEによりネゴシエートされたキーサイズが、ESPによりネゴシエートされたキーサイズより小さい場合、接続は失敗します。</p> <p>IKEによりネゴシエートされたキーサイズが、ESPによりネゴシエートされたキーサイズより大きいか等しい場合、SA適用検査にパスして、接続は成功します。</p>
SA の適用を無効にした場合	SA 適用検査にパスし、接続は成功します。

IPSec セキュア チャネルを設定するには、次の手順を実行します。

### 手順

**ステップ 1** FXOS CLI から、セキュリティ モードに入ります。

```
scope system
```

```
scope security
```

**ステップ 2** キー リングを作成します。

```
enter keyring ssp
```

```
! create certreq subject-name subject-name ip ip
```

**ステップ 3** 関連する証明書要求情報を入力します。

- enter certreq**
- ステップ 4 国を設定します。  
**set country *country***
- ステップ 5 DNS を設定します。  
**set dns *dns***
- ステップ 6 電子メールを設定します。  
**set e-mail *email***
- ステップ 7 IP 情報を設定します。  
**set fi-a-ip *fi-a-ip***  
**set fi-a-ipv6 *fi-a-ipv6***  
**set fi-b-ip *fi-b-ip***  
**set fi-b-ipv6 *fi-b-ipv6***  
**set ipv6 *ipv6***
- ステップ 8 ローカリティを設定します。  
**set locality *locality***
- ステップ 9 組織名を設定します。  
**set org-name *org-name***
- ステップ 10 組織ユニット名を設定します。  
**set org-unit-name *org-unit-name***
- ステップ 11 パスワードを設定します。  
**! set password**
- ステップ 12 状態を設定します。  
**set state *state***
- ステップ 13 certreq のサブジェクト名を設定します。  
**set subject-name *subject-name***
- ステップ 14 終了します。  
**exit**
- ステップ 15 モジュラスを設定します。  
**set modulus *modulus***
- ステップ 16 証明書要求の再生成を設定します。  
**set regenerate { *yes* | *no* }**

**ステップ 17** トラストポイントを設定します。

```
set trustpoint interca
```

**ステップ 18** 終了します。

```
exit
```

**ステップ 19** 新しく作成されたトラストポイントを入力します。

```
enter trustpoint interca
```

**ステップ 20** 証明書署名要求を作成します。

```
set certchain
```

例 :

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxXzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAcCzAJBgNVBAYTAIVT
MQswCQYDVQQIDAJDQTEMAAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMASG
A1UECwwEU1RCVTELMakGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWc3Nzc3BzE3Au
bmV0MIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrlqoi9k9gL/orBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690V18/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FIRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctfSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOPUD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXyWQydzymVvgE
wEzAoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZIO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAIoCCC
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybdAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEA2ukWyMLQuLqTvhq7
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhZyxVZ10DHKlzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPcQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpbQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCgGFmQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqXuoNMmqbS3KjCLXcH6xIN8t+Ukfp89hvJt/flUj+s/VJSVZWK4tAWvR7w1
QngCKRJW6FypzeyNBctj07wO+Wt4e3KhJjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSj+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AJEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ+/7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1ouk+/ZyPtBvFHUKFRnhoWj5SMFyds2IaatI
47N2ViaZBxhU3GicAH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXgxmMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxXzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHAcCzAJBgNVBAYTAIVT
MQswCQYDVQQIDAJDQTEPMAoGA1UECgwGbmV3c3RnMRAwDgYDVQQLEDAuZXZzdGJ1
```

```

MRMwEQYDvQDDAppbnRlcm0xLWNhMSgwJgYJKoZlHvcNAQkBFhlpbnRlcm0xLWNh
QGluDGVybTEtY2EubmV0MIICljANBgkqhkiG9w0BAQEFAAOCAg8AMIICGgKCAgEA
wLpNnyEx514P8uDoWKWF3IZseghLANSodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXI3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguLEDL812ROejQvpmfqGUq11stkIuh+wB+V
VRhUBVg7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLII
E2AkkXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFP/LCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXl0lb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJaw1
hLkfh0IdPA28xInflB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgjCjaujz55TGGd1
GjnxDMX9twzw7Ee51895Xmtr24qqaCXJoW/dPhcIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLIZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECawEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZlHvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3Iz1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqzlb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NwPwF+UDzbMXxx+KAAXCI6tCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZfyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPhgeROzyTFDixCeI6aROIgDP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKIJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF

```

ステップ 21 証明書署名要求を表示します。

**show certreq**

例 :

```

Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
□□□
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTElMAkGA1UEBhMCVVMxGzAJBgNVBAMgMAkNBMDQwCgYDVQQL
DANTSkMxMjE0MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIABAQDQ292Rq3t0laoxPbfE
p/ITKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mISORyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjCIK/tsIxsPkV0

```

```
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPIX9
39TYPIftDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vzwRpHWTdjjU5YnR1
qiR4q7j1RmzVFXCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBkgqhkig9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUlcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNIVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRYujTnp67BWuUZZI03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoM19WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzpzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

ステップ 22 IPsec モードに入ります。

**scope ipsec**

ステップ 23 ログ冗長レベルを設定します。

**set log-level log\_level**

ステップ 24 IPsec 接続を作成し、入力します。

**enter connection connection\_name**

ステップ 25 IPsec モードをトンネリングまたは伝送のために設定します。

**set mode tunnel\_or\_transport**

ステップ 26 ローカル IP アドレスを設定します。

**set local-addr ip\_address**

ステップ 27 リモート IP アドレスを設定します。

**set remote-addr ip\_address**

ステップ 28 トンネルモードを使用している場合、リモートサブネットを設定します。

**set remote-subnet ip/mask**

ステップ 29 (任意) リモート ID を設定します。

**set remote-ike-ident remote\_identity\_name**

ステップ 30 キーリング名を設定します。

**set keyring-name name**

ステップ 31 (任意) キーリングパスワードを設定します。

**set keyring-passwd passphrase**

ステップ 32 (任意) IKE-SA の有効期間を分単位で設定します。

**set ike-rekey-time minutes**

*minutes* 値には、60 ~ 1440 の範囲内の任意の整数を設定できます。

ステップ 33 (任意) 子の SA の有効期間を分単位 (30 ~ 480 分) で設定します。

**set esp-rekey-time minutes**

*minutes* 値には、30 ～ 480 の範囲内の任意の整数を設定できます。

**ステップ 34** (任意) 初期接続中に実行する再送信シーケンスの番号を設定します。

**set keyringtries retry\_number**

*retry\_number* 値には、1 ～ 5 の範囲の任意の整数を指定できます。

**ステップ 35** (任意) 証明書失効リスト検査を、有効または無効にします。

**set revoke-policy { relaxed | strict }**

**ステップ 36** 接続を有効にします。

**set admin-state enable**

**ステップ 37** すべての接続をリロードします。

**reload-conns**

**ステップ 38** (任意) 既存のトラストポイント名を IPsec に追加します。

**create authority trustpoint\_name**

**ステップ 39** IKE 接続と SA 接続との間の、対応する暗号キー強度の適用を設定します。

**set sa-strength-enforcement yes\_or\_no**

## トラストポイントのスタティック CRL の設定

失効した証明書は、証明書失効リスト (CRL) で保持されます。クライアントアプリケーションは、CRL を使用してサーバの認証を確認します。サーバアプリケーションは CRL を使用して、信頼されなくなったクライアントアプリケーションからのアクセス要求を許可または拒否します。

証明書失効リスト (CRL) 情報を使用して、Firepower 4100/9300 シャーシがピア証明書を検証するように設定できます。このオプションは、システムのコモンクライテリア認定への準拠を取得するさまざまなサービスの 1 つです。詳細については、[セキュリティ認定準拠 \(53 ページ\)](#) を参照してください。

CRL 情報を使用してピア証明書を検証するには、次の手順を実行します。

### 手順

**ステップ 1** FXOS CLI から、セキュリティ モードに入ります。

**scope security**

**ステップ 2** トラストポイント モードに入ります。

**scope trustpoint** *trustname*

**ステップ 3** 取り消しモードに入ります。

**scope revoke**

**ステップ 4** CRL ファイルをダウンロードします。

```
import crl protocol://user_id@CA_or_CRL_issuer_IP/tmp/DoDCAICRL1.crl
```

**ステップ 5** (任意) CRL 情報のインポートプロセスのステータスを表示します。

**show import-task detail**

**ステップ 6** CRL 専用の、証明書取り消し方法を設定します。

```
set certrevokemethod {crl}
```

## 証明書失効リストのチェックについて

証明書失効リスト (CRL) チェック モードを、IPSec、HTTPS およびセキュアな LDAP 接続で厳格または緩和に設定できます。

ダイナミック (非スタティック) CRL 情報は、X.509 証明書の CDP 情報から収集され、動的な CRL 情報を示します。スタティック CRL 情報は、システム管理によって手動でダウンロードされ、FXOS システムのローカルな CRL 情報を示します。ダイナミック CRL 情報は、証明書チェーンの現在処理中の証明書に対してのみ処理されます。スタティック CRL は、ピアの証明書チェーン全体に適用されます。

セキュアな IPSec、LDAP および HTTPS 接続の証明書失効のチェックを有効または無効にするステップについては、[IPSec セキュア チャネルの設定 \(55 ページ\)](#)、[LDAP プロバイダーの作成 \(121 ページ\)](#) および [HTTPS の設定 \(114 ページ\)](#) を参照してください。



- (注)
- 証明書失効のチェック モードが厳格に設定されている場合、スタティック CRL はピア証明書チェーンのレベルが 1 以上のときにのみ適用されます（たとえば、ピア証明書チェーンにルート CA 証明書およびルート CA によって署名されたピア証明書のみが含まれているとき）。
  - IPSec に対してスタティック CRL を設定している場合、[Authority Key Identifier (authkey)] フィールドはインポートされた CRL ファイルに存在している必要があります。そうしないと、IPSec はそれを無効と見なします。
  - スタティック CRL は、同じ発行元からのダイナミック CRL より優先されます。ピア証明書を検証するときに、同じ発行者の有効な（決定済みの）スタティック CRL があれば、ピア証明書の CDP は無視されます。
  - 次のシナリオでは、デフォルトで厳格な CRL チェックが有効になっています。
    - 新しく作成したセキュアな LDAP プロバイダー接続、IPSec 接続、またはクライアント証明書エントリ
    - 新しく展開した FXOS シャーシマネージャ（FXOS 2.3.1.x 以降の初期開始バージョンで展開）

次の表は、証明書失効リストのチェックの設定と証明書の検証に応じた接続の結果を示しています。

表 1: 厳格（ローカルスタティック CRL なし）に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンの CDP のチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	あり	利用不可	あり
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）	接続に失敗（syslog メッセージあり）

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
1つのCDPでピア証明書チェーンが欠落しています	接続に失敗 (syslog メッセージあり)	ピア証明書：接続に失敗 (syslog メッセージあり) 中間 CA：接続に失敗	接続に失敗 (syslog メッセージあり)
有効な署名付きピア証明書チェーンの1つのCDP CRL が空です	接続に成功	接続に成功	接続に失敗 (syslog メッセージあり)
ピア証明書チェーンのCDPがダウンロードできません	接続に失敗 (syslog メッセージあり)	ピア証明書：接続に失敗 (syslog メッセージあり) 中間 CA：接続に失敗	接続に失敗 (syslog メッセージあり)
証明書に CDP はありますが、CDPサーバがダウンしています	接続に失敗 (syslog メッセージあり)	ピア証明書：接続に失敗 (syslog メッセージあり) 中間 CA：接続に失敗	接続に失敗 (syslog メッセージあり)
証明書に CDP があり、サーバはアップしており、CRL は CDP にありますが、CRL に無効な署名があります	接続に失敗 (syslog メッセージあり)	ピア証明書：接続に失敗 (syslog メッセージあり) 中間 CA：接続に失敗	接続に失敗 (syslog メッセージあり)

表 2: 厳格 (ローカルスタティック CRL あり) に設定した証明書失効のチェック モード

ローカルスタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのCDPのチェック	完全な証明書チェーンが必要です	完全な証明書チェーンが必要です
ピア証明書チェーンのルート CA 証明書の CDP チェック	あり	利用不可
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)

ローカルスタティック CRL あり	LDAP 接続	IPSec 接続
1つの CDP でピア証明書チェーンが欠落しています (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードできません (証明書チェーンのレベルは 1)	接続に成功	接続に成功
証明書に CDP はありますが、CDP サーバがダウンしていません (証明書チェーンのレベルは 1)	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL は CDP にありますが、CRL に無効な署名があります (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗 (syslog メッセージあり)	CDP と組み合わせて使用すると、接続に成功します  CDP がなければ、接続に失敗し、syslog メッセージが表示されます

表 3: 緩和 (ローカルスタティック CRL なし) に設定した証明書失効のチェック モード

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認証
ピア証明書チェーンのチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンの CDP のチェック	完全な証明書チェーン	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	あり	利用不可	あり

ローカルスタティック CRL なし	LDAP 接続	IPSec 接続	クライアント証明書認 証
ピア証明書チェーンの 証明書検証のいずれか の失敗	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)
ピア証明書チェーンの いずれかの失効した証 明書	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)
1つの CDP でピア証明 書チェーンが欠落して います	接続に成功	接続に成功	接続に失敗 (syslog メッセージあり)
有効な署名付きピア証 明書チェーンの1つの CDP CRL が空です	接続に成功	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードで きません	接続に成功	接続に成功	接続に成功
証明書に CDP はあり ますが、CDP サーバが ダウンしています	接続に成功	接続に成功	接続に成功
証明書に CDP があ り、サーバはアップし ており、CRL は CDP にあります、CRL に 無効な署名があります	接続に成功	接続に成功	接続に成功

表 4: 緩和 (ローカルスタティック CRL あり) に設定した証明書失効のチェック モード

ローカルスタティック CRL あ り	LDAP 接続	IPSec 接続
ピア証明書チェーンのチェッ ク	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンの CDP の チェック	完全な証明書チェーン	完全な証明書チェーン
ピア証明書チェーンのルート CA 証明書の CDP チェック	あり	利用不可

ローカルスタティック CRL あり	LDAP 接続	IPSec 接続
ピア証明書チェーンの証明書検証のいずれかの失敗	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)
ピア証明書チェーンのいずれかの失効した証明書	接続に失敗 (syslog メッセージあり)	接続に失敗 (syslog メッセージあり)
1 つの CDP でピア証明書チェーンが欠落しています (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンの 1 つの CDP CRL が空です (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンの CDP がダウンロードできません (証明書チェーンのレベルは 1)	接続に成功	接続に成功
証明書に CDP はありますが、CDP サーバがダウンしていません (証明書チェーンのレベルは 1)	接続に成功	接続に成功
証明書に CDP があり、サーバはアップしており、CRL は CDP にありますが、CRL に無効な署名があります (証明書チェーンのレベルは 1)	接続に成功	接続に成功
ピア証明書チェーンのレベルが 1 より高くなっています	接続に失敗 (syslog メッセージあり)	CDP と組み合わせて使用すると、接続に成功します  CDP がなければ、接続に失敗し、syslog メッセージが表示されます

## CRL 定期ダウンロードの設定

システムを、CRL を定期的にダウンロードして、証明書の検証に新しい CRL を 1 ~ 24 時間ごとに使用するよう設定できます。

この機能とともに、次のプロトコルとインターフェイスを使用できます。

- FTP
- SCP
- SFTP
- TFTP
- USB



- (注)
- SCEP および OCSP はサポートされません。
  - CRL ごとに設定できるのは 1 つの定期ダウンロードのみです。
  - トラストポイントごとにサポートされるのは 1 つの CRL です。



- (注) 期間は 1 時間間隔でのみ設定できます。

CRL 定期ダウンロードを設定するには、次の手順を実行します。

#### 始める前に

Firepower 4100/9300 シャーシが、ピア証明書を (CRL) 情報を使用して検証するように設定されていることを確認します。詳細については、[トラストポイントのスタティック CRL の設定 \(60 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** FXOS CLI から、セキュリティモードに入ります。

**scope security**

**ステップ 2** トラストポイントモードに入ります。

**scope trustpoint**

**ステップ 3** 取り消しモードに入ります。

**scope revoke**

**ステップ 4** 取り消し設定を編集します。

**sh config**

**ステップ 5** 優先設定を設定します。

例 :

```

set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname

```

**ステップ 6** 設定ファイルを終了します。

**exit**

**ステップ 7** (任意) 新しい CRL をダウンロードして、新しい設定をテストします。

例 :

```

Firepower-chassis /security/trustpoint/revoke # sh import-task

Import task:
File Name Protocol Server      Port  Userid  State
-----
rootCA.crl  Scp    182.23.33.113  0     myname  Downloading

```

## LDAP キー リング証明書の設定

Firepower 4100/9300 シャーシ上で TLS 接続をサポートする、セキュアな LDAP クライアント キー リング証明書を設定できます。このオプションは、システムのコモンクライテリア認定への準拠を取得するさまざまなサービスの1つです。詳細については、[セキュリティ認定準拠 \(53 ページ\)](#) を参照してください。



(注) コモンクライテリア モードを有効にする場合は、SSL が有効になっている必要があります。さらにキー リング証明書を作成するために、サーバ DNS 情報を使用する必要があります。

SSL を LDAP サーバエントリに対して有効にすると、接続の形成時にキー リング情報が参照され、確認されます。

LDAP サーバ情報は、セキュア LDAP 接続 (SSL 使用可能) 用の、CC モードの DNS 情報である必要があります。

セキュア LDAP クライアントのキー リング証明書を設定するには、次の手順を実行します。

### 手順

**ステップ 1** FXOS CLI から、セキュリティ モードに入ります。

**scope security**

ステップ2 LDAP モードに入ります。

**scope ldap**

ステップ3 LDAP サーバモードに入ります。

```
enter server {server_ip|server_dns}
```

ステップ4 LDAP キーリングを設定します。

```
set keyring keyring_name
```

ステップ5 設定をコミットします。

```
commit-buffer
```

## クライアント証明書認証の有効化

HTTPS アクセスのユーザを認証するために、システムにクライアント証明書を LDAP と一緒に使用させることができます。Firepower 4100/9300 シャーシ上でのデフォルトの認証設定は、認証ベースです。



(注) 証明書認証が有効である場合、これは HTTPS に許可されている唯一の認証形式です。証明書失効検査は、FXOS 2.1.1 リリースのクライアント証明書認証機能ではサポートされていません。

この機能を使用するには、クライアント証明書が次の要件を満たしている必要があります。

- ユーザ名が X509 属性 [Subject Alternative Name - Email] に含まれている必要があります。
- クライアント証明書は、その証明書をスーパーバイザ上のトラストポイントにインポートしているルート CA により署名されている必要があります。

### 手順

ステップ1 FXOS CLI から、サービス モードに入ります。

```
scope system
```

```
scope services
```

ステップ2 (任意) HTTPS 認証のオプションを表示します。

```
set https auth-type
```

例：

```
Firepower-chassis /system/services # set https auth-type  
cert-auth Client certificate based authentication  
cred-auth Credential based authentication
```

**ステップ3** HTTPS 認証をクライアントベースに設定します。

**set https auth-type cert-auth**

**ステップ4** 設定をコミットします。

**commit-buffer**

---



## 第 7 章

# システム管理

---

- セッション変更により Firepower Chassis Manager セッションが閉じる場合 (71 ページ)
- 管理 IP アドレスの変更 (72 ページ)
- アプリケーション管理 IP の変更 (74 ページ)
- Firepower 4100/9300 シャーシ名の変更 (77 ページ)
- ログイン前バナー (78 ページ)
- Firepower 4100/9300 シャーシの再起動 (81 ページ)
- Firepower 4100/9300 シャーシの電源オフ (81 ページ)
- 工場出荷時のデフォルト設定の復元 (81 ページ)
- トラスト ID 証明書のインストール (82 ページ)

## セッション変更により Firepower Chassis Manager セッションが閉じる場合

次のようにシステムを変更すると、自動的に Firepower Chassis Manager からログアウトする可能性があります。

- 10 分を超えてシステム時刻を変更した場合。
- Firepower Chassis Manager または FXOS CLI を使用してシステムを再起動またはシャットダウンした場合。
- Firepower 4100/9300 シャーシ上の FXOS のバージョンをアップグレードした場合。
- FIPS またはコモンクライテリアモードを有効または無効にした場合。



- (注) 上記の変更に加えて、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します。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 \(35 ページ\)](#) 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 \(36 ページ\)](#) を参照してください。

## 管理 IP アドレスの変更

### 始める前に

FXOS CLI から Firepower 4100/9300 シャーシの管理 IP アドレスを変更できます。



- (注) 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

### 手順

**ステップ 1** FXOS CLI に接続します ([FXOS CLI へのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

- a) fabric-interconnect a のスコープを設定します。

```
Firepower-chassis# scope fabric-interconnect a
```

- b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。

```
Firepower-chassis /fabric-interconnect # show
```

- c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

```
Firepower-chassis /fabric-interconnect # set out-of-band ip ip_address netmask network_mask gw gateway_ip_address
```

- d) トランザクションをシステム設定にコミットします。

```
Firepower-chassis /fabric-interconnect* # commit-buffer
```

**ステップ 3** IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

- a) fabric-interconnect a のスコープを設定します。

```
Firepower-chassis# scope fabric-interconnect a
```

- b) 管理 IPv6 設定のスコープを設定します。

```
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

- c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```

- d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 ipv6_address ipv6-prefix  
prefix_length ipv6-gw gateway_address
```

- e) トランザクションをシステム設定にコミットします。

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
```

## 例

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a  
Firepower-chassis /fabric-interconnect # show
```

```
Fabric Interconnect:
```

ID	OOB IP Addr	OOB Gateway	OOB Netmask	OOB IPv6 Address	OOB IPv6 Gateway
A	192.0.2.112	192.0.2.1	255.255.255.0	::	::
64	Operable				

```
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask  
255.255.255.0 gw 192.0.2.1  
Warning: When committed, this change may disconnect the current CLI session  
Firepower-chassis /fabric-interconnect* #commit-buffer  
Firepower-chassis /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a  
Firepower-chassis /fabric-interconnect # scope ipv6-config  
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```

```
Management IPv6 Interface:
```

IPv6 Address	Prefix	IPv6 Gateway
2001::8998	64	2001::1

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999  
ipv6-prefix 64 ipv6-gw 2001::1  
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer  
Firepower-chassis /fabric-interconnect/ipv6-config #
```

# アプリケーション管理 IP の変更

FXOS CLI から Firepower 4100/9300 シャーシに接続されたアプリケーションの管理 IP アドレスは変更できます。そのためには、まず FXOS プラットフォーム レベルで IP 情報を変更し、次にアプリケーション レベルで IP 情報を変更する必要があります。



- (注) Firepower Chassis Manager を使用してこれらの変更を行おうとすると、サービスが中断される可能性があります。サービスが中断する可能性を避けるために、これらの変更は、FXOS CLI を使用して実行する必要があります。

## 手順

**ステップ 1** FXOS CLI に接続します。（[FXOS CLI へのアクセス \(10 ページ\)](#) を参照）。

**ステップ 2** 範囲を論理デバイスにします。

**scope ssa**

**scope logical-device** *logical\_device\_name*

**ステップ 3** 範囲を管理ブートストラップにし、新しい管理ブートストラップパラメータを設定します。導入間で違いがあることに注意してください。

ASA 論理デバイスのスタンドアロンの設定の場合。

- a) 論理デバイスのブートストラップに入ります。

**scope mgmt-bootstrap** *asa*

- b) スロットを IP モードにします。

**scope ipv4\_or\_6 slot\_number** *default*

- c) (IPv4 のみ) 新しい IP アドレスを設定します。

**set ip** *ipv4\_address* **mask** *network\_mask*

- d) (IPv6 のみ) 新しい IP アドレスを設定します。

**set ip** *ipv6\_address* **prefix-length** *prefix\_length\_number*

- e) ゲートウェイ アドレスを設定します。

**set gateway** *gateway\_ip\_address*

- f) 設定をコミットします。

**commit-buffer**

ASA 論理デバイスのクラスタ設定の場合。

- a) クラスタ管理ブートストラップに入ります。

**scope cluster-bootstrap asa**

- b) (IPv4 のみ) 新しい仮想 IP を設定します。  
**set virtual ipv4 ip\_address mask network\_mask**
- c) (IPv6 のみ) 新しい仮想 IP を設定します。  
**set virtual ipv6 ipv6\_address prefix-length prefix\_length\_number**
- d) 新しい IP プールを設定します。  
**set ip pool start\_ip end\_ip**
- e) ゲートウェイ アドレスを設定します。  
**set gateway gateway\_ip\_address**
- f) 設定をコミットします。  
**commit-buffer**

Firepower Threat Defense のスタンドアロン設定およびクラスタ設定の場合。

- a) 論理デバイスのブートストラップに入ります。  
**scope mgmt-bootstrap ftd**
- b) スロットを IP モードにします。  
**scope ipv4\_or\_6 slot\_number firepower**
- c) (IPv4 のみ) 新しい IP アドレスを設定します。  
**set ip ipv4\_address mask network\_mask**
- d) (IPv6 のみ) 新しい IP アドレスを設定します。  
**set ip ipv6\_address prefix-length prefix\_length\_number**
- e) ゲートウェイ アドレスを設定します。  
**set gateway gateway\_ip\_address**
- f) 設定をコミットします。  
**commit-buffer**

(注) クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに新しい IP アドレスを設定する必要があります。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

**ステップ 4** アプリケーションごとに管理ブートストラップ情報をクリアします。

- a) 範囲を ssa モードにします。  
**scope ssa**
- b) 範囲をスロットにします。

**scope slot** *slot\_number*

- c) 範囲をアプリケーションインスタンスにします。

**scope app-instance** *asa\_or\_ftd*

- d) 管理ブートストラップ情報をクリアします。

**clear mgmt-bootstrap**

- e) 設定をコミットします。

**commit-buffer**

**ステップ 5** アプリケーションを無効にします。

**disable**

**commit-buffer**

- (注) クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに管理ブートストラップ情報をクリアし、無効にする必要があります。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

**ステップ 6** アプリケーションがオフラインで、スロットが再度オンラインになったときに、アプリケーションを再度有効にします。

- a) 範囲を ssa モードに戻します。

**scope ssa**

- b) 範囲をスロットにします。

**scope slot** *slot\_number*

- c) 範囲をアプリケーションインスタンスにします。

**scope app-instance** *asa\_or\_ftd*

- d) アプリケーションを有効にします。

**enable**

- e) 設定をコミットします。

**commit-buffer**

- (注) クラスタ設定の場合、これらのステップを繰り返して、Firepower 4100/9300 シャーシに接続されている各アプリケーションを再度有効にします。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

# Firepower 4100/9300 シャーシ名の変更

## 始める前に

Firepower 4100/9300 シャーシに使用する名前を FXOS CLI から変更することができます。

## 手順

**ステップ 1** FXOS CLI に接続します ([FXOS CLI へのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** システム モードに入ります。

```
Firepower-chassis-A# scope system
```

**ステップ 3** 現在の名前を表示します。

```
Firepower-chassis-A /system # show
```

**ステップ 4** 新しい名前を構成します。

```
Firepower-chassis-A /system # set name device_name
```

**ステップ 5** トランザクションをシステム設定にコミットします。

```
Firepower-chassis-A /fabric-interconnect* # commit-buffer
```

## 例

次の例では、デバイス名を変更します。

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show
```

```
Systems:
  Name           Mode           System IP Address System IPv6 Address
  -----
  New-name       Stand Alone   192.168.100.10   ::
New-name-A /system #
```

## ログイン前バナー

ログイン前バナーでは、ユーザが Firepower Chassis Manager にログインするとシステムにバナーテキストが表示されます。ユーザ名とパスワードのシステムプロンプトの前に、メッセージの画面で [OK] をクリックする必要があります。ログイン前バナーを設定しないと、システムはユーザ名とパスワードのプロンプトにすぐに進みます。

ユーザが FXOS CLI にログインすると、設定されている場合はシステムがパスワードのプロンプトの前にログインバナーテキストを表示します。

## ログイン前バナーの作成

### 手順

---

**ステップ 1** FXOS CLI に接続します ([FXOS CLI へのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** セキュリティ モードを開始します。

```
Firepower-chassis# scope security
```

**ステップ 3** バナー セキュリティ モードに入ります。

```
Firepower-chassis /security # scope banner
```

**ステップ 4** 次のコマンドを入力して、ログイン前バナーを作成します。

```
Firepower-chassis /security/banner # create pre-login-banner
```

**ステップ 5** Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。

```
Firepower-chassis /security/banner/pre-login-banner* # set message
```

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

**ステップ 6** プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで **Enter** キーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[set message] ダイアログをキャンセルするには、**Ctrl+C** キーを押します。

**ステップ 7** トランザクションをシステム設定にコミットします。

```
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
```

---

## 例

次の例は、ログイン前バナーを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

# ログイン前バナーの変更

## 手順

**ステップ 1** FXOS CLI に接続します ([FXOS CLIへのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** セキュリティ モードを開始します。

```
Firepower-chassis# scope security
```

**ステップ 3** バナー セキュリティ モードに入ります。

```
Firepower-chassis /security # scope banner
```

**ステップ 4** ログイン前バナーのバナー セキュリティ モードに入ります。

```
Firepower-chassis /security/banner # scope pre-login-banner
```

**ステップ 5** Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。

```
Firepower-chassis /security/banner/pre-login-banner # set message
```

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

**ステップ 6** プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで **Enter** キーを押します。

入力内容の次の行に **ENDOFBUF** と入力し、**Enter** キーを押して終了します。

[set message] ダイアログをキャンセルするには、**Ctrl+C** キーを押します。

**ステップ 7** トランザクションをシステム設定にコミットします。

```
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
```

**例**

次に、ログイン前バナーを変更する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

## ログイン前バナーの削除

**手順**

**ステップ 1** FXOS CLI に接続します ([FXOS CLIへのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** セキュリティ モードを開始します。

```
Firepower-chassis# scope security
```

**ステップ 3** バナー セキュリティ モードに入ります。

```
Firepower-chassis /security # scope banner
```

**ステップ 4** システムからログイン前バナーを削除します。

```
Firepower-chassis /security/banner # delete pre-login-banner
```

**ステップ 5** トランザクションをシステム設定にコミットします。

```
Firepower-chassis /security/banner* # commit-buffer
```

**例**

次に、ログイン前バナーを削除する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

## Firepower 4100/9300 シャーシの再起動

### 手順

- ステップ 1 [Overview] を選択して、[Overview] ページを開きます。
- ステップ 2 [Overview] ページの右上隅の [Chassis Uptime] の横にある [Reboot] をクリックします。
- ステップ 3 [Yes] をクリックして、Firepower 4100/9300 シャーシを電源オフを確認します。  
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにして再始動する前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。このプロセスには約 15 ～ 20 分かかります。

## Firepower 4100/9300 シャーシの電源オフ

### 手順

- ステップ 1 [Overview] を選択して、[Overview] ページを開きます。
- ステップ 2 [Overview] ページの右上隅の [Chassis Uptime] の横にある [Shutdown] をクリックします。
- ステップ 3 [Yes] をクリックして、Firepower 4100/9300 シャーシを電源オフを確認します。  
システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにする前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。

## 工場出荷時のデフォルト設定の復元

FXOS CLI を使用して Firepower 4100/9300 シャーシを工場出荷時のデフォルト設定に戻すことができます。



- (注) このプロセスによって、論理デバイス設定を含むすべてのユーザ設定がシャーシから消去されます。この手順が完了したら、Firepower 4100/9300 シャーシのコンソールポートに接続し、セットアップウィザードを使用してシステムを再設定する必要があります ([初期設定 \(6 ページ\)](#) を参照してください)。

## 手順

**ステップ 1** (任意) **erase configuration** コマンドはシャーシからスマート ライセンス設定を削除しません。スマート ライセンス設定も削除する場合は、次の手順を実行します。

**scope license**

**deregister**

Firepower 4100/9300 シャーシの登録を解除すると、アカウントからデバイスが削除されます。デバイスのすべてのライセンス資格と証明書が削除されます。

**ステップ 2** ローカル管理に接続します。

**connect local-mgmt**

**ステップ 3** Firepower 4100/9300 シャーシからすべてのユーザ設定を消去し、最初の工場出荷時のデフォルト設定にシャーシを復元するには、次のコマンドを入力します。

**erase configuration**

すべてのユーザ設定を消去するかどうかを確認するように求められます。

**ステップ 4** 設定の消去を確認するには、コマンドプロンプトに **yes** と入力します。

すべてのユーザ設定が Firepower 4100/9300 シャーシから消去された後、システムがリブートします。

# トラス ID 証明書のインストール

初期設定後に、自己署名 SSL 証明書が Firepower 4100/9300 シャーシ Web アプリケーションで使用するために生成されます。その証明書は自己署名であるため、クライアントブラウザが自動的に信頼することはありません。新しいクライアントブラウザで Firepower 4100/9300 シャーシ Web インターフェイスに初めてアクセスするときに、ブラウザは SSL 警告をスローして、ユーザが Firepower 4100/9300 シャーシにアクセスする前に証明書を受け入れることを要求します。FXOS CLI を使用して証明書署名要求 (CSR) を生成し、Firepower 4100/9300 シャーシで使用する結果の ID 証明書をインストールするには、以下の手順を使用できます。この ID 証明書により、クライアントブラウザは接続を信頼し、警告なしで Web インターフェイスを起動できるようになります。

## 手順

**ステップ 1** FXOS CLI に接続します。( [FXOS CLIへのアクセス \(10 ページ\)](#) を参照)。

**ステップ 2** セキュリティ モジュールを入力します。

**scope security**

**ステップ 3** キーリングを作成します。

**create keyring *keyring\_name***

**ステップ 4** 秘密キーのモジュラス サイズを設定します。

**set modulus *size***

**ステップ 5** 設定をコミットします。

**commit-buffer**

**ステップ 6** CSR フィールドを設定します。証明書は、基本オプション (**subject-name** など) を指定して生成できます。さらに任意で、ロケールや組織などの情報を証明書に組み込むことができる詳細オプションを指定できます。CSR フィールドを設定する場合、システムにより証明書パスワードの入力が求められることに注意してください。

**create certreq *certreq subject\_name****password***set country *country*****set state *state*****set locality *locality*****set org-name *organization\_name*****set org-unit-name *organization\_unit\_name*****set subject-name *subject\_name***

**ステップ 7** 設定をコミットします。

**commit-buffer**

**ステップ 8** 認証局に提供する CSR をエクスポートします。認証局は CSR を使用して ID 証明書を作成します。

a) 完全な CSR を表示します。

**show certreq**

b) 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までの出力をコピーします。

**例 :**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbG1mb3JuaWEEx
ETAPBgNVBACMFNhbWVhbnRlbnR5YFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMzQwYzYy
VQQLDANUQUxvZGJAYBgNVBAMMEWZwNDYyMC50ZXN0LmxyY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDLShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYmGhbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIZOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KozIhvcNAQkOMSAwHjAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAAZUfCbwx9vt5aVdCL+tATu5xFE3LA310ck6j1Nv6W/6r
jBNLxusYilrZzcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ10Ikyx3RzEjgK0
zzyoyrG+EZX5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLz5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
```

```
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ21DXjExp7rCx9
+6bvD1ln70JCegHdCWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

**ステップ 9** certreq モードを終了します。

**exit**

**ステップ 10** キーリング モードを終了します。

**exit**

**ステップ 11** 認証局の登録プロセスに従って認証局に CSR の出力を提供します。要求が成功すると、認証局はこの CA の秘密キーを使用してデジタル署名された ID 証明書が返されます。

**ステップ 12** (注) FXOS にインポートするすべての ID 証明書は、Base64 形式でなければなりません。認証局から受信した ID 証明書チェーンの形式が多様である場合は、まずそれを OpenSSL などの SSL ツールを使用して変換する必要があります。

ID 証明書チェーンを保持する新規トラストポイントを作成します。

**create trustpoint** *trustpoint\_name*

**ステップ 13** 画面の指示に従って、手順 11 で認証局から受信した ID 証明書チェーンを入力します。

(注) 中間証明書を使用する認証局の場合は、ルートと中間証明書とを結合させる必要があります。テキストファイルで、ルート証明書を一番上にペーストし、それに続いてチェーン内の各中間証明書をペーストします。この場合、すべての BEGIN CERTIFICATE フラグと END CERTIFICATE フラグを含めます。この全体のテキストブロックを、トラストポイントにコピーアンドペーストします。

**set certchain**

例：

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkJOPQQDAjBTMRUw
>EwYKCZImiZPyLGBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmfhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjUwNzI4MTc1NjU2
>WhcNMjUwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmfhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkJOPQIBBggqhkJOPQMBBwNCAASvEA27V1Enq1gMtLkVJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUKm1xmqlubaDHPJ5TMGFJQYszLBRJPq+mdrKcDl
>o2kwZzATBgrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYh1sv1gCxsQV0w0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

**ステップ 14** 設定をコミットします。

**commit-buffer**

**ステップ 15**    トラストポイント モードを終了します。

**exit**

**ステップ 16**    キーリング モードに入ります。

**scope keyring** *keyring\_name*

**ステップ 17**    ステップ 13 で作成されたトラストポイントを、CSR に作成されたキーリングに関連付けます。

**set trustpoint** *trustpoint\_name*

**ステップ 18**    サーバの署名付き ID 証明書をインポートします。

**set cert**

**ステップ 19**    認証局により提供された ID 証明書の内容をペーストします。

例 :

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQDDAjbBT
>MRUwEwYKCZImiZPyLQGGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bJEGMB4GA1UEAxMXbmfhdXN0aW4tTkFBVVNUSU4tUEMtdQ0EwHhcNMjYwNDI4MTMw
>OTU0WhcNMjYwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMjQ2F5
>aWZvcms5pYTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXNxDAAKBgNVBAsTA1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
>BwdudS3sulXIwKGco48mMHCQRw1ADWZCxFANxsnfb+wR8xKfKo4vwnMLuK3F5U
>R1HLPv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XafslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8D1ZWcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIAxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtdQ0EesQ049bmFhdXN0aW4tcmMsQ049Q0RQLENOFVB1
>YmXpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3V5YXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldG1vb1BvaW50MIHMBGgrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdG1uLU5B
>QVVVVE10LVBDLUNBLENOFUFJQSxDTj1QdWJsaW1mJmJmJmJmJmJmJmJmJmJmJmJm
>Tj1TZXJ2aWN1cyxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdG1uLERDPWxvY2Fs
>P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzZz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAUgQUHhIAVwB1AGIAUwB1AHIAAdgB1AHIAWdYDVR0P
>AQH/BAQDAgWgMBMGAlUdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0GAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNuU/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

**ステップ 20**    キーリング モードを終了します。

**exit**

**ステップ 21**    セキュリティ モードを終了します。

**exit**

**ステップ 22** システム モードに入ります。

**scope system**

**ステップ 23** サービス モードに入ります。

**scope services**

**ステップ 24** 新しい証明書を使用するように FXOS Web サービスを設定します。

**set https keyring *keyring\_name***

**ステップ 25** 設定をコミットします。

**commit-buffer**

**ステップ 26** HTTPS サーバに関連付けられているキーリングを表示します。これにはこの手順の手順 3 で作成したキーリングの名前が反映されることとなります。画面出力にデフォルトのキーリング名が表示される場合には、HTTPS サーバはまだ、新しい証明書を使用するように更新されていません。

**show https**

例：

```
fp4120 /system/services # show https
Name: https
  Admin State: Enabled
  Port: 443
  Operational port: 443
  Key Ring: firepower_cert
  Cipher suite mode: Medium Strength
  Cipher suite:
ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

**ステップ 27** インポートされた証明書の内容を表示し、**Certificate Status**値が**Valid**と表示されることを確認します。

**scope security**

**show keyring *keyring\_name* detail**

例：

```
fp4120 /security # scope security
fp4120 /security # show keyring firepower_cert detail
Keyring firepower_cert:
  RSA key modulus: Mod2048
  Trustpoint CA: firepower_chain
Certificate status: Valid
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
  Validity
    Not Before: Apr 28 13:09:54 2016 GMT
    Not After : Apr 28 13:09:54 2018 GMT
  Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
```

```

CN=fp4120.test.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
        0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
        a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
        50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
        fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
        d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
        3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
        a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
        9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
        20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
        ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
        87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
        07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
        47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
        cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
        5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
        d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
        1d:85
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Alternative Name:
      DNS:fp4120.test.local
    X509v3 Subject Key Identifier:
      FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
    X509v3 Authority Key Identifier:
      keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
    X509v3 CRL Distribution Points:
      Full Name:
        URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
          CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Authority Information Access:
    CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
      CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
      DC=local?cACertificate?base?objectClass=certificationAuthority
    1.3.6.1.4.1.311.20.2:
      ..W.e.b.S.e.r.v.e.r
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Server Authentication
  Signature Algorithm: ecdsa-with-SHA256
    30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
    e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
    02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
    2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQQAjBT
MRUwEwYKcZImiZPyLGQBGryFbG9jYWwxGDABWgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmfhdXN0aW44tTtkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMkQ2Fs
aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBAOTDUNpc2NvIFN5c3Rl
bXN0aW44bG9uYVBAaTA1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWFwYXN0
MA0GCSqGSIb3DQEBBQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
BwdudS3sulXIwKGo48mMHCRCw1ADWZCxFANxsnbfb+wrR8xKFKo4vvnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZcZrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67Yoyig9WrvqZObwHBg

```

```

yodsks/g+a5GNYTzzIS9XAFs1MSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGaa2H109XR2FAGMB
AAGjggJYMIICVDAcBgNVHREFFtATghFmcDQxMjAudGVzdc5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8D1ZWcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVWVNUU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmXpYyUyMETleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGV5ZXZvY2F0aW9uTG1z
dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMM1MjBLZXk1MjBTZXJ2aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDdbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAQQUHhIAVwBlAGIAUwBlAHIAAdgBlAHIdGyYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCcGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNuU/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

```

Zeroized: No

## 次のタスク

新しい信頼できる証明書が存在していることを確認するには、Web ブラウザのアドレス バーに `https://<FQDN_or_IP>/` と入力して、Firepower Chassis Manager に移動します。



- (注) ブラウザはさらに、アドレス バーの入力内容に照らして証明書のサブジェクト名を確認します。証明書が完全修飾ドメイン名に対して発行されている場合、ブラウザでもそのようにアクセスする必要があります。IP アドレスを使用してアクセスすると、信頼できる証明書が使用されているとしても、別の SSL エラー（共通名が無効）がスローされます。



## 第 8 章

# Platform Settings

- NTP サーバ認証の有効化 (89 ページ)
- 日時の設定 (90 ページ)
- SSH の設定 (93 ページ)
- TLS の設定 (94 ページ)
- Telnet の設定 (96 ページ)
- SNMP の設定 (97 ページ)
- HTTPS の設定 (106 ページ)
- AAA の設定 (118 ページ)
- Syslog の設定 (128 ページ)
- DNS サーバの設定 (131 ページ)
- FIPS モードの有効化 (132 ページ)
- コモンクライテリアモードの有効化 (133 ページ)
- IP アクセスリストの設定 (133 ページ)

## NTP サーバ認証の有効化

NTP サーバ認証を有効にするには、Firepower 4100/9300 シャーシで次の手順を実行します。



- (注)
- 有効にすると、NTP 認証機能は設定済みのすべてのサーバでグローバルに機能します。
  - NTP サーバ認証では SHA1 のみがサポートされます。
  - サーバを認証するには、キー ID とキー値が必要です。キー ID は、メッセージダイジェストのコンピューティング時に、使用するキー値をクライアントとサーバの両方に指示するために使用されます。キー値は、`ntp-keygen` を使用して導出される固定値です。

## 手順

- 
- ステップ 1 ntp 4.2.8p8 をダウンロードします。
  - ステップ 2 NTP サーバを、**ntpd openssl** を有効にしてインストールします。
  - ステップ 3 NTP キー ID とキー値を生成します。

**ntp-keygen -M**

これらの生成されたキーは、次の手順に使用します。

- ステップ 4 Firepower 4100/9300 シャーシに管理者ユーザとしてログインします。
  - ステップ 5 **Platform Settings** を選択して、[Platform Settings] ウィンドウを開きます。
  - ステップ 6 [Set Time Source] 領域で、**Use NTP server** ラジオ ボタンをクリックします。
  - ステップ 7 生成された SHA1 文字列とキーで NTP サーバを追加します。
  - ステップ 8 **Save** をクリックして、NTP サーバ設定を保存します。
  - ステップ 9 **Enable ntp-authentication** チェックボックスをオンにします。
  - ステップ 10 **Save** をクリックします。
- 

## 日時の設定

日付と時刻を手動で設定したり、現在のシステム時刻を表示するには、下記で説明する [NTP] ページのシステムのネットワーク タイム プロトコル (NTP) を設定します。

NTP の設定は、Firepower 4100/9300 シャーシとシャーシにインストールされている論理デバイス間で自動的に同期されます。



- 
- (注) Firepower 4100/9300 シャーシに Firepower Threat Defense を導入すると、スマートライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように Firepower 4100/9300 シャーシに NTP を設定する必要があります。Firepower 4100/9300 シャーシと Firepower Management Center に同じ NTP サーバを使用する必要があります。
- 

NTP を使用すると、[Current Time] タブの全体的な同期ステータスを表示できます。または、[Time Synchronization] タブの [NTP Server] テーブルの [Server Status] フィールドを見ると、設定済みの各 NTP サーバの同期ステータスを表示できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

## 設定された日付と時刻の表示

### 手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Current Time] タブをクリックします。

システムは、デバイスに設定された日付、時刻、タイムゾーンを表示します。

NTP を使用している場合、[Current Time] タブに総合的な同期ステータスを表示することもできます。設定済みの各 NTP サーバの同期ステータスは、[Time Synchronization] タブにある **NTP サーバ** テーブルの [Server Status] フィールドを見て確認できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

## タイムゾーンの設定

### 手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Current Time] タブをクリックします。

ステップ 3 [Time Zone] ドロップダウンリストから、Firepower シャーシの適切なタイムゾーンを選択します。

## NTP を使用した日付と時刻の設定

NTP を利用して階層的なサーバシステムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイムスタンプを含む場合など、時刻が重要な操作で必要になります。最大 4 台の NTP サーバを設定できます。



(注) FXOS 2.2(2) 以降では NTP バージョン 3 を使用します。

### 手順

ステップ 1 [Platform Settings] > [NTP] を選択します。

ステップ 2 [Time Synchronization] タブをクリックします。

**ステップ 3** [Set Time Source] で、[Use NTP Server] をクリックします。

**ステップ 4** 使用する NTP サーバ（最大 4 台）ごとに、それぞれの IP アドレスまたはホスト名を [NTP Server] フィールドに入力し、[Add] をクリックします。

**ステップ 5** [Save] をクリックします。

Firepower シャーシが、指定した NTP サーバ情報で設定されます。

各サーバの同期ステータスは、**NTP サーバ** テーブルの [Server Status] フィールドを見て確認できます。システムが特定の NTP サーバと同期できない場合、[Server Status] の横にある情報アイコンにカーソルを合わせると詳細を確認できます。

(注) システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

---

## NTP サーバの削除

### 手順

---

**ステップ 1** [Platform Settings] > [NTP] を選択します。

**ステップ 2** [Time Synchronization] タブをクリックします。

**ステップ 3** 削除する各 NTP サーバに対して、**NTP サーバ** テーブルでそのサーバの [Delete] アイコンをクリックします。

**ステップ 4** [Save] をクリックします。

---

## 手動での日付と時刻の設定

ここでは、Firepower シャーシで日付と時刻を手動で設定する方法について説明します。

### 手順

---

**ステップ 1** [Platform Settings] > [NTP] を選択します。

**ステップ 2** [Time Synchronization] タブをクリックします。

**ステップ 3** [Set Time Source] で、[Set Time Manually] をクリックします。

**ステップ 4** [Date] ドロップダウンリストをクリックしてカレンダーを表示し、カレンダーで使用できるコントロールを使って日付を設定します。

**ステップ 5** 時、分、および AM/PM のそれぞれのドロップダウン リストを使用して時間を指定します。

ヒント [Get System Time] をクリックすると、Firepower Chassis Manager への接続に使用するシステムの設定に一致する日付と時刻を設定できます。

**ステップ 6** [Save] をクリックします。

指定した日付と時刻が Firepower シャーシに設定されます。

(注) システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Firepower Chassis Manager への再ログインが必要になります。

## SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効または無効にする方法、および FXOS シャーシを SSH クライアントとして有効にする方法について説明します。SSH はデフォルトでイネーブルになります。

### 手順

**ステップ 1** [Platform Settings] > [SSH] > [SSH Server] を選択します。

**ステップ 2** Firepower シャーシへの SSH アクセスを有効化するには、[Enable SSH] チェックボックスをオンにします。SSH アクセスをディセーブルにするには、[Enable SSH] チェックボックスをオフにします。

**ステップ 3** サーバの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

(注) コモンクライテリアでは 3des-cbc がサポートされていません。FXOS シャーシでコモンクライテリア モードが有効な場合、暗号化アルゴリズムとして 3des-cbc を使用することはできません。

**ステップ 4** サーバの [Key Exchange Algorithm] として、許可される Diffie-Hellman (DH) キー交換ごとにチェックボックスをオンにします。DH キー交換は、いずれの当事者も単独では決定できない共有秘密を提供します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用の詳細については、RFC 4253 を参照してください。

**ステップ 5** サーバの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

**ステップ 6** サーバの [Host Key] について、RSA キー ペアのモジュラス サイズを入力します。

モジュラス値 (ビット単位) は、1024 ~ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいくほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

**ステップ 7** サーバの [Volume Rekey Limit] に、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

- ステップ 8** サーバの [Time Rekey Limit] では、FXOS がセッションを切断する前に SSH セッションがアイドル状態を続けられる長さを分単位で設定します。
- ステップ 9** [Save] をクリックします。
- ステップ 10** [SSH Client] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。
- ステップ 11** [Strict Host Keycheck] について、[enable]、[disable]、または [prompt] を選択して、SSH ホストキー チェックを制御します。
- **enable** : FXOS が認識するホストファイルにそのホストキーがまだ存在しない場合、接続は拒否されます。FXOS CLI でシステム スコープまたはサービス スコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
  - **prompt** : シャーシにまだ保存されていないホストキーを許可または拒否するように求められます。
  - **disable** : (デフォルト) シャーシは過去に保存されたことがないホストキーを自動的に許可します。
- ステップ 12** クライアントの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。
- (注) コモンクライテリアでは **3des-cbc** がサポートされていません。FXOS シャーシでコモンクライテリア モードが有効な場合、暗号化アルゴリズムとして **3des-cbc** を使用することはできません。
- ステップ 13** クライアントの [Key Exchange Algorithm] について、許可される Diffie-Hellman (DH) キー交換ごとにチェックボックスをオンにします。DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用の詳細については、RFC 4253 を参照してください。
- ステップ 14** クライアントの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。
- ステップ 15** クライアントの [Volume Rekey Limit] に、FXOS がセッションを切断する前にその接続で許可されるトラフィックの量を KB 単位で設定します。
- ステップ 16** クライアントの [Time Rekey Limit] について、FXOS がセッションを切断する前に SSH セッションがアイドルであることができる時間を分単位で設定します。
- ステップ 17** [Save] をクリックします。

## TLS の設定

Transport Layer Security (TLS) プロトコルは、互いに通信する 2 つのアプリケーションの間でプライバシーとデータの整合性を確保します。FXOS シャーシと外部デバイスとの通信で許容する最小 TLS バージョンは、FXOS CLI を使用して設定できます。新しいバージョンの TLS で

は通信のセキュリティを強化できる一方、古いバージョンの TLS では古いアプリケーションとの後方互換性を維持できます。

たとえば、FXOS シャーシで設定されている最小 TLS バージョンが v1.1 の場合、クライアントブラウザが v1.0 だけを実行するように設定されていると、クライアントは HTTPS を使用して FXOS Chassis Manager との接続を開くことができません。したがって、ピアアプリケーションと LDAP サーバを適切に設定する必要があります。

次の手順で、FXOS シャーシと外部デバイス間の通信で許容する最小 TLS バージョンを設定、表示する方法を説明します。



- (注) **• FXOS 2.3(1) リリースの時点では、FXOS シャーシのデフォルト最小 TLS バージョンは v1.1 です。**

### 手順

**ステップ 1** システム モードに入ります。

```
Firepower-chassis# scope system
```

**ステップ 2** システムで使用できる TLS バージョンのオプションを表示します。

```
Firepower-chassis /system # set services tls-ver
```

例 :

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver
v1_0 v1.0
v1_1 v1.1
v1_2 v1.2
```

**ステップ 3** 最小 TLS バージョンを設定します。

```
Firepower-chassis /system # set services tls-ver version
```

例 :

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver v1_2
```

**ステップ 4** 設定をコミットします。

```
Firepower-chassis /system # commit-buffer
```

**ステップ 5** システムで設定されている最小 TLS バージョンを表示します。

```
Firepower-chassis /system # scope services
```

```
Firepower-chassis /system/services # show
```

例 :

```
Firepower-chassis /system/services # show
Name: ssh
```

```

Admin State: Enabled
Port: 22
Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1
Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256
Encrypt Algo: 3des Cbc,Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Ae
s192 Ctr
Auth Algo: Rsa
Host Key Size: 2048
Volume: None Time: None
Name: telnet
Admin State: Disabled
Port: 23
Name: https
Admin State: Enabled
Port: 443
Operational port: 443
Key Ring: default
Cipher suite mode: Medium Strength
Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU
M:+EXP:+eNULL
Https authentication type: Cert Auth
Crl mode: Relaxed
TLS:
TLS version: v1.2

```

## Telnet の設定

次の手順では、Firepower シャーシへの Telnet アクセスを有効化またはディセーブルにする方法について説明します。Telnet はデフォルトでディセーブルです。



(注) 現在は、CLI を使用した Telnet 設定のみ可能です。

### 手順

**ステップ 1** システム モードに入ります。

```
Firepower-chassis # scope system
```

**ステップ 2** システム サービス モードを開始します。

```
Firepower-chassis /system # scope services
```

**ステップ 3** Firepower シャーシへの Telnet アクセスを設定するには、次のいずれかを実行します。

- Firepower シャーシへの Telnet アクセスを許可するには、次のコマンドを入力します。  
Firepower-chassis /system/services # **enable telnet-server**
- Firepower シャーシへの Telnet アクセスを禁止するには、次のコマンドを入力します。  
Firepower-chassis /system/services # **disable telnet-server**

**ステップ 4** トランザクションをシステム設定にコミットします。

```
Firepower /system/services # commit-buffer
```

#### 例

次に、Telnet を有効にし、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system  
Firepower-chassis /system # scope services  
Firepower-chassis /services # enable telnet-server  
Firepower-chassis /services* # commit-buffer  
Firepower-chassis /services #
```

## SNMP の設定

Firepower シャーシに簡易ネットワーク管理プロトコル (SNMP) を設定するには、[SNMP] ページを使用します。詳細については、次のトピックを参照してください。

## SNMP の概要

簡易ネットワーク管理プロトコル (SNMP) は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ** : SNMP を使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム。
- **SNMP エージェント** : Firepower シャーシ内のソフトウェア コンポーネントで、Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに送信します。Firepower シャーシには、エージェントと一連の MIB が含まれています。SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Firepower Chassis Manager または FXOS CLI で SNMP を有効にし、設定します。
- **管理情報ベース (MIB)** : SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。SNMP は次のように定義されています。

- RFC 3410 (<http://tools.ietf.org/html/rfc3410>)
- RFC 3411 (<http://tools.ietf.org/html/rfc3411>)

- RFC 3412 (<http://tools.ietf.org/html/rfc3412>)
- RFC 3413 (<http://tools.ietf.org/html/rfc3413>)
- RFC 3414 (<http://tools.ietf.org/html/rfc3414>)
- RFC 3415 (<http://tools.ietf.org/html/rfc3415>)
- RFC 3416 (<http://tools.ietf.org/html/rfc3416>)
- RFC 3417 (<http://tools.ietf.org/html/rfc3417>)
- RFC 3418 (<http://tools.ietf.org/html/rfc3418>)
- RFC 3584 (<http://tools.ietf.org/html/rfc3584>)

## SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Firepower シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Firepower シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコルデータユニット (PDU) でメッセージの受信を確認応答します。Firepower シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

## SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルは選択されたセキュリティ レベルと組み合わせられ、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限レベルは、開示されないようメッセージを保護する必要があるか、またはメッセージを認証する必要があるかどうかを決定します。サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- [noAuthNoPriv] : 認証なし、暗号化なし
- [authNoPriv] : 認証あり、暗号化なし
- [authPriv] : 認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ

レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

## SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 5: SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティストリング	未対応	コミュニティストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティストリング	未対応	コミュニティストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	なし	HMAC Secure Hash Algorithm (SHA) に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック連鎖 (CBC) DES (DES-56) 標準に基づいた認証を提供します。

## SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。SNMPv3 ユーザベースセキュリティモデル (USM) は SNMP メッセージレベルセキュリティを参照し、次のサービスを提供します。

- **メッセージの完全性**：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データシーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- **メッセージ発信元の認証**：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- **メッセージの機密性および暗号化**：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

## SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

### MIB のサポート

Firepower シャーシは MIB への読み取り専用アクセスをサポートします。

利用可能な特定の MIB の詳細とその入手場所については、『[Cisco FXOS MIB Reference Guide](#)』を参照してください。

### SNMPv3 ユーザの認証プロトコル

Firepower シャーシは、SNMPv3 ユーザの HMAC-SHA-96 (SHA) 認証プロトコルをサポートします。

### SNMPv3 ユーザの AES プライバシー プロトコル

Firepower シャーシは、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard (AES) を使用し、RFC 3826 に準拠しています。

プライバシーパスワード (priv オプション) では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効化して、SNMPv3 ユーザのプライバシーパスワードを含めると、Firepower シャーシはそのプライバシーパスワードを使用して 128 ビット AES キーを生成します。AES プライバシーパスワードは最小で 8 文字です。パスフレーズをクリアテキストで指定する場合、最大 64 文字を指定できます。

## SNMP のイネーブル化および SNMP プロパティの設定

### 手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] チェックボックス	SNMP が有効化かディセーブルか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
[Port] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルトポートは変更できません。

名前	説明
[Community/Username] フィールド	<p>SNMPv1 およびv2 のポーリングに使用するコミュニティ文字列。</p> <p>このフィールドは SNMP v3 には適用されないことに注意してください。</p> <p>1 ~ 32 文字の英数字文字列を入力します。@ (アットマーク)、\ (バックスラッシュ)、" (二重引用符)、? (疑問符) または空欄スペースは使用しないでください。デフォルトは <b>public</b> です。</p> <p>[Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ることに注意してください。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。</p>
[システム管理者名 (System Administrator Name) ] フィールド	<p>SNMP 実装の担当者の連絡先。</p> <p>電子メールアドレス、名前、電話番号など、255 文字までの文字列を入力します。</p>
[Location] フィールド	<p>SNMP エージェント (サーバ) が実行するホストの場所。</p> <p>最大 510 文字の英数字を入力します。</p>

ステップ 3 [Save] をクリックします。

#### 次のタスク

SNMP トラップおよびユーザを作成します。

## SNMP トラップの作成

#### 手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Traps] 領域で、[Add] をクリックします。

ステップ 3 [Add SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。

名前	説明
[Community/Username] フィールド	<p>Firepower シャーシが SNMP ホストに送信するトラップに含める SNMP v1 または v2 コミュニティ名あるいは SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。</p> <p>1 ～ 32 文字の英数字文字列を入力します。@ (アットマーク)、\ (バックスラッシュ)、" (二重引用符)、? (疑問符) または空欄スペースは使用しないでください。</p>
[Port] フィールド	<p>Firepower シャーシが SNMP ホストとのトラップの通信に使用するポート。</p> <p>1 ～ 65535 の整数を入力します。</p>
[Version] フィールド	<p>トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• V1</li> <li>• V2</li> <li>• V3</li> </ul>
[Type] フィールド	<p>バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Traps</li> <li>• nforms</li> </ul>
[v3 Privilege] フィールド	<p>バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Auth] : 認証あり、暗号化なし</li> <li>• [Noauth] : 認証なし、暗号化なし</li> <li>• [Priv] : 認証あり、暗号化あり</li> </ul>

**ステップ 4** [OK] をクリックして、[Add SNMP Trap] ダイアログボックスを閉じます。

**ステップ 5** [Save] をクリックします。

## SNMP トラップの削除

### 手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Traps] 領域で、削除するトラップに対応するテーブルの行の [Delete] アイコンをクリックします。

## SNMPv3 ユーザの作成

### 手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Users] 領域で、[Add] をクリックします。

ステップ 3 [Add SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字まで入力します。名前の先頭は文字である必要があります。有効な文字は、文字、数字、_ (アンダースコア) です。.(ピリオド)、@ (アットマーク)、- (ハイフン) も指定できます。
[Auth Type] フィールド	許可タイプ : <b>SHA</b>
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。

名前	説明
[Password] フィールド	<p>このユーザのパスワード。</p> <p>Firepower eXtensible Operating System では、次の要件を満たさないパスワードは拒否されます。</p> <ul style="list-style-type: none"> <li>• 8 ～ 80 文字を含む。</li> <li>• 含まれるのは、文字、数字、および次の文字のみです。 ~!@#%^&amp;*()_+{}[]\ :;'"&lt;&gt;./</li> <li>• 次の記号を含まない。\$ (ドル記号)、? (疑問符)、 「=」 (等号)。</li> <li>• 5 つ以上の異なる文字を含める必要があります。</li> <li>• 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約4～6回発生）、簡素化チェックに失敗します。</li> </ul> <p>(注) 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&amp;!21 はパスワードチェックに失敗しますが、abcd&amp;!25 は失敗しません。</p>
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[Privacy Password] フィールド	<p>このユーザのプライバシー パスワード。</p> <p>Firepower eXtensible Operating System では、次の要件を満たさないパスワードは拒否されます。</p> <ul style="list-style-type: none"> <li>• 8 ~ 80 文字を含む。</li> <li>• 含まれるのは、文字、数字、および次の文字のみです。 ~!@#%^&amp;*()_+{}[]\;'"&lt;&gt;./</li> <li>• 次の記号を含まない。\$ (ドル記号)、? (疑問符)、 「=」 (等号)。</li> <li>• 5 つ以上の異なる文字を含める必要があります。</li> <li>• 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約4～6回発生）、簡素化チェックに失敗します。</li> </ul> <p>(注) 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&amp;!21 はパスワードチェックに失敗しますが、abcd&amp;!25 は失敗しません。</p>
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 4 [OK] をクリックして、[Add SNMP User] ダイアログボックスを閉じます。

ステップ 5 [Save] をクリックします。

## SNMPv3 ユーザの削除

### 手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP Users] 領域で、削除するユーザに対応するテーブルの行の [Delete] アイコンをクリックします。

# HTTPS の設定

ここでは、Firepower 4100/9300 シャーシで HTTPS を設定する方法を説明します。



(注) Firepower Chassis Manager または FXOS CLI を使用して HTTPS ポートを変更できます。他の HTTPS の設定はすべて、FXOS CLI を使用してのみ設定できます。

## 証明書、キーリング、トラストポイント

HTTPS は、公開キー インフラストラクチャ (PKI) を使用してクライアントのブラウザと Firepower 4100/9300 シャーシなどの 2 つのデバイス間でセキュアな通信を確立します。

### 暗号キーとキーリング

各 PKI デバイスは、内部キーリングに非対称の Rivest-Shamir-Adleman (RSA) 暗号キーのペア (1 つはプライベート、もう 1 つはパブリック) を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化 (「署名」とも呼ばれます) して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の場合は 512 ビット ~ 2048 ビットです。通常、長いキーは短いキーよりも安全です。FXOS では最初に 2048 ビットのキーペアを含むデフォルトのキーリングが提供されます。そして、追加のキーリングを作成できます。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキーリング証明書を手動で再生成する必要があります。

### 証明書

セキュアな通信を準備するには、まず 2 つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキーペアと独自の自己署名証明書を生成できます。リモートユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、FXOS にはデフォルトのキーリングからの公開キーを含む組み込みの自己署名証明書が含まれます。

### トラストポイント

FXOS に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース (つまり、トラストポイント) からサードパーティ証明書を取得し、インストールできます。サードパー

ティ証明書は、発行元トラストポイント（ルート認証局（CA）、中間CA、またはルートCA）につながるトラストチェーンの一部となるトラストアンカーのいずれか）によって署名されます。新しい証明書を取得するには、FXOSで証明書要求を生成し、トラストポイントに要求を送信する必要があります。



**重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

## キー リングの作成

FXOS は、デフォルト キー リングを含め、最大 8 個のキー リングをサポートします。

### 手順

**ステップ 1** セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

**ステップ 2** キー リングを作成し、名前を付けます。

```
Firepower-chassis # create keyring keyring-name
```

**ステップ 3** SSL キーのビット長を設定します。

```
Firepower-chassis # set modulus {mod1024 | mod1536 | mod2048 | mod512}
```

**ステップ 4** トランザクションをコミットします。

```
Firepower-chassis # commit-buffer
```

### 例

次の例は、1024 ビットのキー サイズのキー リングを作成します。

```
Firepower-chassis# scope security  
Firepower-chassis /security # create keyring kr220  
Firepower-chassis /security/keyring* # set modulus mod1024  
Firepower-chassis /security/keyring* # commit-buffer  
Firepower-chassis /security/keyring #
```

### 次のタスク

このキー リングの証明書要求を作成します。

## デフォルトキーリングの再生成

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキーリング証明書を手動で再生成する必要があります。

### 手順

---

**ステップ1** セキュリティモードを開始します。

```
Firepower-chassis # scope security
```

**ステップ2** デフォルトキーリングでキーリングセキュリティモードに入ります。

```
Firepower-chassis /security # scope keyring default
```

**ステップ3** デフォルトキーリングを再生成します。

```
Firepower-chassis /security/keyring # set regenerate yes
```

**ステップ4** トランザクションをコミットします。

```
Firepower-chassis # commit-buffer
```

---

### 例

次に、デフォルトキーリングを再生成する例を示します。

```
Firepower-chassis# scope security  
Firepower-chassis /security # scope keyring default  
Firepower-chassis /security/keyring* # set regenerate yes  
Firepower-chassis /security/keyring* # commit-buffer  
Firepower-chassis /security/keyring #
```

## キーリングの証明書要求の作成

### 基本オプション付きのキーリングの証明書要求の作成

### 手順

---

**ステップ1** セキュリティモードを開始します。

```
Firepower-chassis # scope security
```

**ステップ2** キーリングのコンフィギュレーションモードに入ります。

```
Firepower-chassis /security # scope keyring keyring-name
```

**ステップ 3** 指定された IPv4 または IPv6 アドレス、またはファブリック インターコネクタの名前を使用して証明書要求を作成します。証明書要求のパスワードを入力するように求められます。

```
Firepower-chassis /security/keyring # create certreq {ip [ipv4-addr | ipv6-v6] | subject-name name}
```

**ステップ 4** トランザクションをコミットします。

```
Firepower-chassis /security/keyring/certreq # commit-buffer
```

**ステップ 5** コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

```
Firepower-chassis /security/keyring # show certreq
```

## 例

次の例では、基本オプション付きのキーリングについて IPv4 アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name
sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLAIYZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1Wsy1wUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBqkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAQBgcqCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWICtWgHhH8BimOb/0OKuG8kwfIGGsED1Av
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
Firepower-chassis /security/keyring #
```

## 次のタスク

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キーリングの証明書を取得するため、証明書要求を含むファイルをトラストアンカーまたは認証局に送信します。

- トラストポイントを作成し、トラストアンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

## 詳細オプション付きのキーリングの証明書要求の作成

### 手順

- 
- ステップ 1** セキュリティモードを開始します。  
Firepower-chassis # **scope security**
- ステップ 2** キーリングのコンフィギュレーションモードに入ります。  
Firepower-chassis /security # **scope keyring** *keyring-name*
- ステップ 3** 証明書要求を作成します。  
Firepower-chassis /security/keyring # **create certreq**
- ステップ 4** 会社が存在している国の国コードを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set country** *country name*
- ステップ 5** 要求に関連付けられたドメインネームサーバ (DNS) アドレスを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set dns** *DNS Name*
- ステップ 6** 証明書要求に関連付けられた電子メールアドレスを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set e-mail** *E-mail name*
- ステップ 7** Firepower 4100/9300 シャーシの IP アドレスを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }
- ステップ 8** 証明書を要求している会社の本社が存在する市または町を指定します。  
Firepower-chassis /security/keyring/certreq\* # **set locality** *locality name (eg, city)*
- ステップ 9** 証明書を要求している組織を指定します。  
Firepower-chassis /security/keyring/certreq\* # **set org-name** *organization name*
- ステップ 10** 組織ユニットを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set org-unit-name** *organizational unit name*
- ステップ 11** 証明書要求に関するオプションのパスワードを指定します。  
Firepower-chassis /security/keyring/certreq\* # **set password** *certificate request password*
- ステップ 12** 証明書を要求している会社の本社が存在する州または行政区分を指定します。  
Firepower-chassis /security/keyring/certreq\* # **set state** *state, province or county*

- ステップ 13** Firepower 4100/9300 シャーシ の完全修飾ドメイン名を指定します。
- ```
Firepower-chassis /security/keyring/certreq* # set subject-name certificate request name
```
- ステップ 14** トランザクションをコミットします。
- ```
Firepower-chassis /security/keyring/certreq # commit-buffer
```
- ステップ 15** コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。
- ```
Firepower-chassis /security/keyring # show certreq
```

### 例

次の例では、詳細オプション付きのキー リングについて IPv4 アドレスで証明書要求を作成して表示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* # set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwZGZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1WsyUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCcsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWicTWgHh8BimOb/00KuG8kwfIGGsED1Av
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPC5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
Firepower-chassis /security/keyring/certreq #
```

## 次のタスク

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キーリングの証明書を取得するため、証明書要求を含むファイルをトラストアンカーまたは認証局に送信します。
- トラストポイントを作成し、トラストアンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

## トラストポイントの作成

## 手順

ステップ1 セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

ステップ2 トラストポイントを作成します。

```
Firepower-chassis /security # create trustpoint name
```

ステップ3 このトラストポイントの証明書情報を指定します。

```
Firepower-chassis /security/trustpoint # set certchain [certchain]
```

コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラストポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、**ENDOFBUF** と入力して終了します。

**重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ4 トランザクションをコミットします。

```
Firepower-chassis /security/trustpoint # commit-buffer
```

## 例

次の例は、トラストポイントを作成し、トラストポイントに証明書を提供します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBGNVBAsT
> C1Rlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
```

```

> ZgAMivycsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmlkLWludj09ZmluZS5kaW50
> gYEAG6lCaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckC1d3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPsSxretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3n04MIGeBgNVHSMegZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3n04oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> ClNhbW50YXV5bW50YXV5bW50YXV5bW50YXV5bW50YXV5bW50YXV5bW50YXV5bW50
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copPLEBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #

```

### 次のタスク

トラストアンカーまたは認証局からキーリング証明書を取得し、キーリングにインポートします。

## キーリングへの証明書のインポート

### 始める前に

- キーリング証明書の証明書チェーンを含むトラストポイントを設定します。
- トラストアンカーまたは認証局からキーリング証明書を取得します。

### 手順

**ステップ 1** セキュリティモードを開始します。

```
Firepower-chassis # scope security
```

**ステップ 2** 証明書を受け取るキーリングでコンフィギュレーションモードに入ります。

```
Firepower-chassis /security # scope keyring keyring-name
```

**ステップ 3** キーリング証明書の取得元のトラストアンカーまたは認証局に対しトラストポイントを指定します。

```
Firepower-chassis /security/keyring # set trustpoint name
```

**ステップ 4** キーリング証明書を入力してアップロードするためのダイアログを起動します。

```
Firepower-chassis /security/keyring # set cert
```

プロンプトで、トラストアンカーまたは認証局から受け取った証明書のテキストを貼り付けます。証明書の次の行に **ENDOFBUF** と入力して、証明書の入力を完了します。

**重要** 証明書は、Base64 エンコード X.509 (CER) フォーマットである必要があります。

**ステップ 5** トランザクションをコミットします。

```
Firepower-chassis /security/keyring # commit-buffer
```

#### 例

次に、トラストポイントを指定し、証明書をキーリングにインポートする例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCAAwgCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgd4VBKOND1
> GmbkPayVlQjbG4MD2dx2+H8EH3LmtdZrgKvPxPTE+bf5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvLWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

#### 次のタスク

キーリングを使用して HTTPS サービスを設定します。

## HTTPS の設定



**注意** HTTPS で使用するポートとキーリングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

#### 手順

**ステップ 1** システム モードに入ります。

Firepower-chassis# **scope system**

**ステップ 2** システム サービス モードを開始します。

Firepower-chassis /system # **scope services**

**ステップ 3** HTTPS サービスを有効にします。

Firepower-chassis /system/services # **enable https**

**ステップ 4** (任意) HTTPS 接続で使用されるポートを指定します。

Firepower-chassis /system/services # **set https port port-num**

**ステップ 5** (任意) HTTPS に対して作成したキー リングの名前を指定します。

Firepower-chassis /system/services # **set https keyring keyring-name**

**ステップ 6** (任意) ドメインで使用される暗号スイートセキュリティのレベルを指定します。

Firepower-chassis /system/services # **set https cipher-suite-mode cipher-suite-mode**

*cipher-suite-mode* には、以下のいずれかのキーワードを指定できます。

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom** : ユーザ定義の暗号スイート仕様の文字列を指定できます。

**ステップ 7** (任意) **cipher-suite-mode** が **custom** に設定されている場合は、ドメインに対してカスタムレベルの暗号スイートセキュリティを指定します。

Firepower-chassis /system/services # **set https cipher-suite cipher-suite-spec-string**

*cipher-suite-spec-string* は最大 256 文字で構成できます。これは OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。!(感嘆符)、+(プラス記号)、-(ハイフン)、および:(コロン)。詳細については、[http://httpd.apache.org/docs/2.0/mod/mod\\_ssl.html#sslcipher-suite](http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslcipher-suite) を参照してください。

たとえば、FXOS がデフォルトとして使用する中強度仕様の文字列は次のようになります。

**ALL: !ADH: !EXPORT56: !LOW: RC4+RSA: +HIGH: +MEDIUM: +EXP: +eNULL**

(注) **cipher-suite-mode** は **custom** 以外に設定されている場合、このオプションは無視されます。

**ステップ 8** (任意) 証明書失効リスト検査を、有効または無効にします。

**set revoke-policy { relaxed | strict }**

**ステップ 9** トランザクションをシステム設定にコミットします。

Firepower-chassis /system/services # **commit-buffer**

### 例

次の例では、HTTPS をイネーブルにし、ポート番号を 443 に設定し、キーリング名を `kring7984` に設定し、暗号スイートのセキュリティレベルを `[high]` に設定し、トランザクションをコミットします。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## HTTPS ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

### 手順

- 
- ステップ 1 **[Platform Settings]** > **[HTTPS]** を選択します。
  - ステップ 2 HTTPS 接続に使用するポートを **[Port]** フィールドに入力します。1 ~ 65535 の整数を指定します。このサービスは、デフォルトでポート 443 でイネーブルになります。
  - ステップ 3 **[Save]** をクリックします。

指定した HTTPS ポートが Firepower シャーシに設定されます。

HTTPS ポートを変更すると、現在のすべての HTTPS セッションが閉じられます。ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

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

<chassis\_mgmt\_ip\_address> は、初期設定時に入力した Firepower シャーシの IP アドレスまたはホスト名で、<chassis\_mgmt\_port> は設定が完了した HTTPS ポートです。

---

## キーリングの削除

### 手順

- 
- ステップ 1 セキュリティ モードを開始します。

```
Firepower-chassis # scope security
```

**ステップ 2** 名前付きのキー リングを削除します。

```
Firepower-chassis /security # delete keyring name
```

**ステップ 3** トランザクションをコミットします。

```
Firepower-chassis /security # commit-buffer
```

---

### 例

次の例では、キー リングを削除します。

```
Firepower-chassis# scope security  
Firepower-chassis /security # delete keyring key10  
Firepower-chassis /security* # commit-buffer  
Firepower-chassis /security #
```

## トラスト ポイントの削除

### 始める前に

トラスト ポイントがキー リングによって使用されていないことを確認してください。

### 手順

---

**ステップ 1** セキュリティ モードに入ります。

```
Firepower-chassis# scope security
```

**ステップ 2** 指定したトラスト ポイントを削除します。

```
Firepower-chassis /security # delete trustpoint name
```

**ステップ 3** トランザクションをコミットします。

```
Firepower-chassis /security # commit-buffer
```

---

### 例

次に、トラスト ポイントを削除する例を示します。

```
Firepower-chassis# scope security  
Firepower-chassis /security # delete trustpoint tPoint10  
Firepower-chassis /security* # commit-buffer  
Firepower-chassis /security #
```

## HTTPS の無効化

### 手順

ステップ 1 システム モードに入ります。

```
Firepower-chassis# scope system
```

ステップ 2 システム サービス モードを開始します。

```
Firepower-chassis /system # scope services
```

ステップ 3 HTTPS サービスを無効にします。

```
Firepower-chassis /system/services # disable https
```

ステップ 4 トランザクションをシステム設定にコミットします。

```
Firepower-chassis /system/services # commit-buffer
```

### 例

次に、HTTPS をディセーブルにし、トランザクションをコミットする例を示します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## AAA の設定

ここでは、認証、認可、アカウンティングについて説明します。詳細については、次のトピックを参照してください。

## AAA について

AAA は、コンピュータ リソースへのアクセスを制御し、ポリシーを使用し、使用率を評価することでサービス課金に必要な情報を提供する、一連のサービスです。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

### 認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、

ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

シャーシへの管理接続を認証するように Firepower 4100/9300 シャーシ を設定できます。これには、次のセッションが含まれます。

- HTTPS
- SSH
- シリアル コンソール

## 認可

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

## アカウントिंग

アカウントिंगは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウントINGは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

## 認証、認可、アカウントING間の相互作用

認証だけで使用することも、認可およびアカウントINGとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウントINGだけで使用することも、認証および認可とともに使用することもできます。

## AAA サーバ

AAA サーバは、アクセス制御に使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウントINGは、課金と分析に使用される時間とデータのリソースを追跡します。

## ローカル データベースのサポート

Firepower シャーシは、ユーザプロファイルを取り込むことができるローカル データベースを維持します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウントINGを提供することもできます。

## LDAP プロバイダーの設定

### LDAP プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザアカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

#### 手順

- ステップ 1 [Platform Settings] > [AAA] を選択します。
- ステップ 2 [LDAP] タブをクリックします。
- ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

| 名前                | 説明                                                                                                                                                                                                                                                                                       |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Timeout] フィールド   | LDAP データベースへの問い合わせがタイムアウトするまでの秒数。<br><br>1 ~ 60 秒の整数を入力します。デフォルト値は 30 秒です。<br>このプロパティは必須です。                                                                                                                                                                                              |
| [Attribute] フィールド | ユーザロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性名と一致する値を検索します。                                                                                                                                                                                                  |
| [Base DN] フィールド   | リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から CN=\$userid の長さを引いた長さに設定することができます。\$userid により、LDAP 認証を使用して Firepower シャーシにアクセスしようとするリモートユーザが識別されます。<br><br>このプロパティは必須です。このタブでベース DN を指定しない場合、定義する LDAP プロバイダーごとに 1 つずつ指定する必要があります。 |

| 名前             | 説明                                                                                                           |
|----------------|--------------------------------------------------------------------------------------------------------------|
| [Filter] フィールド | LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。<br><br>このプロパティは必須です。このタブでフィルタを指定しない場合、定義する LDAP プロバイダーごとに1つずつ指定する必要があります。 |

**ステップ 4** [Save] をクリックします。

#### 次のタスク

LDAP プロバイダーを作成します。

## LDAP プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の LDAP プロバイダーをサポートします。

#### 始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Firepower eXtensible Operating System にバインドするユーザアカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

#### 手順

**ステップ 1** [Platform Settings] > [AAA] を選択します。

**ステップ 2** [LDAP] タブをクリックします。

**ステップ 3** 追加する LDAP プロバイダーごとに、次の手順を実行します。

- a) [LDAP Providers] 領域で、[Add] をクリックします。
- b) [Add LDAP Provider] ダイアログボックスで、次のフィールドに値を入力します。

| 名前                                    | 説明                                                                                                    |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|
| [Hostname/FDQN (or IP Address)] フィールド | LDAP プロバイダーのホスト名または IP アドレス。SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名 (CN) と正確に一致している必要があります。 |

| 名前                    | 説明                                                                                                                                                                                                                                                                                        |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Order] フィールド         | <p>Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。</p> <p>1 ~ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、<b>lowest-available</b> または <b>0</b> (ゼロ) を入力します。</p>         |
| [Bind DN] フィールド       | <p>ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名 (DN)。</p> <p>サポートされるストリングの最大長は 255 文字 (ASCII) です。</p>                                                                                                                                                                       |
| [Base DN] フィールド       | <p>リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字 + CN=\$userid の長さに設定することができます。\$userid により、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI にアクセスしようとするリモートユーザが識別されます。</p> <p>デフォルトのベース DN が [LDAP] タブで設定されていない場合は、この値が必要です。</p> |
| [Port] フィールド          | <p>Firepower Chassis Manager または FXOS CLI が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。</p>                                                                                                                                                                                              |
| [Enable SSL] チェックボックス | <p>このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリアテキストで送信されます。</p> <p>LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。</p>                                                                                                                             |
| [Filter] フィールド        | <p>LDAP 検索は、定義したフィルタと一致するユーザ名に制限されます。</p> <p>デフォルトのフィルタが [LDAP] タブで設定されていない場合は、この値が必要です。</p>                                                                                                                                                                                              |

| 名前                  | 説明                                                                                                                                                                                                                                                                          |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Attribute] フィールド   | ユーザロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性名と一致する値を検索します。<br><br>デフォルトの属性が [LDAP] タブで設定されていない場合は、この値が必要です。                                                                                                                                    |
| [Key] フィールド         | [Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「\$」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。                                                                                                                                                                    |
| [Confirm Key] フィールド | 確認のための LDAP データベース パスワードの再入力。                                                                                                                                                                                                                                               |
| [Timeout] フィールド     | LDAP データベースへの問い合わせがタイムアウトするまでの秒数。<br><br>1～60秒の整数を入力するか、0（ゼロ）を入力して [LDAP] タブで指定したグローバルタイムアウト値を使用します。デフォルトは 30 秒です。                                                                                                                                                          |
| [Vendor] フィールド      | この選択により、LDAP プロバイダーやサーバの詳細を提供するベンダーが識別されます。<br><br><ul style="list-style-type: none"> <li>• LDAP プロバイダーが Microsoft Active Directory の場合は、[MS-AD] を選択します。</li> <li>• LDAP プロバイダーが Microsoft Active Directory でない場合は、[Open LDAP] を選択します。</li> </ul><br>デフォルトは [Open LDAP] です。 |

c) [OK] をクリックして、[Add LDAP Provider] ダイアログボックスを閉じます。

**ステップ 4** [Save] をクリックします。

**ステップ 5** （任意）証明書失効リスト検査を有効にします。

```
Firepower-chassis /security/ldap/server # set revoke-policy {strict | relaxed}
```

(注) この設定は、SSL 接続が使用可能である場合にのみ有効です。

## LDAP プロバイダーの削除

### 手順

- 
- ステップ 1 [Platform Settings] > [AAA] を選択します。
  - ステップ 2 [LDAP] タブをクリックします。
  - ステップ 3 [LDAP Providers] 領域で、削除する LDAP プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。
- 

## RADIUS プロバイダーの設定

### RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

### 手順

- 
- ステップ 1 [Platform Settings] > [AAA] を選択します。
  - ステップ 2 [RADIUS] タブをクリックします。
  - ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

| 名前              | 説明                                                                                       |
|-----------------|------------------------------------------------------------------------------------------|
| [Timeout] フィールド | RADIUS データベースへの問い合わせがタイムアウトするまでの秒数。<br>1 ~ 60 秒の整数を入力します。デフォルト値は 5 秒です。<br>このプロパティは必須です。 |
| [Retries] フィールド | 要求が失敗したと見なされるまでの接続の再試行の回数。                                                               |

- ステップ 4 [Save] をクリックします。
- 

### 次のタスク

RADIUS プロバイダーを作成します。

## RADIUS プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の RADIUS プロバイダーをサポートします。

### 手順

**ステップ 1** [Platform Settings] > [AAA] を選択します。

**ステップ 2** [RADIUS] タブをクリックします。

**ステップ 3** 追加する RADIUS プロバイダーごとに、次の手順を実行します。

- a) [RADIUS Providers] 領域で、[Add] をクリックします。
- b) [Add RADIUS Provider] ダイアログボックスで、次のフィールドに値を入力します。

| 名前                                    | 説明                                                                                                                                                                                                                                                                          |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Hostname/FDQN (or IP Address)] フィールド | RADIUS プロバイダーが存在する場所のホスト名または IP アドレス。                                                                                                                                                                                                                                       |
| [Order] フィールド                         | Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。<br><br>1 ~ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、 <b>lowest-available</b> または <b>0</b> (ゼロ) を入力します。 |
| [Key] フィールド                           | データベースの SSL 暗号キー。                                                                                                                                                                                                                                                           |
| [Confirm Key] フィールド                   | 確認のための SSL 暗号キーの再入力。                                                                                                                                                                                                                                                        |
| [Authorization Port] フィールド            | Firepower Chassis Manager または FXOS CLI が RADIUS データベースと通信するために使用されるポート。有効な範囲は 1 ~ 65535 です。標準ポート番号は 1700 です。                                                                                                                                                                |
| [Timeout] フィールド                       | RADIUS データベースへの問い合わせがタイムアウトするまでの秒数。<br><br>1 ~ 60 秒の整数を入力するか、0 (ゼロ) を入力して [RADIUS] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。                                                                                                                                                 |
| [Retries] フィールド                       | 要求が失敗したと見なされるまでの接続の再試行の回数。<br><br>必要に応じて、0 ~ 5 の整数を入力します。値を指定しない場合、Firepower Chassis Manager は [RADIUS] タブに指定した値を使用します。                                                                                                                                                     |

c) [OK] をクリックして、[Add RADIUS Provider] ダイアログボックスを閉じます。

ステップ 4 [Save] をクリックします。

## RADIUS プロバイダーの削除

### 手順

ステップ 1 [Platform Settings] > [AAA] を選択します。

ステップ 2 [RADIUS] タブをクリックします。

ステップ 3 [RADIUS Providers] 領域で、削除する RADIUS プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。

## TACACS+ プロバイダーの設定

### TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティが、このタイプのすべてのプロバイダー接続のデフォルト設定です。個々のプロバイダーにいずれかのプロパティの設定が含まれている場合、Firepower eXtensible Operating System でその設定が使用され、デフォルト設定は無視されます。

### 手順

ステップ 1 [Platform Settings] > [AAA] を選択します。

ステップ 2 [TACACS] タブをクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

| 名前              | 説明                                                                                           |
|-----------------|----------------------------------------------------------------------------------------------|
| [Timeout] フィールド | タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。<br>1 ~ 60 秒の整数を入力します。デフォルト値は 5 秒です。<br>このプロパティは必須です。 |

ステップ 4 [Save] をクリックします。

### 次のタスク

TACACS+ プロバイダーを作成します。

## TACACS+ プロバイダーの作成

Firepower eXtensible Operating System では、最大 16 の TACACS+ プロバイダーをサポートします。

### 手順

**ステップ 1** [Platform Settings] > [AAA] を選択します。

**ステップ 2** [TACACS] タブをクリックします。

**ステップ 3** 追加する TACACS+ プロバイダーごとに、次の手順を実行します。

- a) [TACACS Providers] 領域で、[Add] をクリックします。
- b) [Add TACACS Provider] ダイアログボックスで、次のフィールドに値を入力します。

| 名前                                    | 説明                                                                                                                                                                                                                                                                          |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Hostname/FDQN (or IP Address)] フィールド | TACACS+ プロバイダーが存在する場所のホスト名または IP アドレス。                                                                                                                                                                                                                                      |
| [Order] フィールド                         | Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。<br><br>1 ~ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、 <b>lowest-available</b> または <b>0</b> (ゼロ) を入力します。 |
| [Key] フィールド                           | データベースの SSL 暗号キー。                                                                                                                                                                                                                                                           |
| [Confirm Key] フィールド                   | 確認のための SSL 暗号キーの再入力。                                                                                                                                                                                                                                                        |
| [Port] フィールド                          | Firepower Chassis Manager または FXOS CLI が TACACS+ データベースと通信するために使用するポート。<br><br>1 ~ 65535 の整数を入力します。デフォルトポートは 49 です。                                                                                                                                                         |
| [Timeout] フィールド                       | タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。<br><br>1 ~ 60 秒の整数を入力するか、0 (ゼロ) を入力して [TACACS+] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。                                                                                                                                            |

- c) [OK] をクリックして、[Add TACACS Provider] ダイアログボックスを閉じます。

**ステップ 4** [Save] をクリックします。

## TACACS+ プロバイダーの削除

### 手順

- 
- ステップ 1** [Platform Settings] > [AAA] を選択します。
- ステップ 2** [TACACS] タブをクリックします。
- ステップ 3** [TACACS Providers] 領域で、削除する TACACS+ プロバイダーに対応するテーブルの行の [Delete] アイコンをクリックします。
- 

## Syslog の設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチントラブルシューティングおよびインシデント処理の両方で役立ちます。

### 手順

- 
- ステップ 1** [Platform Settings] > [Syslog] を選択します。
- ステップ 2** ローカル宛先を設定します。
- [Local Destinations] タブをクリックします。
  - [Local Destinations] タブで、次のフィールドに値を入力します。

| 名前                  | 説明                                                                                                                                                                                      |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Console] セクション     |                                                                                                                                                                                         |
| [Admin State] フィールド | Firepower シャーシでコンソールに syslog メッセージが表示されるかどうか。<br><br>syslog メッセージをログに追加するだけでなく、コンソールにも表示する場合は、[Enable] チェックボックスをオンにします。[Enable] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、コンソールには表示されません。 |

| 名前                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Level] フィールド       | <p>[Console - Admin State] の [Enable] チェックボックスをオンにした場合は、コンソールに表示するメッセージの最も低いレベルを選択します。Firepower シャーシのコンソールにはそのレベル以上のメッセージが表示されます。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>Emergencies</b></li> <li>• <b>Alerts</b></li> <li>• <b>Critical</b></li> </ul>                                                                                                                            |
| [Monitor] セクション     |                                                                                                                                                                                                                                                                                                                                                                                                         |
| [Admin State] フィールド | <p>Firepower シャーシでモニタに syslog メッセージが表示されるかどうか。</p> <p>syslog メッセージをログに追加するだけでなく、モニタにも表示する場合は、[Enable] チェックボックスをオンにします。[Enable] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、モニタには表示されません。</p>                                                                                                                                                                                                                |
| [Level] ドロップダウン リスト | <p>[Monitor - Admin State] の [Enable] チェックボックスをオンにした場合は、モニタに表示するメッセージの最も低いレベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>Emergencies</b></li> <li>• <b>Alerts</b></li> <li>• <b>Critical</b></li> <li>• <b>Errors</b></li> <li>• <b>Warnings</b></li> <li>• <b>Notifications</b></li> <li>• <b>Information</b></li> <li>• <b>Debugging</b></li> </ul> |

c) [Save] をクリックします。

**ステップ 3** リモート宛先を設定します。

a) [Remote Destinations] タブをクリックします。

b) [Remote Destinations] タブで、Firepower シャーシによって生成されたメッセージを保存できる最大 3 つの外部ログについて、次のフィールドに入力します。

syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギングデータを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスク립トを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

| 名前                          | 説明                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Admin State] フィールド         | syslog メッセージをリモートログファイルに保存する場合は、[Enable] チェックボックスをオンにします。                                                                                                                                                                                                                                                                                        |
| [Level] ドロップダウン リスト         | システムに保存するメッセージの最も低いレベルを選択します。リモートファイルにそのレベル以上のメッセージが保存されます。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>Emergencies</b></li> <li>• <b>Alerts</b></li> <li>• <b>Critical</b></li> <li>• <b>Errors</b></li> <li>• <b>Warnings</b></li> <li>• <b>Notifications</b></li> <li>• <b>Information</b></li> <li>• <b>Debugging</b></li> </ul> |
| [Hostname/IP Address] フィールド | リモート ログ ファイルが存在するホスト名または IP アドレス。<br><br>(注) IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。                                                                                                                                                                                                                                                        |

| 名前                     | 説明                                                                                                                                                                                                                                                           |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Facility] ドロップダウン リスト | <p>ファイルメッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• local0</li> <li>• local1</li> <li>• local2</li> <li>• local3</li> <li>• local4</li> <li>• local5</li> <li>• local6</li> <li>• Local7</li> </ul> |

c) [Save] をクリックします。

**ステップ 4** ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) [Local Sources] タブで、次のフィールドに値を入力します。

| 名前                                   | 説明                                                                                     |
|--------------------------------------|----------------------------------------------------------------------------------------|
| [障害管理状態 (Faults Admin State) ] フィールド | システム障害ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム障害をログに記録します。      |
| [Audits Admin State] フィールド           | 監査ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべての監査ログ イベントをログに記録します。       |
| [Events Admin State] フィールド           | システムイベントロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム イベントをログに記録します。 |

c) [Save] をクリックします。

## DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。たとえば、DNS サーバを設定していないと、Firepower シャーシで設定を行うときに、www.cisco.com などの名前を使用できません。サーバの IP アドレスを使用する必要があります。

IPv4 または IPv6 アドレスのいずれかを使用できます。最大 4 台の DNS サーバを設定できます。



- (注) 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

#### 手順

- ステップ 1 [Platform Settings] > [DNS] を選択します。
- ステップ 2 [Enable DNS Server] チェックボックスをオンにします。
- ステップ 3 追加する DNS サーバ (最大 4 台) ごとに、それぞれの IP アドレスを [DNS Server] フィールドに入力し、[Add] をクリックします。
- ステップ 4 [Save] をクリックします。

## FIPS モードの有効化

Firepower 4100/9300 シャーシで FIPS モードを有効にするには、次の手順を実行します。

#### 手順

- ステップ 1 Firepower 4100/9300 シャーシに管理者ユーザとしてログインします。
- ステップ 2 **Platform Settings** を選択して、[Platform Settings] ウィンドウを開きます。
- ステップ 3 **FIPS/CC mode** を選択して、[FIPS and Common Criteria] ウィンドウを開きます。
- ステップ 4 FIPS の **Enable** チェックボックスをオンにします。
- ステップ 5 **Save** をクリックして、設定を保存します。
- ステップ 6 プロンプトに従ってシステムをリブートします。

#### 次のタスク

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホストキーが 1024 ビットにハードコードされていました。FIPS およびコモンクライテリア認定要件に準拠するには、この古いホストキーを破棄し、[SSH ホストキーの生成 \(54 ページ\)](#) で詳細を説明する手順を使用して新しいホストキーを生成する必要があります。これらの追加手順を実行しないと、FIPS モードを有効にしてデバイスをリブートした後に、SSH を使用してスーパーバイザ

に接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホストキーを生成する必要はありません。

## コモンクライテリア モードの有効化

Firepower 4100/9300 シャーシ上でコモンクライテリア モードを有効にするには、次の手順を実行します。

### 手順

- ステップ 1** Firepower 4100/9300 シャーシに管理者ユーザとしてログインします。
- ステップ 2** **Platform Settings** を選択して、[Platform Settings] ウィンドウを開きます。
- ステップ 3** **FIPS/CC mode** を選択して、[FIPS and Common Criteria] ウィンドウを開きます。
- ステップ 4** コモンクライテリアの **Enable** チェックボックスをオンにします。
- ステップ 5** **Save** をクリックして、設定を保存します。
- ステップ 6** プロンプトに従ってシステムをリブートします。

### 次のタスク

FXOS リリース 2.0.1 より以前は、デバイスの最初の設定時に作成した SSH ホストキーが 1024 ビットにハードコードされていました。FIPS およびコモンクライテリア認定要件に準拠するには、この古いホストキーを破棄し、[SSH ホストキーの生成 \(54 ページ\)](#) で詳細を説明する手順を使用して新しいホストキーを生成する必要があります。これらの追加手順を実行しないと、コモンクライテリアモードを有効にしてデバイスをリブートした後に、SSH を使用してスーパーバイザに接続できなくなります。FXOS 2.0.1 以降を使用して初期設定を行った場合は、新しいホストキーを生成する必要はありません。

## IP アクセス リストの設定

デフォルトでは、Firepower 4100/9300 シャーシはローカル Web サーバへのすべてのアクセスを拒否します。IP アクセスリストを、各 IP ブロックの許可されるサービスのリストを使用して設定する必要があります。

IP アクセスリストは、次のプロトコルをサポートします。

- HTTPS
- SNMP
- SSH

IP アドレス (v4 または v6) の各ブロックで、最大 25 個の異なるサブネットを各サービスに対して設定できます。サブネットを 0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。

#### 手順

---

**ステップ 1** Firepower 4100/9300 シャーシに管理者ユーザとしてログインします。

**ステップ 2** **Platform Settings** を選択し、[Platform Settings] ページを開きます。

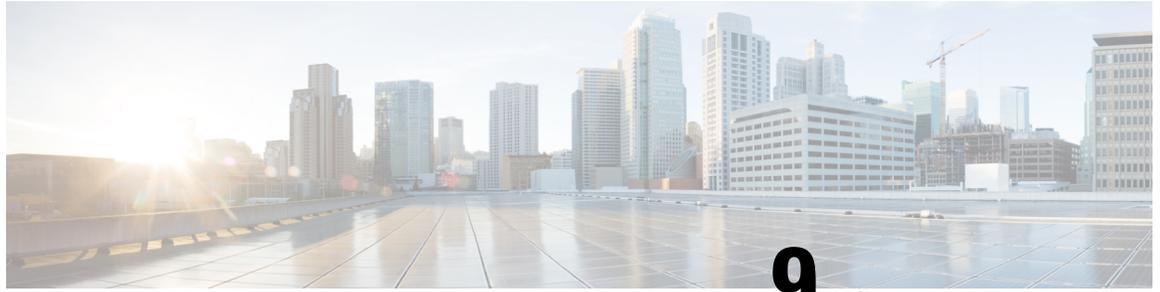
**ステップ 3** **Access List** を選択し、[Access List] 領域を開きます。

**ステップ 4** この領域で、[IP Access List] にリストされている IPv4 および IPv6 アドレスを表示、追加、削除できます。

IPv4 ブロックを追加するには、有効な IPv4 IP アドレスとプレフィックスの長さ (0 ~ 32) を入力し、プロトコルを選択する必要があります。

IPv6 ブロックを追加するには、有効な IPv6 IP アドレスとプレフィックスの長さ (0 ~ 128) を入力し、プロトコルを選択する必要があります。

---



## 第 9 章

# インターフェイス管理

- [Firepower インターフェイスについて](#) (135 ページ)
- [Firepower インターフェイスに関する注意事項と制約事項](#) (138 ページ)
- [インターフェイスの設定](#) (139 ページ)
- [モニタリングインターフェイス](#) (143 ページ)
- [インターフェイスの履歴](#) (144 ページ)

## Firepower インターフェイスについて

Firepower 4100/9300 シャーシは、物理インターフェイスおよび EtherChannel (ポートチャネル) インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

## シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で FXOS シャーシの管理に使用されます。このインターフェイスは [MGMT] として [Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効と無効を切り替えられるだけです。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定する必要があります。[管理 IP アドレスの変更](#) (72 ページ) も参照してください。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

```
Firepower # connect local-mgmt
```

```
Firepower(local-mgmt) # show mgmt-port
```

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

## インターフェイスタイプ

各インターフェイスは、次のいずれかのタイプになります。

- **Data** : データ インターフェイスは論理デバイス間で共有できません。
- **Mgmt** : 管理インターフェイスを使用してアプリケーションインスタンスを管理します。外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。個別のシャーシ管理インターフェイスについては、[シャーシ管理インターフェイス \(135 ページ\)](#) を参照してください。

FTDアプリケーションでは、物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイス間で共有されます。管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、**Firepower Management Center** にデバイスを設定し、登録するために使用されます。独自のローカル認証、IPアドレス、およびスタティックルーティングを使用します。**Firepower Management Center 構成ガイド**の「**System Configuration**」の章にある「**Management Interfaces**」のセクションを参照してください。

診断論理インターフェイスは残りのデータインターフェイスとともに、**FMC**の**[Devices]> [Device Management]> [Interfaces]**画面で構成できます。診断インターフェイスの使用はオプションです。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。

- **Firepower イベント** : このインターフェイスはFTDデバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLIでIPアドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。**Firepower Management Center 構成ガイド**の「**System Configuration**」の章にある「**Management Interfaces**」のセクションを参照してください。**Firepower イベント**インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の論理デバイスと通信することはできません。
- **Cluster** : クラスタ化された論理デバイスに使用する特別なインターフェイスタイプです。このタイプは、ユニット間のクラスタ通信用にクラスタ制御リンクに自動的に割り当てられます。デフォルトでは、クラスタ制御リンクは48番のポートチャネル上に自動的に作成されます。

## ハードウェア バイパス ペア

FTDの場合、**Firepower 9300** および **4100** シリーズの特定のインターフェイス モジュールを使用して、ハードウェア バイパス 機能を有効にします。ハードウェア バイパスにより、停電中のインラインインターフェイス ペア間でトラフィックが流れ続けます。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

ハードウェアバイパス機能は、FTDアプリケーション内で設定されます。これらのインターフェイスをハードウェアバイパスペアとして使用する必要はありません。これらは、ASAとFTDアプリケーションの両方について通常のインターフェイスとして使用できます。ハードウェアバイパス対応のインターフェイスをブレイクアウトポート用に設定することはできないため注意してください。ハードウェアバイパス機能を使用するには、ポートをEtherChannelとして設定しないでください。そうでない場合は、これらのインターフェイスを通常のインターフェイスモードのEtherChannelメンバとして含めることができます。

FTDは、以下のモデルの特定のネットワークモジュールのインターフェイスペアでハードウェアバイパスをサポートします。

- Firepower 9300
- Firepower 4100 シリーズ

これらのモデルでサポートされているハードウェアバイパスネットワークモジュールは以下のとおりです。

- FirePOWER 6ポート 1G SX FTW ネットワークモジュール シングルワイド (FPR-NM-6X1SX-F)
- FirePOWER 6ポート 10G SR FTW ネットワークモジュール シングルワイド (FPR-NM-6X10SR-F)
- FirePOWER 6ポート 10G LR FTW ネットワークモジュール シングルワイド (FPR-NM-6X10LR-F)
- FirePOWER 2ポート 40G SR FTW ネットワークモジュール シングルワイド (FPR-NM-2X40G-F)
- Firepower 8ポート 1G Copper FTW ネットワークモジュール シングルワイド (FPR-NM-8X1G-F)

ハードウェアバイパスでは以下のポートペアのみ使用できます。

- 1と2
- 3と4
- 5と6
- 7および8

## ジャンボフレームサポート

Firepower 4100/9300 シャーシは、デフォルトで有効になっているジャンボフレームをサポートします。Firepower 4100/9300 シャーシにインストールされた特定の論理デバイスのジャンボフレームサポートを有効にするには、論理デバイスのインターフェイスに適切なMTUの設定を構成する必要があります。

Firepower 4100/9300 シャーシのアプリケーションでサポートされている最大 MTU は、9184 です。

## Firepower Threat Defense のインラインセット リンク ステートの伝達

インラインセットはワイヤ上のパンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

FTD アプリケーションでインラインセットを設定し、リンク ステート伝達を有効にすると、FTD はインラインセットメンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インラインインターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンク ステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンク ステートを更新します。ただし、シャーシからリンク ステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

## Firepower インターフェイスに関する注意事項と制約事項

### インラインセット FTD

- 物理インターフェイス（通常かつブレイクアウトポート）と Etherchannel のサポート。
- リンク ステートの伝達はサポートされます。

### ハードウェアバイパス

- FTD をサポート。ASA の通常のインターフェイスとして使用できます。
- FTD はインラインセットを含むハードウェアバイパスのみをサポートします。
- ハードウェアバイパス 対応のインターフェイスをブレイクアウトポート用に設定することはできません。
- ハードウェアバイパス インターフェイスを EtherChannel に含めたり、ハードウェアバイパスに使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。

### デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャンネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

## インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannels、インターフェイス プロパティを編集して、ブレイクアウト ポートを設定できます。

### インターフェイスの有効化または無効化

各インターフェイスの [Admin State] を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスは無効になっています。

#### 手順

---

**ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。

[Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

**ステップ 2** インターフェイスを有効にするには、[disabled] スライダ (  ) をクリックします。これで、[enabled] スライダ (  ) に変わります。

[Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変わります。

**ステップ 3** インターフェイスを無効にするには、[enabled] スライダ (  ) をクリックします。これで、[disabled] スライダ (  ) に変わります。

[Yes] をクリックして、変更を確認します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

---

## 物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOSで物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

### 始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

### 手順

---

**ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。

[Interfaces] ページには、ページの上部に現在インストールされているインターフェイスが視覚的に表示され、下の表にはインストールされているインターフェイスのリストが示されています。

**ステップ 2** 編集するインターフェイスの行の [Edit] をクリックし、[Edit Interface] ダイアログボックスを開きます。

**ステップ 3** インターフェイスをイネーブルにするには、[Enable] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

**ステップ 4** インターフェイスの [Type] を次から選択します。[Data]、[Mgmt]、[Firepower-eventing]、または [Cluster]。

[Cluster] タイプは選択しないでください。デフォルトでは、Cluster Control Link はポートチャネル 48 に自動的に作成されます。

**ステップ 5** (任意) [Speed] ドロップダウン リストからインターフェイスの速度を選択します。

**ステップ 6** (任意) インターフェイスで [Auto Negotiation] がサポートされている場合は、[Yes] または [No] オプション ボタンをクリックします。

**ステップ 7** (任意) [Duplex] ドロップダウン リストからインターフェイスのデュプレックスを選択します。

**ステップ 8** [OK] をクリックします。

---

## EtherChannel (ポートチャネル) の追加

EtherChannel (別名ポートチャネル) には、同じタイプのメンバーインターフェイスを最大16個含めることができます。リンク集約制御プロトコル (LACP) では、2つのネットワークデバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

各メンバインターフェイスが LACP 更新を送受信するように、Firepower 4100/9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネルグループに接続されていることがチェックされます。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [Suspended] 状態になり、物理リンクがアップしても論理デバイスに割り当てられるまでそのままになります。

EtherChannel は次のような状況でこの [Suspended] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てられるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [Suspended] 状態に戻ります。

## 手順

- 
- ステップ 1** [Interfaces] を選択して、[Interfaces] ページを開きます。
- [Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ステップ 2** インターフェイス テーブルの上にある [Add Port Channel] をクリックして、[Add Port Channel] ダイアログボックスを開きます。
- ステップ 3** [Port Channel ID] フィールドに、ポートチャネルの ID を入力します。有効な値は、1 ~ 47 です。
- クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、別の ID で EtherChannel を設定し、インターフェイスにクラスタタイプを選択できます。インターフェイスをクラスタ EtherChannel に割り当てないでください。
- ステップ 4** ポートチャネルを有効化するには、[Enable] チェックボックスをオンにします。ポートチャネルをディセーブルにするには、[Enable] チェックボックスをオフにします。
- ステップ 5** インターフェイスの [タイプ (Type)] を次から選択します。[Data]、[Mgmt]、[Firepower-eventing]、または [Cluster]。

デフォルトの代わりに、このポートチャネルを Cluster Control Link として使用する場合以外は、[Cluster] タイプを選択しないでください。

- ステップ 6** ドロップダウン リストでメンバ インターフェイスの [Admin Speed] を設定します。
- ステップ 7** [Admin Duplex]、[Full Duplex] または [Half Duplex] を設定します。
- ステップ 8** ポート チャネルにインターフェイスを追加するには、[Available Interface] リストでインターフェイスを選択し、[Add Interface] をクリックしてそのインターフェイスを [Member ID] リストに移動します。同じタイプと速度の最大 16 のインターフェイスを追加できます。
- ヒント** 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、**Ctrl** キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift** キーを押しながら最後のインターフェイスをクリックして選択します。
- ステップ 9** ポートチャネルからインターフェイスを削除するには、[Member ID] リストでそのインターフェイスの右側にある [Delete] ボタンをクリックします。
- ステップ 10** [OK] をクリックします。

## ブレイクアウト ケーブルの設定

Firepower 4100/9300 シャーシで使用するブレイクアウトケーブルを設定するには、次の手順に従います。ブレイクアウトケーブルを使用すると、1 つの 40 Gbps ポートの代わりに 4 つの 10 Gbps ポートを実装できます。

### 始める前に

ハードウェア バイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできません。

### 手順

- ステップ 1** [Interfaces] を選択して [Interfaces] ページを開きます。
- [Interfaces] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。
- ブレイクアウトケーブルに対応できるインターフェイスが、現在そのように設定されていない場合は、そのインターフェイスの行に [Breakout Port] アイコンが表示されます。ブレイクアウトケーブルを使用するように設定されているインターフェイスの場合、個々のブレイクアウトインターフェイスが別々にリストされます（例：イーサネット 2/1/1、2/1/2、2/1/3、2/1/4）。
- ステップ 2** 1 つの 40 Gbps インターフェイスを 4 つの 10 Gbps インターフェイスに変換するには、次の手順を実行します。
- a) 変換するインターフェイスの [Breakout Port] アイコンをクリックします。

[Breakout Port Creation] ダイアログボックスが開いて、続行の確認を求められ、シャーシのリポートについての警告が表示されます。

- b) 確認のために [Yes] をクリックします。

Firepower シャーシがリポートし、指定したインターフェイスが4つの10 Gbps インターフェイスに変換されます。

**ステップ 3** 4つの10 Gbps ブレークアウト インターフェイスを1つの40 Gbps インターフェイスに再度変換するには、次の手順を実行します。

- a) いずれかのブレークアウト インターフェイスの [Delete] をクリックします。

続行を確認するダイアログボックスが開いて、4つのブレークアウト インターフェイスがすべて削除されてシャーシがリポートされることを警告します。

- b) 確認のために [Yes] をクリックします。

Firepower シャーシがリポートし、指定したインターフェイスが1つの40 Gbps インターフェイスに変換されます。

## モニタリングインターフェイス

Firepower Chassis Manager の [Interfaces] ページから、シャーシにインストールされているインターフェイスのステータスの表示、インターフェイスのプロパティの編集、インターフェイスの有効化または無効化、ポート チャネルの作成を行えます。

[Interfaces] ページは、次の2つのセクションから構成されています。

- 上部のセクションには、Firepower シャーシにインストールされているインターフェイスが視覚的に表示されます。いずれかのインターフェイスにカーソルを合わせると、そのインターフェイスに関する追加情報が表示されます。

インターフェイスは現在のステータスを示すために色分けされています。

- 緑色：インターフェイスはインストール済みで、有効になっています。
- ダーク グレイ：そのインターフェイスはインストールされていますが、無効になっています。
- 赤色：インターフェイスの動作状態に問題があります。
- 淡い灰色：インターフェイスがインストールされていません。



(注) ポートチャネルのポートとして機能するインターフェイスは、このリストに表示されません。

- 下部のセクションには、[All Interfaces] と [ハードウェア バイパス] の2つのタブが含まれています。[All Interfaces] タブ：インターフェイスごとに、インターフェイスを有効または無効にできます。[Edit] をクリックすると、インターフェイスのプロパティ（速度やインターフェイス タイプなど）を編集することもできます。ハードウェア バイパスについては、[ハードウェア バイパス ペア（136 ページ）](#) を参照してください。



(注) ポート チャネル 48 クラス タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[Operation State] を [Failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバ インターフェイスを必要としないため、この動作状態は無視して構いません。

## インターフェイスの履歴

| 機能名                               | プラットフォーム リリース | 機能情報                                                                                                                                                                                                                      |
|-----------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTD インラインセットでの EtherChannel のサポート | 2.1(1)        | FTD インラインセットで Etherchannel を使用できるようになりました。<br><br>サポートされるプラットフォーム：<br>Firepower 4100/9300 FTD                                                                                                                             |
| FTD のインラインセット リンク ステート伝達サポート      | 2.0(1)        | FTD アプリケーションでインラインセットを設定し、リンクステート伝達を有効にすると、FTD はインラインセットメンバーシップをFXOS シャーシに送信します。リンクステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インラインインターフェイスペアの2番目のインターフェイスも自動的に停止します。<br><br>サポートされるプラットフォーム：<br>Firepower 4100/9300 FTD |

| 機能名                                  | プラットフォーム リリース | 機能情報                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ハードウェア バイパス ネットワーク<br>モジュールのサポート FTD | 2.0(1)        | <p>ハードウェア バイパスは、停電時にトラフィックがインラインインターフェイスペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。</p> <p>新規/変更された Firepower Management Center 画面：</p> <p><b>[Devices] &gt; [Device Management] &gt; [Interfaces] &gt; [Edit Physical Interface]</b></p> <p>サポートされるプラットフォーム：<br/>Firepower 4100/9300 FTD</p>                                                                                                                                            |
| FTD の Firepower イベント タイプ インターフェイス    | 1.1.4         | <p>FTD で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。Firepower Management Center 構成ガイドの「System Configuration」の章にある「Management Interfaces」のセクションを参照してください。</p> <p>新規/変更された [Firepower Chassis Manager] 画面：</p> <p><b>[Interfaces] &gt; [All Interfaces] &gt; [Type]</b></p> <p>サポートされるプラットフォーム：<br/>Firepower 4100/9300 FTD</p> |





## 第 10 章

# 論理デバイス

- 論理デバイスについて (147 ページ)
- 論理デバイスの要件と前提条件 (148 ページ)
- 論理デバイスに関する注意事項と制約事項 (150 ページ)
- スタンドアロン論理デバイスの追加 (156 ページ)
- ハイ アベイラビリティ ペアの追加 (160 ページ)
- クラスタの追加 (161 ページ)
- Radware DefensePro の設定 (177 ページ)
- 論理デバイスの管理 (183 ページ)
- [Logical Devices] ページ (190 ページ)
- サイト間クラスタリングの例 (193 ページ)
- 論理デバイスの履歴 (196 ページ)

## 論理デバイスについて

論理デバイスでは、1つのアプリケーションインスタンス (ASA または Firepower Threat Defense のいずれか) および1つのオプションデコレータアプリケーション (Radware DefensePro) を実行し、サービス チェーンを形成できます。

論理デバイスを追加する場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。



- (注) Firepower 9300 の場合、シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ (ASA または Firepower Threat Defense) をインストールする必要があります。現時点では、他のタイプはサポートされていません。モジュールでは、異なるバージョンのアプリケーション インスタンス タイプを実行できます。

## スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加することができます。

- スタンドアロン：スタンドアロン論理デバイスはスタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数のユニットをグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによるスループットの向上と冗長性を実現できます。Firepower 9300 などの複数モジュールデバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 のすべての3つのモジュールアプリケーションインスタンスは、1つの論理デバイスに属しています。



---

(注) Firepower 9300 の場合、すべてのモジュールがクラスタに属している必要があります。1つのセキュリティ モジュールにスタンドアロン論理デバイスを作成し、残り2つのセキュリティ モジュールを使用してクラスタを作成することはできません。

---

## 論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

### クラスタリングの要件と前提条件

#### クラスタ モデルのサポート

- Firepower 9300 の ASA：シャーシ内、シャーシ間、およびサイト間クラスタリングでサポート。
- Firepower 4100 シリーズの ASA：シャーシ間およびシャーシ内クラスタリングでサポート。
- Firepower 9300 の FTD：シャーシ内およびシャーシ間クラスタリングでサポート。
- Firepower 4100 シリーズの FTD：シャーシ間クラスタリングでサポート。
- Radware DefensePro：ASA によるシャーシ内クラスタリングでサポート。
- Radware DefensePro：FTD によるシャーシ内クラスタリングでサポート。

#### シャーシ間のクラスタリングハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower4100シリーズ：すべてのシャーシが同一モデルである必要があります。Firepower 9300：すべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- イメージアップグレード時を除き、同じFXOS ソフトウェアを実行する必要があります。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイス ID の容量が一致し、インターフェイスが同じバンド EtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイス モジュールの追加または削除、あるいは EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（スレーブ ユニットから始めて、マスターで終わります）。
- 同じ NTP サーバを使用する必要があります。Firepower Threat Defense のため、Firepower Management Center は同じ NTP サーバを使用する必要があります。手動で時間を設定しないでください。
- ASA：各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。スレーブ ユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defense では、すべてのライセンスは Firepower Management Center で処理されます。

#### シャーシ間クラスタリングのスイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「[Cisco FXOS Compatibility](#)」を参照してください。

#### サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect (DCI) に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
  - 合計 4 クラスタ メンバ

- 各サイト 2 メンバ
- メンバあたり 5 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 5 Gbps (2/2 x 5 Gbps)。

- 3 サイトの 6 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps (3/2 x 10 Gbps)。

- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク (10 Gbps) のサイズ未満になってはなりません)。

## 論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

### 一般的なガイドラインと制限事項

#### ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定することができます。ASA の場合、展開後に、ファイアウォール モードをトランスペアレントに変更することができます。[ASA のトランスペアレントファイアウォールモードへの変更 \(185 ページ\)](#) を参照してください。

#### ハイアベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- 詳細については、ハイアベイラビリティのためのアプリケーション設定ガイドの章を参照してください。

### コンテキストモード

- マルチ コンテキスト モードは ASA でのみサポートされています。
- 展開後に、ASA のマルチ コンテキスト モードを有効にします。

## クラスタリング ガイドラインと制限事項

### シャーン間クラスタリングのスイッチ

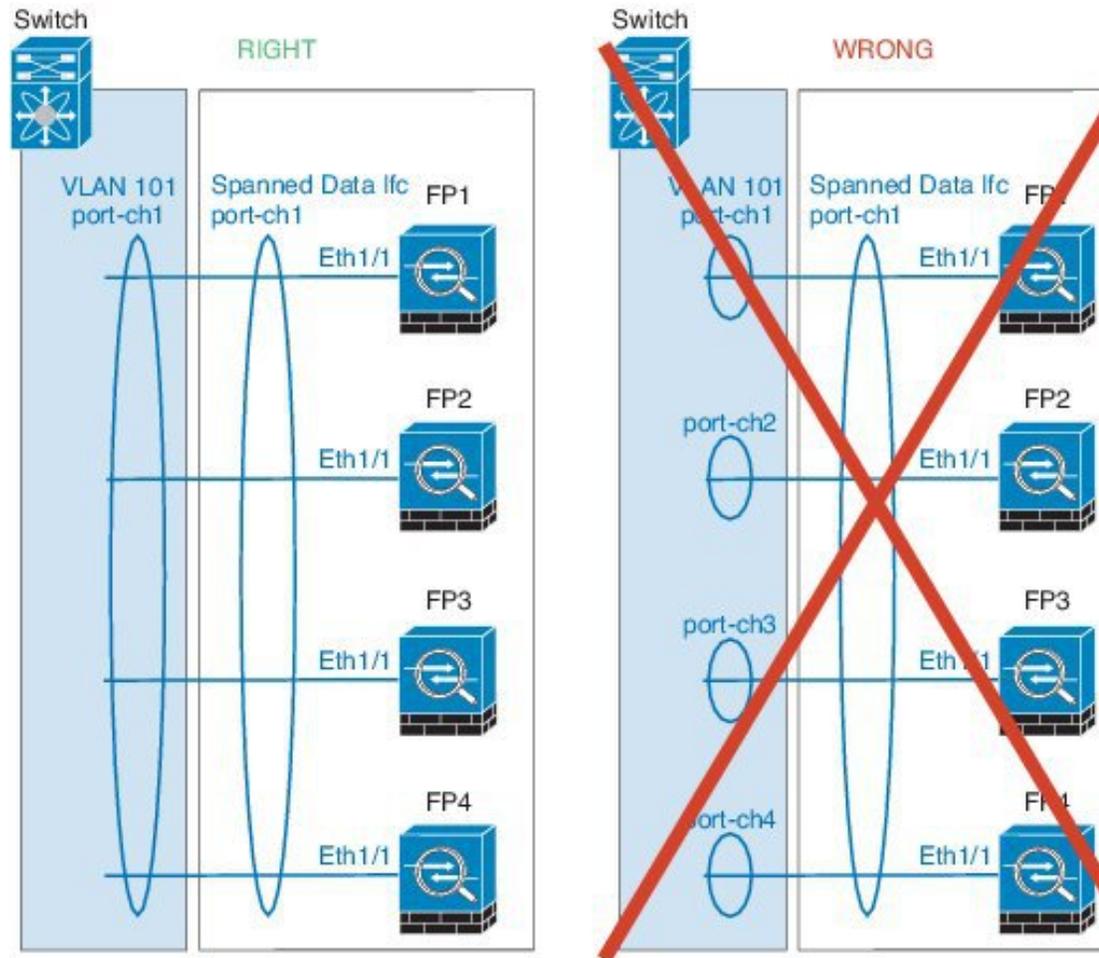
- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係（アジャセンシー）ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR IPv4 MTU と一致する必要があります。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチポートに対してスパンニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスバンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合がありますので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパンニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経路でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネルバンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタデバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

```
router(config)# port-channel id hash-distribution fixed
```

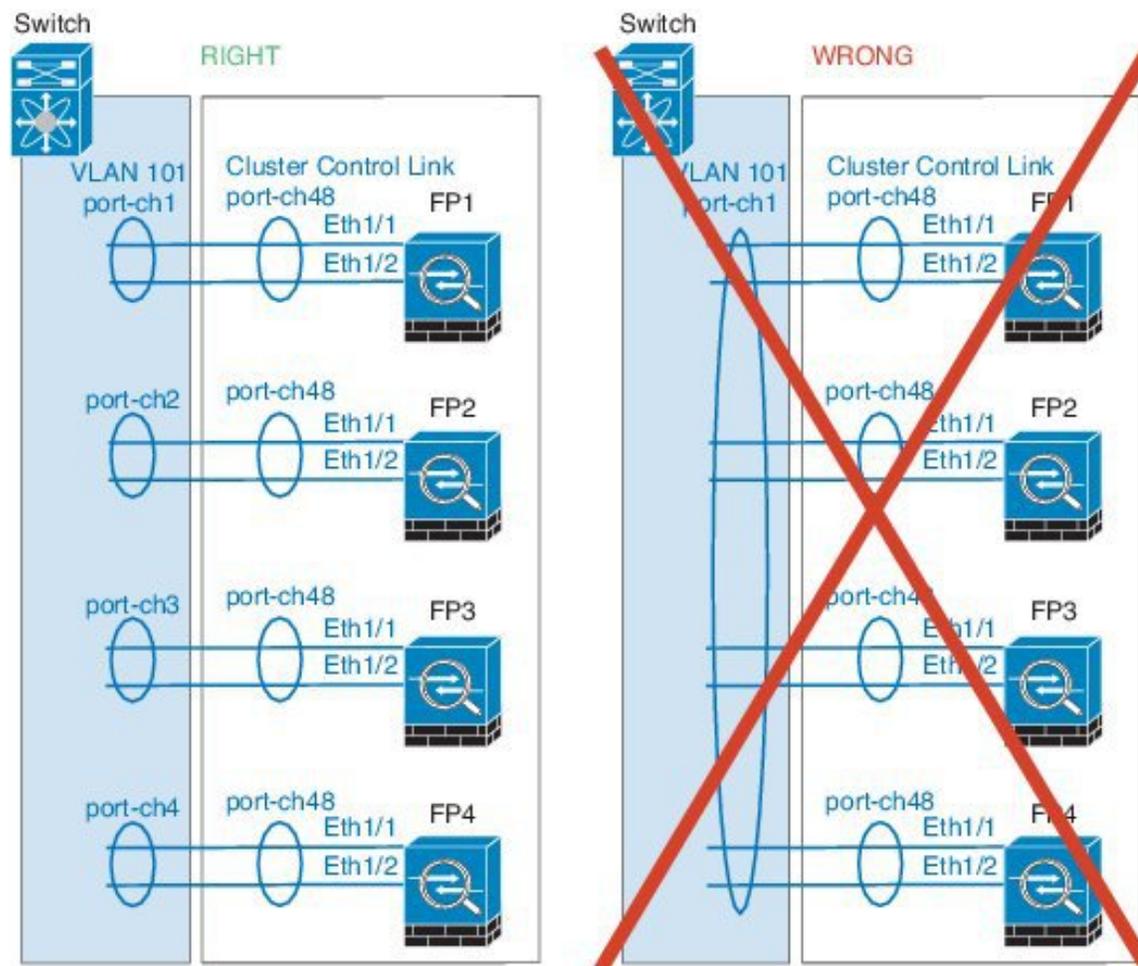
アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

### シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [fast] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサーブिस ソフトウェア アップグレード (ISSU) を実行する際に LACP 高速レートがサポートされないため、クラスタリングで ISSU を使用することは推奨されません。
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロス スタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 (無制限) などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタユニット スパンド EtherChannel (クラスタのすべてのメンバに広がる) の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャンネルグループ内にあることを確認してください。



- デバイスローカル EtherChannel : クラスタユニットデバイスローカル EtherChannel (クラスタ制御リンク用に設定された EtherChannel もこれに含まれます) は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



### サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間 (RTT) 20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタメンバには接続を再分散できません。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタローカリゼーションを有効にすると、接続オーナーと同じサイトからローカルディレクタ権限が常に選択されます (サイト ID に応じて)。また、元のオーナーに障害が発生するとローカルディレクタは同じサイトの新しいオーナーを選択します (注: サイト間でトラフィックが非対称で、元のオーナーに障害

が発生した後もリモートサイトから継続的なトラフィックがある場合、リモートサイトのユニットが re-hosting ウィンドウ内でデータパケットを受信する場合はこのリモートサイトのユニットが新しいオーナーとなることがあります)。

- ディレクタ ローカリゼーションでは、次のトラフィックタイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーションクエリ。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると (AKA ノースサウス挿入)、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタメンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイル用に各サイトのデータネットワークとゲートウェイルータ間にクラスタを配置すると (AKA イーストウェスト挿入)、各ゲートウェイルータは、HSRP などの First Hop Redundancy Protocol (FHRP) を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイトランスポート仮想化 (OTV) または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイルータが 1 つのサイトに到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- スパンド EtherChannel を使用したルーテッドモードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトに到達不能になった場合、トラフィックが正常に他のサイトのクラスタユニットに到達できるようにフィルタを削除する必要があります。ダイナミックルーティングは、サイト間クラスタが拡張セグメントのファーストホップルータとして機能する場合はサポートされません。

### その他のガイドライン

- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロンモードで一部のシャーシセキュリティモジュールをクラスタ化し、他のセキュリティモジュールを実行することはできません。クラスタ内にすべてのセキュリティモジュールを含める必要があります。

### デフォルト

クラスタ制御リンクはポートチャネル 48 を使用します。

## スタンドアロン論理デバイスの追加

スタンドアロン論理デバイスは単独またはハイアベイラビリティユニットとして使用できます。ハイアベイラビリティの使用率の詳細については、[ハイアベイラビリティペアの追加 \(160 ページ\)](#) を参照してください。

### スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイアベイラビリティペアで動作します。Firepower 9300 などの複数のモジュールデバイスでは、クラスタまたはスタンドアロンデバイスを導入できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュールクラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッドファイアウォールモード ASA を展開できます。ASA をトランスペアレントファイアウォールモードに変更するには、この手順を完了し、[ASA のトランスペアレントファイアウォールモードへの変更 \(185 ページ\)](#) を参照してください。

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチコンテキストモードを有効にする必要があります。

#### 始める前に

- 論理デバイスに使用するアプリケーションイメージを [Cisco.com](#) からダウンロードして ([Cisco.com からのイメージのダウンロード \(46 ページ\)](#) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティアプライアンスへのイメージのアップロード \(46 ページ\)](#) を参照)。



(注) シャーシ内のすべてのモジュールに同じアプリケーションインスタンスタイプ (ASA または Firepower Threat Defense) をインストールする必要があります。現時点では、他のアプリケーションタイプはサポートされていません。モジュールは特定のアプリケーションタイプの異なるバージョンを実行できますが、すべてのモジュールを同じタイプのアプリケーションインスタンスとして設定する必要があります。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません (シャーシ管理インターフェイスは、[Interfaces] タブの上部に [MGMT] として表示されます)。

## 手順

- ステップ 1** [Logical Devices] を選択します。  
[Logical Devices] ページに、シャーシ上にある論理デバイスのリストが表示されます。
- ステップ 2** [Add Device] をクリックします。  
[Add Device] ダイアログボックスが表示されます。
- ステップ 3** [Device Name] に論理デバイスの名前を入力します。  
この名前は、Firepower4100/9300 シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはセキュリティ モジュール/エンジン設定で使用されるデバイス名ではありません。
- ステップ 4** [Template] では、[Cisco Adaptive Security Appliance] を選択します。
- ステップ 5** [Image Version] を選択します。
- ステップ 6** [Device Mode] では、[Standalone] オプション ボタンをクリックします。
- ステップ 7** [OK] をクリックします。  
[Provisioning - device name] ウィンドウが表示されます。
- ステップ 8** [Data Ports] 領域を展開し、デバイスに割り当てるポートをそれぞれクリックします。
- ステップ 9** 画面中央のデバイスアイコンをクリックします。  
初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。
- ステップ 10** [General Information] タブで、次の手順を実行します。
- (Firepower 9300 などの複数のモジュールデバイスの場合) [Security Module Selection] の下で、この論理デバイスに使用するセキュリティ モジュールをクリックします。
  - [Management Interface] を選択します。
  - 管理インターフェイスを選択します。[Address Type]、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。
  - [Management IP] アドレスを設定します。
  - ネットワーク マスクまたはプレフィックス長を入力します。
  - ネットワーク ゲートウェイ アドレスを入力します。
- ステップ 11** [Settings] タブをクリックします。
- ステップ 12** 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。  
事前設定されている ASA 管理者ユーザおよびイネーブルパスワードはパスワードの回復時に役立ちます。FXOSアクセスが可能な場合、管理者ユーザパスワードを忘れたときにリセットできます。
- ステップ 13** [OK] をクリックして、設定ダイアログボックスを閉じます。

**ステップ 14** [Save] をクリックします。

シャーシは、指定したソフトウェア バージョンをダウンロードし、指定したセキュリティ モジュール/エンジンにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

**ステップ 15** 論理デバイスを導入後、デバイスの前に配置される DDoS 検出および緩和サービスとして、サードパーティの Radware DefensePro 仮想プラットフォームをインストールできます。Radware DefensePro について (177 ページ) を参照してください。

## スタンドアロン Firepower Threat Defense の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。Firepower 9300 などの複数のモジュールデバイスでは、クラスタまたはスタンドアロンデバイスを導入できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュール クラスタと単一のスタンドアロン デバイスをうまく組み合わせることはできません。

### 始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして (Cisco.com からのイメージのダウンロード (46 ページ) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします (Firepower セキュリティ アプライアンスへのイメージのアップロード (46 ページ) を参照)。



(注) シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ (ASA または Firepower Threat Defense) をインストールする必要があります。現時点では、他のアプリケーション タイプはサポートされていません。モジュールは特定のアプリケーション タイプの異なるバージョンを実行できますが、すべてのモジュールを同じタイプのアプリケーション インスタンスとして設定する必要があります。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません (シャーシ管理インターフェイスは、[Interfaces] タブの上部に [MGMT] として表示されます)。
- また、少なくとも 1 つのデータ型インターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック (Web イベントなど) を運ぶ firepower-eventing インターフェイスも作成できます。詳細については、インターフェイス タイプ (136 ページ) を参照してください。

## 手順

- ステップ 1** [Logical Devices] を選択します。  
[Logical Devices] ページに、シャーシ上にある論理デバイスのリストが表示されます。
- ステップ 2** [Add Device] をクリックします。  
[Add Device] ダイアログボックスが表示されます。
- ステップ 3** [Device Name] に論理デバイスの名前を入力します。  
この名前は、Firepower4100/9300 シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはセキュリティ モジュール/エンジン設定で使用されるデバイス名ではありません。
- ステップ 4** [Template] では、[Cisco Firepower Threat Defense] を選択します。
- ステップ 5** [Image Version] を選択します。
- ステップ 6** [Device Mode] では、[Standalone] オプション ボタンをクリックします。
- ステップ 7** [OK] をクリックします。  
[Provisioning - device name] ウィンドウが表示されます。
- ステップ 8** [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。  
ハードウェアバイパス 対応のポートは次のアイコンで表示されます：。ハードウェアバイパス ペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェアバイパス 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。
- ステップ 9** 画面中央のデバイス アイコンをクリックします。  
初期ブートストラップ設定を設定できるダイアログボックスが表示されます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。
- ステップ 10** [General Information] タブで、次の手順を実行します。
- (Firepower 9300 などの複数のモジュール デバイスの場合) [Security Module Selection] の下で、この論理デバイスに使用するセキュリティ モジュールをクリックします。
  - [Management Interface] を選択します。
  - 管理インターフェイスを選択します。[Address Type]、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。
  - [Management IP] アドレスを設定します。
  - ネットワーク マスクまたはプレフィックス長を入力します。
  - ネットワーク ゲートウェイ アドレスを入力します。
- ステップ 11** [Settings] タブで、次の手順を実行します。

- a) [Registration Key] フィールドで、登録時に Firepower Management Center と デバイス間で共有するキーを入力します。
- b) [Password] フィールドにデバイスのパスワードを入力します。
- c) [Firepower Management Center IP] フィールドに、管理 Firepower Management Center の IP アドレスを入力します。
- d) [Search Domains] フィールドに、デバイスの検索ドメインのカンマ区切りのリストを入力します。
- e) [Firewall Mode]、[Transparent]、または [Routed] を選択します。
- f) [DNS Servers] フィールドに、使用するデバイスの DNS サーバのカンマ区切りのリストを入力します。
- g) [Fully Qualified Hostname] フィールドに、脅威防御デバイスの完全修飾名を入力します。
- h) Firepower イベントの送信に使用する [Eventing Interface] を選択します。指定しない場合は、管理インターフェイスが使用されます。

Firepower イベントに使用するインターフェイスを指定するには、インターフェイスを *firepower-eventing* インターフェイスとして設定する必要があります。詳細については、[Firepower インターフェイスについて \(135 ページ\)](#) を参照してください。

**ステップ 12** [Agreement] タブで、エンドユーザライセンス (EULA) を読んで、同意します。

**ステップ 13** [OK] をクリックして、設定ダイアログボックスを閉じます。

**ステップ 14** [Save] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、指定したセキュリティ モジュール/エンジンにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

**ステップ 15** 論理デバイスを導入後、デバイスの前に配置される DDoS 検出および緩和サービスとして、サードパーティの Radware DefensePro 仮想プラットフォームをインストールできます。[Radware DefensePro について \(177 ページ\)](#) を参照してください。

## ハイアベイラビリティペアの追加

Firepower Threat Defense または ASA ハイアベイラビリティ (フェールオーバーとも呼ばれる) は、FXOS ではなく、アプリケーション内で設定します。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

### 始める前に

- ハイアベイラビリティシステム要件については、ハイアベイラビリティのアプリケーション設定ガイドの章を参照してください。

## 手順

- ステップ 1** 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイアベイラビリティは推奨されず、サポートされない可能性があります。
- ステップ 2** 各論理デバイスに同一のインターフェイスを割り当てます。
- ステップ 3** フェールオーバーリンクとステートリンクに対して1つまたは2つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイアベイラビリティトラフィックを交換します。統合されたフェールオーバーリンクとステートリンクには、10GBのデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがあれば、別のフェールオーバーおよびステートのリンクを使用できます。ステートリンクには、ほとんどの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。同じネットワークセグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

- ステップ 4** 論理デバイスでハイアベイラビリティを有効にします。
- ステップ 5** ハイアベイラビリティを有効にした後にインターフェイスを変更する必要がある場合は、スタンバイユニットを最初に変更し、次にアクティブユニットを変更します。

(注) ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

## クラスタの追加

クラスタリングを利用すると、複数のデバイスをグループ化して1つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。複数のモジュールを含む Firepower 9300 は、1つのシャーシ内のすべてのモジュールをクラスタにグループ化する、シャーシ内クラスタリングをサポートします。複数のシャーシをまとめてグループ化する、シャーシ間クラスタリングも使用できます。シャーシ間クラスタリングは、Firepower 4100 シリーズなどの単一モジュールデバイスの唯一のオプションです。

## Firepower 4100/9300 シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 4100/9300 シャーシにクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、この EtherChannel に物理インターフェイスを手動で割り当てる必要があります。
- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。  
クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 4100/9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。  
シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。シャーシ間クラスタリングでは、すべてのデータインターフェイスでスパンド EtherChannel を使用します。




---

(注) 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

---

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。

## 標準出荷単位とセカンダリ単位の役割

クラスタのメンバーの1つが標準出荷単位です。標準出荷単位は自動的に決定されます。他のすべてのメンバーはセカンダリ単位です。

すべてのコンフィギュレーション作業は標準出荷単位でのみ実行する必要があります。コンフィギュレーションはその後、セカンダリ単位に複製されます。

## クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。シャーシ間クラスタリングでは、このインターフェイスにメンバインターフェイスはありません。シャーシ間クラスタリングでは、EtherChannel に1つ以上のインターフェイスを追加する必要があります。このクラスタタイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。

2メンバシャーシ間クラスタの場合、シャーシと別のシャーシとの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が

発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

### シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロードバランシングが低下するので、すべてのリターントラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

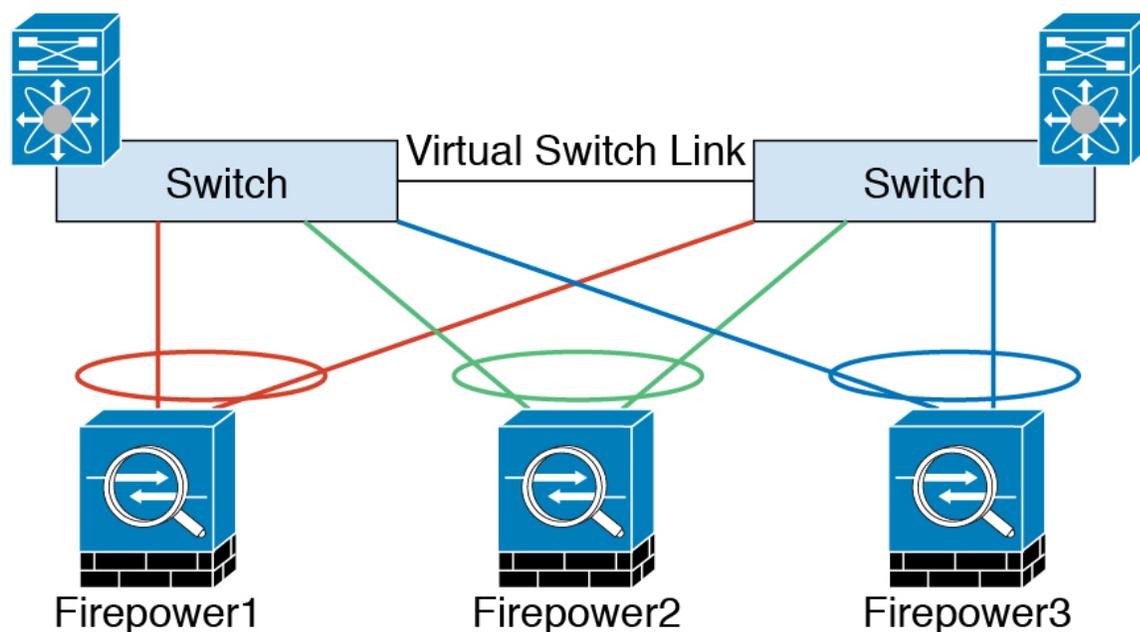
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。



- (注) クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

### シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 4100/9300 シャーシ インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイスローカルであることに注意してください。



### シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間 (RTT) が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

### クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID およびスロット ID (`127.2.chassis_id.slot_id`) に基づいて、各ユニットのクラスタ制御リンクインターフェイス IP アドレスを自動生成します。この IP アドレスは、FXOS でもアプリケーション内でも手動で設定できません。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。サイト間トラフィックには、オーバーレイ トランスポート 仮想化 (OTV) を使用することをお勧めします。

### 管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

### 管理インターフェイス

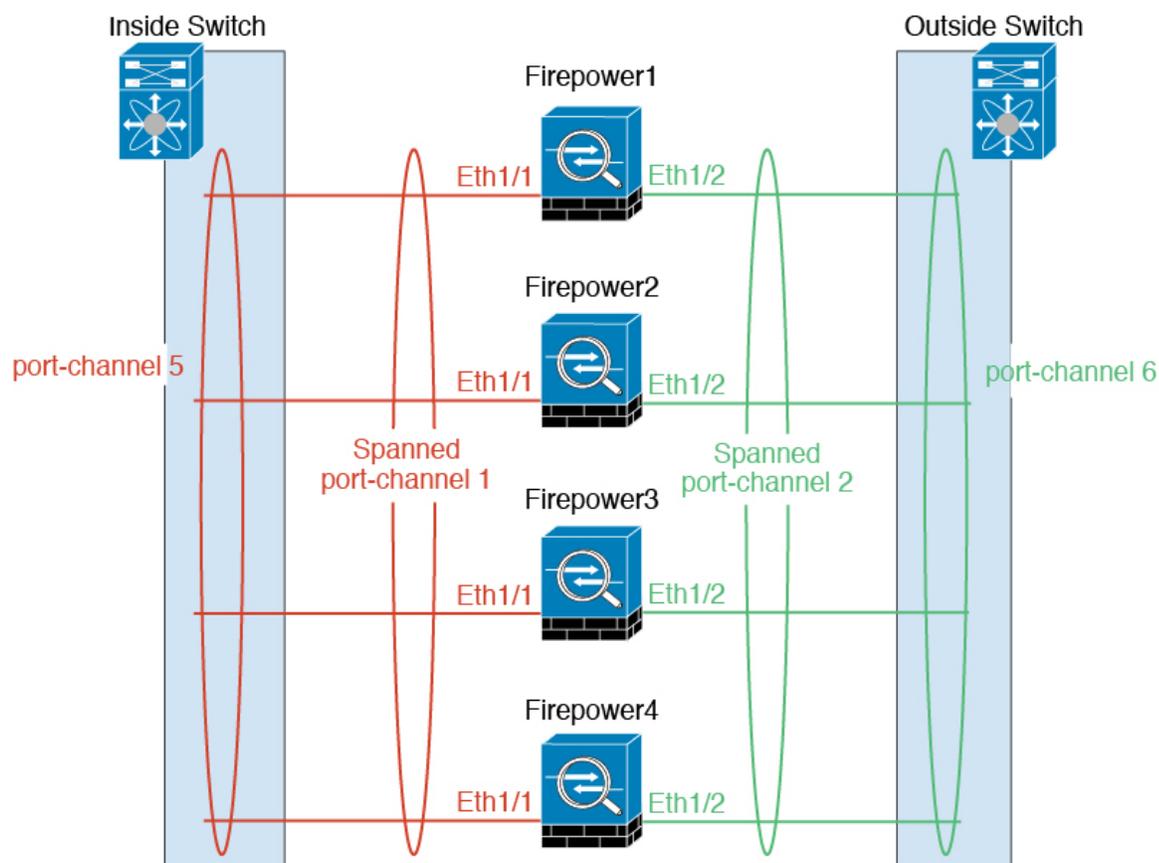
管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

ASA の場合は、メインクラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の標準出荷単位に属します。アドレス範囲も設定して、現在の標準出荷単位を含む各単位がその範囲内のローカルアドレスを使用できるようにする必要があります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。標準出荷単位が変更されると、メインクラスタ IP アドレスは新しい標準出荷単位に移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の標準出荷単位に関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、標準出荷単位を含む各単位は、ローカル IP アドレスを使用してサーバに接続します。

Firepower Threat Defense では、同じネットワークの各単位に管理 IP アドレスを割り当てます。各単位を FMC に追加するときは、次の IP アドレスを使用します。

## スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッドモードでは、EtherChannel は単一の IP アドレスを持つルーテッドインターフェイスとして設定されます。トランスペアレントモードでは、IP アドレスはブリッジグループメンバーではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



## サイト間クラスタリング

サイト間インストールの場合、次の推奨ガイドラインに従う限り、クラスタリングを利用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッドモードでサポートされます。

サイト ID は、LISP インспекションを使用したフローモビリティの有効化、データセンターのサイト間クラスタリングのパフォーマンス向上とラウンドトリップ時間の遅延短縮のためのディレクタローカリゼーションの有効化、およびトラフィックフローのバックアップオーナーが常にオーナーとは異なるサイトに存在する接続に対するサイト冗長性の有効化のためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング : [クラスタリングの要件と前提条件](#) (148 ページ)
- サイト間のガイドライン : [クラスタリング ガイドラインと制限事項](#) (151 ページ)
- サイト間での例 : [サイト間クラスタリングの例](#) (193 ページ)

## ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

## ASA クラスタの作成

Firepower 4100/9300 シャーシにクラスタを展開します。

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

Firepower 4100/9300 シャーシからルーテッドファイアウォールモード ASA を展開できます。ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。

### 始める前に

- モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。
- [Interfaces] タブで、ポートチャネル 48 クラスタタイプのインターフェイスは、メンバインターフェイスが含まれていない場合は、[Operation State] を [failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバインターフェイスを必要としないため、この動作状態は無視して構いません。

### 手順

**ステップ 1** クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel (ポートチャネルとも呼ばれる) を追加します。 [EtherChannel \(ポートチャネル\) の追加](#) (140 ページ) または [物理インターフェイスの設定](#) (140 ページ) を参照してください。

また、データインターフェイスはクラスタを展開した後でも、そのクラスタに追加できます。

シャーシ間クラスタリングでは、全データインターフェイスは 1 つ以上のメンバインターフェイスを持つ EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。

- ステップ 2** 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel (ポートチャネル) の追加 (140 ページ) または物理インターフェイスの設定 (140 ページ) を参照してください。
- シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される ([Interfaces] タブの上部に [MGMT] として表示される) シャーシ管理インターフェイスと同じではありません。
- ステップ 3** シャーシ間クラスタリングでは、ポートチャネル 48 にメンバーインターフェイスを追加し、クラスタ制御リンクとして使用します。
- メンバインターフェイスを含めないと、論理デバイスを展開したときに、Firepower Chassis Manager でこのクラスタがシャーシ内クラスタとみなされ、[Chassis ID] フィールドが表示されません。各シャーシに同じメンバインターフェイスを追加します。
- ステップ 4** [Logical Devices] を選択します。
- [Logical Devices] ページに、シャーシ上にある論理デバイスのリストが表示されます。
- ステップ 5** [Add Device] をクリックします。
- [Add Device] ダイアログボックスが表示されます。
- ステップ 6** [Device Name] に論理デバイスの名前を入力します。
- この名前は、Firepower 4100/9300 シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはセキュリティ モジュール/エンジン設定で使用されるデバイス名ではありません。
- ステップ 7** [Template] では、[Cisco Adaptive Security Appliance] を選択します。
- ステップ 8** [ASA Image Version] を選択します。
- ステップ 9** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 10** [Create New Cluster] ラジオ ボタンをクリックします。
- ステップ 11** [OK] をクリックします。
- スタンドアロンデバイスを設定している場合は、新しいクラスタに置き換えるように求められます。[Provisioning - device name] ウィンドウが表示されます。
- デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。
- ステップ 12** 画面中央のデバイス アイコンをクリックします。
- [ASA Configuration] ダイアログボックスが [Cluster Information] タブが選択された状態で表示されます。
- ステップ 13** [Chassis ID] フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。
- ステップ 14** サイト間クラスタリングの場合、[Site ID] フィールドに、このシャーシのサイト ID を 1 ~ 8 の範囲で入力します。

**ステップ 15** [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

共有秘密は、1～63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

**ステップ 16** [Cluster Group Name] を設定します。これはセキュリティ モジュール設定のクラスタ グループ名です。

名前は 1～38 文字の ASCII 文字列であることが必要です。

**ステップ 17** [Management Interface] をクリックして、先に作成した管理インターフェイスを選択します。

**ステップ 18** 管理インターフェイスの [Address Type] を選択します。

この情報は、セキュリティモジュール設定で管理インターフェイスを設定するために使用されます。

a) [Management IP Pool] フィールドに、開始アドレスと終了アドレスをハイフンで区切って入力し、ローカル IP アドレスのプールを設定します。このうちの1つがインターフェイス用に各クラスタ ユニットに割り当てられます。

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに3つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの1つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

b) ネットワーク マスクまたはプレフィックス長を入力します。

c) ネットワーク ゲートウェイを入力します。

d) 仮想 IP アドレスを入力します。

この IP アドレスは、クラスタ プールアドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

**ステップ 19** [Settings] タブをクリックします。

**ステップ 20** 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

**ステップ 21** [OK] をクリックして、[ASA Configuration] ダイアログボックスを閉じます。

**ステップ 22** [Save] をクリックします。

Firepower 4100/9300 シャーシスーパーバイザは、指定したソフトウェアバージョンをダウンロードし、各セキュリティ モジュールにクラスタ ブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを展開します。

**ステップ 23** シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

- a) 最初のシャーシの Firepower Chassis Manager で、右上の [Show Cluster Details] アイコンをクリックして、表示されるクラスタ設定をコピーします。
- b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。
- c) [Join an Existing Cluster] を選択します。
- d) [Copy config] チェック ボックスをクリックして、[OK] をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。
- e) [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。
- f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **Chassis ID** : 一意のシャーシ ID を入力します。
- **Site ID** : 正しいサイト ID を入力します。
- **Cluster Key** : (事前に入力されていない) 同じクラスタ キーを入力します。

[OK] をクリックします。

- g) [Save] をクリックします。

**ステップ 24** マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

## クラスタ メンバの追加

ASA クラスタ メンバを追加または置き換えます。



- (注) この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

### 始める前に

- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。

- マルチコンテキストモードでは、最初のクラスタメンバのASAアプリケーションでマルチコンテキストモードを有効にします。追加のクラスタメンバはマルチコンテキストモード設定を自動的に継承します。

## 手順

- 
- ステップ 1** 既存のクラスタシャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。
- ステップ 2** 右上の [Show Configuration] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
- ステップ 3** 新しいシャーシの Firepower Chassis Manager に接続して、[Add Device] をクリックします。
- ステップ 4** [Device Name] には、論理デバイスの名前を指定します。
- ステップ 5** [Template] では、[Cisco Adaptive Security Appliance] を選択します。
- ステップ 6** [Image Version] では、ASA のソフトウェアバージョンを選択します。
- ステップ 7** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 8** [Join an Existing Cluster] を選択します。
- ステップ 9** [Copy config] チェック ボックスをクリックして、[OK] をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。
- ステップ 10** [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。
- ステップ 11** 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。
- **Chassis ID** : 一意のシャーシ ID を入力します。
  - **Site ID** : 正しいサイト ID を入力します。
  - **Cluster Key** : (事前に入力されていない) 同じクラスタ キーを入力します。
- [OK] をクリックします。
- ステップ 12** [Save] をクリックします。
- 

## Firepower Threat Defense Cluster の追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。1つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、次のシャーシにほぼ同じ設定を入力します。

## Firepower Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。展開を容易にするために、1つのシャーシにクラスタを展開し、その後、最初のシャーシから次のシャーシにブートストラップコンフィギュレーションをコピーできます。

### 始める前に

- モジュールがインストールされていない場合でも、Firepower 9300 シャーシの3つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。
- [Interfaces] タブで、ポートチャネル 48 クラスタ タイプのインターフェイスは、メンバインターフェイスが含まれていない場合は、[Operation State] を [failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバインターフェイスを必要としないため、この動作状態は無視して構いません。

### 手順

- 
- ステップ 1** クラスタを展開する前に、1つ以上のデータ タイプのインターフェイスまたは EtherChannel (ポートチャネルとも呼ばれる) を追加します。
- 導入後にもクラスタにデータ インターフェイスを追加できます。
- シャーシ間クラスタリングでは、全データ インターフェイスは1つ以上のメンバインターフェイスを持つ EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。
- ステップ 2** 管理タイプのインターフェイスまたは EtherChannel を追加します。
- シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される ([Interfaces] タブの上部に [MGMT] として表示される) シャーシ管理インターフェイスと同じではありません。
- ステップ 3** シャーシ間クラスタリングでは、ポートチャネル 48 にメンバインターフェイスを追加し、クラスタ制御リンクとして使用します。
- メンバインターフェイスを含めないと、論理デバイスを展開したときに、Firepower Chassis Managerでこのクラスタがシャーシ内クラスタとみなされ、[Chassis ID] フィールドが表示されません。各シャーシに同じメンバインターフェイスを追加します。
- ステップ 4** (任意) Firepower-eventing インターフェイスを追加します。
- このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。

Firepower Threat Defense コマンドリファレンスの **configure network** コマンドを参照してください。

シャーシ間クラスタリングの場合、各シャーシに同じイベント インターフェイスを追加します。

**ステップ 5** [Logical Devices] を選択します。

[Logical Devices] ページに、シャーシ上にある論理デバイスのリストが表示されます。

**ステップ 6** [Add Device] をクリックします。

[Add Device] ダイアログボックスが表示されます。

**ステップ 7** [Device Name] に論理デバイスの名前を入力します。

この名前は、Firepower 4100/9300 シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはセキュリティ モジュール/エンジン設定で使用されるデバイス名ではありません。

**ステップ 8** [Template] には、[Cisco Firepower Threat Defense] を選択します。

**ステップ 9** Firepower Threat Defense の [Image Version] を選択します。

**ステップ 10** [Device Mode] では、[Cluster] オプション ボタンをクリックします。

**ステップ 11** [Create New Cluster] ラジオ ボタンをクリックします。

**ステップ 12** [OK] をクリックします。

スタンドアロンデバイスを設定している場合は、新しいクラスタに置き換えるように求められます。[Provisioning - device name] ウィンドウが表示されます。

シャーシ間クラスタリングの場合、デフォルトですべてのインターフェイスがクラスタに割り当てられています。ハードウェアバイパス対応ポートは次のアイコンのように表示されます：  
。ハードウェアバイパスペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェアバイパス機能を使用する必要はないため、必要に応じて単一のインターフェイスを割り当てることができます。ハードウェアバイパス ポートは、EtherChannel のメンバーとしてサポートされないため、シャーシ間クラスタリングではサポートされません。

**ステップ 13** 画面中央のデバイスアイコンをクリックします。

[Cisco Firepower Threat Defense Configuration] ダイアログボックスが表示されます。

**ステップ 14** [Cluster Information] タブで、次の手順を実行します。

- [Chassis ID] フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。
- サイト間クラスタリングの場合は、[Site ID] フィールドにこのシャーシのサイト ID (1 ~ 8) を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィックの認証キーを設定します。

共有秘密は、1～63文字のASCII文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

- d) [Cluster Group Name] を設定します。これは、論理デバイス設定のクラスタグループ名です。
- 名前は1～38文字のASCII文字列であることが必要です。
- e) [Management Interface] ドロップダウンリストから、論理デバイスで使用する管理インターフェイスを選択します。

ハードウェアバイパス対応のインターフェイスをマネジメントインターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

**ステップ 15** [Settings] タブで、次の手順を実行します。

- a) [Registration Key] フィールドに、登録時に Firepower Management Center とクラスタメンバー間で共有するキーを入力します。
- b) [Password] フィールドに、クラスタの管理者ユーザのパスワードを入力します。
- c) [Firepower Management Center IP] フィールドに、管理 Firepower Management Center の IP アドレスを入力します。
- d) [Search Domains] フィールドに、管理ネットワークの検索ドメインのカンマ区切りのリストを入力します。
- e) [Firewall Mode] ドロップダウンリストから、[Transparent] または [Routed] を選択します。
- f) [DNS Servers] フィールドに、FTD デバイスとその管理ネットワーク上で使用する必要がある DNS サーバのカンマ区切りのリストを入力します。
- g) [Fully Qualified Hostname] フィールドに、FTD デバイスの完全修飾名を入力します。
- h) [Eventing Interface] ドロップダウンリストから、Firepower イベントを送信するインターフェイスを選択します。指定しない場合は、管理インターフェイスが使用されます。

Firepower イベントに使用する別のインターフェイスを指定するには、*firepower-eventing* インターフェイスとしてインターフェイスを設定する必要があります。ハードウェアバイパス対応のインターフェイスを Eventing インターフェイスとして割り当てると、割り当てが意図的であることを確認する警告メッセージが表示されます。

**ステップ 16** [Interface Information] タブで、クラスタ内の各セキュリティモジュールの管理 IP アドレスを設定します。[Address Type] ドロップダウンリストからアドレスのタイプを選択し、セキュリティモジュールごとに次の手順を実行します。

(注) モジュールがインストールされていない場合でも、シャーシの3つすべてのモジュールスロットで IP アドレスを設定する必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

- a) [Management IP] フィールドで、IP アドレスを設定します。
- モジュールごとに同じネットワークの IP アドレスを指定します。
- b) ネットワーク マスクまたはプレフィックス長を入力します。

- c) ネットワーク ゲートウェイ アドレスを入力します。

**ステップ 17** [Agreement] タブで、エンドユーザ ライセンス契約 (EULA) を読み、これに同意します。

**ステップ 18** [OK] をクリックして、[Cisco Firepower Threat Defense Configuration] ダイアログボックスを閉じます。

**ステップ 19** [Save] をクリックします。

Firepower 4100/9300 シャーシスーパーバイザは、指定したソフトウェアバージョンをダウンロードし、各セキュリティ モジュールにクラスタ ブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを展開します。

**ステップ 20** シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

- a) 最初のシャーシの Firepower Chassis Manager で、右上にある [Show Configuration] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
- b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。
- c) [Join an Existing Cluster] を選択します。
- d) [Copy config] チェック ボックスをクリックして、[OK] をクリックします。このチェック ボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。
- e) [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。
- f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- **Chassis ID** : 一意のシャーシ ID を入力します。

- **Site ID** : サイト間クラスタリングの場合、このシャーシのサイト ID (1 ~ 8) を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。

- **Cluster Key** : (事前に入力されていない) 同じクラスタ キーを入力します。

- **Management IP** : 各モジュールの管理アドレスを、他のクラスタ メンバーと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

- g) [Save] をクリックします。

**ステップ 21** 管理 IP アドレスを使用して各ユニットを個別に Firepower Management Center に追加し、それらを Web インターフェイスでクラスタにグループ化します。

すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

## クラスタ メンバの追加

既存のクラスタ内の FTD クラスタ メンバを追加または置き換えます。



(注) この手順における FXOS の手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。ただし、Firepower Management Center に新しいモジュールを追加する必要があります。Firepower Management Center の手順までスキップします。

### 始める前に

- 置き換える場合は、Firepower Management Center から古いクラスタ メンバを削除する必要があります。新しいユニットに置き換えると、Firepower Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。

### 手順

- ステップ 1** 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。
- ステップ 2** 右上の [Show Configuration] アイコン () をクリックして、表示されるクラスタの設定をコピーします。
- ステップ 3** 新しいシャーシの Firepower Chassis Manager に接続して、[Add Device] をクリックします。
- ステップ 4** [Device Name] に論理デバイスの名前を入力します。
- ステップ 5** [Template] では、[Cisco Firepower Threat Defense] を選択します。
- ステップ 6** [Image Version] では、FTD ソフトウェア バージョンを選択します。
- ステップ 7** [Device Mode] では、[Cluster] オプション ボタンをクリックします。
- ステップ 8** [Join an Existing Cluster] を選択します。
- ステップ 9** [Copy config] チェック ボックスをクリックして、[OK] をクリックします。このチェックボックスをオフにする場合は、手動で最初のシャーシの設定に一致するように設定を入力する必要があります。
- ステップ 10** [Copy Cluster Details] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。
- ステップ 11** 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。
  - **Chassis ID** : 一意のシャーシ ID を入力します。

- **Site ID** : サイト間クラスタリングの場合、このシャーシのサイト ID (1 ~ 8) を入力します。この機能は、Firepower Management Center FlexConfig 機能を使用した場合にのみ構成可能です。
- **Cluster Key** : (事前に入力されていない) 同じクラスタ キーを入力します。
- **Management IP** : 各モジュールの管理アドレスを、他のクラスタ メンバと同じネットワーク上に存在する一意の IP アドレスとなるように変更します。

[OK] をクリックします。

**ステップ 12** [Save] をクリックします。

**ステップ 13** Firepower Management Center で、**[Devices] > [Device Management]** を選択してから **[Add] > [Add Device]** を選択して、新しい論理デバイスを追加します。

**ステップ 14** **[Add] > [Add Cluster]** を選択します。

**ステップ 15** ドロップダウン リストから現在の **[Master]** デバイスを選択します。

クラスタにすでに含まれているマスターデバイスを選択した場合、既存のクラスタの名前が自動入力され、**[Slave Devices]** ボックスに選択可能なすべてのスレーブ デバイスが表示されます。これには、FMC に追加したばかりの新しいユニットが含まれます。

**ステップ 16** **[Add]** をクリックし、次に **[Deploy]** をクリックします。

クラスタは新しいメンバを追加して更新されます。

## Radware DefensePro の設定

Cisco Firepower 4100/9300 シャーシは、単一ブレードで複数のサービス (ファイアウォール、サードパーティの DDoS アプリケーションなど) をサポートできます。これらのアプリケーションとサービスは、リンクされて、サービス チェーンを形成します。

## Radware DefensePro について

現在サービスされているサービス チェーン コンフィギュレーションでは、サードパーティ製の Radware DefensePro 仮想プラットフォームを ASA ファイアウォールの手前、または Firepower Threat Defense の手前で実行するようにインストールできます。Radware DefensePro は、Firepower 4100/9300 シャーシに分散型サービス妨害 (DDoS) の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。Firepower 4100/9300 シャーシでサービス チェーンが有効になると、ネットワークからのトラフィックは主要な ASA または Firepower Threat Defense ファイアウォールに到達する前に DefensePro 仮想プラットフォームを通過する必要があります。



- (注)
- Radware DefensePro 仮想プラットフォームは、*Radware vDP* (仮想 DefensePro) 、またはシンプルに *vDP* と呼ばれることがあります。
  - Radware DefensePro 仮想プラットフォームは、リンク デコレータと呼ばれることもあります。

## Radware DefensePro の前提条件

Radware DefensePro を Firepower 4100/9300 シヤーンシに導入する前に、**etc/UTC** タイムゾーンで NTP サーバを使用するように Firepower 4100/9300 シヤーンシを構成する必要があります。Firepower 4100/9300 シヤーンシの日付と時刻の設定の詳細については、[日時の設定 \(90 ページ\)](#) を参照してください。

## サービス チェーンのガイドライン

### モデル

- Radware DefensePro (vDP) プラットフォームは、次のセキュリティ アプライアンスの ASA でサポートされています。
  - Firepower 9300
  - Firepower 4120 : このプラットフォームでは、CLI を使用して Radware DefensePro を導入する必要があります。Firepower Chassis Manager は、この機能をサポートしていません。
  - Firepower 4140 : このプラットフォームでは、CLI を使用して Radware DefensePro を導入する必要があります。Firepower Chassis Manager は、この機能をサポートしていません。
  - Firepower 4150
- Radware DefensePro プラットフォームは、次のセキュリティ アプライアンスの Firepower Threat Defense でサポートされています。
  - Firepower 9300
  - Firepower 4110 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。
  - Firepower 4120 : 論理デバイスと同時にデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。
  - Firepower 4140

- Firepower 4150

### その他のガイドライン

- サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro (vDP) アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。
- DefensePro アプリケーションは最大3つのセキュリティ モジュールの個別のインスタンスとして動作できます。

## スタンドアロンの論理デバイスでの Radware DefensePro の設定

Radware DefensePro をスタンドアロン ASA または Firepower Threat Defense 論理デバイスの前にある単一のサービス チェーンにインストールするには、次の手順に従います。



- (注) Firepower 4120 または 4140 セキュリティ アプライアンス上で ASA の前に Radware vDP をインストールする場合、FXOS CLI を使用してデコレータを展開する必要があります。Radware DefensePro を、Firepower 4100 デバイス上で ASA の前にあるサービス チェーンにインストールして設定する方法の詳細な CLI 手順については、『FXOS CLI Configuration Guide』を参照してください。

### 始める前に

- vDP イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロード \(46 ページ\)](#)) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード \(46 ページ\)](#)) を参照)。
- Radware DefensePro アプリケーションは、シャーシ内クラスタのスタンドアロン構成で導入できます。シャーシ内クラスタリングについては、[シャーシ内クラスタの Radware DefensePro の設定 \(180 ページ\)](#) を参照してください。

### 手順

**ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定 \(140 ページ\)](#) に従ってインターフェイスを有効にし、そのタイプが `mgmt` になるように設定してください。そうしない場合、アプリケーション管理インターフェイスを共有できます。

**ステップ 2** [Logical Devices] を選択して [Logical Devices] ページを開きます。

[Logical Devices] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが表示されます。

- ステップ 3** スタンドアロン ASA または Firepower Threat Defense 論理デバイスを作成します（[スタンドアロン ASA の追加（156 ページ）](#) または [スタンドアロン Firepower Threat Defense の追加（158 ページ）](#) を参照）。
- ステップ 4** [Decorators] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - Configuration] ウィンドウが表示されます。[General Information] タブで、次のフィールドを設定します。
- ステップ 5** Firepower 4100/9300 シャーシに複数の vDP バージョンをアップロードしている場合は、[Version] ドロップダウンから使用するバージョンを選択します。
- ステップ 6** リソース構成可能な Radware DefensePro アプリケーションがある場合は、[Resource Profile] ドロップダウンの下に、サポートされているリソースプロファイルのリストが表示されます。デバイスに割り当てるリソースプロファイルを選択してください。リソースプロファイルを選択しない場合、デフォルトの設定が使用されます。
- ステップ 7** [Management Interface] ドロップダウンで、この手順のステップ 1 で作成した管理インターフェイスを選択します。
- ステップ 8** デフォルトの [Address Type]（[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]）を選択します。
- ステップ 9** 前のステップで選択した [Address Type] に基づいて次のフィールドを設定します。
- [Management IP] フィールドで、ローカル IP アドレスを設定します。
  - IPv4 のみ：ネットワーク マスクを入力します。  
IPv6 のみ：プレフィックス長を入力します。
  - ネットワーク ゲートウェイ アドレスを入力します。
- ステップ 10** デバイスに割り当てる各データ ポートの横にあるチェックボックスをクリックします。
- ステップ 11** [OK] をクリックします。
- ステップ 12** [Save] をクリックします。

Firepower eXtensible Operating System は、指定したソフトウェアバージョンをダウンロードし、指定したセキュリティモジュールにブートストラップコンフィギュレーションと管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](http://cisco.com) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## シャーシ内クラスタの Radware DefensePro の設定

Radware DefensePro イメージをインストールして ASA または Firepower Threat Defense シャーシ内クラスタの前にサービス チェーンを設定するには、次の手順に従います。



- (注) サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

### 始める前に

- vDP イメージを Cisco.com からダウンロードして ([Cisco.com からのイメージのダウンロード \(46 ページ\)](#)) を参照)、そのイメージを Firepower 4100/9300 シャーシにアップロードします ([Firepower セキュリティ アプライアンスへのイメージのアップロード \(46 ページ\)](#)) を参照)。

### 手順

- ステップ 1** vDP で別の管理インターフェイスを使用する場合は、[物理インターフェイスの設定 \(140 ページ\)](#) に従ってインターフェイスを有効にし、そのタイプが mgmt になるように設定してください。そうしない場合、アプリケーション管理インターフェイスを共有できます。
- ステップ 2** ASA または Firepower Threat Defense シャーシ内クラスタを設定します ([ASA クラスタの作成 \(167 ページ\)](#)) または [Firepower Threat Defense クラスタの作成 \(172 ページ\)](#) を参照)。  
シャーシ内クラスタを設定する手順の最後で [Save] をクリックする前に、以下のステップに従ってクラスタに vDP デコレータを追加しておく必要があります。
- ステップ 3** [Decorators] 領域で、[vDP] を選択します。[Radware: Virtual DefensePro - Configuration] ダイアログボックスが表示されます。[General Information] タブで、次のフィールドを設定します。
- ステップ 4** Firepower 4100/9300 シャーシに複数の vDP バージョンをアップロードした場合は、使用する vDP バージョンを [Version] ドロップダウンで選択します。
- ステップ 5** リソース構成可能な Radware DefensePro アプリケーションがある場合は、[Resource Profile] ドロップダウンの下に、サポートされているリソースプロファイルのリストが表示されます。デバイスに割り当てるリソースプロファイルを選択してください。リソースプロファイルを選択しない場合、デフォルトの設定が使用されます。
- ステップ 6** [Management Interface] ドロップダウンで管理インターフェイスを選択します。
- ステップ 7** vDP デコレータに割り当てる各データポートの横にあるチェックボックスをクリックします。
- ステップ 8** [Interface Information] タブをクリックします。
- ステップ 9** 使用する [Address Type] ([IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]) を選択します。
- ステップ 10** 各セキュリティモジュールで、次のフィールドを設定します。表示されるフィールドは、前のステップで選択した [Address Type] により異なります。
- [Management IP] フィールドで、ローカル IP アドレスを設定します。
  - IPv4 のみ：ネットワーク マスクを入力します。  
IPv6 のみ：プレフィックス長を入力します。
  - ネットワーク ゲートウェイ アドレスを入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [Save] をクリックします。

Firepower eXtensible Operating System は、指定したソフトウェアバージョンをダウンロードし、指定したセキュリティモジュールにブートストラップコンフィギュレーションと管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

ステップ 13 [Logical Devices] を選択して [Logical Devices] ページを開きます。

ステップ 14 設定された論理デバイスのリストをスクロールして vDP のエントリを表示します。[Management IP] 列に示されている属性を確認します。

- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*unknown*」と表示される場合は、vDP クラスタの作成を完了するために、DefensePro アプリケーションを入力してマスター IP アドレスを設定する必要があります。
- [CLUSTER-ROLE] 要素の DefensePro インスタンスが「*primary*」または「*secondary*」と表示される場合は、アプリケーションはオンラインで、クラスタ化されています。

#### 次のタスク

DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、[cisco.com](http://cisco.com) に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

## UDP/TCP ポートのオープンと vDP Web サービスの有効化

Radware APSolute Vision Manager インターフェイスは、さまざまな UDP/TCP ポートを使用して Radware vDP のアプリケーションと通信します。vDP のアプリケーションが APSolute Vision Manager と通信するために、これらのポートがアクセス可能でありファイアウォールによってブロックされないことを確認します。オープンする特定のポートの詳細については、APSolute Vision ユーザ ガイドの次の表を参照してください。

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

Radware APSolute Vision で FXOS シャーシ内に配置される Virtual DefensePro アプリケーションを管理するために、FXOS CLI を使用して vDP Web サービスを有効にする必要があります。

#### 手順

ステップ 1 FXOS CLI から、vDP のアプリケーション インスタンスに接続します。

```
connect module slot console
```

```
connect vdp
```

ステップ2 vDP Web サービスを有効化します。

```
manage secure-web status set enable
```

ステップ3 vDP アプリケーションのコンソールを終了して FXOS モジュール CLI に戻ります。

```
Ctrl ]
```

---

## 論理デバイスの管理

論理デバイスを削除し、ASA をトランスペアレント モードに変換し、インターフェイス コンフィギュレーションを変更し、既存の論理デバイスで他のタスクを実行できます。

## アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

### 手順

ステップ1 モジュール CLI に接続します。

```
connect module slot_number console
```

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot\_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

ステップ2 アプリケーションのコンソールに接続します。デバイスの適切なコマンドを入力します。

```
connect asa
```

```
connect ftd
```

```
connect vdp name
```

例：

```
Firepower-module1> connect asa
```

```
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

例：

```
Firepower-module1> connect ftd
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
>
```

**ステップ 3** アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA : **Ctrl-a, d** と入力
- FTD : **Ctrl-a, d** と入力
- vDP : **Ctrl-], .** と入力

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

**ステップ 4** FXOS CLI のスーパーバイザ レベルに戻ります。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパーバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

## 論理デバイスの削除

### 手順

**ステップ 1** [Logical Devices] を選択して [Logical Devices] ページを開きます。

[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。

**ステップ 2** 削除する論理デバイスの [Delete] をクリックします。

**ステップ 3** [Yes] をクリックして、論理デバイスの削除を確認します。

**ステップ 4** [Yes] をクリックして、アプリケーション設定の削除を確認します。

## 論理デバイスに関連付けられていないアプリケーションインスタンスの削除

論理デバイスを削除すると、その論理デバイスのアプリケーション設定も削除するかどうか尋ねられます。アプリケーション設定を削除しない場合、そのアプリケーションインスタンスが削除されるまで、別のアプリケーションを使用して論理デバイスを作成することはできません。セキュリティモジュール/エンジンが論理デバイスとすでに関連付けられていない場合は、アプリケーションインスタンスを削除するために以下の手順を使用できます。

### 手順

**ステップ 1** [Logical Devices] を選択して、[Logical Devices] ページを開きます。

[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。論理デバイスのリストの下に、論理デバイスに関連付けられていないアプリケーションインスタンスのリストが表示されます。

**ステップ 2** 削除するアプリケーションインスタンスの [Delete] をクリックします。

**ステップ 3** [Yes] をクリックして、このアプリケーションインスタンスを削除することを確認します。

## ASA のトランスペアレント ファイアウォール モードへの変更

Firepower 4100/9300 シャーシのルーテッドファイアウォールモード ASA のみを導入できません。ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。スタンドアロン ASA の場合、ファイアウォールモードを変更すると設定が消去されるため、Firepower 4100/9300 シャーシから設定を

再導入して、ブートストラップ設定を回復する必要があります。ASA はトランスペアレントモードのまま、ブートストラップ設定が機能した状態になっています。クラスタ化された ASA の場合、設定は消去されないため、FXOS からブートストラップ設定を再導入する必要はありません。

## 手順

**ステップ 1** [アプリケーションのコンソールへの接続 \(183 ページ\)](#) に従って、ASA コンソールに接続します。クラスタの場合、プライマリ ユニットに接続します。フェールオーバー ペアの場合、アクティブ ユニットに接続します。

**ステップ 2** コンフィギュレーション モードに入ります。

**enable**

**configure terminal**

デフォルトでは、イネーブルパスワードは空白です。

**ステップ 3** ファイアウォール モードをトランスペアレントに設定します。

**firewall transparent**

**ステップ 4** 設定を保存します。

**write memory**

クラスタまたはフェールオーバー ペアの場合、この設定はセカンダリ ユニットに複製されます。

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
End Configuration Replication to slave.

asa(config)#
```

**ステップ 5** Firepower Chassis Manager の [Logical Devices] ページで、[Edit] アイコンをクリックして ASA を編集します。

[Provisioning] ページが表示されます。

**ステップ 6** デバイスのアイコンをクリックして、ブートストラップ設定を編集します。設定の値を変更し、[OK] をクリックします。

少なくとも 1 つのフィールド ([Password] フィールドなど) の値を変更する必要があります。

ブートストラップ設定の変更に関する警告が表示されます。[Yes] をクリックします。

**ステップ7** [Restart Now] をクリックして、ASA に設定を再導入します。シャーシ間クラスタまたはフェールオーバーペアの場合、各シャーシでステップ5～7を繰り返してブートストラップ設定を再導入します。

シャーシ/セキュリティ モジュールがリロードし、ASA が再度稼働するまで数分待ちます。ASA は、これでブートストラップ設定が機能するようになりますが、トランスペアレントモードのままです。

## Firepower Threat Defense 論理デバイスのインターフェイスの変更

Firepower Threat Defense 論理デバイスでは、インターフェイスの割り当てや割り当て解除、または管理インターフェイスの置き換えを行うことができます。その後、Firepower Management Center でインターフェイス設定を同期できます。

### 始める前に

- [物理インターフェイスの設定 \(140 ページ\)](#) および [EtherChannel \(ポート チャネル\) の追加 \(140 ページ\)](#) に従って、インターフェイスを設定し、EtherChannel を追加します。
- 論理デバイスに影響を与えず、かつ Firepower Management Center での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスまたは Firepower イベント インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。Firepower Threat Defense デバイスがリブートし（管理インターフェイスを変更するとリブートします）、Firepower Management Center で設定を同期すると、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- クラスタリングや高可用性のため、Firepower Management Center で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスレーブ/スタンバイユニットでインターフェイスを変更してから、マスター/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼさないことに注意してください。

### 手順

**ステップ1** Firepower Chassis Manager で、[Logical Devices] を選択します。

- ステップ 2** 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。
- ステップ 3** [Data Ports] 領域でデータ インターフェイスの選択を解除して、そのインターフェイスの割り当てを解除します。
- ステップ 4** [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。
- ステップ 5** 次のように、管理インターフェイスまたはイベント インターフェイスを置き換えます。  
これらのタイプのインターフェイスでは、変更を保存するとデバイスがリブートします。
- ページ中央のデバイス アイコンをクリックします。
  - [General/Cluster Information] タブで、ドロップダウンリストから新しい [Management Interface] を選択します。
  - [Settings] タブで、ドロップダウンリストから新しい [Eventing Interface] を選択します。
  - [OK] をクリックします。
- 管理インターフェイスの IP アドレスを変更した場合は、Firepower Management Center でデバイスの IP アドレスも変更する必要があります。[Devices] > [Device Management] > [Device/Cluster] と移動します。[Management] 領域で、ブートストラップ設定アドレスと一致するように IP アドレスを設定します。
- ステップ 6** [Save] をクリックします。
- ステップ 7** Firepower Management Center にログインします。
- ステップ 8** [Devices] > [Device Management] の順に選択し、FTD デバイスの編集アイコン (✎) をクリックします。[Interfaces] タブがデフォルトで選択されています。
- ステップ 9** [Interfaces] タブの左上にある [Sync Interfaces from device] ボタンをクリックします。
- ステップ 10** [Save] をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更を展開するまで、変更は有効ではありません。

## ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

### 始める前に

- 物理インターフェイスの設定 (140 ページ) および EtherChannel (ポート チャネル) の追加 (140 ページ) に従って、インターフェイスを設定し、EtherChannel を追加します。
- 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには (たとえば、デフォルトではすべてのインターフェイスがクラスターに割り当てられます)、まず論理デ

デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。

- FXOS で割り当てられたインターフェイスを削除すると（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または割り当てられたインターフェイスの EtherChannel への再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。
- 管理インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータメンバーインターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。ASA がリロードし（管理インターフェイスを変更するとリロードします）、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- クラスタリングまたはフェールオーバーのために、必ずすべてのユニットでインターフェイスを追加または削除します。最初にスレーブ/スタンバイユニットでインターフェイスを変更してから、マスター/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

## 手順

**ステップ 1** Firepower Chassis Manager で、[Logical Devices] を選択します。

**ステップ 2** 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。

**ステップ 3** [Data Ports] 領域でデータ インターフェイスの選択を解除して、そのインターフェイスの割り当てを解除します。

**ステップ 4** [Data Ports] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

**ステップ 5** 次のように、管理インターフェイスを置き換えます。

このタイプのインターフェイスでは、変更を保存するとデバイスがリロードします。

- a) ページ中央のデバイス アイコンをクリックします。
- b) [General/Cluster Information] タブで、ドロップダウンリストから新しい [Management Interface] を選択します。
- c) [OK] をクリックします。

**ステップ 6** [Save] をクリックします。

## 論理デバイスのブートストラップ設定の変更または回復

論理デバイスのブートストラップ設定は、変更することができます。変更した後、直ちに新しい設定を使用してアプリケーションを再起動することも、変更を保存しておいて後で新しい設定を使用してアプリケーションインスタンスを再起動することもできます。

### 手順

- ステップ 1 Firepower Chassis Manager で、[Logical Devices] を選択します。
- ステップ 2 右上にある [Edit] アイコンをクリックして、その論理デバイスを編集します。
- ステップ 3 ページ中央のデバイス アイコンをクリックします。
- ステップ 4 必要に応じて論理デバイスの設定を変更します。
- ステップ 5 [OK] をクリックします。
- ステップ 6 [Restart Now] をクリックして、変更を保存すると同時にアプリケーションインスタンスを再起動します。アプリケーションインスタンスを再起動せずに変更を保存するには、[Restart Later] をクリックします。

(注) [Restart Later] を選択した場合、アプリケーションインスタンスを再起動する準備が整ってから、[Logical Devices] ページで [Restart Instance] をクリックしてアプリケーションインスタンスを再起動できます。

## [Logical Devices] ページ

Firepower Chassis Manager の [Logical Devices] ページを使用して、論理デバイスを作成、編集、削除します。[Logical Devices] ページには、各 Firepower 4100/9300 シャーシセキュリティモジュール/エンジンにインストールされている論理デバイスの情報エリアが含まれています。

各論理デバイス エリアのヘッダーには次の情報が含まれています。

- 論理デバイスの一意の名前。
- 論理デバイスのモード（スタンドアロンまたはクラスタ）。
- [Status] : 論理デバイスの状態を示します。
  - [ok] : 論理デバイスの設定は完了しています。
  - [incomplete-configuration] : 論理デバイス設定は未完了です。

各論理デバイス エリアには次の情報が含まれています。

- [Security Module] : セキュリティ モジュールを示します。
- [Ports] : アプリケーション インスタンスに割り当てられたポートを示します。

- [Application] : セキュリティ モジュールで実行しているアプリケーションを示します。
- [Version] : セキュリティモジュールで実行しているアプリケーションのソフトウェアバージョン番号を示します。



---

(注) FTD の論理デバイスへの更新は Firepower Management Center を使用して行います。Firepower Chassis Manager の **[Logical Devices]** > **[Edit]** および **[System]** > **[Updates]** ページには反映されません。これらのページで、表示されるバージョンは、FTD 論理デバイスを作成するために使用されたソフトウェアバージョン (CSP イメージ) を示します。

---

- [Management IP] : 論理デバイス管理 IP として割り当てられているローカル IP アドレスを示します。
- [Gateway] : アプリケーションインスタンスに割り当てられているネットワーク ゲートウェイ アドレスを示します。
- [Management Port] : アプリケーションインスタンスに割り当てられている管理ポートを示します。
- [Status] : アプリケーション インスタンスの状態を示します。
  - [Online] : アプリケーションは実行中であり、動作しています。
  - [Offline] : アプリケーションは停止され、使用できません。
  - [Installing] : アプリケーションのインストールを実行しています。
  - [Not Installed] : アプリケーションがインストールされていません。
  - [Install Failed] : アプリケーションのインストールに失敗しました。
  - [Starting] : アプリケーションを起動しています。
  - [Start Failed] : アプリケーションの起動に失敗しました。
  - [Started] : アプリケーションは正常に開始し、アプリケーション エージェントのハートビートを待機しています。
  - [Stopping] : アプリケーションは停止処理中です。
  - [Stop Failed] : アプリケーションをオフラインにできませんでした。
  - [Not Responding] : アプリケーションは応答不能です。
  - [Updating] : アプリケーション ソフトウェアの更新が進行中です。
  - [Update Failed] : アプリケーション ソフトウェアの更新に失敗しました。
  - [Update Succeeded] : アプリケーション ソフトウェアの更新に成功しました。

- [Unsupported] : このインストール済みアプリケーションはサポートされていません。

セキュリティモジュールが存在しないか障害状態の場合は、その情報がステータスフィールドに表示されます。情報アイコンにカーソルを合わせると、障害に関する詳細情報が表示されます。セキュリティモジュールの障害について詳しくは、[FXOS セキュリティモジュール/セキュリティエンジンについて \(199 ページ\)](#) を参照してください。

- [Attributes] : 現在実行中のアプリケーションインスタンスの追加属性を示します。



(注) アプリケーションのブートストラップ設定を変更した後、直ちにアプリケーションインスタンスを起動しなければ、[Attributes] フィールドには現在実行中のアプリケーションに関する情報が表示され、アプリケーションを再起動するまで変更は反映されません。

- [Cluster Operation Status] : アプリケーションインスタンスに割り当てられている管理 URL を示します。
- [Management IP/Firepower Management IP] : アプリケーションインスタンスに割り当てられている管理 IP アドレスを示します。
- [Cluster Role] : アプリケーションインスタンス、マスターまたはスレーブのクラスターロールを示します。
- [HA Role] : アプリケーションインスタンス、アクティブまたはスタンバイのハイアベイラビリティロールを示します。
- [Management URL] : アプリケーションインスタンスに割り当てられている管理アプリケーションの URL を示します。
- [UUID] : アプリケーションインスタンスの汎用一意識別子を示します。

Firepower Chassis Manager の [Logical Devices] ページから、論理デバイスに対して次の機能を実行できます。

- [Refresh] : [Logical Devices] ページに表示されている情報が更新されます。
- [Add Device] : 論理デバイスを作成できます。
- [Edit] : 既存の論理デバイスを編集できます。
- [Update Version] : 論理デバイス上のソフトウェアをアップグレードまたはダウングレードできます。
- [Delete] : 論理デバイスが削除されます。
- [Show Configuration] : ダイアログボックスが開き、論理デバイスまたはクラスターの構成情報が JSON 形式で表示されます。クラスタに含める追加デバイスを作成する際は、この構成情報をコピーして使用できます。

- [Enable/Disable] : アプリケーション インスタンスが有効化/無効化されます。
- [Upgrade/Downgrade] : アプリケーション インスタンスをアップグレード/ダウングレードできます。
- [Restart Instance] : アプリケーション インスタンスを再起動できます。デバイスのブートストラップ情報を変更した後、アプリケーションインスタンスをまだ再起動していない場合、[Restart Instance] をクリックすることで、既存の管理ブートストラップ情報をクリアし、新しいブートストラップ情報を使用してアプリケーションインスタンスを再起動できます。
- [Go To Device Manager] : アプリケーション インスタンスに定義されている Firepower Management Center または ASDM へのリンクを提示します。

## サイト間クラスタリングの例

次の例ではサポートされるクラスタの導入を示します。

### スバンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

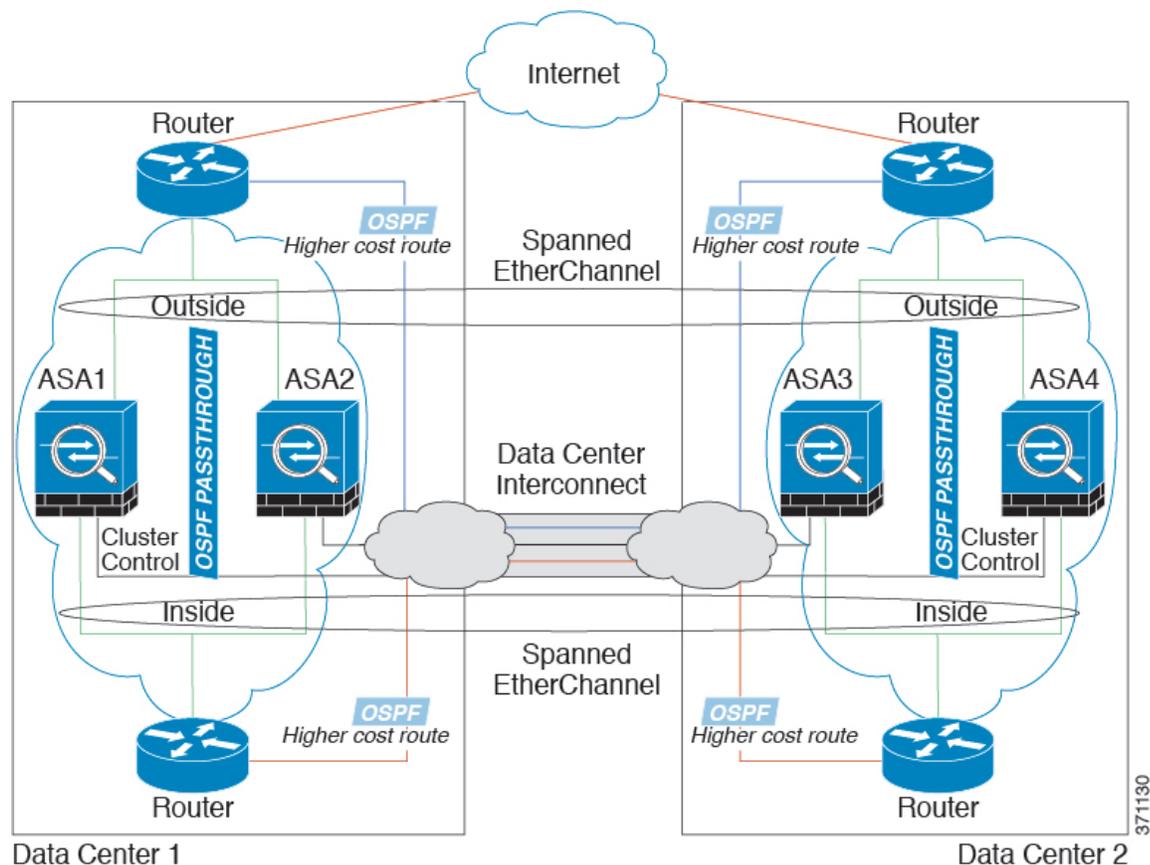
次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2つのデータセンターのそれぞれに2つのクラスタメンバがある場合を示します。クラスタメンバは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバは、内部および外部のスバンドEtherChannelsを使用してローカルスイッチに接続します。各EtherChannelは、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータはOSPFを使用し、トランスペアレントASAを通過します。MACとは異なり、ルータのIPはすべてのルータで一意です。DCIに高コストルートを割り当てることにより、特定のサイトですべてのクラスタメンバがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASAを通過する低コストのルートは、各サイトで同じブリッジグループを横断する必要があります。1つのサイトのすべてのクラスタメンバに障害が発生した場合、トラフィックは各ルータからDCI経由で他のサイトのクラスタメンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間VSS/vPC : このシナリオでは、データセンター1に1台のスイッチをインストールし、データセンター2に別のスイッチをインストールします。1つのオプションとして、各データセンターのクラスタユニットはローカルスイッチだけに接続し、VSS/vPCトラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCIが余分なトラフィック量を処理できる場合、各ユニットをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。

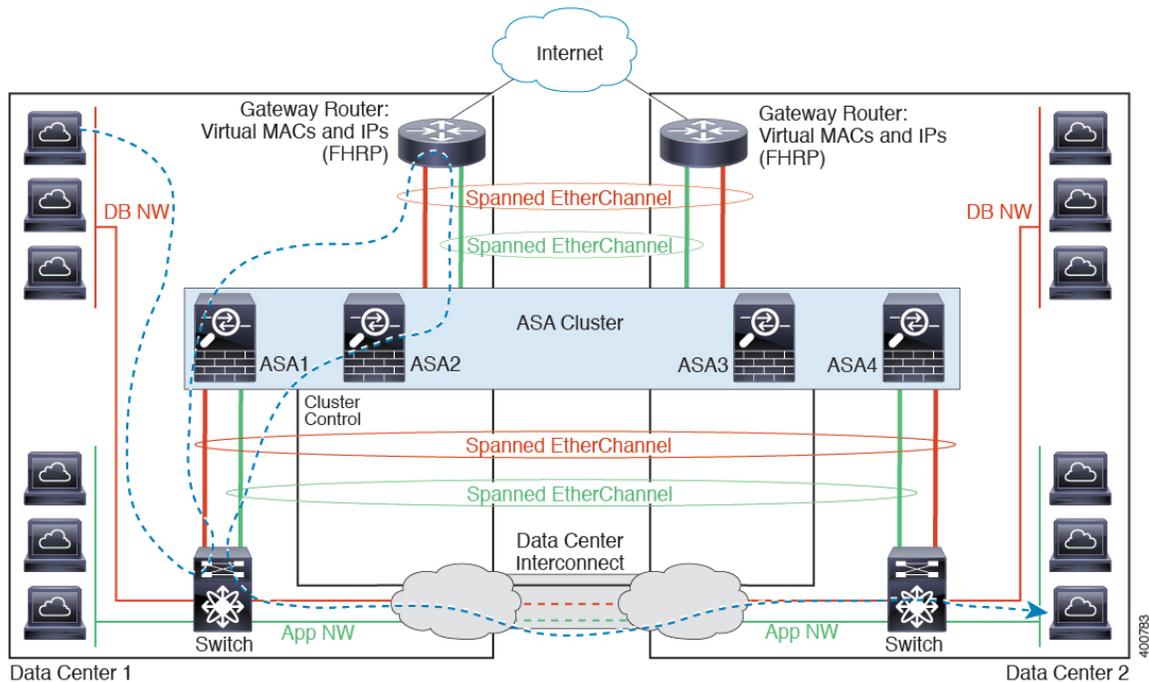
- 各サイトのローカル VSS/vPC : スイッチの冗長性を高めるには、各サイトに2つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタユニットは、両方のローカルスイッチだけに接続されたデータセンター1のシャーシおよびこれらのローカルスイッチに接続されたデータセンター2のシャーシとはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。



## スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイルータと2つの内部ネットワーク（アプリケーションネットワークとDBネットワーク）間に配置された（イーストウェスト挿入）2つのデータセンターのそれぞれに2つのクラスタメンバがある場合を示します。クラスタメンバは、DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタメンバは、内部および外部のアプリケーションネットワークとDBネットワークの両方にスパンド EtherChannels を使用してローカルスイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレスと IP アドレスを提供します。予期せぬ MAC アドレスのフラッピングを避けるために推奨されている方法は、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することです。これらのエントリがないと、サイト1のゲートウェイがサイト2のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト2に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート 仮想化 (OTV) (または同様のもの) を使用してサイト間に拡張されます。トラフィックがゲートウェイルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1つのサイトのゲートウェイルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



vPC/VSS オプションについては、スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例 (193 ページ) を参照してください。

## 論理デバイスの履歴

| 機能名                                            | プラットフォーム リリース | 機能情報                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower 4100/9300 シャーシ上の ASA のサイト間クラスタリングの改善 | 2.1(1)        | <p>ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は、ASA アプリケーション内でサイト ID を設定する必要がありました。この新機能により初期展開が簡単になります。</p> <p>ASA 構成内でサイト ID を設定することはできないことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。</p> <p>次の画面が変更されました。 <b>[Logical Devices] &gt; [Configuration]</b></p> |
| 6つの FTD モジュールのシャーシ間クラスタリング                     | 2.1(1)        | <p>FTD のシャーシ間クラスタリングを有効化できます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。</p> <p>次の画面が変更されました。 <b>[Logical Devices] &gt; [Configuration]</b></p>                                                                                                                                                                                                             |
| Firepower 9300 の FTD でのシャーシ内クラスタリング サポート       | 1.1.4         | <p>Firepower 9300 が FTD アプリケーションでシャーシ内クラスタリングをサポートするようになりました。</p> <p>次の画面が変更されました。 <b>[Logical Devices] &gt; [Configuration]</b></p>                                                                                                                                                                                                                 |
| 6つの ASA モジュールのシャーシ間クラスタリング                     | 1.1.3         | <p>ASA のシャーシ間クラスタリングが実現されました。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。</p> <p>次の画面が変更されました。 <b>[Logical Devices] &gt; [Configuration]</b></p>                                                                                                                                                                                                             |

| 機能名                     | プラットフォーム リリース | 機能情報                                                                                                                                   |
|-------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Cisco ASA のシャーシ内クラスタリング | 1.1.1         | Firepower 9300 シャーシ内のすべての ASA セキュリティ モジュールをクラスタ化できるようになりました。<br><br>次の画面が導入されました。[ <b>Logical Devices</b> ] > [ <b>Configuration</b> ] |





## 第 11 章

# セキュリティ モジュール/エンジン管理

- [FXOS セキュリティ モジュール/セキュリティ エンジンについて \(199 ページ\)](#)
- [セキュリティ モジュールの使用停止/再稼働 \(201 ページ\)](#)
- [セキュリティ モジュール/エンジンの確認応答 \(202 ページ\)](#)
- [セキュリティ モジュール/エンジンのリセット \(202 ページ\)](#)
- [セキュリティ モジュール/エンジンの再初期化 \(203 ページ\)](#)
- [ネットワーク モジュールのオフラインまたはオンラインの切り替え \(204 ページ\)](#)
- [インストールされているモジュール/エンジンの電源オン/オフ \(205 ページ\)](#)

## FXOS セキュリティ モジュール/セキュリティ エンジンについて

Firepower Chassis Manager の [Security Modules/Security Engine] ページから、セキュリティ モジュール/エンジンのステータスを表示したり、セキュリティ モジュール/エンジンに対してさまざまな機能を実行したりできます。

[Security Modules/Security Engine] ページに次の情報が表示されます。

- [Hardware State] : セキュリティ モジュール/エンジンのハードウェアの状態を表示します。
  - [Up] : セキュリティ モジュール/エンジンに正常に電源が投入され、ハードウェア障害は見られません。
  - [Booting Up] : セキュリティ モジュール/エンジンに電源投入中です。
  - [Down] : セキュリティ モジュール/エンジンに電源が投入されていないか、ハードウェア障害によってセキュリティ モジュール/エンジンが正常に起動できません。
  - [Unassociated] : セキュリティ モジュール/エンジンには、関連付けられている論理デバイスがありません。
  - [Mismatch] : セキュリティ モジュールが使用停止となっているか、新しいセキュリティ モジュールがスロットにインストールされていませんでした。再稼働または確認応答機能を使用して、セキュリティ モジュールを機能している状態に戻します。

- [Empty] : スロットにセキュリティ モジュールは取り付けられていません。
- [Service State] : セキュリティ モジュール/エンジンのソフトウェアの状態を表示します。
  - [Not-available] : セキュリティ モジュールはシャーシのスロットから取り外されています。セキュリティ モジュールを再度取り付け、通常の動作状態に戻します。
  - [Offline] : セキュリティ モジュール/エンジンはインストールされていますが、使用が停止されて電源がオフになっているか、この時点では電源投入中になっています。
  - [Online] : セキュリティ モジュール/エンジンはインストールされており、通常の動作モードになっています。
  - [Not Responding] : セキュリティ モジュール/エンジンは応答不能です。
  - [Token Mismatch] : 以前に設定したもの以外のセキュリティ モジュールがシャーシ スロットにインストールされていることを示します。これは、ソフトウェアのインストールエラーが原因である可能性もあります。再初期化機能を使用して、セキュリティ モジュールを機能している状態に戻します。
  - [Online] : セキュリティ モジュール/エンジンは障害状態にあります。障害状態の原因についての詳細情報を得るには、システム障害リストを確認してください。障害の情報アイコンにカーソルを合わせて、詳細情報を表示することもできます。

#### セキュリティ モジュールの障害

- [Failsafe Mode] : セキュリティ モジュールは、フェイルセーフ モードになっています。このモードでは、アプリケーションの起動がブロックされます。セキュリティ モジュールに接続すると、トラブルシューティングを行ったり、フェイルセーフモードを無効にしたりできます。アプリケーション インスタンスを削除することもできます。
- [HDD Error] : セキュリティ モジュールで、ディスク ドライブ エラーが発生しました。ディスク ドライブが存在することを確認してください。エラーが解消されない場合は、障害のあるディスク ドライブを交換します。
- [Filesystem Error] : セキュリティ モジュール上のディスク パーティションに互換性がありません。セキュリティ モジュールを再起動することで回復できる場合があります。それでも障害が解消されない場合は、外部デバイスにデータをバックアップしてからスロットを再初期化してください。
- [Format Failure] : セキュリティ モジュールのディスク ドライブを自動的にフォーマットできませんでした。セキュリティ モジュールを再初期化して再フォーマットしてください。
- [Power] : セキュリティ モジュール/エンジンの電源ステータスを表示します。
  - [On] : [Power off/on] 機能を使用して、セキュリティ モジュール/エンジンの電源ステータスを切り替えます。

- [Off] : [Power off/on] 機能を使用して、セキュリティ モジュール/エンジンの電源ステータスを切り替えます。
- [Application] : セキュリティ モジュール/エンジンにインストールされている論理デバイスのタイプを表示します。

Firepower Chassis Manager の [Security Modules/Security Engine] ページから、セキュリティ モジュール/エンジンに対して次の機能を実行できます。

- [Decommission/Recommission] (セキュリティ モジュールのみ) : セキュリティ モジュールを使用停止にすると、セキュリティ モジュールはメンテナンスモードに設定されます。また、特定の障害状態を修正するために、セキュリティ モジュールを使用停止にしてから再稼働することもできます。 [セキュリティ モジュールの使用停止/再稼働 \(201 ページ\)](#) を参照してください。
- [Acknowledge] : 新たにインストールされたセキュリティ モジュールをオンラインにします。 [セキュリティ モジュール/エンジンの確認応答 \(202 ページ\)](#) を参照してください。
- [Power Cycle] : セキュリティ モジュール/エンジンを再起動します。 [セキュリティ モジュール/エンジンのリセット \(202 ページ\)](#) を参照してください。
- [Reinitialize] : セキュリティ モジュール/エンジンのハードディスクを再フォーマットし、導入済みのすべてのアプリケーションや設定をセキュリティ モジュール/エンジンから削除し、システムを再起動します。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合は、再初期化が完了すると、Firepower eXtensible Operating System はアプリケーションソフトウェアをインストールし、論理デバイスを再度導入し、アプリケーションを自動的に起動します。 [セキュリティ モジュール/エンジンの再初期化 \(203 ページ\)](#) を参照してください。



**警告** セキュリティ モジュール/エンジンのすべてのアプリケーションデータが再初期化時に削除されます。セキュリティ モジュール/エンジンを再初期化する前に、すべてのアプリケーションデータをバックアップしておいてください。

- [Power off/on] : セキュリティ モジュール/エンジンの電源状態を切り替えます。 [インストールされているモジュール/エンジンの電源オン/オフ \(205 ページ\)](#) を参照してください。

## セキュリティ モジュールの使用停止/再稼働

セキュリティ モジュールを使用停止にすると、セキュリティ モジュール オブジェクトが設定から削除され、そのセキュリティ モジュールは管理対象外になります。セキュリティ モジュール上で実行していた論理デバイスやソフトウェアは非アクティブになります。

セキュリティ モジュールの使用を一時的に中止する場合に、セキュリティ モジュールを使用停止にできます。また、セキュリティ モジュールを再起動してもエラー状態が修正されない場

合は、使用停止を試してから、セキュリティモジュールを再稼働させることで、セキュリティモジュールを再初期化しなくてもエラー状態を修正できるかどうかを確認できます。

#### 手順

- 
- ステップ 1** [Security Modules] を選択して、[Security Modules] ページを開きます。
- ステップ 2** セキュリティモジュールを使用停止にするには、そのセキュリティモジュールの [Decommission] をクリックします。
- セキュリティモジュールを再稼働するには、そのセキュリティモジュールの [Recommission] をクリックします。
- ステップ 3** [Yes] をクリックして、指定したセキュリティモジュールを使用停止または再稼働することを確認します。
- 

## セキュリティ モジュール/エンジンの確認応答

新しいセキュリティモジュールがシャーシに取り付けられた後、または既存のモジュールが異なる製品 ID (PID) を持つモジュールで交換された後、セキュリティモジュールを確認応答してからでなければ、そのモジュールを使用することはできません。

セキュリティモジュールのステータスが [mismatch] または [token mismatch] として示されている場合、スロットに取り付けたセキュリティモジュールのデータが、そのスロットに以前インストールされたデータと一致していないことを意味します。セキュリティモジュールに既存のデータがあり、新しいスロットでそのデータを使用する（つまり、そのセキュリティモジュールは不注意で誤ったスロットに取り付けられたのではない）場合は、論理デバイスを展開する前に、セキュリティモジュールを再初期化する必要があります。

#### 手順

- 
- ステップ 1** [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。
- ステップ 2** 確認応答するセキュリティモジュール/エンジンの [Acknowledge] をクリックします。
- ステップ 3** [Yes] をクリックして、指定したセキュリティモジュール/エンジンに確認応答することを確認します。
- 

## セキュリティ モジュール/エンジンのリセット

セキュリティモジュール/エンジンの電源の再投入を行うには、次の手順に従います。

## 手順

- ステップ 1 [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。
- ステップ 2 リセットするセキュリティ モジュール/エンジンの [Power Cycle] をクリックします。
- ステップ 3 次のいずれかを実行します。
  - [Safe Power Cycle] をクリックして、システムに、指定のセキュリティ モジュール/エンジンをリセットする前に、セキュリティ モジュール/エンジンで実行するアプリケーションがシャットダウンするのを最大で 5 分間待機させます。
  - システムに、指定のセキュリティ モジュール/エンジンの電源をすぐにはリセットさせるには、[Power Cycle Immediately] をクリックします。

# セキュリティ モジュール/エンジンの再初期化

セキュリティ モジュール/エンジンを再初期化すると、セキュリティ モジュール/エンジンのハードディスクがフォーマットされ、インストールされているすべてのアプリケーションインスタンス、設定、およびデータが削除されます。論理デバイスがセキュリティ モジュール/エンジンに設定されている場合は、再初期化が完了すると、FXOSはアプリケーションソフトウェアを再インストールし、論理デバイスを再度導入して、アプリケーションを自動的に起動します。



- 注意** セキュリティ モジュール/エンジンのすべてのアプリケーション データが再初期化時に削除されます。セキュリティ モジュール/エンジンを再初期化する前に、すべてのアプリケーションデータをバックアップしておいてください。

## 手順

- ステップ 1 [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。
- ステップ 2 再初期化するセキュリティ モジュール/エンジンの [Reinitialize] をクリックします。
- ステップ 3 [Yes] をクリックして、指定したセキュリティ モジュール/エンジンを再初期化することを確認します。

セキュリティ モジュール/エンジンが再起動し、そのセキュリティ モジュールのすべてのデータが削除されます。このプロセスには数分かかることがあります。

# ネットワークモジュールのオフラインまたはオンラインの切り替え

CLI コマンドを使ってネットワーク モジュールをオフラインにしたりオンラインに戻したりするには、次の手順を実行します。この方法は、モジュールのオンライン挿入や削除（OIR）を実行する場合などに使用されます。



- (注) ネットワーク モジュールを取り外して交換する場合は、お使いのデバイスに該当するインストール ガイドの中で、メンテナンスとアップグレードの章にある指示に従ってください。  
<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>を参照してください。

## 手順

- ステップ 1** 次のコマンドを使用して /fabric-interconnect モードに入った後、オフラインにする対象のモジュールの /card モードに入ります。

```
scope fabric-interconnect a
scope card ID
```

- ステップ 2** `show detail` コマンドを使用すると、このカードに関する、現在のステータスなどの情報を表示することができます。

- ステップ 3** モジュールをオフラインにするには、次のコマンドを入力します。

```
set adminstate offline
```

- ステップ 4** `commit-buffer` コマンドを入力して、設定の変更内容を保存します。

再度 `show detail` コマンドを使用すると、モジュールがオフラインであることを確認できます。

- ステップ 5** ネットワーク モジュールをオンラインに戻すには、次のコマンドを入力します。

```
set adminstate online
commit-buffer
```

## 例

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail
```

```
Fabric Card:
  Id: 2
```

```
Description: Firepower 4x40G QSFP NM
Number of Ports: 16
State: Online
Vendor: Cisco Systems, Inc.
Model: FPR-NM-4X40G
HW Revision: 0
Serial (SN): JAD191601DE
Perf: N/A
Admin State: Online
Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
Id: 2
Description: Firepower 4x40G QSFP NM
Number of Ports: 16
State: Offline
Vendor: Cisco Systems, Inc.
Model: FPR-NM-4X40G
HW Revision: 0
Serial (SN): JAD191601DE
Perf: N/A
Admin State: Offline
Power State: Off
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
FP9300-A /fabric-interconnect/card #
```

## インストールされているモジュール/エンジンの電源オン/オフ

セキュリティ モジュールまたはネットワーク モジュールの電源をオン/オフにするには、次の手順に従います。

### 手順

- ステップ 1 [Security Modules/Security Engine] を選択して、[Security Modules/Security Engine] ページを開きます。
- ステップ 2 セキュリティ モジュール/エンジンの電源をオフにするには、次のようにします。
  - a) そのセキュリティ モジュール/エンジンの [Power off] をクリックします。
  - b) 次のいずれかを実行します。
    - [Safe Power Off] をクリックして、システムに、指定のセキュリティ モジュール/エンジンの電源をオフにする前に、セキュリティ モジュール/エンジンで実行するアプリケーションがシャットダウンするのを最大で 5 分間待機させます。

- システムに、指定のセキュリティ モジュール/エンジンの電源をすぐにオフにさせるには、[Power Off Immediately] をクリックします。

**ステップ 3** セキュリティ モジュール/エンジンの電源をオンにするには、次のようにします。

- a) そのセキュリティ モジュール/エンジンの [Power on] をクリックします。
  - b) [Yes] をクリックして、指定したセキュリティ モジュール/エンジンの電源をオンにすることを確認します。
-



## 第 12 章

# コンフィギュレーションのインポート/エクスポート

- [コンフィギュレーションのインポート/エクスポートについて \(207 ページ\)](#)
- [FXOS コンフィギュレーション ファイルのエクスポート \(208 ページ\)](#)
- [自動設定エクスポートのスケジューリング \(209 ページ\)](#)
- [設定エクスポート リマインダの設定 \(210 ページ\)](#)
- [コンフィギュレーション ファイルのインポート \(211 ページ\)](#)

## コンフィギュレーションのインポート/エクスポートについて

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含む XML ファイルをリモートサーバまたはローカルコンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーション ファイルを後でインポートして Firepower 4100/9300 シャーシに迅速にコンフィギュレーション設定を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

### 注意事項および制約事項

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。
- 用途別のコンフィギュレーション設定は、コンフィギュレーションファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーションバックアップ ツールを使用する必要があります。
- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は

削除され、インポートファイルに含まれるコンフィギュレーションに完全に置き換えられます。

- コンフィギュレーション ファイルのエクスポート元と同じ Firepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずですが、異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先の Firepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワーク モジュールがインストールされている必要があります。
- インポート先の Firepower 4100/9300 シャーシでは、インポートするエクスポート ファイルに定義されているすべての論理デバイスに、正しいソフトウェア アプリケーション イメージがインストールされている必要があります。
- インポートするコンフィギュレーションファイルに、そのアプリケーションにエンドユーザライセンス契約書 (EULA) がある論理デバイスが含まれていると、コンフィギュレーションをインポートする前に、そのアプリケーションの EULA が Firepower 4100/9300 シャーシで受け入れられている必要があります。受け入れられていない場合、操作は失敗します。
- 既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作時にファイル名を変更するか、既存のファイルを別の場所にコピーしてください。

## FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

エクスポート機能の使用に関する重要な情報については、「[コンフィギュレーションのインポート/エクスポートについて](#)」を参照してください。

### 手順

**ステップ 1** [System] > [Configuration] > [Export] の順に選択します。

**ステップ 2** コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、[Export Locally] をクリックします。

コンフィギュレーションファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

- ステップ3** コンフィギュレーション ファイルを設定済みのリモート サーバにエクスポートするには、使用するリモート構成の [Export] をクリックします。  
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。
- ステップ4** コンフィギュレーション ファイルを新しいリモート サーバにエクスポートするには、次の操作を行います。
- a) [On-Demand Export] の下で、[Add On-Demand Configuration] をクリックします。
  - b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
  - c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージアレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。  
IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
  - d) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
  - e) リモートサーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
  - f) リモートサーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
  - g) [Location] フィールドに、ファイル名を含むコンフィギュレーションファイルのエクスポートする場所のフルパスを入力します。ファイル名を省略すると、エクスポート手順によって、ファイルに名前が割り当てられます。
  - h) [OK] をクリックします。  
リモート構成はオンデマンドエクスポート テーブルに追加されます。
  - i) 使用するリモート構成の [Export] をクリックします。  
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

## 自動設定エクスポートのスケジューリング

スケジュールされたエクスポート機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートします。エクスポートは、毎日、毎週、または2週間ごとに実行されるようにスケジュールできます。設定のエクスポートは、スケジュールされたエクスポート機能がいつ有効になるかに基づき、スケジュールに従って実行されます。そのため、たとえば週ごとのスケジュールされたエクスポートが水曜日の午後 10 時に有効になる場合、システムは新しいエクスポートを水曜日の午後 10 時ごとに開始します。

エクスポート機能の使用に関する重要な情報については、「[コンフィギュレーションのインポート/エクスポートについて](#)」を参照してください。

## 手順

- 
- ステップ 1** [System] > [Configuration] > [Export] の順に選択します。
- ステップ 2** [Schedule Export] をクリックします。  
[Configure Scheduled Export] ダイアログボックスが表示されます。
- ステップ 3** リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
- ステップ 4** スケジュールされたエクスポートを有効にするには、[Enable] チェックボックスをオンにします。
- (注) このチェックボックスを使用して、スケジュールされたエクスポートを後から有効または無効にできます。ただし、スケジュールされたエクスポートを有効または無効にするには、もう一度パスワードを指定する必要があります。
- ステップ 5** バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージアレイ、ローカルドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。  
IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
- ステップ 6** デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
- ステップ 7** リモートサーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
- ステップ 8** リモートサーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
- ステップ 9** [Location] フィールドに、ファイル名を含むコンフィギュレーション ファイルをエクスポートする場所のフルパスを入力します。ファイル名を省略すると、エクスポート手順によって、ファイルに名前が割り当てられます。
- ステップ 10** 設定を自動的にエクスポートするスケジュールを選択します。これは、[Daily]、[Weekly]、または [BiWeekly] のいずれかにできます。
- ステップ 11** [OK] をクリックします。  
スケジュールされたエクスポートが作成されます。スケジュールされたエクスポートを有効にすると、システムは、指定の場所に、選択したスケジュールに従ってコンフィギュレーション ファイルを自動的にエクスポートします。
- 

## 設定エクスポート リマインダの設定

設定エクスポートが特定の日数実行されていないときにシステムにエラーを生成させるには、エクスポート リマインダ機能を使用します。

## 手順

- 
- ステップ 1 [System] > [Configuration] > [Export] の順に選択します。
  - ステップ 2 設定エクスポートリマインダを有効にするには、[Reminder to trigger an export] の下のチェックボックスをオンにします。
  - ステップ 3 最後に設定エクスポートが実行されてからリマインダエラーを生成するまでシステムが待機する期間を、1 ~ 365 の範囲の日数で入力します。
  - ステップ 4 [Save Reminder] をクリックします。
- 

# コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。インポート機能の使用に関する重要な情報については、「[コンフィギュレーションのインポート/エクスポートについて](#)」を参照してください。

## 手順

- 
- ステップ 1 [System] > [Configuration] > [Import] の順に選択します。
  - ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。
    - a) [Choose File] をクリックし、インポートするコンフィギュレーション ファイルを選択します。
    - b) [Import] をクリックします。  
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
    - c) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。  
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレイクアウトポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。
  - ステップ 3 設定済みのリモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。
    - a) リモートインポートテーブルで、使用するリモート構成の [Import] をクリックします。  
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
    - b) [Yes] をクリックして、指定したコンフィギュレーション ファイルをインポートします。  
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレイクアウトポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

**ステップ 4** 新しいリモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

- a) [Remote Import] の下にある [Add Remote Configuration] をクリックします。
- b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
- c) デフォルト以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。
- d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージアレイ、ローカルドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

- e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
- f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
- g) [File Path] フィールドに、コンフィギュレーション ファイルのフルパスをファイル名を含めて入力します。
- h) [Save] をクリックします。  
リモート構成がリモート インポート テーブルに追加されます。
- i) 使用するリモート構成の [Import] をクリックします。  
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
- j) [Yes] をクリックして、指定したコンフィギュレーションファイルをインポートします。  
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレイクアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。



## 第 13 章

# トラブルシューティング

- [パケット キャプチャ \(213 ページ\)](#)
- [ネットワーク接続のテスト \(219 ページ\)](#)
- [ポート チャネル ステータスの確認 \(221 ページ\)](#)
- [ソフトウェア障害からの回復 \(223 ページ\)](#)
- [破損ファイル システムの回復 \(228 ページ\)](#)
- [Firepower Threat Defense のクラスタ メンバのディザスタ リカバリ \(238 ページ\)](#)

## パケット キャプチャ

パケット キャプチャ ツールは、接続と設定の問題のデバッグや、Firepower 4100/9300 シャーシを通過するトラフィックフローの理解に使用できる価値ある資産です。パケットキャプチャ ツールを使用すると、Firepower 4100/9300 シャーシの特定のインターフェイスを通過するトラフィックについてログを記録できます。

複数のパケット キャプチャ セッションを作成でき、各セッションで複数のインターフェイスのトラフィックをキャプチャできます。パケットキャプチャセッションに含まれる各インターフェイス用に、個別のパケット キャプチャ (PCAP) ファイルが作成されます。

## バックプレーンポート マッピング

Firepower 4100/9300 シャーシでは、内部バックプレーン ポートに次のマッピング ポートを使用します。

| セキュリティ モジュール               | ポート マッピング    | 説明               |
|----------------------------|--------------|------------------|
| セキュリティ モジュール 1/セキュリティ エンジン | Ethernet1/9  | Internal-Data0/0 |
| セキュリティ モジュール 1/セキュリティ エンジン | Ethernet1/10 | Internal-Data0/1 |
| セキュリティ モジュール 2             | Ethernet1/11 | Internal-Data0/0 |

| セキュリティ モジュール   | ポート マッピング    | 説明               |
|----------------|--------------|------------------|
| セキュリティ モジュール 2 | Ethernet1/12 | Internal-Data0/1 |
| セキュリティ モジュール 3 | Ethernet1/13 | Internal-Data0/0 |
| セキュリティ モジュール 3 | Ethernet1/14 | Internal-Data0/1 |

## パケット キャプチャの注意事項および制限事項

パケット キャプチャ ツールには、次の制限事項があります。

- キャプチャできるのは最大 100 Mbps までです。
- パケット キャプチャセッションの使用に使用可能な十分な記憶域がなくても、パケット キャプチャセッションを作成できます。パケット キャプチャセッションを開始する前に、使用可能な十分な記憶域があることを確認する必要があります。
- 複数のアクティブなパケット キャプチャセッションはサポートされません。
- 内部スイッチの入力の段階でのみキャプチャされます。
- 内部スイッチが認識できないパケット（セキュリティ グループ タグ、ネットワーク サービス ヘッダー パケットなど）にはフィルタの効果がありません。
- EtherChannel 全体のパケットをキャプチャできません。ただし、論理デバイスに割り当てられている EtherChannel の場合、EtherChannel のメンバインターフェイスごとにパケットをキャプチャできます。
- キャプチャセッションがアクティブな間は、PCAP ファイルをコピーしたり、エクスポートできません。
- パケット キャプチャセッションを削除すると、そのセッションに関連するすべてのパケット キャプチャ ファイルも削除されます。

## パケット キャプチャ セッションの作成または編集

### 手順

**ステップ 1** [Tools] > [Packet Capture] の順に選択します。

[Capture Session] タブに、現在設定されているパケット キャプチャセッションのリストが表示されます。パケット キャプチャセッションが現在設定されていない場合は、代わりにそのことを示すメッセージが表示されます。

**ステップ 2** 次のいずれかを実行します。

- パケット キャプチャ セッションを作成するには、[Capture Session] ボタンをクリックします。
- 既存のパケット キャプチャ セッションを編集するには、そのセッションの [Edit] ボタンをクリックします。

ウィンドウの左側では、特定のアプリケーションインスタンスを選択し、そのインスタンスの表記を表示します。この表示は、パケットをキャプチャするインターフェイスを選択するために使用されます。ウィンドウの右側にパケットキャプチャセッションを定義するためのフィールドが含まれています。

- ステップ 3** ウィンドウの左側で、パケットをキャプチャするアプリケーション インスタンスの名前をクリックします。
- ステップ 4** トラフィックをキャプチャするインターフェイスをクリックします。選択したインターフェイスにチェック マークを表示します。
- ステップ 5** 論理デバイスからバックプレーンポート上で送信されるトラフィックをキャプチャするには、次の操作を行います。
- a) アプリケーション インスタンスを示すボックスをクリックします。  
 [Capture On]、[Application Port]、および [Application Capture Direction] フィールドは、[Configure Packet Capture Session] ウィンドウの右側で利用可能になります。
  - b) トラフィックをキャプチャするバックプレーンポートを選択するか、[Capture On] ドロップダウン リストから [All Backplane Ports] を選択します。
- ステップ 6** [Session Name] フィールドにパケット キャプチャ セッションの名前を入力します。
- ステップ 7** [Buffer Size] リストからあらかじめ定義された値の 1 つを選択するか、[Custom in MB] を選択してから目的のバッファ サイズを入力して、パケット キャプチャ セッションに使用するバッファ サイズを指定します。指定するバッファ サイズは 1 ~ 2048 MB にする必要があります。
- ステップ 8** [Snap Length] フィールドに、キャプチャするパケットの長さを指定します。有効値は 64 ~ 9006 バイトです。デフォルトのスナップ長は 1518 バイトです。
- ステップ 9** このパケット キャプチャ セッションを実行したときに、既存の PCAP ファイルを上書きするか、または PCAP ファイルにデータを追加するかを指定します。
- ステップ 10** アプリケーションインスタンスと特定のインターフェイス間のトラフィックをキャプチャするには、次の操作を行います。
- a) 論理デバイスを表すボックスをクリックします。
  - b) [Capture On] ドロップダウン リストから、アプリケーションタイプ ([asa] など) を選択します。
  - c) 受信または送信トラフィックをキャプチャする [Application Port] を選択します。
  - d) 論理デバイスから指定したインターフェイスに向かうトラフィックのみキャプチャするには、[Application Capture Direction] の横にある [Egress Packets] オプションをクリックします。
  - e) 指定したインターフェイスで送信または受信するトラフィックをキャプチャするには、[Application Capture Direction] の横にある [All Packets] オプションをクリックします。
- ステップ 11** キャプチャしたトラフィックをフィルタリングするには、次の操作を行います。

- a) [Capture Filter] フィールドの [Apply Filters] オプションをクリックします。  
フィルタを設定するための一連のフィールドが示されます。
- b) フィルタを作成する必要がある場合、[Create Filter] をクリックします。  
[Create Packet Filter] ダイアログボックスが表示されます。詳細については、[パケットキャプチャのためのフィルタの設定 \(216 ページ\)](#) を参照してください。
- c) [Apply] ドロップダウン リストから、使用するフィルタを選択します。
- d) [To] ドロップダウン リストからフィルタを適用するインターフェイスを選択します。
- e) 追加のフィルタを適用するには、[Apply Another Filter] をクリックしてから上記の追加のフィルタを適用するステップを繰り返します。

**ステップ 12** 次のいずれかを実行します。

- このパケットキャプチャセッションを保存してすぐ実行するには、[Save and Run] ボタンをクリックします。このオプションは、他のパケットキャプチャセッションが現在実行されていない場合のみ使用できます。
- このパケットキャプチャセッションを後で実行できるように保存するには、[Save] ボタンをクリックします。

[Capture Session] タブに作成された他のセッションとともにセッションが一覧表示されます。[Save and Run] を選択した場合、パケットキャプチャセッションは、パケットをキャプチャします。セッションからPCAPファイルをダウンロードする前にキャプチャを停止する必要があります。

## パケットキャプチャのためのフィルタの設定

パケットキャプチャセッションに含まれるトラフィックを制限するためにフィルタを作成できます。パケットキャプチャセッションの作成中にどのインターフェイスが特定のフィルタを使用するかを選択できます。



- (注) 現在実行中のパケットキャプチャセッションに適用されているフィルタを変更または削除する場合、そのセッションを無効にしてから再度有効にするまでは実行されません。

### 手順

**ステップ 1** [Tools] > [Packet Capture] の順に選択します。

[Capture Session] タブに、現在設定されているパケットキャプチャセッションのリストが表示されます。パケットキャプチャセッションが現在設定されていない場合は、代わりにそのことを示すメッセージが表示されます。

**ステップ 2** 次のいずれかを実行します。

- フィルタを作成するには、[Add Filter] ボタンをクリックします。
- 既存のフィルタを編集するには、そのフィルタの [Edit] ボタンをクリックします。

[Create or Edit Packet Filter] ダイアログボックスが表示されます。

**ステップ 3** [Filter Name] フィールドにパケットキャプチャフィルタの名前を入力します。

**ステップ 4** 特定のプロトコルをフィルタリングするには、[Protocol] リストから選択するか、または [Custom] を選択して目的のプロトコルを入力します。カスタムプロトコルは 10 進形式 (0 ~ 255) の IANA によって定義されたプロトコルである必要があります。

**ステップ 5** 特定の EtherType をフィルタリングするには、[EtherType] リストから選択するか、または [Custom] を選択して目的の EtherType を入力します。カスタム EtherType は 10 進形式の IANA によって定義された EtherType である必要があります (たとえば、IPv4 = 2048、IPv6 = 34525、ARP = 2054、SGT = 35081)。

**ステップ 6** 内部 VLAN (ポートを入力する時の VLAN ID) または外部 VLAN (Firepower 4100/9300 シャーシによって追加された VLAN ID) に基づいてトラフィックをフィルタリングするには、指定されたフィールドに VLAN ID を入力します。

**ステップ 7** 特定の送信元または宛先のトラフィックをフィルタリングするには、IP アドレスとポートを入力するか、または特定の送信元または宛先フィールドに MAC アドレスを入力します。

(注) IPv4 または IPv6 アドレスを使用してフィルタリングできますが、同じパケットキャプチャセッションでの両方によるフィルタリングはできません。

**ステップ 8** [Save] をクリックしてフィルタを保存します。

[Filter List] タブに他の作成されたフィルタとともにフィルタがリスト表示されます。

## パケットキャプチャセッションの開始または停止

### 手順

**ステップ 1** [Tools] > [Packet Capture] の順に選択します。

[Capture Session] タブに、現在設定されているパケットキャプチャセッションのリストが表示されます。パケットキャプチャセッションが現在設定されていない場合は、代わりにそのことを示すメッセージが表示されます。

**ステップ 2** パケットキャプチャセッションを開始するには、そのセッションの [Enable Session] ボタンをクリックし、次に確認のために [Yes] をクリックします。

(注) 別のセッションの実行中は、パケットキャプチャセッションを開始できません。

セッションに含まれるインターフェイスの PCAP ファイルがトラフィックの収集を開始します。セッションがセッションデータを上書きするように設定されている場合、既存の PCAP データは消去されます。そうでない場合、データは（もしあれば）既存のファイルに追加されます。

パケットキャプチャセッションの実行中は、トラフィックをキャプチャするにつれて個々の PCAP ファイルのファイルサイズが増加します。バッファのサイズ制限に達すると、システムがパケットの廃棄を開始し、廃棄カウント フィールドの値が増加します。

**ステップ 3** パケットキャプチャセッションを停止するには、そのセッションの [Disable Session] ボタンをクリックし、次に確認のために [Yes] をクリックします。

セッションが無効になった後、PCAP ファイルをダウンロードできます（[パケットキャプチャファイルのダウンロード \(218 ページ\)](#) を参照）。

---

## パケットキャプチャファイルのダウンロード

セッションからローカルコンピュータにパケットキャプチャ (PCAP) ファイルをダウンロードできます。これでネットワークパケットアナライザを使用して分析できるようになります。

### 手順

---

**ステップ 1** [Tools] > [Packet Capture] の順に選択します。

[Capture Session] タブに、現在設定されているパケットキャプチャセッションのリストが表示されます。パケットキャプチャセッションが現在設定されていない場合は、代わりにそのことを示すメッセージが表示されます。

**ステップ 2** パケットキャプチャセッションから特定のインターフェイスの PCAP ファイルをダウンロードするには、そのインターフェイスに対応する [Download] ボタンをクリックします。

(注) パケットキャプチャセッションの実行中は PCAP ファイルをダウンロードできません。

ブラウザによって、指定した PCAP ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するように求められます。

---

## パケットキャプチャセッションの削除

個々のパケットキャプチャセッションは、現在実行していなければ削除できます。非アクティブパケットキャプチャセッションは、いずれも削除できます。

## 手順

**ステップ 1** [Tools] > [Packet Capture] の順に選択します。

[Capture Session] タブに、現在設定されているパケットキャプチャセッションのリストが表示されます。パケットキャプチャセッションが現在設定されていない場合は、代わりにそのことを示すメッセージが表示されます。

**ステップ 2** 特定のパケットキャプチャセッションを削除するには、そのセッションの対応する [Delete] ボタンをクリックします。

**ステップ 3** すべての非アクティブパケットキャプチャセッションを削除するには、パケットキャプチャセッションのリストの上にある [Delete All Sessions] ボタンをクリックします。

# ネットワーク接続のテスト

## 始める前に

基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名または IPv4 アドレスを使って ping を実行するには、**ping** コマンドを使用します。ネットワーク上の別のデバイスのホスト名または IPv6 アドレスを使って ping を実行するには、**ping6** コマンドを使用します。

ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv4 アドレスを使ってトレースするには、**traceroute** コマンドを使用します。ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv6 アドレスを使ってトレースするには、**traceroute6** コマンドを使用します。

- **ping** コマンドおよび **ping6** コマンドは、local-mgmt モードで使用可能です。
- **ping** コマンドは module モードでも使用できます。
- **traceroute** コマンドおよび **traceroute6** コマンドは、local-mgmt モードで使用可能です。
- **traceroute** コマンドは module モードでも使用できます。

## 手順

**ステップ 1** 次のコマンドのいずれか 1 つを入力することにより、local-mgmt モードまたは module モードに接続します。

- **connect local-mgmt**
- **connect module *module-ID*console**

例：

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

**ステップ2** 基本的なネットワーク接続をテストする目的で、ネットワーク上の別のデバイスのホスト名または IPv4 アドレスを使って ping を実行します。

```
ping {hostname|IPv4_address} [count number_packets ] | [deadline seconds ] | [interval seconds ] | [packet-size bytes ]
```

例：

この例は、ネットワーク上の別のデバイスに対して ping 接続を 12 回実行する方法を示しています。

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

**ステップ3** ネットワーク上の別のデバイスに至るルートを、そのホスト名または IPv4 アドレスを使ってトレースします。

```
traceroute {hostname | IPv4_address}
```

例：

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

FP9300-A(local-mgmt)#
```

**ステップ4** (任意) local-mgmt モードを終了して最上位モードに戻るには、**exit** を入力します。

# ポート チャネル ステータスの確認

現在定義されているポート チャネルのステータスを判別するには、次の手順を実行します。

## 手順

**ステップ 1** 次のコマンドを入力して /eth-uplink/fabric モードを開始します。

- **scope eth-uplink**
- **scope fabric {a | b}**

例：

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

**ステップ 2** 現在のポート チャネルとそれぞれの管理状態および動作状態のリストを表示するには、**show port-channel** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State      State Reason
  -----
  10              Port-channel10  Data           Enabl
ed   Failed              No operational members
  11              Port-channel11  Data           Enabl
ed   Failed              No operational members
  12              Port-channel12  Data           Disab
led  Admin Down          Administratively down
  48              Port-channel48  Cluster        Enabl
ed   Up

FP9300-A /eth-uplink/fabric #
```

**ステップ 3** 個々のポート チャネルとポートに関する情報を表示するには、次のコマンドを入力して /port-channel モードを開始します。

- **scope port-channel ID**

例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
```

```
owned by other third parties and used and distributed under
license.
```

```
<--- remaining lines removed for brevity --->
```

```
FP9300-A (fxos) #
```

**ステップ4** 指定したポートチャネルのステータス情報を表示するには、**show** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State             State Reason
  -----
  10          Port-channel10  Data          Enabl
ed          Failed          No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

**ステップ5** ポートチャネルのメンバポートのステータス情報を表示するには、**show member-port** コマンドを入力します。

例：

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
  Port Name      Membership      Oper State      State Reas
on
  -----
  Ethernet2/3    Suspended      Failed          Suspended
  Ethernet2/4    Suspended      Failed          Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

ポートチャネルは、論理デバイスに割り当てられるまでは表示されないことに注意してください。ポートチャネルが論理デバイスから削除された場合や論理デバイスが削除された場合は、ポートチャネルが一時停止状態に戻ります。

**ステップ6** 追加のポートチャネルおよびLACP情報を表示するには、次のコマンドを入力することにより、`/eth-uplink/fabric/port-channel` モードを終了して `fxos` モードに入ります。

- **top**
- **connect fxos**

例：

**ステップ7** 現在のポートチャネルのサマリー情報を表示するには、**show port-channel summary** コマンドを入力します。

例：

```

FP9300-A(fxos)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
-----
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
-----
10    Po10 (SD)    Eth       LACP      Eth2/3 (s)  Eth2/4 (s)
11    Po11 (SD)    Eth       LACP      Eth2/1 (s)  Eth2/2 (s)
12    Po12 (SD)    Eth       LACP      Eth1/4 (D)  Eth1/5 (D)
48    Po48 (SU)    Eth       LACP      Eth1/1 (P)  Eth1/2 (P)

```

fxos モードでは、さらに **show port-channel** コマンドおよび **show lacp** コマンドも使用できます。これらのコマンドを使用すると、容量、トラフィック、カウンタ、使用状況など、さまざまなポート チャネルおよび LACP 情報を表示することができます。

### 次のタスク

ポートチャネルの作成方法については、[EtherChannel \(ポートチャネル\) の追加 \(140ページ\)](#) を参照してください。

## ソフトウェア障害からの回復

### 始める前に

システムが正常にブートできないソフトウェア障害が発生した場合は、以下の手順を実行して、ソフトウェアの新規バージョンをブートできます。このプロセスを実行するには、キックスタートイメージをTFTPブートし、新規システムとマネージャイメージをダウンロードし、新規イメージを使用してブートする必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300 : <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 シリーズ <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

リカバリ イメージには、3つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64 の現在のリカバリ イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

## 手順

### ステップ1 ROMMON にアクセスします。

- a) コンソールポートに接続します。
- b) システムをリブートします。

システムはロードを開始し、そのプロセス中にカウントダウンタイマーを表示します。

- c) カウントダウン中に **Esc** キーを押すと、ROMMON モードに入ります。

#### 例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >
```

### ステップ2 キックスタートイメージを TFTP ブートします。

- a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
```

```
rommon > gateway <default-gateway>
```

- b) キックスタートイメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

(注) キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタートイメージとの間の対応を示す情報は、Cisco.com のソフトウェアダウンロードページにあります。

- c) ブート コマンドを使用して、ROMMON からイメージをブートします。

```
boot tftp://<IP address>/<path to image>
```

(注) さらに、Firepower 4100/9300 シャーシのフロント パネルにある USB スロットに挿入した USB メディア デバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例 :

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

**ステップ 3** Firepower 4100/9300 シャーシに直前にロードしたキックスタートイメージと一致するリカバリシステムとマネージャ イメージをダウンロードします。

- a) リカバリ システムとマネージャ イメージをダウンロードするには、管理 IP アドレスとゲートウェイを設定する必要があります。これらのイメージは、USB を使用してダウンロードすることはできません。

```
switch(boot)# config terminal
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address <ip address> <netmask>
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway <gateway>
switch(boot) (config)# exit
```

- b) リカバリ システムとマネージャ イメージを、リモート サーバからブートフラッシュにコピーします。

```
switch(boot)# copy URL bootflash:
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image\_name**
- **scp://username@hostname/path/image\_name**
- **sftp://username@hostname/path/image\_name**
- **tftp://hostname/path/image\_name**

例 :

```
switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
```

```
switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、nuova-sim-mgmt-nsg.0.1.0.001.bin からマネージャ イメージへの symlink を作成します。このリンクは、ロードするマネージャ イメージをロードメカニズムに指示します。symlink 名は、ロードしようとしているイメージに関係なく、常に nuova-sim-mgmt-nsg.0.1.0.001.bin とする必要があります。

```
switch(boot)# copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例 :

```
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.

switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if)# no shutdown
```

```

switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway 10.0.0.1
switch(boot) (config) # exit
switch(boot) # copy
      tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
      bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
      tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
      bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy bootflash:fxos-k9-manager.4.1.1.69.SPA
      bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot) #

```

**ステップ 4** 直前にダウンロードしたシステム イメージをロードします。

```
switch(boot) # load bootflash:<system-image>
```

例 :

```

switch(boot) # load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful
...
System is coming up ... Please wait ...

Cisco FPR Series Security Appliance
FP9300-A login:

```

**ステップ 5** リカバリ イメージがロードされたら、以下のコマンドを入力して、システムが旧イメージをロードしないようにします。

(注) この手順は、リカバリ イメージのロードの直後に実行する必要があります。

```

FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility
issue.
FP9300-A /org/fw-platform-pack* # commit-buffer

```

**ステップ 6** Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードしてインストールします。詳細については、[イメージ管理 \(45ページ\)](#) を参照してください。

例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
  Tftp      192.168.1.2          0
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

## 破損ファイルシステムの回復

始める前に

スーパーバイザのオンボードフラッシュが破損し、システムが正常に開始できなくなった場合は、次の手順を使用してシステムを回復できます。このプロセスを実行するには、キックスタートイメージを TFTP ブートし、フラッシュを再フォーマットし、新規システムとマネージャ イメージをダウンロードし、新規イメージを使用してブートする必要があります。



(注) この手順には、システムフラッシュの再フォーマットが含まれています。その結果、回復後にはシステムを完全に再設定する必要があります。

特定の FXOS バージョンのリカバリ イメージは、以下のいずれかのロケーションの Cisco.com から入手できます。

- Firepower 9300 : <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 シリーズ <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

リカバリ イメージには、3つの異なるファイルが含まれます。たとえば、FXOS 2.1.1.64 の回復イメージを以下に示します。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

## 手順

### ステップ1 ROMMON にアクセスします。

- a) コンソールポートに接続します。
- b) システムをリブートします。

システムはロードを開始し、そのプロセス中にカウントダウンタイマーを表示します。

- c) カウントダウン中に **Esc** キーを押すと、ROMMON モードに入ります。

#### 例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

### ステップ2 キックスタートイメージを TFTP ブートします。

- a) 管理 IP アドレス、管理ネットマスク、ゲートウェイ IP アドレスが正しく設定されていることを確認します。これらの値は、**set** コマンドを使用して表示できます。**ping** コマンドを使用すると、TFTP サーバへの接続をテストできます。

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) キックスタートイメージは、Firepower 4100/9300 シャーシからアクセス可能な TFTP ディレクトリにコピーします。

(注) キックスタートイメージのバージョン番号は、バンドルのバージョン番号に一致しません。FXOS バージョンとキックスタートイメージとの間の対応を示す情報は、Cisco.com のソフトウェア ダウンロード ページにあります。

- c) ブート コマンドを使用して、ROMMON からイメージをブートします。

```
boot tftp://<IP address>/<path to image>
```

(注) さらに、Firepower 4100/9300 シャーシのフロントパネルにある USB スロットに挿入した USB メディア デバイスを使用して、ROMMON からキックスタートをブートすることもできます。システムの稼動中に USB デバイスを挿入した場合、USB デバイスを認識させるにはシステムを再起動する必要があります。

システムは、イメージを受け取ってキックスタートイメージをロードすることを示す、一連の # を表示します。

例：

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

- ステップ 3** キックスタートイメージをロードしたら、**init system** コマンドを使用してフラッシュを再フォーマットします。

**init system** コマンドを実行すると、システムにダウンロードされているすべてのソフトウェアイメージやシステムのすべての設定を含め、フラッシュの内容は消去されます。コマンドが完了するまで約 20 ～ 30 分かかります。

例：

```
switch(boot)# init system
```

```
This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.
```

```
Do you want to continue? (y/n) [n] y
```

```
Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
```

- ステップ 4** リカバリ イメージを Firepower 4100/9300 シャーシへダウンロードします。

- a) リカバリ イメージをダウンロードするには、管理 IP アドレスとゲートウェイを設定する必要があります。これらのイメージは、USB を使用してダウンロードすることはできません。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

- b) リモートサーバからブートフラッシュに3つすべてのリカバリ イメージをコピーします。

```
switch(boot)# copy URL bootflash:
```

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp://username@hostname/path/image\_name**
- **scp://username@hostname/path/image\_name**
- **sftp://username@hostname/path/image\_name**
- **tftp://hostname/path/image\_name**

例 :

```
switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:

switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:

switch(boot) # copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) Firepower 4100/9300 シャーシにイメージが正常にコピーされたら、`nuova-sim-mgmt-nsg.0.1.0.001.bin` からマネージャイメージへの symlink を作成します。このリンクは、ロードするマネージャイメージをロードメカニズムに指示します。symlink 名は、ロードしようとしているイメージに関係なく、常に `nuova-sim-mgmt-nsg.0.1.0.001.bin` とする必要があります。

```
switch(boot) # copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

例 :

```
switch(boot) # config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot) (config) # interface mgmt 0
switch(boot) (config-if) # ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway 10.0.0.1
switch(boot) (config) # exit
switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
```

```
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

**ステップ 5** スイッチをリロードします。

```
switch(boot)# reload
```

例 :

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.
```

```
!! Rommon image verified successfully !!
```

```
Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb
```

```
autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >
```

**ステップ 6** キックスタート イメージおよびシステム イメージからブートします。

```
rommon 1 > boot <kickstart-image> <system-image>
```

(注) システム イメージのロード中に、ライセンス マネージャのエラー メッセージが表示されることがあります。このようなメッセージは無視して構いません。

例 :

```
rommon 1 > dir
Directory of: bootflash:\
```

```

01/01/12 12:33a <DIR>          4,096 .
01/01/12 12:33a <DIR>          4,096 ..
01/01/12 12:16a <DIR>         16,384 lost+found
01/01/12 12:27a              34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a             330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a             250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a             330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
      4 File(s) 946,269,798 bytes
      3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA

!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S1mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

---- 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 Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time 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? (y/n):

```

**ステップ7** イメージのロードが完了すると、システムにより初期構成設定を入力するように求められます。詳細については、[初期設定 \(6 ページ\)](#) を参照してください。

- ステップ 8** Firepower 4100/9300 シャーシで使用するプラットフォーム バンドル イメージをダウンロードします。詳細については、[イメージ管理 \(45 ページ\)](#) を参照してください。

例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
  Tftp      192.168.1.2          0
  FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

- ステップ 9** 以前の手順でダウンロードしたプラットフォーム バンドル イメージをインストールします。

- a) auto-install モードにします。

Firepower-chassis /firmware # **scope auto-install**

- b) FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis /firmware/auto-install # **install platform platform-vers version\_number**

*version\_number* は、インストールする FXOS プラットフォーム バンドルのバージョン番号です (たとえば、2.1(1.73))。

- c) システムは、まずインストールするソフトウェアパッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェアパッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

**yes** を入力して、検証に進むことを確認します。

- d) インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

Firepower eXtensible Operating System がバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

- e) アップグレードプロセスをモニタするには、次の手順を実行します。

- **scope firmware** を入力します。
- **scope auto-install** を入力します。
- **show fsm status expand** を入力します。

**ステップ 10** インストールしたプラットフォームバンドルイメージがシステムの回復に使用するイメージに対応している場合は、将来的にシステムのロード時で使用できるようにキックスタートイメージおよびシステムイメージを手動で有効にする必要があります。回復イメージとして同じイメージを使用しているプラットフォームバンドルをインストールする場合、自動アクティベーションは発生しません。

- a) `fabric-interconnect a` のスコープを設定します。

```
FP9300-A# scope fabric-interconnect a
```

- b) 実行中のカーネルバージョンと実行中のシステムバージョンを表示するには、`show version` コマンドを使用します。イメージをアクティブにするには、次の文字列を使用します。

```
FP9300-A /fabric-interconnect # show version
```

(注) `Startup-Kern-Vers` および `Startup-Sys-Vers` がすでに設定され、`Running-Kern-Vers` および `Running-Sys-Vers` と一致する場合は、イメージを有効にする必要はなく、手順 11 に進みます。

- c) 次のコマンドを入力して、イメージをアクティブにします。

```
FP9300-A /fabric-interconnect # activate firmware
kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

(注) サーバのステータスは「失敗したディスク (Disk Failed)」に変更される場合があります。このメッセージには注意を払う必要はなく、手順を続行できます。

- d) スタートアップバージョンが正しく設定されていることを確認し、イメージのアクティブ化ステータスをモニタするには、`show version` コマンドを使用します。

**重要** ステータスが「アクティブにしています (Activating)」から「実行可能 (Ready)」に変わるまで、次のステップには進まないでください。

```
FP9300-A /fabric-interconnect # show version
```

例：

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
Running-Kern-Vers: 5.0(3)N2(4.11.69)
Running-Sys-Vers: 5.0(3)N2(4.11.69)
Package-Vers: 2.1(1.73)
Startup-Kern-Vers:
Startup-Sys-Vers:
Act-Kern-Status: Ready
Act-Sys-Status: Ready
Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
```

```

FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Activating
  Act-Sys-Status: Activating
  Bootloader-Vers:

```

```

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

```

**ステップ 11** システムを再起動します。

例 :

```

FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #

```

システムは Firepower 4100/9300 シャーシの電源を最終的にオフにしてから再起動する前に、各セキュリティ モジュール/エンジンの電源をオフにします。このプロセスには約 5 ～ 10 分かかります。

**ステップ 12** システムのステータスをモニタします。サーバのステータスは「検出 (Discovery)」から「構成 (Config)」、最終的には「OK」へと変わります。

例 :

```

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Discovery In Progress
1/2 Equipped Discovery In Progress
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Config Complete
1/2 Equipped Config Complete
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Ok Complete

```

1/3 Empty

総合的なステータスが「OK」になれば、システムは回復したことになります。引き続き、セキュリティアプライアンス（ライセンス設定を含む）を再設定し、論理デバイスがあれば再作成する必要があります。詳細については、次を参照してください。

- Firepower 9300 のクイック スタート ガイド [英語] : <http://www.cisco.com/go/firepower9300-quick>
- Firepower 9300 のコンフィギュレーション ガイド [英語] : <http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 シリーズのクイック スタート ガイド [英語] : <http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 シリーズのコンフィギュレーション ガイド [英語] : <http://www.cisco.com/go/firepower4100-config>

---

## Firepower Threat Defense のクラスタ メンバのディザスタ リカバリ

この手順を使用して、ディザスタリカバリのシナリオの後に、Firepower Threat Defense を備えた Firepower 4100/9300 クラスタ メンバをオンラインにし、クラスタに戻します。クラスタ化されたユニットに関連付けられている Firepower Threat Defense のアプリケーションバージョンが同期していない場合、[論理デバイスのイメージバージョンの更新（48 ページ）](#) の説明手順に従って同じバージョンにアップします。

### 始める前に

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモートサーバまたはローカルコンピュータにエクスポートします。詳細については、[コンフィギュレーションのインポート/エクスポートについて（207 ページ）](#) を参照してください。

### 手順

- 
- ステップ 1** スレーブユニットが起動されると、バックアップが復元されます。設定のインポート方法については、[コンフィギュレーションファイルのインポート（211 ページ）](#) を参照してください。アプリケーションのインストールが開始します。
  - ステップ 2** ライセンス契約書に同意します。
  - ステップ 3** 必要に応じて、クラスタ内の各ユニットのバージョンと一致するように、アプリケーションのスタートアップバージョンを設定します。アプリケーションのスタートアップバージョンを

設定する方法については、[論理デバイスのイメージバージョンの更新 \(48 ページ\)](#) を参照してください。

**ステップ 4** アプリケーションのスタートアップバージョンを変更したら、Firepower Threat Defense が実行されるバージョンとスタートアップバージョンが一致するようセキュリティ モジュールを再初期化します。

- a) [Security Modules/Security Engine] ページに移動します。
- b) **Reinitialize Security Engine** ボタンをクリックします。
- c) [Yes] をクリックして、変更を確認します。セキュリティモジュールを再フォーマットし、スタートアップバージョンのアプリケーションを再インストールします。

アプリケーションがオンラインになり、クラスタに参加します。

**ステップ 5** アプリケーション スタートアップ バージョンと実行中のバージョンが同じであることを確認します。

- a) FXOS CLI で、セキュリティ サービス モードを開始します。

```
firepower scope ssa
```

- b) アプリケーション インスタンスを表示します。

```
firepower /ssa # show app-instance
```

例 :

```
firepower /ssa # show app-instance
App Name      Slot ID      Admin State Oper State      Running Version Startup Version
Profile Name  Cluster     State      Cluster Role
-----
ftd           1           Enabled    Online          6.2.3.1624     6.2.3.1624
              In Cluster  Slave
```

**ステップ 6** Firepower Management Center で、スレーブ メンバを削除します。Firepower Management Center 設定ガイドの「Delete a Slave Member」を参照してください。

**ステップ 7** Firepower Management Center に回復した Firepower 9300/4100 スレーブ ユニットの再度追加します。Firepower Management Center 設定ガイドの「Replace a Cluster Member」を参照してください。





## 索引

### A

- AAA [120, 121, 124, 125, 126, 127, 128](#)
  - LDAP プロバイダー [120, 121, 124](#)
  - RADIUS プロバイダー [124, 125, 126](#)
  - TACACS+ プロバイダー [126, 127, 128](#)
- asa [48, 151, 156, 167, 183, 185](#)
  - アプリケーションインスタンスの削除 [185](#)
  - イメージバージョンの更新 [48](#)
  - クラスタ化の作成 [151](#)
  - クラスタの作成 [167](#)
  - スタンドアロン ASA 論理デバイスの作成 [156](#)
  - 接続 [183](#)
  - 接続の終了 [183](#)
  - 論理デバイスの削除 [185](#)
- ASA イメージ [45, 46](#)
  - Cisco.com からのダウンロード [46](#)
  - Firepower セキュリティ アプライアンスへのアップロード [46](#)
    - 概要 [45](#)
- authNoPriv [98](#)
- authPriv [98](#)

### C

- call home [18](#)
  - HTTP プロキシの設定 [18](#)
- Chassis Manager [1](#)
  - ユーザ インターフェイスの概要 [1](#)
- Cisco Secure Package [45, 46](#)
  - Cisco.com からのダウンロード [46](#)
  - Firepower セキュリティ アプライアンスへのアップロード [46](#)
    - 概要 [45](#)
- CLI。参照先： コマンドライン インターフェイス
- CSP。参照先： Cisco Secure Package

### D

- DNS [131](#)

### F

- Firepower Chassis Manager [1, 9, 71](#)
  - 自動ログアウト [71](#)
  - ユーザ インターフェイスの概要 [1](#)
  - ログイン/ログアウト [9](#)
- Firepower eXtensible OS [47](#)
  - プラットフォーム バンドルのアップグレード [47](#)
- Firepower Threat Defense。参照先： 脅威に対する防御
- Firepower シャーシ [2, 6, 81](#)
  - 初期設定 [6](#)
  - ステータスの監視 [2](#)
  - 電源オフ [81](#)
  - リポート [81](#)
- Firepower シャーシの電源オフ [81](#)
- Firepower セキュリティ アプライアンス [1](#)
  - 概要 [1](#)
- Firepower プラットフォーム バンドル [45, 46, 47](#)
  - Cisco.com からのダウンロード [46](#)
  - Firepower セキュリティ アプライアンスへのアップロード [46](#)
    - アップグレード [47](#)
    - 概要 [45](#)
    - 整合性の確認 [47](#)
- fpga [50](#)
  - アップグレード [50](#)
- ftd。参照先： 脅威に対する防御
- FXOS シャーシ。参照先： Firepower シャーシ

### H

- HTTPS [9, 35, 36, 107, 108, 110, 112, 113, 114, 116, 118](#)
  - キーリングの再生成 [108](#)
  - キーリングの作成 [107](#)
  - 証明書のインポート [113](#)
  - 証明書要求 [108, 110](#)
  - 設定 [114](#)
  - timeout [35, 36](#)
  - トラスト ポイント [112](#)
  - ポートの変更 [116](#)
  - ディセーブル化 [118](#)

## HTTPS (続き)

- ログイン/ログアウト 9

## HTTP プロキシ 18

- 設定 18

## L

## LDAP 120, 121, 124

## LDAP プロバイダー 121, 124

- 削除 124

- 作成 121

## license authority 19

## N

## noAuthNoPriv 98

## NTP 90, 91, 92

- 削除 92

- 設定 90, 91

- 追加 91

## P

PCAP。参照先：パケットキャプチャ

## PCAP ファイル 218

- ダウンロード 218

## ping 219

## PKI 106

## R

## RADIUS 124, 125, 126

## RADIUS プロバイダー 125, 126

- 削除 126

- 作成 125

## rommon 50

- アップグレード 50

## RSA 106

## S

## smart call home 18

- HTTP プロキシの設定 18

## SNMP 97, 98, 99, 100, 101, 103, 105

- イネーブル化 100

- 概要 97

- 権限 98

- コミュニティ 100

- サポート 97, 100

- セキュリティ レベル 98

- 通知 98

## SNMP (続き)

- トラップ 101, 103

- 削除 103

- 作成 101

- バージョン3のセキュリティ機能 99

- ユーザ 103, 105

- 削除 105

- 作成 103

## SNMPv3 99

- セキュリティ機能 99

## SSH 35, 36, 93

- 設定 93

- timeout 35, 36

## syslog 128

- リモート宛先の設定 128

- ローカル宛先の設定 128

- ローカル送信元の設定 128

## T

## TACACS+ 126, 127, 128

## TACACS+ プロバイダー 127, 128

- 削除 128

- 作成 127

## Telnet 35, 36, 96

- 設定 96

- timeout 35, 36

## traceroute 219

- 接続テスト 219

## あ

## アカウント 31, 42

- ローカル認証された 31, 42

## い

## イネーブル化 100

- SNMP 100

## イメージ 45, 46, 47

- Cisco.com からのダウンロード 46

- Firepower セキュリティ アプライアンスへのアップロード 46

- Firepower eXtensible Operating System プラットフォーム バンドルのアップグレード 47

- 管理 45

- 整合性の確認 47

## イメージバージョン 48

- 更新 48

## インターフェイス 140

- 設定 140

インターフェイス (続き)

プロパティ [140](#)

インフォーム [98](#)

概要 [98](#)

## か

管理 IP アドレス [72](#)

変更 [72](#)

## き

キーリング [106, 107, 108, 110, 112, 113, 116](#)

概要 [106](#)

再作成 [108](#)

削除 [116](#)

作成 [107](#)

証明書のインポート [113](#)

証明書要求 [108, 110](#)

トラストポイント [112](#)

脅威に対する防御 [158, 172, 183, 185](#)

アプリケーションインスタンスの削除 [185](#)

クラスタの作成 [172](#)

脅威に対する防御用のスタンドアロン論理デバイスの作成 [158](#)

接続 [183](#)

接続の終了 [183](#)

論理デバイスの削除 [185](#)

脅威防御 [151](#)

クラスタ化の作成 [151](#)

## く

クラスタ [151, 161, 167, 172](#)

概要 [161](#)

作成 [151, 167, 172](#)

クラスタリング [149, 151, 153, 163, 164](#)

管理 [164](#)

ネットワーク [164](#)

クラスタ制御リンク [163](#)

サイズ [163](#)

冗長性 [163](#)

スパニングツリー portfast [151](#)

アップグレード:ソフトウェア[あつぷぐれーど:そふとうえあ] [149](#)

ソフトウェア要件 [149](#)

デバイス ローカル EtherChannel, スイッチで設定 [153](#)

メンバ要件 [149](#)

## こ

工場出荷時のデフォルト設定 [81](#)

復元 [81](#)

工場出荷時のデフォルト設定の復元 [81](#)

コマンドライン インターフェイス [10](#)

アクセス [10](#)

コマンドライン インターフェイスへのアクセス [10](#)

コミュニティ、SNMP [100](#)

console [35, 36](#)

timeout [35, 36](#)

コンフィギュレーションのインポート [207](#)

コンフィギュレーションのインポート/エクスポート [207](#)

制約事項 [207](#)

ガイドライン [207](#)

コンフィギュレーションのエクスポート [207](#)

## し

時刻 [92](#)

手動設定 [92](#)

time [91](#)

表示 [91](#)

システム [6](#)

初期設定 [6](#)

システム リカバリ [223, 228](#)

自動ログアウト [71](#)

シャーシ [2, 6](#)

初期設定 [6](#)

ステータスの監視 [2](#)

シャーシステータスのモニタリング [2](#)

証明書 [106](#)

概要 [106](#)

初期設定 [6](#)

## せ

セキュリティ モジュール [201, 202, 203, 204, 205](#)

オフラインにする [204](#)

オンラインにする [204](#)

確認応答 [202](#)

再初期化 [203](#)

decommissioning [201](#)

電源オフ [205](#)

電源投入 [205](#)

リセット [202](#)

セキュリティ モジュールのオフラインとオンラインの切り替え [204](#)

セキュリティ モジュールの確認応答 [202](#)

セキュリティ モジュールの再初期化 [203](#)

セキュリティ モジュールの使用停止 [201](#)

セキュリティ モジュールの電源オン/オフ **205**  
 セキュリティ モジュールのリセット **202**  
 セッションタイムアウト **35, 36**  
 設定 **107, 108, 110, 112, 113**  
   HTTPS **107, 108, 110, 112, 113**

## そ

ソフトウェア障害 **223**  
 リセット **223**

## た

timeout **35, 36**  
   HTTPS、SSH、および Telnet **35, 36**  
   console **35, 36**  
 タイムゾーン **91, 92**  
   設定 **91, 92**  
 タスク フロー **5**

## つ

通信サービス **100, 107, 108, 110, 112, 113**  
   HTTPS **107, 108, 110, 112, 113**  
   SNMP **100**

## て

device name **77**  
 変更 **77**

## と

トラスト ポイント **106, 112, 117**  
   概要 **106**  
   削除 **117**  
   作成 **112**  
 トラップ **98, 101, 103**  
   概要 **98**  
   削除 **103**  
   作成 **101**  
 トラブルシューティング **221**  
   ポート チャネル ステータス **221**

## に

日時 **90**  
 設定 **90**  
 認証 **32**  
   デフォルト **32**

## は

ハイレベルのタスク リスト **5**  
 パケット キャプチャ **213, 214, 216, 217, 218**  
   PCAP ファイルのダウンロード **218**  
     パケット キャプチャ セッションの開始 **217**  
     パケット キャプチャ セッションの削除 **218**  
     パケット キャプチャ セッションの作成 **214**  
     パケット キャプチャ セッションの停止 **217**  
     フィルタ **216**  
   パケット キャプチャ セッションの削除 **218**  
   パケット キャプチャ セッションの作成 **214**  
   パケット キャプチャ ファイルのダウンロード **218**  
 パスワード **27, 31, 32**  
   強度チェック **32**  
   ガイドライン **27**  
   変更間隔 **32**  
   履歴カウンタ **31**  
 パスワード プロファイル **31, 42**  
   概要 **31**  
   パスワード履歴のクリア **42**  
 破損ファイル システム **228**  
   リセット **228**  
 バナー **78, 79, 80**  
   ログイン前 **78, 79, 80**

## ひ

date **91**  
   表示 **91**  
 日付 **92**  
   手動設定 **92**

## ふ

ファームウェア **50**  
   アップグレード **50**  
 ファームウェアのアップグレード **50**  
 プラットフォーム バンドル **45, 46, 47**  
   Cisco.com からのダウンロード **46**  
   Firepower セキュリティ アプライアンスへのアップロード  
     **46**  
   アップグレード **47**  
   概要 **45**  
   整合性の確認 **47**  
 ブレークアウト ケーブル **142**  
   設定 **142**  
 ブレークアウト ポート **142**  
 プロファイル **31**  
   パスワード **31**

## ほ

ポート チャンネル **140, 221**  
 status **221**  
 設定 **140**

## ゆ

ユーザ **25, 31, 32, 40, 41, 42, 103, 105**  
 SNMP **103, 105**  
 アクティブ化 **42**  
 管理 **25**  
 削除 **41**  
 作成 **40**  
 設定 **32**  
 デフォルト認証 **32**  
 非アクティブ化 **42**  
 ロール **31**  
 ユーザ7 **31, 42**  
 ローカル認証された **31, 42**  
 users **26, 27**  
 パスワードのガイドライン **27**  
 命名のガイドライン **26**  
 ユーザ アカウント **31, 42**  
 パスワード プロファイル **31, 42**  
 ユーザ インターフェイス **1**  
 概要 **1**

## ら

ライセンス **19**  
 登録 **19**

ライセンスの登録 **19**

## り

リポート **81**  
 履歴、パスワード **31**

## ろ

ローカル認証されたユーザ **31, 42**  
 パスワードのプロファイル **31**  
 パスワード履歴のクリア **42**  
 ログイン/ログアウト **9**  
 ログイン前バナー **78, 79, 80**  
 削除 **80**  
 作成 **78**  
 変更 **79**  
 論理デバイス **48, 151, 156, 158, 167, 172, 183, 185, 190**  
 アプリケーション インスタンスの削除 **185**  
 イメージバージョンの更新 **48**  
 クラスタの作成 **151, 167, 172**  
 削除 **185**  
 スタンドアロンの作成 **156, 158**  
 接続 **183**  
 接続の終了 **183**  
 説明 **190**  
 論理デバイス接続の終了 **183**  
 論理デバイスへの接続 **183**

