FXOS CLI の設定

Firepower 2100 は、デバイスの基本的な動作を制御するために FXOS を実行します。FXOS CLI または GUI の Firepower Chassis Manager を使用してこれらの機能を設定できます。このマニュアルでは FXOS CLI について説明します。すべてのセキュリティ ポリシーおよびその他の動作は、ASA OS で設定される（CLI または ASDM を使用）ことに注意してください。

CLI および設定管理

Firepower eXtensible Operating System（FXOS）は、ASA CLI とは異なる動作をします。ここでは、CLI と FXOS 設定の管理方法について説明します。

CLI について

FXOS は管理対象オブジェクトモデルを使用します。このモデルでは、管理対象オブジェクトは管理可能な物理エンティティまたは論理エンティティを抽象的に表現したものです。たとえば、シャーシ、ネットワークモジュール、ポート、プロセッサは、管理対象オブジェクトとして表現される物理エンティティです。また、ユーザロールやプラットフォームポリシーは、管理対象オブジェクトとして表現される論理エンティティです。

オブジェクト管理用に 4 つの一般的なコマンドがあります。

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

scope コマンドは、永続的オブジェクトでもユーザ イスタンス化オブジェクトでも、すべての管理対象オブジェクトで使用できます。その他のコマンドを使用して、ユーザインスタンス化オブジェクトを作成および管理できます。すべての **create** *object* コマンドには、それぞれに対応する **delete** *object* および **enter** *object* コマンドが存在します。**enter** *object* コマンドを使用して、新しいオブジェクトを作成したり既存のオブジェクトを編集したりできます。そのため、オブジェクトがすでに存在する場合にエラーとなる **create** *object* コマンドの代わりに使用できます。

? 文字を入力すれば、いつでもコマンド構文の現在の状態で使用可能なオプションを表示できます。

ASA または FXOS のコンソールへの接続

Firepower 2100 コンソール ポートで FXOS CLI に接続します。次に、FXOS CLI から ASA コンソールに接続し、再度戻ることができます。FXOS に SSH 接続する場合は、ASA CLI にも接続できます。SSH からの接続はコンソール接続ではないため、FXOS SSH 接続から複数の ASA 接続を行うことができます。同様に、ASA に SSH 接続する場合は、FXOS CLI に接続できます。

一度に保持できるコンソール接続は 1 つだけです。FXOS コンソールから ASA のコンソールに接続する場合、Telnet または SSH 接続の場合とは異なり、この接続は永続的接続です。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアル ケーブルが付属しているため、接続するためにはサード パーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティング システムに必要な USB シリアル ドライバを必ずインストールしてください。次のシリアル設定を使用します。

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

FXOS CLI に接続します。ユーザ クレデンシャルを入力します。デフォルトでは、**admin** ユーザとデフォルトのパスワード **Admin123** を使用してログインできます。

ステップ 2 ASA に接続します。

connect asa

例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ciscoasa>
```

ステップ 3 FXOS コンソールに戻るには、Ctrl+a、d と入力します。

SSH を使用した FXOS への接続

デフォルトの IP アドレス 192.168.45.45 を使用して管理 1/1 の FXOS に接続できます。リモート管理を設定する場合（ASA **fxos permit** コマンド）、非標準ポート（デフォルトでは 3022）でデータインターフェイス IP アドレスに接続することもできます。

SSH を使用して ASA に接続するには、まず、ASA の一般的な操作の設定ガイドに従って SSH アクセスを設定する必要があります。

ASA CLI から FXOS、およびその逆方向に接続することができます。

FXOS は最大 8 個の SSH 接続を許可します。

始める前に

管理 IP アドレスを変更するには、FXOS 管理 IP アドレスまたはゲートウェイの変更 （74 ページ）を参照してください。

手順

ステップ 1 管理 1/1 に接続している管理コンピュータで、管理 IP アドレスに SSH 接続します（デフォルトでは、https://192.168.45.45、ユーザ名：**admin**、パスワード：**Admin123**）。

任意のユーザ名でログインできます（ユーザの追加を参照）。リモート管理を設定する場合、ASA データ インターフェイス IP にポート 3022（デフォルトのポート）で SSH 接続します。

ステップ 2 ASA CLI に接続します。

connect asa

FXOS CLI に戻るには、Ctrl+a、d と入力します。

例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 ASA に SSH 接続する場合（ASA で SSH アクセスを設定した後）、FXOS CLI に接続します。

connect fxos

FXOS への認証を求められます。デフォルトのユーザ名：**admin** およびパスワード：**Admin123** を使用します。ASA CLI に戻るには、**exit** と入力するか、または Ctrl-Shift-6、x と入力します。

例：

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

保留中のコマンドのコミット、破棄、表示

CLI でコンフィギュレーション コマンドを入力する場合、設定を保存するまでコマンドは適用されません。コミットされるまでは、コンフィギュレーション コマンドは保留状態となり、廃棄できます。コマンドが保留中の場合、コマンド プロンプトの前にアスタリスク（*）が表示されます。設定の変更を保存または廃棄すると、アスタリスクが表示されなくなります。複数のコマンドモードで保留中の変更を積み重ね、まとめて適用できます。保留中のコマンドはどのコマンドモードでも表示できます。

手順

ステップ 1 保留中の設定変更を表示します。

show configuration pending

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
```

ステップ 2 設定を保存します。

commit-buffer

（注） 複数のコマンドをまとめてコミットすることは、単一の操作ではありません。失敗したコマンドがあっても、成功したコマンドは適用されます。失敗したコマンドはエラー メッセージで報告されます。

例：

```
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

ステップ 3 設定変更を廃棄します。

discard-buffer

例：

```
firepower-2110 /system/services/ntp-server* # discard-buffer
firepower-2110 /system/services/ntp-server #
```

例

次に、プロンプトがコマンド エントリのプロセス中に変わる例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

show コマンド出力の保存とフィルタリング

出力をテキスト ファイルにリダイレクトすると、**show** コマンドの出力を保存できます。出力をフィルタリング コマンドにパイピングすると、**show** コマンドの出力をフィルタリングできます。

出力の保存とフィルタリングはすべての **show** コマンドで使用できますが、大量のテキストを生成するコマンドを処理する場合に最も役立ちます。たとえば、**show configuration** コマンドを使用して、設定のすべてまたは一部を表示できます。設定の出力をコピーすると、設定をバックアップおよび復元できます。

（注） show コマンドではシークレット（パスワードフィールド）が表示されないため、新しいデバイスに設定を貼り付ける場合は、実際のパスワードを含めるように show 出力を変更する必要があります。

show コマンド出力のフィルタリング

show コマンドの出力をフィルタリングするには、次のサブコマンドを使用します。次の構文の説明で、 **show** コマンドの後の最初の縦棒 | はパイプ文字であり、コマンドに含まれ、構文の説明の一部ではありません。フィルタリング オプションはコマンドの最初の | 文字の後に入力します。

show *command* **|** {**begin** *expression* | **count** | **cut** *expression* | **egrep** *expression* | **end** *expression* | **exclude** *expression* | **grep** *expression* | **head** | **include** *expression* | **last** | **less** | **no-more** | **sort** *expression* | **tr** *expression* | **uniq** *expression* | **wc**}

フィルタリング オプション

フィルタリング サブコマンドは次のとおりです。

- **begin**：指定されたパターンを含む最初の行を検索し、その行と後続のすべての行を表示します。
- **count**：行数をカウントします。
- **cut**：各行の一部分を削除（「カット」）します。
- **egrep**：拡張タイプのパターンと一致する行のみを表示します。
- **end**：パターンと一致する行で終了します。
- **exclude**：パターンと一致するすべての行を除外し、その他のすべての行を表示します。
- **grep**：パターンと一致する行のみを表示します。
- **head**：最初の行を表示します。
- **include**：パターンと一致する行のみを表示します。
- **last**：最後の行を表示します。
- **less**：ページングのフィルタです。
- **no-more**：コマンド出力の改ページをオフにします。
- **sort**：行をソートします（ストリーム ソーター）。
- **tr**：文字を変換、スクイーズ、および削除します。
- **uniq**：連続した同一行の 1 つを除くすべてを破棄します。
- **wc**：行、単語、および文字の数を表示します。

expression

通常、式、つまりパターンは単純なテキスト文字列です。式を一重引用符または二重引用符で囲まないでください。式の一部として表示されます。また、末尾のスペースは式に含まれます。

（注） 次のサブコマンドのいくつかには、フィルタリングを詳細に制御できる追加オプションがあります。たとえば、**show configuration | head** および **show configuration | last** と指定すると、 **lines** キーワードを使用して表示される行数を変更できます。デフォルトは 10 です。さらに、**show configuration | sort** と指定すると、出力から重複行を削除するためのオプション **-u** を追加できます。（このオプションの詳細な説明は本ドキュメントの対象外です。さまざまなコマンドについては、FXOS のヘルプ出力を参照してください。詳細については、該当する Linux のヘルプを参照してください。）

例

次の例では、システム イベント ログ内の現在の行数を確認する方法を示します。

```
FP9300-A# show sel 1/1 | count
3008
FP9300-A#
```

次の例では、文字列「error」を含むシステム イベント ログの行を表示する方法を示します。

```
FP9300-A# show sel 1/1 | include error
968 | 05/15/2016 16:46:25 | CIMC | System Event DDR4_P2_H2_EC
C #0x99 | Upper critical - going high | Asserted | Reading 20
000 >= Threshold 20000 error
FP9300-A#
```

関連項目

show コマンド出力の保存 （7 ページ）

show コマンド出力の保存

出力をテキスト ファイルにリダイレクトすると、**show** コマンドの出力を保存できます。

show *command* [> {**ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:**}] | [>> {**volatile:** | **workspace:**}]

構文の説明		
	> {**ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }	選択したトランスポート プロトコルを使用して指定されたテキスト ファイルに **show** コマンド出力をリダイレクトします。 コマンドを入力すると、リモート サーバ名、IP アドレス、ユーザ名、ファイル パスなどがクエリされます。 この時点で **Enter** を押すと、出力がローカルに保存されます。
	>> {**volatile:** | **workspace:** }	**show** コマンド出力を適切なテキスト ファイルに追加します。このファイルはすでに存在している必要があります。

例

次の例では、現在の設定をシステム ワークスペースに保存しようとしています。設定ファイルがすでに存在しており、上書きするかどうかを選択できます。

```
FP9300-A# show configuration > workspace
File already exists, overwrite (y/n)?[n]n
Reissue command with >> if you want to append to existing file

FP9300-A#
```

関連項目

show コマンド出力のフィルタリング （6 ページ）

インターフェイス

FXOS で物理インタ フェースを管理できます。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、ASA で論理的に有効にする必要があります。

Firepower 2100 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。最大 MTU は 9184 です。

管理インターフェイスの詳細については、ASA と FXOS の管理を参照してください。

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、ASA で論理的に有効にする必要があります。FXOS と ASA の両方で、イーサネット 1/1 とイーサネット 1/2 のみがデフォルトで有効になっています。

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 イーサネットアップリンクを入力してから、fabric a モードを開始します。

scope eth-uplink

scope fabric a

例：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

ステップ 2 インターフェイスを有効にします。

enter interface *interface_id*

enable

例：

```
firepower-2110 /eth-uplink/fabric # enter interface Ethernet1/8
firepower-2110 /eth-uplink/fabric/interface # enable
firepower-2110 /eth-uplink/fabric/interface* #
```

ステップ 3 自動ネゴシエーションを有効または無効にします。

set auto-negotiation {**on** | **off**}

RJ-45 インターフェイスの場合、デフォルト設定は [on] です。

SFPインターフェイスの場合、デフォルト設定は[off]であり、自動ネゴシエーションを有効にすることはできません。

例：

```
firepower-2110 /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 4 自動ネゴシエーションを無効にする場合は、インターフェイス速度を設定します。

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

銅線インターフェイスの場合、この速度は自動ネゴシエーションを無効にした場合にのみ使用されます。

例：

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

ステップ 5 インターフェイスのデュプレックスモードを設定します。

set admin-duplex {**fullduplex** | **halfduplex**}

銅線インターフェイスの場合、このデュプレックスは自動ネゴシエーションを無効にした場合にのみ使用されます。

例：

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

ステップ 6 設定を保存します。

commit-buffer

例：

```
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

例

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink* # scope fabric a
firepower-2110 /eth-uplink/fabric* # enter interface ethernet1/6
firepower-2110 /eth-uplink/fabric/interface* # enable
firepower-2110 /eth-uplink/fabric/interface* # set flow-control-policy FlowControlPolicy23
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

EtherChannel の追加

EtherChannel（別名ポートチャネル）には、速度とデュプレックスが同じ最大 8 個のメンバーインターフェイスを含めることができます。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

（注） EtherChannel メンバー ポートは ASA に表示されますが、EtherChannel およびポート メンバーシップは FXOS でのみ設定できます。

（注） ASA は、LACP 高速レートをサポートしていません。 LACP では常に通常のレートが使用されます。

始める前に

Firepower 2100 は、アクティブまたはオンの Link Aggregation Control Protocol（LACP）モードで EtherChannel をサポートします。デフォルトでは、LACP モードはアクティブに設定されています。CLI でモードをオンに変更できます。最適な互換性を得るために、接続スイッチ ポートをアクティブ モードに設定することを推奨します。

手順

ステップ 1 イーサネットアップリンクを入力してから、fabric a モードを開始します。

scope eth-uplink

scope fabric a

例：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

ステップ 2 ポートチャネルを有効にします。

enter port-channel *ID*

enable

[ID] を 1 ～ 47 の整数に設定します。

例：

```
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
```

ステップ 3 メンバインターフェイスを割り当てます。

enter member-port *interface_id*

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/4
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
```

```
firepower-2110 /eth-uplink/fabric/port-channel* #
```

ステップ 4 （任意） LACP モードを設定します。

set port-channel-mode {**active** | **on**}

デフォルトは [Active] モードです。

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

ステップ 5 （任意） ポートチャネルのすべてのメンバについてインターフェイス速度を設定します。この設定は、個別のインターフェイスで設定されたプロパティよりも優先されます。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

これらのパラメータはポートチャネルのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 1gbps
```

ステップ 6 （任意）銅線ポートの場合、ポートチャネルのすべてのメンバについてインターフェイスデュプレックスモードを設定します。この設定は、個別のインターフェイスで設定されたプロパティよりも優先されます。

set duplex {**fullduplex** | **halfduplex**}

これらのパラメータはポートチャネルのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

ステップ 7 （任意） 説明を 256 文字以内で設定します。

set descr "*text***"**

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set descr "Inside Interface"
```

ステップ 8 設定を保存します。

commit-buffer

例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
```

```
firepower-2110 /eth-uplink/fabric/port-channel #
```

例

次に、3 つのインターフェイスを EtherChannel に追加し、LACP モードをオンに設定し、速度とフロー制御ポリシーを設定する例を示します。

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 10gbps

firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

モニタリング インターフェイス

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を表示します。

手順

ステップ 1 イーサネットアップリンクを入力してから、fabric a モードを開始します。

scope eth-uplink

scope fabric a

例：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

ステップ 2 シャーシにインストールされているインターフェイスを表示します。

show interface

Etherchannel のメンバ インターフェイスは、このリストには表示されません。

例：

```
firepower-2110 /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
    --------------- ------------------ ----------- ---------------- ------------
    Ethernet1/1     Mgmt               Enabled     Up
    Ethernet1/2     Data               Enabled     Link Down        Link failure
 or not-connected
    Ethernet1/3     Data               Enabled     Up
    Ethernet1/4     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/6     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/7     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
    Ethernet2/1     Data               Enabled     Up
    Ethernet2/2     Data               Enabled     Up
    Ethernet2/4     Data               Enabled     Up
    Ethernet2/5     Data               Enabled     Up
    Ethernet2/6     Data               Enabled     Up
    Ethernet3/2     Data               Enabled     Up
    Ethernet3/4     Data               Enabled     Up
```

プラットフォーム設定

時間や管理アクセスなどの FXOS の基本的な操作を設定できます。

日時の設定

Network Time Protocol（NTP）を設定したり、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したりできます。クロック設定は、Firepower 2100 シャーシと ASA OS の間で自動的に同期されます。

NTP を使用した日付と時刻の設定

NTP を使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。NTP はデフォルトで設定されているため、ASA はライセンスサーバに到達できます。最大 4 台の NTP サーバを設定できます。Firepower 2100 は NTP バージョン 3 を使用します。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 NTPサーバを追加します。

enter ntp-server {*hostname* | *ip_addr* | *ip6_addr*}

例：

```
firepower-2110 /system/services # enter ntp-server 192.168.6.5
firepower-2110 /system/services/ntp-server* #
```

ステップ 3 （任意）（ASA 9.10(1) 以降）NTP 認証を設定します。

NTP サーバ認証では SHA1 のみがサポートされます。NTP サーバからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーバ バージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp. keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージダイジェストの計算時に使用するキー値を通知するために使用します。

a) SHA1 キー ID を設定します。

set ntp-sha1-key-id *key_id*

b) SHA1 キー文字列を設定します。

set ntp-sha1-key-string

キー文字列を入力するように求められます。

c) ntp-server モードを修了します。

exit

d) NTP 認証をイネーブルにします。

enable ntp-authentication

例：

```
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower-2110 /system/services/ntp-server* # exit
firepower-2110 /system/services* # enable authentication
```

ステップ 4 タイム ゾーンを設定します。

set timezone

大陸、国、およびタイムゾーン地域に対応する番号を入力するように求められます。プロンプトごとに適切な情報を入力します。

例：

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
```

```
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

ステップ 5 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

ステップ 6 クロックの詳細を表示します。

- すべての設定済み NTP サーバの同期ステータスを表示します。

  show ntp-server [*hostname* | *ip_addr* | *ip6_addr*]

```
firepower-2110 /system/services # show ntp-server

NTP server hostname:
    Name                 Time Sync Status
    -------------------- ----------------
    0.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    1.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    2.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
```

- 特定の NTP サーバの同期ステータスを表示します。

  enter ntp-server {*hostname* | *ip_addr* | *ip6_addr*}

  show detail

  exit

```
firepower-2110 /system/services # enter ntp-server 0.sourcefire.pool.ntp.org
firepower-2110 /system/services/ntp-server # show detail

NTP server hostname:
    Name: 0.sourcefire.pool.ntp.org
    Time Sync Status: Unreachable Or Invalid Ntp Server
    Error Msg: Failed to translate domain name to IP, please verify the domain name
 or check if DNS server is configured.
```

```
firepower-2110 /system/services/ntp-server # exit
firepower-2110 /system/services #
```

- 設定されたタイムゾーンを表示します。

  show timezone

```
firepower-2110 /system/services # show timezone
Timezone: America/Los_Angeles
```

- 設定された日付と時刻を表示します。

  show clock

```
firepower-2110 /system/services # show clock
Wed Apr 18 08:49:35 PDT 2018
```

例

次に、IP アドレス 192.168.200.101 を持つ NTP サーバを設定する例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 192.168.200.101
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

手動での日時の設定

ここでは、Firepower 2100 シャーシで日付と時刻を手動で設定する方法ついて説明します。システム クロックの変更はただちに反映されます。システム クロックが NTP サーバと同期中である場合は、日付と時刻を手動で設定することはできません。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 時刻と日付を設定します。

set clock *month day year hour min sec*

- *month*：月を英語の月名の先頭 3 文字で設定します（1 月（January）の場合は jan）。
- *day*：日を 1 ～ 31 の範囲で設定します。
- *year*：年を 4 桁で設定します（2018 など）。
- *hour*：時を 24 時間形式で設定します。たとえば、午後 7 時は 19 と入力します。
- *min*：分を 0 ～ 59 の範囲で設定します。
- *sec*：秒を 0 ～ 59 の範囲で設定します。

システム クロックの変更はただちに反映されます。バッファをコミットする必要はありません。

例：

```
firepower-2110 /system/services # set clock apr 18 2018 9 39 30
Wed Apr 18 09:39:30 PDT 2018
firepower-2110 /system/services #
```

ステップ 3 タイム ゾーンを設定します。

set timezone

大陸、国、およびタイムゾーン地域に対応する番号を入力するように求められます。プロンプトごとに適切な情報を入力します。

例：

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
```

```
18) Dominica                  45) St Vincent
19) Dominican Republic        46) Suriname
20) Ecuador                   47) Trinidad & Tobago
21) El Salvador               48) Turks & Caicos Is
22) French Guiana             49) United States
23) Greenland                 50) Uruguay
24) Grenada                   51) Venezuela
25) Guadeloupe                52) Virgin Islands (UK)
26) Guatemala                 53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

ステップ 4 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

ステップ 5 クロックの詳細を表示します。

- 設定されたタイムゾーンを表示します。

  show timezone

  ```
  firepower-2110 /system/services # show timezone
  Timezone: America/Los_Angeles
  ```

- 設定された日付と時刻を表示します。

  show clock

  ```
  firepower-2110 /system/services # show clock
  Wed Apr 18 08:49:35 PDT 2018
  ```

例

次に、システムクロックを設定する例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set clock jun 24 2015 15 27 00
firepower-2110 /system/services #
```

シャーシ名の設定

始める前に

Firepower 2100 に使用する名前を FXOS CLI から設定できます。

手順

ステップ 1 システム モードに入ります。

scope system

例：

```
firepower-2110# scope system
firepower-2110 /system #
```

ステップ 2 現在の名前を表示します。

show

例：

```
firepower-2110 /system # show
Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- -------------------
    firepower-2110
               Stand Alone 10.122.203.17     ::
```

ステップ 3 新しい名前を設定します。

set name *device_name*

例：

```
firepower-2110 /system # set name fp2110-2
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* #
```

ステップ 4 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system* # commit-buffer
firepower-2110 /system #
fp2110-2 /system #
```

例

次の例では、デバイス名を変更します。

```
firepower-2110# scope system
firepower-2110 /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* # commit-buffer
firepower-2110 /system # show

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

ドメイン名の設定

Firepower 2100 は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、Firepower 2100 によって名前が修飾されて「jupiter.example.com」となります。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 ドメイン名を設定します。

set domain-name *name*

例：

```
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* #
```

ステップ 3 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

例

次に、ドメイン名を example.com に設定する例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

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。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。NTP サーバとの通信には DNS が必要です。

始める前に

DNS は、デフォルトでは次の OpenDNS サーバで構成されています：208.67.222.222、208.67.220.220。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 最大 4 台の DNS サーバを追加します。

enter dns {*ipv4_addr* | *ipv6_addr*}

例：

```
firepower-2110 /system/services* # enter dns 10.10.5.6
firepower-2110 /system/services* # enter dns 192.168.7.2
```

ステップ 3 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

例

次に、IPv4 アドレス 192.168.200.105 を持つ DNS サーバを設定する例を示します。

```
firepower-2110# scope system
```

```
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

次に、IPv6 アドレス 2001:db8::22:F376:FF3B:AB3F を持つ DNS サーバを設定する例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 2001:db8::22:F376:FF3B:AB3F
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

次に、IP アドレス 192.168.200.105 を持つ DNS サーバを削除する例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # delete dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

ログイン前バナーの追加

ログイン前バナーでは、ユーザが Firepower Chassis Manager にログインするとブラウザにバナーテキストが表示され、ユーザは、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、パスワードのプロンプトの前に端末でバナーテキストが表示されます。

手順

ステップ 1 セキュリティモードを開始し、次にバナーモードを開始します。

scope security

scope banner

例：

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner #
```

ステップ 2 ログイン前バナーを作成します。

enter pre-login-banner

例：

```
firepower-2110 /security/banner # enter pre-login-banner
firepower-2110 /security/banner/pre-login-banner* #
```

ステップ 3 Firepower Chassis Manager または FXOS CLI へのログイン前に FXOS でユーザに表示するメッセージを指定します。

set message

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。

メッセージの設定ダイアログをキャンセルするには、Ctrl+C キーを押します。

例：

```
firepower-2110 /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 2100
>**Unauthorized use is prohibited**
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* #
```

ステップ 4 設定を保存します。

commit-buffer

例：

```
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

例

次の例は、ログイン前バナーを作成します。

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner # create pre-login-banner
firepower-2110 /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 2110
>**Unauthorized use is prohibited**
>Contact admin@example.com for information.
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

SSH の設定

次の手順では、FXOS への SSH アクセスを有効または無効にする方法について説明します。SSH はデフォルトで有効になっています。

始める前に

これらの手順はコンソールで実行することをお勧めします。そうしないと SSH セッションから切断される場合があります。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 Firepower シャーシへの SSH 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 SSH アクセスを許可します。

  enable ssh-server

- Firepower シャーシへの SSH アクセスを禁止します。

  disable ssh-server

例：

```
firepower-2110 /system/services # disable ssh-server
firepower-2110 /system/services* #
```

ステップ 3 暗号化アルゴリズムを指定します。

set ssh-server encrypt-algorithm プロトコル

次の 1 つ以上のプロトコルを、スペースまたはカンマで区切って設定します。

- 3des-cbc
- aes128-cbc
- aes128-ctr
- aes128-gcm_openssh_com
- aes192-cbc

- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm_openssh_com
- chacha20-poly1305_openssh_com

デフォルトでは、すべてのプロトコルが許可されます。

例：

```
firepower-2110 /system/services* # set ssh-server encrypt-algorithm aes256-ctr,aes256-cbc
```

ステップ 4 キー交換アルゴリズムを設定します。

set ssh-server kex-algorithm *algorithms*

次の 1 つ以上のアルゴリズムを、スペースまたはカンマで区切って設定します。

- curve25519-sha256
- curve25519-sha256_libssh_org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

デフォルトでは、すべてのプロトコルが許可されます。

例：

```
firepower-2110 /system/services* # set ssh-server kex-algorithm
diffie-hellman-group14-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

ステップ 5 整合性アルゴリズムを設定します。

set ssh-server mac-algorithm プロトコル

次の 1 つ以上のプロトコルを、スペースまたはカンマで区切って設定します。

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

デフォルトでは、すべてのプロトコルが許可されます。

例：

```
firepower-2110 /system/services* # set ssh-server mac-algorithm hmac-sha2-512
```

ステップ 6 サーバのホストキーを設定します。

set ssh-server host-key rsa *modulus*

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。

例：

```
firepower-2110 /system/services* # set ssh-server host-key rsa 2048
```

ステップ 7 サーバのキー再生成制限を設定し、ボリューム（接続で許可されるトラフィックの量、KB 単位）と、FXOS がセッションを切断するまでの時間（SSH セッションがアイドル状態を続けられる長さ、分単位）を設定します。

set ssh-server rekey-limit volume {*kb* | **none**} **time** {*minutes* | **none**}

- **volume** *kb*：トラフィックの最大量を 100 ～ 4194303 KB の間で設定します。デフォルトは無制限（なし）です。
- **time** *minutes*：最大時間を 10 ～ 1440 分の間で設定します。デフォルトは無制限（なし）です。
- **none**: 制限を無効にします。この設定は、デフォルトです。

例：

```
firepower-2110 /system/services* # set ssh-server rekey-limit volume none time 1440
```

ステップ 8 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

例

次に、Firepower シャーシへの SSH アクセスを有効にする例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable ssh-server
```

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

HTTPS または IPSec の証明書、キーリング、およびトラストポイントの設定

HTTPS および IPSec は、公開キーインフラストラクチャ（PKI）を使用して、2 つのデバイス（クライアントのブラウザと Firepower 2100 など）の間でセキュアな通信を確立します。

証明書、キーリング、およびトラストポイントについて

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 2100 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）暗号キーまたは楕円曲線デジタル署名アルゴリズム（ECDSA）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、通常の長さは 512 ビット ～ 2048 ビットです。通常、長いキーは短いキーよりもより安全です。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。

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。

証明書が期限切れになった場合は、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。

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。

（注） 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。

トラスト ID 証明書のインストール

デフォルトでは、Firepower Chassis Manager で使用する自己署名 SSL 証明書が生成されます。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から初めて Firepower Chassis Manager にアクセスするとき、ブラウザには SSL の警告が表示され、ユーザに対して Firepower Chassis Manager にアクセスする前に証明書を受け入れるよう要求します。FXOS CLI を使用して証明書署名要求（CSR）を生成し、Firepower Chassis Manager 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。FXOS は、「デフォルト」のキーリングを含め最大 8 個のキーリングをサポートしています。

始める前に

DNS サーバの設定 （24 ページ）。

手順

ステップ 1 セキュリティモードを開始します。

scope security

例：

```
firepower-2110# scope security
firepower-2110 /security #
```

ステップ 2 キーリングに追加する証明書のトラストポイントを定義します。

create trustpoint *name*

例：

```
firepower-2110 /security # create trustpoint trust1
firepower-2110 /security/trustpoint* #
```

ステップ 3 証明書チェーンに貼り付けます。この証明書チェーンはトラストアンカーまたは認証局から入手します。

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。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。

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。FXOS CLI でテキストブロック全体をコピーして貼り付けます。

例：

```
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* #
```

ステップ 4 トラストポイントモードを終了します。

exit

例：

```
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* #
```

ステップ 5 キー リングを作成します。

create keyring *keyring_name*

例：

```
firepower-2110 /security # create keyring keyring1
```

```
firepower-2110 /security/keyring* #
```

ステップ 6 キータイプを RSA（デフォルト）または ECDSA に設定します。

set keypair-type {**rsa** | **edcsa**}

例：

```
firepower-2110 /security/keyring* # set keypair-type edcsa
```

ステップ 7 （RSA の場合）SSL キーのビット長を設定します。

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

例：

```
firepower-2110 /security/keyring* # set modulus mod2048
```

ステップ 8 （EDCSA の場合）楕円曲線を設定します。

set elliptic-curve {**secp256r1** | **secp384r1** | **secp384r1**}

例：

```
firepower-2110 /security/keyring* # set elliptic-curve secp384r1
```

ステップ 9 証明書要求を作成します。

create certreq

例：

```
firepower-2110 /security/keyring* # create certreq
firepower-2110 /security/keyring/certreq* #
```

ステップ 10 証明書パスワードを設定します。

set password

例：

```
firepower-2110 /security/keyring/certreq* # set password
Certificate request password: diagonalapple
Confirm certificate request password: diagonalapple
```

ステップ 11 Firepower 2100 の IP アドレスまたは FQDN を指定します。

set {**ip** | **ipv6**} {*ipv_address* | *fqdn*}

複数の IP アドレスを設定できます。

例：

```
firepower-2110 /security/keyring/certreq* # set ip 10.10.9.2
```

ステップ 12 シャーシの DNS ルックアップに使用されるシャーシの完全修飾ドメイン名を指定します。

set subject-name *fqdn*

SubjectName と、少なくとも 1 つの DNS SubjectAlternateName 名が必要です。SubjectName は、DNS SubjectAlternateName として自動的に追加されます。

例：

```
firepower-2110 /security/keyring/certreq* # set subject-name firepower1.example.com
```

ステップ 13 （任意） 詳細オプションを設定します。

a) 会社が所在する国の 2 文字の国コードを指定します。

set country *country_name*

例：

```
firepower-2110 /security/keyring/certreq* # set country us
```

b) この証明書を別のホスト名に適用する場合は、サブジェクトの別名を指定します。

set dns *subject_alt_name*

複数の DNS 名を設定できます。

例：

```
firepower-2110 /security/keyring/certreq* # set dns firepower2.example.com
```

c) 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。

set e-mail *E-mail_name*

複数の電子メールアドレスを設定できます。

例：

```
firepower-2110 /security/keyring/certreq* # set e-mail admin@example.com
```

d) 証明書を要求している会社の本社が所在する市または町を指定します。

set locality *locality_name*

例：

```
firepower-2110 /security/keyring/certreq* # set locality boulder
```

e) 証明書を要求している組織を指定します。

set org-name *organization_name*

例：

```
firepower-2110 /security/keyring/certreq* # set org-name Example.com
```

f) 組織単位を指定します。

set org-unit-name *organizational_unit_name*

例：

```
firepower-2110 /security/keyring/certreq* # set org-unit-name engineering
```

g) 証明書を要求している会社の本社が所在する州または行政区分を指定します。

set state *state_province_or_county*

例：

```
firepower-2110 /security/keyring/certreq* # set state co
```

ステップ 14 設定を保存します。

commit-buffer

証明書署名要求を生成する前に、すべてのホスト名が DNS を使用して解決されます。ホスト名の解決に失敗した場合、コマンドはエラーを出力します。

例：

```
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq #
```

ステップ 15 証明書要求を表示し、要求をコピーして、トラストアンカーまたは認証局に送信します。

show certreq

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。

例：

```
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: firepower1.example.com
Certificate request ip address: 10.10.10.9
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request country name:
State, province or county (full name):
Locality name (eg, city):
Organisation name (eg, company):
Organisational Unit Name (eg, section):
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwITEfMB0GA1UEAwwWZmlyZXBvd2VyMS5leGFtcGxlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJM7bmSCJte3gAU9DgDVN3E
tEfrbf0hMeLYgs5qkkvW7T8x3gHKn2Lwk4wFFAdHPxceVZwaBnXW8F5MFzdtyBY+
```

```
Du+RkpraLtle4HEMdNw1rnoDcv4ZHmbK47XYR1SFXSzer5lOXptGbOCloUn34L6/
pKlDlfV+1L+LlDYD++RG2DhbekWcFk13loZvCVhw99Wmc4X7CsypKY4uGH3lAwnl
/TF32ORXi0t2GXju6kbqUahhxN2kGxL7+4eLBeA/ninajCkJDIGJlnXuFa2ArfbF
39p+3UuVzcc9V/OH6d+buLjmQvtn+DwoPQhCVDYlNt+p3ZgnqnJWULNLBPMlof0C
AwEAAaA6MDgGCSqGSIb3DQEJDjErMCkwJwYDVR0RBCAwHoIWZmlyZXBvd2VyMS5l
eGFtcGxlLmNvbYcECgoKCTANBgkqhkiG9w0BAQsFAAOCAQEAjBw8lEb6cRapyMh/
Dfiyuet4wT0QmXQKy3xLXQjv6RGb5SOf3NkcaNvcx3KuKJwoJQGhdRV4Jhk4rgmT
QmlWX4rY7B2MFUwf6qSaj/E5W0N0RQg+5aZ/hZjPGV3zcuzY6yfixxXBpoPAirZQ
2luPaa21+HR4LTDInRj0127xMIkeKmv7AHSjyMoJdgs8DGJilTwPy93kZV//Iq9P
LrnKR7gpsXzXOoK6PTxP3pwhC21qjdmevn3ICPjDI68AtqjAuB15p/T2l+GFi/gB
XJMx2Mm9qiope3FEXIGH2ZhbJ+P7oBfGzgx2EHSI8H98O8a9uO8WV2yd/dKtv2IG
ICxHEw==
-----END CERTIFICATE REQUEST-----
```

ステップ 16 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 17 certreq モードを終了します。

exit

例：

```
firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
```

ステップ 18 以前に作成したトラストポイントを指定します。

set trustpoint *name*

例：

```
firepower-2110 /security/keyring # set trustpoint trust1
firepower-2110 /security/keyring* #
```

ステップ 19 トラストアンカーまたは認証局から入手した証明書をアップロードします。

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。証明書の後の行に **ENDOFBUF** と入力して、証明書の入力を完了します。

（注） 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。

例：

```
firepower-2110 /security/keyring* #
```

ステップ 20 設定を保存します。

commit-buffer

例：

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

ステップ 21 インポートした証明書の内容を表示し、**Certificate Status** の値が **Valid** と表示されることを確認します。

show keyring *keyring_name* **detail**

例：

```
firepower-2110 /security #  scope security
firepower-2110 /security #  show keyring kr1 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-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

例

次に、新しいキーリングに証明書を追加する例を示します。

```
firepower-2110# scope security
firepower-2110 /security # enter trustpoint tPoint10
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
```

```
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* # enter keyring kr220
firepower-2110 /security/keyring* # set modulus mod1024
firepower-2110 /security/keyring* # enter certreq
Certificate request password: peonygarage
Confirm certificate request password: peonygarage
firepower-2110 /security/keyring/certreq* # set ip 192.168.200.123
firepower-2110 /security/keyring/certreq* # set subject-name sjc04.example.com
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: sjc04.example.com
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/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
firepower-2110 /security/keyring # set trustpoint tPoint10
firepower-2110 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
```

```
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

デフォルトのキーリング証明書の再生成

証明書が期限切れになった場合は、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。

scope security

例：

```
firepower-2110# scope security
firepower-2110 /security #
```

ステップ 2 デフォルトのキーリングを入力します。

enter keyring default

例：

```
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring #
```

ステップ 3 デフォルト キー リングを再生成します。

set regenerate yes

例：

```
firepower-2110 /security/keyring # set regenerate yes
```

ステップ 4 設定を保存します。

commit-buffer

例：

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

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-2110# scope security
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring # set regenerate yes
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

HTTPS の設定

デフォルトでは、HTTPS サービスはポート 443 で有効になっています。Firepower Chassis Manager のアクセスを禁止する場合、または HTTPS 設定をカスタマイズする場合は（HTTPS セッションに使用するキーリングを指定するなど）、HTTPS を無効にできます。デフォルトでは、Firepower 2100 は自己署名証明書でデフォルトのキーリングを使用します。

（注） 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 （任意） トラスト ID 証明書のインストール （31 ページ）。

ステップ 2 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
Firepower-chassis /system/services #
```

ステップ 3 Firepower シャーシへの HTTPS 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 HTTPS アクセスを許可します。

  enable https

- Firepower シャーシへの HTTPS アクセスを禁止します。

  disable https

例：

```
firepower-2110 /system/services # disable https
firepower-2110 /system/services* #
```

ステップ 4 （任意） HTTPS ポートを指定します。ポート 443 がデフォルト ポートです。

set https port *port_num*

例：

```
Firepower-chassis /system/services* # set https port 4443
```

ステップ 5 （任意） 追加したキーリングの名前を指定します。「トラスト ID 証明書のインストール （31 ページ）」を参照してください。

set https keyring *keyring_name*

例：

```
Firepower-chassis /system/services* # set https keyring kr1
```

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。

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**
- （デフォルト） **medium-strength**
- **low-strength**
- **custom**：**set https cipher-suite** コマンドを使用して、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。

例：

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

ステップ 7 （任意） 暗号スイートモードを **custom** に設定した場合は、カスタム暗号スイートを指定します。

set https cipher-suite *cipher_suite_string*

cipher_suite_string では最大 256 文字まで使用できますが、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#sslciphersuite 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

例：

```
Firepower-chassis /system/services* # set https cipher-suite
DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
```

ステップ 8 SSL バージョンを設定します。

set https access-protocols *comma_separated_values*

comma_separated_values には次があります。

- **tlsv1**
- **tlsv1.1**
- **tlsv1.2**
- **sslv3**

（注） 新しいブラウザはSSLv3をサポートしていないため、他のプロトコルも指定する必要があります。SSLv3のみを指定した場合は、サポートされていないセキュリティ プロトコル バージョンを示すエラーがブラウザに表示されることがあります。

ステップ 9 （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**}

例：

```
Firepower-chassis /system/services* # set revoke-policy strict
```

ステップ 10 設定を保存します。

commit-buffer

例：

```
Firepower-chassis /system/services* # commit-buffer
firepower-2110 /system/services #
```

例

次の例では、HTTPS を有効にし、ポート番号を 4443 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 レベルを高に設定します。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 4443
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 #
```

IPSec セキュアチャネルの設定

管理トラフィックを暗号化するように IPSec トンネルを設定できます。Firepower 2100 は、次の暗号とアルゴリズムをサポートしています。

表 *1: IKE* および *ESP* の暗号とアルゴリズム

タイプ	値
暗号	aes128、aes192、aes256、aes128gcm16
疑似ランダム関数（PRF）（IKE のみ）	prfsha1、prfsha384、prfsha512、prfsha256
整合性アルゴリズム	sha1、sha256、sha384、sha512、sha1_160
Diffie-Hellman グループ	modp2048、curve25519、ecp256、ecp384、ecp521、modp3072、modp4096

（注） curve25519 は FIPS またはコモンクライテリアモードではサポートされていません。

始める前に

FIPS モードの場合、IPSec ピアは RFC 7427 をサポートしている必要があります。

手順

ステップ 1 トラスト ID 証明書のインストール （31 ページ）。

ステップ 2 セキュリティモードを開始し、次に IPSec モードを開始します。

scope security

scope ipsec

例：

```
Firepower-2110# scope security
Firepower-2110 /security # scope ipsec
Firepower-2110 /security/ipsec #
```

ステップ 3 （任意） ログ冗長レベルを設定します。

set log-level *0-4*

例：

```
Firepower-2110 /security/ipsec # set log-level 3
Firepower-2110 /security/ipsec* #
```

ステップ 4 （任意） 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** | **no**}

- **yes**：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。
- **no**：SA 適用検査にパスし、接続は成功します。

例：

```
Firepower-2110 /security/ipsec # set sa-strength-enforcement yes
Firepower-2110 /security/ipsec* #
```

ステップ 5 IPSec 接続を作成し、入力します。

create connection *connection_name*

ステップ 6 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 7 ローカル IP アドレスを設定します。

set local-address *ip_address*

ステップ 8 リモート IP アドレスを設定します。

set remote-address *ip_address*

DNS サーバを設定した場合は、FQDN としてリモートアドレスを指定できます（DNS サーバの設定 （24 ページ）を参照）。

例：

```
Firepower-2110 /security/ipsec/connection* # set remote-address
```

ステップ 9 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 10 リモート ID を設定します。

set remote-ike-id *remote_identity_name*

set fqdn-enforce コマンドで FQDN の使用を適用する場合は、このコマンドで FQDN を使用する必要があります。

例：

```
Firepower-2110 /security/ipsec/connection* # set remote-ike-id charlesdarwin.cisco.com
```

ステップ 11 FQDN の使用を適用します。

set fqdn-enforce {**none** | **remote-ike-id**}

この機能を有効にする場合は、DNS を設定する必要があります（DNS サーバの設定 （24 ページ）を参照）。9.13(1) より前に作成された接続を除き、適用はデフォルトで有効になっています。古い接続への適用は手動で有効にする必要があります。

有効なリモート IKE ID（**set remote-ike-id**）を FQDN 形式で設定する必要があります。FQDN の適用を無効にした場合、リモート IKE ID はオプションとなり、任意の形式（FQDN、IP アドレス、サブジェクト名など）で設定できます。

例：

```
Firepower-2110 /security/ipsec/connection* # set fqdn-enforce remote-ike-id
```

ステップ 12 キーリング名を設定します。

set keyring-name *name*

ステップ 13 （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 14 （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 15 （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 16 （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 17 （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 18 接続を有効にします。

set admin-state enable

ステップ 19 接続をリロードします。

reload-conns

以前に確立されていなかった接続は再試行されます。確立された接続は維持されます。

ステップ 20 （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*

管理アクセスの設定

デフォルトでは、Firepower 2100 は、管理 1/1 192.168.45.0/24 ネットワークで、Firepower Chassis Manager への HTTPS アクセス、および SSH アクセスを許可します。他のネットワークからのアクセスを許可、または SNMP を許可する場合は、アクセス リストを追加または変更する必要があります。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 アクセスを有効にする必要があるサービスのアクセスリストを作成します。

IPv4 の場合：

enter ip-block *ip prefix_length* {**https** | **snmp** | **ssh**}

IPv6 の場合：

enter ipv6-block *ip prefix_length* **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。

- *ip*：サブネットを 0.0.0.0、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。
- *prefix_length*：IPv4 の場合、プレフィックス長は 0 ～ 32 です。IPv6 の場合、プレフィックス長は 0 ～ 128 です。

例：

```
firepower-2110 /system/services # enter ip-block 0.0.0.0 0 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.0.0.0 8 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.0.0 16 ssh
```

```
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.10.3.0 24 snmp
firepower-2110 /system/services/ip-block* #
```

ステップ 3 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block #
```

例

IPv4：

```
firepower-2110 # scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ip-block 10.1.1.0 24 https
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.2.1.0 24 ssh
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.3.1.0 24 snmp
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # show ip-block
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    10.1.1.0        24            Https
    10.2.1.0        24            Ssh
    10.3.1.0        24            Snmp
```

IPv6

```
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 ssh
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 snmp
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 https
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # show ipv6-block
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    2001:0DB8:BA98::   64      Https
    2001:0DB8:BA98::   64      Snmp
    2001:0DB8:BA98::   64      Ssh
```

管理クライアントの DHCP サーバの設定

管理 1/1 インターフェイスに接続しているクライアントに対して DHCP サーバを有効にすることができます。デフォルトでは、サーバはアドレス範囲 192.168.45.10 ～ 192.168.45.12 で有効になっています。管理 IP アドレスを変更する場合、DHCP を無効にする必要があります（FXOS 管理 IP アドレスまたはゲートウェイの変更 （74 ページ）を参照）。その後、新しいネットワークの DHCP を再度有効にすることができます。

手順

ステップ 1 システムモードを開始し、次にサービスモードを開始します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

ステップ 2 DHCP サーバを設定するには、次のいずれかを実行します。

- DHCP サーバを有効にします。

  enable dhcp-server *start_ip end_ip*

- DHCP サーバを無効にします。

  disable dhcp-server

例：

```
firepower-2110 /system/services # enable dhcp-server 10.10.10.5 10.10.10.50
firepower-2110 /system/services* #
```

ステップ 3 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

例

次に、DHCP サーバを有効にする例を示します。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.1.8 192.168.1.40
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

syslog メッセージの設定

ログは、ルーチンの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。syslog メッセージは、Firepower 2100 コンソール、SSH セッション、またはローカルファイルに送信できます。

これらの syslog メッセージは FXOS シャーシにのみ適用されます。ASA syslog メッセージの場合、ASA 設定でロギングを設定する必要があります。

手順

ステップ 1 モニタリング モードを開始します。

scope monitoring

例：

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

ステップ 2 syslog メッセージを生成するローカルソースを設定します。

- **enable syslog source** {**audits** | **events** | **faults**}
- **disable syslog source** {**audits** | **events** | **faults**}

例：

```
firepower-2110 /monitoring # disable syslog source audits
firepower-2110 /monitoring* # enable syslog source events
firepower-2110 /monitoring* # enable syslog source faults
```

ステップ 3 コンソールに syslog メッセージを送信します。

a) コンソールへの syslog の送信を有効または無効にします。

- **enable syslog console**
- **disable syslog console**

例：

```
firepower-2110 /monitoring* # enable syslog console
```

b) コンソールに表示するメッセージの最低レベルを選択します。

set syslog console level {**emergencies** | **alerts** | **critical**}

コンソールにはこのレベル以上のメッセージが表示されます。レベルオプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。

例：

```
firepower-2110 /monitoring* # set syslog console level alerts
```

ステップ 4 SSH セッションに syslog メッセージを送信します。

a) SSH セッションへの syslog メッセージの送信を有効または無効にします。

- **enable syslog monitor**
- **disable syslog monitor**

例：

```
firepower-2110 /monitoring* # enable syslog monitor
```

b) SSH セッションに表示するメッセージの最低レベルを選択します。

set syslog monitor level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

このレベル以上のメッセージが表示されます。レベルオプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。

（注） **terminal monitor** コマンドを入力した場合にだけ、Critical より下のレベルのメッセージが端末のモニタに表示されます。

例：

```
firepower-2110 /monitoring* # set syslog monitor level alerts
```

ステップ 5 ファイルに syslog メッセージを送信します。

a) syslog ファイルへの syslog 情報の書き込みを有効または無効にします。

- **enable syslog file**
- **disable syslog file**

例：

```
firepower-2110 /monitoring* # enable syslog file
```

b) メッセージが記録されるファイルの名前を指定します。

set syslog file name *filename*

ファイル名は 16 文字まで入力できます。

例：

```
firepower-2110 /monitoring* # set syslog file name syslog1
```

c) ファイルに保存するメッセージの最低レベルを選択します。

set syslog file level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

このレベル以上の syslog ファイルが保存されます。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。

例：

```
firepower-2110 /monitoring* # set syslog file level debugging
```

d) 最大ファイルサイズ（バイト単位）を指定します。このサイズを超えると、最も古いメッセージを最新のメッセージで上書きします。

set syslog file size *filesize*

有効な範囲は 4096 ～ 4194304 バイトです。

例：

```
firepower-2110 /monitoring* # set syslog file size 60000
```

ステップ 6 設定を保存します。

commit-buffer

例：

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

例

次の例は、ローカルファイルへの syslog メッセージの保存を有効にする方法を示しています。

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # disable syslog console
firepower-2110 /monitoring* # disable syslog monitor
firepower-2110 /monitoring* # enable syslog file
```

```
firepower-2110 /monitoring* # set syslog file name SysMsgsFirepower
firepower-2110 /monitoring* # set syslog file level notifications
firepower-2110 /monitoring* # set syslog file size 4194304
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

SNMP の有効化

このセクションでは、Firepowerシャーシに簡易ネットワーク管理プロトコル（SNMP）を設定する方法を説明します。

SNMP の概要

SNMPは、アプリケーション層プロトコルであり、SNMPマネージャとSNMPエージェントとの通信に使用されるメッセージフォーマットを提供します。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 のデータを維持し、必要に応じてそのデータを SNMP マネージャに報告するFirepowerシャーシ内のソフトウェア コンポーネント。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。
- 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 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 モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

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、メッセージが開示されないよう保護または認証の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 *2: 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	水準器	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング（Community string）	なし	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（Community string）	なし	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（Username）]	なし	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。

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

SHAベースの認証に加えて、FirepowerシャーシはAES-128ビットAdvanced Encryption Standardを使用したプライバシーも提供します。Firepower シャーシは、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 80 文字を指定できます。

SNMP の設定

SNMP を有効にし、トラップおよび SNMPv3 ユーザを追加します。

手順

ステップ 1 モニタリング モードを開始します。

scope monitoring

例：

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

ステップ 2 SNMP をイネーブルにします。

enable snmp

例：

```
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* #
```

ステップ 3 SNMP コミュニティ名を設定します。

set snmp community

SNMP コミュニティ名を入力するよう求められます。コミュニティ名は、最大 32 文字の英数字で指定できます。

例：

```
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: community1
firepower-2110 /monitoring* #
```

ステップ 4 SNMP のシステム担当者の連絡先を指定します。

set snmp syscontact *system-contact-name*

システム担当者の連絡先名（電子メールアドレスや、名前と電話番号など）は、最大255 文字の英数字で指定できます。

例：

```
firepower-2110 /monitoring* # set snmp syscontact jcrichton@example.com
firepower-2110 /monitoring* #
```

ステップ 5 SNMP エージェント（サーバ）が実行するホストの場所を指定します。

set snmp syslocation *system-location-name*

システム ロケーション名は、最大 512 文字の英数字で指定できます。

例：

```
firepower-2110 /monitoring* # set snmp syslocation boulder, co
firepower-2110 /monitoring* #
```

ステップ 6 SNMPv3 ユーザを作成します。

a) ユーザ名とパスワードを指定します。

enter snmp-user *user-name*

パスワードを入力するよう求められます。

例：

```
firepower-2110 /monitoring* # enter snmp-user jcrichton
Password: aerynsun
```

```
firepower-2110 /monitoring/snmp-user* #
```

b) AES-128 暗号化を有効にする

set aes-128 {**no** | **yes**}

デフォルトでは、AES-128 暗号化は無効になっています。

例：

```
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* #
```

c) ユーザプライバシーパスワードを指定します。

set priv-password

プライバシーパスワードを入力して確認するよう求められます。

例：

```
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: moyahome
Confirm the password: moyahome
firepower-2110 /monitoring/snmp-user* #
```

d) SNMP ユーザモードを終了します。

exit

例：

```
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
```

ステップ 7 SNMP トラップを追加します。

a) SNMP トラップを作成します。

enter snmp-trap {*hostname* | *ip-addr* | *ip6-addr*}

例：

```
firepower-2110 /monitoring* # enter snmp-trap 10.10.10.67
firepower-2110 /monitoring/snmp-trap* #
```

b) SNMP トラップに使用する SNMP コミュニティ名を指定します。

set community *community-name*

例：

```
firepower-2110 /monitoring/snmp-trap* # set community community1
firepower-2110 /monitoring/snmp-trap* #
```

c) SNMP トラップに使用するポートを指定します。

set port *port-num*

例：

```
firepower-2110 /monitoring/snmp-trap* # set port 3434
firepower-2110 /monitoring/snmp-trap* #
```

d) トラップに使用する SNMP バージョンおよびモデルを指定します。

set version {**v1** | **v2c** | **v3**}

例：

```
firepower-2110 /monitoring/snmp-trap* # set version v2c
firepower-2110 /monitoring/snmp-trap* #
```

e) （任意） 送信するトラップのタイプを指定します。

set notificationtype {**traps** | **informs**}

- **traps**：バージョンに v2c または v3 を選択した場合は、トラップのタイプを設定します。
- **informs**：バージョンに v2c を選択した場合は、通知のタイプを設定します。

例：

```
firepower-2110 /monitoring/snmp-trap* # set notificationtype informs
firepower-2110 /monitoring/snmp-trap* #
```

f) （任意） ：バージョンに v3 を選択した場合は、トラップに関連付けられる権限を指定します。

set v3privilege {**auth** | **noauth** | **priv**}

- **auth**：認証を有効にしますが、暗号化しません。
- **noauth**：認証または暗号化を有効にしません。
- **priv**：認証と暗号化を有効にします。

例：

```
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* #
```

g) SNMP トラップモードを終了します。

exit

例：

```
firepower-2110 /monitoring/snmp-trap* # exit
```

```
    firepower-2110 /monitoring* #
```

ステップ 8 設定を保存します。

commit-buffer

例：

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

例

次の例では、SNMP を有効にします。

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
firepower-2110 /monitoring* # set snmp syscontact contactperson1
firepower-2110 /monitoring* # set snmp syslocation systemlocation
firepower-2110 /monitoring* # enter snmp-user snmp-user14
Password: happy
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: ecstatic
Confirm the password: ecstatic
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 192.168.100.112
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem2
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 2001::1
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem3
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # commit-buffer
firepower-2110 /monitoring/snmp-trap #
```

FIPS およびコモンクライテリアモードの有効化

Firepower 2100 で FIPS またはコモン クライテリア（CC）モードを有効にするには、次の手順を実行します。

また、**fips enable** コマンドを使用して ASA で個別に FIPS モードを有効にする必要もあります。ASA には、コモン クライテリア モードに関する個別の設定はありません。CC または UCAPL のコンプライアンスに関する追加の制限があれば、シスコのセキュリティ ポリシーのマニュアルに従って設定する必要があります。

最初に ASA で FIPS モードを設定し、デバイスのリロードを待ってから、FXOS で FIPS モードを設定することをお勧めします。

手順

ステップ 1 セキュリティモードを開始します。

scope security

例：

```
firepower-2110# scope security
firepower-2110 /security #
```

ステップ 2 FIPS モードを有効にします。

enable fips-mode

例：

```
firepower-2110 /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in
a FIPS approved mode.
firepower-2110 /security* #
```

ステップ 3 コモンクライテリアモードを有効にします。

enable cc-mode

例：

```
firepower-2110 /security* # enable cc-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's CC Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in
a CC approved mode.
```

ステップ 4 設定を保存します。

commit-buffer

例：

```
firepower-2110 /security* # commit-buffer
firepower-2110 /security #
```

ステップ 5 システムをリブートします。

scope chassis 1

reboot

例：

```
firepower-2110 /security # scope chassis 1
firepower-2110 /chassis # reboot
```

ユーザ管理

ユーザ アカウントは、Firepower 2100 シャーシにアクセスするために使用されます。これらのアカウントは、Firepower Chassis Manager および SSH アクセスで使用されます。ASA には別のユーザ アカウントと認証があります。

ユーザ アカウントについて

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。デフォルトのパスワードは **Admin123** です。

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することはできません。

ローカル認証されたユーザ アカウント

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。

ローカル認証されたユーザアカウントは、管理者権限を持つユーザであれば誰でも有効または無効にすることができます。

ユーザ アカウントに関するガイドライン

ユーザ名

ユーザ名は、Firepower Chassis Manager および FXOS CLI のログイン ID として使用されます。ログイン ID の割り当てにあたっては、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。数字やアンダースコアなどの特殊文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

ローカル認証されたユーザアカウントごとに、パスワードが必要です。管理者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。ローカル認証ユーザのパスワード強度チェックを有効にすると、FXOS は次の要件を満たしていないパスワードを拒否します。

- 少なくとも 8 文字を含み、最大 127 文字であること

（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。

- 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、辞書に記載されている標準的な単語に基づくパスワード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）。
- 空白にすることはできません。

ユーザの追加

Firepower Chassis Manager および FXOS CLI アクセスのローカル ユーザを追加します。

始める前に

ローカルユーザアカウントを追加または編集するには、admin 権限を持つユーザである必要があります。

手順

ステップ 1 セキュリティ モードに入ります。

scope security

例：

```
firepower-2110# scope security
firepower-2110 /security #
```

ステップ 2 ユーザ アカウントを作成します。

enter local-user *local-user-name*

- *local-user-name*：このアカウントへのログイン時に使用するアカウント名を設定します。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（ユーザ アカウントに関するガイドライン （61 ページ）を参照）。

ユーザを作成した後は、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。

例：

```
firepower-2110 /security # enter local-user johncrichton
firepower-2110 /security/local-user* #
```

ステップ 3 ローカル ユーザ アカウントをアクティブ化するか非アクティブ化するかを指定します。

set account-status {**active**| **inactive**}

デフォルトでは、ユーザはアクティブです。

例：

```
firepower-2110 /security/local-user* # set account-status inactive
```

ステップ 4 ユーザ アカウントのパスワードを設定します。

set password

パスワードを入力します。*password*

パスワードを確認します。*password*

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。FXOS 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（ユーザ設定値の設定（66 ページ）およびユーザ アカウントに関するガイドライン（61 ページ）を参照）。

例：

```
firepower-2110 /security/local-user* # set password
Enter a password: aeryn
Confirm the password: aeryn
firepower-2110 /security/local-user* #
```

ステップ 5　（任意）ユーザの名を指定します。

set firstname　*first-name*

例：

```
firepower-2110 /security/local-user* # set firstname John
```

ステップ 6　（任意）ユーザの姓を指定します。

set lastname　*last-name*

例：

```
firepower-2110 /security/local-user* # set lastname Crichton
```

ステップ 7　（任意）ユーザ アカウントが期限切れになる日付を指定します。

set expiration　*month*　*day-of-month*　*year*

- *month*：月を英語の月名の先頭 3 文字で設定します。

アカウントは、指定された日付の後には使用できません。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、使用できる最新の有効期限日付でアカウントを設定することは可能です。

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。

例：

```
firepower-2110 /security/local-user* # set expiration oct 10 2019
```

ステップ 8　（任意）ユーザの電子メール アドレスを指定します。

set email　*email-addr*

例：

```
firepower-2110 /security/local-user* # set email jcrichton@example.com
```

ステップ 9 （任意）ユーザの電話番号を指定します。

set phone *phone-num*

例：

```
firepower-2110 /security/local-user* # set phone 303-555-7891
```

ステップ 10 （任意）ユーザに管理者ロールを割り当てます。

enter role admin

すべてのユーザにはデフォルトで **read-only** ロールが割り当てられ、このロールは削除できません。**admin** ロールにより、設定への読み取りと書き込みのアクセスが許可されます。

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。

例：

```
firepower-2110 /security/local-user* # enter role admin
```

ステップ 11 設定を保存します。

commit-buffer

例：

```
firepower-2110 security/local-user* # commit-buffer
firepower-2110 security/local-user #
```

例

次の例は、aerynsun という名前のユーザアカウントを作成し、ユーザアカウントを有効にし、rygel にパスワードを設定し、管理者ユーザロールを割り当て、トランザクションを確定します。

```
firepower-2110# scope security
firepower-2110 /security # create local-user aerynsun
firepower-2110 /security/local-user* # set password
Enter a password: rygel
Confirm the password: rygel
firepower-2110 /security/local-user* # enter role admin
firepower-2110 /security/local-user* # commit-buffer
firepower-2110 /security/local-user #
```

ユーザ設定値の設定

すべてのユーザのグローバル設定値を設定できます。

手順

ステップ 1 セキュリティ モードに入ります。

scope security

例：

```
firepower-2110# scope security
firepower-2110 /security #
```

ステップ 2 パスワード強度チェックを有効または無効にします。

set enforce-strong-password {yes | no}

パスワードの強度チェックが有効になっている場合、Firepower 2100 では、強力なパスワードのガイドラインを満たしていないパスワードを選択できません（ユーザアカウントに関するガイドライン（61 ページ）を参照）。デフォルトでは、強力なパスワードチェックが有効になっています。

例：

```
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* #
```

ステップ 3 パスワード プロファイル モードを開始します。

scope password-profile

例：

```
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* #
```

ステップ 4 最小パスワード長を設定します。

set min-password-length *min_length*

最小パスワード長チェックを有効にした場合は、指定した最小文字数のパスワードを作成する必要があります。

例：

```
firepower-2110 /security/password-profile* # set min-password-length 8
```

ステップ 5 ローカル認証されたユーザが指定された時間内にパスワードを変更できるかどうかを有効または無効にします。

変更を許可します。

set change-interval *num-of-hours*

set change-count *pass-change-num*

- *num_of_hours*：パスワード変更の回数が適用される時間数を 1 ～ 745 時間の間で設定します。
- *pass_change_num*：ローカル認証されたユーザが、変更間隔の間に自分のパスワードを変更できる最大回数を設定します。

変更を禁止するには、**set change-interval** を **disabled** に設定します。

例：

```
firepower-2110 /security/password-profile* # set change-count 2
firepower-2110 /security/password-profile* # set change-interval 24
```

変更を禁止します。

set no-change-interval *min_num_hours* }

- *min_num_hours*：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必要がある最小時間数を 1 ～ 745 時間の間で設定します。

変更を許可するには、**set no-change-interval** を **disabled** に設定します。

例：

```
firepower-2110 /security/password-profile* # set no-change-interval 1
```

ステップ 6 パスワード再利用の要件を設定します。

set history-count {*num_of_passwords* | **disabled**}

set password-reuse-interval {*days* | **disabled**}

- *num_of_passwords*：ローカル認証されたユーザが、以前に使用していたパスワードを再利用できるまでに作成する必要がある一意のパスワードの数を 0 ～ 15 の間で指定します。デフォルトでは、最小数は 0 で、履歴カウントが無効になり、ユーザは以前に使用していたパスワードを再利用できます。
- *days*：パスワードの再利用が可能になるまでの日数を 1 ～ 365 の間で設定します。デフォルトは 15 日です。

両方のコマンドを有効にする場合は、両方の要件を満たす必要があります。たとえば、履歴カウントを 3 に設定し、再利用間隔を 10 日に設定すると、パスワードを変更できるのは 10 日間経過した後で、パスワードを 3 回変更した場合に限られます。

例：

```
firepower-2110 /security/password-profile* # set history-count 5
```

```
firepower-2110 /security/password-profile* # set password-reuse-interval 120
```

ステップ 7 パスワード有効期限の設定を行います。

set password-expiration {*days* | **never**}

set expiration-warning-period *days*

set expiration-grace-period *days*

- **set password-expiration** {*days* | **never**}：有効期限を 1 ～ 9999 日の間で設定します。デフォルトでは、有効期限は無効になっています（**never**）。
- **set expiration-warning-period** *days*：ログインごとに有効期限の何日前にパスワードの有効期限をユーザに警告するかを 0 ～ 9999 の間で設定します。デフォルトは、14 日です。
- **set expiration-grace-period** *days*：有効期限の何日後までにユーザがパスワードを変更する必要があるかを 0 ~ 9999 の間で設定します。デフォルトは 3 日です。

例：

```
firepower-2110 /security/password-profile* # set password-expiration 120
firepower-2110 /security/password-profile* # set expiration-warning-period 5
firepower-2110 /security/password-profile* # set expiration-grace-period 5
```

ステップ 8 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する絶対セッションタイムアウトを設定します。

scope default-auth

set absolute-session-timeout *seconds*

- *seconds*：絶対タイムアウト値を 0 ～ 7200 秒の間で設定します。デフォルト値は 3600 秒（60 分）です。この設定を無効にするには、値を 0 に設定します。

例：

```
firepower-2110 /security* scope default-auth#
firepower-2110 /security/default-auth* # set absolute-session-timeout 7200
```

ステップ 9 設定を保存します。

commit-buffer

例：

```
firepower-2110 /security/default-auth* # commit-buffer
firepower-2110 /security/default-auth #
```

例

次に、多数のユーザ要件を設定する例を示します。

```
firepower-2110 # scope security
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* # set change-during-interval enable
firepower-2110 /security/password-profile* # set change-count 5
firepower-2110 /security/password-profile* # set change-interval 72
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # commit-buffer
firepower-2110 /security/password-profile #
```

システム管理

ASA パッケージのアップグレード、シャーシのリロード、または電源オフを行うことができます。

イメージのアップグレード

この作業はスタンドアロン ASA に適用されます。フェールオーバー ペアをアップグレードする場合は、『Cisco ASA Upgrade Guide』を参照してください。アップグレード プロセスには通常 20 ～ 30 分かかります。

ASA、ASDM、および FXOS のイメージは 1 つのパッケージにバンドルされています。パッケージのアップデートは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。

ASDM の場合は例外です。ASA オペレーティング システム内からアップグレードできるため、必ずしもバンドルされた ASDM イメージを使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージ リストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが前の ASDM バンドル イメージを置き換えます。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

始める前に

アップロードするイメージが FTP、SCP、SFTP、TFTP サーバ、または USB ドライブで使用可能であることを確認します。

手順

ステップ 1 コンソール ポート（推奨）または SSH を使用して、FXOS CLI に接続します。コンソール ポートで接続する場合は、FXOS CLI にすぐにアクセスします。FXOS ログイン クレデンシャルを入力します。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

SSH を使用して ASA 管理 IP アドレスに接続する場合は、FXOS にアクセスするために **connect fxos** と入力します。

ステップ 2 シャーシにパッケージをダウンロードします。

a) ファームウェア モードを入力します。

scope firmware

例：

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) パッケージをダウンロードします。

download image *url*

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

例：

```
firepower-2110 /firmware # download image
tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
 download progress.
```

c) ダウンロード プロセスをモニタします。

show download-task

例：

```
firepower-2110 /firmware # show download
```

```
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

ステップ 3 新しいパッケージのダウンロードが終了（[Downloaded] の状態）したら、パッケージを起動します。

a) 新しいパッケージのバージョン番号を表示します。

show package

例：

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
firepower-2110 /firmware #
```

b) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA パッケージをインストールして再起動します。

例：

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.2.2

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.2.2, it will do the following:
   - upgrade to the CSP asa version 9.8.2.2

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

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be
lost,
   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 9.8.2.2
```

```
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

（注） 「すべての既存の構成が失われ、デフォルト設定が適用されます」のメッセージは無視します。構成が消去されることはなく、デフォルト設定が適用されることもありません。デフォルト設定は、アップグレードではなく、再イメージ化の間にのみ適用されます。

ステップ 4 シャーシのリブートが完了するのを待ちます（5 ～ 10 分）。FXOS が最初に起動しますが、ASA が起動するまで待つ必要があります。

ASA の起動後、アプリケーションに接続したら、CLI でユーザ EXEC モードにアクセスします。

例：

```
 [...]
Cisco FPR Series Security Appliance
firepower-2140 login: admin
Password:

Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2018, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2140# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

シャーシのリブート

手順

ステップ 1 シャーシモードを開始します。

scope chassis 1

例：

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

ステップ 2 シャーシをリブートします。

reboot [**"***reason***"**] [**no-prompt**]

no-prompt キーワードを使用した場合、コマンドを入力するとシャーシはすぐにリブートします。そうしないと、**commit-buffer** コマンドを入力するまでシャーシは再起動しません。

例：

```
firepower-2110 /chassis # reboot "This system is rebooting" no-prompt
```

ステップ 3 リブートプロセスをモニタします。

show fsm status

シャーシの電源オフ

シャーシは、Firepower 2100 シャーシの電源をオフにする前に、ASA OS を正常にシャットダウンします。このプロセスには約 15 ～ 20 分かかります。シャーシの電源が正常にオフになれば、シャーシの電源コードを物理的に抜くことができます。

手順

ステップ 1 シャーシモードを開始します。

scope chassis 1

例：

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

ステップ 2 シャーシの電源を切ります。

shutdown [**"***reason***"**] [**no-prompt**]

no-prompt キーワードを使用した場合、コマンドを入力するとシャーシはすぐにシャットダウンします。そうしないと、**commit-buffer** コマンドを入力するまでシャーシはシャットダウンしません。

例：

```
firepower-2110 /chassis # shutdown "This system is powering off" no-prompt
```

ステップ 3 シャットダウンプロセスをモニタします。

show fsm status

FXOS 管理 IP アドレスまたはゲートウェイの変更

FXOS CLI から Firepower 2100 シャーシの FXOS 管理 IP アドレスを変更できます。デフォルトのアドレスは 192.168.45.45 です。FXOS 管理トラフィックのデフォルトゲートウェイを変更することもできます。デフォルトゲートウェイは 0.0.0.0 に設定されており、FXOS トラフィックはバックプレーン経由で送信され、ASA データインターフェイスを介してルーティングされます。代わりに管理 1/1 ネットワークでルータにトラフィックをルーティングする場合、ゲートウェイ IP アドレスを変更します。管理接続のアクセス リストを新しいネットワークに一致するように変更する必要もあります。ゲートウェイをデフォルトの 0.0.0.0（ASA データインターフェイス）から変更すると、データインターフェイスで FXOS にアクセスできなくなり、FXOS はデータインターフェイスでトラフィックを開始できなくなります。データインターフェイスでの FXOS アクセスについては、スタートアップガイドを参照してください。

通常、FXOS 管理 1/1 IP アドレスは ASA 管理 1/1 IP アドレスと同じネットワーク上にあります。そのため、この手順では ASA の ASA IP アドレスを変更する方法も示します。

始める前に

- 管理 IP アドレスを変更した後で、新しいアドレスを使用して Firepower Chassis Manager および SSH 接続を再確立する必要があります。
- DHCP サーバはデフォルトでは管理 1/1 で有効になっているため、管理 IP アドレスを変更する前に DHCP を無効にする必要があります。

手順

ステップ 1 コンソール ポートに接続します（ASA または FXOS のコンソールへの接続 （2 ページ）を参照）。接続が失われないようにするために、コンソールに接続することをお勧めします。

ステップ 2 DHCP サーバを無効にします。

scope system

scope services

disable dhcp-server

commit-buffer

管理 IP アドレスを変更した後で、新しいクライアント IP アドレスを使用して DHCP を再び有効にすることができます。Firepower Chassis Manager で DHCP サーバを有効および無効にすることもできます（**[Platform Settings]** > **[DHCP]**）。

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

```
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

ステップ 3 IPv4 管理 IP アドレス、および必要に応じてゲートウェイを設定します。

a) fabric-interconnect a のスコープを設定します。

scope fabric-interconnect a

例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) 現在の管理 IP アドレスを表示します。

show

例：

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6
Gateway Prefix Operability
    ---- --------------- --------------- --------------- -----------------
---------------- ------ -----------
    A    192.168.45.45    0.0.0.0         0.0.0.0          ::               ::
         64     Operable
```

c) 新しい管理 IP アドレス、および必要に応じて新しいデフォルト ゲートウェイを設定します。

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

現在設定されているゲートウェイを維持するには、**gw** キーワードを省略します。同様に、既存の管理 IP アドレスを維持したままゲートウェイを変更するには、**ip** キーワードと **netmask** キーワードを省略します。

ゲートウェイを ASA データインターフェイスに設定するには、 **gw** を 0.0.0.0 に設定します。これがデフォルトの設定です。

例：

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
 255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

ステップ 4 IPv6 管理 IP アドレスとゲートウェイを設定します。

a) fabric-interconnect a のスコープ、次に IPv6 設定のスコープを設定します。

scope fabric-interconnect a

scope ipv6-config

例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) 現在の管理 IPv6 アドレスを表示します。

show ipv6-if

例：

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                      Prefix     IPv6 Gateway
    --------------------------------- ---------- ------------
    ::                                ::         ::
```

c) 新しい管理 IPv6 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 static ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

現在設定されているゲートウェイを維持するには、**ipv6-gw** キーワードを省略します。同様に、既存の管理 IP アドレスを維持したままゲートウェイを変更するには、**ipv6** キーワードと **ipv6-prefix** キーワードを省略します。

ゲートウェイを ASA データインターフェイスに設定するには、**gw** を :: に設定します。これがデフォルトの設定です。

例：

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6
2001:DB8::34 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

ステップ 5 HTTPS、SSH、および SNMP のアクセス リストを削除して新しいアクセス リストを追加し、新しいネットワークからの管理接続を可能にします。

a) システム/サービスの範囲を設定します。

scope system

scope services

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) 現在のアクセス リストを表示します。

show ip-block

例：

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) 新しいアクセス リストを追加します。

IPv4 の場合：

enter ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6 の場合：

enter ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

IPv4 の場合、すべてのネットワークを許可するには **0.0.0.0** とプレフィックス **0** を入力します。IPv6 の場合、すべてのネットワークを許可するには **::** とプレフィックス **0** を入力します。Firepower Chassis Manager でアクセス リストを追加することもできます（**[Platform Settings]** > **[Access List]**）。

例：

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) 古いアクセス リストを削除します。

IPv4 の場合：

delete ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6 の場合：

delete ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

例：

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

ステップ 6 （任意） IPv4 DHCP サーバを再び有効にします。

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

Firepower Chassis Manager で DHCP サーバを有効および無効にすることもできます（**[Platform Settings]** > **[DHCP]**）。

例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

ステップ 7 設定を保存します。

commit-buffer

例：

```
firepower-2110 /system/services* # commit-buffer
```

ステップ 8 ASAアドレスを、正しいネットワーク上となるように変更します。デフォルトのASA管理1/1インターフェイス IP アドレスは 192.168.45.1 です。

a) コンソールから、ASA CLI に接続して、グローバル コンフィギュレーション モードにアクセスします。

connect asa

enable

configure terminal

例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

b) 管理 1/1 IP アドレスを変更します。

interface management1/1

ip address *ip_address mask*

例：

```
ciscoasa(config)# interface management1/1
```

```
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) ASDM にアクセス可能なネットワークに変更します。

no http 192.168.45.0 255.255.255.0 management

http *ip_address mask* **management**

例：

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) 設定を保存します。

write memory

e) FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

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-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
     64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /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-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    2001:DB8::2                          64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

FXOS CLI 設定の履歴

機能	バージョン	詳細
設定可能な HTTPS プロトコル	9.13(1)	HTTPS アクセス用の SSL/TLS のバージョンを設定できます。 新規/変更されたコマンド： **set https access-protocols**
IPSec およびキーリングの FQDN の適用	9.13(1)	ピアの FQDN がそのピアによって提示された x.509 証明書の DNS 名と一致する必要があるように、FQDN の適用を設定できます。IPSec の場合、9.13(1) より前に作成された接続を除き、適用はデフォルトで有効になっています。古い接続への適用は手動で有効にする必要があります。キーリングの場合、すべてのホスト名が FQDN である必要があり、ワイルドカードは使用できません。 新規/変更されたコマンド：**set dns**、**set e-mail**、**set fqdn-enforce**、**set ip**、**set ipv6**、**set remote-address**、**set remote-ike-id** 削除されたコマンド：**fi-a-ip**、**fi-a-ipv6**、**fi-b-ip**、**fi-b-ipv6**

機能	バージョン	詳細
新しい IPSec 暗号とアルゴリズム	9.13(1)	次の IKE および ESP 暗号とアルゴリズムが追加されました（設定不可）。 • 暗号：aes192。既存の暗号には、aes128、aes256、aes128gcm16 などがあります。 • 疑似乱数関数（PRF）（IKE のみ）：prfsha384、prfsha512、prfsha256。既存の PRF：prfsha1。 • 整合性アルゴリズム：sha256、sha384、sha512、sha1_160。既存のアルゴリズム：sha1。 • Diffie-Hellman グループ：curve25519、ecp256、ecp384、ecp521、modp3072、modp4096。既存のグループ：modp2048。
SSH 認証の機能拡張	9.13(1)	次の SSH サーバ暗号化アルゴリズムが追加されました。 • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com 次の SSH サーバ キー交換方式が追加されました。 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 新規/変更されたコマンド：**set ssh-server encrypt-algorithm**、**set ssh-server kex-algorithm**

機能	バージョン	詳細
X.509 証明書の EDCS キー	9.13(1)	証明書に EDCS キーを使用できるようになりました。以前は、RSA キーだけがサポートされていました。 新規/変更されたコマンド：**set elliptic-curve**、**set keypair-type**
ユーザパスワードの改善	9.13(1)	次のようなパスワードセキュリティの改善が追加されました。 • ユーザ パスワードには最大 127 文字を使用できます。古い制限は 80 文字でした。 • デフォルトでは、強力なパスワード チェックが有効になっています。 • 管理者パスワードの設定を求めるプロンプトが表示されます。 • パスワードの有効期限切れ。 • パスワード再利用の制限。 • **set change-during-interval** コマンドを削除し、**set change-interval**、**set no-change-interval**、および **set history-count** コマンドの **disabled** オプションを追加しました。 新規/変更されたコマンド：**set change-during-interval**、**set expiration-grace-period**、**set expiration-warning-period**、**set history-count**、**set no-change-interval**、**set password**、**set password-expiration**、**set password-reuse-interval**
set lacp-mode コマンドが **set port-channel-mode** に変更されました。	9.10(1)	**set lacp-mode** コマンドは、Firepower 4100/9300 でのコマンドの使用方法に合わせるために **set port-channel-mode** に変更されています。 新規/変更されたコマンド： **set port-channel-mode**

機能	バージョン	詳細
Firepower 2100 の NTP 認証のサポート	9.10(1)	FXOS で SHA1 NTP サーバ認証を設定できるようになりました。 新規/変更された FXOS コマンド：**enable ntp-authentication**、**set ntp-sha1-key-id**、**set ntp-sha1-key-string**