プラットフォーム設定

日時の設定

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

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

（注） Firepower 4100/9300 シャーシに Firepower Threat Defense を導入すると、スマート ライセンスが正しく機能し、デバイス登録に適切なタイムスタンプを確保するように Firepower 4100/9300 シャーシに NTP を設定する必要があります。Firepower 4100/9300 シャーシ と Firepower Management Center の両方で同じ NTP サーバを使用する必要がありますが、Firepower Management Center は Firepower 4100/9300 シャーシ の NTP サーバとして使用できないので注意してください。

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

設定された日付と時刻の表示

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [Current Time] タブをクリックします。

システムは、デバイスに設定された日付、時刻、タイム ゾーンを表示します。

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

タイム ゾーンの設定

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [Current Time] タブをクリックします。

ステップ 3 Firepower シャーシに適切なタイムゾーンを [タイムゾーン（Time Zone）] ドロップダウン リストから選択します。

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。 最大 4 台の NTP サーバを設定できます。

（注）

- FXOS では、NTP バージョン 3 を使用します。
- 外部 NTP サーバのストラタム値が 13 以上の場合、アプリケーションインスタンスは FXOS シャーシ上の NTP サーバと同期できません。NTP クライアントが NTP サーバと同期するたびに、ストラタム値が 1 ずつ増加します。

  独自の NTP サーバをセットアップしている場合は、サーバ上の /etc/ntp.conf ファイルでそのストラタム値を確認できます。NTP サーバのストラタム値が 13 以上の場合は、ntp.conf ファイルのストラタム値を変更してサーバを再起動するか、別の NTP サーバ（たとえば、pool.ntp.org）を使用することができます。

始める前に

NTP サーバのホスト名を使用する場合は、DNS サーバを設定する必要があります。DNS サーバの設定 （48 ページ）を参照してください。

手順

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

[Time Synchronization] タブがデフォルトで選択されています。

ステップ 2 [Set Time Source] で、[Use NTP Server] をクリックします。

ステップ 3 （任意） NTP サーバで認証が必要な場合は、[NTP Server Authentication: Enable] チェックボックスをオンにします。

認証キー ID と値が必要な場合は、[Yes] をクリックします。

NTP サーバ認証では SHA1 のみがサポートされます。

ステップ 4 [Add] をクリックして、IP アドレスまたはホスト名で最大 4 つの NTP サーバを識別します。

ステップ 5 （任意） NTP サーバの [Authentication Key] ID と [Authentication Value] を入力します。

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。

ステップ 6 **[保存（Save）]** をクリックします。

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

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

NTP サーバの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

ステップ 2 [時刻同期（Time Synchronization）] タブをクリックします。

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

ステップ 4 [Save] をクリックします。

日付と時刻の手動での設定

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

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

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

ステップ 3 [時刻源の設定（Set Time Source）] で、[時刻を手動で設定（Set Time Manually）] をクリックします。

ステップ 4 [日付（Date）] ドロップダウンリストをクリックしてカレンダーを表示し、そのカレンダーで使用可能なコントロールを使用して日付を設定します。

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

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

ステップ 6 [保存（Save）] をクリックします。

Firepower シャーシが指定した日付と時刻で設定されます。

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

Configuring SSH

次の手順では、Firepower シャーシへの SSH アクセスを有効または無効にする方法、FXOS シャーシを SSH クライアントとして有効にする方法、さらに SSH で使用する暗号化、キー交換、およびメッセージ認証用のさまざまなアルゴリズムを SSH サーバと SSH クライアントに設定する方法について説明します。

SSH はデフォルトでイネーブルになります。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [SSH] > [SSH サーバ（SSH Server）]** の順に選択します。

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

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

（注）
- 次の暗号化アルゴリズムは、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。
  - 3des-cbc
  - chacha20-poly1305@openssh.com
- chacha20-poly1305@openssh.com は FIPS ではサポートされていません。FXOS シャーシで FIPS モードが有効になっている場合、chacha20-poly1305@openssh.com を暗号化アルゴリズムとして使用することはできません。
- 次の暗号化アルゴリズムは、デフォルトでは有効になっていません。

```
aes128-cbc
aes192-cbc
aes265-cbc
```

ステップ 4 サーバの [Key Exchange Algorithm] として、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認

証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

（注）
- 次のキー交換アルゴリズムは、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。
  - diffie-hellman-group14-sha256
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- FIPS モードでは、次のキー交換アルゴリズムはサポートされていません。
  - curve25519-sha256
  - curve25519-sha256@libssh.org

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

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

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

ステップ 7 サーバの [キー再生成のボリューム制限（Volume Rekey Limit）] に、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 8 サーバの [キー再生成の時間制限（Time Rekey Limit）] では、FXOS がセッションを切断する前に SSH セッションがアイドル状態を続けられる長さを分単位で設定します。

ステップ 9 [Save]をクリックします。

ステップ 10 [SSH クライアント（SSH Client）] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。

ステップ 11 [厳密なホスト キー検査（Strict Host Keycheck）] について、[有効（enable）]、[無効（disable）]、または [プロンプト（prompt）] を選択して、SSH ホスト キー チェックを制御します。

- [enable]：FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。 FXOS CLI でシステム スコープまたはサービス スコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
- [プロンプト（prompt）]：シャーシにまだ保存されていないホストキーを許可または拒否するように求められます。
- **disable**：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

ステップ 12 クライアントの [暗号化アルゴリズム（Encryption Algorithm）] として、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

（注）
- 次の暗号化アルゴリズムは、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。
  - 3des-cbc
  - chacha20-poly1305@openssh.com

  FXOS シャーシでコモン クライテリア モードが有効な場合、暗号化アルゴリズムとして 3des-cbc を使用することはできません。
- chacha20-poly1305@openssh.com は FIPS ではサポートされていません。FXOS シャーシで FIPS モードが有効になっている場合、chacha20-poly1305@openssh.com を暗号化アルゴリズムとして使用することはできません。
- 次の暗号化アルゴリズムは、デフォルトでは有効になっていません。

```
aes128-cbc
aes192-cbc
aes265-cbc
```

ステップ 13 クライアントの [キー交換アルゴリズム（Key Exchange Algorithm）] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

（注）
- 次のキー交換アルゴリズムは、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。
  - diffie-hellman-group14-sha256
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- FIPS モードでは、次のキー交換アルゴリズムはサポートされていません。
  - curve25519-sha256
  - curve25519-sha256@libssh.org

ステップ 14 クライアントの [Mac アルゴリズム（Mac Algorithm）] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 15 クライアントの [キー再生成のボリューム制限（Volume Rekey Limit）] について、FXOS がセッションを切断する前にその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 16 クライアントの [キー再生成の時間制限（Time Rekey Limit）] について、FXOS がセッションを切断する前に SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 17 [Save] をクリックします。

TLS の設定

Transport Layer Security（TLS）プロトコルは、互いに通信する 2 つのアプリケーションの間でプライバシーとデータの整合性を確保します。FXOS シャーシと外部デバイスとの通信で許容する最小 TLS バージョンは、FXOS CLI を使用して設定できます。新しいバージョンの TLS では通信のセキュリティを強化できる一方、古いバージョンの TLS では古いアプリケーションとの後方互換性を維持できます。

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

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

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

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

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

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

例：

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

ステップ 3 最小 TLS バージョンを設定します。

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

例：

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

ステップ 4 設定をコミットします。

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

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

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

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

例：

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

Telnet の設定

次の手順は、Firepower シャーシへの Telnet アクセスを有効または無効にする方法を示しています。デフォルトでは、Telnet はディセーブルになっています。

（注） 現在、Telnet は CLI を使用してのみ設定できます。

手順

ステップ 1 システム モードに入ります。

Firepower-chassis # **scope system**

ステップ 2 システム サービス モードを開始します。

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

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

- Firepower シャーシへの Telnet アクセスを許可するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **enable telnet-server**

- Firepower シャーシへの Telnet アクセスを拒否するには、次のコマンドを入力します。

  Firepower-chassis /system/services # **disable telnet-server**

ステップ 4 トランザクションをシステム設定にコミットします。

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

例

次に、Telnet を有効にし、トランザクションを確定する例を示します。

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

SNMP の設定

Firepower シャーシに Simple Network Management Protocol（SNMP）を設定するには、[SNMP] ページを使用します。詳細については、次のトピックを参照してください。

SNMP の概要

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

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：Firepower 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。SNMP エージェントを有効にし、

マネージャとエージェント間のリレーションシップを作成するには、Firepower Chassis Manager または FXOS CLI で SNMP を有効にし、設定します。

- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

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

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

（注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。

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。

ただし、インフォームは SNMPv2c でのみ使用可能ですが、安全ではないと考えられているため、推奨されません。

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 *1: 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。

モデル	水準器	認証	暗号化	結果
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。 （注） 設定することはできますが、FXOS では SNMP バージョン 3 で `noAuthNoPriv` を使用することはできません。
v3	authNoPriv	HMAC-SHA	なし	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

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

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

SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

MIB のサポート

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

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

SNMPv3 ユーザの認証プロトコル

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

SNMPv3 ユーザの AES プライバシー プロトコル

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

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

SNMP の有効化および SNMP プロパティの設定

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[管理状態（Admin State）] チェックボックス	SNMP を有効にするかまたは無効にするか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスを有効にします。
[ポート（Port）] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。

名前	説明
[Community/Username] フィールド	（任意）SNMP v1 および v2 のポーリングに使用するコミュニティストリング。 SNMP コミュニティ名を指定すると、SNMP リモートマネージャからのポーリング要求に対して SNMP バージョン 1 および 2c も自動的に有効になります。このフィールドは SNMP v3 には適用されません。 SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。コミュニティ ストリングは、これらのバージョンで唯一の認証形式として機能します。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは **public** です。 [Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ります。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。 （注） CLI コマンド **set snmp community** を使用して既存のコミュニティ ストリングを削除することで、SNMP リモートマネージャからのポーリング要求に対して SNMP バージョン 1 および 2c を無効にすることができます。
[System Administrator Name] フィールド	SNMP の実装担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location]フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

次の手順では、SNMP トラップを作成する方法について説明します。

（注） 最大 8 つの SNMP トラップを定義できます。

手順

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

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

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

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[Community/Username] フィールド	トラップの宛先へのアクセスを許可するために必要な SNMPv1/v2c コミュニティストリングまたは SNMPv3 ユーザ名を入力します。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	Firepower シャーシがトラップのために SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。

名前	説明
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **V1** • **[V2]** • **V3** （注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。
[Type] フィールド	送信するトラップのタイプを指定します。 • **[Traps]** • [Informs]（[Version] が**V2**の場合にのみ有効）
[v3 Privilege] フィールド	バージョンで**V3** を選択した場合は、トラップに関連付ける権限を指定します。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし これを選択することはできますが、FXOS は SNMPv3 でこのセキュリティレベルをサポートしていないことに注意してください。 • [Priv]：認証あり、暗号化あり

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

ステップ 5 [保存（Save）] をクリックします。

SNMP トラップの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

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

SNMPv3 ユーザの作成

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

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

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

名前	説明
[Name] フィールド	SNMPv3 ユーザに割り当てられているユーザ名。 32 文字まで入力します。名前の先頭は文字である必要があります。有効な文字は、文字、数字、_（アンダースコア）です。.（ピリオド）、@（アットマーク）、-（ハイフン）も指定できます。
[Auth Type] フィールド	許可タイプ：**SHA**。
[AES-128 の使用（Use AES-128）] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。

名前	説明
[Password] フィールド	このユーザのパスワード。 Firepower eXtensible Operating System では、次の要件を満たさないパスワードは拒否されます。 • 8 ～ 80 文字を含む。 • 含められるのは、文字、数字、および次の文字のみです。 ~`!@#%^&*()_-+{}[]\\:;"'<,>./ • 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。 • 5 つ以上の異なる文字を含める必要があります。 • 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。 （注） 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[プライバシー パスワード（Privacy Password）] フィールド	このユーザのプライバシー パスワード。 Firepower eXtensible Operating System では、次の要件を満たさないパスワードは拒否されます。 • 8 ～ 80 文字を含む。 • 含められるのは、文字、数字、および次の文字のみです。 ~`!@#%^&*()_-+{}[]\\:;"'<,>./ • 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。 • 5 つ以上の異なる文字を含める必要があります。 • 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は4つ、「ZYXW」は3つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。 （注） 連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

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

ステップ 5 [保存（Save）] をクリックします。

SNMPv3 ユーザの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[SNMP]** を選択します。

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

HTTPS の設定

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

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

証明書、キー リング、トラスト ポイント

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

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 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。

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

証明書

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

トラスト ポイント

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

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

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

キー リングの作成

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

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングを作成し、名前を付けます。

Firepower-chassis # **create keyring** *keyring-name*

ステップ 3 SSL キーのビット長を設定します。

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

ステップ 4 トランザクションをコミットします。

Firepower-chassis # **commit-buffer**

例

次の例は、1024 ビットのキー サイズのキー リングを作成します。

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

次のタスク

このキー リングの証明書要求を作成します。

デフォルト キー リングの再生成

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

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

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

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

ステップ 3 デフォルト キー リングを再生成します。

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

ステップ 4 トランザクションをコミットします。

Firepower-chassis # **commit-buffer**

例

次に、デフォルト キー リングを再生成する例を示します。

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

キー リングの証明書要求の作成

基本オプション付きのキー リングの証明書要求の作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングのコンフィギュレーション モードに入ります。

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

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

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

ステップ 4 トランザクションをコミットします。

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

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

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

例

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

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name
sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

次のタスク

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

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

詳細オプション付きのキー リングの証明書要求の作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 キー リングのコンフィギュレーション モードに入ります。

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

ステップ 3 証明書要求を作成します。

Firepower-chassis /security/keyring # **create certreq**

ステップ 4 会社が存在している国の国コードを指定します。

Firepower-chassis /security/keyring/certreq* # **set country** *country name*

ステップ 5 要求に関連付けられたドメイン ネーム サーバ（DNS）アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set dns** *DNS Name*

ステップ 6 証明書要求に関連付けられた電子メール アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set e-mail** *E-mail name*

ステップ 7 Firepower 4100/9300 シャーシの IP アドレスを指定します。

Firepower-chassis /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }

ステップ 8 証明書を要求している会社の本社が存在する市または町を指定します。

Firepower-chassis /security/keyring/certreq* # **set locality** *locality name (eg, city)*

ステップ 9 証明書を要求している組織を指定します。

Firepower-chassis /security/keyring/certreq* # **set org-name** *organization name*

ステップ 10 組織ユニットを指定します。

Firepower-chassis /security/keyring/certreq* # **set org-unit-name** *organizational unit name*

ステップ 11 証明書要求に関するオプションのパスワードを指定します。

Firepower-chassis /security/keyring/certreq* # **set password** *certificate request password*

ステップ 12 証明書を要求している会社の本社が存在する州または行政区分を指定します。

Firepower-chassis /security/keyring/certreq* # **set state** *state, province or county*

ステップ 13 Firepower 4100/9300 シャーシ の完全修飾ドメイン名を指定します。

Firepower-chassis /security/keyring/certreq* # **set subject-name** *certificate request name*

ステップ 14 トランザクションをコミットします。

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

ステップ 15 コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

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

例

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

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* #  set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

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

次のタスク

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

トラスト ポイントの作成

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 トラストポイントを作成します。

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

ステップ 3 このトラスト ポイントの証明書情報を指定します。

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

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

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

ステップ 4 トランザクションをコミットします。

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

例

次の例は、トラスト ポイントを作成し、トラスト ポイントに証明書を提供します。

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

次のタスク

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

キー リングへの証明書のインポート

始める前に

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

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

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

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

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

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

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

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

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

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

ステップ 5 トランザクションをコミットします。

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

例

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

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

次のタスク

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

⚠

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

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システム サービス モードを開始します。

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

ステップ 3 HTTPS サービスを有効にします。

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

ステップ 4 （任意） HTTPS 接続で使用されるポートを指定します。

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

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

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

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

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

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

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

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

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

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

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

ステップ 8 （任意） 証明書失効リスト検査を、有効または無効にします。

set revoke-policy *{ relaxed | strict }*

ステップ 9 トランザクションをシステム設定にコミットします。

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

例

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

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

HTTPS ポートの変更

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

手順

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

ステップ 2 HTTPS 接続に使用するポートを [Port] フィールドに入力します。1 ～ 65535 の範囲内の整数を指定します。このサービスは、デフォルトではポート 443 で有効になっています。

ステップ 3 [Save] をクリックします。

Firepower シャーシが指定した HTTPS ポートで設定されます。

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

https://*<chassis_mgmt_ip_address>*:*<chassis_mgmt_port>*

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

キーリングの削除

手順

ステップ 1 セキュリティ モードを開始します。

Firepower-chassis # **scope security**

ステップ 2 名前付きのキー リングを削除します。

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

ステップ 3 トランザクションをコミットします。

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

例

次の例では、キー リングを削除します。

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

トラスト ポイントの削除

始める前に

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

手順

ステップ 1 セキュリティ モードに入ります。

Firepower-chassis# **scope security**

ステップ 2 指定したトラスト ポイントを削除します。

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

ステップ 3 トランザクションをコミットします。

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

例

次に、トラスト ポイントを削除する例を示します。

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

HTTPS の無効化

手順

ステップ 1 システム モードに入ります。

Firepower-chassis# **scope system**

ステップ 2 システム サービス モードを開始します。

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

ステップ 3 HTTPS サービスを無効にします。

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

ステップ 4 トランザクションをシステム設定にコミットします。

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

例

次に、HTTPS を無効にし、トランザクションをコミットする例を示します。

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

AAA の設定

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

AAA について

認証、許可、およびアカウンティング（AAA）は、ネットワークリソースへのアクセス制御、ポリシーの強化、使用状況の評価、およびサービスの課金に必要な情報提供を行う一連のサービスです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実装します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

認証

認証はユーザを識別する方法です。通常、ユーザが有効なユーザ名と有効なパスワードを入力すると、アクセスが許可されます。AAA サーバは、ユーザが入力したログイン情報とデータベースに保存されているユーザのログイン情報を比較します。ログイン情報が一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

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

- HTTPS
- SSH
- シリアル コンソール

認可

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

アカウンティング

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

認証、認可、アカウンティング間の相互作用

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

サポートされている認証タイプ

FXOS は次の認証タイプをサポートします。

- [Remote]：次のネットワーク AAA サービスがサポートされています。
  - LDAP
  - RADIUS
  - TACACS+
- [Local]：Firepowerシャーシは、ユーザプロファイルを取り込むことができるローカルデータベースを維持します。 AAAサーバの代わりに、このローカルデータベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

ユーザ ロール

FXOS は、ユーザロール割り当ての形式でローカルおよびリモート認証をサポートします。割り当てることができるロールは次のとおりです。

- [Admin]：システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。
- [AAA Administrator]：ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- [Operations]：NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- [Read-Only]：システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

ローカルユーザとロールの割り当ての詳細については、「ユーザ管理」を参照してください。

AAA の設定

Firepower 4100/9300 アプライアンスで認証、許可、アカウンティング（AAA）を設定するための基本的な手順の概要を紹介します。

1. ユーザ認証の目的タイプを設定します。
   - [Local]：ユーザ定義とローカル認証は ユーザ管理 の一部です。
   - [Remote]：リモート AAA サーバ アクセスの設定は、[Platform Settings] の一部です。具体的には次のとおりです。
     - LDAP プロバイダーの設定 （36 ページ）
     - RADIUS プロバイダーの設定 （40 ページ）
     - TACACS+ プロバイダーの設定 （42 ページ）

   （注） リモート AAA サーバを使用する場合は、Firepower シャーシでリモート AAA サーバアクセスを設定する前に、リモートサーバで AAA サービスを有効にして設定する必要があります。

2. デフォルトの認証方式を指定します。これも ユーザ管理 の一部です。

（注） デフォルトの認証とコンソール認証の両方が同じリモート認証プロトコル（RADIUS、TACACS+、または LDAP）を使用するように設定されている場合、そのサーバの設定の特定の側面を変更することは（たとえば、サーバの削除や、割り当ての順序の変更）、これらのユーザ設定を更新することなしではできません。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

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

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

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

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

名前	説明
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 30 秒です。このプロパティは必須です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性と一致する値を検索します。

名前	説明
[Base DN] フィールド	リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から *cn=$userid* の長さを引いた長さに設定することができます。$userid により、LDAP 認証を使用して Firepower シャーシにアクセスしようとするリモートユーザが識別されます。 このプロパティは、LDAP プロバイダーに必要です。このタブでベース DN を指定しない場合、定義する LDAP プロバイダーごとに 1 つずつ指定する必要があります。
[Filter] フィールド	LDAP サーバで使用するフィルタ属性を入力します（*cn = $userid*、*sAMAccountName = $userid* など）。LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。フィルタには *$userid* が含まれている必要があります。 このプロパティは必須です。このタブでフィルタを指定しない場合は、定義する LDAP プロバイダーごとにフィルタを指定する必要があります。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

LDAP プロバイダを作成します。

LDAP プロバイダーの作成

次の手順に従い、LDAP プロバイダー（この Firepower アプライアンスに LDAP ベースの AAA サービスを提供する特定のリモートサーバ）を定義および設定します。

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

始める前に

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

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

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

a) [LDAP プロバイダー（LDAP Providers）] 領域で、[追加（Add）] をクリックします。

b) [LDAP プロバイダーの追加（Add LDAP Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	LDAP サーバのホスト名および IP アドレス。SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。
[Order] フィールド	Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、**`lowest-available`** または **`0`**（ゼロ）を入力します。
[Bind DN] フィールド	ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
[Base DN] フィールド	リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字 + CN=$userid の長さに設定することができます。$userid により、LDAP 認証を使用して Firepower Chassis Manager または FXOS CLI にアクセスしようとするリモート ユーザが識別されます。 デフォルトのベース DN が [LDAP] タブで設定されていない場合は、この値が必要です。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。

名前	説明
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリアテキストで送信されます。 LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。
[Filter] フィールド	LDAP サーバで使用するフィルタ属性を入力します（*cn = $userid*、*sAMAccountName = $userid* など）。LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。フィルタには *$userid* が含まれている必要があります。 デフォルトのフィルタが [LDAP] タブで設定されていない場合は、この値が必要です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 デフォルトの属性が [LDAP] タブで設定されていない場合は、この値が必要です。
[Key] フィールド	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための LDAP データベースパスワードの再入力。
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [LDAP] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 30 秒です。
[Vendor] フィールド	この選択により、LDAP プロバイダーやサーバの詳細を提供するベンダーが識別されます。 • LDAP プロバイダーが Microsoft Active Directory の場合は、[MS AD] を選択します。 • LDAP プロバイダーが Microsoft Active Directory でない場合は、[Open LDAP] を選択します。 デフォルトは [Open LDAP] です。

c) [OK] をクリックして [LDAP プロバイダーの追加（Add LDAP Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 （任意）証明書失効リスト検査を有効にします。

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

（注） この設定は、SSL 接続が使用可能である場合にのみ有効です。

LDAP プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [LDAP] タブをクリックします。

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

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

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

手順

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

ステップ 2 [RADIUS] タブをクリックします。

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

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

ステップ 4 [保存（Save）] をクリックします。

次のタスク

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

次の手順に従い、RADIUS プロバイダー（この Firepower アプライアンスに RADIUS ベースの AAA サービスを提供する特定のリモートサーバ）を定義および設定します。

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

手順

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

ステップ 2 [RADIUS] タブをクリックします。

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

a) [RADIUS プロバイダー（RADIUS Providers）] 領域で、[追加（Add）] をクリックします。

b) [RADIUS プロバイダーの追加（Add RADIUS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	RADIUS サーバのホスト名または IP アドレス。
[Order] フィールド	Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、**`lowest-available`** または **`0`**（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。

名前	説明
[Authorization Port] フィールド	Firepower Chassis Manager または FXOS CLI が RADIUS データベースと通信するために使用されるポート。有効な範囲は 1 ～ 65535 です。標準ポート番号は 1700 です。
[Timeout] フィールド	RADIUS データベースへの問い合わせがタイムアウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [RADIUS] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。 必要に応じて、0 ～ 5 の整数を入力します。値を指定しない場合、Firepower Chassis Manager は [RADIUS] タブに指定した値を使用します。

c) [OK] をクリックして [RADIUS プロバイダーの追加（Add RADIUS Provider）] ダイアログボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

RADIUS プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [RADIUS] タブをクリックします。

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

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

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

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

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

名前	説明
[Timeout] フィールド	TACACS+ データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。デフォルト値は 5 秒です。 このプロパティは必須です。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

次の手順に従い、TACACS+ プロバイダー（この Firepower アプライアンスに TACACS+ ベースの AAA サービスを提供する特定のリモートサーバ）を定義および設定します。

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

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

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

a) [TACACS プロバイダー（TACACS Providers）] 領域で、[追加（Add）] をクリックします。

b) [TACACS プロバイダーの追加（Add TACACS Provider）] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Hostname/FQDN (または IP アドレス)] フィールド	TACACS+ サーバのホスト名または IP アドレス。

名前	説明
[Order] フィールド	Firepower eXtensible Operating System でこのプロバイダーをユーザの認証に使用する順序。 1 ～ 16 の範囲の整数を入力します。または、Firepower Chassis Manager または FXOS CLI で定義されている他のプロバイダーに基づいて、次に使用できる順序を Firepower eXtensible Operating System で自動的に割り当てるには、**`lowest-available`** または **`0`**（ゼロ）を入力します。
[Key] フィールド	データベースの SSL 暗号キー。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Port] フィールド	Firepower Chassis Manager または FXOS CLI が TACACS+ サーバと通信するために使用するポート。 1 ～ 65535 の整数を入力します。デフォルト ポートは 49 です。
[Timeout] フィールド	TACACS+ データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して [TACACS+] タブで指定したグローバル タイムアウト値を使用します。デフォルトは 5 秒です。

c) [OK] をクリックして [TACACS プロバイダーの追加（Add TACACS Provider）] ダイアログ ボックスを閉じます。

ステップ 4 [保存（Save）] をクリックします。

TACACS+ プロバイダーの削除

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[AAA]** を選択します。

ステップ 2 [TACACS] タブをクリックします。

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

Syslog の設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央 syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。syslogサービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。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。

手順

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

ステップ 2 ローカル宛先を設定します。

a) [Local Destinations] タブをクリックします。

b) [ローカル宛先（Local Destinations）] タブで、次のフィールドに入力します。

名前	説明
[コンソール（Console）] セクション	
[管理状態（Administrative State）] フィールド	Firepower シャーシがコンソールに syslog メッセージを表示するかどうかを指定します。 ログに追加するとともに、コンソールに syslog メッセージを表示する場合は、[有効化（Enable）] チェックボックスをオンにします。[有効化（Enable）] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、コンソールに表示されません。
[レベル（Level）] フィールド	[コンソール（Console）]>[管理状態（Admin State）] で [有効化（Enable）] チェックボックスをオンにした場合は、コンソールに表示する最低のメッセージ レベルを選択します。Firepower シャーシのコンソールにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]**
[モニタ（Monitor）] セクション	

名前	説明
[管理状態（Administrative State）] フィールド	Firepower シャーシがモニタに syslog メッセージを表示するかどうかを指定します。 syslog メッセージをログに追加するとともに、モニタに表示する場合は、[有効化（Enable）] チェックボックスをオンにします。[有効化（Enable）] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、モニタに表示されません。
[レベル（Level）] ドロップダウン リスト	[モニタ（Monitor）]>[管理状態（Admin State）] で [有効化（Enable）] チェックボックスをオンにした場合は、モニタに表示する最低のメッセージ レベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**

c) [Save] をクリックします。

ステップ 3 リモート宛先を設定します。

a) [リモート宛先（Remote Destinations）] タブをクリックします。

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

syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

名前	説明
[Admin State] フィールド	リモート ログ ファイルに syslog メッセージを保存する場合は、[有効（Enable）] チェックボックスをオンにします。

名前	説明
[レベル（Level）] ドロップダウン リスト	システムに保存するメッセージの最低レベルを選択します。そのレベル以上のメッセージがリモート ファイルに保存されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**
[ホスト名/IP アドレス（Hostname/IP Address）] フィールド	リモート ログ ファイルが存在するホスト名または IP アドレス。 （注） IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。
[ファシリティ（Facility）] ドロップダウン リスト	ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。次のいずれかになります。 • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **local7**

c) [Save] をクリックします。

ステップ 4 ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) [ローカル送信元（Local Sources）] タブで、次のフィールドに入力します。

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

c) [保存（Save）] をクリックします。

DNS サーバの設定

システムでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバを指定する必要があります。たとえば、DNS サーバを設定していない場合は、Firepower シャーシに関する設定を行うときに、www.cisco.com などの名前を使用できません。サーバの IP アドレスを使用する必要があります。これには、IPv4 または IPv6 アドレスのいずれかを使用できます。最大 4 台の DNS サーバを設定できます。

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

手順

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

ステップ 2 [Enable DNS Server] チェックボックスをオンにします。

ステップ 3 追加する DNS サーバ（最大 4 台）ごとに、それぞれの IP アドレスを [DNS Server） フィールドに入力し、[Add] をクリックします。

ステップ 4 [Save] をクリックします。

FIPS モードの有効化

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

手順

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

次のタスク

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

コモン クライテリア モードの有効化

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

手順

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

次のタスク

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

IP アクセスリストの設定

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

IP アクセスリストは、次のプロトコルをサポートします。

- HTTPS
- SNMP
- SSH

IP アドレス（v4 または v6）の各ブロックで、最大 100 個の異なるサブネットを各サービスに対して設定できます。サブネットを 0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。

手順

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

ステップ 2 **Platform Settings** を選択し、[プラットフォーム設定（Platform Settings）] ページを開きます。

ステップ 3 **Access List** を選択し、[アクセスリスト（Access List）] 領域を開きます。

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

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

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

MAC プール プレフィックスの追加とコンテナ インスタンス インターフェイスの MAC アドレスの表示

FXOS シャーシは、各インスタンスの共有インターフェイスが一意の MAC アドレスを使用するように、コンテナインスタンスインターフェイスのMACアドレスを自動的に生成します。FXOS シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義のプレフィックスまたはシステム定義のプレフィックスであり、*zz.zzzz* はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROMにプログラムされている Burned-in MAC アドレス プール内の最初の MAC アドレスの下部 2 バイトと一致します。**connect fxos**を使用し、次に**show module**を使用して、MAC アドレスプールを表示します。たとえば、モジュール 1 について示されている MAC アドレスの範囲が b0aa.772f.f0b0 ～ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

詳細については、「コンテナ インスタンス インターフェイスの自動 MAC アドレス」を参照してください。

この手順では、MAC アドレスの表示方法と生成で使用されるプレフィックスのオプションの定義方法について説明します。

（注） 論理デバイスの展開後に MAC アドレスのプレフィックスを変更すると、トラフィックが中断される可能性があります。

手順

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

このページには、MAC アドレスを使用したコンテナ インスタンスやインターフェイスとともに生成された MAC アドレスが表示されます。

ステップ 2 （任意）MACアドレスの生成時に使用されるMACアドレスのプレフィックスを追加します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。

[Set the Prefix for the MAC Pool] ダイアログ ボックスが表示されます。

a) 1 ～ 65535 の 10 進数を入力します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、シャーシは 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスはシャーシ ネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

b) [OK] をクリックします。

プレフィックスを使用して新しい MAC アドレスが生成され、割り当てられます。現在のプレフィックスと生成される 16 進数はテーブルの上に表示されます。

コンテナインスタンスにリソースプロファイルを追加

コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソースプロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。

（注） コア数が少ないインスタンスは、コア数が多いインスタンスよりも、CPU 使用率が比較的高くなる場合があります。コア数が少ないインスタンスは、トラフィック負荷の変化の影響を受けやすくなります。トラフィックのドロップが発生した場合には、より多くのコアを割り当ててください。

- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。8 コアの使用は推奨されません。8 コアを使用した場合、6 コアの場合よりパフォーマンスがわずかに向上するにすぎません。
- 利用可能な最大コア数は、セキュリティモジュール/シャーシモデルによって異なります。「コンテナインスタンスの要件と前提条件」を参照してください。

シャーシには、「Default-Small」と呼ばれるデフォルトリソースプロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

使用中のリソースプロファイルの設定を変更することはできません。リソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペアまたはクラスタ内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

FTD インスタンスを FMC に追加した後でリソースプロファイルの設定を変更した場合は、FMC の **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[システム（System）]** > **[インベントリ（Inventory）]** ダイアログボックスで各ユニットのインベントリを更新します。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[リソースプロファイル（Resource Profiles）]** を選択し、[追加（Add）] をクリックします。

[リソースプロファイルの追加（Add Resource Profile）] ダイアログボックスが表示されます。

ステップ 2 次のパラメータを設定します。

- [名前（Name）]：プロファイルの名前を 1 ～ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
- [説明（Description）]：プロファイルの説明を最大 510 文字で設定します。
- [コア数（Number of Cores）]：プロファイルのコア数を 6 ～ 最大数（偶数）で設定します。最大数はシャーシによって異なります。

ステップ 3 **[OK]** をクリックします。

ネットワーク制御ポリシーの設定

他社製デバイスのディスカバリを許可するために、FXOS は、IEEE 802.1ab 規格で定義されているベンダーニュートラルなデバイス ディスカバリ プロトコルである Link Layer Discovery Protocol（LLDP）をサポートしています。LLDP を使用すると、ネットワークデバイスはネットワークデバイスに関する情報を、ネットワーク上の他のデバイスにアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信する単一方向のプロトコルです。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

FXOS シャーシでこの機能を有効にするために、ネットワーク制御ポリシーを設定できます。このポリシーにより、LLDP の伝送と受信の動作が指定されます。ネットワーク制御ポリシーを作成した後、インターフェイスに割り当てる必要があります。固定ポート、EPM ポート、ポートチャネル、およびブレイクアウトポートなどの任意の前面インターフェイスで LLDP を有効にできます。

（注）
- LLDP を専用管理ポートで設定することはできません。
- ブレードに接続する内部バックプレーンポートでは、デフォルトでLLDPが有効になっていて、無効にするオプションはありません。他のすべてのポートでは、LLDP はデフォルトで無効になっています。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）] > [ネットワーク制御ポリシー（Network Control Policy）]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [ネットワーク制御ポリシー（Network Control Policy）] ダイアログボックスで、次のフィールドを編集します。

名前	説明
[Description] フィールド	ネットワーク制御ポリシーの説明。
[LLDP受信（LLDP receive）] チェックボックス	FXOS が LLDP パケットを受信できるようにします。
[LLDP transmit] チェックボックスを選択します	FXOS が LLDP パケットを送信できるようにします。

ステップ 4 **[保存（Save）]**をクリックします。ネットワーク制御ポリシーを作成した後、インターフェイスに割り当てる必要があります。ネットワーク制御ポリシーでインターフェイスを編集および設定する手順については、物理インターフェイスの設定 を参照してください。

シャーシ URL の設定

管理 URL を指定して、FMC から直接、FTD インスタンスの Firepower Chassis Manager を簡単に開くことができます。シャーシ管理 URL を指定しない場合には、代わりにシャーシ名が使用されます。

FTD インスタンスを FMC に追加した後にシャーシ URL 設定を変更する場合は、**[Devices] > [Device Management] > [Device] > [System] > [Inventory]** ダイアログボックスで各ユニットのインベントリを更新します。

手順

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

ステップ 2 次のパラメータを設定します。

- [Chassis Name]：シャーシの名前を 1 ～ 60 文字で設定します。
- [Chassis URL]：Firepower Chassis Manager 内で FMC が FTD インスタンスに接続するために使用する URL を設定します。URL は https:// で始まる必要があります。シャーシ管理 URL を指定しない場合、代わりにシャーシ名が使用されます。

ステップ 3 [更新（Update）] をクリックします。