セキュリティ

この章は、次の項で構成されています。

TACACS+クライアント

組織は Terminal Access Controller Access Control System（TACACS+）サーバを構築して、すべてのデバイスに対する一元化されたセキュリティを提供できます。この方法では、認証と認可は組織内のすべてのデバイスを単一サーバ上で処理することができます。

デバイスは、次のサービスを提供する TACACS+ サーバーを使用する TACACS+ クライアントとして機能します。[TACACS+] ページでは、TACACS+ サーバーの設定ができます。

- 認証（Authentication）：ユーザ名とユーザ定義のパスワードを使用してデバイスにログインしているユーザの認証を提供します。
- [Authorization]：ログイン時に実行されます。認証セッションが完了すると、認証されたユーザ名を使用して認可セッションを開始します。その後、TACACS+ サーバがユーザの権限を確認します。
- アカウンティング（Accounting）：TACACS+ サーバを使用してログイン セッションのアカウンティングを有効にします。これにより、システム管理者は TACACS+ サーバからアカウンティング レポートを生成できるようになります。

TACACS+ サーバーパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ] > [TACACS+ クライアント] をクリックします。

ステップ 2 必要に応じて、[TACACS+ Accounting] を有効にします。

ステップ 3 次のデフォルト パラメータを入力します。

オプション	説明
Key String	暗号化モードまたはプレーンテキストモードのすべての TACACS+ サーバーとの通信に使用されるデフォルトのキーストリングを入力します。 ここで、キー文字列と個々の TACACS+ サーバのキー文字列の両方を入力する場合、個々の TACACS+ サーバに設定されているキー文字列が優先されます。
Timeout for Reply	デバイスと TACACS+ サーバーの間の接続がタイムアウトになるまでの経過時間を入力します。特定のサーバーに関する値が [Add TACACS+ Server] ページで入力されない場合、このフィールドの値が採用されます。
Source IPv4 Interface	TACACS+ サーバーとの通信のために送られるメッセージで使用されるデバイス IPv4 送信元インターフェイスを選択します。
Source IPv6 Interface	TACACS+ サーバーとの通信のために送られるメッセージで使用されるデバイス IPv6 送信元インターフェイスを選択します。 （注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 4 [Apply] をクリックします。TACACS+ のデフォルト設定が実行コンフィギュレーション ファイルに追加されます。それらの設定は、[Add] ページに同等のパラメータが定義されていない場合に使用されます。

各 TACACS サーバの情報は、TACACS+ サーバ テーブルに表示されます。このテーブルのフィールドは、[Status] フィールドを除き、[Add] ページで入力します。このフィールドは、サーバーがデバイスに接続されているかどうかを示します。

ステップ 5 TACACS+ サーバを追加するには、[Add] をクリックします。TACACS+ サーバーを編集するには、TACACS+ サーバーを選択して [Edit] をクリックします。

ステップ 6 次に、パラメータを構成します。

オプション	説明
Server Definition	TACACS+ サーバーを識別する方法として、次のいずれか 1 つを選択します。 • [By IP address]：これを選択した場合は、[Server IP Address/Name] フィールドにサーバーの IP アドレスを入力します。 • [By name]：これを選択した場合は、[Server IP Address/Name] フィールドにサーバーの名前を入力します。
IP Version	送信元 IP アドレスのサポート対象 IP バージョン（IPv6 または IPv4）を選択します。
IPv6 Address Type	IPv6 アドレスタイプを選択します（IPv6 が使用されている場合）。次のオプションがあります。 • [Link Local]：IPv6 アドレスによって、単一ネットワークリンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6 アドレスは、他のネットワークから表示可能で到達可能なグローバルユニキャスト IPV6 タイプです。
Link Local Interface	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
サーバーのIPアドレス/名前	TACACS+ サーバーの IP アドレスまたは名前を入力します。
Priority	この TACACS+ サーバーの使用順序を入力します。ゼロは優先順位が最も高い TACACS+ サーバかつ最初に使用されるサーバを示します。優先順位が最も高いサーバーとのセッションを確立できない場合、デバイスは次に優先順位が高いサーバーとの接続を試みます。
Key String	デバイスと TACACS+ サーバーの間の認証と暗号化に使用されるデフォルトのキーストリングを入力します。このキーは、TACACS+ サーバに設定されているキーと一致する必要があります。

オプション	説明
	キー文字列は、MD5を使用して通信を暗号化するために使用されます。デバイスのデフォルト キーを選択するか、暗号化（Encrypted）またはプレーン テキスト（Plaintext）形式でキーを入力することができます。（別のデバイスからの）暗号化キーストリングがない場合は、プレーンテキストモードでキーストリングを入力して [Apply] をクリックします。暗号化されたキー文字列が生成されて表示されます。
Timeout for Reply	[User Defined] を選択して、デバイスと TACACS+ サーバーの間の接続がタイムアウトになるまでの経過時間を入力します。ページに表示されているデフォルト値を使用する場合は、[Use Default] を選択します。
認証IPポート	TACACS+ セッションが発生するポート番号を入力します。
単一接続	すべての情報を単一の接続で受信できるようにするには、このフィールドを選択します。TACACS+ サーバーがこれをサポートしない場合、デバイスは複数接続に戻ります。

ステップ 7 [Apply] をクリックします。TACACS+ サーバがデバイスの実行コンフィギュレーション ファイルに追加されます。

ステップ 8 このページでプレーン テキスト形式でセンシティブ データを表示するには、[Display Sensitive Data As Plaintext] をクリックします。

RADIUS Client

Remote Authorization Dial-In User Service（RADIUS）サーバは、一元化された 802.1X または MAC ベースのネットワーク アクセス コントロールを提供します。デバイスは、一元化されたセキュリティを提供するために RADIUS サーバを使用できる RADIUS クライアントとなるように設定、およびRADIUS サーバとして設定できます。組織は、デバイスを Remote Authorization Dial-In User Service（RADIUS）サーバとして使用して、一元化された 802.1X または MAC ベースのネットワーク アクセス コントロールをすべてのデバイスに対して提供できます。この方法では、認証と認可は組織内のすべてのデバイスを単一サーバ上で処理することができます。

RADIUS は、アクセスのセキュリティが必要なネットワーク環境で使用します。RADIUS サーバーのパラメータ値を設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Client] をクリックします。

ステップ 2 RADIUS アカウンティング オプションを入力します。次のオプションを使用できます。

- [Port Based Access Control (802 1X, MAC Based, Web Authentication)]：802.1X ポートアカウンティングに RADIUS サーバーが使用されることを指定します。
- 管理アクセス（Management Access）：RADIUS サーバがユーザ ログイン アカウンティングに使用されることを指定します。
- [Both Port Based Access Control and Management Access]：ユーザー ログイン アカウンティングと 802.1X ポートアカウンティングの両方に RADIUS サーバーが使用されることを指定します。
- なし（None）：RADIUS サーバがアカウンティングに使用されないことを指定します。

ステップ 3 アカウンティング期間を設定します。範囲は 0 ～ 65535 です。

ステップ 4 必要に応じて、デフォルトの RADIUS パラメータを入力します。[Default Parameters] で入力した値は、すべてのサーバに適用されます。特定のサーバの値が [Add RADIUS Server] ページで入力されていない場合、これらのフィールドの値がデバイスで使用されます。

- [リトライ回数]：RADIUS サーバーに要求を送信する最大試行回数を入力します。こ の回数送信しても要求が受け付けられなかった場合、エラーになります。
- 応答のタイムアウト（Timeout for Reply）：クエリを再試行するか、次のサーバに切り替える前にデバイスが RADIUS サーバからの応答を待機する秒数を入力します。
- [デッドタイム（Dead Time）]：応答のない RADIUS サーバーへのサービス要求がバイパスされるようになるまでのタイムインターバル（単位：分）を入力します。デッドタイムは、非応答 RADIUS サーバーがトランザクション要求によって省略される間のタイムインターバルを分単位で指定します（範囲：0 ー 2000）。デフォルトのインターバルは 0 です（非応答 RADIUS サーバーは省略されません）。
- キー文字列（Key String）：デバイスと RADIUS サーバ間の認証と暗号化に使用されるデフォルト キー文字列を入力します。キーは、RADIUS サーバで設定されたキーと一致する必要があります。キー文字列は、MD5 を使用して通信を暗号化するために使用されます。暗号化（Encrypted）またはプレーン テキスト（Plaintext）形式でキーを入力することができます。（別のデバイスからの）暗号化キー文字列がない場合、プレーン テキスト モードでキー文字列を入力し、[Apply] をクリックします。暗号化されたキー文字列が生成されて表示されます。

これで、デフォルト キー文字列がオーバーライドされます（定義されている場合）。

- 送信元 IPv4 インターフェイス（Source IPv4 Interface）：RADIUS サーバと通信するためのメッセージで使用されるデバイスの IPv4 送信元インターフェイスを選択します。
- 送信元 IPv6 インターフェイス（Source IPv6 Interface）：RADIUS サーバと通信するためのメッセージで使用されるデバイスの IPv6 送信元インターフェイスを選択します。

（注）
自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 5 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

ステップ 6 RADIUS サーバーを追加するには、[Add] をクリックします。

ステップ 7 各 RADIUS サーバのフィールドに値を入力します。

- [サーバー指定方法] : RADIUS サーバーを IP アドレスで指定するか、名前で指定するか を選択します。
- IP バージョン（IP Version） : RADIUS サーバの IP アドレスのバージョンを選択します。
- [IPv6 Address Type] : IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local] : IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックスは FE 80 で、ルーティングはできません。また、ローカル ネットワーク上の通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global] : IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- [リンクローカルインターフェイス] : リストからリンク ローカル インターフェイス（IPv6 アドレス タイプとしてリンク ローカルが選択されている場合）を選択します。•
- [Server IP Address/Name] : RADIUS サーバーを、IP アドレスまたは名前で入力します。
- [プライオリティ] : RADIUS サーバーのプライオリティを入力します。優先順位によって、デバイスがユーザ認証のために通信を試みるサーバの順序が決まります。デバイスは最初に、優先順位が最も高い RADIUS サーバとの接続を開始します。ゼロが最も高い優先順位です。
- キー文字列（Key String） : デバイスと RADIUS サーバ間の通信の認証と暗号化に使用されるキー文字列を入力します。キーは、RADIUS サーバで設定されたキーと一致する必要があります。キーは、暗号化（Encrypted）またはプレーンテキスト（Plaintext）形式で入力することができます。[Use Default] を選択した場合、デバイスはデフォルト キー文字列を使用して、RADIUS サーバの認証を試みます。
- 応答のタイムアウト（Timeout for Reply） : 最大試行回数に達した場合、[User Defined] を選択して、クエリを再試行するか、次のサーバに切り替える前にデバイスが RADIUS サーバからの応答を待機する秒数を入力します。[デフォルトを使用] を選択した場合、デバイスはデフォルトのタイムアウト値を使用します。
- [Authentication Port] : 認証要求用の RADIUS サーバーポートの UDP ポート番号を入力します。
- アカウンティング ポート（Accounting Port） : アカウンティング要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。
- 再試行回数（Retries） : [User Defined] を選択して、障害が発生したと見なされる前に、RADIUS サーバに送信される要求の数を入力します。[Use Default] を選択した場合、デバイスは再試行回数のデフォルト値を使用します。
- [デッドタイム（Dead Time）] : 応答のない RADIUS サーバーへのサービス要求がバイパスされるようになるまでのタイムインターバル（単位：分）を入力します。デッドタイムは、非応答 RADIUS サーバーがトランザクション要求によって省略される間のタイムインターバルを分単位で指定します（範囲：0 ー 2000）。デフォルトのインターバルは 0 です（非応答 RADIUS サーバーは省略されません）。

- [使用タイプ] : RADIUS サーバーの認証タイプを入力します。次のオプションがあります。
  - ログイン（Login）：RADIUS サーバは、デバイスの管理を要求するユーザの認証に使用されます。
  - [802.1X] : RADIUS サーバーは 802.1X 認証に使用されます。
  - すべて（All）：RADIUS サーバは、デバイスの管理を要求するユーザの認証および 802.1X 認証に使用されます。
- [Force Message Authenticator] : 指定した RADIUS サーバーからのすべてのタイプの RADIUS 応答に Message-Authenticator 属性（RADIUS 属性 80）を含める必要があることを定義するには、この設定を使用します。この設定を有効にすると、Message-Authenticator 属性を含まないすべてのタイプの RADIUS 応答が警告なしで破棄され、イベントがログに記録されます。この設定が無効になっている場合、この属性を含まない RADIUS 応答は、EAP 認証を使用する RADIUS 交換の一部である場合にのみ破棄されます。デフォルトでは、この設定は無効です。

ステップ 8 [Apply] をクリックします。RADIUS サーバの定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

ステップ 9 ページでプレーン テキスト形式でセンシティブ データを表示するには、[Display Sensitive Data As Plaintext] をクリックします。

RADIUS サーバ

組織のすべてのデバイスを対象として 802.1X または MAC に基づくネットワークアクセスの一元的な制御を行うために、デバイスを Remote Authorization Dial-In User Service（RADIUS）サーバーとして使用することができます。この方法により、すべてのデバイスに関する認証と認可を 1 つのサーバーで扱うことができます。

デバイスが RADIUS クライアントとして設定されている場合、次のサービスに RADIUS サーバを使用できます。

- 認証：ユーザー名およびユーザー定義のパスワードを使用して、通常のユーザーおよび 802.1X ユーザーを認証する機能を提供します。
- 認可：ログイン時に実行します。認証セッションが完了すると、認証されたユーザー名を使用して認可セッションが開始します。その後、RADIUS サーバがユーザの権限を確認します。

アカウンティング：RADIUS サーバーを使用したログインセッションのアカウンティングを有効にします。これにより、システム管理者は RADIUS サーバからアカウンティング レポートを生成できるようになります。RADIUS サーバのアカウンティングに使用されるユーザが設定可能な TCP ポートは、RADIUS サーバの認証と認可に使用されるのと同じ TCP ポートです。

RADIUSサーバーグローバル設定

デバイスは、RADIUS サーバとして設定できます。RADIUS サーバーのグローバルパラメータ値を設定するには、次のようにします。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Global Settings] の順にクリックします。

ステップ 2 次のパラメータを入力します。

- RADIUS サーバのステータス（RADIUS Server Status）：RADIUS サーバ機能のステータスを有効にする場合に選択します。
- 認証ポート（Authentication Port）：認証要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。
- アカウンティング ポート（Accounting Port）：アカウンティング要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。

トラップの設定

- [RADIUS Accounting Traps]：RADIUS アカウンティングイベントのトラップを生成する場合は [Enable] チェックボックスをオンにします。
- [RADIUS Authentication Failure Traps]：失敗したログインのトラップを生成する場合は [Enable] チェックボックスをオンにします。
- [RADIUS Authentication Success Traps]：成功したログインのトラップを生成する場合は [Enable] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

RADIUSサーバーキー

RADIUS サーバーキーを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Keys] の順にクリックします。

ステップ 2 必要に応じて、デフォルトの RADIUS キーを入力します。[Default Key] に入力した値は、（[ADD RADIUS Server] ページで）デフォルト キーを使用するように設定されているすべてのサーバに適用されます。

- デフォルト キー（Default Key）：デバイスと RADIUS サーバ間の認証と暗号化に使用されるデフォルト キー文字列を入力します。次のオプションのいずれかを選択します。
  - 既存のデフォルト キーを保持（Keep existing default key）：デバイスは、指定されたサーバに対して、既存のデフォルト キー文字列を使用して RADIUS クライアントの認証を試みます。
  - 暗号化（Encrypted）：MD5 を使用して通信を暗号化するには、暗号化された形式でキーを入力します。
  - プレーン テキスト（Plaintext）：プレーン テキスト モードでキー文字列を入力します。
- MD5 Digest（MD5 ダイジェスト）：ユーザが入力したパスワードの MD5 ダイジェストが表示されます。

ステップ 3 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

ステップ 4 [Add] をクリックして秘密鍵を追加するか、[Edit] をクリックして、秘密鍵テーブルの既存の秘密鍵を編集します。次に、次のフィールドに入力します。

- NAS アドレス（NAS Address）：RADIUS クライアントが含まれているスイッチのアドレス。
- [Key's MD5 Digest]：デフォルトでは定義されていません。これは、秘密鍵テーブルを編集する場合にのみ表示されます。
- 秘密キー（Secret Key）：RADIUS クライアントが含まれているスイッチのアドレス。
  - [Use default key]：指定されたサーバーに対して、デバイスは既存のデフォルトキーストリングを使用して、RADIUS クライアントの認証を試行します。
  - [Keep current user defined key]：既存のユーザー定義キーを保持する場合に選択します。
  - 暗号化（Encrypted）：MD5 を使用して通信を暗号化するには、暗号化された形式でキーを入力します。
  - プレーン テキスト（Plaintext）：プレーン テキスト モードでキー文字列を入力します。

ステップ 5 [Apply] をクリックします。デバイスのキーが実行コンフィギュレーション ファイルで更新されます。

RADIUS サーバー グループ

デバイスを RADIUS サーバーとして使用するユーザーのグループを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Groups] の順にクリックします。

ステップ 2 [Add] をクリックしてRADIUS サーバーグループを追加するか、[Edit] をクリックして既存のグループを編集します。次のフィールドに入力します。

- [Group Name]：グループの名前を入力します。
- 権限レベル（Privilege Level）：グループの管理アクセス権限レベルを入力します。
- 時間範囲（Time Range）：このグループに時間範囲を適用する場合に選択します。
- 時間範囲名（Time Range Name）：[Time Range] を選択した場合、使用する時間範囲を選択します。時間範囲を定義するには、[Edit] をクリックします。このフィールドは、時間範囲が作成済みである場合にのみ表示されます。
- VLAN：ユーザの VLAN を選択します。
  - [None]：VLAN ID は送信されません。
  - [VLAN ID]：送信される VLAN ID。
  - VLAN 名（VLAN Name）：送信される VLAN 名。

ステップ 3 [Apply] をクリックします。RADIUS グループの定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

RADIUSサーバーユーザー

ユーザを追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Users] の順にクリックします。

現在のユーザが表示されます。

ステップ 2 [Add] または [Edit] をクリックして、以下を設定します。

- [User Name]：ユーザーの名前を入力します。
- [Group Name]：以前に定義したグループを選択します。
- [Password's MD5]：パスワードの MD5 暗号化ハッシュが表示されます。
- [Password]：次のいずれかのオプションを入力します。
  - [Keep current password]：現在のパスワードを保持するには、このオプションを使用します。
  - 暗号化（Encrypted）：キー文字列は MD5 を使用して通信を暗号化するために使用されます。暗号化を使用するには、暗号化された形式でキーを入力します。

- [Plaintext]：（別のデバイスからの）暗号化キーストリングがない場合は、プレーンテキストモードでキーストリングを入力します。暗号化されたキー文字列が生成されて表示されます。

ステップ 3 [Apply] をクリックします。ユーザ定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

RADIUS サーバアカウンティング

RADIUS サーバは、FLASH のサイクル ファイルに最後のアカウンティング ログを保存します。アカウンティング ログは表示することができます。

RADIUS サーバーアカウンティングを表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Accounting] をクリックします。

RADIUS アカウンティング イベントが次のフィールドとともに表示されます。

- [User Name]：ユーザーの名前。
- イベント タイプ（Event Type）：値は次のいずれかです。
  - [Start]：セッションが開始されました。
  - [Stop]：セッションは停止されました。
  - 日付/時刻変更（Date/Time Change）：デバイスの日付/時刻が変更されました。
  - リセット（Reset）：デバイスが指定された時間にリセットされました。
- 認証方式（Authentication Method）：ユーザによって使用されている認証方式。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- NAS アドレス（NAS Address）：RADIUS クライアントが含まれているスイッチのアドレス。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- ユーザアドレス（User Address）：認証されたユーザがネットワーク管理者の場合、これはその管理者の IP アドレスで、ユーザがステーションの場合、これはそのステーションの MAC アドレスです。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- [Event Time]：イベントの時間。

ステップ 2 RADIUS サーバー アカウンティング イベントをクリアするには、[Clear] をクリックします。

ステップ 3 ユーザまたはイベントの詳細情報を表示するには、ユーザまたはイベントを選択して、[Details] をクリックします。

次のフィールドが表示されます。

（注） このページのフィールドは、閲覧しているアカウントのタイプとそのアカウントで受信した詳細情報によって異なります。常にすべてのフィールドが表示されるわけではありません。

- [Event Time]：上記参照。
- [Event Type]：上記参照。
- [User Name]：上記参照。
- [Authentication Method]：上記参照。
- [NAS IPv4 Address]：上記の [NAS Address] 参照。
- [User Address]：上記参照。
- アカウンティングセッション時間（Accounting Session Time）：上記のイベント時間（Event Time）を参照してください。
- セッションの終了理由（Session Termination Reason）：セッションの終了理由（ユーザの要求など）が表示されます。

RADIUSサーバー拒否ユーザー

RADIUS サーバーを使用して認証を試行し、拒否されたユーザーを表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Rejected Users] をクリックします。

拒否されたユーザが次のフィールドとともに表示されます。

- [Event Type]：次のいずれかのオプションが表示されます。
  - Rejected：ユーザーは拒否されました。
  - 時間変更（Time Change）：デバイスの時計が管理者によって変更されました。
  - リセット（Reset）：デバイスが管理者によってリセットされました。
- ユーザ名（User Name）：拒否されたユーザの名前。

- ユーザ タイプ（User Type）：ユーザに関連する次の認証オプションのいずれかが表示されます。
  - [Login]：管理アクセスユーザー
  - [802.1x]：802.1x ネットワーク アクセス ユーザー
  - [N/A]：リセットイベント用
- [Reason]：ユーザーが拒否された理由。
- [Time]：ユーザーが拒否された時間。

ステップ 2 拒否されたユーザの詳細情報を表示するには、そのユーザを選択して、[Details] をクリックします。

次のフィールドが表示されます。

（注） このページのフィールドは、閲覧しているアカウントのタイプとそのアカウントで受信した詳細情報によって異なります。常にすべてのフィールドが表示されるわけではありません。

- [Event Time]：上記参照。
- [User Name]：上記参照。
- [User Type]：上記参照。
- 拒否理由（Rejection Reason）：ユーザが拒否された理由。
- NAS IP アドレス（NAS IP Address）：Network Accessed Server（NAS）のアドレス。NAS は、RADIUS クライアントを実行しているスイッチです。

拒否されたユーザのテーブルをクリアするには、[Clear] をクリックします。

RADIUSサーバー不明NASエントリ

NAS が RADIUS サーバーに認識されていないことが原因の認証拒否を表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Unknown NAS Entries] の順にクリックします。

次のフィールドが表示されます。

- イベント タイプ
  - 不明な NAS（Unknown NAS）：不明な NAS イベントが発生しました。

- 時間変更（Time Change）：デバイスの時計が管理者によって変更されました。
- リセット（Reset）：デバイスが管理者によってリセットされました。

- IPアドレス（IP Address）：不明な NAS の IP アドレス。
- [Time]：イベントのタイムスタンプ。

ステップ 2 エントリを削除するには、[Clear] をクリックします。

RADIUSサーバー統計情報

RADIUS サーバの統計情報を表示する手順は、次のとおりです。

手順

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Statistics] の順にクリックします。
ステップ 2 次のオプションから統計情報ソースを選択します。

- [Global]：すべてのユーザーの統計情報
- [Specific NAS]：特定の NAS の統計情報。

ステップ 3 [Refresh Rate] を選択します。
ステップ 4 次の統計情報が表示されます。

認証ポート上の着信パケット数	認証ポートで受信したパケットの数。
不明なアドレスからの着信アクセス要求数	不明な NAS アドレスからの着信アクセス要求数。
重複着信アクセス要求数	受信した再送されたパケットの数。
送信済みアクセス許可数	送信されたアクセス許可の数。
送信済みアクセス拒否数	送信されたアクセス拒否の数。
送信済みアクセスチャレンジ数	送信されたアクセスチャレンジの数。
着信無効アクセス要求数	受信した不正なアクセス要求の数。
不正な認証コードを伴う着信認証要求数	パスワードが正しくない着信パケットの数。
その他の誤りを伴う着信認証パケット数	その他の誤りを伴う着信認証パケットの数。
不明なタイプの着信認証パケット数	不明なタイプの着信認証パケットの数。

アカウンティングポート上の着信パケット数	アカウンティングポート上の着信パケットの数。
不明なアドレスからの着信アカウンティング要求数	不明なアドレスからの着信アカウンティング要求の数。
着信重複アカウンティング要求数	着信重複アカウント要求の数。
送信済みアカウンティング応答数	送信済みアカウンティング応答の数。
着信無効アカウンティング要求数	無効アカウンティング要求の数。
不正な認証コードを伴う着信アカウンティング要求数	不正な認証コードを伴う着信アカウンティング要求の数。
その他の誤りを伴う着信アカウンティングパケット数	その他の誤りを伴う着信アカウンティングパケットの数。
着信未記録アカウンティング要求数	着信未記録アカウンティング要求の数。
不明なタイプの着信アカウンティングパケット数	タイプ不明の着信アカウンティングパケットの数。

ステップ5 カウンタをクリアするには、[Clear Counters] をクリックします。

ステップ6 カウンタを更新するには、[Refresh] をクリックします。

ダイナミック承認サーバー

（注） CoA 機能は、C1300 スイッチおよびファームウェアバージョン 4.1.3.36 以降でサポートされています。

認可変更（CoA）は RADIUS プロトコルの拡張であり、AAA または dot1x ユーザーセッションをダイナミックに変更できます。これには、ユーザーの切断およびユーザーセッションに適用される認可の変更のサポートが含まれます。デバイスは、次の CoA アクションをサポートします。

- セッションの切断
- ホストポート CoA コマンドの無効化
- ホストポート CoA コマンドのバウンス
- ホスト CoA コマンドの再認証

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。認可変更（CoA）は RADIUS プロトコルの拡張であり、AAA ま

たは dot1x ユーザーセッションをダイナミックに変更できます。これには、ユーザーの切断およびユーザーセッションに適用される認可の変更のサポートが含まれます。

手順

ステップ 1 [Security] > [Dynamic Authorization Server] をクリックします。

ステップ 2 次の設定を行います。

設定	説明
デフォルトのサーバーキー MD5	デバイスと CoA クライアント間の共有キーを定義します。次のいずれかを選択します。 • なし • 既存のデフォルトキーを維持する • ユーザー定義(暗号化) • ユーザー定義(平文)
キーのMD5ダイジェスト	デフォルトでは未定義
UDP Port	CoA 要求の UDP ポートを設定する値を入力します（範囲 0 ～ 59999、デフォルト：1700）。
ドメイン ストリッピング	CoA アプリケーションのユーザー名ドメインのオプションを設定します。以下のいずれかのオプションを選択します。 • [None]：ドメインの削除なし • [Left to Right]：この左から右キーワードは、左から右に向かって移動して最初に見つかったデリミタで文字列を終わらせます。 • [Right to Left]：この右から左キーワードは、右から左に向かって移動して最初に見つかったデリミタで文字列を終わらせます
ドメインデリミタ	このデリミタフィールドは、ドメインデリミタを指定します。文字引数として次のいずれかのオプションを選択できます：@、/、$、%、\、#、または -。

ステップ 3 [Client] テーブルは、特定の CoA クライアントの CoA クライアントごとの MD5 サーバーキーを定義します。クライアントごとのキーは、[Default Server Key MD5] 設定で定義されたキーを上書きします。特定の CoA クライアントに対してキーが定義されていない場合、クライアントは [Default Server Key MD5] を使用します。特定の CoA クライアントのキーを追加または編集するには、[Add] または [Edit] をクリックし、次のように設定します。

- [IP Address]：CoA クライアントの IPv4 または IPv6 アドレス

- [MD5 Digest]：未定義（デフォルト）
- [Server Key]：次のいずれかを選択します。
  - [Use default key]：この場合、デフォルトのサーバーキーが使用されます。
  - [Keep current user defined key]：現在のユーザー定義キーが維持されます。
  - [User Defined (Encrypted)]：暗号化された形式でキーを入力します。
  - [User Defined (Plaintext)]：プレーンテキスト形式でキーを入力します。

ステップ 4 [Apply] をクリックして設定を適用します。

ステップ 5 次に、[Client Address] を選択し、[Counters] をクリックしてカウンタを表示します。次の表で、ポップアップに表示されるフィールドについて説明します。

フィールド	説明
IPアドレス	IP address
Average ACK response time	ミリ秒単位の平均 ACK 応答時間。
Requests	CoA クライアントから受信した要求をカウントします。
Transactions	CoA の完了トランザクションをカウントします。スイッチが CoA クライアントからの要求に応答して ACK または NAK を送信すると、完了トランザクションが発生します。
再送信	受信した再送信された CoA 要求をカウントします。再送信された CoA 要求は、要求識別子が前の要求の識別子と同じである要求です。
Active Transactions	現在アクティブなトランザクション。アクティブなトランザクションとは、CoA クライアントからの要求を受信したが、ACK または NAK 応答がまだ送信されていないトランザクションです。ACK または NAK が送信されると、このカウンタはデクリメントされます。
ACX Responses	スイッチから送信された ACK 応答の数をカウントします。
NAK Responses	スイッチから送信された NAK 応答の数をカウントします。

フィールド	説明
Invalid Requests	スイッチが受信した無効な要求をカウントします。無効な要求は、次のいずれかです。 • 要求内のシークレットがデバイスに設定されているシークレットと一致しない要求。 • セッション識別子のない要求。 • サポートされていない属性を持つ要求。 • サポートされている属性が空の要求。 • event-timestamp が最新ではないため、または event-timestamp が必須で、受信した要求にこの属性が含まれていないために破棄された要求。 • Event-Timestamp 属性が最新ではないか、欠落している要求。 • ユーザー設定が原因でドロップされた「disable port」または「bounce port」コマンドで受信した要求。
Errors	エラーをカウントします。エラーは、リソースの問題が原因で要求を処理できない内部エラーであるか、CoA クライアントにシークレットが設定されていない場合に発生する可能性があります。

ログイン設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

デフォルトのユーザー名/パスワードは、**cisco/cisco** です。デフォルトのユーザー名とパスワードで初めてログインすると、新しいパスワードを入力するように求められます。パスワードの複雑性は、デフォルトで有効になっています。選択したパスワードが十分に複雑でない場合は、別のパスワードを作成するように求められます。

手順

ステップ 1 [Security] > [Login Settings] をクリックします。

ステップ 2 次に、以下の項目を設定します。

オプション	説明
パスワード エージング	[Enable] をオンにし、パスワードエージングを有効にします。この機能はデフォルトでは無効になっています。
パスワードエージング時間	これを行うには、日数を入力します。（範囲：1 ～ 365、デフォルト：180） （注） パスワードの有効期限の 10 日前に、パスワードを変更できる警告メッセージが表示されます。ユーザーは警告を無視して、実際の有効期限まで既存のパスワードを引き続き使用できます。
最近のパスワード防御	この機能を有効にするには[Enable] をオンにします。この機能はデフォルトでは無効になっています。
パスワード履歴カウント	最近のパスワード防御の数を定義します。指定できる範囲は 1 ～ 24 で、デフォルトは 12 です。
最小パスワード長	パスワードの文字数を入力します。（範囲：8 ～ 64、デフォルト：8）
許容される文字の繰り返し	文字を連続して繰り返すことはできません。許容される文字の繰り返し回数を入力します。（範囲：1 ～ 16、デフォルト：3）
キーボードパターンの防止	[Allowed character repetition]：この機能を有効にするには、[Enable] をオンにします。この機能はデフォルトではディセーブルになっています。有効にすると、パスワードに 3 つ以上の隣接する QWERTY キーボード文字または数字を含めることはできません。
文字クラスの最小数：	文字クラスの最小数を入力します。（範囲：1～4、デフォルト：3）

（注）
パスワードの複雑さのルールは次のとおりです。

- デフォルトのパスワードの最小長は 8 文字です。パスワードは、8 ～ 64 文字の範囲で設定できます。
- 文字クラスの最小数：パスワードに使用する必要があるさまざまな文字クラスの数（クラスとは、大文字、小文字、数字、特殊文字です）。デフォルトでは、最小数は 3 で、0 ～ 4 の範囲で設定できます（0 と 1 は機能的に同じです）。
- ユーザーによって設定または変更されたパスワード（以降「シークレット」）は、一般的なパスワードのリストと比較されます。SecLists/パスワード共通のログイン情報。シークレットにリスト内の単語が含まれている場合、ユーザーは次のエラーメッセージを受け取り、別のパスワードを再入力する必

要があります：「Password rejected- Passwords must not match words in the dictionary, and must not contain commonly used passwords」。

- コンテキスト固有の単語（プロジェクトおよびベンダー名）：パスワードには、ユーザー名、「cisco」、「catalyst」、またはその派生語を含めてはなりません。これらの単語の逆読みや大文字と小文字の組み合わせもこの制限の対象となります。次のような他の文字に置き換えられる文字もこの制限に含まれます：「s」の代わりの「$」、「a」の代わりの「@」、「o」の代わりの「0」、「l」の代わりの「1」、「i」の代わりの「!」、「e」の代わりの「3」は使用できません。たとえば、C!$c0678! は許可されていません。
- パスワードを変更する場合、新しいパスワードは現在のパスワードと異なる必要があります。
- パスワードにユーザー名またはその派生形（逆にした文字列、「s」を $ に変えるといった一般的な置換など）を含めることはできません。
- パスワードに製造元の名前またはその派生形（cisco、C!$c0、oc$is など）を含めることはできません。

既知のパスワードの定義

ユーザーが新しいパスワードを設定しようとすると、一般的に使用されるパスワードのリストと比較されます。新しいパスワードが、共通のパスワードリスト内のいずれかのパスワードと一致するか、そのパスワードで始まる場合です。リストのパスワードとの比較では、大文字と小文字が区別されません。

新しいパスワードが上記の要件に準拠していない場合、ユーザー設定は拒否され、ユーザーは別のパスワードを設定する必要があります。

連続文字の定義

パスワードには、2 文字以上の連続する文字または数字を含めることはできません。この制限は、大文字と小文字の区別なく連続した文字に適用されます（例：AbC または aBC）。

禁止パスワードの例：「eFg152!$」、「aztb567%」。

パスワードがこれらのルールに準拠していない場合、設定は拒否され、ユーザーは新しいパスワードを設定する必要があります。

ログインロックダウン

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

デバイスのアドレスがわかっている場合、悪意のあるユーザーが辞書攻撃を試みる可能性があります。辞書攻撃とは、数千、時には数百万ものログイン情報でログインを試行する自動化されたプロセスです。辞書攻撃の目的は、実際にデバイスへの管理アクセス権を取得することです。

これらの攻撃を防ぐために、特定の時間範囲内で許可されるログイン試行回数を制限するようにデバイスを設定し、失敗した試行が指定の回数に達した後に続く静音モード時間を定義することができます。指定の時間（within seconds）内に、指定された回数の接続試行が失敗した（attempt tries）場合、デバイスは指定された時間（block-for seconds）の間、追加のログイン試行を受け入れません。これは、ユーザーがログイン情報を忘れ、何度かログインを試みてもログインできなかった場合にも発生する可能性があります。

（注） 指定の時間内に指定された回数のログイン試行が失敗すると、デバイスは静音モードに入ります。telnet、SSH、SNMP、HTTP、HTTPS を含め、静音モードの間は接続要求を受け付けなくなります。静音モードの時間が終了すると、デバイスは接続要求の受け入れを再開します。静音モードの開始時間と終了時間は、Syslog メッセージで示されます。

失敗した試行回数は、各失敗した試行が測定される期間全体を通じてカウントする必要があります。静音期間中は、失敗した試行はカウントされません。待機時間が終了すると、失敗した試行のカウントが再開されます。タイマーが切れる前でも、この機能を無効にすることで待機時間を終了できます。

手順

ステップ 1 [Login Response Delay] で、[Enable] をオンにして、ログイン応答遅延を有効にします。

ステップ 2 次に、以下の項目を設定します。

オプション	説明
Response Delay Period	応答遅延期間を秒数で入力して設定します。（範囲：1 ～ 10、デフォルト：1）
Quiet Period Enforcement	[Enable] をオンにして、静音時間を適用します。
Quiet Period Length	待機時間の長さを秒数で入力して設定します。（範囲：1 ～ 65535、デフォルト：300）
Triggering Attempts	トリガーの試行回数を入力します。（範囲：1 ～ 100、デフォルト：4）
Triggering Interval	トリガー間隔の秒数を入力します。（範囲：1 ～ 3600、デフォルト：60）
静音時間アクセスプロファイル （27 ページ）。 （注）	デフォルト設定は [Console Only] です。 （注）

オプション	説明
このリンクをクリックすると、[Security] → [Management Access Method] → [Access Profiles] ページに移動します。	このドロップダウンには、既存のすべてのアクセスプロファイルのオプションが含まれています。

ログイン保護ステータス

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[Login Protection Status] ページは、試行された攻撃やログインエラーを追跡して表示します。（ログインエラーがログイン情報を忘れたユーザーに起因するか、実際の攻撃に起因するかは区別されません）。[Refresh] ボタンをクリックするとデータが更新されます。

[Login Protection Status] の設定を表示するには、[Security] > [Login Protection Status] の順に選択します。

- [Quiet Mode Status]：アクティブまたは非アクティブのいずれかのステータスになります。
- [Login Failures in the Last 3600 Seconds]：[Quiet Period Length] パラメータで定義された時間の経過中に発生したログインエラーの数を表示します。[Quiet Period Length] は、[Security] > [Login Settings] ページで設定された秒単位の値です。

ログインエラーテーブルには、次の項目が表示されます。

- [Username]：ユーザーの名前
- [IP Address]：ユーザーの IP アドレス
- [Service]：使用されているサービス。これは、HTTP、HTTPS、Telnet、SSH、またはSNMPのいずれかです。
- [Count]：試行されたログインエラーの数。
- [Most Recent Attempt Time]：失敗したログインが試行された最近の時間。

キー管理

このセクションでは、RIPなど、アプリケーションやプロトコルのキーチェーンの設定方法について説明します。

キーチェーン設定

新しいキー チェーンを作成するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Key Management] > [Key Chain Settings] をクリックします。

ステップ 2 新しいキー チェーンを追加するには、[Add] をクリックして [Add Key Chain] ページを開き、次のフィールドに入力します。

- [Key Chain]：キーチェーンの名前。
- [Key Identifier]：キーチェーンを識別する整数の ID。
- [Key String]：キーチェーンストリングの値。次のいずれかのオプションを入力します。
  - [User Defined (Encrypted)]：暗号化バージョンを入力します。
  - [User Defined (Plaintext)]：プレーンテキストバージョンを入力します。

    （注）
    [Accept Life Time] と [Send Life Time] の両方の値を入力することができます。[Accept Life Time] は、受信しているパケットのキー識別子が有効な場合に表示されます。[Send Life Time] は、送信しているパケットのキー識別子が有効な場合に表示されます。

- [Accept Life Time/Send Life Time]：このキーを含むパケットが受け入れられる時点を指定します。次のオプションのいずれかを選択します。
  - [Always Valid]：キー識別子の存続期間に制限はありません。
  - [User Defined]：キーチェーンの存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。

    （注）
    [User Defined] を選択すると、システム時刻を手動で設定するか、または SNTP から設定する必要があります。そうしないと、[Accept Life Time] と [Send Life Time] は常に失敗します。

    次のフィールドは、[Accept Life Time] フィールドと [Send Life Time] フィールドに関係しています。

- [Start Date]：キー識別子が有効になる最も早い日付を入力します。
- [Start Time]：[Start Date] において、キー識別子が有効になる最も早い時刻を入力します。
- [End Time]：キー識別子が有効である最後の日付を指定します。次のオプションのいずれかを選択します。
  - [Infinite]：キー識別子の存続期間に制限はありません。

- [Duration]：キー識別子の存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。

- [Duration]：キー識別子が有効である時間の長さ。次のフィールドに入力します。
  - [Days]：キー識別子が有効である日数。
  - [Hours]：キー識別子が有効である時間数。
  - [Minutes]：キー識別子が有効である分数。
  - [Seconds]：キー識別子が有効である秒数。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

キー設定

既存のキー チェーンにキーを追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Key Management] > [Key Settings] をクリックします。
ステップ 2 新しいキー文字列を追加するには、[Add] をクリックします。
ステップ 3 次のフィールドに入力します。

- [Key Chain]：キーチェーンの名前。
- [Key Identifier]：キーチェーンを識別する整数の ID。
- [Key String (Encrypted)]：キーチェーン文字列の値。次のいずれかのオプションを入力します。
  - [User Defined (Encrypted)]：暗号化バージョンを入力します。
  - [User Defined (Plaintext)]：プレーンテキストバージョンを入力します。
- [Accept Life Time]：このキーを含むパケットがいつ受け入れられるかを指定します。次のオプションのいずれかを選択します。
  - [Always Valid]：キー識別子の存続期間に制限はありません。
  - [User Defined]：キーチェーンの存続期間には制限があります。このオプションを選択した場合は、下の [Start Date] と [Start Time] に値を入力します。
- [Start Date]：キー識別子が有効になる最も早い日付を入力します。
- [Start Time]：[Start Date] において、キー識別子が有効になる最も早い時刻を入力します。

- [End Time]：キー識別子が有効である最後の時刻を指定します。次のオプションのいずれかを選択します。
  - [Infinite]：キー識別子の存続期間に制限はありません。
  - [Duration]：キー識別子の存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。
- [Duration]：キー識別子が有効である時間の長さ。次のフィールドに入力します。
  - [Days]：キー識別子が有効である日数。
  - [Hours]：キー識別子が有効である時間数。
  - [Minutes]：キー識別子が有効である分数。
  - [Seconds]：キー識別子が有効である秒数。
- [Send Life Time]：このキーを含むパケットがいつ受け入れられるかを指定します。デフォルトのオプションをオンにします。
  - [Always Valid]：キー識別子の存続期間に制限はありません。
  - [Duration]：キー識別子の存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。
- [Start Date]：送信ライフタイムが有効な最も早い日付を入力します。
- [Start Time]：[Start Date] において、送信ライフタイムが有効な最も早い時刻を入力します。
- [End Time]：送信ライフタイムが有効な最後の時刻を指定します。次のオプションのいずれかを選択します。
  - [Infinite]：送信ライフタイムの有効期間が制限されません
  - [Duration]：送信ライフタイムの有効期間が制限されます。このオプションが選択されている場合は、次のフィールドに値を入力します。
    - [Days]：キー識別子が有効である日数。
    - [Hours]：キー識別子が有効である時間数。
    - [Minutes]：キー識別子が有効である分数。
    - [Seconds]：キー識別子が有効である秒数。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

管理アクセス方式

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

このセクションでは、さまざまな管理方式のアクセス ルールについて説明します。

アクセスプロファイルにより、さまざまアクセス方式でデバイスにアクセスしているユーザの認証および認可方法が決まります。アクセスプロファイルは、特定の送信元からの管理アクセスを制限できます。

アクティブなアクセスプロファイルおよび管理アクセス認証方式の両方にパスしたユーザにのみ、デバイスへの管理アクセスが付与されます。

デバイスでは一度に 1 つのアクセス プロファイルのみアクティブにできます。

アクセス プロファイルは 1 つまたは複数のルールで構成されます。ルールは、アクセス プロファイル内の優先順位の順序（上から下）で実行されます。

ルールは、次の要素を含むフィルタで構成されます。

- [Access Methods]：デバイスにアクセスして管理するための方式。
  - Telnet
  - セキュア Telnet（SSH）
  - Hypertext Transfer Protocol（HTTP）
  - セキュア HTTP（HTTPS）
  - Simple Network Management Protocol（SNMP）
  - All of the above
- [Action]：インターフェイスまたは送信元アドレスへのアクセスを許可するか拒否するか。
- [Interface]：Web ベースの設定ユーティリティへのアクセスを許可または拒否されるポート、LAG、または VLAN。
- [Source IP Address]：IP アドレスまたはサブネット。管理方式へのアクセスは、ユーザ グループ間で異なることがあります。たとえば、1 つのユーザ グループは HTTPS セッションを使用してのみデバイス モジュールにアクセスでき、別のユーザ グループは HTTPS と Telnet の両方のセッションを使用してデバイス モジュールにアクセスできる場合があります。

アクセスプロファイル

[Access Profiles] ページには定義されているアクセス プロファイルが表示されます。また、アクティブにする 1 つのアクセス プロファイルを選択することができます。

ユーザがアクセス方式を介してデバイスへのアクセスを試みると、デバイスは、この方式によるデバイスへの管理アクセスがアクティブなアクセスプロファイルによって明示的に許可されているかどうかをチェックします。一致するアクセスプロファイルが見つからない場合、アクセスは拒否されます。

デバイスへのアクセスの試みが、アクティブなアクセスプロファイルに違反している場合、デバイスは、システム管理者にそのアクセスの試みを警告する Syslog メッセージを生成します。

コンソール専用アクセスプロファイルをアクティブ化した場合、それを非アクティブにする唯一の方法は、管理ステーションからデバイスの物理コンソールポートに直接接続することです。

詳細については、プロファイル ルール （29 ページ）を参照してください。

[Access Profiles] ページを使用してアクセス プロファイルを作成し、最初のルールを追加します。アクセスプロファイルに 1 つのルールしか含めない場合は、それで終了です。プロファイルにルールを追加するには、[Profile Rules] ページを使用します。

手順

ステップ 1 [Security] > [Mgmt Access Method] > [Access Profiles] をクリックします。

ステップ 2 アクティブなアクセスプロファイルを切り替えるには、[Active Access Profile] ドロップダウンメニューからプロファイルを選択し、[Apply] をクリックします。

ステップ 3 アクティブ アクセス プロファイル変更を確認するポップアップが表示されます。[OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

ステップ 4 [Add] をクリックして、[Add Access Profile] ページを開きます。このページでは、新しいプロファイルと 1 つのルールを設定できます。

ステップ 5 [Access Profile Name] を入力します。名前は最大 32 文字で指定できます。

ステップ 6 パラメータを入力します。

- [ルールプライオリティ]：ルールのプライオリティを入力します。パケットがルールに一致した場合、ユーザ グループはデバイスへのアクセスを許可または拒否されます。パケットは最初の一致に基づき照合されるため、ルールの優先順位はパケットとルールのマッチングにとって重要です。最も高い優先順位は「1」です。
- [管理方式]：ルールの対象となるアクセス方式を選択します。次のオプションがあります。
  - [All]：すべての管理方式をこのルールに割り当てます。
  - Telnet：Telnetアクセスプロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。

- セキュア Telnet（SSH）（Secure Telnet (SSH)）：SSH アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- HTTP：HTTP アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。
- セキュア HTTP（HTTPS）（Secure HTTP (HTTPS)）：HTTPS アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- SNMP：SNMP アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。

- [アクション]：このルールに割り当てる処理を選択します。次のオプションがあります。
  - 許可（Permit）：ユーザがプロファイルの設定と一致している場合、デバイスへのアクセスを許可します。
  - [Deny]：ユーザーがプロファイルの設定に一致する場合、デバイスへのアクセスを拒否します。
- [インターフェイスに適用]：このルールに割り当てるインターフェイスを選択します。次のオプションがあります。
  - [All]：すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザー定義]:選択したインターフェイスに適用されます。
- [インターフェイス]：[ユーザー定義] を選択した場合は、インターフェイス番号を入 力します。
- [送信元 IP アドレスに適用]：このアクセス プロファイルに割り当てる送信元 IP アドレスのタイプを選択します。[Source IP Address] フィールドはサブネットワークに対して有効です。次のいずれかの値を選択します。
  - [All]：すべてのタイプの IP アドレスに適用されます。
  - [ユーザー定義]：フィールドで指定したタイプの IP アドレスだけが割り当てられ ます。
- IP バージョン（IP Version）：送信元 IP アドレスのバージョン（バージョン 6 またはバージョン 4）を入力します。
- [IP アドレス]：送信元 IP アドレスを入力します。
- [マスク]：送信元 IP アドレスに対するサブネット マスクの形式を選択し、いずれか のフィールドに値を入力します。
  - ネットワーク マスク（Network Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - プレフィックス長（Prefix Length）：プレフィックス長を選択し、送信元 IP アドレス プレフィックスを構成するビットの数を入力します。

ステップ 7 [Apply] をクリックします。アクセス プロファイルが実行コンフィギュレーション ファイルに書き込まれます。これで、このアクセス プロファイルをアクティブなアクセス プロファイルとして選択できます。

プロファイル ルール

アクセスプロファイルには、デバイスの管理とアクセスが許可されているユーザ、および使用される可能性があるアクセス方式を判断するための最大128個のルールを含めることができます。アクセスプロファイル内の各ルールには、照合するためのアクションと条件（1つ以上のパラメータ）が含まれています。各ルールには優先順位があり、優先順位が一番低いルールが最初にチェックされます。着信パケットがルールと一致すると、そのルールに関連付けられたアクションが実行されます。アクティブなアクセスプロファイル内で一致するルールが見つからない場合、そのパケットはドロップされます。

たとえば、IT 管理センターに割り当てられている IP アドレスを除くすべての IP アドレスからデバイスへのアクセスを制限することができます。この方法でもデバイスは管理でき、追加のセキュリティ レベルを得ることができます。

プロファイルルールをアクセスプロファイルに追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Mgmt Access Method] > [Profile Rules] の順にクリックします。

ステップ 2 [Filter] フィールドで、アクセス プロファイルを選択します。[Go] をクリックします。

選択したアクセス プロファイルがプロファイル ルール テーブルに表示されます。

ステップ 3 [Add] をクリックしてルールを追加します。

ステップ 4 パラメータを入力します。

- [アクセスプロファイル名] : アクセス プロファイルを選択します。
- [ルールプライオリティ] : ルールのプライオリティを入力します。パケットがルールに一致した場合、ユーザ グループはデバイスへのアクセスを許可または拒否されます。パケットは最初の一致に基づき照合されるため、ルールの優先順位はパケットとルールのマッチングにとって重要です。
- [管理方式] : ルールの対象となるアクセス方式を選択します。次のオプションがあります。
  - [All] : すべての管理方式をこのルールに割り当てます。
  - Telnet：Telnetアクセスプロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
  - セキュア Telnet（SSH）（Secure Telnet (SSH)）：Telnet アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
  - [HTTP] : HTTPアクセスをこのルールに割り当てます。デバイスへのアクセスを要求しているユーザーがHTTPアクセスプロファイル基準を満たす場合、そのユーザーは許可または拒否されます。

- セキュア HTTP（HTTPS）（Secure HTTP (HTTPS)）：HTTPS アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- SNMP：SNMP アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。

- [Action]：次のいずれかのオプションを選択します。
  - 許可（Permit）：このルールに定義されているインターフェイスと IP ソースからのユーザに対するデバイス アクセスを許可します。
  - 拒否（Deny）：このルールに定義されているインターフェイスと IP ソースからのユーザに対するデバイス アクセスを拒否します。
- [インターフェイスに適用]：このルールに割り当てるインターフェイスを選択します。次のオプションがあります。
  - [All]：すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザー定義]：選択したポート、VLAN、または LAG が割り当てられます。
- [Interface]：前述のフィールドで [User Defined] オプションを選択した場合は、インターフェイス番号を入力します。
- [送信元 IP アドレスに適用]：このアクセス プロファイルに割り当てる送信元 IP アドレスのタイプを選択します。[Source IP Address] フィールドはサブネットワークに対して有効です。次のいずれかの値を選択します。
  - [All]：すべてのタイプの IP アドレスに適用されます。
  - [ユーザー定義]：フィールドで指定したタイプの IP アドレスだけが割り当てられ ます。
- [IP バージョン]：送信元 IP アドレスのサポート対象 IP バージョン（IPv6 またはIPv4）を選択します。
- [IP アドレス]：送信元 IP アドレスを入力します。
- [マスク]：送信元 IP アドレスに対するサブネット マスクの形式を選択し、いずれか のフィールドに値を入力します。
  - ネットワーク マスク（Network Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - プレフィックス長（Prefix Length）：プレフィックス長を選択し、送信元 IP アドレス プレフィックスを構成するビットの数を入力します。

ステップ 5 [Apply] をクリックすると、ルールがアクセスプロファイルに追加されます。

管理アクセス認証

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SSH、Telnet、HTTP、HTTPSなど、さまざまな管理アクセス方式に認証方式を割り当てることができます。認証処理は、ローカルで、またはサーバーで実行可能です。

認可が有効になっている場合は、ユーザのアイデンティティと読み取り/書き込み権限の両方が検証されます。承認処理が有効になっていない場合、ユーザーの ID だけが検証されます。

使用される認可および認証方式は、認証方式の選択順序によって決まります。最初に選択した認証方式が使用不能の場合、次に選択した認証方式が使用されます。たとえば、[RADIUS]、[Local] の順に認証方式を選択した場合、設定されたすべての RADIUS サーバーに対してプライオリティ順にクエリが送られて応答がなければ、ユーザーはローカルに承認/認証されます。

認可が有効になっていて、認証方式が失敗した場合、またはユーザーの権限レベルが不十分な場合、ユーザーはデバイスへのアクセスを拒否されます。つまり、ある認証方式で認証に失敗した場合、デバイスは認証の試行を停止します（そのまま続行して次の認証方式を使用することはありません）。

同様に、承認処理が無効になっていて、ある方式で認証に失敗した場合、デバイスは認証の試行を停止します。

アクセス方式の認証方式を定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Management Access Authentication] をクリックします。

ステップ 2 管理アクセス方式の [Application]（タイプ）を入力します。

ステップ 3 [Authorization] を選択し、後述の方式の一覧から選択して、ユーザの認証と認可の両方を有効にします。フィールドが選択されていない場合は、認証のみ実行されます。認可が有効になっている場合、ユーザの読み取り/書き込み権限がチェックされます。この権限レベルは、[User Accounts] ページで設定します。

ステップ 4 矢印を使用して、[Optional Methods] 列と [選択した方式（Selected Methods] 列の間で認証方式を移動させます。最初に選択した方式が最初に使用される方式です。

- RADIUS：ユーザは RADIUS サーバで認可および認証されます。1 つまたは複数の RADIUS サーバを設定しておく必要があります。Web ベースの設定ユーティリティへのアクセス権限が RADIUS サーバーによって付与されるようにするには、RADIUS サーバーが RADIUS 属性「Service-Type 6」値「Administrative」を返す必要があります。
- TACACS+：ユーザは TACACS+ サーバで認可および認証されます。1 つまたは複数の TACACS+ サーバを設定しておく必要があります。
- None（なし）：ユーザは認可も認証もされなくてもデバイスにアクセスできます。

- ローカル（Local）：ローカルデバイスに保存されたデータと照らしてユーザ名とパスワードがチェックされます。ユーザ名とパスワードのペアは [User Accounts] ページで定義します。

（注）
認証方式の [Local] または [None] は、常に最後に選択する必要があります。[Local] または [None] の後に選択して認証方式はすべて無視されます。

ステップ 5 [Apply] をクリックします。選択した認証方式がアクセス方式と関連付けられます。

セキュア センシティブ データ管理

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SSD は、デバイスの機密データ（パスワードやキーなど）の保護、ユーザー資格情報および SSD ルールに基づき暗号化された機密データや機密データへのプレーンテキストでのアクセスの許可/拒否、機密データを含むコンフィギュレーション ファイルの改ざんからの保護を実施します。

さらに SSD では、機密データを含むコンフィギュレーション ファイルのセキュアなバックアップと共有を可能にします。

SSD により、機密データの保護レベルを目的に合わせて柔軟に設定できます。機密データの保護レベルには、保護のないプレーンテキストから、デフォルトのパスフレーズに基づく暗号化による最小限の保護、ユーザー定義のパスフレーズに基づく暗号化によるセキュアな保護まであります。

SSD は、SSD 規則に従って、認証された承認済みのユーザにのみ、センシティブ データへの読み取りアクセス許可を付与します。デバイスは、ユーザ認証プロセスを通じて、ユーザに対する管理アクセスを認証および承認します。

SSD を使用しているかどうかにかかわらず、管理者は、ローカル認証データベースを使用して認証プロセスの安全性を確保したり、ユーザー認証プロセスで使用される外部認証サーバーへの通信の安全性を確保したりすることが推奨されます。

すなわち SSD は、SSD ルール、SSD プロパティ、およびユーザー認証を使用してデバイスの機密データを保護するものです。さらに、デバイスの SSD 規則、SSD プロパティ、およびユーザ認証の設定は、それ自体が SSD によって保護されているセンシティブ データです。

SSD プロパティ

SSD プロパティは、SSD 規則を使用してデバイスの SSD 環境を定義および制御する一連のパラメータです。SSD 環境は、次のようなプロパティで構成されています。

- センシティブ データを暗号化する方法を制御する。

- コンフィギュレーション ファイルのセキュリティの強度を制御する。
- 現在のセッション内で機密データを表示する方法を制御する。

SSD プロパティを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Secure Sensitive Data Management] > [Properties] の順にクリックします。

次のフィールドが表示されます。

- 現在のローカル パスフレーズ タイプ（Current Local Passphrase Type）：現在、デフォルト パスフレーズまたはユーザ定義のパスフレーズのいずれが使用されているかが表示されます。

ステップ 2 [Configuration File Passphrase Control]：次のオプションを選択します。

- 無制限（Unrestricted）（デフォルト）：設定ファイルを作成するときに、デバイスはそのパスフレーズを含めます。これによって、デバイスは設定ファイルを受け入れ、ファイルからパスフレーズを学習できます。
- 制限付き（Restricted）：デバイスは、パスフレーズが設定ファイルにエクスポートされるのを制限します。制限モードは、構成ファイルの暗号化された機密データをパスフレーズがないデバイスから保護します。ユーザーが構成ファイルでパスフレーズを公開したくない場合には、このモードを使用する必要があります。

ステップ 3 次に、[Configuration File Integrity Control] を有効にします。

ステップ 4 現在のセッションの読み取りモードを選択します。

- [Plaintext]：ユーザーはプレーンテキストの機密データにのみアクセスを許可されます。ユーザーには SSD パラメータへの読み取り権限と書き込み権限も付与されます。
- [Encrypted]：ユーザーは暗号化された機密データにのみアクセスを許可されます。

ステップ 5 [Change Local Passphrase] をクリックして、新しいローカルパスフレーズを入力します。

- デフォルト（Default）：デバイスのデフォルト パスフレーズを使用します。
- ユーザ定義（プレーン テキスト）（User Defined (Plaintext)）：新しいパスフレーズを入力します。最大文字数は 16 です。
- パスフレーズの確認（Confirm Passphrase）：新しいパスフレーズを確認します。

ステップ 6 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

SSDルール

SSD 読み取りアクセス許可が [Plaintext-only] または [Both] のユーザのみが、SSD 規則を設定できます。

SSD ルールを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Secure Sensitive Data Management] > [SSD Rules] の順にクリックします。

現在、定義されている規則が表示されます。[Rule Type] フィールドは、規則がユーザ定義の規則であるか、またはデフォルトの規則であるかを示します。

ステップ 2 新しい規則を追加するには、[Add] をクリックします。次のフィールドに入力します。

- ユーザ（User）：規則が適用されるユーザを定義します。次のオプションのいずれかを選択します。
  - 特定のユーザ（Specific User）：選択して、この規則が適用される特定のユーザ名を入力します（このユーザは必ずしも定義されている必要はありません）。
  - 既定のユーザ（cisco）（Default User (cisco)）：この規則は既定のユーザに適用されることを示します。
  - レベル 15（Level 15）：この規則は、権限レベル 15 を持つすべてのユーザに適用されることを示します。
  - すべて（All）：この規則は、すべてのユーザに適用されることを示します。
- チャネル（Channel）：規則が適用される入力チャネルのセキュリティ レベルを定義します。次のオプションのいずれかを選択します。
  - セキュア（Secure）：この規則は、SNMP および XML チャネルを含まない、セキュア チャネル（コンソール、SCP、SSH、HTTPS）のみに適用されることを示します。
  - [Insecure]：ルールが、セキュアでないチャネル（Telnet、TFTP および HTTP）にのみ適用されることを示します。SNMP と XML チャネルは含みません。
  - セキュア XML SNMP（Secure XML SNMP）：この規則が HTTPS またはプライバシー保護付きの SNMPv3 経由の XML にのみ適用されるように指定します。
  - 非セキュア XML SNMP（Insecure XML SNMP）：この規則が HTTP または SNMPv1/v2 およびプライバシー保護なしの SNMPv3 経由の XML にのみ適用されるように指定します。
- 読み取りアクセス許可（Read Permission）：読み取りアクセス許可と規則を関連付けます。有効な値は次のとおりです。
  - [Exclude]：最も低い読み取りアクセス許可。ユーザはいかなる形式でも、センシティブ データの取得は許可されません。

- プレーン テキストのみ（Plaintext Only）：上記より高い読み取りアクセス許可です。ユーザは、プレーン テキストのみのセンシティブ データの取得が許可されます。
- 暗号化のみ（Encrypted Only）：中程度の読み取りアクセス許可です。ユーザは、暗号化のみのセンシティブ データの取得が許可されます。
- 両方（プレーン テキストと暗号化）（Both (Plaintext and Encrypted)）：最高の読み取りアクセス許可です。ユーザは暗号化およびプレーン テキストの両方のアクセス許可を保持し、暗号化形式とプレーン テキストのセンシティブ データの取得が許可されます。

- デフォルト読み取りモード（Default Read Mode）：すべてのデフォルト読み取りモードは、規則の読み取りアクセス許可に従います。次のオプションが存在しますが、規則の読み取りアクセス許可に応じて、一部は拒否されることがあります。
  - 除外（Exclude）：センシティブ データの読み取りを許可しません。
  - 暗号化（Encrypted）：センシティブ データは暗号化形式で表示されます。
  - プレーン テキスト（Plaintext）：センシティブ データはプレーン テキストで表示されます。

ステップ 3 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 4 選択した規則に対して、次のアクションを実行できます。

- ルールの [追加]、[編集]、もしくは [削除]、または [デフォルトへの復元]。
- すべての規則をデフォルトに復元（Restore All Rules to Default）：ユーザが変更したデフォルト規則をデフォルト規則に復元します。

SSL Server

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

セキュア ソケット レイヤ（SSL）機能は、デバイスへの HTTPS セッションを開くために使用します。HTTPS セッションは、デバイス上に存在するデフォルト証明書で開くこともできます。デフォルトの証明書は証明機関（CA）によって署名されていないため、一部のブラウザではデフォルトの証明書を使用すると警告が表示されます。信頼できる CA によって署名された証明書を使用することをお勧めします。デフォルトでは、デバイスには変更可能な証明書が含まれています。HTTPS はデフォルトで有効になっています。

SSLサーバー認証設定

セキュアソケットレイヤ（SSL）認証は、ユーザーとサーバーがやり取りするためのセキュアな接続を作成するためのプロトコルです。サーバーとユーザーは、すべての Web インタラクションに関与します。ユーザーは、機密性の高い個人情報を Web サイトに入力することが多く、人やシステムが危険にさらされます。より適切な認証によって、特に金融、医療、または個人データを保存するサイトのセキュリティが強化されます。安定した、検証可能でセキュアなユーザーインタラクションが求められています。サーバーは、ユーザーが実在の人物であることを確認する手段として、情報を収集します。これはいくつかの方法で実行できます。

手順

ステップ 1 [Security] > [SSL Server] > [SSL Server Authentication Settings] の順にクリックします。

SSL サーバ キー テーブルに証明書 1 と 2 の情報が表示されます。フィールドは、次のフィールドを除いて [Edit] ページで定義されています。

- 有効期間の開始日（Valid From）：証明書の有効期間の開始日を指定します。
- 有効期間の終了日（Valid To）：証明書の有効期間の終了日を指定します。
- 証明書の生成元（Certificate Source）：証明書の生成元、システム（自動生成）またはユーザ（ユーザ定義）を指定します。

ステップ 2 デバイスには 2 つの証明書が含まれています。そのうちの 1 つだけが、HTTPS セッションに使用できるアクティブな証明書です。どちらがアクティブな証明書かを定義するには、[SSL Active Certificate Number] で、アクティブな証明書（**1** または **2**）を選択します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [HTTPS Session Logging] セクションで、[Enable] をオンにして有効にします。HTTPS セッションロギングを有効にすることにより、ユーザーは、デバイスによって生成された syslog メッセージを介して、HTTPS セッションのセットアップと切断の進行状況を追跡できます。

ステップ 5 [Apply] をクリックします。

証明書要求の生成

デバイスにある証明書を置換するために、新しい自己署名証明書が必要になる場合があります。新しい証明書を作成するには、次の手順を実行します。

手順

ステップ 1 [Generate Certificate Request] をクリックします。

ステップ 2 次に、次のフィールドに入力します。

- [Certificate ID]：証明書 ID を選択します。
- [Regenerate RSA Key]：チェックボックスを選択して、RSA キーを再生成します。
- [Key Length]：2 つのオプション（2048 ビットまたは 3072 ビット）のいずれかからキーの長さを選択します。
- [Common Name]：証明書の名前を入力します。
- [Organization Unit]：組織単位を入力します。
- [Organization Name]：組織名を入力します。
- [Location]：場所または市町村名を入力します。
- [State]：州/都道府県を入力します。
- [Country]：国の名前を入力します。
- [Certificate Request]：証明書要求の開始が表示されます。
- [Duration]：証明書が有効な日数が表示されます。（範囲は 30 ～ 1095 日、デフォルトは 730 日です。）

（注）
[Duration] フィールドは、既存の証明書を編集しようとした場合にのみ表示されます。

ステップ 3 [Generate Certificate Request] をクリックします。新しい証明書が生成され、既存の証明書が置き換えられます。

ステップ 4 CA によって署名された証明書をインポートするには、アクティブな証明書を選択し、[Import Certificate] をクリックします。

ステップ 5 次のフィールドに入力します。

- [Certificate ID]：証明書を選択します。
- [Certificate Source]：自動生成された証明書であることを表示します。
- 証明書（Certificate）：受信した証明書にコピーされます。
- [Import RSA Key-Pair]：新しい RSA キーペアへのコピーを有効にするには、このフィールドを選択します。
- 公開キー（Public Key）：RSA 公開キーにコピーされます。
- [Private Key (Encrypted)]：暗号化形式で RSA 秘密キーをコピーするには、このフィールドを選択します。
- [Private Key (Plaintext)]：プレーンテキスト形式で RSA 秘密キーをコピーするには、このフィールドを選択します。

ステップ 6 [Apply] をクリックして、変更内容を実行コンフィギュレーションに適用します。

ステップ 7 [Details] ボタンをクリックして、SSL 証明書の詳細を表示します。

ステップ 8 次に、[Display Sensitive Data as Encrypted] をクリックして、このキーを暗号化して表示します。このボタンをクリックすると、（[Apply] をクリックしたときに）秘密キーが暗号化された形式で設定ファイルに書き

込まれます。テキストが暗号化された形式で表示されると、ボタンが [Display Sensitive Data As Plaintext] に変わり、再びプレーン テキストでテキストを表示できるようになります。

次のタスク

証明書チェーンの表示

デバイス証明書が CA ルート認証局ではなく中間 CA 認証局によって署名されている場合、ユーザーはデバイス証明書の署名に使用された中間証明書と、ルート証明書までのチェーン内の各証明書をインポートする必要があります。中間証明書は、[CA Certificate Settings] を使用してインポートできます。この証明書チェーンを表示するには、SSL サーバーキーテーブルから証明書 1 または 2 を選択し、[Certificate Chain] をクリックします。これにより、[Certificate Chain] モーダルが開き、デバイス証明書とデバイス証明書チェーンの中間証明書部分が表示されます。

SSL サーバーキーテーブルには、[Delete] ボタンがあります。[Delete] ボタンを使用すると、ユーザーがインポートした証明書を削除できます。ただし、自動生成された証明書は削除できません。

自己署名証明書の更新

自己署名証明書を更新するには、次の手順を実行します。

手順

ステップ 1 更新する証明書を選択して [Edit] をクリックします。

ステップ 2 次に、次のフィールドに入力します。

- [Certificate ID]：証明書 ID を選択します。
- [Regenerate RSA Key]：チェックボックスを選択して、RSA キーを再生成します。
- [Key Length]：2 つのオプション（2048 ビットまたは 3072 ビット）のいずれかからキーの長さを選択します。
- [Common Name]：証明書の名前を入力します。
- [Organization Unit]：組織単位を入力します。
- [Organization Name]：組織名を入力します。
- [Location]：場所または市町村名を入力します。
- [State]：州/都道府県を入力します。
- [Country]：国の名前を入力します。
- [Certificate Request]：証明書要求の開始が表示されます。

• [Duration]：証明書が有効な日数が表示されます。（範囲は 30 ～ 1095 日、デフォルトは 730 日です）

ステップ 3 [Generate] ボタンを押します。

SSH サーバ

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SSH サーバー機能を使用すれば、リモートユーザーは、デバイスに対して SSH セッションを確立することができます。これは、セッションがセキュリティで保護されていることを除いて、Telnet セッションの確立と同様です。

デバイスは、SSHサーバーとして、パスワードと公開キーのどちらかでリモートユーザーを認証する SSH ユーザー認証をサポートします。一方、リモートユーザーは、SSH クライアントとして、デバイス公開キー（フィンガープリント）を使用してデバイスを認証することでSSH サーバー認証を実行することができます。

SSH サーバには、次の動作モードがあります。

- [By Internally generated RSA/DSA Keys]（デフォルト設定）：RSA キーと DSA キーが生成されます。ユーザーは、SSH サーバーアプリケーションにログオンして、デバイスの IP アドレスを入力し、デバイス上でセッションを開こうとしたときに自動的に認証されます。
- [Public Key Mode]：ユーザはデバイスで定義されています。ユーザの RSA キーまたは DSA キーは、PuTTY などの外部 SSH サーバ アプリケーションで生成されます。公開キーはデバイスに入力されます。その後、ユーザは、外部 SSH サーバ アプリケーションを使用して、デバイスで SSH セッションを開くことができます。

SSH ユーザ認証

SSHユーザ認証ページを使用して、ローカルユーザデータベースにすでに設定されているユーザの SSH ユーザ名を作成する場合には、自動ログイン機能を設定することで、追加の認証を回避することができます。これは次のように動作します。

- [Enabled]：ユーザがローカルデータベースに定義されており、このユーザが公開キーを使用して SSH 認証をパスした場合、ローカル データベースのユーザ名とパスワードによる認証はスキップされます。

（注） このような特定の管理方法（コンソール、Telnet、SSH など）に設定されている認証方法はローカルである必要があります。

- [Not Enabled]：SSH 公開キーによる認証が成功したら、ユーザー名がローカルユーザーデータベース内で設定されている場合でも、設定された認証方式によってユーザーが再度認証されます。

認証を有効にして、ユーザを追加します。

手順

ステップ 1 [Security] > [SSH Server] > [SSH User Authentication] の順にクリックします。

ステップ 2 次のフィールドを選択します。

- [SSH User Authentication by Password]：ローカルデータベース内で設定されたユーザー名とパスワードを使用して SSH クライアントユーザーの認証を実行する場合に [Enable] を選択します。
- [SSH Session Logging]：[Enable] を選択すると、SSH セッションロギングが有効になります。SSH セッションロギングを使用すると、ユーザーは、デバイスによって生成された syslog メッセージを介して、SSH セッションのセットアップと切断の進行状況を追跡できます。
- [SSH User Authentication by Public Key]：公開キーを使用した SSH クライアントユーザーの認証を有効にする場合に [Enable] を選択します。
- [Automatic Login]：[SSH User Authentication by Public Key] 機能を有効にする場合に [Enable] を選択します。

ステップ 3 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

設定したユーザに関する次のフィールドが表示されます。

- [SSH User Name]：ユーザーのユーザー名
- [Key Type]：RSA キーまたは DSA キーのいずれであるかを示します。
- [Fingerprint]：公開キーから生成されたフィンガープリント

（注）
DSA キーは、FIPS 準拠モードではサポートされません。

ステップ 4 [Add or Edit] をクリックしてユーザーを追加または編集し、次のフィールドに値を入力します。

- [SSH User Name]：ユーザー名を入力します。
- [Key Type]：[RSA] または [DSA] のいずれかを選択します。
- [Public Key]：PuTTYなどの外部 SSH クライアント アプリケーションによって生成された公開キーをこのテキスト ボックスにコピーします。

ステップ 5 [Apply] をクリックして、新しいユーザーを保存します。

すべてのアクティブなユーザに関して、次のフィールドが表示されます。

- [IP Address]：アクティブユーザーの IP アドレス
- [SSH User Name]：アクティブユーザーのユーザー名
- [SSH Version]：アクティブユーザーが使用する SSH のバージョン
- [Cypher]：アクティブユーザーの暗号
- [Authentication Code]：アクティブユーザーの認証コード

SSH サーバ認証

リモート SSH クライアントは、SSH サーバー認証を実行することによって、想定された SSH ドライバへの SSH セッションが確立されるようにします。SSH サーバー認証を実行するには、リモート SSH クライアントにターゲット SSH サーバーの SSH サーバー公開キー（またはフィンガープリント）のコピーが保存されている必要があります。

[SSH Server Authentication] ページで、SSH サーバーとしてのデバイスの秘密/公開キーが生成/インポートされます。ユーザーは、SSH セッションで SSH サーバー認証を実行する場合に、このデバイスの SSH サーバー公開キー（またはフィンガープリント）をアプリケーションにコピーする必要があります。RSA と DSA の公開キーと秘密キーは、デバイスを工場出荷時の初期状態でブートすると自動的に生成されます。これらのキーは、適切なユーザ設定キーをユーザが削除した場合にも自動的に作成されます。

RSA キーまたは DSA キーを再生成、または別のデバイスで生成された RSA キーまたは DSA キーをコピーするには、次の手順を実行します。

（注） DSA キーは、FIPS 準拠モードではサポートされません。

手順

ステップ 1 [Security] > [SSH Server] > [SSH Server Authentication] の順にクリックします。

[Fingerprint] セクションのキーごとに次のフィールドが表示されます。

- [Key Type]：RSA または DSA。
- [Key Source]：自動生成またはユーザ定義。
- [Fingerprint]：キーから生成されるフィンガープリント。

ステップ 2 RSA キーまたは DSA キーのいずれかを選択します。

ステップ 3 次のいずれかのアクションを実行できます。

- [Generate]：選択した種類のキーを生成します。
- [Edit]：別のデバイスからキーをコピーすることができます。次のフィールドに入力します。
  - [Key Type]：前述のとおりです。
  - [Public Key]：公開キーを入力します。
  - [Private Key]：[Plaintext] または [Encrypted] のいずれかを選択して、秘密キーを入力します。

    [Plaintext]：プレーンテキストとしてキーを入力します。
  - [Apply] をクリックして設定を保存します。
- [Delete]：キーを削除できるようにします。

  （注）
  自動生成されたキーは削除できません。
- [Details]：生成されたキーを表示できるようにします。[Details] ウィンドウでは、[Display Sensitive Data as Plaintext] をクリックすることもできます。これをクリックすると、キーが暗号化された形式ではなく、プレーンテキストで表示されます。キーがすでに平文で表示されている場合は、[Display Sensitive Data as Encrypted] をクリックできます。暗号化された形式でテキストを表示します。

SSH クライアント

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SSH クライアントによりユーザーは、ネットワークが 1 つ以上のスイッチで構成されていて、さまざまなシステムファイルが 1 つの中央 SSH サーバーに保管されている場合に、ネットワークの管理作業を実行できます。ネットワークを通じて構成ファイルが転送される際、SSH プロトコルを利用するアプリケーションの 1 つであるセキュアコピー（SCP）により、ユーザー名/パスワードなどの機密データが盗まれないことが保証されます。

SSH クライアントは、信頼できる SSH サーバーとのみ通信します。SSH サーバ認証が無効になっている場合（デフォルト設定）、SSH サーバは信頼できるものと見なされます。SSH サーバ認証を有効にすると、ユーザは、信頼できるサーバのエントリを信頼できる SSH サーバテーブルに追加する必要があります。

一般に、SSH プロトコルはファイル転送と端末アクセスの 2 つの目的に使用できます。

SSH ユーザ認証

デバイス（SSH クライアント）が SSH サーバへの SSH セッションの確立を試行した場合、SSH サーバはクライアントを認証するためにさまざまな方式を使用します。パスワード方式が選択されている場合は、このページを使用して、SSH ユーザ認証方式を選択し、ユーザ名とパスワードをデバイスに設定するか、または、公開/秘密キー方式が選択されている場合は、RSA キーまたは DSA キーを生成使用します。

（注） DSA キーは、FIPS 準拠モードではサポートされません。

認証方式を選択し、ユーザー名/パスワード/キーを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [SSH Client] > [SSH User Authentication] の順にクリックします。

ステップ 2 [Global Configuration] で、[SSH User Authentication Method] を選択します。これは、Secure Copy（SCP）に定義されるグローバル方式です。次のいずれかのオプションを選択します。

- [By Password]：これはデフォルトの設定です。これが選択されている場合は、パスワードを入力するか、またはデフォルト パスワードを保持します。
- [By RSA Public Key]：これが選択されている場合は、[SSH User Key Table] ブロックで、RSA 公開キーと秘密キーを作成します。
- [By DSA Public Key]：これが選択されている場合は、[SSH User Key Table] ブロックで、DSA 公開キーと秘密キーを作成します。

ステップ 3 [Credentials] で、（どの方式が選択されている場合でも）[Username] を入力するか、またはデフォルトのユーザー名をそのまま使用します。これは、SSH サーバで定義されているユーザ名と一致している必要があります。

ステップ 4 [By Password] 方式が選択された場合は、パスワードを入力するか（[Encrypted] または [Plaintext] 形式）、またはデフォルトの暗号化パスワードのままにします。

ステップ 5 次のいずれかの操作を実行します。

- 適用（Apply）：選択した認証方式がアクセス方式に関連付けられます。
- デフォルトのクレデンシャルを復元（Restore Default Credentials）：デフォルトのユーザ名とパスワード（anonymous）を復元します。
- センシティブ データをプレーン テキストとして表示（Display Sensitive Data As Plaintext）：現在のページのセンシティブ データがプレーン テキストとして表示されます。

  [SSH User Key Table] には、各キーの次のフィールドが含まれています。

- [Key Type]：RSA または DSA。

- [Key Source]：自動生成またはユーザ定義。
- [Fingerprint]：キーから生成されるフィンガープリント。

ステップ 6 RSA または DSA キーを処理するには、RSA または DSA のどちらかを選択して、次のアクションのいずれかを実行します。

- [Generate]：新しいキーを生成します。
- [Edit]：別のデバイスにコピー/貼り付けするためのキーを表示します。
- [Delete]：キーを削除します。
- [Details]：各 SSH サーバータイプの公開キーと秘密キー（暗号化）が表示されます。

（注）
公開/秘密キーは暗号化され、デバイスのメモリに保存されます。キーはデバイス コンフィギュレーション ファイルの一部であり、秘密キーは暗号化形式またはプレーン テキスト形式でユーザに表示できます。

SSH サーバ認証

SSH サーバー認証を有効にし、信頼できるサーバーを定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [SSH Client] > [SSH Server Authentication] の順にクリックします。

ステップ 2 [Enable] を選択し、SSH サーバ認証を有効にします。

- IPv4 送信元インターフェイス（IPv4 Source Interface）：IPv4 SSH サーバとの通信で使用されるメッセージの送信元 IPv4 アドレスとして使用される IPv4 アドレスを保持している送信元インターフェイスを選択します。
- IPv6 送信元インターフェイス（IPv6 Source Interface）：IPv6 SSH サーバとの通信で使用されるメッセージの送信元 IPv6 アドレスとして使用される IPv6 アドレスを保持している送信元インターフェイスを選択します。

（注）
自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [追加] をクリックし、信頼済み SSH サーバーについての下記フィールドに入力します。

- サーバ定義（Server Definition）：SSH サーバを特定するための方法として、次のいずれかを選択します。

- IP アドレスによる（By IP address）：これが選択されている場合は、下のフィールドにサーバの IP アドレスを入力します。
- 名前による（By name）：これが選択されている場合は、[Server IP Address/Name] フィールドにサーバの名前を入力します。

- IP バージョン（IP Version）：IP アドレスで SSH サーバを指定するように選択した場合は、その IP アドレスが IPv4 または IPv6 アドレスのどちらであるかを選択します。
- IPv6 アドレス タイプ（IPv6 Address Type）：SSH サーバの IP アドレスが IPv6 アドレスの場合は、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、単一ネットワークリンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- リンク ローカル インターフェイス（Link Local Interface）：インターフェイスのリストからリンク ローカル インターフェイスを選択します。
- サーバ IP アドレス/名前（Server IP Address/Name）：[Server Definition] での選択に応じて、SSH サーバの IP アドレスまたはその名前のいずれかを入力します。
- フィンガープリント（Fingerprint）：SSH サーバの（そのサーバからコピーされた）フィンガープリントを入力します。

ステップ 5 [Apply] をクリックします。信頼できるサーバ定義は、実行コンフィギュレーション ファイルに保存されます。

SSHサーバーのユーザーパスワードの変更

SSH クライアントサーバーでパスワードを変更すると、リモート SSH サーバーにのみ影響します。SSH サーバーのパスワードを変更するには、次の手順を実行します。

手順

ステップ 1 [Security] > [SSH Client] > [Change User Password on SSH Server] をクリックします。

ステップ 2 次のフィールドに入力します。

- サーバ定義（Server Definition）：[By IP Address] または [By Name] のいずれかを選択して、SSH サーバを定義します。[Server IP Address/Name] フィールドにサーバのサーバ名または IP アドレスを入力します。
- IP バージョン（IP Version）：IP アドレスで SSH サーバを指定するように選択した場合は、その IP アドレスが IPv4 または IPv6 アドレスのどちらであるかを選択します。
- IPv6 アドレス タイプ（IPv6 Address Type）：SSH サーバの IP アドレスが IPv6 アドレスの場合は、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能なグローバルユニキャスト IPv6 タイプになります。
- リンク ローカル インターフェイス（Link Local Interface）：インターフェイスのリストからリンク ローカル インターフェイスを選択します。
- サーバ IP アドレス/名前（Server IP Address/Name）：[Server Definition] での選択に応じて、SSH サーバの IP アドレスまたはその名前のいずれかを入力します。
- ユーザ名（Username）：これは、サーバ上のユーザ名と一致している必要があります。
- 古いパスワード（Old Password）：これは、サーバ上のパスワードと一致している必要があります。
- 新しいパスワード（New Password）：新しいパスワードを入力し、[Confirm Password] フィールドでそれを確定します。

ステップ 3 [Apply] をクリックします。SSH サーバのパスワードが変更されます。

TCP/UDPサービス

[TCP/UDP Services] ページでは、デバイス上で TCP または UDP ベースのサービスを有効にできます（通常はセキュリティの理由により行う）。

デバイスには次の TCP/UDP サービスがあります。

- HTTP：出荷時設定では有効
- HTTPS：出荷時設定では有効
- SNMP：出荷時設定では無効
- Telnet：出荷時設定では有効

• SSH：出荷時設定では無効

TCP/UDP サービスを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [TCP/UDP サービス（TCP/UDP Services] をクリックします。

ステップ 2 表示されたサービスで、次の TCP/UDP サービスを有効化または無効化します。

- [HTTP Service]：HTTP サービスが有効/無効のどちらになっているかを示します。
- [HTTPS Service]：HTTPS サービスが有効/無効のどちらになっているかを示します。
- [SNMP Service]：SNMP サービスが有効/無効のどちらになっているかを示します。
- [Telnet Service]：Telnet サービスが有効/無効のどちらになっているかを示します。
- [SSH Service]：SSH サーバー サービスが有効/無効のどちらになっているかを示します。

ステップ 3 [Apply] をクリックします。サービスが実行コンフィギュレーション ファイルに書き込まれます。

TCP サービス テーブルには、サービスごとに次のフィールドが表示されます。

- [Service Name]：TCP サービスを提供するためにデバイスが使用するアクセス方式。
- [Type]：サービスが使用する IP プロトコル。
- [Local IP Address]：サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [Local Port]：サービスを提供するためにデバイスが使用するローカル TCP ポート。
- [Remote IP Address]：サービスを要求しているリモートデバイスの IP アドレス。
- [Remote Port]：サービスを要求しているリモートデバイスの TCP ポート。
- [State]：サービスの状態。

UDP サービス テーブルには、次の情報が表示されます。

- [Service Name]：UDP サービスを提供するためにデバイスが使用するアクセス方式。
- [Type]：サービスが使用する IP プロトコル。
- [Local IP Address]：サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [Local Port]：サービスを提供するためにデバイスが使用するローカル UDP ポート。
- [Application Instance]：UDP サービスのサービスインスタンス。

ストーム制御

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

ブロードキャスト、マルチキャスト、または不明なユニキャストフレームを受信した場合、それらのフレームが重複していると、すべての可能な出力ポートにコピーが送信されます。つまり、実際には、関連するVLANに属しているすべてのポートに送信されます。この方法では、1つの入力フレームが多数のポートに送信され、トラフィック ストームが発生する可能性が生まれます。

ストームプロテクションを使用すると、デバイスに入るフレーム数を制限して、この制限に対してカウントされるフレームの種類を定義できます。

ブロードキャスト、マルチキャスト、または不明なユニキャストフレームのレートがユーザ定義のしきい値よりも高い場合、しきい値を超えた受信フレームは破棄されます。

ストーム制御の設定

ストーム制御を定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Storm Control] > [Storm Control Settings] をクリックします。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：ストーム制御が有効になっているポートを選択します。

  不明なユニキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、ユニキャスト パケットのストーム制御を有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

  マルチキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、マルチキャスト パケットのストーム制御を有効にします。
- マルチキャスト タイプ（Multicast Type）：ストーム制御を実装するマルチキャスト パケットの種類を次から 1 つ選択します。
  - すべて（All）：ポート上のすべてのマルチキャスト パケットでストーム制御を有効にします。
  - 登録済みマルチキャスト（Registered Multicast）：ポート上の登録済みマルチキャスト アドレスでのみストーム制御を有効にします。
  - 未登録のマルチキャスト（Unregistered Multicast）：ポート上の未登録のマルチキャストでのみストーム制御を有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

ブロードキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、ブロードキャスト パケットのストーム制御を有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

ステップ 4 [Apply] をクリックします。ストーム制御が変更されて、実行コンフィギュレーション ファイルが更新されます。

ストーム制御統計情報

ストーム制御統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Storm Control] > [Storm Control Statistics] の順にクリックします。

ステップ 2 インターフェイスを選択します。

ステップ 3 [Refresh Rate] を選択します。使用可能なオプションは次のとおりです。

リフレッシュなし	統計情報は更新されません。
15 秒	統計情報は 15 秒ごとに更新されます。
30 秒	統計情報は 30 秒ごとに更新されます。
60 秒	統計情報は 60 秒ごとに更新されます。

不明なユニキャスト、マルチキャスト、およびブロードキャストストーム制御に関する次の統計情報が表示されます。

マルチキャストトラフィックタイプ	（マルチキャストストーム制御についてのみ）すべて。
通過したバイト数	受信したバイト数。
ドロップされたバイト数	ストーム制御が原因でドロップされたバイト数。
最終ドロップ時刻	最後のバイトがドロップされた時刻。

ステップ 4 すべてのインターフェイス上のカウンタをすべてクリアするには、[Clear All Interfaces Counters] をクリックします。インターフェイス上のすべてのカウンタをクリアするには、選択して [Clear Interface Counters] をクリックします。

ポート セキュリティ

（注） ポート セキュリティは、802.1X が有効になっているポートまたは SPAN 宛先として定義されたポート上では有効にすることができません。

ネットワーク セキュリティは、特定の MAC アドレスを持つユーザへのポートでのアクセスを制限することで向上できます。MAC アドレスは動的に学習することも、静的に設定することもできます。

ポートセキュリティは、受信および学習したパケットをモニタします。ロックされたポートへのアクセスは、特定の MAC アドレスを持つユーザに限定されます。

ポート セキュリティには次の 4 つのモードがあります。

- [Classic Lock]：ポート上で学習済みのすべての MAC アドレスがロックされます。新しい MAC アドレスは学習されません。学習済みの MAC アドレスは、エージングや再学習の対象にはなりません。

- 限定された動的ロック（Limited Dynamic Lock）：デバイスは許可されたアドレスの設定済みの制限まで MAC アドレスを学習します。上限数に達すると、デバイスはそれ以上 MAC アドレスを学習しません。このモードでは、学習済みの MAC アドレスがエージングと再学習の対象になります。
- [無期限セキュア]：ポートに関連付けられている現在のダイナミック MAC アドレスを保持します（スタート コンフィギュレーション ファイルにコンフィギュレーションが保存されている間）。ポートの許容最大アドレス数に達するまで、新しい MAC アドレスを「無制限セキュア」対象として学習することができます。再学習とエージングは無効になっています。
- リセット時の安全な削除（Secure Delete on Reset）：リセット後に、ポートに関連付けられている最新の動的MACアドレスを削除します。新しいMACアドレスは、Delete-On-Resetアドレスとして、ポートで許可されている最大アドレス数まで学習できます。再学習とエージングは無効になっています。

ポートで許可されていない新しい MAC アドレスからのフレームが検出された場合（クラシックロックモードで新しい MAC アドレスからのフレームが届いた場合か、限定ダイナミックロックモードで許容最大アドレス数を超過した場合）、保護メカニズムが働き、次のいずれかの処理が実行されます。

- フレームが破棄される
- フレームが転送される
- ポートがシャットダウンする

セキュア MAC アドレスから送信されたフレームが別のポートに届いた場合、そのフレームは転送されますが、そのポート上でその MAC アドレスが学習されることはありません。

次のいずれかの操作に加えて、トラップを生成し、デバイスのオーバーロードを回避するためにトラップの頻度と数を制限できます。

ポートセキュリティを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Port Security] をクリックします。

ステップ 2 変更するインターフェイスを選択して、[Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：インターフェイス名を選択します。
- [インターフェイスステータス]：ポートをロックする場合、チェックボックスをオン にします。
- [学習モード]：ポートのロック モードを選択します。このフィールドを設定するには、[Interface Status] のロックを解除する必要があります。[Learning Mode] フィールドは、[Interface Status] フィールドがロックされている場合にのみ有効になります。[Learning Mode] を変更するには、[Lock Interface] をク

リアする必要があります。モードを変更したら、[Lock Interface] を元に戻すことができます。次のオプションがあります。

- [クラシックロック] : すでに学習されている MAC アドレスの数にかかわらず、 ポートをすぐにロックします。
- [限定ダイナミックロック] : 現在このポートに動的に関連付けられている MAC アドレスを削除し、ポートをロックします。ポートは、そのポートで許可されている最大数までアドレスを学習します。MAC アドレスの再学習とエージングの両方が有効になります。
- セキュアな相手先固定（Secure Permanent）：ポートに関連付けられている現在の動的な MAC アドレスを保持し、そのポートで許可されているアドレスの最大数（[Max No. of Addresses Allowed] で設定）まで学習します。再学習とエージングは無効になっています。
- リセット時の安全な削除（Secure Delete on Reset）：リセット後に、ポートに関連付けられている最新の動的 MAC アドレスを削除します。新しい MAC アドレスは、Delete-On-Reset アドレスとして、ポートで許可されている最大アドレス数まで学習できます。再学習とエージングは無効になっています。

- [最大 許可アドレス数] : [学習モード] で [限定ダイナミックロック] を選択した場合、 このポート上で学習できる MAC アドレスの上限数を入力します。数字の 0 は、スタティック アドレスのみインターフェイスでサポートされることを示します。
- [違反時アクション] : ロックされているポートに届いたパケットに適用する処理を選 択します。次のオプションがあります。
  - [Discard]：学習されていない送信元から届いたパケットを破棄します。
  - [Forward]：不明な送信元 MAC アドレスから届いたパケットを転送します。MAC アドレスは学習されません。
  - [Shutdown]：学習されていない送信元からのパケットを破棄し、ポートが再アクティブ化されるか、デバイスがリブートされるまで、ポートをシャットダウンします。
- [トラップ] : ロックされているポートにパケットが届いたときにトラップを有効にする場合、選択します。これは、ロック違反に関係します。[Classic Lock] の場合、受信したすべての新しいアドレスに関係します。[Limited Dynamic Lock] の場合、許可されているアドレス数を超過した新しいアドレスに関係します。
- [トラップ間隔] : トラップの最短間隔を入力します（単位：秒）。

ステップ 4 [Apply] をクリックします。ポート セキュリティが変更されて、実行コンフィギュレーション ファイルが更新されます。

802.1X 認証

802.1X 認証は、未認可クライアントが一般にアクセス可能なポートから LAN に接続することを制限します。802.1X 認証はクライアント/サーバ モデルです。このモデルでは、ネットワーク デバイスが次の固有の役割を持ちます。

- クライアントまたはサプリカント：ネットワークに接続しようとしているPCやラップトップなどのデバイス。
- オーセンティケータ：サプリカントとネットワーク間の接続を提供するネットワークデバイス（Catalyst 1200 や Catalyst 1300 スイッチなど）。サプリカントと認証サーバーの間で認証データをリレーします。
- 認証サーバー：RADIUS サーバーなど、オーセンティケータからの認証要求を受信して応答する信頼できるサーバー。ネットワーク上でサプリカントを許可する必要があるかどうか、およびスイッチに対して認証するデバイスまたはユーザーに関連する特別な情報または設定をオーセンティケータに通知します。

ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、または両方として使用できます。

（注） ネットワーク アクセスデバイスで802.1x認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。

プロパティ

[Properties]ページは、ポート/デバイス認証をグローバルに有効にするために使用されます。認証を機能させるには、認証をグローバルに有効にするとともに各ポートでも個別に有効にする必要があります。

ポートベースの認証を定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Properties] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ポートベース認証]：ポートベース認証を有効または無効にします。
- [認証方式]：ユーザー認証方式を選択します。次のオプションがあります。
  - [RADIUS、なし]：まずRADIUS サーバーを使用してポート認証を実行します。RADIUS サーバーから応答がない場合、認証処理は実行されず、セッションが許可されます。

- [RADIUS]：RADIUS サーバー上でユーザーを認証します。認証が行われない場合、セッションは許可されません。
- [None]：ユーザーを認証しません。セッションは許可されます。

- [Guest VLAN]：未認可ポート用にゲスト VLAN を使用できるようにする場合に選択します。ゲスト VLAN が有効になっている場合は、すべての未認可ポートが、[Guest VLAN ID] フィールドで選択した VLAN に自動的に追加されます。ポートが後で許可された場合、そのポートはゲスト VLAN から削除されます。ゲスト VLAN は、他の VLAN と同様に、レイヤ 3 インターフェイス（IP アドレスが割り当てられている）として定義できます。ただし、ゲスト VLAN IP アドレス経由ではデバイス管理が使用できません。
- [Guest VLAN ID]：VLAN のリストからゲスト VLAN を選択します。
- [Guest VLAN Timeout]：[Immediate]を選択するか[User Defined]に値を入力してタイムアウト時間を定義します。この値は次のように使用されます。

  リンクアップ後にソフトウェアで 802.1x サプリカントが検出されない場合、または認証に失敗した場合、ゲスト VLAN タイムアウトで設定した時間の経過後に、そのポートがゲスト VLAN に追加されます。

  ポート状態が [Authorized] から [Not Authorized] に変わる場合、[Guest VLAN Timeout] の時間が経過すると、そのポートはゲスト VLAN だけに追加されます。
- [トラップ設定]：トラップを有効にするには、次のオプションの中から 1 つ以上を選択します。
  - [802.1X Authentication Failure Traps]：選択すると、802.1X 認証が失敗したときにトラップが生成されます。
  - [802.1X Authentication Success Traps]：選択すると、802.1X 認証が成功したときにトラップが生成されます。
  - [MAC Authentication Failure Traps]：選択すると、MAC 認証が失敗したときにトラップが生成されます。
  - [MAC Authentication Success Traps]：選択すると、MAC 認証が成功したときにトラップが生成されます。
  - [サプリカント認証失敗トラップ]：選択すると、サプリカント認証が失敗したときにトラップが生成されます。
  - [サプリカント認証成功トラップ]：選択すると、サプリカント認証が成功したときにトラップが生成されます。
  - [Web Authentication Failure Traps]：選択すると、Web 認証が失敗したときにトラップが生成されます。
  - [Web Authentication Success Traps]：選択すると、Web 認証が成功したときにトラップが生成されます。
  - [Web Authentication Quiet Traps]：選択すると、待機時間が始まったときにトラップが生成されます。

VLAN 認証テーブルにすべての VLAN が表示され、認証が有効になっているかどうかが表示されます。

ステップ 3 [Apply] をクリックします。802.1X プロパティは、実行コンフィギュレーション ファイルに書き込まれます。

VLAN での認証の有効/無効を変更するには、VLAN を選択し、[Edit] をクリックして、[Enable] または [Disable] のいずれかを選択します。

ポート認証

[Port Authentication] ページでは、各ポートのパラメータを設定できます。ホスト認証などのいくつかの設定は、ポートが [Force Authorized] 状態の間しか変更できないため、ポート制御を [Force Authorized] に変更してから設定を変更するようにお勧めします。設定が完了したら、ポート制御を元の状態に戻してください。

（注） 802.1X が定義されたポートが LAG のメンバーになることはできません。802.1X とポートのセキュリティは、同じポートで同時に有効にすることはできません。あるインターフェイス上でポートセキュリティを有効にした場合は、[Administrative Port Control] を [Auto] モードに変更できません。

802.1X 認証を設定するには、次の手順に従います。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Port Authentication] の順にクリックします。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 インターフェイスを選択し、以下のパラメータを設定します。

オプション	説明
Interface	ユニットとポートを選択します。
Current Port Control	現在のポート許可状態が表示されます。状態が [Authorized] の場合は、そのポートが認証されているか、[Administrative Port Control] が [強制認可（Force Authorized] になっています。反対に状態が [Unauthorized] の場合は、ポートが認証されていないか、[Administrative Port Control] が [Force Unauthorized] になっています。サプリカントをインターフェイス上で有効にすると、現在のポート制御がサプリカントになります。
Administrative Port Control	管理ポートの許可状態を選択します。次のオプションがあります。

オプション	説明
	• [Force Unauthorized]：インターフェイスを未承認状態に移行することにより、インターフェイス アクセスを拒否します。デバイスが、このインターフェイスを介してクライアントに認証サービスを提供することはありません。 • [Auto]：デバイスでのポートベース認証および認可を有効にします。デバイスとクライアントの間で交換される認証情報に基づいて、インターフェイスの状態は認可済みになったり未認可になったりします。 • [Force Authorized]：認証せずにインターフェイスを承認します。
RADIUS VLAN Assignment	選択すると、選択したポート上でダイナミック VLAN 割り当てが有効になります。 • [Disable]：機能が有効になっていません。 • [Reject]：RADIUS サーバーがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは拒否されます。 • [Static]：RADIUS サーバーがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは許可されます。
Guest VLAN	選択すると、未許可のポートにゲスト VLAN を使用できるようになります。
Open Access	選択すると、認証が失敗した場合でもポートは正常に認証されます。
802.1X Based Authentication	選択すると、ポート上で 802.1x 認証が有効になります。
MAC-Based Authentication	選択すると、サプリカント MAC アドレスに基づくポート認証が有効になります。このポートでは 8 つの MAC ベース認証のみを使用できます。 （注） MAC ベース認証が成功するには、RADIUS サーバのサプリカントのユーザ名とパスワードが、サプリカント MAC アドレスである必要があります。MAC アドレスは、小文字で、ピリオドやハイフン（「.」や「-」）の区切り文字を使用せずに入力する必要があります（例：0020aa00bbcc）。
Web-Based Authentication	選択すると、サプリカント MAC アドレスに基づく Web ベース認証が有効になります。
Periodic Reauthentication	選択すると、[再認証期間（Reauthentication Period）] で指定した間隔で、ポートの再認証試行が有効になります。
Reauthenticate Period	値を入力します。（範囲：300 ～ 4294967295、デフォルトは 3600）
Reauthenticate Now	再認証するにはチェックボックスをオンにします。

オプション	説明
Authenticator State	定義されているポート認可状態が表示されます。次のオプションがあります。 • [初期化]：起動処理中。 • [Force Authorized]：ポート制御状態は Force Authorized（トラフィックを転 送）に設定されています。 • [Force-Unauthorized]：制御ポート状態が [Force-Unauthorized]（トラフィックの破棄）に設定されています。 （注） [Force-Authorized] でも [Force-Unauthorized] でもない場合、ポートは自動モードになっていて、オーセンティケータには現在の認証状態が表示されます。ポートが認証されると、状態は [Authenticated] と表示されます。
Time Range	選択すると、認証が指定した時間範囲に制限されます。
Time Range Name	[Time Range] が選択されている場合は、[Edit] ボタンをクリックすると、時間範囲のページにリダイレクトされるので、使用する時間範囲名を選択します。
Maximum WBA Login Attempts	Web ベース認証で許可されるログインの最大試行回数を入力します。[無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。
Maximum WBA Silence Period	[無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。[ユーザー定義（User Defined）] には、範囲（1 ～ 4294967295）を入力します。
Max Hosts	このインターフェイスで使用できる、許可されたホストの最大数を入力します。 [無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。[ユーザー定義（User Defined）] には、範囲（1 ～ 4294967295）を入力します。 （注） 値を 1 に設定すると、複数セッションモードの Web ベース認証に対して単一ホストモードがシミュレートされます。
Quiet Period	待機期間の長さを入力します。
Resending EAP	サプリカント（クライアント）からの、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）要求/ID フレームに対する応答をデバイスが

オプション	説明
	待機する時間を入力します（単位：秒）。この時間内に応答がない場合、要求が再送信されます。
Max EAP Requests	送信されるEAP要求の最大数を入力します。定義された期間内に応答が受信されなかった（サプリカントタイムアウト）場合は、認証プロセスが再開されます。（範囲：1 ～ 10、デフォルト：2）
EAP Max Retries	送信可能なEAP再試行の最大数を入力します。（範囲：1～10、デフォルト：2）
EAP Timeout	タイムアウトが発生するまでEAP応答を待機する最大時間を入力します。
Supplicant Timeout	EAP要求がサプリカントに再送信されるまでの経過時間を入力します（単位：秒）。
Server Timeout:	デバイスが認証サーバーに要求を再送信するまでの経過時間を入力します（単位：秒）。
Supplicant	802.1X を有効にする場合に選択します。
Credentials	このサプリカントに使用するクレデンシャルをドロップダウンリストから選択します。このパラメータは、サプリカントがインターフェイスで有効になっている場合にのみ使用できます。クレデンシャルを設定できる [Supplicant Credentials] ページへのリンクを編集してください。
Supplicant Timeout	EAP要求がサプリカントに再送信されるまでの経過時間を入力します（単位：秒）。
Server Timeout	デバイスが認証サーバーに要求を再送信するまでの経過時間を入力します（単位：秒）。
Supplicant	802.1X を有効にする場合に選択します。
Credentials	このサプリカントに使用するクレデンシャルをドロップダウンリストから選択します。このパラメータは、サプリカントがインターフェイスで有効になっている場合にのみ使用できます。クレデンシャルを設定できる [Supplicant Credentials] ページへのリンクを編集してください。
Supplicant Held Timeout	サプリカントが RADIUS サーバーから FAIL 応答を受信してから認証を再開するまで待機する期間を入力します。

ステップ 4 [Apply] をクリックします。ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

ホストおよびセッション認証

[Host and Session Authentication] ページでは、ポートでの 802.1X の動作モードと、違反検出時に実行するアクションを定義できます。

ポートの 802.1X 詳細設定を定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Host and Session Authentication] の順にクリックします。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：ホスト認証を有効にするポート番号を入力します。
- [Host Authentication]：いずれかのモードを選択します。
  - [Single-Host]：許可されたクライアントが存在する場合にポートが許可されます。1 つのポートでは 1 つのホストのみ認可されます。
  - [Multiple Host (802.1X)]：許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。
  - [Multi-Sessions]：シングルホストおよびマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスがありません。このステータスは、ポートに接続している各クライアントに割り当てられます。

  [Single Host Violation Settings]：ホスト認証が [Single-Host] の場合にのみ選択できます。
- [Action on Violation]：サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから、シングルセッションモードかシングルホストモードで受信したパケットに適用する処理を選択します。次のオプションがあります。
  - [保護(破棄)]：パケットを破棄します。
  - [制限(転送)]：パケットを転送します。
  - [シャットダウン]：パケットを廃棄し、ポートを停止します。ポートは、再アクティブ化されるかデバイスが再起動するまで、シャットダウンした状態になります。
- [トラップ]：選択すると、トラップが有効になります。
- [Trap Frequency]：ホストにトラップを送信する頻度を定義します。このフィールドの値を定義できるのは、複数ホストが無効になっている場合だけです。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

[Host and Session Authentication Table] の [Number of Violations] 列に違反数が表示されます。

サプリカントクレデンシャル

802.1X オーセンティケータとしての機能に加えて、スイッチ自体を、ネイバーからのポートアクセス権限を求める802.1Xサプリカントとして設定できます。このサプリカントは、RFC3748で規定されている EAP MD5-Challenge 方式をサポートします。この方式では、クライアントが、その名前とパスワードによって認証されます。サプリカントがインターフェイスで有効になっている場合、そのインターフェイスは未認可になります。802.1X認証プロセスが成功すると、インターフェイスの状態が認可済みに変更されます。このページでは、802.1Xサプリカントとして設定されたインターフェイスで使用できるクレデンシャルを作成および設定することができます。

（注） スイッチインターフェイスを802.1xサプリカントとして設定する場合、サプリカントの送信元 MAC に基づく ISE ポリシーは期待どおりに機能しないことに注意してください（リダイレクト ACL やダウンロード可能な ACL など）。

サプリカントのログイン情報を追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Supplicant Credentials] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [クレデンシャル名]：クレデンシャルを識別するための名前。
- [User Name]：クレデンシャル名に関連付けられるユーザ名を入力します。
- [Description]：ユーザを説明するテキストを入力します。
- [Password]：パスワードのタイプ（[Encrypted] または [Plaintext]）を選択し、パスワードを追加します。

ステップ 4 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 5 [Display Sensitive Data as Plaintext] をクリックすると、サプリカントクレデンシャルがプレーンテキスト形式で表示されます。

MACベース認証設定

MAC ベース認証は、802.1X のサプリカント機能を持たない装置（プリンタおよび IP Phone など）へのネットワーク アクセスを可能にする、802.1X 認証に代わるものです。MAC ベース認証は、接続装置の MAC アドレスを使用してネットワーク アクセスを許可または拒否します。

MAC ベース認証を設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [MAC-Based Authentication Settings] の順にクリックします

ステップ 2 次のフィールドに入力します。

- [MAC認証タイプ]：次のいずれかのオプションを選択します。
  - [EAP]：スイッチ（RADIUS クライアント）と RADIUS サーバー（MAC ベースのサプリカントを認証するサーバー）の間のトラフィックに対し、RADIUS と EAP カプセル化を使用します。
  - [RADIUS]：スイッチ（RADIUS クライアント）と RADIUS サーバー（MAC ベースのサプリカントを認証するサーバー）の間のトラフィックに対して、RADIUS（EAP カプセル化なし）を使用します。

ユーザ名の形式

MAC ベースの認証では、サプリカント ユーザー名はサプリカント デバイスの MAC アドレスに基づいています。この MAC ベースのユーザー名の形式は、次のように定義されます。このユーザー名は、認証プロセスの一部としてスイッチから RADIUS サーバーへ送信されます。

- [グループサイズ]：MAC アドレスで区切り文字で囲まれ、ユーザー名として送信される ASCII 文字の数。
- [グループ区切り]：MACアドレス内で定義される文字グループを区切る区切り文字として使用される文字。
- [大文字小文字]：ユーザー名を小文字または大文字で送信します。

MAC認証パスワード

- [Password]：スイッチが RADIUS サーバーでの認証に使用するパスワードを定義します。次のオプションのいずれかを選択します。
  - [デフォルトの使用(ユーザー名)]：定義されているユーザー名をパスワードとして使用する場合は、このオプションを選択します。
  - [暗号化]：パスワードを暗号化形式で定義します。
  - [プレーンテキスト]：パスワードをプレーンテキスト形式で定義します。
- [パスワードMD5ダイジェスト]：MD5 Digest パスワードを表示します。

ステップ 3 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。暗号化されたパスワードを表示するには、[機密データを平文で表示] をクリックします。

認証済みホスト

認証済みユーザーの詳細情報を表示するには、[Security] > [802.1X Authentication] > [Authenticated Hosts] の順にクリックします。

このページには、次のフィールドが表示されます。

- [User Name]：各ポートで認証されたサプリカントの名前。
- [Port]：ポート番号。
- [Session Time (DD:HH:MM:SS)]：そのポートでサプリカントが認証および認可されていた時間の長さ。
- [認証方式]：最後のセッションの認証に使用された方式。有効な値は、[802.1x]、[MAC]、または [Web] です。
- [認証サーバ（Authentication Server）]：RADIUS サーバ。可能な値は、[Remote]、[Local]、または [None] です。
- [MAC アドレス]：サプリカントの MAC アドレスが表示されます。
- [VLAN ID]：ポートの VLAN。

（注） [Authenticated Sessions] テーブルボタンをクリックして、デバイスインターフェイスごとの認証済みセッションの詳細を表示します。

ロック済みクライアント

ログインに失敗してロックアウトされたクライアントを表示し、ロック済みクライアントをロック解除するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Locked Client] の順にクリックします。

次のフィールドが表示されます。

- [Interface]：ロックされたポート。
- [MACアドレス]：ロック済みステーションの MAC アドレスが表示されます。

• [Remaining Time (Sec)]：ポートがロックされるまでの残り時間。

ステップ 2 ポートを選択します。

ステップ 3 [Unlock] をクリックします。

Web認証のカスタマイズ

このページでは、さまざまな言語の Web ベース認証ページを設計できます。

最大 4 つの言語を追加できます。

（注） 最大 5 人の HTTP ユーザと 1 人の HTTPS ユーザが同時に Web ベース認証を要求できます。これらのユーザが認証されると、さらに別のユーザが認証を要求できます。

Web ベース認証用の言語を追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1X Authentication] > [Web Authentication Customization] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 [Language] ドロップダウン リストから言語を選択します。

ステップ 4 この言語をデフォルト言語にする場合は、[Set as Default Display Language] を選択します。エンドユーザーが言語を選択していない場合はデフォルト言語のページが表示されます。

ステップ 5 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

Web 認証ページをカスタマイズするには、次の手順に従います。

ステップ 6 [Security] > [802.1X Authentication] > [Web Authentication Customization] の順にクリックします。

このページには、カスタマイズ可能な言語が表示されます。

ステップ 7 [Edit Login Page] をクリックします。

ステップ 8 [Edit label 1] をクリックします。次のフィールドが表示されます。

- [言語]：ページの言語が表示されます。
- [Color Scheme]：いずれかのコントラスト オプションを選択します。

  [Custom] カラー スキームが選択されている場合は、次のオプションを使用できます。

  - [Page Background Color]：背景の色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。

- [Page Text Color]：テキストの色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
- [Header and Footer Background Color]：ヘッダーとフッターの背景の色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
- [Header and Footer Text Color]：ヘッダーとフッターのテキストの色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
- [Hyperlink Color]：テキストの色の ASCII コードを入力します。選択した色がテキストフィールドに表示されます。

- [現在のロゴ画像]：現在のログ画像を含むファイルの名前が表示されます。
- [ロゴ画像]：次のいずれかのオプションを選択します。
  - [None]：ロゴを使用しません。
  - [デフォルト]：デフォルトのロゴを使用します。
  - [Other]：カスタマイズしたロゴを入力する場合に選択します。

    [Other] ロゴ オプションが選択されている場合は、次のオプションを使用できます。
  - [Logo Image Filename]：ロゴ ファイル名を入力するか、[Browse] をクリックして画像を選択します。
- [Application Text]：ロゴに添えるテキストを入力します。
- [Window Title Text]：ログイン ページのタイトルを入力します。

ステップ 9 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 10 [Edit label 2] をクリックします。次のフィールドが表示されます。

- [Invalid User Credentials]：エンドユーザが無効なユーザ名またはパスワードを入力したときに表示されるメッセージのテキストを入力します。
- [Service Not Available]：認証サービスを使用できないときに表示されるメッセージのテキストを入力します。

ステップ 11 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 12 [Edit label 3] をクリックします。次のフィールドが表示されます。

- [Welcome Message]：エンドユーザがログオンしたときに表示されるメッセージのテキストを入力します。
- [Instructional Message]：エンドユーザに表示される指示を入力します。
- [RADIUS Authentication]：RADIUS 認証が有効になっているかどうかが示されます。有効になっている場合は、ログイン ページにユーザ名とパスワードを含める必要があります。
- [Username Textbox]：選択すると、ユーザ名のテキスト ボックスが表示されます。

- [Username Textbox Label]：ユーザ名のテキスト ボックスの前に表示されるラベルを選択します。
- [Password Textbox]：選択すると、パスワードのテキスト ボックスが表示されます。
- [Password Textbox Label]：パスワードのテキスト ボックスの前に表示されるラベルを選択します。
- [Language Selection]：選択すると、エンドユーザが言語を選択できるようになります。
- [Language Dropdown Label]：言語選択ドロップダウンのラベルを入力します。
- [Login Button Label]：ログイン ボタンのラベルを入力します。
- [Login Progress Label]：ログイン プロセス中に表示されるテキストを入力します。

ステップ 13 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 14 [Edit label 4] をクリックします。次のフィールドが表示されます。

- [Terms and Conditions]：選択すると、契約条件のテキスト ボックスが有効になります。
- [Terms and Conditions Warning]：契約条件入力の指示として表示されるメッセージのテキストを入力します。
- [Terms and Conditions Content]：契約条件として表示されるメッセージのテキストを入力します。

ステップ 15 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 16 [Edit label 5] では、次のフィールドが表示されます。

- [Copyright]：選択すると、著作権のテキストの表示が有効になります。
- [著作権のテキスト]：著作権のテキストを入力します。

ステップ 17 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 18 [Edit Success Page] をクリックします。

ステップ 19 ページの右側にある [Edit] をクリックします。

ステップ 20 [Success Message] に、エンドユーザが正常にログインしたときに表示されるテキストを入力します。

ステップ 21 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ログインまたは成功メッセージをプレビューするには、[Preview] をクリックします。

GUI インターフェイスのデフォルト言語を Web ベース認証のデフォルト言語として設定するには、[Set Default Display Language] をクリックします。

認証セッション

（注） この設定は、[Advanced Mode] でのみ使用できます。

インターフェイスで認証されたセッションの詳細を表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1x Authentication] > [Authenticated Sessions] の順に選択します。

ステップ 2 [Authenticated Sessions] テーブルをフィルタリングするには、ドロップダウンメニューからユニットとインターフェイスを選択し、[Go] をクリックします。

ステップ 3 [Authenticated Sessions] テーブルには、インターフェイス上のすべての 802.1x 認証済みセッションに関する次のフィールドが表示されます。

- [Port]：情報が表示されているポート ID。
- [User Name]：このセッションで認証に使用されるサプリカント名。
- [Mac Address]：サプリカントの MAC アドレスが表示されます。
- [Status]：セッションの現在のステータス。[Authorized] または [Unauthorized] のいずれか
- [Authentication Method]：セッションの認証に使用された方式。
- [Common Session ID]：このセッションを一意に識別するセッション ID。

ステップ 4 特定のセッションの詳細を表示するには、目的のセッションを選択して、[Details] をクリックします。ポップアップには、メインテーブルに表示されるフィールドに加えて、次のフィールドが表示されます。

- [Supplicant IP Address]：サプリカントの IP アドレス。
- [Reason]：認証が失敗した理由。セッションステータスが [Unauthorized] に設定されている場合にのみ表示されます。
- [Host Authentication]：インターフェイスに設定されている認証モード。
- [Session Time]：このセッションがアクティブな時間。
- [Accounting Session ID]：アカウンティングセッションのセッション ID。
- [VLAN ID]：このセッションによってインターフェイスに適用された VLAN ID。
- [Tagging]：VLAN ID のモードをタグ付きまたはタグなしで表示します。
- [ACL Name 1]：このセッションでインターフェイスに適用される最初の ACL の名前。
- [ACL Type 1]：このセッションでインターフェイスに適用される ACL のタイプ。フィルタ ID（リダイレクトまたはダウンロード可能）を指定できます
- [Redirect URL]：このセッションに指定されたリダイレクト URL。このフィールドは、ACL タイプがリダイレクトの場合にのみ表示されます。

（注）

同じセッションで複数の ACL を適用できます。この場合、[ACL Name 2] … [ACL Name 3] などの追加情報が表示されます。

サービス拒絶防御

サービス妨害（DoS）攻撃では、ハッカーはデバイスをユーザが使用できない状態にしようとします。

DoS 攻撃では、デバイスが外部の通信要求で満たされ、正当なトラフィックに応答できないようになります。この攻撃では通常、デバイスの CPU がオーバーロードになります。

デバイスによって使用される DoS 攻撃に対抗する方法の 1 つは、セキュアコアテクノロジー（SCT）を利用する方法です。SCT はデフォルトで有効になっており、無効化できません。シスコデバイスは、エンドユーザ（TCP）トラフィックに加えて、管理トラフィック、プロトコル トラフィック、およびスヌーピング トラフィックを処理する高度なデバイスです。SCT を使用することで、デバイスは、受信するトラフィック量に関係なく、管理およびプロトコル トラフィックを受信して処理できます。これは、CPU に対する TCP トラフィックのレートを制限することで実現されます。

セキュリティスイート設定

（注） DoS 防御を有効化する前に、ポートにバインドされているすべてのアクセス コントロール リスト（ACL）または高度な QoS ポリシーをアンバインドする必要があります。ポートで DoS 防御機能がアクティブ化されている間、ACL と拡張 QoS ポリシーは非アクティブ化されます。

DoS 防御のグローバル設定を構成し、SCT をモニタするには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [Security Suite Settings] をクリックします。

CPU 保護メカニズム：有効化（CPU Protection Mechanism: Enabled）は SCT が有効であることを示します。

ステップ 2 [CPU Utilization] の横の [Details] をクリックすると CPU 使用率ページに移動し、CPU リソース利用率情報が表示されます。

ステップ 3 この機能を設定するには、[TCP SYN Protection] の横にある [Edit] をクリックします。

ステップ 4 [DoS防御] を設定します。

- [Disable]：すべてのタイプのサービス妨害機能を無効にします（デバイスレベルの TCP SYN 保護は除く）。

- [System-Level Prevention]：Stacheldraht（分散型）、Invasor（トロイの木馬）、Back Orifice（トロイの木馬）、Martian アドレスからの攻撃の防御を有効にします。
- [System-Level and Interface-Level Prevention]：システムレベルの防御に加えて、インターフェイスレベルの設定（SYN フィルタリング、SYN レート保護、ICMP フィルタリング、IP フラグメント化）を有効化して設定できます。

ステップ 5 [システムレベルの防御] または [システムレベルおよびインターフェイスレベルの防御] を選択した場合、次の [DoS防御] オプションの 1 つまたは複数を有効にしてください。

- [Stacheldraht Distribution]：送信元 TCP ポートが 16660 に等しい TCP パケットを破棄します。
- [Invasor Trojan]：宛先 TCP ポートが 2140 に等しく、送信元 TCP ポートが 1024 に等しい TCP パケットを破棄します。
- [Back Orifice Trojan]：宛先 UDP ポートが 31337 に等しく、送信元 UDP ポートが 1024 に等しい UDP パケットを破棄します。

ステップ 6 必要に応じて、以下をクリックします。

- [Martian Addresses]：[Edit] をクリックするとMartianアドレス （69 ページ）ページに移動します。
- [SYN Filtering]：[Edit] をクリックするとSYN フィルタリング （71 ページ）ページに移動します。
- [SYN Rate Protection]：（レイヤ 2 のみ）[Edit] をクリックするとSYNレート保護 （72 ページ）ページに移動します。
- [ICMP Filtering]：[Edit] をクリックするとICMPフィルタリング （73 ページ）ページに移動します。
- [IP Fragmented]：[Edit] をクリックするとIPフラグメントフィルタリング （73 ページ）ページに移動します。

ステップ 7 [Apply]をクリックします。サービス妨害（DoS）防御セキュリティ スイートの設定が、実行コンフィギュレーション ファイルに書き込まれます。

SYN保護

ネットワーク ポートは、SYN 攻撃でデバイスを攻撃するためにハッカーによって使用される可能性があります。SYN 攻撃は TCP リソース（バッファ）と CPU パワーを消費します。

CPU は SCT を使用して保護されているため、CPU への TCP トラフィックは制限されます。ただし、1 つまたは複数のポートが高いレートの SYN パケットで攻撃された場合、CPU は攻撃者のパケットのみ受け取るためサービス妨害が発生します。

SYN 保護機能を使用している場合、CPU は各ネットワーク ポートから CPU に送られる 1 秒あたりの SYN パケットの入力をカウントします。

SYN 保護を設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Protection] をクリックします。

ステップ 2 パラメータを入力します。

- [Block SYN-FIN Packets]：選択すると、この機能が有効になります。すべてのポートで、SYN と FIN の両方のフラグを持つすべての TCP パケットがドロップされます。
- [SYN Protection Mode]：次の 3 つのモードから選択します。
  - [Disable]：特定のインターフェイスでこの機能が無効になります。
  - [Report]：SYSLOG メッセージを生成します。しきい値を超えた場合、ポートのステータスが [Attacked] に変わります。
  - [Block and Report]：TCP SYN 攻撃が見つかった場合、システム宛ての TCP SYN パケットはドロップされて、ポートのステータスが [Blocked] に変わります。
- [SYN Protection Threshold]：SYN パケットがブロックされるまでの 1 秒あたりの SYN パケット数（「自分への MAC を含む SYN を拒否」ルールがポートに適用されます）。
- [SYN Protection Period]：SYN パケットのブロックを解除するまでの秒数（「自分への MAC を含む SYN を拒否」ルールはポートからバインド解除されます）。

ステップ 3 [Apply] をクリックします。SYN 保護が定義され、実行コンフィギュレーション ファイルが更新されます。

SYN 保護インターフェイス テーブルに、（ユーザのリクエストに応じて）すべてのポートまたは LAG に関する次のフィールドが表示されます。

- [Current Status]：インターフェイスのステータス。次の値が可能です。
  - [Normal]：このインターフェイスで攻撃は検出されませんでした。
  - [Blocked]：トラフィックはこのインターフェイスでは転送されません。
  - [Attacked]：このインターフェイスで攻撃が検出されました。
- [Last Attack]：システムで最後に検出された SYN-FIN 攻撃の日付と、それに対するシステムのアクション。

Martianアドレス

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[Martian Addresses] ページでは、ネットワーク上で確認された攻撃を示す IP アドレスを入力できます。それらのアドレスからのパケットは破棄されます。デバイスは、IP プロトコルの観点からは不正な一連の予約済み Martian アドレスをサポートします。サポートされている予約済み Martian アドレスは次のとおりです。

- [Martian アドレス（Martian Addresses）] ページで不正だと定義されているアドレス。
- ループバック アドレスなど、プロトコルの観点からは不正なアドレス。次の範囲内のアドレスが含まれます。
  - 0.0.0.0/8（ただし送信元アドレスとしての 0.0.0.0/32 を除く）：このブロックのアドレスは、このネットワーク上の送信元ホストを参照します。
  - 127.0.0.0/8：インターネットホストのループバックアドレスとして使用されます。
  - 192.0.2.0/24：ドキュメンテーションおよびコード例で TEST-NET として使用されます。
  - 224.0.0.0/4（送信元 IP アドレスとして）：IPv4 マルチキャストアドレス割り当てで使用されます。以前は「クラス D アドレス空間」と呼ばれていました。
  - 240.0.0.0/4（ただし宛先アドレスとしての 255.255.255.255/32 を除く）：予約済みアドレス範囲。以前は「クラス E アドレス空間」と呼ばれていました。

DoS 防御用の新しい Martian アドレスを追加することもできます。Martian アドレスを含むパケットは破棄されます。

Martian アドレスを定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [Martian Addresses] をクリックします。

ステップ 2 [Reserved Martian Addresses] を選択し、[Apply] をクリックして、[System Level Prevention] リストに予約済の Martian アドレスを含めます。

ステップ 3 Martian アドレスを追加するには、[Add] をクリックします。

ステップ 4 パラメータを入力します。

- [IP Version]：サポートされる IP バージョンを示します。現時点では、IPv4 のサポートのみ提供されています。
- [IP Address]：拒否する IP アドレスを入力します。次の値が可能です。
  - [From Reserved List]：予約済みリストからウェルノウン IP アドレスを選択します。
  - [New IP Address]：IP アドレスを入力します。
- [Mask]：拒否する IP アドレスの範囲を定義するために IP アドレスのマスクを入力します。値は次のとおりです。

- [Network Mask]：ドット付き 10 進表記でのネットワークマスク。
- [Prefix Length]：サービス拒絶防御を有効にする対象の IP アドレス範囲を定義するための IP アドレスプレフィックスを入力します。

ステップ 5 [Apply] をクリックします。

SYN フィルタリング

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[SYN Filtering] ページでは、SYN フラグを含み、1 つまたは複数のポートに送信される TCP パケットをフィルタリングできます。

SYN フィルタを定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Interface]：フィルタを定義するインターフェイスを選択します。
- [IPv4アドレス]：フィルタを定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。
- ネットワーク マスク（Network Mask）：フィルタが有効になっているネットワーク マスクを IP アドレス形式で入力します。次のいずれか 1 つを入力します。
  - [Mask]：ドット付き 10 進表記のネットワークマスク。
  - [プレフィックス長]：DoS 防御を有効にする対象の IP アドレス範囲を定義するための IP アドレスプレフィックス長を入力します。
- TCP ポート（TCP Port）：フィルタ処理されている宛先 TCP ポートを選択します。
  - [Known ports]：リストからポートを選択します。
  - [User Defined]：ポート番号を入力します。
  - [すべてのポート]：すべてのポートをフィルタするには、このフィールドを選択します。

ステップ 4 [Apply] をクリックします。SYN フィルタが定義され、実行コンフィギュレーション ファイルが更新されます。

SYNレート保護

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[SYN Rate Protection] ページでは、入力ポートで受信する SYN パケットの数を制限できます。そのため、パケット処理のために開かれる新しい接続数をレート制限することで、サーバに対する SYN フラッドの影響を緩和できます。

SYN レート保護を定義するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Rate Protection] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：レート保護が定義されているインターフェイスを選択します。
- [IP Address]：SYN レート保護をユーザー定義する対象の IP アドレスを入力するか、[All addresses] を選択します。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- [Network Mask]：送信元 IP アドレスのサブネットマスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - [プレフィックス長] : [プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。
- SYN レート制限（SYN Rate Limit）：受信する SYN パケットの数を入力します。

ステップ 4 [Apply] をクリックします。SYN レート保護が定義され、実行コンフィギュレーションが更新されます。

ICMPフィルタリング

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[ICMP Filtering] ページでは、特定の送信元からの ICMP パケットをブロックできます。ブロックすることで、ICMP 攻撃の発生時にネットワークの負荷を軽減できます。

ICMP フィルタリングを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [ICMP Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：ICMP フィルタリングが定義されているインターフェイスを選択します。
- [IPアドレス]：ICMP パケットフィルタリングをアクティブにする対象の IPv4 アドレスを入力するか、または [すべてのアドレス] を選択してすべての送信元アドレスからの ICMP パケットをブロックします。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- [Network Mask]：送信元 IP アドレスのサブネットマスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - [プレフィックス長]：[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [Apply] をクリックします。ICMP フィルタリングが定義され、実行コンフィギュレーションが更新されます。

IPフラグメントフィルタリング

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

IP フラグメンテーションは、ネットワーク層のデータが大きすぎて、データリンク層を介して一度に送信できない場合に発生します。その場合、ネットワーク層のデータがいくつかの断片（フラグメント）に分割されます。このプロセスが IP フラグメンテーションと呼ばれます。

フラグメント化された IP のフィルタ処理を設定し、フラグメント化された IP パケットをブロックするには、次の手順を実行します。

手順

ステップ 1 [Security] > [Denial of Service Prevention] > [IP Fragments Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：IP フラグメンテーションが定義されているインターフェイスを選択します。
- [IP Address]：フラグメント化 IP パケットをフィルタリングする対象の IP ネットワークを入力するか、または [All addresses] を選択してすべてのアドレスからの IP フラグメント化パケットをブロックします。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- [Network Mask]：送信元 IP アドレスのサブネットマスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - [プレフィックス長]：[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [Apply] をクリックします。IP フラグメンテーションが定義され、実行コンフィギュレーション ファイルが更新されます。

IP ソース ガード

IP ソース ガードは、ホストがネイバーの IP アドレスを使用しようとしたときに発生するトラフィック攻撃を防ぐために使用できるセキュリティ機能です。

IP ソース ガードが有効になっている場合、デバイスは、DHCP スヌーピング バインディング データベースに含まれている IP アドレスにのみクライアント IP トラフィックを送信します。このデータベースには、DHCP スヌーピングによって追加されたアドレスと手動で追加したエントリの両方のアドレスが含まれます。パケットがデータベース内のエントリと一致した場合、デバイスはそのパケットを転送します。一致しない場合、パケットはドロップされます。

ポートで IP ソース ガードが有効になっている場合：

- DHCP スヌーピングによって許可される DHCP パケットが受け入れられます。
- 送信元 IP アドレス フィルタリングを有効になっている場合：
  - IPv4 トラフィック：ポートに関連付けられている送信元 IP アドレスを持つトラフィックのみ許可されます。
  - 非 IPv4 トラフィック：許可されます（ARP パケットを含む）。

プロパティ

IP ソース ガードをグローバルに有効にするには、次の手順を実行します。

手順

ステップ 1 [Security] > [IP Source Guard] > [Properties] の順にクリックします。
ステップ 2 [Enable] を選択して、IP ソース ガードをグローバルに有効にします。
ステップ 3 [Apply] をクリックして、IP ソース ガードを有効にします。

インターフェイスの設定

IP ソース ガードが信頼できないポートや LAG で有効になっている場合、DHCP スヌーピングによって許可された DHCP パケットが送信されます。送信元 IP アドレス フィルタリングが有効になっている場合、パケット送信は次のように許可されます。

- [IPv4 traffic]：特定のポートに関連付けられている送信元 IP アドレスを含む IPv4 トラフィックだけが許可されます。
- [Non IPv4 traffic]：IPv4 以外のトラフィックはすべて許可されます。

インターフェイスで IP ソース ガードを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [IP Source Guard] > [Interface Settings] をクリックします。
ステップ 2 [Filter] フィールドからポート/LAG を選択して、[Go] をクリックします。このユニット上のポートまたは LAG が次の情報とともに表示されます。
- [IP Source Guard]：ポートで IP ソースガードが有効になっているかどうかを示します。
- DHCP スヌーピングの信頼できるインターフェイス（DHCP Snooping Trusted Interface）：信頼できる DHCP インターフェイスであるかどうかを示します。

ステップ 3 ポートまたはLAGを選択し、[Edit] をクリックします。[IP Source Guard] フィールドの [Enable] を選択すると、インターフェイスで IP ソースガードが有効になります。

ステップ 4 [Apply] をクリックして、設定を実行コンフィギュレーション ファイルにコピーします。

バインディング データベース

IP ソースガードでは、信頼されていないポートからのパケットをチェックするために DHCP スヌーピング バインディング データベースを使用します。デバイスが DHCP スヌーピング バインディングデータベースに書き込もうとするエントリの数が多すぎる場合、余分なエントリが非アクティブステータスで維持されます。エントリはリース時間が期限切れになると削除されるため、非アクティブなエントリがアクティブになることがあります。

「DHCP リレー」を参照してください。

（注） バインディングデータベースのページには、IP ソースガードが有効になったポートで定義された DHCP スヌーピング バインディング データベース内のエントリのみが表示されます。

DHCP スヌーピングを表示し、消費された TCAM リソースを確認するには、次の手順を実行します。

手順

ステップ 1 [Security] > [IP Source Guard] > [Binding Database] をクリックします。

[Supported IP Format and TCAM Resources Consumed] が表示されます。

ステップ 2 DHCP スヌーピングでは、データベースの管理に TCAM リソースが使用されます。デバイスで非アクティブ エントリをアクティブ化する試行をどの程度の頻度で行うかを選択するために、[挿入非アクティブ] フィールドを設定します。次のオプションがあります。

- 再試行頻度（Retry Frequency）：TCAM リソースがチェックされる頻度。
- 実行しない（Never）：非アクティブなアドレスの再アクティブ化を試みない。

ステップ 3 [Apply] をクリックすると上記の変更が実行コンフィギュレーションに保存されます。また、[Retry Now] をクリックすると TCAM リソースが検査されます。

次のエントリが表示されます。

- [VLAN ID]：パケットを受信すると予想される VLAN。
- [MAC Address]：照合される MAC アドレス。
- [IP Address]：照合される IP アドレス。

- インターフェイス（Interface）：パケットが予測されるインターフェイス。
- [Status]：インターフェイスがアクティブであるかどうかを表示します。
- タイプ（Type）：エントリのタイプ（動的または静的）が表示されます。
- [Reason]：インターフェイスがアクティブでない場合、その理由を表示します。次の理由があります。
  - [No Problem]：インターフェイスはアクティブです。
  - [No Snoop VLAN]：VLAN で DHCP スヌーピングが有効になっていません。
  - [Trusted Port]：ポートが信頼されるようになりました。
  - リソースの問題（Resource Problem）：TCAM リソースが使い果たされました。

ステップ 4 これらのエントリのサブセットを表示するには、サブセットを選択し、関連する検索条件を入力してデータをフィルタ処理し、[Retry Now] をクリックします。

ARP インスペクション

ARP を使用すると、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内での IP 通信が可能になります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。この状況は、ARP は、ARP 要求を受信していないホストからの Gratuitous 応答も許可するため発生します。攻撃が開始されると、攻撃を受けたデバイスからのトラフィックはすべて、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されます。

ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。それぞれの IP アドレスと MAC アドレスはカッコ内に表示されています。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用します。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。ホスト B は ARP 応答を使用して応答します。スイッチとホスト A は、ホスト B の MAC と IP を使用して、それぞれの ARP キャッシュを更新します。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。このため、ホスト C はそのトラフィックを代行受信できます。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホスト

に転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。これが、従来の中間者攻撃です。

ARP インスペクションプロパティ

ARP インスペクションのプロパティを設定するには、次の手順を実行します。

手順

ステップ 1 [Security] > [ARP Inspection] > [Properties] の順にクリックします。

次のフィールドに入力します。

- [ARP Inspection Status]：ARP インスペクションを有効にする場合に選択します。
- [ARP Packet Validation]：検証チェックを有効にする場合に選択します。
- [Log Buffer Interval]：次のいずれかのオプションを選択します。
  - [Retry Frequency]：ドロップされたパケットに関する SYSLOG メッセージの送信を有効にします。入力した頻度でメッセージが送信されます。
  - [Never]：ドロップされたパケットに関する SYSLOG メッセージが無効になります。

ステップ 2 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARP インスペクション インターフェイス設定

信頼されていないポート/LAG からのパケットは ARP アクセスルールテーブルに対してチェックされ、さらに DHCP スヌーピングが有効になっていれば DHCP スヌーピング バインディング データベースに対してチェックされます。

デフォルトでは、ポートや LAG は、ARP インスペクションで信頼されていません。

ポートや LAG の ARP 信頼ステータスを変更するには、次の手順を実行します。

手順

ステップ 1 [Security] > [ARP Inspection] > [Interface Settings] をクリックします。

ポートと LAG およびそれぞれの ARP 信頼/非信頼ステータスが表示されます。

ステップ 2 あるポート/LAG を「信頼できる」または「信頼できない」に設定するには、そのポート/LAG を選択して [Edit] をクリックします。

ステップ 3 [Trusted] または [Untrusted] を選択し、[Apply] をクリックして、実行コンフィギュレーション ファイルに設定を保存します。

ARPアクセスコントロール

ARP インスペクション テーブルにエントリを追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [ARP Inspection] > [ARP Access Control] の順にクリックします。

ステップ 2 エントリを追加するには、[Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [ARP Access Control Name]：ユーザーが作成した名前を入力します。
- [IP Address]：パケットの IP アドレス。
- [MAC Address]：パケットの MAC アドレス。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARPアクセスコントロールルール

作成済みの ARP アクセス コントロール グループにルールを追加するには、次の手順を実行します。

手順

ステップ 1 [Security] > [ARP Inspection] > [ARP Access Control Rules] の順にクリックします。

ARP アクセス コントロール ルール テーブルに、現在定義されているアクセスルールが表示されます。

特定のグループを選択するには、[Filter] を選択し、コントロール名を選択して [Go] をクリックします。

ステップ 2 グループに追加のルールを追加するには、[Add] をクリックします。

ステップ 3 [ARP Access Control Name] を選択し、次のフィールドに入力します。

- [IP Address]：パケットの IP アドレス。
- [MAC Address]：パケットの MAC アドレス。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARP インスペクション VLAN 設定

VLAN 上の ARP インスペクションを有効にして、アクセス コントロール グループを VLAN と関連付けるには、次の手順を実行します。

手順

ステップ 1 [Security] > [ARP Inspection] > [VLAN Settings] の順にクリックします。

ステップ 2 VLAN 上の ARP インスペクションを有効にするには、[Available VLANs] リストから [Enabled VLANs] リストに VLAN を移動します。

ステップ 3 ARP アクセス コントロール グループと VLAN を関連付けるには、[Add] をクリックします。VLAN 番号を選択し、定義済みの [ARP Access Control Name] を選択します。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv6 ファースト ホップ セキュリティ

IPv6 ファースト ホップ セキュリティ（FHS）は、IPv6 が有効なネットワークでのセキュアなリンク操作を実現するために設計された機能のスイートです。これは、ネイバー探索プロトコルと DHCPv6 メッセージに基づいています。

この機能では、レイヤ 2 スイッチが各種の規則に従って、ネイバー探索プロトコル メッセージ、DHCPv6 メッセージ、およびユーザー データ メッセージをフィルタリングします。

IPv6 ファースト ホップ セキュリティのコンポーネント

IPv6 ファースト ホップ セキュリティには、次の機能があります。

- IPv6 ファースト ホップ セキュリティの共通機能
- RA ガード
- ND インスペクション
- ネイバー バインド整合性
- DHCPv6 ガード
- IPv6 ソース ガード

これらのコンポーネントは、VLAN で有効または無効にできます。機能ごとに、vlan_default と port_default という 2 つの空の事前定義済みポリシーが存在します。最初のポリシーは、ユー

ザ定義ポリシーに接続されていない各 VLAN に接続され、2 番目のポリシーは、ユーザ定義ポリシーに接続されていない各インターフェイスと VLAN に接続されます。

FHS の設定

[FHS Settings] ページを使用して、指定した VLAN グループで FHS 共通機能を有効にし、ドロップされたパケットのロギング用のグローバル設定値を設定します。必要に応じて、ポリシーを追加できます。また、パケットドロップロギングもシステム定義のデフォルトポリシーに追加できます。

IPv6 ファースト ホップ セキュリティの共通パラメータを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- FHS VLAN リスト（FHS VLAN List）：IPv6 ファースト ホップ セキュリティを有効にする 1 つまたは複数の VLAN を入力します。
- パケット ドロップ ロギング（Packet Drop Logging）：選択すると、パケットがファーストホップ セキュリティ ポリシーによってドロップされたときに SYSLOG が作成されます。これは、ポリシーが定義されていない場合のグローバル デフォルト値です。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要な場合は、[Add] をクリックして FHS ポリシーを作成します。

次のフィールドに入力します。

- [Policy Name]：ユーザ定義のポリシー名を入力します。
- [Packet Drop Logging]：選択すると、パケットがこのポリシー内のファーストホップ セキュリティ ポリシーの結果としてドロップされたときに SYSLOG が作成されます。
  - [Inherited]：VLAN またはグローバル設定の値を使用します。
  - [Enable]：ファーストホップセキュリティの結果としてパケットがドロップされたときに SYSLOG が作成されます。
  - [Disable]：ファースト ホップ セキュリティによってパケットがドロップされても SYSLOG は作成されません。

ステップ 5 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 6 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN) （94 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート) （95 ページ）」 ページにジャンプし、このポリシーをポートにアタッチできます。

RAガード設定

IPv6 RA ガード機能を使用すると、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガードメッセージを、ネットワーク管理者がブロックまたは拒否できます。デバイスでは RA を使用して、リンクで自身をアナウンスします。IPv6 RA ガード機能は、それらの RA を調査して、承認されていないデバイスから送信された RA を除外します。

ホストモードでは、RA とルータ リダイレクト メッセージはポート上ですべてブロックされます。RA ガード機能は、レイヤ 2（L2）デバイスの構成データを、受信した RA フレーム内のデータと比較します。L2 デバイスは、RA フレームとルータリダイレクトフレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます

[RA Guard Settings] ページを使用して、指定した VLAN グループで RA ガード機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト RA ガード ポリシーを設定できます。

RA ガードを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [RA Guard Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 [RA Guard VLAN List] で、RA ガードが有効になっている VLAN を 1 つ以上入力します。

ステップ 3 次に、以下の項目を設定します。

- [Minimum Hop Limit]：RA ガードポリシーが、受信したパケットの最大ホップ限度を確認するかどうかを示します。次のいずれかを選択します。
  - [No Limit]：ホップカウント限度の下限の検証を無効にします。
  - [User Defined]：ホップカウント制限がこの値以下であることを確認します。高位境界の値は、低位境界の値以上でなければなりません。
- [Maximum Hop Limit]：RA ガードポリシーが、受信したパケットの最大ホップ限度を確認するかどうかを示します。次のいずれかを選択します。

- リミットなし（No Limit）：ホップカウント制限の上限値の検証を無効にします。
- [User Defined]：ホップカウント制限がこの値以下であることを確認します。高位境界の値は、低位境界の値以上でなければなりません。

- [Managed Configuration Flag]：このフィールドには、IPv6 RA ガードポリシー内でのアドバタイズされた管理アドレス設定フラグの検証を指定します。次のいずれかを選択します。
  - 検証なし（No Verification）：アドバタイズされた管理アドレス設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされた管理アドレス設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- [Other Configuration Flag]：このフィールドは、IPv6 RA ガードポリシー内での、アドバタイズされた他のコンフィギュレーション フラグの検証について指定します。次のいずれかを選択します。
  - 検証なし（No Verification）：アドバタイズされたその他の設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされたその他の設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- 最小ルータ プリファレンス（Minimal Router Preference）：このフィールドは、RA ガードポリシーで、RA ガード ポリシー内で RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最小値を検証するかどうかを指定します。次のいずれかを選択します。
  - 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの下限値の検証を無効にします。
  - 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。
  - 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。
  - 高（High）：許容されるアドバタイズされたデフォルトルータ プリファレンスの最小値を指定します。
- 最大ルータ プリファレンス（Maximal Router Preference）：このフィールドは、RA ガード ポリシーで、RA ガード ポリシー内で RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最大値を検証するかどうかを指定します。次のいずれかを選択します。
  - 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの上限値の検証を無効にします。
  - 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。
  - 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。

- 高（High）：許容されるアドバタイズされたデフォルトルータプリファレンスの最大値を指定します。

ステップ 4 [RA Guard Policy Table] にポリシーを追加するには、[Add] をクリックして、以下のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：RA ガードの対象ポートに接続されているデバイスのロールを指定するために、次のオプションのいずれかが表示されます。
  - [Inherited]：デバイス ロールは、VLAN またはシステム デフォルト（クライアント）から継承されます。
  - [Host]：デバイスロールはホストです。
  - [Router]：デバイス ロールはルータです。
- 管理設定フラグ（Managed Configuration Flag）：このフィールドには、IPv6 RA ガードポリシー内でのアドバタイズされた管理アドレス設定フラグの検証を指定します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされた管理アドレス設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされた管理アドレス設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- その他の設定フラグ（Other Configuration Flag）：このフィールドには、IPv6 RA ガード ポリシー内でのアドバタイズされたその他の設定フラグの検証を指定します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされたその他の設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされたその他の設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- RA アドレス リスト（RA Address List）：フィルタ処理するアドレスのリストを指定します。
  - [Inherited]：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - [No Verification]：アドバタイズされたアドレスは検証されません。
  - [Match List]：照合される IPv6 アドレスリスト。
- RA プレフィックス リスト（RA Prefix List）：フィルタ処理するアドレスのリストを指定します。

- [Inherited]：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
- [No Verification]：アドバタイズされたプレフィックスは検証されません。
- [Match List]：照合されるプレフィックスリスト。

- [Minimal Hop Limit]：RA ガードポリシーが、受信したパケットの最小ホップ限度をチェックするかどうかを示します。
  - 継承（Inherited）：機能は、VLANまたはシステムのデフォルト（クライアント）から継承されます。
  - リミットなし（No Limit）：ホップ カウント制限の下限値の検証を無効にします。
  - ユーザ定義（User Defined）：ホップカウント制限がこの値以上であることを確認します。
- [Maximal Hop Limit]：RA ガードポリシーが、受信したパケットの最大ホップ限度をチェックするかどうかを示します。
  - 継承（Inherited）：機能は、VLANまたはシステムのデフォルト（クライアント）から継承されます。
  - リミットなし（No Limit）：ホップカウント制限の上限値の検証を無効にします。
  - [User Defined]：ホップカウント制限がこの値以下であることを確認します。高位境界の値は、低位境界の値以上でなければなりません。
- [Minimal Router Preference]：このフィールドは、RA ガードポリシーで、RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最小値を検証するかどうかを示します。
  - 継承（Inherited）：機能は、VLANまたはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの下限値の検証を無効にします。
  - 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
  - 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
  - 高（High）：許容されるアドバタイズされたデフォルトルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- [Maximal Router Preference]：このフィールドは、RA ガードポリシーで、RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最大値を検証するかどうかを示します。
  - 継承（Inherited）：機能は、VLANまたはシステムのデフォルト（クライアント）から継承されます。

- 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの上限値の検証を無効にします。
- 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- 高（High）：許容されるアドバタイズされたデフォルトルータプリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。

ステップ 5 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 6 システム定義のデフォルト ポリシーまたは既存のユーザ定義ポリシーを設定するには、ポリシーテーブルでポリシーを選択し、[Edit] をクリックします。

ステップ 7 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN) （94 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート) （95 ページ）」 ページにジャンプし、このポリシーをポートにアタッチできます。

DHCPv6ガード設定

[DHCPv6 Guard Settings] ページを使用して、指定した VLAN グループで DHCPv6 ガード機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト DHCPv6 ガード ポリシーを設定できます。

DHCPv6 ガードを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [DHCPv6 Guard Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- [DHCPv6 Guard VLAN List]：DHCPv6 ガードが有効になっている VLAN を 1 つ以上入力します。
- [Device Role]：デバイスロールを表示します。[追加] ページの定義を参照してください。

- [Minimal Preference]：このフィールドは、受信したパケットのアドバタイズされた最小プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。
  - 検証なし（No Verification）：受信したパケットのアドバタイズされた最小設定値の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以上であることを確認します。この値は最大設定値未満である必要があります。
- [Maximal Preference]：このフィールドは、受信したパケットのアドバタイズされた最大プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。この値は最小設定値より大きくなければなりません。
  - 検証なし（No Verification）：ホップ カウント制限の下限の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以下であることを確認します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 4 必要に応じて、[Add] をクリックして DHCPv6 ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

- [Policy Name]：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：DHCPv6 ガードの対象ポートに接続されているデバイスのロールを指定するには、[Server] または [Client] のいずれかを選択します。
  - 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - クライアント（Client）：デバイスのロールはクライアントです。
  - サーバ（Server）：デバイスのロールはサーバです。
- 応答プレフィックスを一致（Match Reply Prefixes）：選択すると、DHCPv6 ガード ポリシー内での受信した DHCP 応答メッセージ内のアドバタイズされたプレフィックスの検証が有効になります。
  - [Inherited]：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - [No Verification]：アドバタイズされたプレフィックスは検証されません。
  - [Match List]：照合される IPv6 プレフィックスリスト。
- サーバ アドレスを一致（Match Server Address）：選択すると、DHCPv6 ガード ポリシー内での受信した DHCP 応答メッセージ内の DHCP サーバおよびリレーの IPv6 アドレスの検証が有効になります。
  - 継承（Inherited）：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - 検証なし（No Verification）：DHCP サーバおよびリレーの IPv6 アドレスの検証を無効にします。

- 一致リスト（Match List）：一致させる IPv6 プレフィックスのリスト。

- [Minimal Preference]：このフィールドは、受信したパケットのアドバタイズされた最小プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。
  - 継承（Inherited）：最小設定は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：受信したパケットのアドバタイズされた最小設定値の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以上であることを確認します。この値は最大設定値未満である必要があります。

- [Maximal Preference]：このフィールドは、受信したパケットのアドバタイズされた最大プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。この値は最小設定値より大きくなければなりません。
  - 継承（Inherited）：最小設定は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：ホップ カウント制限の下限の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以下であることを確認します。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN) （94 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート) （95 ページ）」 ページにジャンプし、このポリシーをポートにアタッチできます。

NDインスペクション設定

[Neighbor Discovery (ND) Inspection Settings] ページを使用して、指定した VLAN グループで ND インスペクション機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト ND インスペクション ポリシーを設定できます。

ND インスペクションを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [ND Inspection Settings] をクリックします。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- ND インスペクション VLAN リスト（ND Inspection VLAN List）：ND インスペクションを有効にする 1 つまたは複数の VLAN を入力します。
- デバイス ロール（Device Role）：次に説明するデバイス ロールが表示されます。
- 安全でないメッセージをドロップ（Drop Unsecure）：選択すると、IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが有効になります。
- [Minimal Security Level]：非セキュアなメッセージがドロップされない場合、メッセージが転送されるための最低限のセキュリティ レベルを選択します。
  - 検証なし（No Verification）：セキュリティ レベルの検証を無効にします。
  - ユーザ定義（User Defined）：転送するメッセージのセキュリティ レベルを指定します。
- 送信元 MAC を検証（Validate Source MAC）：選択すると、リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックがグローバルに有効になります。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要に応じて、[Add] をクリックして ND インスペクション ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

- [Policy Name]：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：ND インスペクションの対象ポートに接続されているデバイスのロールを指定するには、次のオプションのいずれかを選択します。
  - 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - ホスト（Host）：デバイスのロールはホストです。
  - ルータ（Router）：デバイスのロールはルータです。
- 安全でないメッセージをドロップ（Drop Unsecure）：次のいずれかのオプションを選択します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 有効化（Enable）：選択すると、IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが有効になります。

- 無効化（Disable）：IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが無効になります。

- [Minimal Security Level]：非セキュアなメッセージがドロップされない場合、メッセージが転送されるための最低限のセキュリティレベルを選択します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 検証なし（No Verification）：セキュリティ レベルの検証を無効にします。
  - ユーザ定義（User Defined）：転送するメッセージのセキュリティ レベルを指定します。

- 送信元 MAC を検証（Validate Source MAC）：リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックをグローバルに有効にするかどうかを指定します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 有効化（Enable）：リンク層アドレスと照らし合わせた送信元MACアドレスのチェックが有効になります。
  - 無効化（Disable）：リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックが無効になります。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：このポリシーを VLAN にアタッチする手順については、ポリシー適用(VLAN)（94 ページ）を参照してください。
- [Attach Policy to Interface]：このポリシーをインターフェイスにアタッチする手順については、ポリシー適用(ポート)（95 ページ）を参照してください。

ネイバーバインディング設定

ネイバー バインド テーブルは、デバイスに接続されている IPv6 ネイバーのデータベース テーブルであり、ネイバー探索プロトコル（NDP）スヌーピングなどの情報ソースから作成されます。このデータベース（またはバインド）テーブルは、スヌーピングを防止し、攻撃をリダイレクトするためにさまざまな IPv6 ガード機能で使用されます。

[Neighbor Binding Settings] ページを使用して、指定した VLAN グループでネイバー バインド機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト ネイバー バインド ポリシーを設定できます。

ネイバー バインドを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Binding Settings] をクリックします。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

ネイバーバインディング VLANリスト	ネイバーバインディングが有効になっている VLAN を 1 つまたは複数入力します。
Device Role	デバイスのグローバルなデフォルトロール（境界）を表示します。
ネイバーバインディング ライフタイム	アドレスがネイバー バインディング テーブルに留まる時間の長さを入力します。
ネイバーバインディング ロギング	選択すると、ネイバー バインディング テーブルのメインイベントのロギングが有効になります。
アドレスプレフィックス検証	選択すると、アドレスの IPv6 ソースガード検証が有効になります。

グローバルアドレスバインディングコンフィギュレーション

NDPメッセージからのバインディング	許可されるグローバル IPv6 アドレスの設定方法のグローバル設定を IPv6 ネイバー バインディング ポリシー内で変更するには、次のオプションのいずれかを選択します。 • [Any]：NDP メッセージからバインドされたグローバル IPv6 に対して、任意の設定方法（ステートレスおよび手動）を許可します。 • ステートレス（Stateless）：NDP メッセージからバインドされるグローバル IPv6 に対して、ステートレス自動設定のみが許可されます。 • 無効化（Disable）：NDP メッセージからのバインディングが無効になります。
DHCPv6メッセージからのバインディング	DHCPv6 からのバインドが許可されます。

ネイバーバインディングエントリ限度

VLAN毎のエントリ数	グローバル値を使用する場合、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[User Defined] を選択します。
インターフェイス毎のエントリ数	グローバル値を使用する場合、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[User Defined] を選択します。

MACアドレス毎のエントリ数	グローバル値を使用する場合、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[User Defined] を選択します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要に応じて、[Add] をクリックしてネイバー バインド ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

[Policy Name]	ユーザー定義のポリシー名を入力します。
Device Role	次のオプションの**いずれか**を選択して、ネイバー バインディング ポリシーのポートにアタッチされているデバイスのロールを指定します。 • 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。 • 境界（Perimeter）：ポートは、IPv6 ファースト ホップ セキュリティをサポートしていないデバイスに接続されています。 • 内部（Internal）：ポートは、IPv6 ファーストホップセキュリティをサポートしているデバイスに接続されています。
ネイバーバインディング ロギング	次のオプションのいずれかを選択して、ロギングを指定します。 • 継承（Inherited）：ロギング オプションは、グローバル値と同じです。 • 有効化（Enable）：バインディング テーブル メイン イベントのロギングを有効にします。 • 無効化（Disable）：バインディング テーブル メイン イベントのロギングを無効にします。
アドレスプレフィックス検証	次のオプションのいずれかを選択して、アドレスの検証を指定します。 • 継承（Inherited）：検証オプションは、グローバル値と同じです。 • 有効化（Enable）：アドレスの検証を有効にします。 • 無効化（Disable）：アドレスの検証を無効にします。

グローバルアドレスバインディングコンフィギュレーション

アドレスバインディング設定の継承	グローバル アドレス バインディング設定の使用を有効にします。

NDPメッセージからのバインディング	許可されるグローバル IPv6 アドレスの設定方法のグローバル設定を IPv6 ネイバー バインディング ポリシー内で変更するには、次のオプションのいずれかを選択します。 • [Any]：NDP メッセージからバインドされたグローバル IPv6 に対して、任意の設定方法（ステートレスおよび手動）を許可します。 • ステートレス（Stateless）：NDP メッセージからバインドされるグローバル IPv6 に対して、ステートレス自動設定のみが許可されます。 • 無効化（Disable）：NDP メッセージからのバインディングが無効になります。
DHCPv6メッセージからのバインディング	DHCPv6 からのバインドを有効にする場合に選択します。

ネイバーバインディングエントリ限度

VLAN毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
インターフェイス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
MACアドレス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

ポリシーをVLANにアタッチ	クリックするとポリシー適用(VLAN)（94 ページ）ページにジャンプし、このポリシーを VLAN にアタッチできます。
ポリシーをインターフェイスにアタッチ	クリックするとポリシー適用(ポート)（95 ページ）ページにジャンプし、このポリシーをポートにアタッチできます。

IPv6ソースガード設定

[IPv6 Source Guard Settings] ページを使用して、指定した VLAN グループで IPv6 ソース ガード機能を有効にします。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト IPv6 ソース ガード ポリシーを設定できます。

IPv6 ソース ガードを設定するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [IPv6 Source Guard Settings] をクリックします。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- IPv6 ソース ガード VLAN リスト（IPv6 Source Guard VLAN List）：IPv6 ソース ガードを有効にする 1 つまたは複数の VLAN を入力します。
- ポートの信頼（Port Trust）：デフォルトでポリシーが信頼できないポートを対象とすることが表示されます。これはポリシーごとに変更できます。

ステップ 3 新しい設定を適用するには、[Apply] をクリックします。

ステップ 4 必要に応じて、[Add] をクリックしてファースト ホップ セキュリティ ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

- [Policy Name]：ユーザ定義のポリシー名を入力します。
- ポートの信頼（Port Trust）：ポリシーのポート信頼状態を選択します。
  - [Inherited]：ポリシーをポートにアタッチした時点では、信頼されていません。
  - [Trusted]：ポリシーをポートにアタッチした時点で、信頼済みです。

ステップ 6 [Apply] をクリックしてポリシーを接続します。

ステップ 7 このポリシーをインターフェイスにアタッチするには、[Attach Policy to Interface] をクリックします。

ポリシー適用(VLAN)

1 つまたは複数の VLAN にポリシーを接続するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [Policy Attachment (VLAN)] をクリックします。

すでに接続されているポリシーのリストが、そのポリシータイプ、ポリシー名、およびVLANリストとともに表示されます。

ステップ 2 ポリシーをフィルタ処理するには、[Filter] チェックボックスを選択し、ドロップダウンメニューから [Policy Type] を選択して、[Go] をクリックします。

ステップ 3 VLAN にポリシーを接続するには、[Add] をクリックして次のフィールドに入力します。

- ポリシー タイプ（Policy Type）：インターフェイスに接続するポリシー タイプを選択します。
- [Policy Name]：インターフェイスにアタッチするポリシーの名前を選択します。
- [VLAN List]：ポリシーがアタッチされる VLAN を選択します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ポリシー適用(ポート)

1 つまたは複数のポートまたは LAG にポリシーを接続するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [Policy Attachment (Port)] をクリックします。

すでに接続されているポリシーのリストが、そのインターフェイス、ポリシー タイプ、ポリシー名、および VLAN リストとともに表示されます。

ステップ 2 [Filter] をオンにしてフィルタをアクティブ化し、ドロップダウンリストからポリシータイプを選択します。次に、[Go] をクリックしてデータをフィルタリングします。

ステップ 3 ポートまたは LAG にポリシーを接続するには、[Add] をクリックして次のフィールドに入力します。

- [Interface]：ポリシーをアタッチするインターフェイスを選択します。
- ポリシー タイプ（Policy Type）：インターフェイスに接続するポリシー タイプを選択します。
- [Policy Name]：インターフェイスにアタッチするポリシーの名前を選択します。
- [VLAN List]：ポリシーがアタッチされる VLAN を選択します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ネイバーバインディングテーブル

ネイバー バインド テーブルのエントリを表示するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Binding Table] をクリックします。

ステップ 2 次のテーブル クリア オプションのいずれかを選択します。

- [None]：何もクリアしません。
- スタティックのみ（Static Only）：テーブル内のすべてのスタティック エントリをクリアします。
- ダイナミックのみ（Dynamic Only）：テーブル内のすべてのダイナミック エントリをクリアします。
- [All Dynamic & Static]：テーブルに含まれるダイナミックなエントリとスタティックなエントリすべてをクリアします。

  ポリシーごとに、次のフィールドが表示されます（[Add]ページに存在しないフィールドのみが表示されます）。

- 発生元（Origin）：IPv6 アドレスを追加したプロトコル（ダイナミック エントリにのみ使用可能）。
  - [Static]：手動で追加したもの。
  - NDP：ネイバー探索プロトコル メッセージから学習しました。
  - DHCP：DHCPv6 プロトコル メッセージから学習しました。
- [State]：エントリの状態。
  - [Tentative]：新しいホストの IPv6 アドレスを検証中。そのライフタイムは 1 秒未満であるため、その有効期限は表示されません。
  - 有効（Valid）：ホストの IPv6 アドレスがバインドされました。
- 有効期限（秒）（Expiry Time (Sec.)）：確認されない場合、エントリが削除されるまでの残りの秒数。
- [TCAM Overflow]：[No] のマークが付けられたエントリは、TCAM オーバーフローが原因で TCAM に追加されなかったものです。

ステップ 3 ポリシーを追加するには、[Add] をクリックし、次のフィールドに入力します。

- VLAN ID：エントリの VLAN ID。
- [IPv6 Address]：エントリの送信元 IPv6 アドレス。
- [Interface]：パケットを受信するポートまたは LAG。
- [MAC Address]：パケットのネイバー MAC アドレス。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ネイバープレフィックステーブル

ネイバー プレフィックス テーブルに、NDP メッセージからバインドされたグローバル IPv6 アドレスのスタティック プレフィックスを追加できます。ダイナミックエントリが学習されます。

ネイバー プレフィックス テーブルにエントリを追加するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Prefix Table] をクリックします。

ステップ 2 ネイバー プレフィックス テーブルをクリアするには、[テーブルをクリア（Clear Table）] フィールドで次のオプションのいずれかを選択します。

- [None]：何もクリアしません。
- スタティックのみ（Static Only）：スタティック エントリのみをクリアします。
- ダイナミックのみ（Dynamic Only）：ダイナミック エントリのみをクリアします。
- すべてのダイナミック & スタティック（All Dynamic & Static）：スタティック エントリとダイナミック エントリをクリアします。

ステップ 3 既存のエントリについて、次のフィールドが表示されます。

- [VLAN ID]：プレフィックスが適用される VLAN
- [IPv6 Prefix]：IPv6 プレフィックス。
- [Prefix Length]：IPv6 プレフィックス長。
- 発生元（Origin）：エントリはダイナミック（学習されたもの）またはスタティック（手動で設定されたもの）です。
- 自動設定（Autoconfig）：プレフィックスはステートレス設定で使用できます。
- 有効期限（秒）（Expiry Time (Sec)）：エントリが削除されるまでの残り時間。

ステップ 4 [Add]をクリックしてテーブルに新しいエントリを追加し、新しいエントリについて上記のフィールドに入力します。

ステップ 5 次のフィールドを設定します。

- [VLAN ID]：プレフィックスが適用される VLAN ID を選択します。
- [IPv6 Prefix]：IPv6 プレフィックスを入力します。
- [Prefix length]：IPv6 プレフィックス長を入力します。

• [Autoconfig]：オンにすると、ステートレス構成の自動設定が有効になります。

FHS の状態

FHS 機能のグローバル設定を表示するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Status] をクリックします。

ステップ 2 FHS の状態を報告するポート、LAG、または VLAN を選択します。

ステップ 3 次のフィールドが選択したインターフェイスに表示されます。

FHS の状態

現在のVLAN上のFHS状態	現在の VLAN で FHS が有効になっているかどうか。
パケットドロップロギング	現在のインターフェイスに対して（グローバル設定のレベルか、そのインターフェイスにアタッチされているポリシー内で）この機能が有効になっているかどうか。

RA ガードの状態

現在のVLAN上のRAガード状態	現在の VLAN で RA ガードが有効になっているかどうか。
Device Role	RA デバイスの役割。
マネージドコンフィギュレーションフラグ	マネージド設定フラグの検証が有効かどうか。
他のコンフィギュレーションフラグ	他の設定フラグの検証が有効かどうか。
RAアドレスリスト	照合される RA アドレスリスト。
RAプレフィックスリスト	照合される RA プレフィックスリスト。
最小ホップ限度	最小 RA ホップ限度の検証が有効かどうか。
最大ホップ限度	最大 RA ホップ限度の検証が有効かどうか。
最小ルータプリファレンス	最小ルータプリファレンスの検証が有効かどうか。
最大ルータプリファレンス	最大ルータプリファレンスの検証が有効かどうか。

DHCPv6 ガードの状態

現在VLAN上のDHCPv6ガード状態	現在の VLAN で DHCPv6 ガードが有効になっているかどうか。
Device Role	DHCP デバイスロール
一致リプレイプレフィックス	DHCP 応答プレフィックスの検証が有効かどうか。
一致サーバーアドレス	DHCP サーバーアドレスの検証が有効かどうか。
最小プリファレンス	最小プリファレンスの検証が有効かどうか。
最大プリファレンス	最大プリファレンスの検証が有効かどうか。

ND インスペクションの状態

現在のVLAN上のNDインスペクション状態	現在の VLAN で ND インスペクションが有効になっているかどうか。
Device Role	ND インスペクションのデバイスロール。
ドロップアンセキュア	非セキュアなメッセージをドロップするかどうか。
最低セキュリティレベル	非セキュアなメッセージがドロップされない場合、パケットが転送されるのに必要な最低セキュリティレベル。
ソースMACの検証	送信元 MAC アドレスの検証が有効かどうか。

ネイバー バインドの状態

現在のVLAN上のネイバーバインディング状態	現在の VLAN でネイバーバインディングが有効になっているかどうか。
Device Role	ネイバー バインディング デバイスのロール。
ロギングバインディング	ネイバーバインディングテーブルのイベントのロギングが有効かどうか。
アドレスプレフィックス検証	アドレスプレフィックスの検証が有効かどうか。
グローバルアドレスコンフィギュレーション	検証されるメッセージ。
VLAN毎の最大エントリ	VLAN ごとに許可されるダイナミック ネイバー バインディング テーブルの最大エントリ数。
インターフェイス毎の最大エントリ数	インターフェイスごとに許可されるネイバー バインディング テーブルの最大エントリ数。
MACアドレス毎の最大エントリ数	MAC アドレスごとに許可されるネイバー バインディング テーブルの最大エントリ数。

IPv6ソースガードステータス

現在のVLAN上のIPv6ソースガード状態	現在の VLAN で IPv6 ソースガードが有効になっているかどうか。
ポートの信頼性	ポートが信頼されているかどうか、およびその信頼状態の受信方法。

FHS統計情報

FHS 統計を表示するには：

手順

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Statistics] をクリックします。

ステップ 2 [Refresh Rate]（統計が更新されるまでの経過期間）を選択します。

ステップ 3 次のグローバル オーバーフロー カウンタが表示されます。

ネイバーバインディングテーブル	テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
ネイバープレフィックステーブル	テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
TCAM	TCAM オーバーフローが原因で追加できなかったエントリ数。

ステップ 4 インターフェイス（ポートまたは LAG）を選択すると、次のフィールドが表示されます。

NDP（ネイバー探索プロトコルメッセージ）	次のタイプのメッセージについて、受信済みメッセージ数とドロップ済みメッセージ数が表示されます。 • RA：ルータ アドバタイズメント メッセージ • [REDIR]：リダイレクトメッセージ • NS：ネイバー要請メッセージ • NA：ネイバー アドバタイズメント メッセージ • RS：ルータ要請メッセージ

DHCPv6メッセージ	次のタイプのDHCPv6メッセージについて、受信済みメッセージ数とドロップ済みメッセージ数が表示されます。 • ADV：アドバタイズ メッセージ • [REP]：応答メッセージ • [REC]：再設定メッセージ • [REL-REP]：リレー応答メッセージ • LEAS-REP：リース クエリ応答メッセージ • [RLS]：リリース済みメッセージ • [DEC]：拒否済みメッセージ

次のフィールドが FHS ドロップ メッセージ テーブルに表示されます。

機能	ドロップされたメッセージのタイプ（DHCPv6 ガード、RA ガードなど）。
Count	ドロップされたメッセージの数。
理由	メッセージがドロップされた理由。

ステップ 5 カウンタをクリアするには、[Clear Interface Counters]、[Clear All Interface Counters]、[Clear Global Counters] のいずれかをクリックします。

ステップ 6 カウンタを更新するには、[Refresh] をクリックします。

証明書の設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

Cisco Business ダッシュボードプローブ（CBD）およびプラグアンドプレイ（PNP）機能では、CBD または PNP サーバーとの HTTPS 通信を確立するために CA 証明書が必要です。証明書設定機能により、これらのアプリケーションとデバイスマネージャは次のことを実行できます。

- 信頼された CA 証明書をインストールし、不要になった証明書を削除する
- デバイスの構成ファイルに証明書を静的に追加する
- 信頼されていない証明書の失効リストを管理する

また、証明書設定機能を使用して、デバイスの HTTPS サーバー証明書チェーンを作成する中間証明書をインポートできます。詳細については、SSLサーバー認証設定 （36 ページ）を参照してください。

（注） 証明書の有効期限は、システムクロックが基準になります。デフォルトのシステムクロックを使用します。そうしなければ適切な検証は提供されません。そのため、システムクロックがデバイスのリアルタイムクロックに基づいていること（サポートされている場合）、または最後のリブート以降にアクティブに設定されていることを確認します（SNTP サービスの使用を推奨）。システムクロックがRTCに基づいておらず、また最後のリブート以降に設定されなかった場合、システムクロックが証明書の有効期間内であっても、証明書の検証は失敗します。

ダイナミック証明書

CBDおよびPNPアプリケーションは、動的に信頼された証明書をデバイスメモリにインストールできます。インストールされる証明書には次の属性が必要です。

- [Certificate name]：証明書を識別するために使用される文字列。
- [Owner]：証明書をインストールしたアプリケーション名（PNP、CBD など）
- 証明書は PEM 形式です

アプリケーションによってインストールされた特定のまたはすべてのダイナミック証明書を削除することもできます。

考慮事項

- 最大 512 のダイナミック証明書をデバイスにインストールできます。
- デバイスのリブート時にダイナミック証明書は削除されます。

スタティック証明書

リセットしても削除されない証明書をアプリケーションで追加したい場合、またはスイッチのユーザーが証明書を追加したい場合、デバイスの HTTPS サーバー証明書の署名に使用される中間証明書を含むスタティック証明書を追加できます。これらの証明書は、デバイス実行コンフィギュレーションに保存されるため、スタートアップコンフィギュレーションにコピーできます。

スタティック証明書を追加するには、次の属性を指定する必要があります。

- [Certificate name]：証明書を識別するために使用される文字列です。
- [Owner]：証明書をインストールしたアプリケーション名（PNP、CBD など）。ユーザーが追加した場合は「static」になります。
- 証明書は PEM 形式です。

考慮事項

- 最大 256 のスタティック証明書をデバイスにインストールできます。
- 証明書の識別に使用する名前が異なっていれば、各アプリケーションまたは各ユーザーが追加する証明書は同じにできます。

CA 証明書設定

ユーザーは、インストールされているすべての証明書（動的および静的）に関する情報にアクセスできます。証明書ごとに次の情報が表示されます。

手順

ステップ 1 [Security] > [Certificate Settings] > [CA Certificate Settings] の順にクリックします。

ステップ 2 新しい証明書をインポートするには、[Add] をクリックし、次の項目を入力します。

- [Certificate Name]：証明書の名前を入力します。
- [Certificate Type]：証明書のタイプとして、[root]（デフォルト）または [intermediate]（デバイスの HTTPS サーバー証明書チェーンの一部）を選択します。
- [Certificate]：証明書を PEM 形式で貼り付けます（開始マーカー行と終了マーカー行を含みます）。

ステップ 3 新しい設定を適用するには、[Apply] をクリックします。

ステップ 4 既存の証明書の詳細を表示するには、リストから証明書を選択し、[Details] をクリックします。次のように表示されます。

オプション	説明
証明書名	証明書の名前または一意の識別子。
タイプ	これには、[signer]、[static]、または [dynamic] を選択できます。
CA Type	[Root]、[Intermediate]、または [N/A]（署名者証明書の場合）を選択できます。
Owner	これには、[signer]、[static]、[CBD]、または [PNP] を選択できます。
バージョン	証明書のバージョン。
Serial Number	証明書のシリアル番号。
Status	証明書のステータス。
Valid From	証明書の有効期限の開始日時。
Valid To	証明書の有効期限の終了日時。
発行元（Issuer）	証明書に署名したエンティティまたは CA。

オプション	説明
Subject	証明書の識別名（DN）情報。
公開キータイプ	公開キーのタイプ。
公開キー長	公開キーの長さ（ビット単位）。
Signature Algorithm	CA が証明書に署名するために使用する暗号化アルゴリズム。
Certificate	PEM 形式の証明書の詳細。

ステップ 5 次のフィルタを使用して、特定の証明書を検索できます。

- [Type equals to]：このチェックボックスをオンにして、ドロップダウンリストから [Signer]、[Static]、または [Dynamic] を選択し、これらの証明書タイプでフィルタ処理します。
- [Owner equals to]：証明書を PEM 形式で貼り付けます（開始マーカー行と終了マーカー行を含みます）。

ステップ 6 1 つまたは複数の証明書を削除するには、証明書を選択して Delete を押します。スタティック証明書のみ削除できます。

CA 証明書失効リスト

何らかの理由で証明書が信頼できなくなった場合は、ユーザーまたはいずれかのアプリケーションによって失効リストに追加されます。証明書が失効リストに含まれている場合は無効と見なされ、デバイスでは使用できなくなります。失効リストに証明書を追加しても、失効した証明書は証明書データベースから削除されません。証明書のステータスのみが、[Not Valid (Revoked)] に更新されます。証明書が失効リストから削除されると、その証明書のステータスは証明書データベースで自動的に更新されます。証明書を再インストールする必要はありません。

証明書を失効リストに追加または失効リストから削除するには、次の手順を実行します。

手順

ステップ 1 [Security] > [Certificate Settings] > [CA Certificate Revocation List] の順にクリックします。

ステップ 2 [Add] をクリックして [Add Revoked Certificate] ダイアログボックスを開きます。

ステップ 3 次の詳細事項を入力します。

- [Issuer]：発行元を特定する文字列（「C=US、O=MyTrustOrg、CN=MyCommonName」など）（0 ～ 160 文字）。
- [Serial Number]：失効した証明書のシリアル番号。これは 16 進数のペアの文字列です（長さ 2 ～ 40）。

ステップ 4 [Apply] をクリックして証明書を追加します。

説明

- 最大 512 の証明書を失効リストに追加できます。
- 失効リストのエントリに一致するすべての証明書は無効と見なされます（証明書データベース内で異なる名前で特定された場合でも同様）。

ステップ 5 既存の証明書を削除するには、失効した CA 証明書テーブルから証明書を選択し、[Delete] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。