CHAPTER 32

# SSL 設定の指定

## SSL

**Configuration > Properties > SSL**

セキュリティ アプライアンスは、Secure Sockets Layer（SSL）プロトコルおよびその後継である Transport Layer Security（TLS）を使用して、ASDM セッションと Web VPN セッションのセキュアなメッセージ伝送を実現します。SSL ウィンドウでは、クライアントとサーバ、および暗号化アルゴリズムの SSL バージョンを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバック トラストポイントを設定したりすることもできます。

### フィールド

- Server SSL Version：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Server SSL バージョンのオプションは、次のとおりです。

| | |
|---|---|
| Any | セキュリティ アプライアンスは、SSL バージョン クライアントの hello を受け入れ、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。 |
| Negotiate SSL V3 | セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 をネゴシエートします。 |
| Negotiate TLS V1 | セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、TSL バージョン 1 をネゴシエートします。 |
| SSL V3 Only | セキュリティ アプライアンスは、SSL バージョン 3 クライアントの hello のみを受け入れ、SSL バージョン 3 のみを使用します。 |
| TLS V1 Only | セキュリティ アプライアンスは、TLSv1 クライアントの hello のみを受け入れ、TLS バージョン 1 のみを使用します。 |

（注） WebVPN ポート転送を使用するには、Any または Negotiate SSL V3 を選択する必要があります。ポート転送アプリケーションを起動すると、JAVA がクライアントの Hello パケットで SSLv3 のみをネゴシエートする点が問題です。

- Client SSL Version：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Client SSL バージョンのオプションは、次のとおりです。

| | |
|---|---|
| *any* | セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。 |
| *sslv3-only* | セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 のみを受け入れます。 |
| *tlsv1-only* | セキュリティ アプライアンスは、TLSv1 クライアントの hello を送信し、TLS バージョン 1 のみを受け入れます。 |

- Encryption：SSL 暗号化アルゴリズムを設定できます。
  - Available Algorithms：セキュリティ アプライアンスがサポートし、SSL 接続で使用されていない暗号化アルゴリズムを一覧表示します。使用可能なアルゴリズムを使用するか、またはアクティブにするには、アルゴリズムを選択して **Add** をクリックします。
  - Active Algorithms：セキュリティ アプライアンスがサポートし、現在 SSL 接続で使用中の暗号化アルゴリズムを一覧表示します。使用を中止するか、アクティブなアルゴリズムを Available ステータスに変更するには、アルゴリズムを選択して **Remove** をクリックします。
  - Add/Remove：Available または Active Algorithms カラムの暗号化アルゴリズムのステータスを変更します。
  - Move Up/Move Down：アルゴリズムを選択し、これらのボタンをクリックして優先順位を変更します。セキュリティ アプライアンスは、アルゴリズムの使用を試みます。
- Trustpoints：フォールバック トラストポイントを選択し、設定済みのインターフェイスおよびそれらに関連付けられている設定済みのトラストポイントを表示します。トラストポイントを登録するには、**Configuration > Properties > Certificate > Enrollment** を選択します。
  - Fallback Trustpoint：トラストポイントが関連付けられていないインターフェイスに使用するトラストポイントを選択します。None を選択すると、セキュリティ アプライアンスはデフォルトの RSA キー ペアと証明書を使用します。

**（注）** このドロップダウン リストに表示するには、トラストポイントに証明書が関連付けられている必要があります。

  - Interface and Trustpoint カラム：設定済みインターフェイスと、ある場合はそのインターフェイスのトラストポイントを表示します。
  - Edit：選択したインターフェイスのトラストポイントを変更します。
- Apply：変更を適用します。
- Reset：変更内容を取り消し、SSL パラメータをウィンドウを開いた際に保存していた値にリセットします。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |

## Edit SSL Trustpoint

**Configuration > Properties > SSL > Edit SSL Trustpoint**

### フィールド

- Interface：編集中のインターフェイスの名前を表示します。
- Enrolled Trustpoint：名前付きインターフェイスに関連付けられている登録済みのトラストポイントを選択します。

### モード

次の表に、この機能を使用できるモードを示します。

| ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|
| | | | マルチ | |
| ルーテッド | 透過 | シングル | コンテキスト | システム |
| • | • | • | • | — |