SSL 設定の指定

SSL 設定

[Configuration] > [Device Management] > [Advanced] > [SSL Settings]

[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]

ASA 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、クライアントレス、VPN、およびブラウザベースの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 Settings] ウィンドウでは、クライアントとサーバの SSL バージョンおよび暗号化アルゴリズムを設定できます。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]：サーバとしてネゴシエートするときに ASA 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。

Any	ASA によって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
Negotiate SSL V3	ASA によって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 にネゴシエートされます。
Negotiate TLS V1	ASA によって SSL バージョン 2 クライアントの hello が受け入れられ、TLS バージョン 1 にネゴシエートされます。
SSL V3 Only	セキュリティ アプライアンスによって SSL バージョン 3 クライアントの hello のみが受け入れられ、SSL バージョン 3 のみが使用されます。
TLS V1 Only	セキュリティ アプライアンスによって TLSv1 クライアントの hello のみが受け入れられ、TLS バージョン 1 のみが使用されます。

（注） クライアントレス SSL VPN の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。問題は、ポート フォワーディング アプリケーションを起動すると、JAVA ではクライアントの Hello パケットで SSLv3 のみがネゴシエートされることです。

- [Client SSL Version]：クライアントとしてネゴシエートするときに ASA 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。

any	ASA によって SSL バージョン 3 の hello が送信され、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 のみが受け入れられます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello が送信され、TLS バージョン 1 のみが受け入れられます。

- [Encryption]：サポートする SSL 暗号化アルゴリズムを設定できます。
  - [Available Algorithms]：ASA 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] および [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。ASA は、アルゴリズムの使用を試みます。
- [Certificates]：各インターフェイスの SSL 認証に使用する証明書を割り当てます。[Edit] をクリックして、インターフェイスのトラストポイントを定義または変更します。トラストポイントは [Configuration] で設定されます。
  - [Primary Enrolled Certificate]：このインターフェイスの証明書に使用するトラストポイントを選択します。
  - [Load Balancing Enrolled Certificate]：VPN ロード バランシングが設定されている場合、証明書で使用するトラストポイントを選択します。
- [Fallback Certificate]：証明書が関連付けられていないインターフェイスで使用する証明書を選択します。[None] を選択すると、ASA はデフォルトの RSA キー ペアと証明書を使用します。
- [Forced Certification Authentication Timeout]：証明書認証がタイムアウトするまでの分数を設定します。
- [Apply]：変更を適用します。
- [Reset]：変更内容を取り消し、SSL パラメータをリセットして、ウィンドウを開いたときに保存されていた値に戻します。

SSL