SSL 設定

SSL 設定

次の場所のいずれかで SSL 設定を構成します。

- **[Configuration] > [Device Management] > [Advanced] > [SSL Settings]**
- **[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]**

ASA は、Secure Sockets Layer（SSL）プロトコルと Transport Layer Security（TLS）を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースの各セッションのセキュアなメッセージ伝送を実現します。また、DTLS は AnyConnect VPN クライアントの接続に使用されます。[SSL Settings] ペインでは、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。

（注） リリース 9.3（2）では、SSLv3 は廃止されています。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。[any]、[sslv3] または [sslv3-only] を選択した場合、設定は受け入れられますが警告が表示されます。[OK] をクリックして作業を続行します。ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

バージョン 9.4（1）では、SSLv3 キーワードはすべて ASA 設定から削除されており、SSLv3 のサポートが ASA から削除されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。

Citrix モバイル レシーバは TLS 1.1/1.2 プロトコルをサポートしていない可能性があります。互換性については、https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf を参照してください。

フィールド

- [Server SSL Version]：ASA がサーバとして動作するときに使用する、最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

いずれか（Any）	SSLv2 クライアントの hello を受け入れ、共通の最新バージョンをネゴシエートします。
SSL V3	SSLv2 クライアントの hello を受け入れ、SSLv3（以降）をネゴシエートします。
TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。
DTLSv1	DTLSv1 クライアントの hello を受け入れ、DTLSv1（以降）をネゴシエートします。
DTLS1.2	DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2（以降）をネゴシエートします。

（注） DTLS の設定および使用は、Cisco AnyConnect リモート アクセス接続のみに適用されます。

DTLS と同等以上の TLS バージョンを使用して、TLS セッションを DTLS セッションと同等以上にセキュアにする必要があります。これにより、DTLSV1.2 を選択したときに、TLSV1.2 が許容される唯一の TLS バージョンになります。また、すべての TLS バージョンは DTLS 1 と同等以上であるため、任意の TLS バージョンを DTLS1 と一緒に使用することができます。

- [Client SSL Version]：ASA がクライアントとして動作するときに使用する、最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。（SSL クライアント ロールに対して DTLS は使用不可）

いずれか（Any）	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
SSL V3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。

SSL 設定

TLS V1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
TLSV1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。

- [Diffie-Hellmann group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group2] です。
- [ECDH group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group19]（256 ビット EC）、[Group20]（384 ビット EC）、および [Group21]（521 ビット EC）です。デフォルト値は [Group19] です。

（注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。

- [Encryption]：サポートするバージョン、セキュリティ レベル、および SSL 暗号化アルゴリズムを指定します。[Configure Cipher Algorithms/Custom String] ダイアログボックスを使用してテーブル エントリを定義または変更するには、[Edit] をクリックします。SSL 暗号のセキュリティ レベルを選択し、[OK] をクリックします。
  - [Cipher Version]：ASA でサポートされ、SSL 接続に使用される暗号バージョンを一覧表示します。
  - [Cipher Security Level]：ASA でサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。

    [All]：NULL-SHA を含むすべての暗号。

    [Low]：NULL-SHA を除くすべての暗号。

    [Medium]：NULL-SHA、DES-CBC-SHA、RC4-MD5（これがデフォルトです）、RC4-SHA、および DES-CBC3-SHA を除くすべての暗号。

    [Fips]：NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号。

    [High]：SHA-2 を使用する AES-256 暗号だけが含まれ、TLS バージョン 1.2 にのみ適用されます。

    [Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。

- [Cipher Algorithms/Custom String]：ASA でサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用する暗号の詳細については、https://www.openssl.org/docs/manmaster/man1/ciphers.htmlを参照してください。

  ASA は、サポートされている暗号方式の優先順位を、TLSv1.2 のみでサポートされている暗号方式、TLSv1.1 または TLSv1.2 でサポートされていない暗号方式の順に指定します。

説明したように、次の暗号方式がサポートされています。

- [Server Name Indication (SNI)]：ドメイン名とそのドメインに関連付ける

暗号化方式	TLSv1.1 / DTLS V1	TLSV1.2
AES128-GCM-SHA256	いいえ	はい
AES128-SHA	はい	はい
AES128-SHA256	いいえ	はい
AES256-GCM-SHA384	いいえ	はい
AES256-SHA	はい	はい
AES256-SHA256	いいえ	はい
DERS-CBC-SHA	いいえ	いいえ
DES-CBC-SHA	はい	はい
DHE-RSA-AES128-GCM-SHA256	いいえ	はい
DHE-RSA-AES128-SHA	はい	はい
DHE-RSA-AES128-SHA256	いいえ	はい
DHE-RSA-AES256-GCM-SHA384	no	l
DHE-RSA-AES256-SHA	はい	はい
ECDHE-ECDSA-AES128-GCM-SHA256	いいえ	はい
ECDHE-ECDSA-AES128-SHA256	いいえ	はい
ECDHE-ECDSA-AES256-GCM-SHA384	いいえ	はい
ECDHE-ECDSA-AES256-SHA384	いいえ	はい
ECDHE-RSA-AES128-GCM-SHA256	はい	はい
ECDHE-RSA-AES128-SHA256	いいえ	はい
ECDHE-RSA-AES256-GCM-SHA384	いいえ	はい
ECDHE-RSA-AES256-SHA384	いいえ	はい

SSL 設定

暗号化方式	TLSv1.1 / DTLS V1	TLSV1.2
NULL-SHA	いいえ	いいえ
RC4-MD5	いいえ	いいえ
RC4-SHA	いいえ	いいえ

を指定します。[Add/Edit Server Name Indication (SNI)] ダイアログボックスを使用して各インターフェイスのドメインやトラストポイントを定義または変更するには、[Add] または [Edit] をクリックします。

- [Specify domain]：ドメイン名を入力します。
- [Select trustpoint to associate with domain]：ドロップダウン リストからトラストポイントを選択します。

- [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。[Select SSL Certificate] ダイアログボックスを使用して各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するには、[Edit] をクリックします。
  - [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]：変更内容を保存します。
- [Reset]：変更内容を取り消し、SSL パラメータを以前に定義した値にリセットします。

SSL 設定