デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

- デジタル証明書の概要 （1 ページ）
- デジタル証明書のガイドライン （11 ページ）
- デジタル証明書の設定 （13 ページ）
- 特定の証明書タイプの設定方法 （15 ページ）
- 証明書の有効期限アラートの設定（ID 証明書または CA 証明書用） （35 ページ）
- デジタル証明書のモニタリング （36 ページ）
- 証明書管理の履歴 （37 ページ）

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL（認証局の失効リストとも呼ばれます）に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。
- ID 証明書は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。

- コード署名者証明書は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ローカルCAは、ASAの独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザ登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。

（注） CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。
- 別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

CA は、証明書要求の管理とデジタル証明書の発行を行います。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。

ヒント 証明書コンフィギュレーションおよびロード バランシングの例は、次の URL を参照してください。https://supportforums.cisco.com/docs/DOC-5964

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザを認証する手段です。RSA 暗号化システムなどの Public Key Cryptography では、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

キーペア

キー ペアは、RSA または楕円曲線署名アルゴリズム（ECDSA）キーであり、次の特性があります。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- RSA キー サイズの最大値は 4096 で、デフォルトは 2048 です。
- ECDSA キー長の最大値は 521 で、デフォルトは 384 です。
- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。

（注） Cisco ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザ証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

認証登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、

ASA には署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つだけです。

ASA は、SCEP を使用した自動登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各 ASA を登録する必要があります。リモート アクセス VPN の場合は、各 ASA と各リモート アクセス VPN クライアントを登録する必要があります。

SCEP 要求のプロキシ

ASA は、AnyConnect とサードパーティ CA 間の SCEP 要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのは CA が ASA からアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA は、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠 CA をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA は、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効確認を有効にすることにより、CA が認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASA によってチェックされます。

失効確認を有効にすると、PKI 証明書検証プロセス時に ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェック、OCSP、またはその両方が使用されます。OCSP は、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバが使用不可であることを示すエラー）。

CRL チェックを使用すると、ASA によって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされている CRL が取得、解析、およびキャッシュされます。ASA は CRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSP は、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバ

ASA は次の CA サーバをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。CRL コンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用して、CRL チェックをオプションにすることもできます。オプションにすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

CRL のキャッシュに設定された時間を超過して ASA にキャッシュされている CRL がある場合、ASA はその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。ASA は、次回の証明書認証で失効した CRL のチェックが必要な場合に、より新しいバージョンの CRL を取得しようとします。

CRL のエントリ制限を超えると、ユーザ接続/証明書で失効チェックエラーが表示されることがあります。CRL あたりの最大エントリ数が 65534 を超えている場合、処理するエントリ数が多すぎることを示すメッセージが syslog から返されます。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。

- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバ、応答側とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。

（注） ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用して、OCSP チェックをオプションにすることもできます。オプションにすると、更新された OCSP データが検証局から提供されない場合でも、証明書認証は成功します。

OCSP を利用すると、OCSP サーバの URL を 3 つの方法で定義できます。ASA は、これらのサーバを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されている OCSP サーバの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバの URL
3. クライアント証明書の AIA フィールド

（注） トラストポイントでOCSPの応答側の自己署名した証明書を検証するように設定するには、信頼できるCA証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSP サーバ（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASAはトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

ローカル CA

ローカル CA では、次のタスクが実行されます。

- ASA で基本的な証明機関動作を統合する。
- 証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザベースとクライアントベースの両方で SSL VPN 接続とともに使用するために、ASA 上に認証局を提供する。
- 外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単なユーザ登録を実現する。

ローカル CA ファイル用のストレージ

ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CAデータベースが使用されます。このデータベースは、デフォルトでローカル フラッシュ メモリに存在するか、または、マウントされて ASA にアクセス可能な外部のファイル システム上に設定することもできます。

ローカルCAユーザデータベースに保存できるユーザの数に制限はありませんが、フラッシュ メモリ ストレージに問題がある場合、管理者に対策を取るように警告するsyslogが作成され、ローカル CA はストレージの問題が解決されるまでディセーブルになることがあります。フ

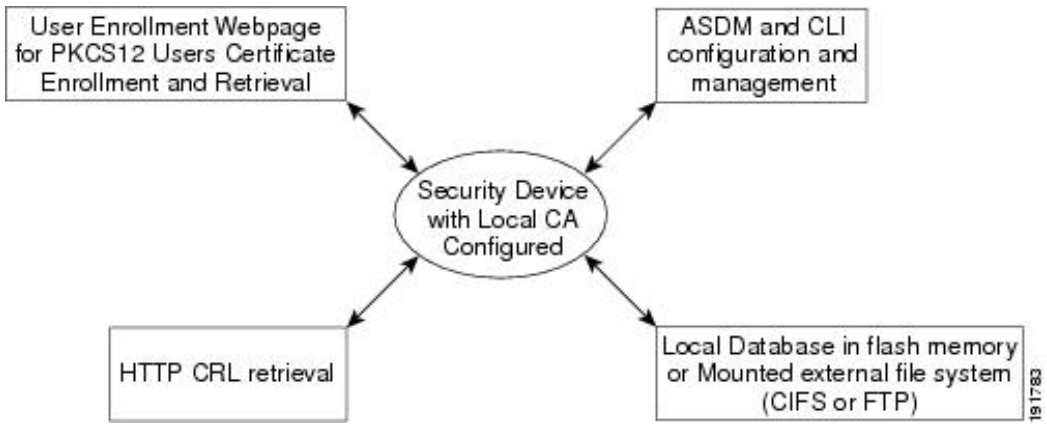
ラッシュ メモリは、3500 人以下のユーザを持つデータベースを保存できますが、ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ローカル CA サーバ

ASA にローカル CA サーバを設定すると、ユーザは、Web サイトにログインし、ユーザの登録資格を検証するためにローカル CA 管理者によって与えられたユーザ名とワンタイム パスワードを入力することで、証明書を登録できます。

次の図に示すように、ローカル CA サーバは ASA に常駐し、Web サイト ユーザからの登録要求や、その他の証明書を検証するデバイスおよび ASA から発信された CRL の問い合わせを処理します。ローカル CA データベースおよびコンフィギュレーション ファイルは、ASA のフラッシュ メモリ（デフォルトのストレージ）または個別のストレージ デバイスに保持されます。

図 *1 :* ローカル *CA*



証明書とユーザ ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP 認可では、パスワードをクレデンシャルとして使用しません。RADIUS 認可では、すべてのユーザの共通パスワードまたはユーザ名のいずれかを、パスワードとして使用します。

ユーザ ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認証サーバ グループ設定によりイネーブルにされます。

- ユーザ名とパスワードをクレデンシャルとして使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認可サーバ グループ設定によりイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

証明書

ユーザ デジタル証明書が設定されている場合、ASA によって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASAによって、ユーザの認証と認可の両方にユーザ ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。

- 認証
  - 認可サーバ グループ設定によってイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバ グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。

- 認証
  - 認可サーバ グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンデリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザ証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンデリ DN = CN（一般名）の場合、許可要求で使われるユーザ名は anyuser@example.com になります。

デジタル証明書のガイドライン

この項では、デジタル証明書を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

ローカル CA 証明書

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定が正しくないと、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明書を取得するとき、ASA は現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。
- ローカル CA 証明書の有効期限の 30 日前に、ロールオーバー代替証明書が生成され、syslog メッセージ情報で管理者にローカル CA のロールオーバーの時期であることが知らされます。新しいローカル CA 証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカル CA 証明書としてロールオーバー証明書をインストールして応答しない場合、検証が失敗する可能性があります。
- ローカル CA 証明書は、同じキー ペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64 形式でエクスポートに使用できます。

次に、base 64 で符号化されたローカル CA 証明書の例を示します。

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP プロキシ サポート

- ASA と Cisco ISE ポリシー ノードが、同じ NTP サーバを使用して同期されていることを確認します。
- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

ローカル CA 証明書データベース

ローカル CA 証明書データベースを維持するため、データベースに変更が加えられるたびに **write memory** コマンドを使用して、証明書データベース ファイル LOCAL-CA-SERVER.cdb を保存してください。ローカル CA 証明書データベースには、次のファイルが含まれます。

- LOCAL-CA-SERVER.p12 は、ローカル CA サーバを最初にイネーブルにしたときに生成されたローカル CA 証明書とキー ペアのアーカイブです。
- LOCAL-CA-SERVER.crl ファイルは、実際の CRL です。
- LOCAL-CA-SERVER.ser ファイルでは、発行済み証明書のシリアル番号が追跡されます。

その他のガイドライン

- ASA が CA サーバまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してください。このガイドラインは、サードパーティ ベンダーからインポートした証明書にも適用されます。
- フェールオーバーがイネーブルになっている場合、ローカル CA は設定できません。ローカル CA サーバを設定できるのは、フェールオーバーのないスタンドアロン ASA のみです。詳細については、「CSCty43366」を参照してください。

- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- **lifetime ca-certificate** コマンドは、ローカル CA サーバ証明書の初回生成時（初めてローカル CA サーバを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。
- 管理インターフェイスへの ASDM トラフィックと HTTPS トラフィックを保護するために、アイデンティティ証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はリブートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこのプロシージャの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA および AnyConnect クライアントで検証できるのは、[X520Serialnumber] フィールド（[Subject Name] のシリアル番号）が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。
- ワイルドカード（*）記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA は、インポート中に無効な文字または値が見つかると、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

デジタル証明書の設定

ここでは、デジタル証明書の設定方法について説明します。

参照 ID の設定

ASA が TLS クライアントとして動作する場合、ASA は RFC 6125 で定義されているアプリケーション サーバの ID の検証ルールをサポートします。この RFC では、参照 ID を表現（ASA 上で設定）し、（アプリケーション サーバから送信）提示された ID に対して参照 ID を照合する手順を示しています。提示された ID が設定済みの参照 ID と一致しなければ、接続は確立されず、エラーがログに記録されます。

接続の確立中、サーバは自身の ID を提示するために、1 つ以上の識別子を含めたサーバ証明書を ASA に提示します。ASA で設定される参照 ID は、接続の確立中にサーバ証明書で提示される ID と比較されます。これらの ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。4 つの ID タイプは次のとおりです。

- CN_ID：証明書のサブジェクト フィールドに設定される、共通名（CN）タイプの 1 つの属性タイプと値のペアだけが含まれる相対識別名（RDN）。この値は、完全な形のドメイン名と一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
- DNS-ID：dNSName タイプの subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
- SRV-ID：RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
- URI-ID：uniformResourceIdentifier タイプの subjectAltName エントリ。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。

参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

始める前に

- 参照 ID は、syslog サーバおよびスマート ライセンス サーバへの接続時にのみ使用されます。その他の ASA SSL クライアント モードの接続では、現時点では、参照 ID の設定や使用はサポートされていません。
- 対話式クライアントの固定証明書およびフォールバックを除き、ASA は RFC 6125 で説明されている ID と一致させるためのすべてのルールを実装します。

- 証明書を固定する機能は実装されません。したがって、「No Match Found, Pinned Certificate」メッセージが発生することはありません。また、シスコで実装するクライアントは対話式クライアントではないため、一致が見つからない場合にユーザが証明書を固定することもできません。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Reference Identity] に移動します。

設定済みの参照 ID がリストされます。新しい参照 ID を追加するには [Add] をクリックします。既存の参照 ID を編集するには、対象の参照 ID を選択してから [Edit] をクリックします。既存の参照 ID を削除するには、対象の参照 ID を選択してから [Delete] をクリックします。使用中の参照 ID を削除することはできません。

ステップ 2 参照 ID を作成または変更するには、それぞれ [Add]、[Edit] をクリックします。

[Add Reference Identity] または [Edit Reference Identity] ダイアログボックスを使用して、参照 ID を選択および指定します。

- 参照 ID には、任意のタイプの複数の参照 ID を追加できます。
- 参照 ID を設定した後に、その名前を変更することはできません。名前を変更するには、参照 ID を削除してから作成し直す必要があります。

次のタスク

設定した参照 ID は、syslog および Smart Call Home サーバ接続を設定する際に使用します。

特定の証明書タイプの設定方法

信頼できる証明書を確立すると、アイデンティティ証明書の確立などの基本的なタスクや、ローカル CA 証明書やコード署名証明書の確立などのさらに高度な設定を行なえるようになります。

始める前に

デジタル証明書情報に目を通し、信頼できる証明書を確立します。秘密キーが設定されていない CA 証明書は、すべての VPN プロトコルと webvpn で使用され、トラストポイントで着信クライアント証明書を検証するように設定されています。また、トラストポイントとは、HTTPS サーバにプロキシ接続された接続を検証し、smart-call-home 証明書を検証する、webvpn 機能によって使用される信頼できる証明書の一覧のことです。

手順

ステップ 1 アイデンティティ証明書は、対応する秘密キーとともに ASA に設定される証明書です。これは、SSL サービスや IPsec サービスを確立する際のアウトバウンドの暗号化またはシグネチャの生成に使用され、トラストポイントを登録することによって取得されます。アイデンティティ証明書を設定するには、ID 証明書 （16 ページ） を参照してください。

ステップ 2 ローカル CA を設定すると、VPN クライアントが ASA から証明書を直接登録できるようになります。この高度な設定により、ASA はCA に変換されます。CA を設定するには、CA Certificate （23 ページ） を参照してください。

ステップ 3 WebVPN Java コード署名機能の一部としてアイデンティティ証明書を使用する場合は、コード署名者証明書 （34 ページ） を参照してください。

次のタスク

証明書の有効期限にアラートを設定するか、デジタル証明書や証明書の管理履歴をモニタします。

ID 証明書

アイデンティティ証明書は、ASA 内の VPN アクセスの認証に使用できます。

[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- アイデンティティ証明書の追加またはインポート （16 ページ）。
- CA からの要求として CMPv2 登録の有効化
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。
- アイデンティティ証明書のエクスポート （21 ページ）。
- 証明書有効期限のアラートを設定する。
- Etrust でアイデンティティ証明書を登録する証明書署名要求の生成 （21 ページ）。

アイデンティティ証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Identity Certificates]** の順に選択します。

ステップ 2 [Add] をクリックします。

選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。

ステップ 3 [Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)] オプション ボタンをクリックして、既存のファイルから ID 証明書をインポートします。

ステップ 4 PKCS12 ファイルの復号化に使用するパスフレーズを入力します。

ステップ 5 ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。

ステップ 6 [Add a new Global Controller] オプション ボタンをクリックして、新しい ID 証明書を追加します。

ステップ 7 [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。

ステップ 8 **RSA** または **ECDSA** キーのタイプを選択します。

ステップ 9 [Use default keypair name] オプション ボタンをクリックして、デフォルトのキー ペア名を使用します。

ステップ 10 [Enter a new key pair name] オプション ボタンをクリックして、新しい名前を入力します。

ステップ 11 ドロップダウン リストから係数サイズを選択します。係数サイズが不明な場合は、Entrust にお問い合わせください。

ステップ 12 [General purpose] オプション ボタン（デフォルト）または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、ASA により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。

ステップ 13 [Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の表示専用の情報が示されます。

- 公開キーが認証の対象となるキー ペアの名前。
- キー ペアの生成日時。
- RSA キー ペアの用途。
- キー ペアの係数サイズ（512、768、1024、2048、および 4096 ビット）。デフォルトは 1024 です。
- テキスト形式の特定のキー データを含むキー データ。

ステップ 14 完了したら、[OK] をクリックします。

ステップ 15 ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。その後、[Select] をクリックして [Certificate Subject DN] ダイアログボックスを表示します。

ステップ 16 ドロップダウンリストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- **Common Name（CN）**
- **Department（OU）**

- **Company Name（O）**
- **Country（C）**
- **State/Province（ST）**
- **Location（L）**
- **E-mail Address（EA）**

ステップ 17 完了したら、[OK] をクリックします。

ステップ 18 自己署名証明書を作成するには、[Generate self-signed certificate] チェック ボックスをオンにします。

ステップ 19 アイデンティティ証明書をローカル CA として機能させるには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

ステップ 20 追加のアイデンティティ証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

（注） 登録モード設定と SCEP チャレンジ パスワードは自己署名証明書では使用できません。

ステップ 21 [Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN（完全修飾ドメイン名）。
- ID 証明書に関連付けられている電子メール アドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [Include serial number of the device] チェックボックスをオンにして、ASA のシリアル番号を証明書パラメータに追加します。

ステップ 22 [Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。[Request from a CA] を選択して CMPV2 登録を有効にする場合は、CA からの要求としての CMPv2 登録の有効化 （19 ページ）を参照してください。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行分数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 23 [SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード

- SCEP パスワードを確認のために再入力

ステップ 24 完了したら、[OK] をクリックします。

ステップ 25 この証明書で他の証明書に署名できるようにする場合は、[Enable CA flag in basic constraints extension] をオンにします。

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。このオプションをオンのままにしておいても、特に問題はありません。

ステップ 26 [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

ステップ 27 [Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

ステップ 28 [Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ステップ 29 ID 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA からの要求としての CMPv2 登録の有効化

LTE ワイヤレス ネットワークでセキュリティ ゲートウェイ デバイスとして機能するために、ASA は Certificate Management Protocol（CMPv2）を使用していくつかの証明書管理機能をサポートします。ASA デバイス証明書の登録に CMPv2 を使用することで、CMPv2 が有効な CA からの最初の証明書とセカンダリ証明書を手動登録したり、同じキーペアを使用する以前に発行済みの証明書を差し替えるための証明書を手動更新したりできます。受信した証明書は従来の設定の外部に保存され、証明書が有効になっている IPsec の設定で使用されます。

（注） ASA では CMPv2 のすべての機能を利用できるわけではありません。

最初の要求で CA との信頼を確立し、最初の証明書を取得します。CA 証明書はトラストポイントで事前に設定される必要があります。インストール中の証明書のフィンガープリントを認知すると、認証が実行されます。

[Advanced Options] ウィンドウの [Enrollment Mode] タブ上で [Request from a CA] をクリックした後、CMPv2 登録のために以下の手順を実行します。

始める前に

アイデンティティ証明書の追加またはインポート （16 ページ） の手順を実行します。

手順

ステップ 1 CMP を登録プロトコルとして選択し、http:// 領域に CMP URL を入力します。

ステップ 2 すべての CMP 手動/自動登録用に自動的に新しいキー ペアを生成するには、[RSA] または [EDCSA] を選択します。

[RSA] を選択した場合、[Modulus] ドロップダウン メニューから値を選択します。[EDCSA] を選択した場合、楕円曲線のドロップダウン メニューから値を選択します。

ステップ 3 （オプション）証明書の更新中、あるいは登録要求の作成前にキー ペアを生成するには、[Regenerate the key pair] をクリックします。

ステップ 4 [Shared Key] をクリックし、CA によってアウトオブバンド提供された値を入力します。この値は、CA および ASA が交換するメッセージの信頼性および整合性を確認するために使用されます。

ステップ 5 [Signing Trustpoint] をクリックし、CMP 登録要求に署名する際に使用された発行済みデバイス証明書を含むトラストポイントの名前を入力します。

これらのオプションは、トラストポイント登録プロトコルが CMP に設定されているときにのみ使用できます。CMP トラストポイントが設定されている場合、共有秘密または署名証明書のいずれかを指定ができますが、両方は指定できません。

ステップ 6 CA 証明書を指定するには [Browse Certificate] をクリックします。

ステップ 7 （オプション）CMPv2 の自動登録を起動するには、[Auto Enroll] チェックボックスをオンにします。

ステップ 8 [Auto Enroll Lifetime] フィールドには、自動登録が必要になるまでの、証明書の絶対的な有効期間のパーセンテージを入力します。

ステップ 9 証明書の更新中に新しいキーを生成するには、[Auto Enroll Regenerate Key] をクリックします。

アイデンティティ証明書のエクスポート

ID 証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2 証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 3 [PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。

ステップ 4 PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。

ステップ 5 暗号化パスフレーズを確認のために再入力します。

ステップ 6 [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

証明書署名要求の生成

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

手順

ステップ 1 [Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。

ステップ 2 [Key Pair] 領域で次の手順を実行します。

a) ドロップダウン リストから、設定されたキー ペアのいずれかを選択します。

b) [Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキー データといった情報が示されます。

c) 完了したら、[OK] をクリックします。

d) [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。生成したキー ペアを ASA に送信するか、ファイルに保存することができます。

ステップ 3 [Certificate Subject DN] 領域に次の情報を入力します。

a) ASA の FQDN または IP アドレス。

b) 会社の名前。

c) 2 文字の国番号。

ステップ 4 [Optional Parameters] 領域で次の手順を実行します。

a) [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。
b) ドロップダウンリストから追加する属性を選択し、値を入力します。
c) [Add] をクリックして、各属性を [attribute] テーブルに追加します。
d) [Delete] をクリックして、[attribute] テーブルから属性を削除します。
e) 完了したら、[OK] をクリックします。

[Additional DN Attributes] フィールドに追加された属性が表示されます。

ステップ 5 CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

ステップ 6 [Generate Request] をクリックして、証明書署名要求を生成します。これを Entrust に送信することも、ファイルに保存して後で送信することもできます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

ステップ 7 [request a certificate from Entrust] リンクをクリックして、登録プロセスを完了します。その後、示された CSR をコピーして貼り付け、それを Entrust Web フォーム（http://www.entrust.net/cisco/）を使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインで [enroll with Entrust] リンクをクリックします。

ステップ 8 Entrust により、要求の認証が確認された後、証明書が発行されます。これには数分かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。

ステップ 9 [Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

アイデンティティ証明書のインストール

新しい ID 証明書をインストールするには、次の手順を実行します。

手順

ステップ 1 [Identity Certificates] ペインで [Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。

ステップ 2 [Add a new identity certificate] オプション ボタンをクリックします。

ステップ 3 キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。

ステップ 4 証明書サブジェクト DN 情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5 関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 6 [Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。

ステップ 7 以降の手順については、アイデンティティ証明書の追加またはインポート （16 ページ）の手順 17 ～ 23 を参照してください。

ステップ 8 [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificate Request] ダイアログボックスが表示されます。

ステップ 9 テキスト タイプの CSR ファイル名（c:\verisign-csr.txt など）を入力し、[OK] をクリックします。

ステップ 10 CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。

ステップ 11 CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。

[Install Identity Certificate] ダイアログボックスが表示されます。

ステップ 12 該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- Install from a file

  または、[Browse] をクリックし、ファイルを検索します。

- Paste the certificate data in base-64 format

  コピーした証明書データを指定された領域に貼り付けます。

ステップ 13 [Install Certificate] をクリックします。

ステップ 14 [Apply] をクリックし、新しくインストールした証明書とその ASA コンフィギュレーションを保存します。

ステップ 15 選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

[General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。

[Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。

[Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ステップ 16 コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA Certificate

このページで、CA 証明書を管理します。次のトピックでは、実行できることについて説明します。

CA 証明書の追加またはインストール

CA 証明書を追加またはインストールするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[CA Certificates]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Install Certificate] ダイアログボックスが表示されます。

ステップ 3 [Install from a file] オプション ボタンをクリックして、既存のファイルから証明書設定を追加します（これがデフォルト設定です）。

ステップ 4 パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。

ステップ 5 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 6 [Paste certificate in PEM format] オプション ボタンをクリックして、手動で登録します。

ステップ 7 PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。

ステップ 8 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 9 [Use SCEP] オプション ボタンをクリックして、自動で登録します。ASA が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザは次の情報を入力する必要があります。

- 自動インストールする証明書のパスとファイル名。
- 証明書のインストールの最大再試行分数。デフォルトは 1 分です。
- 証明書のインストールの再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 10 新規および既存の証明書のその他のコンフィギュレーション オプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

ステップ 11 既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

ステップ 12 CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

ステップ 13 [Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

失効に関する CA 証明書の設定

失効に関して CA 証明書を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Revocation Check] タブをクリックします。

ステップ 3 証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

ステップ 4 1 つ以上の失効チェック方式（CRL または OCSP）を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

ステップ 5 [Add] をクリックして失効方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。

選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。

ステップ 6 証明書の検証中に失効チェックのエラーを無視するには、[Consider certificate valid if revocation checking returns errors] チェックボックスをオンにします。

ステップ 7 [OK] をクリックして、[Revocation Check] タブを閉じます。

CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。

ステップ 3 [Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。

ステップ 4 [Static Configuration] 領域の [Add] をクリックします。

[Add Static URL] ダイアログボックスが表示されます。

ステップ 5 CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。

入力した URL が [Static URLs] リストに表示されます。

ステップ 6 [OK] をクリックして、このダイアログボックスを閉じます。

CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [CRL Retrieval Methods] タブをクリックします。

ステップ 3 次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 を使用されます。次の必須パラメータを入力します。
  - **Name**

- **Password**
- **Confirm Password**
- **デフォルト サーバ**（サーバ名）
- **デフォルト ポート**（389）

- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。

ステップ 4 [OK] をクリックして、このタブを閉じます。

OCSP ルールの設定

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

始める前に

OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラー メッセージが表示されます。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [OCSP Rules] タブをクリックします。

ステップ 3 この OCSP ルールと一致する証明書マップを選択します。証明書マップにより、ユーザ権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、ASA において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールのプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバの URL が表示されます。

ステップ 4 [Add] をクリックします。

[Add OCSP Rule] ダイアログボックスが表示されます。

ステップ 5 使用する証明書マップをドロップダウン リストから選択します。

ステップ 6 使用する証明書をドロップダウン リストから選択します。

ステップ 7 ルールのプライオリティ番号を入力します。

ステップ 8 この証明書の OCSP サーバの URL を入力します。

ステップ 9 完了したら、[OK] をクリックして、このダイアログボックスを閉じます。

新しく追加された OCSP ルールがリストに表示されます。

ステップ 10 [OK] をクリックして、このタブを閉じます。

高度な CRL および OCSP の設定

CRL および OCSP の追加設定を行うには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [Advanced] タブをクリックします。

ステップ 3 [CRL Options] 領域にキャッシュの更新間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

ステップ 4 [Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。

ステップ 5 [OCSP Options] 領域に OCSP サーバの URL を入力します。ASA で使用される OCSP サーバは、次の順で選択されます。

a) 一致証明書上書きルールの OCSP URL に対応するサーバ
b) 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバ
c) ユーザ証明書の AIA フィールド

ステップ 6 デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイアタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

ステップ 7 [Other Options] 領域で、次のいずれかのオプションを選択します。

- 指定した CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

ステップ 8 [OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

ローカル CA サーバの設定

ASA でローカル CA サーバを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [CA Server]** の順に選択します。

ステップ 2 ローカル CA サーバをアクティブにするには、[Enable Certificate Authority Server] チェックボックスをオンにします。デフォルト設定は、ディセーブル（オフ）です。ローカル CA サーバをイネーブルにすると、ASA によりローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルが生成され、ローカル CA サーバ証明書とキー ペアが PKCS12 ファイルにアーカイブされます。

（注） 設定済みのローカル CA をイネーブルにする前に、オプションのすべての設定を慎重に見直してください。イネーブルにした後で、証明書の発行者名とキー サイズ サーバ値を変更することはできません。

自己署名した証明書のキーの使用拡張により、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名がイネーブルになります。

ステップ 3 ローカル CA を初めてイネーブルにするときには、英数字のイネーブル パスフレーズを入力し、確認のために再入力する必要があります。イネーブル パスフレーズは、7 文字以上の英数字である必要があります。このパスフレーズにより、ストレージにアーカイブされたローカル CA 証明書およびローカル CA 証明書のキー ペアが保護され、不正なシャットダウンや予期しないシャットダウンが発生しないようにローカル CA サーバが保護されます。ローカル CA 証明書またはキーペアが失われ、その復元が必要となった場合、PKCS12 アーカイブのロックを解除するためには、このパスフレーズが必要です。

（注） ローカル CA サーバをイネーブルにするには、イネーブル パスフレーズが必要です。イネーブル パスフレーズの記録は、必ず安全な場所に保管してください。

ステップ 4 ASA をリブートしてもコンフィギュレーションが失われないように、[Apply] をクリックして、ローカル CA 証明書とキー ペアを保存します。

ステップ 5 ローカル CA の初回設定後にローカル CA を変更または再設定する場合は、[Enable Certificate Authority Server] チェックボックスをオフにして、ASA 上のローカル CA サーバをシャットダウンする必要があります。この状態では、コンフィギュレーションおよびすべての関連ファイルはストレージ内に保持され、登録はディセーブルになっています。

設定したローカル CA がイネーブルになると、次の 2 つの設定が表示専用になります。

- [Issuer Name] フィールド。発行元のサブジェクト名とドメイン名がリストで示されます。これは、ユーザ名とサブジェクト名のデフォルト DN 設定により構成され、cn=FQDN という形式で示されます。ローカル CA サーバは、証明書を付与するエンティティです。証明書のデフォルト名は、cn=hostname.domainname という形式で表示されます。
- [CA Server Key Size] 設定。これは、ローカル CA サーバに生成されるサーバ証明書を対象とします。キー サイズには、キーごとに 512、768、1024、2048、または 4096 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キー サイズは 2048 以上を使用することをお勧めします。

ステップ 6 ドロップダウン リストから、ローカル CA サーバが発行した各ユーザ証明書に対して生成されるキー ペアのクライアント キー サイズを選択します。キー サイズには、キーごとに 512、768、1024、2048、または 4096 ビットのいずれかを指定できます。デフォルトは、1 つのキーあたり 1024 ビットです。キー サイズは 2048 以上を使用することをお勧めします。

ステップ 7 CA 証明書のライフタイム値を入力します。これは、CA サーバ証明書の有効期間を日数単位で指定するものです。デフォルトは 3650 日（10 年）です。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。

期限切れが近付いていることをユーザに通知するために、次の syslog メッセージが [Latest ASDM Syslog Messages] ペインに表示されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and
a replacement certificate is available for export.
```

（注） この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

ステップ 8 クライアント証明書のライフタイム値を入力します。これは、CA サーバが発行したユーザ証明書の有効期間を日数単位で指定するものです。365 日（1 年）です。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

ステップ 9 [SMTP Server & Email Settings] 領域で次の設定を指定することで、ローカル CA サーバの電子メール アクセスを設定します。

a) SMTP メール サーバ名または IP アドレスを入力します。または、省略符号（[...]）をクリックして [Browse Server Name/IP Address] ダイアログボックスを表示し、ここからサーバ名または IP アドレスを選択します。完了したら、[OK] をクリックします。

b) ローカル CA ユーザに電子メール メッセージを送信する際に使用する From アドレスを「adminname@host.com」という形式で入力します。自動電子メール メッセージは、新規登録ユーザへのワンタイム パスワードの送信や、証明書の更新が必要なときの電子メール メッセージの発行に使用されます。

c) ローカル CA サーバからユーザに送信されるすべてのメッセージで使用される件名を入力します。件名を指定しない場合のデフォルトは「Certificate Enrollment Invitation」です。

ステップ 10 追加オプションを設定するには、[More Options] ドロップダウン矢印をクリックします。

ステップ 11 CRL 分散ポイント（ASA 上の CRL の場所）を入力します。デフォルトの場所は http://hostname.domain/+CSCOCA+/asa_ca.crl です。

ステップ 12 特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにするには、ドロップダウン リストから publish-CRL インターフェイスを選択します。次に、1 ～ 65535 の任意のポート番号を入力します。デフォルトのポート番号は TCP ポート 80 です。

（注） CRL の名前は変更できません。LOCAL-CA-SERVER.crl という名前が常に使用されます。

たとえば、http://10.10.10.100/user8/my_crl_file という URL を入力します。この場合、指定された IP アドレスを持つインターフェイスのみが動作します。要求を受信すると、ASA によってパス /user8/my_crl_file と設定済み URL が照合されます。パスが一致すると、ASA から、保存されている CRL ファイルが返されます。

ステップ 13 CRL の有効期間である CRL ライフタイムを時間単位で入力します。CA 証明書のデフォルトは 6 時間です。

ローカル CA では、ユーザ証明書が失効するたびまたは失効解除されるたびに、更新された CRL が再発行されますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回しか行われません。[CA Certificates] ペインで [Request CRL] をクリックすると、CRL を即時に更新して再生成できます。

ステップ 14 データベース ストレージの場所を入力して、ローカル CA コンフィギュレーションとデータファイル用のストレージ領域を指定します。ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CA データベースが使用されます。外部ファイルを指定する場合は、外部ファイルへのパス名を入力するか、[Browse] をクリックして [Database Storage Location] ダイアログボックスを表示します。

ステップ 15 表示されるフォルダのリストからストレージの場所を選択し、[OK] をクリックします。

（注） フラッシュ メモリには、3500 人以下のユーザを持つデータベースを保存できます。ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ステップ 16 発行された証明書のユーザ名に追加されるデフォルト サブジェクト（DN 文字列）を入力します。次に示す DN 属性を指定できます。

- **CN（一般名）**
- **SN（姓名の姓）**
- **O（組織名）**
- **L（地名）**
- **C（国）**
- **OU（組織ユニット）**

- **EA（電子メール アドレス）**
- **ST（州/都道府県）**
- **T（タイトル）**

ステップ 17 登録されたユーザがユーザ証明書を登録および取得するための PKCS12 登録ファイルを取得できる期間を、時間単位で入力します。この登録期間は、ワンタイムパスワード（OTP）の有効期間とは関係ありません。デフォルトは 24 時間です。

（注） ローカル CA の証明書の登録は、クライアントレス SSL VPN 接続でのみサポートされます。このタイプの接続の場合、クライアントと ASA の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

ステップ 18 登録ユーザに電子メールで送信されたワンタイムパスワードの有効期間を入力します。デフォルトは 72 時間です。次に、[Email OTP] をクリックします。

OTP が新規ユーザに送信されたことを示す [Information] ダイアログボックスが表示されます。

[Replace OTP] をクリックし、自動的に新しい OTP を再発行して、新しいパスワードが記載された電子メール通知を既存のユーザまたは新規ユーザに送信します。

OTP を表示または再生成するには、リストからユーザを選択し、[View/Regenerate OTP] をクリックして [View & Regenerate OTP] ダイアログボックスを表示します。

現在の OTP が表示されます。

[Regenerate OTP] をクリックします。

新しく再生成された OTP が表示されます。

ステップ 19 [OK] をクリックします。

ステップ 20 期限の何日前になったら、ユーザに期限切れ通知の電子メールを送信するかを入力します。デフォルトは、14 日です。

ステップ 21 [Apply] をクリックし、新しいまたは変更された CA 証明書コンフィギュレーションを保存します。

ASA からローカル CA サーバを削除するには、[Delete Certificate Authority Server] をクリックして [Delete Certificate Authority] ダイアログボックスを表示します。[OK] をクリックします。

（注） 削除したローカル CA サーバは、復元および復旧できません。削除した CA サーバ コンフィギュレーションを再作成する場合は、CA サーバ コンフィギュレーション情報をすべて再入力する必要があります。

CA サーバ管理

ローカル CA ユーザの追加

ローカル CA 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 新しいユーザをローカル CA データベースに追加するには、[Add] をクリックして、[Add User] ダイアログボックスを表示します。

ステップ 2 有効なユーザ名を入力します。

ステップ 3 既存の有効な電子メール アドレスを入力します。

ステップ 4 サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5 ドロップダウン リストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- **Common Name（CN）**
- **Department（OU）**
- **Company Name（O）**
- **Country（C）**
- **State/Province（ST）**
- **Location（L）**
- **E-mail Address（EA）**

ステップ 6 完了したら、[OK] をクリックします。

ステップ 7 [Allow enrollment] チェック ボックスをオンにしてユーザを登録し、[Add User] をクリックします。

[Manage User Database] ペインに新しいユーザが表示されます。

ローカル CA ユーザの編集

データベース内の既存のローカル CA ユーザに関する情報を変更するには、次の手順を実行します。

手順

ステップ 1 特定のユーザを選択し、[Edit] をクリックして [Edit User] ダイアログボックスを表示します。

ステップ 2 有効なユーザ名を入力します。

ステップ 3 既存の有効な電子メール アドレスを入力します。

ステップ 4 サブジェクト（DN 文字列）を入力します。または、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5 ドロップダウン リストから変更する DN 属性を 1 つ以上選択し、値を入力し、[Add] または [Delete] をクリックします。

ステップ 6 完了したら、[OK] をクリックします。

ユーザをデータベースから削除し、そのユーザに発行されたすべての証明書をローカル CA データベースから削除するには、ユーザを選択し、[Delete] をクリックします。

（注） 削除されたユーザは復元できません。削除したユーザ レコードを再作成するには、[Add] をクリックして、そのユーザの情報をすべて再入力します。

ステップ 7 [Allow enrollment] チェック ボックスをオンにしてユーザを登録し、[Edit User] をクリックします。

（注） ユーザがすでに登録されている場合は、エラー メッセージが表示されます。

[Manage User Database] ペインに更新されたユーザ詳細が表示されます。

コード署名者証明書

コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

手順

ステップ 1 [Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。

ステップ 2 PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 3 インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

ステップ 4 インポートするファイルを選択し、[Import ID Certificate File] をクリックします。

[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 5 [Import Certificate] をクリックします。

[Code Signer] ペインにインポートされた証明書が表示されます。

ステップ 6 [Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。

コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2 証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。

ステップ 3 公開キー暗号化標準（base64 エンコードまたは 16 進数形式を使用できます）を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。

ステップ 4 [Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 5 ファイルを選択し、[Export ID Certificate File] をクリックします。

[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 6 エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 7 復号化パスフレーズを確認のために再入力します。

ステップ 8 [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

証明書の有効期限アラートの設定（ID 証明書または CA 証明書用）

ASA は、トラストポイントの CA 証明書および ID 証明書について有効期限を24時間ごとに 1 回チェックします。証明書の有効期限がまもなく終了する場合、syslog がアラートとして発行されます。

更新リマインダに加え、コンフィギュレーションに期限が切れた証明書が見つかった場合、その証明書を更新するか、または削除することで、コンフィギュレーションを修正するために syslog が毎日 1 回生成されます。

たとえば、有効期限アラートが 60 日に開始され、その後 6 日ごとに繰り返すように設定されているとします。ASAが 40 日に再起動されると、アラートはその日に送信され、次のアラートは 36 日目に送信されます。

（注） 有効期限チェックは、トラストプールの証明書では実行されません。ローカルCA トラストポイントは、有効期限チェックの通常のトラストポイントとしても扱われます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate/CA Certificate]** を参照します。

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

ステップ 3 目的の日数を入力します。

- [Repeat the alert for]：最初のアラートが発行される有効期限までの日数（1 ～ 90）を設定します。
- [Repeat the alert for]：証明書が更新されない場合のアラート頻度（1 ～ 14 日）を設定します。デフォルトでは、最初のアラートは有効期限の 60 日前に送信され、その後は証明書が更新または削除されるまで毎週 1 回送信されます。また、アラートは有効期限日に送信され、その後は毎日 1 回送信され、アラートの設定に関係なく、有効期限の直前の週はアラートが毎日送信されます。

デジタル証明書のモニタリング

デジタル証明書ステータスのモニタリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [CRL]**

  このペインには、CRL の詳細が表示されます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

証明書管理の履歴

表 *1:* 証明書管理の履歴

機能名	プラットフォーム リリース	説明
証明書管理	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。 次の画面が導入されました。 [Configuration] > [Remote Access VPN] > [Certificate Management Configuration] > [Site-to-Site VPN] > [Certificate Management]。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [CA Certificates Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]。
証明書管理	7.2(1)	
証明書管理	8.0(2)	
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。

機能名	プラットフォーム リリース	説明
参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバ ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバとスマート ライセンス サーバへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次の画面を変更しました。[Configuration] > [Remote Access VPN] > [Advanced Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add/Edit Configuration] > [Device Management] > [Smart Call Home]。
ローカル CA サーバ	9.12(1)	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、crypto ca server の smpt モードに追加されます。 ローカル CA サーバは廃止され、以降のリリースで削除されます。ASA がローカル CA サーバとして設定されている場合、デジタル証明書の発行、証明書失効リスト（CRL）の発行、および発行された証明書の安全な取り消しを行うために有効になります。この機能は古くなったため、crypto ca server コマンドは廃止されています。