CHAPTER 38

証明書の設定

デジタル証明書は、認証のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、社名、部署、IP アドレスなどのデバイスまたはユーザを特定する情報が含まれています。CA は、公開鍵 / 秘密鍵の暗号化を使用してセキュリティを確保する PKI のコンテキストでデジタル証明書を発行します。CA は、証明書に「署名」してその信頼性を確認し、デバイスまたはユーザの ID を保証する信頼できる認証局です。

デジタル証明書を使用する認証の場合、セキュリティ アプライアンスに 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。これによって、複数の ID、ルートおよび証明書の階層が許可されます。次のような異なるタイプのデジタル証明書があります。

- *CA 証明書*は、他の証明書に署名するために使われるものです。自己署名される CA 証明書は*ルート証明書*と呼ばれ、他の CA 証明書によって発行される CA 証明書は*下位証明書*と呼ばれます。「CA 証明書の認証」を参照してください。
- また、CA は、特定のシステムまたはホストの証明書である *ID 証明書*も発行します。「ID 証明書の認証」を参照してください。
- *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の作成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発生元を示します。を参照してください。
- ローカル認証局（CA）は、セキュリティ アプライアンスの独立認証局機能を統合し、証明書の展開と、発行された証明書のセキュアな失効チェックを行います。ローカル CA は、ブラウザ Web ページ ログインによるユーザ登録に、証明書を認証するためのセキュアで設定可能な内部認証局機能を提供します。「ローカル認証局」、「ローカル CA 証明書の管理」および「ローカル CA ユーザ データベースの管理」を参照してください。

CA 証明書の認証

CA Certificates パネルでは、自己署名証明書または下位 CA 証明書の認証とセキュリティ アプライアンスへのインストールを行うことができます。新しい証明書コンフィギュレーションを作成することも、既存の証明書コンフィギュレーションを編集することもできます。

選択した証明書が手動登録用に設定されている場合、このパネルで CA 証明書を手動で取得してインポートできます。選択した証明書が自動登録用に設定されている場合、セキュリティ アプライアンスは SCEP プロトコルを使用して CA にアクセスし、証明書を自動的に取得およびインストールします。

CA Certificates のフィールド

- **Certificates**：発行先および発行者によって識別される使用可能な証明書、証明書の期限が切れる日付、および証明書の使用方法または目的のリストを表示します。リストの証明書をクリックしてそのコンフィギュレーションを編集したり、新しい証明書を表示リストに追加したりできます。
- **Add ボタン**：リストに新しい証明書コンフィギュレーションを追加します。「CA 証明書の追加とインストール」を参照してください。
- **Edit ボタン**：既存の証明書コンフィギュレーションを変更します。「CA 証明書コンフィギュレーションの編集」を参照してください。
- **Show Details ボタン**：選択した証明書の詳細と発行者情報を表示します。「CA 証明書の詳細の表示」を参照してください。
- **Request CRL ボタン**：既存の CA 証明書の Certificate Revocation List（CRL; 証明書失効リスト）にアクセスします。「CRL の要求」を参照してください。
- **Delete ボタン**：既存の CA 証明書のコンフィギュレーションを削除します。「CA 証明書の削除」を参照してください。
- **Apply ボタン**：新規または変更した CA 証明書コンフィギュレーションを保存します。
- **Reset ボタン**：編集内容をすべて削除し、表示を元のコンテンツに戻します。

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
•	•	•	•	•

CA 証明書の追加とインストール

CA Certificate パネルでは、手動による証明書の貼り付けや自動登録を使用して、既存のファイルから新しい証明書コンフィギュレーションを追加できます。適切なオプションをクリックして、次のいずれかをアクティブにします。

- **Install from a File:**：既存のファイルから証明書コンフィギュレーションを追加するには、パスとファイル名を入力し、**Install Certificate** をクリックします。ボックスにファイルのパス名を入力することも、**Browse** をクリックしてファイルを検索することもできます。**Browse** をクリックすると Load CA certificate file ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。
- **Paste certificate in PEM format**：手動登録の場合、PEM 形式の証明書（base64 または 16 進数形式）をコピーしてパネルに貼り付け、**Install Certificate** をクリックします。

- **Use SCEP:**：自動登録の場合、セキュリティ アプライアンスは Simple Certificate Enrollment Protocol（SCEP）プロトコルを使用して CA にアクセスし、証明書を取得してデバイスにインストールします（SCEP）。SCEP は、ユーザによる介入が最小限ですむセキュアなメッセージ プロトコルです。SCEP を使用すると、VPN Concentrator Manager だけを使用して証明書を登録およびインストールできます。SCEP を使用するには、SCEP をサポートする CA に、インターネット経由で登録する必要があります。

  SCEP 自動登録には、次のフィールドを指定する必要があります。

  - **SCEP URL: HTTP://**：自動インストールする証明書のパスとファイル名を入力します。
  - **Retry Period**：証明書のインストールを再試行する時間の上限を分単位で指定します。デフォルトは 1 分です。
  - **Retry Count**：証明書のインストールの再試行回数を指定します。デフォルトは 0 です。これは、再試行時間内であれば無制限に再試行することを示します。

More Options...：新しい証明書に追加オプションを指定する場合、**More Options...** ボタンをクリックして新規および既存の証明書のコンフィギュレーション オプションを表示します。「CA 証明書の設定オプション」を参照してください。

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
•	•	•	•	•

CA 証明書コンフィギュレーションの編集

既存の証明書の特性を変更するには、証明書を選択し、**Edit** ボタンをクリックします。複数のタブが表示されるので、そこからタブを選択して CA 証明書コンフィギュレーションの詳細を指定します。詳細については、「CA 証明書の設定オプション」を参照してください。

CA 証明書の詳細の表示

Show Details ボタンをクリックすると、Certificate Details ダイアログボックスが表示されます。ここには選択した証明書に関する次の情報が表示されます。

- **General**：タイプ、シリアル番号、ステータス、使用方法、公開鍵タイプ、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証明書を表示します。これは、Available および Pending ステータスの両方に適用されます。
- **Issued to**：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を表示します。これは、Available ステータスだけに適用されます。
- **Issued by**：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。

CRL の要求

Request CRL ボタンを使用すると、現在のバージョンの証明書失効リスト（CRL）がアップデートされます。CRL アップデートにより、証明書ユーザの現在のステータスが提供されます。要求が失敗すると、エラー メッセージが表示されます。

CRL は、生成された後、期限が切れるまで自動的に再生成されます。**Request CRL** ボタンを使用すると、ただちに CRL ファイルの強制的なアップデートおよび再生成が行われます。

CA 証明書の削除

Delete ボタンをクリックすると、選択した CA 証明書コンフィギュレーションがただちにセキュリティ アプライアンスから削除されます。証明書コンフィギュレーションは、一度削除すると復元できません。削除された証明書を再作成するには、**Add** ボタンを使用して証明書コンフィギュレーション情報を最初から再入力する必要があります。

（注） 証明書コンフィギュレーションは、一度削除すると復元できません。

CA 証明書の設定オプション

Add ボタンで新しい CA 証明書を追加する場合と、**Edit** ボタンで既存の CA 証明書を変更する場合のどちらでも、追加の設定オプションを使用できます。

次のパネルからタブを選択し、CA 証明書コンフィギュレーションの詳細を指定します。各タブには、次の内容が表示されます。

Revocation Check ：Revocation Check パネルでは、失効チェックのオン / オフと失効チェック方法の指定（CRL または OCSP）ができます。また、証明書の検証時に失効チェック エラーを無視するように指定できます。Revocation Check パネルの詳細については、「失効チェックの設定」を参照してください。

CRL Retrieval Policy：CRL Retrieval Policy パネルでは、CRL 分散ポイントの使用やスタティック CRL URL の設定ができます。ステータス CRL URL の追加、編集、および削除もできます。詳細については、「CRL 取得ポリシーの設定」を参照してください。

CRL Retrieval Method：CRL Retrieval Method パネルでは、CRL 取得に使用する方式として、Lightweight Directory Access Protocol（LDAP）、HTTP、または Simple Certificate Enrollment Protocol（SCEP）を選択できます。LDAP 方式の場合、LDAP パラメータとセキュリティを設定できます。「CRL 取得方式の設定」を参照してください。

OCSP Rules：Online Certificate Status Protocol（OCSP）は、X.509 デジタル証明書の失効ステータスの取得に使用され、証明書失効リスト（CRL）の代替手段となります。詳細については、OSCP ルール コンフィギュレーションに関する説明を参照してください。「OCSP ルールの設定」を参照してください。

Advanced：Advanced パネルでは、CRL アップデート パラメータ、OCSP パラメータ、証明書の受け入れパラメータおよび検証パラメータを設定できます。**「高度な設定オプション」**を参照してください。

失効チェックの設定

Revocation Check Edit Option パネルでは、ユーザ証明書の失効チェックのレベルを次のように指定できます。

No Revocation Checking：**Do not check certificates for revocation** ボタンをクリックして証明書の失効チェックをディセーブルにします。

Revocation Checking Method(s)：**Check certificates for revocation** をクリックして失効チェック方式を 1 つ以上選択します。使用できる方式が左側に表示されるので、**Add** ボタンを使用して方式を右側に移動します。

選択した方式は、追加した順序で実装されます。ある方式でエラーが検出されると、後続の失効チェック方式がアクティブになります。

Revocation Checking Override：**Consider certificate valid if revocation checking returns errors** ボタンをクリックして失効チェックのエラーを無視します。

CRL 取得ポリシーの設定

CRL Retrieval Policy パネルでは、CRL 失効チェックの CRL 分散ポイントまたは固定の移動先を指定します。

- Certificate CRL Distribution Point：**Use CRL Distribution Point from the certificate** ボタンをクリックし、チェック中の証明書に含まれている CRL 分散ポイントに失効チェックを転送します。
- Static URL：**Use Static URLs configured below** ボタンをクリックし、CRL の取得に使用する特定の URL をリストします。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、後続の URL が順序に従ってアクセスされます。

://：CRL を分散する場所を入力します。

CRL 取得方式の設定

CRL Retrieval Method パネルでは、CRL の取得に使用する方式を選択できます。

- **Enable Lightweight Directory Access Protocol (LDAP)** ボタンをクリックして LDAP による CRL 取得を指定します。LDAP を使用すると、CRL の取得では、指定した LDAP サーバにパスワードでアクセスして接続し、LDAP セッションが開始されます。この接続はデフォルトで TCP ポート 389 を使用します。次の特定の必須 LDAP パラメータを入力します。
  - Name:
  - Password:
  - Confirm Password:
  - Default Server:（サーバ名）
  - Default Port: 389（デフォルト）
- HTTP：**Enable HTTP** ボタンをクリックして HTTP による CRL 取得を選択します。
- SCEP：**Enable Simple Certificate Enrollment Protocol (SCEP)** をクリックし、SCEP による CRL 取得を選択します。

OCSP ルールの設定

Online Certificate Status Protocol (OCSP) パネルでは、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 ルールを設定できます。

OCSP ルールのフィールド

- **Certificate Map**：この OCSP ルールに一致する証明書マップの名前を表示します。証明書マップは、ユーザ権限と証明書の特定のフィールドを照合します。OCSP ルールを設定する前に、証明書マップを設定する必要があります。
- **Certificate**：セキュリティ アプライアンスが応答側の証明書の検証に使用する CA の名前を表示します。
- **Index**：ルールのプライオリティ番号を表示します。セキュリティ アプライアンスは、プライオリティ順に OCSP ルールを検査し、一致する最初のルールを適用します。
- **URL**：この証明書の OCSP サーバの URL を指定します。
- **Add**：新しい OCSP ルールを追加します。
- **Edit**：既存の OCSP ルールを編集します。
- **Delete**：OCSP ルールを削除します。

高度な設定オプション

Advanced タブでは、CRL と OCSP のオプションを指定できます。証明書は、発行されると一定の期間有効です。CA は、この期間が終了する前に証明書を無効にすることがあります。たとえば、セキュリティ上の問題が起こる可能性がある場合や、名前やアソシエーションが変わった場合です。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ています。失効チェックをイネーブルにすることにより、セキュリティ アプライアンスに、CA が検証中の証明書を無効にしていないかをチェックさせるようにします。

セキュリティ アプライアンスは、CRL と OCSP という 2 つの失効ステータスのチェック方法をサポートします。

フィールド

- **CRL Options**
  - **Cache Refresh Time**：キャッシュのリフレッシュ間隔を分単位で指定します。デフォルトは 60 分で、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、セキュリティ アプライアンスは、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で累積されます。新しく取得した CRL をキャッシュすると保存制限を超えそうな場合、セキュリティ アプライアンスは使用頻度が最も低い CRL を削除して容量を空けます。
  - **Enforce next CRL update**：Next Update 値の有効期限が切れていない有効な CRL を要求します。このボックスをオフにすると、Next Update 値のない有効な CRL、または Next Update 値の有効期限が切れた有効な CRL が許可されます。
- **OCSP Options**
  - **Server URL:** : OCSP サーバの URL を入力します。セキュリティ アプライアンスは、OCSP サーバを次の順で使用します。

    1. 証明書の照合の上書き規則の OCSP URL
    2. この OCSP Options アトリビュートで設定した OCSP URL
    3. リモート ユーザ証明書の AIA フィールド
  - **Disable nonce extension**：デフォルトで、OCSP 要求には nonce 拡張が含まれます。nonce 拡張は、リプレイ攻撃を防ぐために、要求と応答を暗号化してバインドします。これは、要求の拡張と応答の拡張を照合し、それらが同一であることを確認して機能します。使用している OCSP サーバが、この一致する nonce 拡張を含まない生成済みの応答を送信する場合、nonce 拡張をディセーブルにします。
- **Accept certificates issued by this CA**：セキュリティ アプライアンスで、**CA Name** から証明書を受け取る必要があるかどうかを指定します。
- **Accept certificates issued by the subordinate CAs of this CA**
- **Validate the SSL client connections using this CA**：イネーブルにすると、この CA がリモート証明書を発行した CA に認証されている場合、リモート ユーザ証明書の検証時にアクティブなコンフィギュレーション設定をこの CA から取得できます。

ID 証明書の認証

ID 証明書は、セキュリティ アプライアンス経由の VPN アクセスの認証に使用できます。Identity Certificates パネルで、*SSL Settings* か *IPsec Connections* リンクをクリックして、追加のコンフィギュレーション情報を表示します。

Identity Certificates Authentication パネルでは、次の操作を実行できます。

- ID 証明書を追加する。「ID 証明書の追加とインストール」を参照してください。
- ID 証明書の詳細を表示する。「ID 証明書の詳細の表示」を参照してください。
- 既存の ID 証明書を削除する。「ID 証明書の削除」を参照してください。
- 既存の ID 証明書をエクスポートする。「ID 証明書のエクスポート」を参照してください。
- ID 証明書をインストールする。「ID 証明書のインストール」を参照してください。

ID 証明書の追加とインストール

Identity Certificate パネルでは、ファイルから既存の ID 証明書をインポートしたり、既存のファイルから新しい証明書コンフィギュレーションを追加したりできます。

適切なオプションをクリックして、次のいずれかをアクティブにします。

Add Identity Certificate のフィールド

Add Identity Certificate ダイアログボックスのフィールドに、次のように値を割り当てます。

- 既存のファイルから ID 証明書をインポートするには、**Import the identity certificate from a file** を選択し、次の情報を入力します。
  - Decryption Pass Phrase：PKCS12 ファイルの復号化に使用するパスフレーズを指定します。
  - File to Import From：ボックスにファイルのパス名を入力することも、**Browse** をクリックしてファイルを検索することもできます。**Browse** をクリックすると Load Identity Certificate file ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。
- 新しい ID 証明書を追加するには、次の情報が必要です。
  - Key Pair：RSA キー ペアは、ID 証明書の登録に必要です。セキュリティ アプライアンスでは、複数のキー ペアをサポートします。
  - Key Pair name（Key Pair > Show ウィンドウ）：公開鍵の認証が必要なキー ペアの名前を指定します。
  - Generation time（Key Pair > Show ウィンドウ）：キー ペアが生成された日付と時刻を表示します。
  - Usage（Key Pair > Show ウィンドウ）：RSA キー ペアの使用方法を表示します。RSA キーの使用方法には、*General Purpose*（デフォルト）と *Special* の 2 種類があります。Special を選択すると、セキュリティ アプライアンスは、署名用と暗号化用の 2 つのキー ペアを生成します。したがって、対応する ID ごとに 2 つの証明書が必要になります。
  - Modulus Size (bits)（Key Pair > Show ウィンドウ）：キー ペアの係数サイズが、512、768、1024 および 2048 で表示されます。デフォルトの係数サイズは 1024 です。
  - Key Data（Key Pair > Show ウィンドウ）：特定のキー データを含むウィンドウを示します。
  - Name（Key Pair > New ウィンドウ）：デフォルトのキー ペア名（<Default-RSA-Key>）を選択するか、新しいキー ペアの名前を入力します。
  - Size（Key Pair > New ウィンドウ）：デフォルトのキー ペア サイズを 512、788、1024（デフォルト）、または 2048 から選択します。
  - Usage（Key Pair > New ウィンドウ）：キー ペアの使用方法を *General purpose* または *Special* から選択します。

- **Add Identity Certificate** ペインの **Advanced** ボタンを使用すると、次の証明書パラメータと登録モードを設定できます。さらにオプションで、デバイス固有の ID 証明書の失効パスワードも設定できます。
  - **FQDN**（Advanced > Certificate Parameters）: あいまいでないドメイン名である Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）によって、DNS ツリー階層内のノードの位置を指定します。
  - **E-mail**（Advanced > Certificate Parameters）：ID 証明書に関連付けられている電子メール アドレス。
  - **IP Address**（Advanced > Certificate Parameters）: ネットワーク上のセキュリティ アプライアンスのアドレス。4 つの部分からなるドット付き 10 進数表記で指定します。
  - **Include serial number of the device** チェックボックスを使用すると、セキュリティ アプライアンスのシリアル番号を証明書パラメータに追加できます。
  - Advanced > Enrollment Mode では、手動登録（**Request by manual enrollment**）または CA による登録（**Request from a CA**）のどちらかを選択できます。CA による登録には次の情報を指定する必要があります。
  - **Enrollment URL (SCEP): HTTP://**：自動インストールする証明書のパスとファイル名を入力します。
  - **Retry Period**：ID 証明書のインストールを再試行する時間の上限を分単位で指定します。デフォルトは 1 分です。
  - **Retry Count**：ID 証明書のインストールの再試行回数を指定します。デフォルトは 0 です。これは、再試行時間内であれば無制限に再試行することを示します。
- **Add Identity Certificate** ペインに、次の証明書サブジェクト DN 情報を入力します。
  - **Certificate Subject DN**：証明書サブジェクト名 DN を指定して、ID 証明書内に DN を形成し、Certificate Subject DN ペインで **Select...** ボタンをクリックして DN アトリビュートを追加します。
  - **Attribute:**（Certificate Subject DN > Select ウィンドウ）: プルダウン メニューから DN アトリビュートを 1 つ以上選択します。Certificate Subject DN には、X.500 のアトリビュートとして次のフィールドを選択できます。

Certificate Subject DN のアトリビュート
CN = Common Name
OU = Department
O = Company Name
C = Country
ST = State/Province
L = Location
EA = E-mail Address

  - **Value**（Certificate Subject DN > Select ウィンドウ）: **Attribute** リストで選択した DN アトリビュートごとに値を入力します。アトリビュートに値を割り当てると、**Add** ボタンがアクティブになるので、このボタンを使用して右側にある Attribute/Value フィールドにアトリビュートを追加します。アトリビュートとその値を削除するには、アトリビュートを選択し、アクティブになった **Delete** ボタンをクリックします。

ID 証明書の設定が完了したら、Add Identity Certificate ペインの **Add Certificate** をクリックします。その後、必ず **Identity Certificates** ウィンドウの **Apply** ボタンをクリックして、新しい証明書コンフィギュレーションを保存します。

ID 証明書の詳細の表示

Show Details ボタンをクリックすると、Certificate Details ダイアログボックスが表示されます。ここには選択した証明書に関する次の情報が表示されます。

- **General**：タイプ、シリアル番号、ステータス、使用方法、公開鍵タイプ、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証明書を表示します。これは、Available および Pending ステータスの両方に適用されます。
- **Issued to**：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を表示します。これは、Available ステータスだけに適用されます。
- **Issued by**：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。

ID 証明書の削除

Delete ボタンをクリックすると、選択した ID 証明書コンフィギュレーションがセキュリティ アプライアンスからただちに削除されます。証明書コンフィギュレーションは、一度削除すると復元できません。削除した証明書を再作成するには、**Add** ボタンを使用して証明書コンフィギュレーション情報を最初から再入力します。

（注） 証明書コンフィギュレーションは、一度削除すると復元できません。

ID 証明書のエクスポート

Export パネルでは、PKCS12 形式のすべての関連付けられているキーおよび証明書と一緒に証明書コンフィギュレーションをエクスポートできます。これは base64 形式である必要があります。コンフィギュレーション全体には、チェーン全体（ルート CA 証明書、ID 証明書、キー ペア）が含まれますが、登録設定（サブジェクト名、FQDN など）は含まれません。通常、この機能は、フェールオーバーまたはロードバランシング コンフィギュレーションで使用され、セキュリティ アプライアンスのグループ間で証明書を複製します。たとえば、リモート アクセス クライアント コールをそのコールを提供する複数の装置を持つ中央組織に複製します。これらの装置には、同等の証明書コンフィギュレーションが必要です。この場合、管理者は、証明書コンフィギュレーションをエクスポートして、セキュリティ アプライアンスのグループ全体にインポートできます。

Export Identity Certificate のフィールド

- **Export to a file**：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指定します。
- Certificate Format：PKCS12 format または PEM format をクリックします。PKCS12 形式は公開鍵暗号化標準で、base64 エンコードまたは 16 進数を使用できます。
  - **Browse**：**Select a File** ダイアログボックスが表示され、ここで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に移動できます。
- **Encryption Passphrase**：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指定します。
  - **Confirm Passphrase**：暗号化パスフレーズを確認します。
- **Export Certificate**：証明書コンフィギュレーションをエクスポートします。

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
•	•	•	•	•

ID 証明書のインストール

Identity Certificates ウィンドウの **Install** ボタンは、保留中の登録がある場合だけアクティブになります。セキュリティ アプライアンスが Certificate Signing Request（CSR; 証明書署名要求）を受信すると常に、Identity Certificates ウィンドウに保留中の ID 証明書が表示されます。保留中の ID 証明書を選択すると、Install ボタンがアクティブになります。

保留中のファイルを CA に送信すると、CA がそのファイルを登録して証明書をセキュリティ アプライアンスに返します。証明書を取得したら、Install ボタンをクリックし、該当する ID 証明書と CA 証明書を選択して操作を完了します。

次の手順では、保留中の ID 証明書の追加およびインストールについて説明します。

ID 証明書を追加する手順

ステップ 1　**Identity Certificates** パネルで、**Add** ボタンをクリックします。

ステップ 2　**Add Identity Certificate** パネルで、**Add a new identity certificate** を選択します。

ステップ 3　オプションで、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　**Certificate Subject DN:** 情報を入力し、**Select...** ボタンをクリックします。

ステップ 5　**Certificate Subject DN** パネルで、関連する CA が要求するサブジェクト DN アトリビュートを必ずすべて指定します。「Certificate Subject DN のアトリビュート」を参照してください。次に、**OK** をクリックし、**Certificate Subject DN** パネルを閉じます。

ステップ 6　**Add Identity Certificate** パネルで、**Advanced...** ボタンをクリックします。

ステップ 7　**Advanced Options** パネルで、**FQDN:** フィールドがセキュリティ アプライアンスの正しい FQDN であることを確認し、**OK** をクリックしてウィンドウを閉じます。

ステップ 8　**Add Identity Certificate** パネルで、下部にある **Add Certificate** をクリックします。

ステップ 9　CSR の名前の入力を求めるプロンプトが表示されたら、テキスト タイプのアクセスしやすいファイル名（*c:\verisign-csr.txt* など）を入力します。

ステップ 10　CSR テキスト ファイルを CA に送信します。または、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。

ID 証明書をインストールする手順

ステップ 1　CA から ID 証明書が返されたら、Identity Certificates パネルに戻り、保留中の証明書エントリを選択して、アクティブになった **Install** ボタンをクリックします。

ステップ 2　新しくインストールされた証明書を SSL VPN で使用できるように割り当てるには、証明書リストの下にあるテキストの SSL Settings ホットリンクから **SSL Settings** パネルに移動します。

ステップ 3　**SSL Settings** パネルで、証明書に割り当てるインターフェイスをダブルクリックします。**Edit SSL Certificate** パネルが開きます。

ステップ 4　**Edit SSL Certificate** パネルで、**Certificate:** プルダウン リストから証明書を選択し、**OK** をクリックします。選択した ID 証明書は、選択した **Interface** フィールドの右にある **ID Certificate** フィールドに表示されます。

ステップ 5　必ず **SSL Settings** パネルの下部にある **Apply** ボタンをクリックして、新しくインストールした証明書を ASA コンフィギュレーションと一緒に保存します。

コード署名者証明書

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名は、署名者の認証と、コードが署名以降に変更されていないことの保証に十分な情報を提供します。

コード署名者証明書は、関連付けられている秘密鍵がデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。このパネルの **Import** ボタンを使用してコード署名者証明書をインポートしたり、Java Code Signer パネルで Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer を選択したりできます。

Code-signer Certificate Authentication パネルでは次の操作を実行できます。

- ID 証明書の詳細を表示する。「コード署名者証明書の詳細の表示」を参照してください。
- 既存の ID 証明書を削除する。「コード署名者証明書の削除」を参照してください。

既存の ID 証明書をエクスポートする。「コード署名者証明書のインポートまたはエクスポート」を参照してください。

コード署名者証明書の詳細の表示

Show Details ボタンをクリックすると、Code Signer Details ダイアログボックスが表示されます。ここには選択した証明書に関する次の情報が表示されます。

- **General**：タイプ、シリアル番号、ステータス、使用方法、公開鍵タイプ、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証明書を表示します。これは、Available および Pending ステータスの両方に適用されます。
- **Issued to**：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を表示します。これは、Available ステータスだけに適用されます。
- **Issued by**：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。

コード署名者証明書の削除

Delete ボタンをクリックすると、選択したコード署名者証明書コンフィギュレーションがセキュリティ アプライアンスからただちに削除されます。コンフィギュレーションは一度削除すると復元できません。コンフィギュレーションを再作成するには、**Import** ボタンを使用してコンフィギュレーション情報を最初から再入力する必要があります。

（注）　コード署名者コンフィギュレーションは、一度削除すると復元できません。

コード署名者証明書のインポートまたはエクスポート

Import Certificate ウィンドウのフィールドに、次のように値を割り当てます。

- **Decryption Passphrase**：PKCS12 ファイルの復号化に使用するパスフレーズを指定します。
- **File to Import From**：ボックスにファイルのパス名を入力することも、**Browse** をクリックしてファイルを検索することもできます。**Browse** をクリックすると **Import Certificate** ダイアログボックスが表示されます。ここで証明書が含まれるファイルに移動できます。

Export Certificate ウィンドウのフィールドに、次のように値を割り当てます。

- **Export to file**：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指定します。

- Certificate Format：**PKCS12 format** または **PEM format** をクリックします。PKCS12 形式は公開鍵暗号化標準で、base64 エンコードまたは 16 進数を使用できます。
  - **Browse**：**Select a File** ダイアログボックスが表示され、ここで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に移動できます。
- **Decryption Passphrase**：PKCS12 ファイルをエクスポート用に復号化するために使用するパスフレーズを指定します。
  - **Confirm Passphrase**：復号化パスフレーズを確認します。
- **Export Certificate**：コンフィギュレーションをエクスポートします。

ローカル認証局

ローカル認証局（CA）は、証明書を認証するためにセキュリティ アプライアンスに常駐する、セキュアで設定可能な内部認証局です。ユーザ登録はブラウザの Web ページへのログインによって行われます。ローカル CA は、セキュリティ アプライアンスの基本認証局機能を統合し、証明書の展開と、発行された証明書のセキュアな失効チェックを行います。

次の Local CA オプションを使用すると、ローカル CA サーバとユーザ データベースの初期化とセットアップを行うことができます。

- セキュリティ アプライアンスのローカル CA サーバの設定。「ローカル CA サーバの設定」を参照してください。
- ローカル CA 証明書の失効 / 失効解除と CRL の更新。「ローカル CA 証明書の管理」を参照してください。
- ローカル CA ユーザの追加、編集、および削除。「ローカル CA ユーザ データベースの管理」を参照してください。

デフォルト ローカル CA サーバ

Local CA ウィンドウには、セキュリティ アプライアンスにローカル CA サーバをセットアップするために設定するパラメータが表示されます。初期ローカル CA サーバには次のデフォルト特性があります。

設定可能なパラメータ	デフォルト
Enable/Disable ボタン。ローカル CA サーバをアクティブまたは非アクティブにします。	デフォルトは **Disable** になっています。ローカル CA サーバをアクティブにするには Enable を選択します。
Enable passphrase。不正な、または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 サーバを保護します。	必須で、デフォルト値はありません。7 文字以上の英数字の語を 1 つ指定します。
証明書発行元の名前	cn=*hostname.domainname*
発行された証明書のキー ペア サイズ	キーごとに 1024 ビット。
ローカル CA 証明書のキー ペア サイズ	キーごとに 1024 ビット。
サーバ証明書の有効期間	サーバ証明書は 3 年間です。
発行されたユーザ証明書の存続期間	ユーザ証明書は 1 年間です。
ローカル CA の電子メール用 Simple Mail Transfer Protocol（SMTP）サーバの IP アドレス	必須で、デフォルト値はありません。SMTP メール サーバの IP アドレスを指定します。

設定可能なパラメータ	デフォルト
ローカル CA のユーザ証明書電子メール通知を発行する電子メール送信者アドレス	必須で、デフォルト値はありません。*adminname@host.com* 形式で電子メール アドレスを指定します。
ローカル CA 電子メール通知の件名	「Certificate Enrollment Invitation」
More Options	それぞれのデフォルト値。
証明書失効リスト（CRL）分散ポイント（CDP）、ローカル CA セキュリティ アプライアンス上の CRL の場所	ローカル CA セキュリティ アプライアンス上の CRL の場所。http://*hostname.domain*/+CSCOCA+/asa_ca.crl
CRL の有効期間	CRL は 6 時間です。
データベース ストレージの場所	オンボード フラッシュ メモリ。
発行された証明書のユーザ名に追加されるデフォルトのサブジェクト名 DN	オプションで、デフォルト値はありません。サブジェクト名のデフォルト値を指定します。
登録後/更新時に、発行された証明書 PKC12 ファイルを取得できる期間	24 時間。
ワンタイム パスワードの有効期間	72 時間（3 日間）。
何日前に期限切れ通知を送信するか	証明書期限切れの 14 日前。
ワンタイム パスワードの有効期間	72 時間（3 日間）。

注意 : Delete Certificate Authority Server ボタンをクリックすると、サーバ コンフィギュレーションが完全に削除されます。

ローカル CA サーバの設定

CA Server ウィンドウでは、ローカル CA サーバの操作をカスタマイズ、変更、および制御できます。この項では、指定可能なパラメータについて説明します。**More Options** をクリックすると、追加のパラメータを指定できます。「その他のローカル CA 設定オプション」を参照してください。設定したローカル CA を完全に削除するには、「ローカル CA サーバの削除」を参照してください。ローカル CA サーバをカスタマイズするには、まず上記の表に記載されている初期設定を確認する必要があります。

（注）　**Issuer-name** と **keysize server** の値は、ローカル CA をイネーブルにした後は変更できません。設定したローカル CA をイネーブルにする前に、オプションのパラメータすべてを慎重に見直してください。

Enable/Disable ボタン

Enable/Disable ボタンは、ローカル CA をアクティブまたは非アクティブにします。**Enable** ボタンでローカル CA サーバをイネーブルにすると、セキュリティ アプライアンスがローカル CA サーバ証明書、キー ペア、および必要なデータベース ファイルを生成します。

自己署名証明書のキー使用拡張機能には、キー暗号化、キー署名、CRL 署名、および証明書署名機能が含まれます。また、**Enable** ボタンをクリックすると、ローカル CA サーバ証明書とキー ペアがストレージに PKCS12 ファイルとしてアーカイブされます。

（注）　**Apply** をクリックして必ずローカル CA 証明書とキー ペアを保存し、セキュリティ アプライアンス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します。

Disable ボタンを使用してローカル CA サーバを停止するときには、セキュリティ アプライアンスで稼働するローカル CA サーバをシャットダウンします。コンフィギュレーションと関連するファイルはすべてストレージに残ります。Web ページ登録は、ローカル CA の変更または再設定中はディセーブルになっています。

パスフレーズ

最初にローカル CA サーバをイネーブルにするとき、英数字のイネーブル パスフレーズを指定する必要があります。パスフレーズは、ストレージにアーカイブされたローカル CA 証明書とローカル CA 証明書キー ペアを保護します。パスフレーズは、ローカル CA 証明書またはキー ペアが失われ、復元が必要な場合に、PKCS12 アーカイブのロックを解除するために必要です。

（注）　イネーブル パスフレーズにデフォルト値はありません。また、パスフレーズはローカル CA サーバをイネーブルにするために必須の引数です。必ず、イネーブル パスフレーズの記録を安全な場所に保管してください。

発行元の名前

Certificate Issuer Name フィールドには、*username* とサブジェクト名のデフォルト DN 設定で形成される、発行元のサブジェクト名 DN が cn=<FQDN> として含まれます。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。デフォルトの証明書名は、cn=*hostname.domainname* 形式で提供されます。

CA サーバのキー サイズ

CA Key Size パラメータは、ローカル CA サーバ用に生成されたサーバ証明書に使用されるキーのサイズです。キー サイズは、キーごとに 512、768、1024、または 2048 ビットを指定できます。デフォルト サイズは、キーごとに 1024 ビットです。

クライアント キー サイズ

Key Size フィールドには、ローカル CA サーバが発行する各ユーザ証明書に対して生成されるキーペアのサイズを指定します。キー サイズは、キーごとに 512、768、1024、または 2048 ビットを指定できます。デフォルト サイズは、キーごとに 1024 ビットです。

CA 証明書のライフタイム

CA Certificate Lifetime フィールドには、CA サーバ証明書の有効期間を日数単位で指定します。CA 証明書のデフォルトは 3650 日（10 年）です。

ローカル CA サーバは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書を自動的に生成します。この証明書を他のデバイスにエクスポートまたはインポートして、ローカル CA 証明書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。期限切れ前の syslog メッセージは次のとおりです。

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

（注）　この自動移行が通知されたら、管理者は期限が切れる前に、新しいローカル CA 証明書が必要なすべてのデバイスにインポートされるよう措置を取る必要があります。

クライアント証明書のライフタイム

Client Certificate Lifetime フィールドには、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します。CA 証明書のデフォルトは 365 日（1 年）です。

SMTP サーバおよび電子メール設定

ローカル CA サーバの電子メール アクセスを設定するには、ローカル CA ユーザに電子メールを送信するための Simple Mail Transfer Protocol（SMTP）電子メール サーバと発信者の電子メール アドレスを設定します。また、ローカル CA の電子メールで使用する標準の件名を指定します。

- **Server IP Address**：Server IP Address フィールドには、ローカル CA の電子メール サーバの IP アドレスを指定します。サーバ IP アドレスにはデフォルトがないため、SMTP メール サーバの IP アドレスは必ず指定します。
- **From Address**：From Address フィールドには、ローカル CA ユーザに電子メールを送信するための発信者の電子メール アドレスを指定します。自動電子メール メッセージを使用して、新しく登録されたユーザへのワンタイム パスワードの送信、証明書の更新が必要なときのメッセージの発行、およびローカル CA ユーザ証明書の電子メール通知の発行を行います。From Address にはデフォルト値がないため、必ず電子メール アドレスを *adminname@host.com* 形式で指定します。
- **Subject** : Subject フィールドは、ローカル CA サーバからユーザに送信されるすべての電子メールの件名を指定する 1 行のテキストです。Subject フィールドを指定しないと、「Certificate Enrollment Invitation」というデフォルトの件名が挿入されます。

その他のローカル CA 設定オプション

CRL 分散ポイントの URL

Certificate Revocation List（CRL; 証明書失効リスト）Distribution Point（DP; 分散ポイント）は、セキュリティ アプライアンス上の CRL の場所です。CRL DP のデフォルトの場所は、http://*hostname.domain*/+CSCOCA+/asa_ca.crl です。

CRL インターフェイスとポートの指定

CRL を、所定のインターフェイスまたはポートで HTTP ダウンロードできるようにします。インターフェイスをプルダウン リストから選択します。任意指定の Port オプションには、1 ～ 65535 の範囲内のポート番号を指定できます。TCP ポート 80 は、HTTP のデフォルト ポート番号です。

CDP URL は、インターフェイスの IP アドレスを利用するように設定することもできます。CDP URL のパスとファイル名も設定できます（CRL の名前は変更できません。常に固定の名前 LOCAL-CA-SERVER.crl が使用されます）。

たとえば、CDP URL を `http://10.10.10.100/user8/my_crl_file` と設定できます。この場合、この IP アドレスを持つインターフェイスだけが機能し、要求を受信すると、セキュリティ アプライアンスはパス /user8/my_crl_file を設定されている CDP URL と照合します。パスが一致すると、セキュリティ アプライアンスはストレージに保存されている CRL ファイルを返します。プロトコルは HTTP でなければなりません。したがって、プレフィックスは http:// となります。

CRL ライフタイム

Certificate Revocation List (CRL) Lifetime フィールドには、CRL の有効期間を時間単位で指定します。CA 証明書のデフォルトは 6 時間です。

ローカル CA は、ユーザ証明書が失効または失効解除されるたびに CRL を更新し、再発行しますが、失効状態に変更がない場合、CRL はその存続期間中に 1 回だけ再発行されます。Manage CA Certificates パネルの **CRL Issue** ボタンをクリックすると、ただちに CRL の更新とリストの再生成を強制的に実行できます。

データベース ストレージの場所

Database Storage Location フィールドでは、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できます。セキュリティ アプライアンスは、ユーザ情報、発行された証明書、失効リストなどに対して、ローカル CA データベースを使用してアクセスおよび実装します。

ローカル CA データベースの常駐場所は、セキュリティ アプライアンスにマウントされてアクセス可能な外部のファイル システム上に設定できます。外部ファイルまたは共有を指定するには、外部ファイルへのパス名を入力するか、**Browse** をクリックしてファイルを検索します。

（注） フラッシュ メモリにも 3500 ユーザ以下のデータベースを保存できますが、3500 ユーザを超えるデータベースには外部ストレージが必要です。

Default Subject Name

Default Subject Name (DN) フィールドには、発行される証明書のユーザ名に追加されるデフォルトのサブジェクト名を指定できます。次のような DN アトリビュートのキーワードを指定できます。

デフォルトのサブジェクト名デフォルト DN キーワード
CN = Common Name
SN = Surname
O = Organization Name
L = Locality
C = Country
OU = Organization Unit
EA = E-mail Address
ST = State/Province
T = Title

Enrollment Period

Enrollment Period フィールドには、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、時間単位で指定します。この登録期間は、ワンタイム パスワードの有効期間とは関係ありません。デフォルトの登録期間は 24 時間です。

（注） ローカル CA の証明書登録は、クライアントレス SSL VPN 接続にのみサポートされており、CVC などその他の SSL VPN クライアントや IPSec VPN 接続にはサポートされていません。クライアントレス SSL VPN 接続の場合、クライアントとヘッドエンドの間の通信は、標準の HTML を使用して Web ブラウザ経由で行われます。

One-Time-Password Expiration

One-Time-Password (OTP) expiration フィールドには、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指定します。デフォルト値は 72 時間です。

Certificate Expiration Reminder

Certificate Expiration Reminder フィールドには、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指定します。デフォルトは 14 日です。

Apply ボタン

Apply ボタンを使用すると、新規または変更した CA 証明書コンフィギュレーションを保存できます。

Reset ボタン

Reset ボタンは、すべての変更内容や編集内容を削除し、表示を元のコンテンツに戻します。

ローカル CA サーバの削除

CA Server パネルの **More Options** セクションの下部にある **Delete Certificate Authority Server** ボタンをクリックすると、セキュリティ アプライアンスからローカル CA 証明書コンフィギュレーションがただちに削除されます。ローカル CA コンフィギュレーションは一度削除すると復元できません。削除したコンフィギュレーションを再作成するには、証明書コンフィギュレーション情報を最初から再入力する必要があります。

（注） ローカル CA サーバを削除すると、セキュリティ アプライアンスからコンフィギュレーションが削除されます。コンフィギュレーションは、一度削除すると復元できません。

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
•	—	•	—	—

ローカル CA 証明書の管理

ローカル CA サーバは、必要に応じて証明書の更新の管理、ユーザ証明書の再発行、証明書失効リスト（CRL）の管理、特権の失効または復元を行います。Manager CA Certificates ウィンドウで、ユーザ名または証明書のシリアル番号を指定して特定の証明書を選択し、証明書ステータス（失効 / 失効解除）を変更できます。

証明書ステータスを変更した場合は、常に CRL を更新して最新の変更が反映されるようにします。

- 証明書ステータスを変更するには、「ローカル CA 証明書の失効」および「ローカル CA 証明書の失効解除」を参照してください。
- CRL を更新して最新の変更を反映するには、「CRL の発行」を参照してください。

ローカル CA 証明書の失効

ローカル CA サーバは、すべてのユーザ証明書のライフタイムを追跡し、必要に応じて電子メールによる更新通知を送信します。ユーザの証明書のライフタイムが切れると、ユーザのアクセス権は失効します。また、ローカル CA は、証明書データベース内の証明書に失効とマーク付けし、情報を自動的に更新して、CRL を再発行します。

ローカル CA 証明書の失効解除

すでに失効したユーザ証明書は、電子メールによる通知を使用して特権を復元できます。失効したユーザの証明書を選択して Unrevoke をクリックすると、アクセス権を復元できます。また、ローカル CA は、証明書データベース内の証明書に失効解除とマーク付けし、証明書情報を自動的に更新して、更新された CRL を再発行します。

CRL の発行

CRL は、生成された後、期限が切れるまで自動的に再生成されますが、**CRL Issue** ボタンを使用すると、ただちに CRL の更新とリストの再生成を強制的に実行できます。証明書を失効または失効解除して変更したら、常に **CRL Issue** ボタンをクリックして CRL を更新します。**A New CRL has been issued** という情報メッセージが表示されます。

ローカル CA ユーザ データベースの管理

ローカル CA ユーザ データベースには、ユーザ識別情報と、システムでの各ユーザのステータス（登録済み、許可、失効など）が含まれます。Manager User Database ウィンドウでは、新規ユーザの追加、ユーザ名で選択した特定のユーザ情報の編集、および既存ユーザとその証明書の削除を行うことができます。ユーザの追加やユーザのステータス変更があるたびに、ローカル CA は自動的に CRL を更新して最新の変更を反映します。

- ローカル CA データベースにユーザを追加するには、「ローカル CA ユーザの追加」を参照してください。
- 既存ユーザのユーザ識別情報を変更するには、「ローカル CA ユーザの編集」を参照してください。
- ユーザをデータベースから削除するには、「ローカル CA ユーザの削除」を参照してください。
- データベース ユーザのグループの登録ステータスを変更するには、「Allow All Certificates」または「Allow All Unenrolled」を参照してください。
- データベース ユーザのグループにワンタイム パスワード（OTP）を電子メールで送信するには、「Email OTP for All Certificate Holders」または「Email OTP for All Unenrolled」を参照してください。

ローカル CA ユーザの追加

Add ボタンを使用して、ローカル CA データベースに新しいユーザを入力できます。データベースに入力される各新規ユーザには、事前定義済みのユーザ名、電子メール アドレス、およびサブジェクト名が必要です。

Local CA Add User のフィールド

- Username：有効なユーザ名を入力します。
- Email：既存の有効な電子メール アドレスを指定します。
- Subject：ユーザのサブジェクト名を入力します。

Email OTP

Email OTP ボタンを使用すると、一意のワンタイム パスワード（OTP）とローカル CA 登録 Web ページの URL が記載された登録許可の電子メール通知が、新規追加されたユーザに自動的に送信されます。

Replace OTP

Replace OTP ボタンを使用すると、新しいワンタイム パスワードが自動的に再発行され、その新しいパスワードが記載された電子メール通知が、新規追加されたユーザに送信されます。

ローカル CA ユーザの編集

Edit ボタンを使用すると、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できます。特定のユーザを選択して、**Edit** ボタンをクリックします。

ローカル CA ユーザの追加のボタンと同じフィールドを変更できます。新規または交換用の OTP を電子メールでユーザに送信できます。変更できる既存のユーザ情報として、ユーザ名、電子メール アドレス、およびサブジェクト名があります。

ローカル CA ユーザの削除

Delete ボタンを使用すると、選択したユーザがデータベースから削除され、そのユーザに対して発行されたすべての証明書がローカル CA データベースから削除されます。削除したユーザは復元できません。削除したユーザのレコードを再作成するには、**Add** ボタンを使用してユーザ情報を再入力する必要があります。

Allow All Certificates

Allow All Certificates ボタンを使用すると、現在登録を許可されているすべてのユーザのステータスが自動的に更新されます。

Allow All Unenrolled

Allow All Unenrolled ボタンを使用すると、現在のデータベース ユーザのうち、未登録で、有効な証明書がないユーザすべてのステータスが自動的に更新されます。

Email OTP for All Certificate Holders

Email OTP for All Certificate Holders ボタンを使用すると、データベース内のユーザのうち、有効な証明書があるユーザすべてに OTP が自動的に送信されます。

Email OTP for All Unenrolled

Email OTP for All Unenrolled ボタンを使用すると、データベース内のユーザのうち、未登録で、有効なユーザ証明書がないユーザすべてに自動的に OTP が送信されます。