



証明書

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。

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。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。

デジタル証明書を使用する認証の場合、FWSM 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。

ここでは、次の項目について説明します。

- [Authentication \(P.24-2\)](#)
- [Enrollment \(P.24-3\)](#)
- [Import Certificate \(P.24-4\)](#)
- [Key Pair \(P.24-5\)](#)
- [Manage Certificate \(P.24-7\)](#)
- [Trustpoint \(P.24-9\)](#)
- [デジタル証明書の認証、登録および管理 \(P.24-17\)](#)

Authentication

Authentication ペインでは、CA 証明書をトラストポイントに関連付けて、FWSM にインストールする CA 証明書を認証できます。既存のトラストポイント コンフィギュレーションを選択して編集することも、新しいトラストポイント コンフィギュレーションを作成することもできます。

選択したトラストポイント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。選択したトラストポイントが自動登録用に設定されている場合、FWSM 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してデバイスにインストールします。

フィールド

- **Trustpoint Name**: CA 証明書を取得するために使用可能なトラストポイントが含まれるリストを表示します。リストのトラストポイント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、新しいトラストポイント コンフィギュレーションを追加したりします。
- **Edit**: Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- **New**: リストに新しいトラストポイント コンフィギュレーションを追加します。
- **Fingerprint**: FWSM が CA 証明書の認証に使用する、英数字で構成されるキーを指定します。フィンガープリントを指定すると、FWSM は、そのフィンガープリントと CA 証明書の計算されたフィンガープリントを照合して、2 つの値が一致する場合のみ証明書を受け入れます。フィンガープリントがない場合、FWSM はフィンガープリントの照合を行わずに証明書を受け入れます。
- **Import from a file**: 手動登録のみで、証明書をインポートするファイルを特定します。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**: Load 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。
- **Enter the certificate text in base64 format**: 手動登録の場合、base64 形式でトラストポイント コンフィギュレーションを入力します。
- **Authenticate**: 認証手順を完了させます。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

[デジタル証明書の認証、登録および管理](#)

Enrollment

Enrollment ペインでは、リストからトラストポイント コンフィギュレーションを選択し、トラストポイント コンフィギュレーションを編集、または新規作成できます。ただし、自動登録の場合、CA 証明書を認証するまで登録要求を生成できません。

自動登録の場合、FWSM は SCEP プロトコルを使用して CA にアクセスし、ID 証明書を取得してデバイスにインストールします。手動登録の場合、証明書の登録要求を示す **enrollment request** ダイアログボックスが表示されます。この登録要求を使用して、CA の管理インターフェイスから ID 証明書を取得します。取得した ID 証明書は、base 64 形式または 16 進数形式である必要があります。その後、**Import Certificate** ダイアログボックスで ID 証明書をインポートできます。

フィールド

- **Trustpoint Name** : 登録要求を生成するトラストポイントを指定します。リストから名前を選択したり、ボックスに表示されている名前を編集したり、または新しいトラストポイント コンフィギュレーションを追加します。
- **Edit** : **Trustpoint Name** ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- **New** : リストに新しいトラストポイント コンフィギュレーションを追加します。
- **Enroll** : CA での登録プロセスを開始します。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

[デジタル証明書の認証、登録および管理](#)

Import Certificate

Import Certificate ペインでは、手動登録時に CA から受け取ったデバイス証明書をインストールできます。CA からの証明書をインポートするには、選択したトラストポイントに関連付けられている CA 証明書がある必要があります。該当する CA 証明書がない場合は、FWSM に警告が表示されます。

フィールド

- **Trustpoint Name** : 証明書を受け取ったトラストポイントの名前を指定します。リストから名前を選択したり、ボックスに表示されている名前を編集したり、または新しいトラストポイントコンフィギュレーションを追加します。
- **Edit : Trustpoint Name** ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- **New** : リストに新しいトラストポイント コンフィギュレーションを追加します。
- **Import from a file** : ID 証明書をインポートするファイルを特定します。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 : 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。
- **Enter the certificate text in base64 format** : 手動登録では、カット アンド ペーストを使用して、エクスポート元から、この FWSM に証明書データを転送できます。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Key Pair

キー ペアは、ID 証明書の登録時に必要です。FWSM では、複数のキー ペアをサポートします。

フィールド

- **Key-pair Name** : キー ペアに指定されている名前を表示します。
- **Usage** : 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、FWSM 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。
- **Size** : 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。
- **Add** : Add Key Pair ダイアログボックスが開きます。
- **Show Details** : 名前、生成日、タイプ、係数サイズ、使用方法および DER-encoded キー データを表示します。
- **Delete** : 選択したキー ペアを削除します。
- **Refresh** : 表示をアップデートします。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Add Key Pair

Add Key Pair ダイアログボックスで、キー ペアのリストに新しいキー ペアを追加できます。

フィールド

- **Name** : キー ペアの名前 (デフォルトのキー <Default-RSA-Key> または特定のキー) を指定します。トラストポイントにキー ペアが設定されていない場合、FWSM はデフォルトのキー ペアを使用します。
- **Size** : 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。
- **Usage** : キー ペアの使用方法を指定します。このフィールドは、RSA キー ペアのみにも適用されます。RSA キーの使用方法には、**General Purpose** (デフォルト) または **Special** の 2 種類があります。**Special** をクリックすると、FWSM 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。
- **Generate Now** : キー ペアを生成します。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Key Pair Details

Key Pair Details ダイアログボックスには、選択したキー ペアの情報が表示されます。

フィールド

- **Key Pair** : キー ペアに指定されている名前を表示します。
- **Generation Time** : キーが生成された日付と時刻を表示します。
- **Size** : キー ペアのタイプによって異なる係数サイズを表示します。RSA キーの場合、サイズは 512、768、1024 または 2048 を指定できます。デフォルトの係数サイズは 1024 です。
- **Usage** : 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。キー ペアの使用方法が Special の場合、FWSM 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。
- **Key Data text** : DER-encoded キー データを表示します。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Manage Certificate

Manage Certificates ペインには、テーブルの証明書がすべて表示されます。ここで証明書を追加および編集したり、証明書情報を表示したり、表示をリフレッシュしたり、FWSM から証明書を削除することができます。

フィールド

- **Subject** : 証明書の所有者を特定します。
- **Type** : タイプ (CA、RA 汎用、RA 暗号化、RA シグニチャ、ID) を特定します。
- **Trustpoint** : トラストポイントを特定します。
- **Status** : ステータス (Available または Pending) を特定します。
 - Available は、CA が登録要求を受け入れて、ID 証明書を発行したことを意味します。
 - Pending は、登録要求が処理中であるため、CA が ID 証明書をまだ発行していないことを意味します。
- **Usage** : 証明書が使用される方法 (シグニチャ、汎用、または暗号化) を特定します。
- **Add** : Add Certificate ダイアログボックスを表示します。ここで FWSM に CA/RA/ID 証明書を追加できます。このダイアログボックスを使って、エクスポートしたファイルから証明書をインポートしたり、カットアンドペーストで FWSM に証明書を入力できます。
- **Show Details** : Certificate Details ダイアログボックスを表示します。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 table** : タイプ、シリアル番号、ステータス、使用方法、CRL 分散ポイント、および証明書の有効期間を表示します。これは、Available および Pending ステータスの両方に適用されます。
 - **Subject table** : 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。
 - **Issuer table** : 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。
- **Refresh** : Manage Certificates ペインのテーブルの表示を更新します。
- **Delete** : 証明書の削除を確認する Delete Certificate ダイアログボックスを表示します。CA 証明書を削除すると、FWSM では関連付けられている ID 証明書もすべて削除します。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

[デジタル証明書の認証、登録および管理](#)

Add Certificate

Add Certificate ダイアログボックスでは、CA/RA/ID 証明書を手動で追加できます。

フィールド

- Trustpoint Name : Manage Certificates テーブルに追加する証明書を指定します。
- Edit : Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New : リストに新しいトラストポイント コンフィギュレーションを追加します。
- Certificate Type : タイプ (CA、RA 汎用、RA 暗号化、RA シグニチャ、ID) を指定します。
- Serial Number : 証明書に FWSM のシリアル番号を含めます。
- Import from a file : 証明書をインポートするファイルを特定します。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 : Add 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。
- Enter the certificate text in base64 format : カット アンド ペースを使用してエクスポートしたソース テキストから、この FWSM に証明書データを 16 進数形式のみで転送できます。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Trustpoint

トラストポイントは CA と ID のペアを表し、CA の ID、CA 固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。

ここでは、次の項目について説明します。

- [Configuration \(P.24-9\)](#)
- [Export \(P.24-15\)](#)
- [Import \(P.24-16\)](#)

Configuration

Configuration ペインでは CA を特定し、ルート CA にすることができ、独自の公開鍵を含む自己署名された証明書を作成することができます。Configuration ペインでは、トラストポイントとして CA を追加、編集または削除したり、CRL を要求したりすることができます。

フィールド

- Trustpoint Name : トラストポイントの名前 (IP アドレスやホスト名など) を表示します。
- Device Certificate Subject : FWSM システムの証明書を所有するサブジェクト DN を表示します。
- CA Certificate Subject : CA 証明書のサブジェクト名を表示します。
- Add : Add Trustpoint Configuration ダイアログボックスが開きます。
- Edit : Edit Trustpoint Configuration ダイアログボックスが開きます。
- Delete : 選択したトラストポイントを削除します。
- Request CRL : 選択したトラストポイントの CRL を取得します。CRL を参照するには、**Monitoring > Administration > CRL** を表示してください。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Trustpoint Configuration > Enrollment Settings タブ

Add Trustpoint Configuration > Enrollment Settings タブでは、トラストポイント テーブルにトラストポイントを追加できます。また、Edit Trustpoint Configuration > Enrollment Settings タブでは、選択したトラストポイントの情報を変更できます。

フィールド

- Trustpoint Name : CA に対応するトラストポイントの名前を指定します。たとえば、IP アドレスやホスト名を指定します。
- Generate a self-signed certificate on enrollment : 登録時に FWSM の自己署名デバイス証明書を生成するためにクリックします。この操作により、SSL 接続を終了するときに使われる自己署名証明書を作成できます。この機能はデフォルトでオフになっています。このオプションがオンになっている場合、キー ペアと証明書パラメータのみを設定できます。

- **Key Pair** : リストで事前に定義したキー ペアを選択します。トラストポイントを追加する前に、キー ペアを設定する必要があります。このリストが空の場合、**New Key Pair** を選択してキー ペアを追加できます。
- **Show Details** : 生成された場合に、名前、係数、使用方法 (General Purpose または Special) および DER-encoded 形式のキー データといったキー ペアの情報を表示します。
- **New Key Pair** : **Add Key Pair** ダイアログボックスを表示します。ここで新しいキー ペア (RSA の場合) の名前、サイズ、タイプおよび使用方法を入力できます。
- **Challenge Password** : 登録時に CA に登録されるチャレンジフレーズを指定します。
- **Confirm Challenge Password** : チャレンジパスワードを確認します。
- **Use manual enrollment** : PKCS10 証明書要求を生成することを指定します。CA は要求に基づいて FWSM 証明書を発行し、新しい証明書をインポートすることによって、FWSM に証明書がインストールされます。
- **Use automatic enrollment** : SCEP モードを使用することを指定します。トラストポイントが SCEP 登録用に設定されている場合、FWSM は SCEP プロトコルを使用して証明書をダウンロードします。
- **Enrollment URL** : 自動登録の URL 名を指定します。最大長は 1000 文字です (事実上無制限)。
- **Retry Period** : 証明書を要求した後、FWSM は CA からの証明書の受信を待ちます。FWSM は、指定されたリトライ間隔内に証明書を受け取らなかった場合は、証明書要求を再送信します。このフィールドに、登録要求の送信試行間隔を分単位で指定します。有効な範囲は 1 ~ 60 分です。デフォルト値は 1 です。
- **Retry Count** : 証明書を要求した後、FWSM は CA からの証明書の受信を待ちます。FWSM は、指定されたリトライ間隔内に証明書を受け取らなかった場合は、証明書要求を再送信します。FWSM は、応答を受信するか、または指定したリトライの回数に達するまで要求を繰り返します。このフィールドで、登録要求の送信を試行する最大回数を指定します。有効なリトライの範囲は 0、1 ~ 100 回です。デフォルト値は 0 です。0 の場合はリトライ回数が無制限になります。
- **Certificate Parameters** : **Certificate Parameters** ダイアログボックスを表示します。ここで DN、FQDN など、登録時に証明書に含めるアトリビュートとその値を指定できます。

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		
ルールセット	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add Key Pair

Add Key Pair ダイアログボックスで、キー ペアのリストに新しいキー ペアを追加できます。

フィールド

- **Name** : キー ペアの名前 (デフォルトのキー <Default-RSA-Key> または特定のキー) を指定します。トラストポイントにキー ペアが設定されていない場合、FWSM はデフォルトのキー ペアを使用します。
- **Size** : 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。
- **Usage** : キー ペアの使用方法を指定します。このフィールドは、RSA キー ペアのみに適用されます。RSA キーの使用方法には、General Purpose (デフォルト) または Special の 2 種類があります。Special をクリックすると、FWSM 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。

- Generate Now : キー ペアを生成します。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	•

Certificate Parameters

Certificate Parameters ダイアログボックスで、登録時に含めるサブジェクト DN、FQDN、IP アドレスを指定できます。また、このダイアログボックスを使って、デバイスのシリアル番号を含めます。

フィールド

- Subject DN : サブジェクトの X.500 名に使用するアトリビュートと値を指定します。サブジェクトは証明書の所有者です。
 - **Edit** ボタンをクリックして Edit DN ダイアログボックスを表示して、Subject DN のアトリビュートと値を選択します。
- FQDN : 証明書の Subject Alternative Name 拡張子に Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を含めます。FQDN は、要求が送信されるサーバプログラムを完全に識別する URL の一部で、たとえば `www.examplesite.com` のようになります。
- E-mail : 証明書の Subject Alternative Name 拡張子に指定の電子メール アドレスを含めます。
- IP Address : 証明書の Subject Alternative Name 拡張子に指定の IP アドレスを含めます。
- Include device serial number : 登録時に、証明書に FWSM のシリアル番号を含めます。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Edit DN

Edit DN ダイアログボックスで証明書 DN を編集します。

Attributes リストで次のいずれかのアトリビュートを選択し、Value ボックスに値を入力して Add をクリックします。アトリビュートは必要な数だけ選択します。

フィールド

- Common Name (CN) : 個々のユーザに指定されている名前。Pat など。
- Department (OU) : 企業や大学といった大規模な組織の組織ユニットまたはサブグループ。Geology (地質学) 部門など。

- Company Name (O) : 企業や大学などの組織。University of Oz など。
- Country (C) : 特定の国の 2 文字表記。OZ など。
- State (St) : 国内の州や県。Kansas (カンザス州) など。
- Location (L) : サブジェクトの住所。49 Wizard St. など。
- Email Address (EA) : Pat@example.com。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Add/Edit Trustpoint Configuration > CRL Retrieval Policy タブ

CRL Retrieval Policy タブでは、CRL DP から CRL を取得するのか、または Static URLs テーブルに記載されている URL から CRL を取得するのかを指定できます。

フィールド

- Use CRL Distribution Point from the certificate: 証明書に記載されている分散ポイントから CRL を取得します。
- Use Static URLs configured below : FWSM が CRL の取得を試みる URL を最大 5 つまで追加します。
- Add : Add Static URL ボックスを表示します。このボックスで、URL を最大 5 つ追加します。
 - URL : URL のタイプ (HTTP または LDAP) を選択します。
 - :// : CRL を分散する場所を入力します。
- Edit : Edit Static URL ボックスを表示して、選択した URL を変更します。
- Delete : 選択した URL を削除します。
- Move Up : 選択した URL をテーブルの一番上まで移動します。
- Move Down : 選択した URL をテーブルの一番下まで移動します。

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		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Add/Edit Static URL

フィールド

- URL: : URL のタイプ (HTTP、LDAP または SCEP) を選択します。
- :// : CRL を分散する場所を入力します。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Trustpoint Configuration > CRL Retrieval Method タブ

CRL Retrieval Method タブで、CRL の取得方法を指定できます。すべての方法をイネーブルにすることができます。複数の方式をイネーブルにした場合、ASDM は指定した順番で使用します。

フィールド

- Enable Lightweight Directory Access Protocol (LDAP): 次のように LDAP パラメータを指定します。
 - Name : サーバ上の CRL へのアクセス権を持つユーザを指定します。
 - Password : Name に記載されているユーザのパスワードを指定します。
 - Confirm Password : パスワードを確認します。
 - Default Server : LDAP サーバのホスト名または IP アドレスを指定します。
 - Default Port : サーバのポート番号を指定します。デフォルトは 389 です。
- Enable HTTP : HTTP を CRL の取得に使用するプロトコルとして指定します。
- Enable Simple Certificate Enrollment Protocol (SCEP) : 登録時ではなく、CRL の取得に登録時用と同じ方式を使用します。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Trustpoint Configuration > Advanced タブ

Advanced タブで、CRL チェックおよびキャッシングのパラメータを指定できます。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。CRL チェックをイネーブルにすることにより、FWSM が認証で証明書を使用するたびに、CA がその証明書を無効にしていないかどうかをチェックするようにします。

CA から同じ CRL を何度も受け取る必要のないように、FWSM 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、FWSM は使用頻度が最も低い CRL を削除して容量を空けます。

フィールド

- CRL Check : CRL チェックの実行内容を決定します。次のいずれかをクリックします。
 - No Check : CRL チェックを実行しないことを示します。
 - Optional : 要求した CRL が使用できない場合、FWSM がピア証明書を受け入れられることを示します。
 - Required : 要求した CRL が使用可能でない限り、FWSM がピア証明書を検証しないことを示します。
- Cache Refresh Time : キャッシュのリフレッシュ間隔を分数で指定します。デフォルトは 60 分で、範囲は 1 ～ 1440 分です。
- 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。
- Accept certificates issued by this trustpoint : FWSM で、Trustpoint 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。
- Use the configuration of this trustpoint to validate any remote user certificate issued by the CA corresponding to this trustpoint : イネーブルにすると、このトラストポイント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をこのトラストポイントから取得できます。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Export

Export ペインでは、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トラストポイント 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。トラストポイント 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、FWSM のグループ間でトラストポイントを複製します。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、同等のトラストポイント コンフィギュレーションが必要です。この場合、管理者は、トラストポイント コンフィギュレーションをエクスポートして、FWSM のグループ全体にインポートできます。

フィールド

- Trustpoint Name : リストのトラストポイント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、新しいトラストポイント コンフィギュレーションを追加したりします。
- Edit : Trustpoint Name ボックスに表示されているトラストポイント コンフィギュレーションを変更します。
- New : リストに新しいトラストポイント コンフィギュレーションを追加します。
- 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 to a file : トラストポイント 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。PKCS12 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、ここでトラストポイント 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。
- Display the trustpoint configuration in PKCS12 format : Export Trustpoint Configuration ダイアログボックスが表示され、テキスト ボックスにトラストポイント コンフィギュレーションが表示されます。カット アンド ペーストを使用してデータを抽出し、Import ペインのウィンドウに配置することができます。終了するには OK をクリックします。
- Export : トラストポイント 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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Import

Import ペインで、トラストポイント コンフィギュレーション全体を PKCS12 形式でインストールできます。トラストポイント 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、RA 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、FWSM のグループ間でトラストポイントを複製します。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、同等のトラストポイント コンフィギュレーションが必要です。この場合、管理者は、トラストポイント コンフィギュレーションをエクスポートして、FWSM のグループ全体にインポートできます。

フィールド

- **Trustpoint Name** : トラストポイントを特定します。フェールオーバーまたはロードバランシング用に他の FWSM からインポートする場合、トラストポイント コンフィギュレーションがエクスポートされた FWSM と同じトラストポイント名を使用できます。ただし、同じ名前のトラストポイント / キー ペアがまだ存在していないことを確認する必要があります。
- **Decryption Passphrase** : トラストポイント コンフィギュレーションのエクスポート時に指定した暗号化パスフレーズを指定します。
- **Confirm Passphrase** : パスフレーズを確認します。
- **Import from a file** : 証明書をインポートするファイルを特定します。ファイルからインポートされたテキストは、base64 形式または 16 進数形式の PKCS12 データである必要があります。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 : Load Certificate File** ダイアログボックスが表示されます。ここでトラストポイント コンフィギュレーションが含まれるファイルに移動できます。
- **Enter the trustpoint configuration in PKCS12 format** : PKCS12 形式のトラストポイント コンフィギュレーションを base64 または 16 進数形式で貼り付けられます。この際、テキスト ボックスにカット アンド ペーストでデータを入力できます。
- **Import** : トラストポイント コンフィギュレーションをインポートします。

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		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

デジタル証明書の認証、登録および管理

この項では、デジタル証明書の登録方法について説明します。登録が完了すると、証明書を使用してデバイスを VPN 管理ピアに認証することができます。

ここでは、次の項目について説明します。

- [設定手順の要約 \(P.24-17\)](#)
- [キー ペアの作成 \(P.24-17\)](#)
- [自動登録による証明書の登録 \(SCEP\) \(P.24-18\)](#)
- [CA に対する認証 \(P.24-19\)](#)
- [CA の登録 \(P.24-19\)](#)
- [手動登録による証明書の登録 \(P.24-20\)](#)
- [フェールオーバー コンフィギュレーション向けの追加手順 \(P.24-21\)](#)
- [Managing Certificates \(P.24-22\)](#)

設定手順の要約

CA を登録し、トンネルの認証に使用する ID 証明書を取得するための基本手順は次のとおりです。この例では、自動 (SCEP) 登録と手動登録の両方を示します。この手順に説明のないフィールドについては、**Help** ボタンをクリックしてください。

1. ID 証明書のキー ペアを作成します。
2. トラストポイントを作成します。
3. 登録 URL を設定します。
4. CA を認証します。
5. CA を登録し、ID 証明書を FWSM 上に置きます。



(注)

認証と登録はプロセスの 2 つの別個のフェーズです。まず認証する必要があります。その後、自動登録または手動登録のいずれかで登録することができます。

キー ペアの作成

最初に証明書のキー ペアを作成します。作成したキー ペアは、キー ペアの設定時に指定したラベルで識別されます。RSA キー ペアには、General Purpose と Usage の 2 種類があります。デフォルトは General Purpose で、1 組のキー ペアを作成します。Usage は、署名用と暗号化用の 2 つのキー ペアを作成します。したがって、対応する ID ごとに 2 つの証明書が必要です。

ASDM を使用して RSA キー ペアを作成するには、次の手順を実行します。

-
- ステップ 1** **Configuration > Properties > Certificate > Key Pair** で、**Add** ボタンをクリックします。
 - ステップ 2** **Add Key Pair** ダイアログボックスで情報を設定します。
 - ステップ 3** **Generate Now** ボタンをクリックします。

- ステップ 4** 生成されたキー ペアを表示するには、**Show Details** ボタンをクリックします。ASDM に、キー ペアに関する情報が表示されます。

自動登録による証明書の登録 (SCEP)

トラストポイントを作成します。トラストポイントは CA と ID のペアを表し、CA の ID、固有のコンフィギュレーション パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。

トラストポイントを作成するには、次の手順を実行します。

- ステップ 1** **Configuration > Properties > Certificate > Trustpoint > Configuration** で、**Add** ボタンをクリックします。

- ステップ 2** **Add Trustpoint Configuration** ダイアログボックスで、基本情報を設定します。その他のすべてのパラメータについては、デフォルト値を受け入れます。

- a. **Trustpoint Name** : **Trustpoint Name** ボックスにトラストポイント名を入力します。
- b. **Enrollment URL** : **Enrollment Settings** ペインの **Enrollment Mode** グループ ボックスで、SCEP の場合は **Use automatic enrollment** オプションをクリックします。次に、このボックスに登録 URL を入力します。たとえば、10.20.30.40/cgi-bin/pkiclient.exe のように入力します。
- c. 証明書のパスワード確認をする場合は、**Challenge Password** ボックスおよび **Confirm Password** ボックスにパスワードを入力します。証明書を無効にする必要がある場合、このパスワードを CA 管理者に渡して自分が証明書所有者であることを証明することができます。このパスワードはコンフィギュレーションに保存されないため、書き留めておく必要があります。

- ステップ 3** 次にコンフィギュレーション パラメータを設定します。少なくとも、X.500 フィールドを使って証明書のサブジェクト名を設定する必要があります (Common Name (CN; 通常名) や Organizational Unit (OU; 組織ユニット) など)。

- a. **Enrollment Settings** ペインの **Key Pair** リストから、このトラストポイントに対して設定したキー ペアを選択します。
- b. **Enrollment Settings** ペインで、**Certificate Parameters** ボタンをクリックします。
- c. サブジェクト DN の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** ボタンをクリックします。
- d. **Edit DN** ボックスで、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** ボックスに値を入力します。次に **Add** ボタンをクリックします。たとえば、まず **Command Name (CN)** を選択し、**Value** ボックスに Pat と入力します。次に **Department (OU)** を選択して、**Value** ボックスに Engineering と入力します。
- e. サブジェクト DN 情報をすべて入力したら、**OK** ボタンをクリックします。
- f. 必要に応じて、**FQDN**、**E-mail** および **IP Address** の値を入力し、**Include device serial number** オプションをオンにします。
- g. **OK** ボタンをクリックします。

- ステップ 4** **Apply** をクリックします。**preview** コマンドをオンにしておくと、ASDM には ASDM のコンフィギュレーションに基づいて CLI コマンドが表示され、送信するかキャンセルするかを選択できます。**Send** をクリックします。この手順を設定するすべての機能に対して実行します。

CA に対する認証

CA に対する認証により、CA 証明書を FWSM に置きます。SCEP 登録のトラストポイントを設定すると、CA 証明書は SCEP を通してダウンロードされます。設定しない場合は、CA 証明書をテキストボックスに貼り付けるか、または **Browse** ボタンを使用してファイルを指定する必要があります。この項では、SCEP 登録について説明します。

CA に対して認証するには、次の手順を実行します。

- ステップ 1** **Configuration > Properties > Certificate > Authentication** で、**Trustpoint Name** リストからトラストポイントの名前を選択します。
- ステップ 2** **Authenticate** ボタンをクリックします。
- ステップ 3** ASDM で **Authentication Successful** ダイアログが表示されたら、**OK** ボタンをクリックします。

CA の登録

トラストポイントを設定して認証したら、ID 証明書を登録できます。

ASDM を使用して ID 証明書を登録するには、次の手順を実行します。

- ステップ 1** **Configuration > Properties > Certificate > Enrollment** で、**Trustpoint Name** リストからトラストポイントを選択します。
- ステップ 2** **Enroll** ボタンをクリックします。

作業が完了すると、ASDM に、トラストポイント コンフィギュレーションのエクスポート方法と登録ステータスのチェック方法を示す **Copy Trustpoint Configuration to Standby** ダイアログボックスが表示されます。このメッセージは、フェールオーバー コンフィギュレーションのみに関連します。フェールオーバーを設定していない場合は、この手順を無視して **OK** ボタンをクリックします。フェールオーバーを設定している場合、ダイアログボックスの指示に従ってスタンバイ デバイスに証明書をバックアップします。

手動登録による証明書の登録

自動登録以外の方法で CA から ID 証明書を受け取るときに、この方法を使用します。

- ステップ 1** **Configuration > Properties > Certificate > Trustpoint > Configuration** で、**Add** ボタンをクリックします。
- ステップ 2** **Add Trustpoint Configuration** ダイアログで、**Trustpoint Name** ボックスに名前を入力します。
- ステップ 3** **Enrollment Settings** ペインで、**Key Pair** リストからキー ペアを選択するか、または **New Key Pair** ボタンをクリックして新しいキー ペアを追加します。
- ステップ 4** 必要に応じて、**Challenge Password** ボックスにパスワードを入力し、**Confirm Challenge Password** ボックスに再度入力して確認します。
- ステップ 5** **Use manual enrollment** オプションをクリックします。
- ステップ 6** **Certificate Parameters** ボタンをクリックします。

- a. サブジェクト DN の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** ボタンをクリックします。
- b. **Edit DN** ボックスで、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** ボックスに値を入力します。次に **Add** ボタンをクリックします。たとえば、まず **Command Name (CN)** を選択し、**Value** ボックスに Pat と入力します。次に **Department (OU)** を選択して、**Value** ボックスに Engineering と入力します。
- c. サブジェクト DN アトリビュートをすべて追加したら、**OK** ボタンをクリックします。
- d. 必要に応じて、**FQDN**、**E-mail** および **IP Address** の値を入力し、**Include device serial number** オプションをクリックします。
- e. **OK** ボタンをクリックします。

- ステップ 7** **Configuration > Properties > Certificate > Enrollment** をクリックして、**Trustpoint Name** リストでトラストポイントを選択します。

- ステップ 8** **Enroll** ボタンをクリックします。**Enrollment Request** ダイアログボックスに、次に行う作業の指示が表示されます。指示を読んだら **OK** ボタンをクリックします。

電子メールで要求を送信するか、または CA の Web インターフェイスを使用して登録します。

- ステップ 9** CA から証明書を受け取ったら、**Configuration > Properties > Certificate > Import Certificate** をクリックし、**Trustpoint Name** リストでトラストポイントの名前を選択します。

- ステップ 10** 証明書のインポート方法を選択します。

- a. **Import from a File** : ファイル名を入力するか、またはファイルを参照します。システムには、選択したトラストポイントに関連付けられている CA 証明書が必ずあり、CA からファイルで ID 証明書を受け取っているはずです。
または
- b. **Enter the certificate text in base64 format** : テキスト ボックスに CA から受け取った ID 証明書のテキストを貼り付けます。詳細については、**Help** をクリックしてください。

ステップ 11 **Import** をクリックします。

ステップ 12 証明書登録設定をフラッシュ メモリに保存するには、**Save** をクリックします。

フェールオーバー コンフィギュレーション向けの追加手順

ID 証明書、CA 証明書、および使用するネットワークの他の FWSM のキーをバックアップするには、まずそれらをファイルにエクスポートするか、またはエクスポート機能を使用してポップアップ ウィンドウに証明書を表示し、インポート機能で他の FWSM にコピー アンドペーストします。

証明書のファイルまたは PKCS12 データへのエクスポート

トラストポイント コンフィギュレーションをエクスポートするには、次の手順を実行します。

ステップ 1 **Configuration > Properties > Certificate > Trustpoint > Export** に移動します。

ステップ 2 **Trustpoint Name**、**Encryption Passphrase**、および **Confirm Passphrase** フィールドに入力します。これらのフィールドの詳細については、**Help** をクリックしてください。

ステップ 3 トラストポイント コンフィギュレーションのエクスポート方法を選択します。

- a. **Export to a File** : ファイル名を入力するか、またはファイルを参照します。
または
- b. **Display the trustpoint configuration in PKCS12 format** : テキスト ボックスにトラストポイント コンフィギュレーション全体を表示し、コピーしてインポートすることができます。詳細については、**Help** をクリックしてください。

ステップ 4 **Export** をクリックします。

証明書のスタンバイ デバイスへのインポート

トラストポイント コンフィギュレーションをインポートするには、次の手順を実行します。

ステップ 1 **Configuration > Properties > Certificate > Trustpoint > Import** に移動します。

ステップ 2 **Trustpoint Name**、**Decryption Passphrase**、および **Confirm Passphrase** フィールドに入力します。これらのフィールドの詳細については、**Help** をクリックしてください。復号化パスフレーズは、トラストポイント コンフィギュレーションをエクスポートしたときに使用した暗号化パスフレーズと同じです。

ステップ 3 トラストポイント コンフィギュレーションのインポート方法を選択します。

- a. **Import from a File** : ファイル名を入力するか、またはファイルを参照します。
または

- b. **Enter the trustpoint configuration in PKCS12 format** : トラストポイント コンフィギュレーション全体をエクスポート元からテキスト ボックスに貼り付けます。詳細については、**Help** をクリックしてください。

Managing Certificates

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** に移動します。

このペインを使用して、新しい証明書の追加や証明書の削除を行うことができます。また、**Show Detail** ボタンをクリックして証明書に関する情報を表示することもできます。**Certificate Details** ダイアログボックスに、**General**、**Subject** および **Issuer** の 3 つのテーブルが表示されます。

General テーブルには次の情報が表示されます。

- Type : CA、RA または ID。
- Serial number : 証明書のシリアル番号。
- Status : Available、in progress、error、fail。
- Usage : 汎用またはシグニチャ。
- CRL DP : 証明書の検証用に CRL が含まれる分散ポイントの URL。
- Dates/times within which the certificate is valid : 証明書の有効期間の開始日と終了日。

Subject ペインには次の情報が表示されます。

- Name : 証明書を所有するユーザまたはエンティティの名前。
- Serial Number : FWSM のシリアル番号。
- X.500 fields for the subject of the certificate : CN、OU など。
- Hostname of the certificate holder : wland.com など。
- Serial Number of the hostname : セキュリティ アプライアンスのシリアル番号。

Issuer ペインには、証明書を付与したエンティティの X.500 DN フィールドが表示されます。

- Common name (CN)
- Organizational unit or department (OU)
- Organization (O)
- Locality (L)
- State (ST)
- Country code (C)
- Email address of the issuer (EA)