Firepower Threat Defense Certificate ベースの認証

Firepower Threat Defense VPN 証明書の注意事項と制約事項

- 証明書登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書登録プロセスが開始されます。プロセスは、自己署名および SCEP 登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。
- 登録が完了すると、証明書の登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。VPN 認証方式の設定でこのトラストポイントを使用します。
- FTD デバイスは、Microsoft CA サービスと、Cisco 適応型セキュリティ アプライアンス（ASA）および Cisco IOS ルータで提供される CA サービスを使用した証明書の登録をサポートしており、検証済みです。
- FTD デバイスは、CA として設定することはできません。

ドメインとデバイス間での証明書の管理のガイドライン

- 証明書の登録は、子ドメインまたは親ドメインで行うことができます。

- 親ドメインからの登録が完了したら、証明書の登録オブジェクトもそのドメイン内に存在する必要があります。デバイスのトラストポイントが子ドメインで上書きされた場合、上書きされた値がデバイスに展開されます。
- リーフ ドメインのデバイスで証明書の登録が行われる場合、その登録は親ドメインまたは他の子ドメインに表示されます。また、証明書を追加することもできます。
- リーフ ドメインが削除されると、含まれているデバイス上の証明書の登録が自動的に削除されます。
- あるドメインに登録されている証明書を持つデバイスは、他のドメインに登録できます。他のドメインに証明書を追加できます。
- あるドメインから別のドメインにデバイスを移動すると、証明書もそれに応じて移動します。これらのデバイスの登録を削除するための警告が表示されます。

FTD 証明書の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin/Security Approver

デジタル証明書の概要については、PKI インフラストラクチャとデジタル証明書を参照してください。

管理対象デバイスの証明書を登録および取得するために使用するオブジェクトの説明については、証明書の登録オブジェクトを参照してください。

ステップ 1 **[Devices]** > **[Certificates]** に進みます。

この画面で、次の操作を実行します。

- すでにトラストポイントが関連付けられているデバイスは、[名前（Name）] 列にリスト表示されます。デバイスを展開して、関連付けられたトラストポイントのリストを確認します。

  このトラストポイントに使用する登録タイプは、[登録タイプ（Enrollment Type）] 列に表示されます。

  特定のドメインに登録された証明書が [ドメイン] 列に表示されます。

- [ステータス（Status）] 列には、[CA 証明書（CA Certificate）] と [アイデンティティ証明書（Identity Certificate）] のステータスが表示されます。虫めがねをクリックすることで、証明書の内容を表示できます（`Available` の場合）。

  登録に失敗した場合は、アイコンをクリックして失敗メッセージを表示します。

- 管理対象デバイスの証明書を更新します（環状の矢印）。証明書を更新すると、Firepower Threat Defense デバイスの証明書ステータスが Firepower Management Center に同期されます。
- 再登録アイコンを使用して、アイデンティティ証明書を登録します。

  ポリシーの展開中に、証明書の登録プロセスが失敗した場合は、再登録オプションを使用してアイデンティティ証明書を再度登録します。
- 設定済みの証明書を削除（ゴミ箱に移動）します。

ステップ 2 [（+）追加（(+) Add）] を選択して、登録オブジェクトをデバイスに関連付けてインストールします。

証明書登録オブジェクトがデバイスに関連付けられ、デバイスにインストールされるとすぐに、証明書登録プロセスが開始されます。プロセスは、自己署名およびSCEP登録タイプの場合は自動的に行われます。つまり、管理者による追加のアクションは必要ありません。手動証明書登録では、さらに管理者の操作が必要になります。

（注） デバイス上の証明書の登録ではユーザインターフェイスがブロックされず、登録プロセスはバックグラウンドで実行され、ユーザは他のデバイスで証明書の登録を並行して実行できます。これらの並列操作の進行状況は、同じユーザインターフェイスでモニタできます。それぞれのアイコンには、証明書の登録ステータスが表示されます。

関連トピック

自己署名登録を使用した証明書のインストール （3 ページ）
SCEP の登録を使用した証明書のインストール （4 ページ）
手動登録を使用した証明書のインストール （5 ページ）
PKCS12 ファイルを使用した証明書のインストール （6 ページ）

自己署名登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [自己署名（Self-Signed）] の証明書登録オブジェクトを選択します。

- [(+)] をクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加 を参照してください。

ステップ 4 [追加（Add）] をクリックして、自己署名の自動登録プロセスを開始します。

自己署名登録タイプのトラストポイントの場合、[CA 証明書（CA Certificate）] ステータスは、常にアイコンで表示されます。これは、管理対象デバイス自体が独自の CA として機能し、独自のアイデンティティ証明書を生成するために CA 証明書を必要としないためです。

[ID 証明書（Identity Certificate）] は、デバイスが独自の自己署名アイデンティティ証明書を作成すると、InProgress から Available に変化します。

ステップ 5 虫めがねをクリックして、このデバイスの自己署名アイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

SCEP の登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

始める前に

（注） SCEP 登録を使用すると、管理対象デバイスと CA サーバとの間に直接接続が確立されます。したがって、登録プロセスを開始する前に、デバイスが CA サーバに接続されていることを確認してください。

ステップ 1 [デバイス（Devices）] > [証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [SCEP] の証明書登録オブジェクトを選択します。
- [(+)] アイコンをクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加を参照してください。

ステップ 4 [追加（Add）] をクリックして、自動登録プロセスを開始します。

SCEP 登録タイプのトラストポイントの場合、[CA 証明書（CA Certificate）] ステータスは、CA サーバから CA 証明書が取得され、デバイスにインストールされると、InProgress から Available に遷移します。

[アイデンティティ証明書（Identity Certificate）] は、デバイスが SCEP を使用したアイデンティティ証明書を指定の CA から取得すると、`InProgress` から `Available` に変化します。場合によっては、アイデンティティ証明書の取得には手動更新が必要になります。

ステップ 5 虫めがねをクリックして、このデバイスに作成してインストールしたアイデンティティ証明書を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

手動登録を使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面で [追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウン リストからデバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウンリストからタイプが [マニュアル（Manual）] の証明書登録オブジェクトを選択します。
- [(+)] アイコンをクリックして、新しい証明書登録オブジェクトを追加します。証明書の登録オブジェクトの追加を参照してください。

ステップ 4 [追加（Add）] をクリックして、登録プロセスを開始します。

ステップ 5

ステップ 6 アイデンティティ証明書を取得するための PKI CA サーバに対する適切なアクティビティを実行します。

a) [アイデンティティ証明書（Identity Certificate）] の警告アイコンをクリックして、CSR を表示してコピーします。

b) この CSR を使用してアイデンティティ証明書を取得するための PKI CA サーバに対する適切なアクティビティを実行します。

このアクティビティは、Firepower Management Center または管理対象デバイスとは完全に無関係です。完了すると、管理対象デバイスのアイデンティティ証明書が生成されます。ファイルに配置できます。

c) 手動プロセスを終了するには、取得したアイデンティティ証明書を管理対象デバイスにインストールします。

Firepower Management Center ダイアログに戻って、[アイデンティティ証明書の参照（Browse Identity Certificate）] を選択して、アイデンティティ証明書ファイルを選択します。

ステップ 7 [インポート（Import）] を選択して、アイデンティティ証明書をインポートします。

[アイデンティティ証明書（Identity Certificate）] のステータスは、インポートが完了すると `Available` になります。

ステップ 8 虫めがねをクリックして、このデバイスの [アイデンティティ証明書（Identity Certificate）] を表示します。

次のタスク

登録が完了すると、証明書登録オブジェクトと同じ名前のトラストポイントがデバイス上に生成されます。サイト間およびリモート アクセス VPN 認証方式の設定でこのトラストポイントを使用します。

PKCS12 ファイルを使用した証明書のインストール

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin

ステップ 1 [デバイス（Devices）]>[証明書（Certificates）] 画面の順に移動し、[追加（Add）] を選択して、[新規証明書の追加（Add New Certificate）] ダイアログを開きます。

ステップ 2 [デバイス（Device）] ドロップダウンリストから、事前設定された管理対象デバイスを選択します。

ステップ 3 次のいずれかの方法で、証明書の登録オブジェクトとこのデバイスを関連付けます。

- ドロップダウン リストから PKCS タイプの 証明書の登録オブジェクト を選択します。
- [(+)] アイコンをクリックして新しい証明書の登録オブジェクト を追加します。証明書の登録オブジェクトの追加を参照してください。

ステップ 4 [ツイカ（Add）] を押します。

[CA証明書（CA Certificate）] および [アイデンティティ証明書（Identity Certificate）] のステータスは、デバイスに PKCS12 ファイルがインストールされるときに `In Progress` から `Available` に変化します。

（注） 初めて PKCS12 ファイルをアップロードすると、ファイルが CertEnrollment オブジェクトの一部として Firepower Management Center に格納されます。不正なパスフレーズや展開の失敗が原因で登録できなかった場合は、ファイルをアップロードせずに PKCS12 証明書の登録を再試行します。PKCS12 ファイル サイズは 24 K を超えてはなりません。

ステップ 5 `Available` になったら、虫めがねをクリックして、このデバイスのアイデンティティ証明書を表示します。

次のタスク

管理対象デバイスの証明書（トラストポイント）には、PKCS#12 ファイルと同じ名前が付けられます。この証明書は、VPN 認証設定で使用します。

FTD 証明書のトラブルシューティング

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin/Network Admin/Security Approver

Firepower Threat Defense VPN 証明書の注意事項と制約事項 （1 ページ）を参照して、証明書の登録環境のバリエーションが原因で問題が発生しているかどうかを判断してください。その後、次の点を確認します。

- デバイスから CA サーバへのルートがあることを確認します。

  CA サーバのホスト名が登録オブジェクトで指定されている場合、Flex コンフィギュレーションを使用して、サーバに到達できるように DNS を適切に設定します。あるいは、CA サーバの IP アドレスを使用することもできます。

- Microsoft 2012 CA サーバを使用している場合、デフォルトの IPsec テンプレートは管理対象デバイスで受け入れられないため、これを変更する必要があります。

  作業テンプレートを設定するには、MS CA のドキュメントを参照しながら次の手順に従います。

  1. IPsec（オフライン要求）テンプレートを複製します。
  2. [拡張子（Extensions）] タブで、[アプリケーション ポリシー（Application policies）] として [*IP* セキュリティ *IKE* 中間（*IP security IKE intermediate*）]ではなく、[*IP* セキュリティ末端システム（*IP security end system*）] を選択します。
  3. アクセス許可とテンプレート名を設定します。
  4. 新しいテンプレートを追加し、レジストリ設定を変更して新しいテンプレート名を反映させます。