証明書

証明書の要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

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

- PKI 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、証明書の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。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、管理者によるアクションが必要になります。

- 証明書の登録が完了すると、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。
- Firewall Threat Defenseデバイスは、Microsoft Certificate Authority（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います。
- Firewall Threat Defenseデバイスは、認証局（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管理ガイドライン

- 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同じ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。

Firewall Threat Defense 証明書の管理

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。

手順

ステップ1 **[デバイス（Devices）]** > **[証明書（Certificates）]** を選択します。

この画面には、リスト表示されるデバイスごとに次の列が表示されます。

- [名前（Name）]：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が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。

- [ドメイン（Domain）]：特定のドメインに登録された証明書が表示されます。
- [登録タイプ（Enrollment Type）]：トラストポイントに使用される登録のタイプが表示されます。
- [ステータス（Status）]：[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）。

  CA 証明書の情報を表示すると、CA 証明書を発行したすべての認証局の階層を確認できます。

  登録に失敗した場合は、ステータスをクリックして失敗メッセージを表示します。
- 証明書で弱い暗号の使用を有効にするには、右側の [Enable weak-crypto] をクリックします。トグルボタンをクリックすると、弱い暗号を有効にする前に確認のための警告が表示されます。[Yes] をクリックして、弱い暗号を有効にします。

  （注）
  弱い暗号の使用が原因で証明書の登録が失敗した場合は、弱い暗号を有効にすることを求めるメッセージが表示されます。弱い暗号化を使用する必要がある場合は、弱い暗号を有効にするができます。
- 追加の列には、次のタスクを実行するためのアイコンが一覧表示されます。
  - 証明書のエクスポート：クリックして、証明書のコピーをエクスポートおよびダウンロードします。PKCS12（完全な証明書チェーン）形式または PEM（アイデンティティ証明書のみ）形式のエクスポートを選択できます。

    PKCS12 証明書形式でエクスポートして後でファイルをインポートするには、パスフレーズを指定する必要があります。
  - 証明書の再登録：既存の証明書を再登録します。
  - 証明書ステータスの更新：証明書を更新して、Firepower Threat Defense デバイスの証明書ステータスを Firepower Management Center に同期させます。
  - 証明書の削除：トラストポイントに関連付けられているすべての証明書を削除します。

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ー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、ユーザー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 （6 ページ）
SCEP の登録を使用した証明書のインストール （8 ページ）
手動登録を使用した証明書のインストール （9 ページ）
PKCS12 ファイルを使用した証明書のインストール （10 ページ）

CA バンドルの自動更新

CLI コマンドを使用して CA 証明書を自動的に更新するように Management Center を設定できます。デフォルトでは、バージョン 7.0.5 をインストールまたは 7.0.5 にアップグレードすると、CA 証明書が自動的に更新されます。

（注） IPv6 のみの展開では、一部のシスコのサーバーが IPv6 をサポートしていないため、CA 証明書の自動更新が失敗することがあります。このような場合は、**configure cert-update run-now force** コマンドを使用して CA 証明書を強制的に更新します。

手順

ステップ 1 SSH を使用して FMC CLI にログインします。仮想の場合は VM コンソールを開きます。

ステップ 2 ローカルシステムの CA 証明書が最新の証明書であるか確認できます。

configure cert-update test

このコマンドは、ローカルシステムの CA バンドルを（シスコサーバーからの）最新の CA バンドルと比較します。CA バンドルが最新の場合、接続チェックは実行されず、以下の例のようなテスト結果が表示されます。

例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

CA バンドルが古い場合、ダウンロードされた CA バンドルに対して接続チェックが実行され、テスト結果が表示されます。

例：

接続チェックが失敗した場合：

```
> configure cert-update test
Test failed, not able to fully connect.
```

例：

接続チェックが成功した場合、または CA バンドルがすでに最新の場合：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

ステップ 3 （任意）CA バンドルをすぐに更新する場合：

configure cert-update run-now

例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

このコマンドを実行すると、（シスコサーバーからの）CA 証明書が SSL 接続に対して検証されます。シスコサーバーのうち 1 つでも SSL 接続チェックが失敗した場合、プロセスは終了します。

例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

接続に失敗しても更新を続行するには、**force** キーワードを使用します。

例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

ステップ 4 CA バンドルが自動的に更新されないようにする場合は、構成を無効にします。

configure cert-update auto-update disable

例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

ステップ 5 CA バンドルの自動更新を再度有効にするには、次のコマンドを入力します。

configure cert-update auto-update enable

例：

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

CA 証明書の自動更新を有効にすると、更新プロセスはシステムで定義された時刻に毎日実行されます。

ステップ 6 （任意）CA 証明書の自動更新のステータスを表示します。

show cert-update

例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

自己署名登録を使用した証明書のインストール

手順

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 [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は、[CA 証明書（CA Certificate）] ステータスが常に表示されます。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。

EST 登録を使用した証明書のインストール

始める前に

（注） EST 登録を使用すると、管理対象デバイスと CA サーバー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 サーバーに接続されていることを確認してください。

（注） 証明書の有効期限が切れたときにデバイスを自動登録する EST の機能はサポートされていません。

手順

ステップ 1 [Devices] > [Certificates] 画面で [Add] をクリックして、[Add New Certificate] ダイアログを開きます。

ステップ 2 [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。

- [Cert Enrollment] ドロップダウンリストから EST 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）。

ステップ 4 [Add] をクリックして、デバイスに証明書を登録します。

[Identity Certificate] は、デバイスが EST 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。

SCEP の登録を使用した証明書のインストール

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 サーバー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 サーバーに接続されていることを確認してください。

手順

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 [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。
- [(+)] 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

手順

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 [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。
- [(+)] 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 アイデンティティ証明書を取得するための PKI CA サーバー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 サーバー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、Secure Firewall 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。これを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。

Secure Firewall 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。

（注）
バイナリ証明書（PKCS12、DER など）ファイルは Firewall Threat Defense でサポートされていないため、選択しないでください。

ステップ 6 [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 7 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

手順

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。
- [(+)] 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）。

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 Firewall 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。また、登録を成功させるには、オーバーライドを許可するように証明書の登録オブジェクトを変更するたびに、証明書の [パスフレーズ（Passphrase）] を更新する必要があります。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。

Firewall Threat Defense 証明書のトラブルシューティング

Secure Firewall 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）]>[アプリケーションポリシー（Application policies）] で、[*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。

- Firewall Management Center で、Firewall Threat Defense デバイスに関連する次のヘルスアラートが表示される場合があります。

  ```
  Code - F0853; Description - default Keyring's certificate is invalid, reason: expired
  ```

  （コード：F0853。説明：デフォルトのキーリングの証明書が無効です。理由：期限切れ。）

  解決策：このような場合は、CLISH CLI で、次のコマンドを使用してデフォルトの証明書を再生成します。

  ```
  > system support regenerate-security-keyring default
  ```

- CA 証明書のステータスに赤いバツ印が表示され、次のエラーが発生します。

  ```
  CA 証明書の設定に失敗する
  ```

  解決策：FMC での証明書エラーのトラブルシュートを参照してください。

- .pfx ファイル内の証明書のリストを確認するには、`certutil` や `openssl` などのツールを使用します。ID 証明書、SubCA 証明書、および CA 証明書（存在する場合）を含むチェーン全体を確認できます。
  - `certutil -dump cert.pfx`
  - `openssl pkcs12 -info -in cert.pfx`
- 次のエラーが表示されます。

  `ID 証明書のインポートが必要`

  解決策：FMC の「アイデンティティ証明書のインポートが必要」証明書エラーのトラブルシュートを参照してください。

証明書の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
手動登録の拡張機能	6.7	いずれか	アイデンティティ証明書なしで、CA 証明書のみを作成できるようになりました。CA 証明書がなくても CSR を生成し、CA からアイデンティティ証明書を取得することができます。
PKCS CA チェーン	6.7	いずれか	証明書を発行する認証局（CA）のチェーンを表示および管理できるようになりました。証明書のコピーをエクスポートすることもできます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。