Cisco Secure Firewall Management Center におけるリモートアクセス VPN ポリシーでの ACME 証明書の使用

Secure Firewall Management Center におけるリモートアクセス VPN ポリシーでの ACME 証明書の使用 2

対象読者 2

ACME 登録の概要 2

システム要件 4

ACME 証明書を使用するための前提条件 4

ACME 証明書の使用に関するガイドラインと制限事項 6

Firewall Management Center における ACME 登録のワークフロー 7

ACME 証明書の登録の検証 17

ACME 証明書のトラブルシュート 18

改訂：2026 年 3 月 9 日

Secure Firewall Management Center におけるリモートアクセス VPN ポリシーでの ACME 証明書の使用

対象読者

このガイドは、Management Center によって管理される 脅威防御 デバイスの SSL および TLS 証明書を管理するネットワーク管理者向けの内容です。Let's Encrypt からの Automated Certificate Management Environment （ACME）証明書を使用して、脅威防御 デバイスをリモートアクセス VPN ゲートウェイとして認証する詳細な手順を説明しています。

他の ACME サーバーから ACME 証明書を取得することもできますが、このガイドでは ACME サーバーとして Let's Encrypt を使用します。

サンプル シナリオ

Alex は Management Center を使用して複数の 脅威防御 デバイスを管理している企業のネットワーク管理者です。認証局である Let's Encrypt からの ACME 証明書を使用して、脅威防御 デバイス上のリモートアクセス VPN を保護しています。

ACME 登録の概要

ACME プロトコルは、SSL および TLS 証明書の発行、更新、管理を自動化するために設計された、オープンで標準化されたプロトコルです。ACME は認証局（CA）とクライアントとのやり取りを自動化することで、証明書を管理するための手動による複雑なプロセスを排除します。

Firewall Management Center は、認証インターフェイス経由で認証プロトコルを使用して ACME 対応 CA サーバーと通信します。ACME サーバーとの認証および通信には、デバイスごとに手動の CA 証明書が必要です。ACME サーバーは、Firewall Threat Defense デバイスの認証インターフェイスのポート 80 経由でドメイン所有権を検証します。ドメイン検証後、ACME サーバーはデバイスに SSL または TLS 証明書を発行します。

HA ペアでは、スタンバイデバイスが、アクティブデバイスの ACME 証明書の登録オブジェクトから ACME 証明書とすべての関連設定を継承します。

ACME 登録を使用する利点

- 自動化：次のようなタスクを含む、SSL および TLS 証明書のライフサイクルを自動化します。
  - 証明書の要求
  - ドメイン検証の管理
  - 証明書の更新

    ACME 登録オブジェクトを編集することで、ACME 証明書のドメイン情報を更新することもできます。

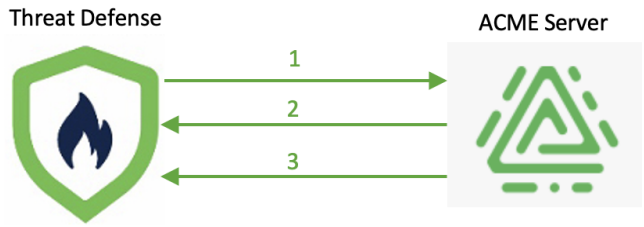
- 証明書の失効

- セキュリティ：次のようなさまざまなメカニズムでセキュリティを確実に維持します。
  - クライアントと CA サーバー間のセキュア通信に HTTPS を使用。
  - 認証要求にキーペアを使用。
  - 期限切れの証明書によるサービスの障害や拠点の脆弱性のリスクを軽減。
  - ドメイン所有権の検証。
- コスト効率：Let's Encrypt をはじめとする無料の証明書サービスの使用を許可し、SSL および TLS 認証のコストを削減します。
- 拡張性：複数のドメインやサブドメインにまたがる多数の証明書を効率的に管理し、拡張可能な SSL および TLS 証明書管理ソリューションを提供します。

ACME 証明書の仕組み

次の図は、ACME 証明書の登録のステージを示しています。

図 *1 : ACME* 証明書の登録のステージ



この表は、Firewall Threat Defense デバイスの ACME 証明書の登録のプロセスを説明しています。

ステージ	説明
1	Firewall Threat Defense デバイスが、送信元インターフェイスを介して特定のドメインまたはドメインのリストの ACME 証明書を要求します。
2	ACME サーバーが、Firewall Threat Defense デバイスの認証インターフェイスの TCP ポート 80 経由でドメイン所有権を検証します。 Firewall Threat Defense デバイスは、ドメイン検証に HTTP ベースのチャレンジメカニズム（HTTP-01）を使用します。 （注） Firewall Threat Defense は、登録チャレンジ応答プロセス中にポート 80 を開き、ACME チャレンジデータのみを提供します。ポートは、登録が成功または失敗した直後に閉じられます。

ステージ	説明
3	ドメイン検証後、ACME サーバーが Firewall Threat Defense デバイスに SSL または TLS 証明書を発行します。

（注） これらのステージが、証明書の登録要求の FQDN ごとに繰り返されます。

システム要件

表 1 は、このユースケースのプラットフォームとバージョンを示します。

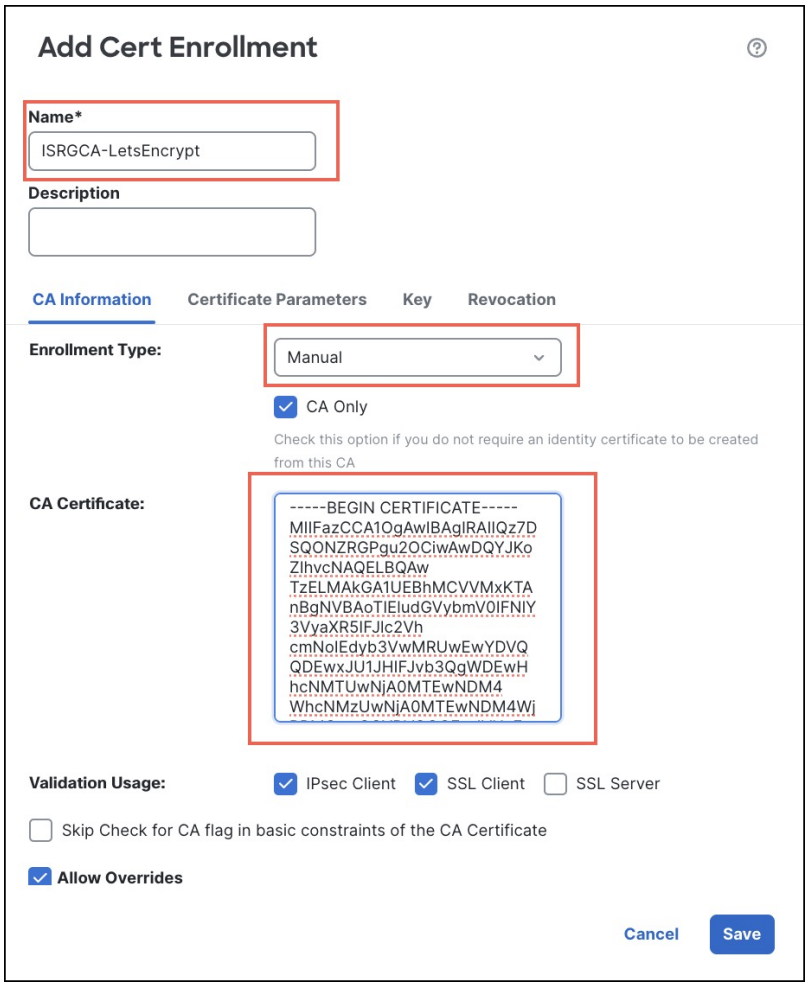
製品	バージョン	このマニュアルで使用するバージョン
Cisco Secure Firewall Management Center	10.0 以降	10.0
Cisco Secure Firewall Threat Defense	10.0 以降	10.0
ACME サーバー	-	Let’s Encrypt

ACME 証明書を使用するための前提条件

一般的な前提条件

- Firewall Threat Defense デバイスがバージョン 10.0 以降であることを確認します。
- Firewall Threat Defense プラットフォーム設定で DNS を設定して、ACME サーバーのドメイン名を解決します。
- ドメインがパブリック IP アドレスにマッピングされていることを確認します。この IP アドレスを使用してデバイスインターフェイスを設定し、ACME 証明書の登録で認証インターフェイスとして設定します。
- ACME CA 証明書（ACME サーバーを認証する手動 CA 専用証明書）をデバイスに登録します。
  - ACME サーバーとして Let’s Encrypt を使用する際は、https://letsencrypt.org/certificates/ から Internet Security Research Group（ISRG）ルート証明書を取得し、手動 CA 専用証明書としてデバイスにアタッチする必要があります。

    たとえば、https://letsencrypt.org/certs/isrgrootx1.pem.txt のルート証明書を使用して、ACME サーバーの手動 CA 証明書を設定します。



- デバイスのオブジェクトオーバーライドを設定する場合は、そのデバイスのACME CA証明書も登録する必要があります。

- ACME サーバーと Firewall Threat Defense デバイスに同じ NTP サーバーを設定します。

ACME サーバーの前提条件

- Let's Encrypt ACME サーバーにアクセスできることを確認します。
- ACME サーバーが Firewall Threat Defense デバイスから到達可能であることを確認します。
- ACME サーバーがドメイン名と代替 FQDN を検証できることを確認します。
- 認証インターフェイスが送信元インターフェイスと異なる場合は、デバイスの送信元インターフェイスからACMEサーバーに到達できることを確認します。

VPN ロードバランシングの前提条件

VPN ロードバランシンググループに ACME 登録オブジェクトを設定する場合は、[**Alternate FQDN**] フィールドにディレクタとメンバーの FQDN を必ず含めてください。ACME 証明書はワイルドカード証明書をサポートしていないことに注意してください。

ACME 証明書の使用に関するガイドラインと制限事項

ガイドライン

有効期間より前にデバイス上の ACME 証明書を更新するには、証明書を再登録し、デバイスに設定を展開します。

制限事項

- ACME 証明書は以下をサポートしていません。
  - サイト間 VPN
  - 統合モードの管理インターフェイス
  - DNS 認証（DNS-01）。サポートしているのは HTTP-01 のみです。
  - ドメインのオーバーライド
  - ワイルドカード証明書：これらの証明書は、ドメイン名フィールドでワイルドカード文字（*）を使用して、単一のドメインと複数のサブドメインをセキュア化するものです。
  - クラスタリング
- ACME 証明書は、RSA キーの場合は 2048、3072、および 4096 のキーサイズ、ECDSA キーの場合は 256、384、および 521 のキーサイズのみをサポートします。
- ACME 登録は、コントロールプレーン ACL と互換性がありません。

  コントロールプレーン ACL で Let's Encrypt を使用する場合は、次の手順を実行します。

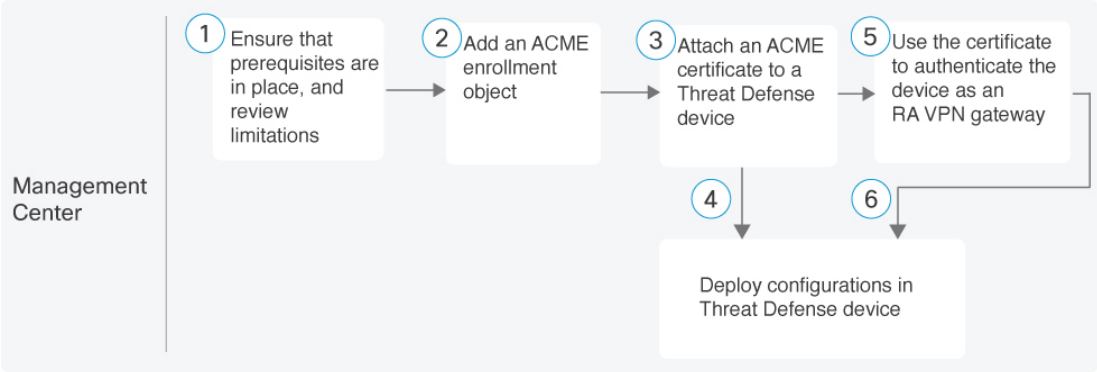
  1. ACME 登録の前に ACL を無効化し、ポート 80 アクセスを許可します。
  2. ACME 証明書を登録します。
  3. 登録を確認します。
  4. ACL を再度有効化します。

  コントロールプレーン ACL で Let's Encrypt 以外の ACME サーバーを使用する場合は、ACL にサーバーの FQDN を含めます。

Firewall Management Center における ACME 登録のワークフロー

process_workflow

Firewall Management Center で ACME 証明書を登録する各段階は次のとおりです。



1. ACME 証明書を使用するための前提条件 （4 ページ） が満たされていることを確かめ、ACME 証明書の使用に関するガイドラインと制限事項 （6 ページ） を確認します。
2. ACME 証明書の登録オブジェクトの追加 （7 ページ）。
3. Firewall Threat Defense デバイスへの ACME 証明書のアタッチ （12 ページ）。
4. 設定をデバイスに展開します。
5. ACME 証明書をアイデンティティ証明書として使用して、デバイスを RA VPN ゲートウェイとして認証します。詳細については、「ACME 証明書を使用した新しいリモートアクセス VPN ポリシーの設定 （14 ページ）」を参照してください。
6. 設定をデバイスに展開します。

ACME 証明書の登録オブジェクトの追加

始める前に

必ずACME 証明書を使用するための前提条件 （4 ページ）およびACME 証明書の使用に関するガイドラインと制限事項 （6 ページ）を確認してください。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[PKI]** > **[証明書登録（Certificate Enrollment）]**を選択します。

ステップ 2 **[Add Cert Enrollment]** をクリックします。

ステップ 3 [**Name**] フィールドに ACME 証明書の登録の名前を入力します。

登録が完了すると、管理デバイスのトラストポイント名は指定された名前になります。

ステップ 4 （オプション）[**Description**] フィールドに登録の説明を入力します。

ステップ 5 [**CA Information**] タブで次の手順を実行します。

a) [**Enrollment Type**] ドロップダウンリストから、[**ACME**] を選択します。

b) [**Enrollment URL**] フィールドで、デフォルトの URL https://acme-v02.api.letsencrypt.org/directory を使用します。これは Let's Encrypt の ACME CA サーバーの URL です。

[**Authentication Protocol**] フィールドの [**HTTP-01**] は、ドメイン所有権の検証に使用される事前定義されたプロトコルです。

c) [**Authentication Interface**] ドロップダウンリストから、ACME サーバーがドメインの所有権を確認するためにデバイスと通信するインターフェイスがある、セキュリティゾーンまたはインターフェイスグループを選択します。

[+] をクリックして、セキュリティゾーンまたはインターフェイスグループを追加します。デフォルトのインターフェイスは管理インターフェイスです。

d) [**Source Interface**] ドロップダウンリストから、デバイスが ACME サーバーと通信して登録済みの ACME 証明書を要求および受信するインターフェイスがある、セキュリティゾーンまたはインターフェイスグループを選択します。

[+] をクリックして、セキュリティゾーンまたはインターフェイスグループを追加します。デフォルトのインターフェイスは管理インターフェイスです。送信元インターフェイスと認証インターフェイスは同じものにすることできます。

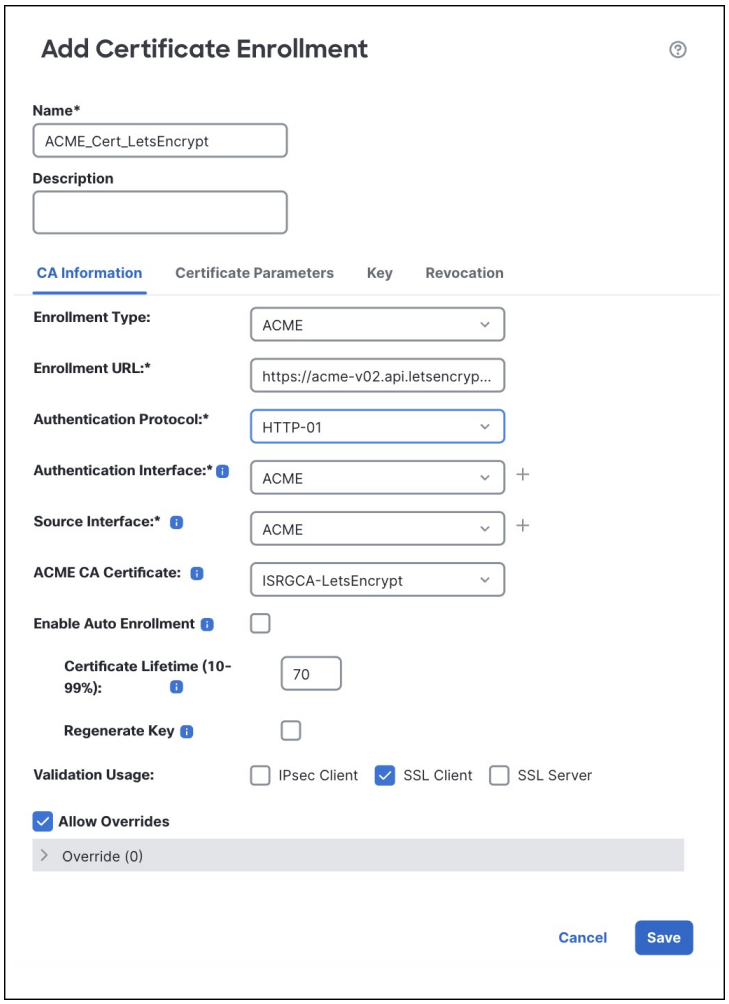
e) [**CA only Certificate**] ドロップダウンリストから、ACME サーバーを認証する手動 CA 専用証明書を選択します。

f) [**Auto Enroll**] チェックボックスをオンにして、設定した有効期間に基づいて ACME 証明書の自動登録を有効にします。

g) [**Lifetime**] フィールドに、証明書の再登録が自動的に開始されるまでの ACME 証明書の有効期間の割合を入力します。デフォルト値は 70 です。

たとえば、証明書の有効期間が 100 日で、このフィールドが 80 に設定されている場合、自動更新は 81 日にトリガーされます。

h) ACME 登録ごとに新しいキーを再生成するには、[**Regenerate Key**] チェックボックスをオンにします。このチェックボックスをオフにすると、以前のキーが登録に使用されます。



ステップ 6 [**Certificate Parameters**] タブで次の手順を実行します。

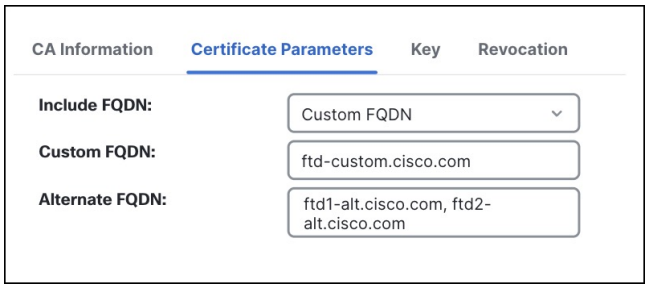
a) [**Include FQDN**] ドロップダウンリストから、次のいずれかを選択して証明書の FQDN を定義します。

- [**Use Device Hostname as FQDN**]（デフォルト）
- [**Custom FQDN**]：このオプションを選択した場合は、[**Custom FQDN**] フィールドに FQDN を入力します。

  この例では、こちらのオプションを使用します。

b) [**Alternate FQDN**] フィールドに、証明書のサブジェクト代替名（SAN）フィールドに追加する FQDN のカンマ区切り値を入力します。

デジタル証明書では、このフィールドにより、1 つの証明書で複数のドメイン名、サブドメイン、または IP アドレスを保護できます。



ステップ 7 [**Key**] タブで次の手順を実行します。

a) [**RSA**] または [**ECDSA**] キータイプをクリックします。

b) [**Key Name**] フィールドで、次のように選択します。

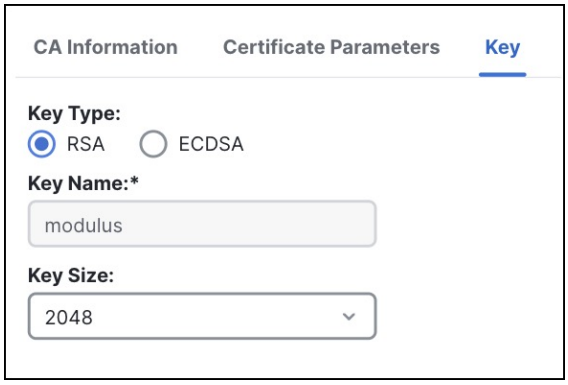
- RSA キーの場合、[**modulus**] のみがサポートされます。
- ECDSA キーの場合、[**elliptic-curve name**] のみがサポートされます。

c) [Key Size] ドロップダウンリストからキーサイズを選択します。

- RSA キーの場合は、2048、3072、または 4096 を使用します。

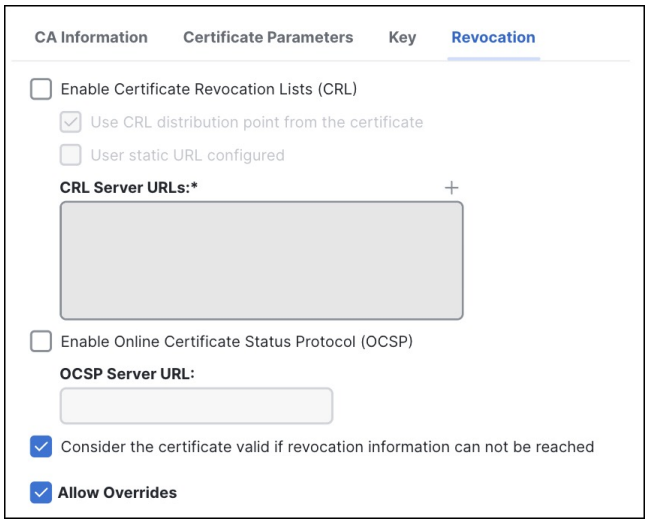
  この例では、値が 2048 の RSA キーを使用します。

- ECDSA キーの場合は、256、384、または 521 を使用します。



ステップ 8 （オプション）必要に応じて、[**Advanced Settings**] を構成します。

ステップ 9 [**Revocation**] タブでは、デフォルト値をそのまま使用できます。

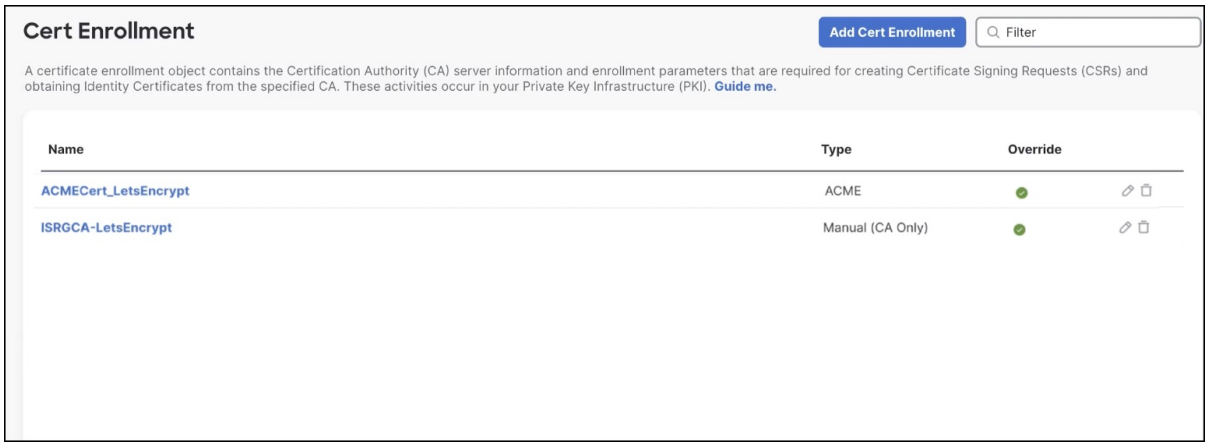


ステップ 10 [**Allow Overrides**] チェックボックスをオンにし、任意のデバイスまたはドメインのオブジェクトのオーバーライドを設定します。

デフォルトで、このオプションは有効になっています。オブジェクトのオーバーライドを設定する場合は、最初のデバイスに証明書を登録する前に、このオプションを有効にする必要があります。

ステップ 11 [保存（Save）] をクリックします。

ACME 証明書の登録オブジェクトは [**Certificate Enrollment**] ページで確認できます。



次のタスク

ACME 証明書の登録オブジェクトの編集 （12 ページ） または Firewall Threat Defense デバイスへの ACME 証明書のアタッチ （12 ページ）

ACME 証明書の登録オブジェクトの編集

始める前に

ACME 証明書の登録オブジェクトを作成します。詳細については、「ACME 証明書の登録オブジェクトの追加 （7 ページ）」を参照してください。

手順

ステップ 1 証明書の登録オブジェクトのページで、編集する ACME 証明書登録オブジェクトの横にある編集アイコンをクリックします。

ステップ 2 [**CA Information**] タブをクリックします。

ステップ 3 必要に応じて [**Auto-Enroll**]、[**Lifetime**]、[**Regenerate Key**] の各フィールドを更新します。

このタブの他のフィールドは編集できません。

ステップ 4 [**Certificate Parameters**] タブをクリックします。

ステップ 5 必要に応じて [**Alternate FQDN**] フィールドを編集します。

このタブの他のフィールドは編集できません。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 **[デバイス（Devices）] > [証明書（Certificates）]**を選択します。

ACME 証明書の横に、「展開は保留中です。再登録して証明書を更新してください」というメッセージが表示されます。

ステップ 8 ACME 証明書を再登録して、更新された設定をデバイスにプッシュします。

再登録時に既存の代替 FQDN が削除され、新しい FQDN がデバイスにプッシュされます。

次のタスク

Firewall Threat Defense デバイスへの ACME 証明書のアタッチ （12 ページ）

Firewall Threat Defense デバイスへの ACME 証明書のアタッチ

始める前に

ACME 証明書の登録オブジェクトを追加します。詳細については、ACME 証明書の登録オブジェクトの追加 （7 ページ）を参照してください。

手順

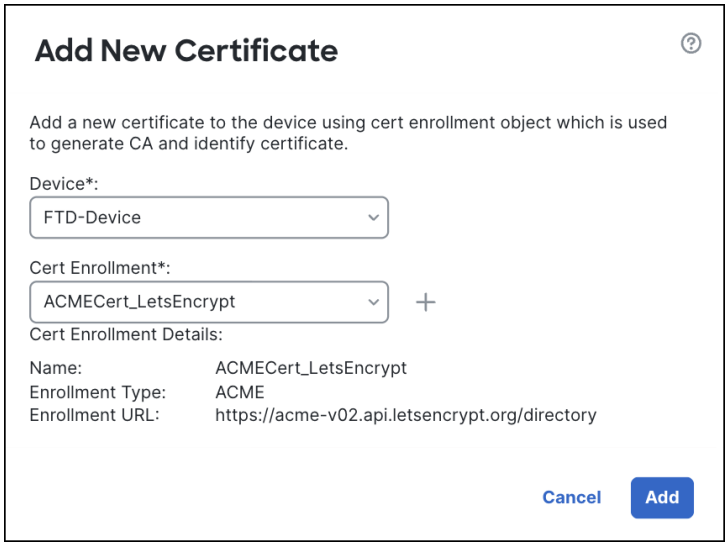
ステップ 1 **[デバイス（Devices）] > [証明書（Certificates）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [**Device**] ドロップダウンリストから Firewall Threat Defense デバイスを選択します。

ステップ 4 [**Cert Enrollment**] ドロップダウンリストから ACME 証明書を選択するか、[+] をクリックして ACME 証明書の登録を作成します。

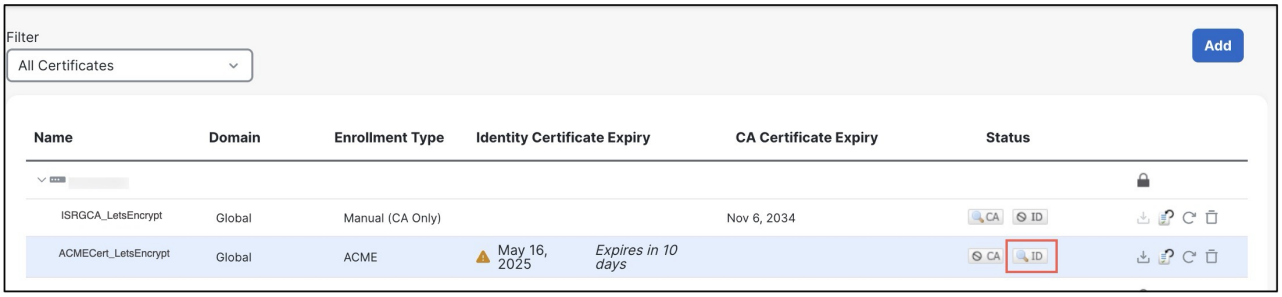
証明書の詳細を確認します。



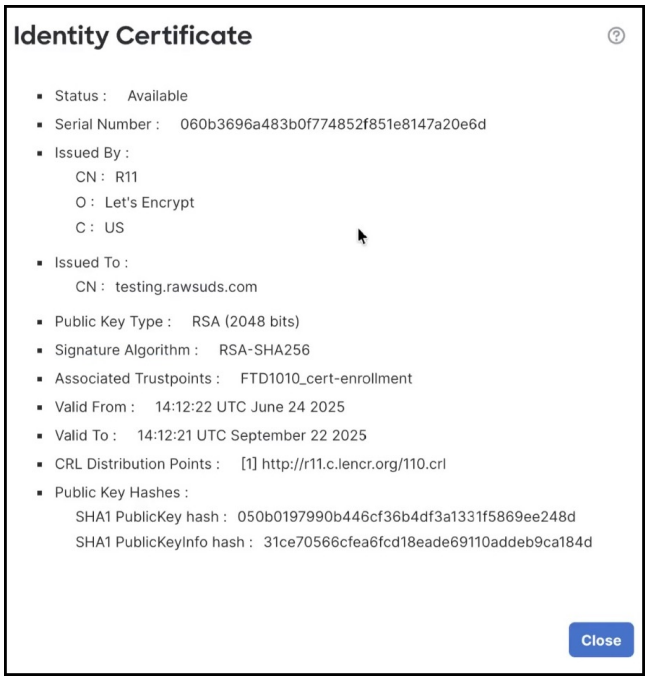
ステップ 5 [**Add**] をクリックして、デバイスに証明書をアタッチします。

このプロセス中、[**Certificates**] ページの [**Status**] はタスクが完了するまで [**In Progress**] になります。

証明書がデバイスに正常にアタッチされると、[**Status**] の下に [**ID**] アイコンが表示されます。



[**ID**] アイコンをクリックして証明書の詳細を表示します。詳細を確認して [**Close**] をクリックします。



次のタスク

1. 設定をデバイスに展開します。

   デプロイメントが成功すると、デバイスは ACME サーバーに ACME 証明書を要求します。ドメインの検証後、ACME サーバーは ACME 証明書を発行します。

2. ACME 証明書を使用して、デバイスを RA VPN ゲートウェイとして認証します。詳細については、ACME 証明書を使用した新しいリモートアクセス VPN ポリシーの設定 （14 ページ）またはACME 証明書を使用したリモートアクセス VPN ポリシーの更新 （16 ページ）を参照してください。

ACME 証明書を使用した新しいリモートアクセス VPN ポリシーの設定

始める前に

ACME 証明書を Firewall Threat Defense にアタッチし、デバイスに設定を展開したことを確認します。詳細については、Firewall Threat Defense デバイスへの ACME 証明書のアタッチ （12 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**を選択します。

ステップ 2 [**Add**] をクリックして新しいリモートアクセス VPN ポリシーを作成します。

ステップ 3 [**Name**] フィールドにリモートアクセス VPN ポリシーの名前を入力します。

ステップ 4 [**Description**] フィールドにポリシーの説明を入力します。

ステップ 5 [**VPN Protocols**] でプロトコルを選択します。

SSL または **IPSec-IKEv2**、あるいはその両方の VPN プロトコルを選択できます。Firewall Threat Defense は、VPN トンネルを経由するパブリックネットワークを介してセキュアな接続を確立するために両方のプロトコルをサポートしています。

ステップ 6 [**Targeted Devices**] でデバイスを選択します。

ここで選択するデバイスは、VPN クライアントユーザーのリモートアクセス VPN ゲートウェイとして機能します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [接続プロファイル（Connection Profile）] および [グループポリシー（Group Policy）] 設定を設定します。

ステップ 9 [認証、認可、およびアカウンティング（Authentication, Authorization & Accounting）] の設定を指定します。

ステップ 10 [クライアントアドレスの割り当て（Client Address Assignment）] の設定を指定します。

ステップ 11 [グループポリシー（Group Policy）] の設定を指定します。

ステップ 12 [次へ（Next）] をクリックします。

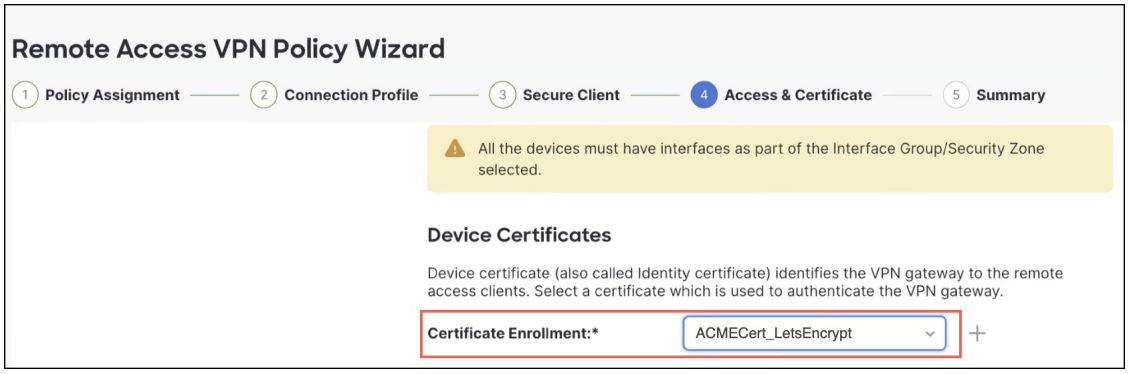
ステップ 13 VPN ユーザーがリモートアクセス VPN への接続に使用する AnyConnect イメージを選択します。

ステップ 14 [次へ（Next）] をクリックします。

ステップ 15 [入力 VPN アクセスのネットワーク インターフェイス（Network Interface for Incoming VPN Access）] を設定します。

ステップ 16 [デバイス証明書（Device Certificates）] を設定します。

デバイス証明書（アイデンティティ証明書とも呼ばれる）により、リモートアクセスクライアントへの VPN ゲートウェイが識別されます。VPN ゲートウェイの認証に使用する証明書を選択します。[**Certificate Enrollment**] ドロップダウンリストから ACME 証明書を選択し、VPN ゲートウェイを認証します。



ステップ 17 [**サービスアクセス制御（Service Access Control**）] を設定します。

ステップ 18 [VPN トラフィックのアクセス制御（Access Control for VPN Traffic）] を設定します。

ステップ 19 [次へ（Next）] をクリックします。

ステップ 20 リモートアクセス VPN ポリシー構成の [概要（Summary）] を表示します。

[**Remote Access Summary**] ページには、これまでに設定したすべてのリモートアクセス VPN 設定が表示され、選択したデバイスにリモートアクセス VPN ポリシーを展開する前に実行する必要がある追加設定へのリンクが示されます。

必要に応じて、[戻る（Back）] をクリックして設定に変更を加えます。

ステップ 21 リモート アクセス VPN ポリシーの基本設定を完了するには、[終了（Finish）] をクリックします。

ステップ 22 設定をデバイスに展開します。

次のタスク

ACME 証明書の登録の検証 （17 ページ）

リモートアクセス VPN の設定に関する詳細については、Firewall Management Center デバイス設定ガイドの「新規リモートアクセス VPN 接続の設定」を参照してください。

ACME 証明書を使用したリモートアクセス VPN ポリシーの更新

既存のリモートアクセス VPN ポリシーのデバイスに ACME 証明書を追加するには、次の手順を実行します。

始める前に

1. ACME 証明書を Firewall Threat Defense にアタッチし、デバイスに設定を展開したことを確認します。詳細については、「Firewall Threat Defense デバイスへの ACME 証明書のアタッチ （12 ページ）」を参照してください。
2. リモートアクセスポリシーが設定されていることを確認します。

手順

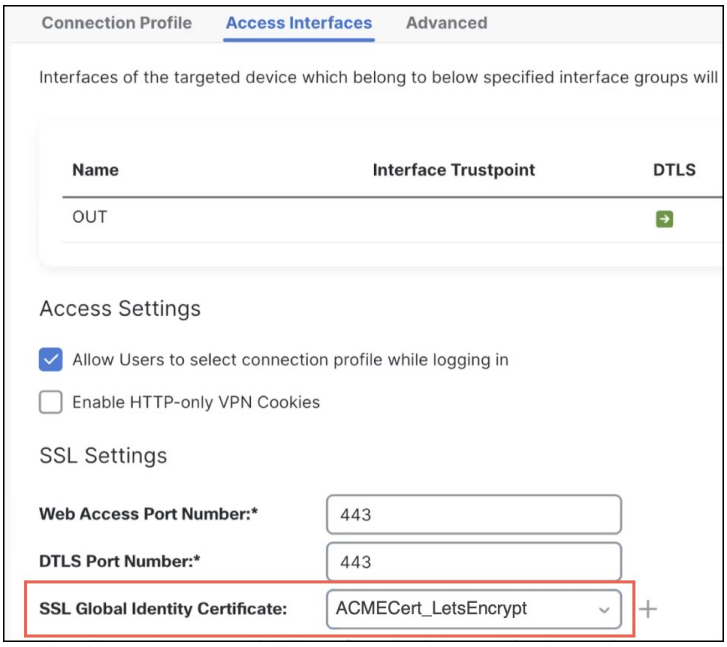
ステップ 1 **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**を選択します。

ステップ 2 編集するリモートアクセスポリシーの横にある編集アイコンをクリックします。

ステップ 3 [**Access Interfaces**] をクリックします。

ステップ 4 [**SSL Global Identity Certificate**] ドロップダウンリストで、ACME 証明書を選択します。

図 *2*：



ステップ 5 [保存（Save）] をクリックします。

ステップ 6 設定をデバイスに展開します。

デプロイメント中、ACME 証明書がデバイスの SSL トラストポイントにリンクされ、リモートアクセス VPN 接続でセキュアな SSL 通信のために新しい証明書が使用されるようになります。

次のタスク

ACME 証明書の登録の検証 （17 ページ）

ACME 証明書の登録の検証

Firewall Threat Defense デバイスの CLI から次のコマンドを実行します。

- **show crypto ca certificates**

  Firewall Threat Defense デバイスに存在する証明書の詳細を表示します。ACME 証明書がデバイスにインストールされているかどうかを確認できます。

```
firepower#show crypto ca certificates LE_ACME_cert_FTD1010
Certificate
  Status: Available
  Certificate Serial Number: 060b3696a483b0f774852f851e8147a20e6d
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: RSA-SHA256
  Issuer Name:
    CN=R11
```

```
    O=Let's Encrypt
    C=US
  Subject Name:
    CN=test.rawsuds.com
  CRL Distribution Points:
    [1]  http://r11.c.lencr.org/110.crl
  Validity Date:
    start date: 14:12:22 UTC Jun 24 2025
    end   date: 14:12:21 UTC Sep 22 2025
    renew date: 14:12:21 UTC Aug 26 2025
  Storage: immediate
  Associated Trustpoints: FTD1010_cert-enrollment
  Public Key Hashes:
   SHA1 PublicKey hash:     050b0197990b446cf36b4df3a1331f5869ee248d
   SHA1 PublicKeyInfo hash: 31ce70566cfea6fcd18eade69110addeb9ca184d
```

- **show crypto ca trustpoints**

  Firewall Threat Defense デバイスに存在するトラストポイントに関する詳細を表示します。

  [**Device Certificate**] フィールドは、証明書がデバイスにインストールされているかどうかを示します。

  [**Last Enrollment Result**] フィールドには、最後の再登録が成功したことが表示されます。

```
firepower# show crypto ca trustpoints
Trustpoint LE_ACME_cert_FTD1010:
    Not authenticated.
    Device certificate: Expires at 14:12:21 UTC Sep 22 2025
    ACME URL: https://acme-v02.api.letsencrypt.org:443/directory
    Current enrollment status:       Idle
    Last enrollment attempt:         15:10:57 UTC Jun 24 2025
    Last enrollment type:            Manual
    Last enrollment result:          SUCCESS
    Auto enrollment request count:   0
    Manual enrollment request count: 3


Trustpoint ISRG_root-cert:
    Subject Name:
        CN=ISRG Root X1
        O=Internet Security Research Group
        C=US
    Serial Number: 8210cfb0d240e3594463e0bb63828b00
    CA Certificate configured.
    Device certificate: Not present
```

ACME 証明書のトラブルシュート

debug コマンドの使用

（注） debug コマンドによって CPU 使用率が上昇するため、ネットワーク通信が少ない期間中、特定の障害対応または TAC セッションにのみ使用してください。

- **debug crypto ca <debug-level>** コマンドを使用して、暗号 CA 動作に関連するデバッグログをキャプチャします。

- **debug crypto ca acme <debug-level>** コマンドを使用して、ACME 登録に関連するデバッグログをキャプチャします。

ACME 登録エラーのトラブルシュート

- **症状**：デバイスに ACME 証明書をアタッチすると、ステータスに `Failed` と表示されます。

  解決策：警告にカーソルを合わせて、推奨アクションを表示します。詳細については、「ACME 証明書を使用するための前提条件 （4 ページ）」を参照してください。

- **症状**：デバイスに ACME 証明書をアタッチすると、ステータスに `Failed` と表示されます。ID 記号にカーソルを合わせると、「アイデンティティ証明書の設定に失敗しました（Failed to configure identity certificate）」というエラーが表示されます。

  考えられる原因：ACME CA 証明書がデバイスにアタッチされていません。

  解決策：ACME CA 証明書をデバイスにアタッチします。

- **症状**：「サーバーに接続できません（Unable to connect to the server）」または「<ACME_server>に接続できません（Unable to connect to <ACME_server>）」というエラーメッセージが表示されます。

  考えられる原因：

  - ACME サーバーが到達不能です。
  - ACME サーバーは到達可能ですが、ACME サービスが実行されていません。
  - ACME CA 証明書がデバイスにアタッチされていません。

  解決策:

  - Firewall Management Center から ACME サーバーに到達可能であることを確認します。
  - ACME サービスの状態を確認し、実行されていない場合は再起動します。
  - デバイスに ACME CA 証明書をアタッチします。

- **症状**：「ACME サーバー証明書を検証できません（Unable to validate the ACME server certificate）」というエラーメッセージが表示されます。

  考えられる原因：デバイスの ACME CA 証明書が Firewall Management Center に登録されていません。

  解決策：Firewall Management Center でデバイスの ACME CA 証明書をアタッチします。

- **症状**：「ACME 処理のタイムアウト（ACME processing timeout）」というエラーメッセージが表示されます。

  考えられる原因：

  - Firewall Management Center が、要求された FQDN を [**Authentication Interface**] に解決できません。
  - ACME サーバーの URL が正しくありません。
  - デバイスプラットフォーム設定で DNS が構成されていません。
  - ドメイン名が不正確です。

解決策:

- Firewall Management Center が、要求された FQDN を [**Authentication Interface**] に解決できることを確認します。
- ACME サーバーの URL を確認します。
- `ping <interface><acme-ca-fqdn>` コマンドを実行して DNS 解決を確認し、デバイスのプラットフォーム設定で DNS が構成されているかどうかを確認します。
- FQDN または代替 FQDN を確認します。FQDN を更新する場合は、証明書を再登録します。

syslog の使用

ACME 登録 syslog を有効化するには、次の手順を実行します。

1. **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**を選択します。
2. プラットフォーム設定ポリシーを作成または編集します。
3. 左側のペインで、[Syslog] をクリックします。
4. [**Logging Setup**] タブをクリックし、[**Enable Logging**] チェックボックスをオンにします。
5. [**Basic Logging Settings**] で、[**Enable Logging**] チェックボックスをオンにします。
6. [**Logging to Secure Firewall Management Center**] で、[**All Logs**] または [**VPN Logs**] を選択します。
7. [**Syslog Settings**] タブをクリックします。
8. [**Enable All Syslog Messages**] タブをクリックします。

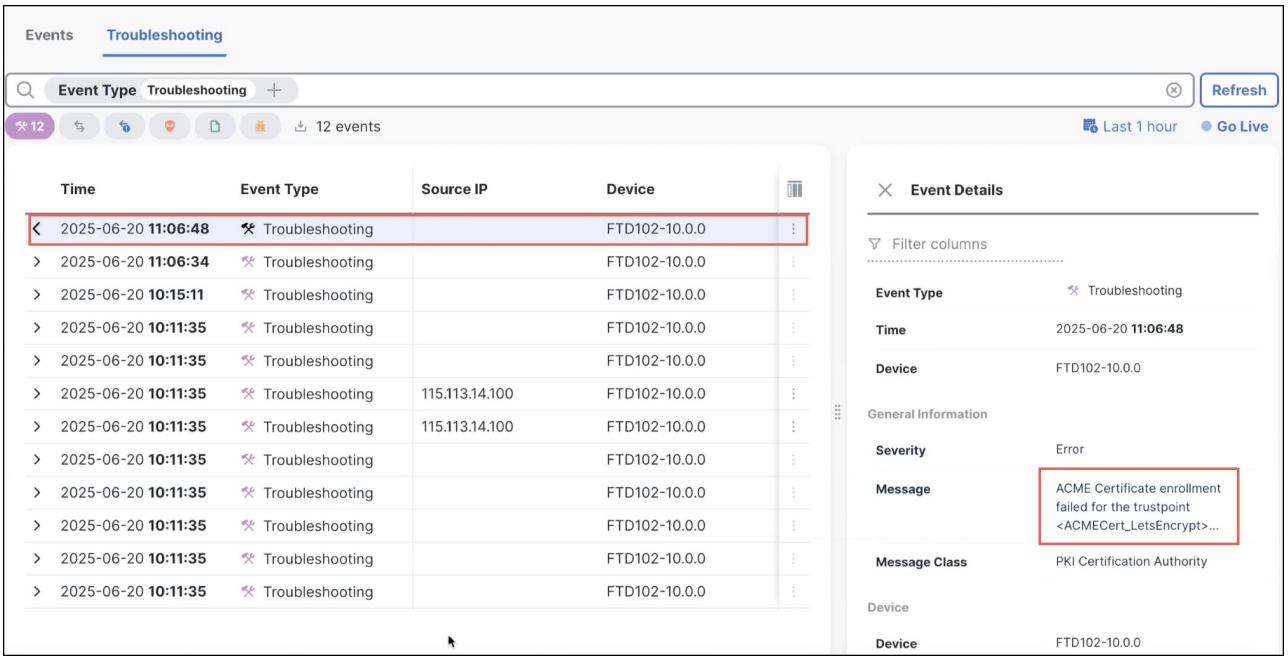
   ACME 登録 syslog は、717067、717068、717069、および 717070 です。

障害対応ログの使用

（注） デバイスプラットフォーム設定で syslog 設定を行ってください。

ACME 登録ログをモニターするには、次の手順を実行します。

1. **[分析（Analysis）] > [統合イベント（Unified Events）]**を選択します。
2. [**Troubleshooting**] タブをクリックします。
3. [**Troubleshooting Events**] テーブルでは、次の操作を実行できます。
   - 障害対応イベントの表示と分析。
   - [**Go Live**] をクリックすると、障害対応イベントをリアルタイムでモニターし、デバイスログと最近行った設定変更を関連付けることができます。


Events
Troubleshooting
Event Type Troubleshooting
Refresh
12
12 events
Last 1 hour
Go Live
Time
Event Type
Source IP
Device
2025-06-20 11:06:48 Troubleshooting FTD102-10.0.0
2025-06-20 11:06:34 Troubleshooting FTD102-10.0.0
2025-06-20 10:15:11 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting 115.113.14.100 FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting 115.113.14.100 FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
2025-06-20 10:11:35 Troubleshooting FTD102-10.0.0
Event Details
Filter columns
Event Type Troubleshooting
Time 2025-06-20 11:06:48
Device FTD102-10.0.0
General Information
Severity Error
Message ACME Certificate enrollment failed for the trustpoint <ACMECert_LetsEncrypt>...
Message Class PKI Certification Authority
Device
Device FTD102-10.0.0

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。