証明書の管理

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

Cisco Catalyst SD-WAN Manager での証明書の管理

[Configuration] > [Certificates] ページで Cisco SD-WAN Manager の証明書操作を実行します。

- トップバー：左側には、Cisco SD-WAN Manager メニューを展開および折りたたむためのメニューアイコン、および Cisco SD-WAN Manager 製品名が表示されます。右側には、多くのアイコンとユーザープロファイルのドロップダウンがあります。
- タイトルバー：画面のタイトルである証明書を含みます。
- [WAN Edge List] タブ：オーバーレイネットワークのコントローラにルータ認定シリアル番号ファイルをインストールし、ファイル内のシリアル番号を管理します。[Certificates] 画面を最初に開いたときには、[WAN Edge List] タブが選択されています。
  - [Send to Controllers]：WAN エッジルータシャーシ番号とシリアル番号をネットワーク内のコントローラに送信します。
  - [Table of WAN edge routers in the overlay network]：列を再配置するには、列のタイトルを目的の位置にドラッグします。
- [Controllers] タブ：証明書をインストールし、デバイスのシリアル番号を Cisco SD-WAN Validator にダウンロードします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

  - [Send to Cisco SD-WAN Validator]：コントローラのシリアル番号を Cisco SD-WAN Validator に送信します。
  - [Install Certificate]：コントローラデバイスに署名付き証明書をインストールします。このボタンは、**[Administration]** > **[Settings]** > **[Certificate Signing by Symantec]**で [Manual] を選択した場合のみ使用できます。
  - [Export Root Certificate]：ファイルにダウンロードできるコントローラデバイスのルート証明書のコピーを表示します。
  - [Table of controller devices in the overlay network]：列を再配置するには、列のタイトルを目的の位置にドラッグします。
  - [Certificate] ステータスバー：このバーは画面の下部にあり、**[Administration]** > **[Settings]** > **[Certificate Authorization]**で [Server Automated] を選択した場合のみ表示されます。 証明書のインストールプロセスの状態が表示されます。
    - Device Added
    - CSR の作成

- 証明書を待機中
- コントローラに送信

緑色のチェックマークは、ステップが完了したことを示します。灰色のチェックマークは、ステップがまだ実行されていないことを示します。

- 検索ボックス：[Contains] または [Match] 文字列の [Search Options] ドロップダウンが含まれています。
- [Refresh]アイコン：クリックすると、デバイステーブルのデータが最新のデータで更新されます。
- [Export]アイコン：クリックして、すべてのデータをCSV形式でファイルにダウンロードします。
- [Show Table Fields] アイコン：アイコンをクリックして、デバイステーブルの列を表示または非表示にします。デフォルトでは、すべての列が表示されます。

WAN Edge ルータ証明書ステータスの確認

[WAN Edge List]タブで、[Validate]列を確認します。ステータスは、次のいずれかになります。

- [Valid]（緑色で表示）：ルータの証明書は有効です。
- [Staging]（黄色で表示）：ルータはステージング状態です。
- [Invalid]（赤色で表示）：ルータの証明書は無効です。

WAN Edge ルータの検証

[Configuration] > **[Devices]** 画面を使用して Cisco vEdge デバイス と WAN ルータをネットワークに追加する際、[Validate the uploaded WAN Edge List and send to controllers] チェックボックスをクリックすることにより、ルータを自動的に検証し、そのシャーシ番号とシリアル番号をコントローラデバイスに送信することができます。このオプションをオンにしない場合は、各ルータを個別に検証し、そのシャーシ番号とシリアル番号をコントローラデバイスに送信する必要があります。次の手順を実行します。

1. [WAN Edge List] タブで、検証するルータを選択します。
2. [Validate] 列で、[Valid] をクリックします。
3. [OK] をクリックして、有効な状態への移行を確認します。
4. 検証するルータごとに上記の手順を繰り返します。
5. 画面の左上隅にある [Send to Controllers] ボタンをクリックして、検証済みルータのシャーシ番号とシリアル番号をネットワーク内のコントローラデバイスに送信します。Cisco

SD-WAN Manager NMS は、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。

WAN エッジルータのステージング

WAN エッジルータを最初に起動して設定する場合、Cisco SD-WAN Manager インスタンスを使用してステージング状態にできます。ルータがステージングの状態の場合、ルータを設定し、ルータが Cisco SD-WAN コントローラ および Cisco SD-WAN Manager インスタンスとの動作可能な接続を確立できることをテストできます。

ルータを実稼働サイトに物理的に配置した後、ルータの状態をステージングから有効に変更します。ルータが実稼働ネットワークに参加するのは、この時点でのみです。ルータをステージングするには、次の手順を実行します。

1. [WAN Edge List] タブで、ステージングするルータを選択します。
2. [Validate] 列で、[Staging] をクリックします。
3. [OK] をクリックして、ステージング状態への移行を確認します。
4. 画面の左上隅にある [Send to Controllers] をクリックして、WAN エッジ認証シリアル番号ファイルをコントローラと同期します。Cisco SD-WAN Manager NMS は、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。
5. ステージングを解除するには、WAN エッジルータを検証します。

WAN エッジルータの無効化

1. [WAN Edge List] タブで、無効にするルータを選択します。
2. [Validate] 列で、[Invalid] をクリックします。
3. [OK] をクリックして、無効な状態への移行を確認します。
4. 無効にするルータごとに上記の手順を繰り返します。
5. 画面の左上隅にある [Send to Controllers] ボタンをクリックして、検証済みルータのシャーシとシリアル番号をネットワーク内のコントローラデバイスに送信します。 Cisco SD-WAN Manager インスタンスは、プッシュ操作のステータスを示す [Push WAN Edge List] 画面を表示します。

コントローラのシリアル番号を Cisco Catalyst SD-WAN Validator に送信する

Cisco SD-WAN Validator は、オーバーレイネットワーク内の有効なコントローラを判別するために、コントローラのシリアル番号のリストを保持しています。Cisco SD-WAN Manager インスタンスは、証明書生成プロセス中にこれらのシリアル番号を学習します。

コントローラのシリアル番号を Cisco SD-WAN Validator に送信するには、次の手順を実行します。

1. [Controllers] タブで、画面の下部にある証明書ステータスバーを確認します。[Send to Controllers] チェックマークが緑色の場合、すべてのシリアル番号はすでに Cisco SD-WAN Validator に送信されています。灰色の場合は、1 つ以上のシリアル番号を Cisco SD-WAN Validator に送信できます。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. [Controllers] タブの [Send to Validator] ボタンをクリックします。コントローラのシリアル番号は 1 回だけ Cisco SD-WAN Validator に送信されます。すべてのシリアル番号が送信済みの場合、[Send to Validator] をクリックすると、エラーメッセージが表示されます。コントローラのシリアル番号を再送信するには、最初にデバイスを選択してから、[Validity] 列で [Invalid] を選択する必要があります。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

シリアル番号が送信されたら、Cisco SD-WAN Manager ツールバーの [Tasks] アイコンをクリックして、ファイルのダウンロードおよびその他の最近のアクティビティのログを表示します。

署名付き証明書のインストール

[Administration] > **[Settings]** > **[Certificate Signing by Symantec]** で、証明書生成プロセスに [Manual] オプションを選択した場合は、[Install Certificate] ボタンを使用して、コントローラデバイスに証明書を手動でインストールします。

Symantec またはエンタープライズルート CA は、証明書に署名すると、個別の署名済み証明書を含むファイルを返します。それらをローカルネットワーク内のサーバーに配置します。その後、それらを各コントローラーにインストールします。

1. [Controllers] タブの [Install Certificate] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. [Install Certificate] ウィンドウで、ファイルを選択するか、証明書のテキストをコピーして貼り付けます。
3. [Install] をクリックしてデバイスに証明書をインストールします。証明書にはコントローラを識別する情報が含まれているため、証明書をインストールするデバイスを選択する必要はありません。
4. 上記の手順を繰り返して、追加の証明書をインストールします。

ルート証明書のエクスポート

1. [Controllers] タブで、[Export Root Certificate] ボタンをクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. [Export Root Certificate] ウィンドウで、[Download] をクリックしてルート証明書をファイルにエクスポートします。
3. [閉じる（**Close**）] をクリックします。

証明書署名要求の表示

1. [WAN Edge List] または [Controllers] タブで、デバイスを選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[View CSR] をクリックして証明書署名要求（CSR）を表示します。

デバイス証明書署名要求の表示

1. [WAN Edge List] または [Controllers] タブで、Cisco IOS XE Catalyst SD-WAN デバイス を選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[View Device CSR] をクリックして証明書署名要求（CSR）を表示します。

   トラストポイントが設定されている Cisco IOS XE Catalyst SD-WAN デバイス の場合は、[More Actions] アイコンをクリックすると、次の 3 つのオプションを表示できます。

   - [View Device CSR]
   - [Generate Feature CSR]
   - [View Feature CSR]

（注） Cisco SD-WAN Manager は、デバイス証明書が Cisco SD-WAN Manager を介してインストールされている場合にのみアラームを生成します。証明書を手動でインストールした場合、Cisco SD-WAN Manager は証明書の期限切れのアラームを生成しません。

証明書の表示

1. [Controllers] タブで、デバイスを選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[View Certificate] をクリックします。

証明書署名要求の生成

以下の手順では、CSR の生成プロセスについて説明します。

コントローラ証明書署名要求の生成

1. Cisco SD-WAN Manager メニューから **[Configuration]** > **[Certificates]** の順に選択します。
2. [Controllers] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

3. 目的のコントローラについて、[…] をクリックし、[Generate CSR] を選択します。

   [Generate CSR] ウィンドウが表示されます。

4. [Generate CSR] ウィンドウで、[Download] をクリックしてファイルをローカル PC（つまり、Cisco SD-WAN Manager NMS への接続に使用している PC）にダウンロードします。

5. 上記の手順を繰り返して、別のコントローラの CSR を生成します。

機能証明書署名要求の生成

1. Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. [WAN Edge List] をクリックします。
3. 目的のデバイスで […] をクリックし、[Generate Feature CSR] を選択します。

   [Generate Feature CSR] ウィンドウが表示されます。

4. [Generate Feature CSR] ウィンドウで、[OK] をクリックして、機能 CSR の生成を続行します。この手順では、設定されているデバイスのトラストポイントを認証し、デバイスから CSR を抽出します。
5. CSR を生成するデバイスごとに、上記の手順を繰り返します。

WAN エッジデバイス証明書署名要求の生成

1. Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. [WAN Edge List] をクリックします。
3. 目的のデバイスで […] をクリックし、[Renew Device CSR] を選択します。

   [Renew Device CSR] ウィンドウが表示されます。

4. [Renew Device CSR] ウィンドウで、[OK] をクリックして新しい CSR の生成を続行します。

（注） Cisco vManage リリース 20.9.1 以降のリリース：[Renew Device CSR] をクリックすると、RSA 秘密キーと公開キーがリセットされ、新しいキーペアを使用する CSR が生成されます。また、Cisco SD-WAN Manager は Cisco vManage リリース 20.6.4 および以降の Cisco vManage 20.6.x リリースで新しい CSR を生成する前に、RSA 秘密キーと公開キーをリセットします。

前述のリリース以外の Cisco SD-WAN Manager リリース：[Renew Device CSR] をクリックすると、既存のキーペアを使用して CSR が生成されます。

RSA キーペアのリセット

1. [Controllers] タブで、デバイスを選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[Reset RSA] をクリックします。
3. [OK] をクリックしてデバイスの RSA キーのリセットを確認し、新しい公開キーまたは秘密キーで新しい CSR を生成します。

デバイスの無効化

1. [Controllers] タブで、デバイスを選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

2. 行の右側にある [More Actions] アイコンをクリックし、[Invalidate] をクリックします。
3. [OK] をクリックして、デバイスの無効化を確認します。

認定アクティビティログの表示

証明書関連のアクティビティのステータスを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager ツールバーにある [Task] アイコンをクリックします。Cisco SD-WAN Manager NMS には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。

2. 行をクリックして、タスクの詳細情報を表示します。Cisco SD-WAN Manager NMS ではステータスウィンドウが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

署名付き証明書の表示

署名付き証明書は、オーバーレイネットワーク内の Cisco SD-WAN デバイスの認証に使用されます。Cisco SD-WAN Manager を使用して署名付き証明書の内容を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから **[Configuration]** > **[Certificates]** の順に選択します。
2. [Controllers] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

3. 目的のデバイスの [...] をクリックし、[View Certificate] を選択して、インストールされている証明書を表示します。

証明書の失効

表 *1:* 機能の履歴

機能名	リリース情報	機能説明
証明書の失効	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco SD-WAN リリース 20.7.1 Cisco vManage リリース 20.7.1	この機能は、Cisco SD-WAN Manager がルート認証局から取得した証明書失効リストに基づいて、デバイスからエンタープライズ証明書を失効させます。

証明書の失効に関する情報

Cisco Catalyst SD-WAN でエンタープライズ証明書を使用している場合は、必要に応じて、Cisco SD-WAN Manager が指定された証明書をデバイスから取り消せるようにすることができます。たとえば、サイトでセキュリティの問題が発生した場合、証明書を取り消す必要がある場合があります。

（注） 証明書の失効機能は、デフォルトで無効になっています。

Cisco SD-WAN Manager は、Cisco SD-WAN Manager がルート認証局（CA）から取得した証明書失効リスト（CRL）に含まれている証明書を失効させます。

証明書失効機能を有効にして、CRL の URL を Cisco SD-WAN Manager に提供すると、Cisco SD-WAN Manager は設定された間隔でルート CA をポーリングし、CRL を取得して、CRL をオーバーレイネットワークの Cisco IOS XE Catalyst SD-WAN デバイス、Cisco vEdge デバイス、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ にプッシュします。CRL に含まれる証明書は、デバイスから取り消されます。

証明書が取り消されると、無効としてマークされます。デバイス制御接続は、次の制御接続フラップが発生するまで稼働し続け、その発生時点でデバイス制御接続はダウンします。デバイス制御接続を再び稼働させるには、デバイスに証明書を再インストールし、デバイスをオンボードします。

Cisco SD-WAN Manager がデバイスから証明書を取り消しても、デバイスがオーバーレイネットワークから削除されることはありませんが、オーバーレイネットワーク内の他のデバイスとは通信できなくなります。ピアデバイスは、証明書が CRL にあるデバイスからの接続試行を拒否します。

証明書の失効に関する制約事項

- デフォルトでは、証明書失効機能は無効になっています。証明書失効機能を初めて有効にするときは、ネットワークフラップ内のすべてのデバイスへの接続を制御します。サービスの中断を避けるために、最初はこの機能をメンテナンス時間中に有効にすることをお勧めします。

  証明書失効機能を無効にするときは、ネットワークフラップ内のすべてのデバイスへの接続を制御します。サービスの中断を避けるために、この機能をメンテナンス時間中に無効にすることをお勧めします。

- エンタープライズ CA を使用してハードウェア WAN エッジ証明書承認、コントローラ証明書承認、または WAN エッジクラウド証明書承認の証明書に署名している場合にのみ、証明書失効機能を使用できます。

- Cisco SD-WAN Manager は、VPN 0 インターフェイスを介してのみサーバーに接続して CRL を取得できます。

（注） Cisco vManage リリース 20.11.1 以降、VPN 512 を介した接続がサポートされます。

証明書の失効の設定

はじめる前に

ルート CA CRL の URL を書き留めます。

手順

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
2. [Administration Settings] ウィンドウで、[Certificate Revocation List] の横にある [Edit] をクリックします。

   証明書失効オプションが表示されます。
3. [Enabled] をクリックします。
4. [CRL Server URL] フィールドに、セキュアサーバーで作成した CRL の URL を入力します。
5. [Retrieval Interval] フィールドに、Cisco SD-WAN Manager がセキュアサーバーから CRL を取得し、CRL が指定する証明書を失効させる間隔を時間単位で入力します。

   1 ～ 24 の値を入力します。デフォルトの取得間隔は 1 時間です。
6. [Save] をクリックします。

   Cisco SD-WAN Manager はすぐに CRL を取得し、CRL が指定する証明書を取り消します。これ以降、Cisco SD-WAN Manager は指定した取得間隔の期間に従って CRL を取得します。

Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパーティ CA 証明書の設定

表 *2 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのサードパーティ CA 証明書の設定	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	Cisco SD-WAN Manager を使用すると、一般的なサードパーティ CA 証明書をトラストポイント名とともに Cisco IOS XE Catalyst SD-WAN デバイス にアップロードしてプッシュできます。プロビジョニングは設定グループパーセルを介して実行され、ステータスはモニタリングですぐに確認できます。

Cisco SD-WAN Manager を使用した CA 証明書の設定に関する情報

Cisco SD-WAN Manager は現在、Cisco Catalyst SD-WAN ファブリックとの統合中にデバイスへのサードパーティ証明書のアップロードを許可していますが、この機能は制御接続の確立と初期デバイスのセットアップ中にのみ使用できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、この機能により、UI を使用した証明書のアップロードが可能になります。Cisco SD-WAN Manager は、デバイスのセットアップ後でも CA 証明書のアップロードをサポートします。

CA 証明書はサーバー ID を認証し、不正アクセスを防止します。Cisco IOS XE Catalyst SD-WAN デバイス は、CA 証明書を使用して、ネットワーク内のさまざまなサーバーとのセキュアな接続を確立および管理します。Cisco SD-WAN Manager に CA 証明書をアップロードすると、Cisco IOS XE Catalyst SD-WAN デバイス は設定グループパーセルからのこの証明書情報を使用して、ネットワーク全体のサーバーと確立する接続を検証および認証します。これにより、ネットワークトラフィックの全体的なセキュリティと整合性が向上します。

（注） CA 証明書は、ルータの信頼できるルートを使用した SSL ベースのアクセスには適していません。

CA 証明書のアップロードでサポートされるデバイス

Cisco IOS XE Catalyst SD-WAN デバイスについて

CA 証明書を設定するための前提条件

- CA 証明書をアップロードするには、Cisco SD-WAN Manager で Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリースを実行する必要があります。
- CA 証明書をアップロードするには、Cisco IOS XE Catalyst SD-WAN デバイス で Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降のリリースを実行する必要があります。

CA 証明書のアップロードの制約事項

- PEM でエンコードされた証明書ファイルのみをサポートします。
- 証明書の最大ファイルサイズは 10 MB です。
- Cisco Catalyst SD-WAN マルチテナンシーを使用している場合、CA 証明書をアップロードして管理するには、テナントである必要があります。詳細については、「Tenant Role」を参照してください。

（注） プロバイダーとして Cisco SD-WAN Manager にログインすると、CA 証明書をアップロードして管理することはできません。

CA 証明書のアップロード

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** の順に選択します。
2. [CA Cert] タブをクリックします。
3. [Add CA Certificate] をクリックします。
4. [Add CA Certificate] ペインで、[Certificate Name] を入力します。
5. ファイルを選択するか、ドラッグアンドドロップして CA 証明書をアップロードします。
6. [Paste] タブをクリックし、証明書の詳細を貼り付けます。
7. [Save] をクリックします。

[Certificate Authority] ページで、[Device Group] テーブルにリストされている CA 証明書を見つけます。

（注） [Device Group] テーブルで CA 証明書の [Expiration Date] を見つけ、[...] をクリックしてさらに [Actions] を実行します。

CA 証明書の削除

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** の順に選択します。
2. [CA Cert] タブをクリックします。
3. [Device Group] テーブルで、削除する CA 証明書を選択します。
4. [Delete] をクリックします。

（注） CA 証明書を削除する別の方法：[Actions] 列の [...] アイコンをクリックし、[Delete] をクリックします。

Cisco SD-WAN Manager を使用した CA 証明書の設定

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] を選択します。

   設定グループの作成の詳細については、「Configuration Group Workflows」を参照してください。
2. 設定グループに機能を追加します。

   機能の追加の詳細については、「Feature Management」を参照してください。
3. [System Profile] で、[Add Feature] をクリックします。
4. [Add Feature] ペインで、[CA Certificate] を選択します。
5. [CA Certificates] セクションを設定します。

表 *3 : CA* 証明書

フィールド	説明
Type	ドロップダウンリストから [CA Certificates] を選択します。
[Name]	証明書の名前を入力します。

フィールド	説明
説明	（任意）証明書の説明を入力します。
Add CA Certificate	[Add CA Certificate] をクリックして、CA 証明書を追加します。
TrustPoint Name	トラストポイント名を入力します。
証明書名	ドロップダウンリストから CA 証明書を選択します。

6. [Save] をクリックします。
7. 設定グループに関連付けられているデバイスを展開します。詳細については、「Deploy Devices」を参照してください。

（注） [Device Group] テーブルから証明書を変更すると、変更はデバイスにミラーリングされません。これは、証明書とトラストポイントの関連付けによるものです。証明書を更新するには、証明書情報を含む既存のトラストポイントを削除する必要があります。その後、新しいトラストポイントを作成し、証明書を追加します。最後に、証明書を有効にするために変更をデバイスに展開します。

[Certificates] タブから証明書を削除しても、関連付けられているトラストポイントは自動的に削除されません。トラストポイントを削除するには、トラストポイントへの変更を手動で削除してから保存する必要があります。

CA 証明書の取り消し

CA 証明書を取り消すには、次の手順を使用します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. 目的のシステムプロファイルをクリックします。
4. CA 証明書の横にある [...] をクリックし、[Delete Feature] を選択します。
5. 変更をデバイスに展開します。

CA 証明書の更新

CA 証明書を更新するには、次の手順を使用します。

1. 更新する CA 証明書を Cisco SD-WAN Manager にアップロードします。
2. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
3. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
4. 目的のシステムプロファイルをクリックします。
5. CA 証明書の横にある […] をクリックし、[Delete Feature] を選択します。
6. [Configuration Groups] を使用して、設定グループに機能を追加し、「**CA 証明書の設定**」トピックのステップ 3 からステップ 7 の手順に従います。

CA 証明書と PKI トラストポイントの監視

CA 証明書の追跡

Cisco SD-WAN Manager に記載されている [Issuer Name]、[Certificate Serial No.] および [Expiration Date] を使用して CA 証明書を追跡します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Certificates]**の順に選択します。
2. [CA Cert] タブをクリックします。
3. Cisco SD-WAN Manager に追加された CA 証明書が [Device Group] テーブルに表示されます。

CA 証明書のインストールの監視

CA 証明書のインストールが完了すると、Cisco IOS XE Catalyst SD-WAN デバイス はイベントログを Cisco Catalyst SD-WAN Manager に送信します。

Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Logs]** > **[Events]**の順に選択します。

CA 証明書のインストールはイベントとしてリストされ、[Events] テーブルに表示されます。

PKI トラストポイントの監視

リアルタイムコマンド **`PKI Trustpoint`** を使用して、PKI トラストポイントを監視します。詳細については、「View PKI Trustpoint information」を参照してください。

CRLベースの検疫

表 *4:* 機能の履歴

機能名	リリース情報	機能説明
CRLベースの検疫	Cisco vManage リリース 20.11.1	この機能を使用すると、認証局から Cisco SD-WAN Manager が取得した証明書失効リストに基づいて SD-WAN エッジデバイスを検疫できます。

CRL ベースの検疫に関する情報

Cisco Catalyst SD-WAN でエンタープライズ証明書を使用すると、Cisco SD-WAN Manager を使用して、侵害され、証明書が取り消された SD-WAN エッジデバイスを検疫できます。

（注） 証明書失効リスト (CRL) ベースの検疫機能は、デフォルトで無効になっています。

- Cisco SD-WAN Manager は、証明書失効リスト（CRL）に含まれている証明書を失効させます。 Cisco SD-WAN Manager は、認証局（CA）からこのリストを取得します。
- Cisco SD-WAN Manager は、定義された間隔で、最新の CRL について CRL サーバーをポーリングします。リストを受信すると、Cisco SD-WAN Manager はそれを分析して、隔離する SD-WAN エッジデバイスを決定します。
- Cisco SD-WAN Manager は、ネットワーク内の有効な各 SD-WAN エッジデバイスの証明書のシリアル番号が CRL 内の証明書のシリアル番号と一致するかどうかを確認します。一致が見つかった場合、SD-WAN エッジデバイス上の証明書は削除されないため、SD-WAN エッジデバイスは Cisco SD-WAN Manager への制御接続を保持できます。

SD-WAN エッジデバイスの検疫プロセスは次のとおりです。

- 検疫された各 SD-WAN エッジデバイスについて：
  - Cisco SD-WAN Manager は SD-WAN エッジデバイスをステージングモードに移行します。ステージングモードでは、Cisco SD-WAN Manager への制御接続を維持しながらデータトラフィックをシャットダウンします。
  - Cisco SD-WAN Manager は隔離されている SD-WAN エッジデバイスの通知を生成します。

隔離されたそれぞれの Cisco SD-WAN コントローラ について、Cisco SD-WAN Manager はコントローラへの通知を生成します。

（注） CRL サーバーは、VPN 0 または VPN 512 を介して Cisco SD-WAN Manager に接続します。

CRL ベースの検疫の制限

- CRL ベースの検疫機能を使用できるのは、ハードウェア WAN エッジ証明書承認、コントローラ証明書承認、または WAN エッジ クラウド証明書承認の証明書に署名するエンタープライズ CA（認証局）がある場合のみです。
- CRL を無効にして、証明書の失効から検疫、または検疫から証明書の失効に切り替えます。証明書の失効と CRL ベースの検疫オプションを同時に有効にすることはできません。

CRLベースの検疫の構成

はじめる前に

- Cisco SD-WAN Manager のメニューから**[Administration]** > **[Settings]** の順に選択します。次のいずれかのオプションをクリックし、エンタープライズモードを選択して CRL（証明書失効リスト）を有効にします。
  - [Controller Certificate Authorization] フィールドで、[Enterprise Root Certificate] または
  - [Hardware WAN Edge Certificate Authorization] フィールドで、[Enterprise Certificate (signed by Enterprise CA)] または
  - [WAN Edge Cloud Certificate Authorization] フィールドで、[Manual (Enterprise CA - 推奨)] を選択します。
- CA CRL の URL をメモします。

（注） デフォルトでは、CRL ベースの検疫機能は無効になっています。

CRL ベースの検疫を構成するには：

1. Cisco SD-WAN Manager のメニューから**[Administration]** > **[Settings]** の順に選択します。
2. [Administration Settings] ページで、[Certificate Revocation List] の横にある [Edit] をクリックします。

   [Certificate Revocation] オプションと [CRL-Based Quarantine] オプションが表示されます。
3. [CRL-Based Quarantine] をクリックします。
4. [CRL Server URL] フィールドに、セキュアサーバーで作成した CRL の URL を入力します。

5. [Retrieval Interval] フィールドに、間隔を時間単位で入力します。Cisco SD-WAN Manager は証明書失効リスト（CRL）を使用して、SD-WAN エッジデバイスを検疫します。

   1 ～ 24 の値を入力します。デフォルトの取得間隔は 24 時間です。

6. [VPN 0] または [VPN 512] をクリックします。Cisco SD-WAN Manager ではサーバーに接続し、VPN 0 または VPN 512 インターフェイスを介して CRL を取得します。

7. [Save] をクリックします。

   Cisco SD-WAN Manager は定期的に CRL サーバーをポーリングして最新の CRL を取得します。このリストを分析して、隔離する SD-WAN エッジデバイスを決定します。

（注） 以前のリリースで CRL が無効になっている場合、Cisco vManage リリース 20.11.1 にアップグレードした後も CRL は無効のままです。Cisco vManage リリース 20.11.1 より前のリリースで CRL が有効になっていた場合、Cisco vManage リリース 20.11.1 にアップグレードした後、VPN0 をデフォルトとして証明書失効オプションが有効になります。

Cisco Catalyst SD-WAN Manager でのルート認証局証明書の管理

機能名	リリース情報	説明
Cisco SD-WAN Manager でのルート CA 証明書の管理のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco SD-WAN リリース 20.4.1 Cisco vManage リリース 20.4.1	この機能により、ルート認証局（CA）証明書を追加および管理できます。

ルート証明機関証明書の追加

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. [Modify Root CA] をクリックします。
3. [Root Certificate] フィールドに証明書のテキストを貼り付けるか、[Select a File] をクリックしてファイルから証明書をロードします。
4. [Add]をクリックします。証明書テーブルで新しい証明書が表示されます。[Recent Status] 列は、証明書がまだインストールされていないことを示しています。
5. [Next] をクリックして、インストールされていない証明書の詳細を確認します。

6. [Save] をクリックして証明書をインストールします。証明書テーブルで新しい証明書が表示されます。

ルート認証局証明書の表示

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. （オプション）[検索] フィールドにテキストを入力して、証明書ビューをフィルタ処理します。証明書のテキストまたは属性値（シリアル番号など）でフィルタ処理できます。
3. 証明書のテーブルで、[More Actions (…)] をクリックし、[View] を選択します。ポップアップウィンドウが開き、証明書と詳細が表示されます。

ルート証明書の削除

この手順を使用して、ルート認証局（CA）証明書を削除します。

1. Cisco SD-WAN Manager で、[Administration] > [Root CA Management] を選択します。
2. [Modify Root CA] をクリックします。
3. テーブルにあるルート証明書を 1 つ以上選択し、[Action] 列のごみ箱アイコンをクリックします。削除対象としてマークされた証明書がテーブルに表示されます。
4. [Next] をクリックして、削除対象としてマークされている証明書の詳細を確認します。
5. [Save] をクリックして証明書を削除します。

エンタープライズ証明書

Cisco IOS XE SD-WAN リリース 16.11.1 および Cisco SD-WAN リリース 19.1 でエンタープライズ証明書が導入されました。エンタープライズ証明書は、以前に使用されていたコントローラ証明書の承認に置き換わるものです。

（注） Cisco SD-WAN コントローラにエンタープライズ証明書を使用する場合は、少なくとも 2048 ビットの RSA キーでルート証明書を使用してください。

（注） 証明書管理の目的では、「コントローラ」という用語は、Cisco SD-WAN Manager、Cisco Catalyst SD-WAN コントローラ、および Cisco Catalyst SD-WAN Validator をまとめて指すために使用されます。

（注） エンタープライズ証明書に関するさらなる詳細については、『Cisco Catalyst SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide』を参照してください。

[Certificates] ページを使用して、証明書を管理し、オーバーレイネットワーク内の WAN エッジデバイスおよびコントローラデバイスを認証します。

Cisco Catalyst SD-WAN ソリューションの 2 つのコンポーネントで、デバイス認証が実行されます。

- 署名付き証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証されたデバイスは、相互にセキュアなセッションを確立できます。これらの証明書を生成し、それらをコントローラデバイス（Cisco SD-WAN Manager、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ）にインストールするのは Cisco SD-WAN Manager からです。
- WAN Edge 認定シリアル番号ファイルには、ネットワーク内のすべての有効な vEdge ルータと WAN ルータのシリアル番号が含まれています。Cisco Catalyst SD-WAN からこのファイルを受信し、各ルータを有効または無効としてマークし、Cisco SD-WAN Manager からネットワーク内のコントローラデバイスにファイルを送信します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにするには、証明書と WAN Edge 認定シリアル番号ファイルをコントローラデバイスにインストールします。インストールすると、オーバーレイネットワークが動作可能になります。

Cisco SD-WAN コントローラ のエンタープライズ証明書の設定

機能名	リリース情報	説明
セカンダリ組織単位のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r Cisco SD-WAN リリース 20.1.1	このオプション機能を使用すると、証明書を設定するときにセカンダリ組織単位を設定できます。指定した場合、この設定はすべてのコントローラとエッジデバイスに適用されます。
サブジェクト代替名（SAN）のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco SD-WAN リリース 20.4.1 Cisco vManage リリース 20.4.1	この機能により、サブジェクト代替名（SAN）DNS 名または Uniform Resource Identifier（URI）を設定でき、複数のホスト名と URI で同じ SSL 証明書を使用できるようになります。

機能名	リリース情報	説明
WAN エッジ クラウド デバイス エンタープライズ証明書の全組織の指定に関するサポート	Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1	WAN エッジ クラウド デバイスでエンタープライズ証明書のコントローラ証明書認証を構成する場合、[Organization] フィールドで任意の組織を指定できます。[Viptela LLC]、[vIPtela Inc]、[Cisco Systems] などの名前に限定されません。これにより、組織の認証局名またはサードパーティの認証局名を使用できます。
組織単位フィールドのない証明書のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.1	デバイスにインストールするエンタープライズ証明書では、組織単位（OU）フィールドを定義する必要はありません。以前は、このフィールドはデバイスの認証の一部として使用されていました。

エンタープライズ証明書に関する情報

エンタープライズ証明書を使用すると、組織は、公的証明書署名機関に依存することなく、独自のプライベート証明書署名機関を使用できます。[Set CSR Properties] フィールドを使用して、カスタム証明書プロパティを適用することもできます。

（注） 16.11/19.1 リリースでは、エンタープライズ証明書が導入されました。エンタープライズ証明書は、以前に使用されていたコントローラ証明書の承認に置き換わるものです。独立した組織がエンタープライズ証明書の署名を実施します。

[Configuration] > **[Certificates]**ページを使用して、証明書を管理し、オーバーレイネットワーク内の WAN エッジデバイスおよびコントローラデバイスを認証します。

Cisco Catalyst SD-WAN ソリューションの 2 つのコンポーネントで、デバイス認証が実行されます。

- 署名付き証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証されたデバイスは、相互にセキュアなセッションを確立できます。これらの証明書を生成し、それらをコントローラデバイス（Cisco SD-WAN Manager インスタンス、Cisco SD-WAN Validator、および Cisco SD-WAN コントローラ）にインストールするのは Cisco SD-WAN Manager からです。

- WANエッジ認証シリアル番号ファイルには、ネットワーク内のすべての有効なvEdgeルータとWANルータのシリアル番号が含まれています。Ciscoプラグアンドプレイ（PnP）からこのファイルを受信し、各ルータを有効または無効としてマークし、Cisco SD-WAN Managerからネットワーク内のコントローラデバイスにファイルを送信します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにするには、証明書とWAN Edge認定シリアル番号ファイルをコントローラデバイスにインストールする必要があります。インストールすると、オーバーレイネットワークが動作可能になります。

（注） 証明書管理の目的で、コントローラという用語は、Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、およびCisco SD-WAN Validatorをまとめて指します。

WAN エッジデバイスをリセットしたら、エンタープライズルート証明書を手動でデバイスにインストールする必要があります。アップグレードを実行しても、証明書は保持されます。

（注） Cisco SD-WAN Manager は、Base 64 でエンコードされた証明書のみをサポートします。エンコードされた他の形式（DER など）はサポートされていません。

たとえば、PEM 拡張機能は、**--BEGIN...** 行のプレフィックスが付いた ASCII（Base64）装甲データを含むさまざまなタイプの X.509v3 ファイルに使用されます。

エンタープライズ証明書の OU フィールドへの依存関係

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.1 以降、デバイスのオンボーディング時に、Cisco Catalyst SD-WAN では、関連付けられたエンタープライズ証明書に OU フィールドが定義されている必要はありません。ただし、少なくとも 1 つの OU フィールドが定義されている場合、Cisco Catalyst SD-WAN では、OU フィールドの 1 つがファブリックの組織名と一致する必要があります。

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.12.2 から、デバイスのオンボーディング時に、関連付けられたエンタープライズ証明書に 1 つ以上の OU フィールドが定義されている場合、OU フィールドはファブリックの組織名と一致する必要はありません。

エンタープライズ証明書をサポートするデバイス

デバイス	エンタープライズ証明書サポート
Cisco SD-WAN Manager	対応
Cisco SD-WAN Validator	対応
Cisco SD-WAN コントローラ	対応

デバイス	エンタープライズ証明書サポート
エッジルータ	すべてのハードウェア WAN エッジルータ ASR1002-X、ISRv、CSR1000v を除く vEdge/IOS-XE-SD-WAN

エンタープライズ証明書の設定

1. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]** > **[Hardware WAN Edge Certificate Authorization]** の順に選択します。
2. [Enterprise Certificate]（エンタープライズ CA によって署名済み）をクリックします。

   [On Box Certificate (TPM/SUDI Certificate)] はデフォルトのオプションです。
3. カスタム証明書プロパティを指定する場合は、[Set CSR Properties] をクリックします。次のプロパティが表示されます。
   - [Domain Name]：ネットワークドメイン名
   - **Organizational Unit**

（注） [Organizational Unit] フィールドは編集できません。組織単位は、Cisco SD-WAN Manager で使用されている組織名と同じである必要があります。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.3a、または Cisco IOS XE Release 17.9.x 以降、あるいは Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降を使用するデバイスの場合、デバイスにインストールする証明書では、組織単位フィールドを定義する必要はありません。ただし、署名付き証明書に組織単位フィールドが含まれている場合、フィールドはデバイスで構成されている組織名と一致する必要があります。これは、2022 年 9 月の時点で、認証局ブラウザフォーラム (CA/ブラウザフォーラム) のポリシーに対応し、署名付き証明書に組織単位を含めることを停止します。CA/ブラウザフォーラムのポリシーが変更されたにもかかわらず、一部の認証局では、署名付き証明書に組織単位が含まれている場合があります。

   - [Secondary Organization Unit]：このオプションのフィールドは、Cisco IOS XE SD-WAN リリース 17.2 または Cisco SD-WAN リリース 20.1.x 以降でのみ使用できます。このオプションのフィールドを指定すると、すべてのコントローラとエッジデバイスに適用されることに注意してください。

（注） 署名付き証明書に [Organizational Unit] フィールドまたは [Secondary Organizational Unit] フィールドが含まれている場合、これらのフィールドのいずれかが、デバイスに設定されている組織名と一致する必要があります。これは、2022 年 9 月の時点で、認証局ブラウザフォーラム (CA/ブラウザフォーラム) のポリシーに対応し、署名付き証明書に組織単位を含めることを停止します。CA/ブラウザフォーラムのポリシーが変更されたにもかかわらず、一部の認証局では、署名付き証明書に組織単位が含まれている場合があります。

- [Organization]
- **市区町村郡（City）**
- [State]
- **電子メール**
- **2 文字の国コード**
- [Subject Altenative Name (SAN) DNS Names]：（オプション）同じ SSL 証明書を使用するように複数のホスト名を設定できます。例：cisco.com および cisco2.com
- [Subject Altenative Name (SAN) URIs]：（オプション）複数の Uniform Resource Identifier（URI）を設定して、同じ SSL 証明書を使用できます。例：cisco.com および support.cisco.com

4. [Select a file] を選択して、ルート認証局ファイルをアップロードします。

   アップロードされたルート認証局がテキストボックスに表示されます。

5. [Save] をクリックします。
6. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]**の順に選択します。
7. [Upload WAN Edge List] タブを選択します。
8. Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス リストの場所を参照し、[Upload] をクリックします。
9. **[Configuration]** > **[Certificates]**ページで [...] をクリックし、アクションを選択します。
   - [View Enterprise CSR]（証明書署名要求）：CSR をコピーし、エンタープライズルート証明書を使用して署名し、証明書のインストール操作を使用して Cisco SD-WAN Manager に署名済み証明書をアップロードします。Cisco SD-WAN Manager は、証明書をインストールする必要があるハードウェアエッジを自動的に検出します。
   - [View Enterprise Certificate]：証明書をインストールすると、インストールされた証明書を表示してダウンロードできます。

- [Renew Enterprise CSR]：ハードウェアデバイスに新しい証明書をインストールする必要がある場合は、[Renew Enterprise CSR] オプションを使用できます。[Renew Enterprise CSR] オプションは CSR を生成します。次に、証明書を表示し（[View Enterprise CSR] オプション)、証明書をインストールします（[Install Certificate] オプション）。この手順により、制御接続が新しいシリアル番号としてフラップされます。新しいシリアル番号と有効期限のデータは、[Configuration] > [Certificates] ページで確認できます。

（注） Cisco Catalyst SD-WAN オーバーレイ内のデバイスにインストールする証明書では、組織単位フィールドを定義する必要はありません。ただし、署名付き証明書に組織単位フィールドが含まれている場合、フィールドはデバイスで構成されている組織名と一致する必要があります。

- [Revoke Enterprise Certificate]：このオプションは、デバイスからエンタープライズ証明書を削除し、プレステージングに戻します。デバイスでは、Cisco SD-WAN Validator と Cisco SD-WAN Manager のコントロールのみが動作しています。

Cisco IOS XE Catalyst SD-WAN デバイス の場合は、[...] をクリックしてアクションを選択します。

- [View Feature CSR]：
  - Cisco IOS XE Catalyst SD-WAN デバイス から入手可能な CSR をコピーします。
  - 証明機関からのエンタープライズルート証明書を使用して証明書に署名します。
  - [Install Feature Certificate] 操作を使用して、署名付き証明書を Cisco SD-WAN Manager にアップロードします。

    Cisco SD-WAN Manager は、証明書をインストールする必要があるハードウェアエッジを自動的に検出します。機能証明書をインストールすると、[View Feature Certificate] オプションが使用可能になります。

- [View Feature Certificate]：機能証明書をインストールすると、機能証明書を表示してダウンロードできます。
- [Revoke Feature Certificate]：このオプションは、機能証明書またはトラストポイント情報を Cisco IOS XE Catalyst SD-WAN デバイス から削除します。証明書を取り消すと、デバイスに対するすべてのアクションが使用できなくなります。デバイスのすべてのアクションを表示するには、デバイスのログ情報を、認証タイプをサーバーとして Transport Layer Security（TLS）プロファイルに設定してから、相互に設定し直します。また、アクションを表示するには、Cisco IOS XE Catalyst SD-WAN デバイス を工場出荷時のデフォルト設定にリセットします。

  デバイスを工場出荷時のデフォルトにリセットするには、次の手順を実行します。

- Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
- 工場出荷時のデフォルトテンプレートを使用してデバイステンプレートを作成します。

  工場出荷時のデフォルトテンプレートは、Factory_Default_ feature-name _Template です。機能テンプレートを使用してデバイステンプレートを作成する方法については、Create a Device Template from Feature Templates [英語] を参照してください。

10. [Install Certificate] または [Install Feature Certificate] をクリックして、署名付き証明書をアップロードします。

    証明書は、署名付き証明書である必要があります。最初の状態は「CSR Generated」です。

    正常にインストールされると、状態が「Certificate Installed」に変わります。

11. Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Certificates]**の順に選択します。デバイスタイプ、シャーシID、エンタープライズシリアル番号、エンタープライズ証明書の日付など、エンタープライズ証明書の列を確認できます。

デバイス証明書の無効化

WAN エッジデバイスを削除する前に、デバイスを無効にします。

1. Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. デバイスが表示されている行で、[Invalid] をクリックしてデバイスを無効にします。

エンタープライズルート証明書のコントローラ証明書の承認

1. Cisco SD-WAN Manager のメニューから**[Administration]** > **[Settings]** の順に選択します。
2. [Controller Certificate Authorization] 領域で、[Edit] をクリックします。
3. [Enterprise Root Certificate] をクリックします。警告が表示されたら、[Proceed] をクリックして続行します。
4. 必要に応じて、[Set CSR Properties] をクリックして、証明書署名要求（CSR）の詳細を手動で構成します。

（注） マルチテナントシナリオで、CSR プロパティを手動で構成し、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.11.1 以降を使用している場合は、ネットワーク内のデバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降を使用していることを確認してください。シングルテナントのシナリオでは、これは必要ありません。

マルチテナントシナリオで、CSR プロパティを手動で構成する場合、テナントデバイスの CSR を生成する準備ができたら、以下で説明する [Secondary Organizational Unit] フィールドにテナントの組織名を入力します。マルチテナントシナリオで、サービス プロバイダー デバイスの CSR を生成する場合、これは必要ありません。

次のプロパティが表示されます。

- [Domain Name]：ネットワークドメイン名
- **Organizational Unit**

（注） [Organizational Unit] フィールドは編集できません。このフィールドには、**[Administration]** > **[Settings]** > **[Organization Name]** の Cisco SD-WAN Manager に対して構成した組織名が自動的に入力されます。

- [Secondary Organizational Unit]：このオプションのフィールドは Cisco IOS XE SD-WAN リリース 17.2 または Cisco SD-WAN リリース 20.1.x 以降でのみ使用できます。このオプションのフィールドを指定すると、すべてのコントローラとエッジデバイスに適用されることに注意してください。
- [Organization]：Cisco vManage リリース 20.11.1 以降では、WAN エッジクラウドデバイスでエンタープライズ証明書のコントローラ証明書認証を構成するときに、このフィールドで任意の組織を指定できます。[Viptela LLC]、[vIPtela Inc]、[Cisco Systems] などの名前に限定されません。これにより、組織の認証局名またはサードパーティの認証局名を使用できます。最大長は 64 文字で、スペースと特殊文字を含めることができます。名前を入力すると、Cisco SD-WAN Manager により、名前が検証されます。
- **市区町村郡（City）**
- [State]
- **電子メール**
- **2 文字の国コード**
- [Subject Altenative Name (SAN) DNS Names]：（オプション）同じ SSL 証明書を使用するように複数のホスト名を設定できます。例：cisco.com および cisco2.com
- [Subject Altenative Name (SAN) URIs]：（オプション）複数の Uniform Resource Identifier（URI）を設定して、同じ SSL 証明書を使用できます。例：cisco.com および support.cisco.com

5. SSL 証明書を [Certificate] フィールドに貼り付けるか、[Select a file] をクリックして SSL 証明書ファイルに移動します。
6. （任意）[Subject Alternative Name (SAN) DNS Names] フィールドに複数のホスト名を入力して同じ SSL 証明書を使用することができます。

   たとえば、cisco.com と cisco2.com を入力します。
7. （任意）[Subject Alternative Name (SAN) URIs] フィールドに複数の URI を入力して同じ SSL 証明書を使用することができます。

   たとえば、cisco.com と support.cisco.com を入力します。

   これは、組織の異なる部分に異なるサブドメインを使用せず、ホスト名に単一の証明書を使用する組織に役立ちます。

ブートストラップ構成の生成

オンサイト ブートストラップ プロセスには、ブート可能な USB ドライブまたは内部ブートフラッシュから SD-WAN をサポートするデバイスにロードするブートストラップ構成ファイルの生成が含まれます。デバイスは起動すると、構成ファイルの情報を使用してネットワークに接続します。

（注） ブートストラップ構成を生成する必要がある場合は、**[Configuration]** > **[Devices]**ページを使用して […] をクリックし、[Generate Bootstrap Configuration] を選択します。

（注） Cisco vManage リリース 20.7.1 以降、Cisco vEdge デバイス のブートストラップ構成ファイルを生成するときに使用できるオプションがあり、2 つの異なる形式のブートストラップ構成ファイルを生成できます。

- Cisco Catalyst SD-WAN リリース 20.4.x 以前を使用している Cisco vEdge デバイス のブートストラップ構成ファイルを生成している場合は、[The version of this device is 20.4.x or earlier] チェックボックスをオンにします。
- Cisco SD-WAN リリース 20.5.1 以降を使用している Cisco vEdge デバイス のブートストラップ構成を生成する場合は、チェックボックスを使用しないでください。

Cisco PKI コントローラの証明書

ソフトウェアリリース 19.x 以降では、Cisco Catalyst SD-WAN コントローラ証明書の Symantec/DigiCert の代わりに、Cisco を認証局（CA）として使用するオプションがあります。

このセクションでは、展開タイプ、および Cisco Public Key Infrastructure（PKI）を使用してコントローラ証明書を管理、インストール、およびトラブルシューティングするシナリオについて説明します。Cisco PKI を使用すると、IP セキュリティ（IPSec）、セキュアシェル（SSH）、セキュアソケットレイヤ（SSL）などのセキュリティプロトコルをサポートする証明書管理を実現できます。

Symantec/DigiCert 証明書と Cisco PKI 証明書の主な違いは、Cisco PKI 証明書がプラグアンドプレイ（PnP）のスマートアカウント（SA）およびバーチャルアカウント（VA）にリンクされており、DigiCert などのポータルを使用した手動の承認が不要な点です。各 VA には 100 の証明書の制限、つまり、各オーバーレイには 100 の証明書の制限があり、証明書署名要求（CSR）が生成された後、Cisco SD-WAN Manager 設定が正しく設定されていれば、承認とインストールが自動的に行われます。

デバイスが追加され、証明書が Cisco PKI サーバーから自動的にインストールされます。証明書を承認するための操作は不要です。

Cisco PKI 証明書のサポート対象デバイス

Cisco PKI 証明書を使用するためにサポートされているデバイスは次のとおりです。

デバイス	サポート
Cisco SD-WAN Manager	対応
Cisco Catalyst SD-WAN Validator	対応
Cisco Catalyst SD-WAN コントローラ	対応
Cisco vEdge デバイスについて	対応
Cisco IOS XE Catalyst SD-WAN デバイスについて	対応

Cisco PKI コントローラ証明書のユースケース

- 使用例：ソフトウェアバージョン 19.x 以降によるシスコがホストするクラウドのオーバーレイ （32 ページ）
- ユースケース：証明書更新時の DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行 （34 ページ）
- 使用例：オンプレミスコントローラでの CSR の送信と証明書のダウンロード （37 ページ）

使用例：ソフトウェアバージョン19.x以降によるシスコがホストするクラウドのオーバーレイ

前提条件

Cisco SD-WAN Manager およびコントローラはすべて同じソフトウェアバージョンを実行している必要があります。

[Configuration] > **[Devices]** > **[Controllers]**ページで、すべてのコントローラの OOB IP アドレスとログイン情報が更新されていることを確認します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

SSH を使用した制御接続を設定せずに、新規または期限切れのオーバーレイのソフトウェアバージョンを確認できます。

1. 各コントローラに SSH で接続すると、SSH プロセス中にバージョンが表示されます。
2. 実際にログイン情報を機能させる必要がないため、ログイン情報が機能しないコントローラでこの操作を実行できます。

   オーバーレイ内のすべてのコントローラに対してこのプロセスを繰り返して確認します。
3. 次のいずれかの方法を使用して、お客様のスマートアカウントのログイン情報を準備する必要があります。
   1. PnP トリガー通知からお客様の連絡先に個別に電子メールを送信し、スマートアカウントのログイン情報を提供するように依頼します。

      または
   2. お客様の連絡先に電子メールを送信し、お客様自身で Cisco SD-WAN Manager にログオンして自身を追加するように依頼します。また、お客様の IP を許可リストに追加するように依頼します。

      お客様にお客様の連絡先のログイン情報の入力を求める場合は、お客様が Cisco SD-WAN Manager GUI にアクセスしてログオンし、スマートアカウントのログイン情報を入力できるように、IP を許可リストに追加するようにお客様に求めてから、この手順を実行するようにしてください。

      スマートアカウントのログイン情報を表示するには、Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]** > **[Smart Account Credentials]**の順に選択します。

      ユーザ名およびパスワードを入力し、[Save] をクリックします。

Cisco PKI 証明書を要求してインストールするための Runbook

1. 前提条件を満たしていること、およびスマートアカウントのログイン情報を追加したことを確認します。
2. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]** > **[Controller Certificate Authorization]**の順に選択し、[Edit] をクリックします。
3. [Cisco (Recommended)] をクリックします。

（注） スマートアカウントのログイン情報が追加されていない場合、Cisco SD-WAN Manager にエラーが表示されます。前提条件を確認します。

4. ドロップダウンで、有効期間を POC の場合は 1 年、生産オーバーレイの場合は 2 年に設定します。
5. [Certificate Retrieve Interval] を 1 分に設定し、[Save] を押します。

（注） CSR リクエストが完了するとすぐに証明書が自動承認されるため、現在、承認についてお客様に通知するための電子メールフィールドはありません。

6. このステップ以降のプロセスは、Cisco SD-WAN Manager GUI の Symantec/DigiCert コントローラの場合と同じです。

   Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]**の順に選択し、[Controllers] をクリックします。[…] をクリックし、[Generate CSR] を選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

   操作ステータスには、署名のために送信された CSR、人手による処理を必要とせずに自動的に署名およびインストールされた証明書が表示されます。

7. 証明書は自動的にインストールされます。成功すると、**[Configuration]** > **[Certificates]** > **[Controllers]**ページに次の内容が表示されます。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

   - 各コントローラの証明書の期限日

- [Operation Status] 列：
  - Cisco SD-WAN Validator：[Installed]
  - Cisco SD-WAN Manager および Cisco Catalyst SD-WAN コントローラ："Cisco SD-WAN Validator Updated"
- [Certificate Serial] 列：証明書のシリアル番号

8. 制御接続が起動し、Cisco SD-WAN Manager ダッシュボードのコントローラに接続されていることを確認します。

ユースケース：証明書更新時の DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行

前提条件

Cisco SD-WAN Manager、コントローラ、および vEdge はすべて、制御接続が稼働している必要があります。

[Configuration] > **[Devices]** > **[Controllers]**で OOB IP アドレスとログイン情報が更新されていることを確認します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

コントローラごとに [...] をクリックして更新を確認します。

DigiCert 証明書から Cisco PKI コントローラ証明書へのアクティブな既存オーバーレイの移行

1. Cisco SD-WAN Manager で、コントローラおよび Cisco vEdge デバイス への制御接続が稼働していることを確認します。

   制御接続が稼働していない場合、DigiCert から Cisco PKI への移行は続行できません。

   制御接続が部分的にのみ稼働している場合、つまり、一部の Cisco vEdge デバイス の制御がダウンしている場合、証明書を Cisco PKI に移行した後に制御が確立されても、それらの Cisco vEdge デバイス はコントローラに自動的に再接続できません。

   証明書が期限切れで制御接続がダウンしている場合は、まず DigiCert で証明書を更新し、制御接続を起動してから Cisco PKI コントローラ証明書に移行する必要があります。

2. コントローラのソフトウェアバージョンが 19.x 以降であることを確認します。

   Cisco SD-WAN Manager を使用して、アクティブな既存オーバーレイのソフトウェアバージョンを確認する方法（コントローラへの有効な制御接続あり）

1. Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. [Manager] をクリックして、[Current Version] 列を確認します。バージョンが 19.x 以降であることを確認します。

   制御接続が稼働しており、Cisco SD-WAN Manager とコントローラのバージョンが 19.x 以降でない場合は、Cisco PKI への移行を実行する前に、まずそれらをアップグレードします（Cisco vEdge デバイス のアップグレードは不要）。

（注） 19.x にアップグレードしたコントローラでは、アップグレードの一環として Cisco PKI を使用して証明書をすぐに更新する必要があります。既存のシマンテック証明書が有効なままだとしても、それらの証明書を使用して実行することはできません。

3. 前提条件を確認したら、Cisco PKI ルート CA がすべてのコントローラと Cisco vEdge デバイスに伝播されていることを確認します。これには、コントローラへの SSH アクセスが必要です。
   1. Cisco SD-WAN Manager およびコントローラに SSH で接続し、**show certificate root-ca-cert | include Cisco** コマンドを実行します。

      出力が空白の場合、または結果が表示されない場合は、クラウドインフラ管理チームにエスカレーションします。

4. 次のいずれかの方法で、お客様のスマートアカウントのログイン情報を準備する必要があります。
   1. PnP トリガー通知からお客様の連絡先に個別に電子メールを送信し、スマートアカウントのログイン情報を提供するように依頼します。

      または

   2. お客様の連絡先に電子メールを送信し、お客様自身で Cisco SD-WAN Manager にログオンしてご自身を追加するように依頼します。また、お客様の IP を許可リストに追加するように依頼します。

      お客様に情報の入力を求める場合は、お客様が Cisco SD-WAN Manager GUI にアクセスしてログオンし、スマートアカウントのログイン情報を入力できるように、IP を許可リストに追加するようにお客様に求めてから、この手順を実行するようにしてください。

      スマートアカウントのログイン情報を表示するには、Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]**の順に選択し、[Smart Account Credentials] セクションを表示します。

   3. ユーザー名とパスワードを入力し、[Save] をクリックします。

      すべての前提条件が満たしたら、「**Cisco PKI 証明書を要求してインストールするための Runbook**」の手順に従って CSR を要求し、Cisco 証明書をインストールし

ます。コントローラと Cisco vEdge デバイスへのすべての制御接続が復旧したことを確認します。復旧していない場合は、クラウドインフラ管理チームにエスカレーションします。

Cisco PKI 証明書を要求してインストールするための Runbook

1. 前提条件を満たしていること、およびスマートアカウントのログイン情報を追加したことを確認します。
2. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]**の順に選択し、[Controller Certificate Authorization] セクションで [Edit] をクリックします。
3. [Cisco (Recommended)] をクリックします。

（注） スマートアカウントのログイン情報が追加されていない場合、Cisco SD-WAN Manager にエラーが表示されます。前提条件を確認します。

4. ドロップダウンで、有効期間を POC の場合は 1 年、生産オーバーレイの場合は 2 年に設定します。
5. [Certificate Retrieve Interval] を 1 分に設定し、[Save] を押します。

（注） CSR リクエストが完了するとすぐに証明書が自動承認されるため、現在、承認についてお客様に通知するための電子メールフィールドはありません。

6. このステップ以降のプロセスは、Cisco SD-WAN Manager GUI の Symantec/DigiCert コントローラの場合と同じです。

   Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]**の順に選択し、[Controllers] をクリックします。[…] をクリックし、[Generate CSR] を選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

   操作ステータスには、署名のために送信された CSR、ユーザーの操作を必要とせずに自動的に署名およびインストールされた証明書が表示されます。

7. 証明書は自動的にインストールされます。成功すると、**[Configuration]** > **[Certificates]** > **[Controllers]**ページに次の内容が表示されます。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

- 各コントローラの証明書の期限日
- [Operation Status] 列：
  - Cisco SD-WAN Validator：[Installed]
  - Cisco SD-WAN Manager および Cisco SD-WAN コントローラ："Cisco SD-WAN Validator Updated"
- [Certificate Serial] 列：証明書のシリアル番号

8. 制御接続が起動し、Cisco SD-WAN Manager ダッシュボードのコントローラに接続されていることを確認します。
9. [Certificate Retrieve Interval] を 1 分に設定します。
10. [Sync Root Certificate] をクリックして、Cisco SD-WAN Manager の Cisco vEdge デバイスまたは Cisco IOS XE Catalyst SD-WAN デバイス を Cisco PKI に移行します。このサポートは、19.2.1 バージョン以降から利用できます。
11. [Save] をクリックします。

使用例：オンプレミスコントローラでの CSR の送信と証明書のダウンロード

次の手順では、PnP および対象の SA/VA にアクセスできる必要があります。お客様は、独自の SA/VA にアクセスできます。

前提条件

証明書のインストールに手動の手法を使用することを除き、前提条件は上記の場合と同じです。

ランブック

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。[Controller Certificate Authorization] セクションで、[Manual] に設定されていることを確認します。
2. コントローラの CSR を生成します。

   Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]**の順に選択し、[Controllers] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

[…] をクリックし、[Generate CSR] を選択します。

各 CSR をファイル名の拡張子が `.csr` のファイルにダウンロードし、署名付き証明書を取得するためにそれを PnP ポータルに送信できるように準備します。

3. 必要な SA/VA の PnP ポータルにログオンし、[Certificates] タブを選択します。
4. [Generate Certificate] をクリックし、手順に従って証明書ファイルの名前を指定してから、CSR を貼り付けて、署名付き証明書をダウンロードします。

   これで、完成した証明書をダウンロードできます。CSR ごとにこのプロセスを繰り返して、必要なすべての証明書をダウンロードします。
5. ダウンロードした証明書をインストールするには、Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** の順に選択し、[Controllers] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

[Install Certificate] をクリックします。

インストール後、制御接続が稼働していることを確認します。

デバッグおよびログ情報

1. PnP の VA で Cisco Catalyst SD-WAN Validator プロファイルを調べて、正しい組織名が存在することを確認します。
2. 証明書プロセス全体のログについて、Cisco SD-WAN Manager で `/var/log/nms/vmanage-server.log` を確認します。
3. Cisco SD-WAN Manager に、Cisco PKI サーバーに到達するためのインターネット接続があることを確認します。

Cisco SD-WAN Manager の Web サーバー証明書

認証証明書を使用して Web ブラウザと Cisco SD-WAN Manager サーバー間のセキュアな接続を確立するには、CSR を生成して証明書を作成し、ルート CA による署名を得てから、インス

トールする必要があります。サーバーごとに次の手順を実行して、クラスタ内の各 Cisco SD-WAN Manager サーバーに個別の証明書をインストールする必要があります。

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
2. [Web Server Certificate] 領域で、[CSR] をクリックします。
3. [Common Name] フィールドに、Cisco SD-WAN Manager サーバードメイン名または IP アドレスを入力します。たとえば、Cisco SD-WAN Manager の完全修飾ドメイン名は vmanage.org.local になります。
4. [Organizational Unit] フィールドに、組織内の単位名を入力します（例：Network Engineering）。
5. [Organization] フィールドに、ルート CA によって指定された組織の正確な名前を入力します（例：Viptela Inc.）。
6. [City] フィールドに、組織がある都市の名前（例：川崎）を入力します。
7. [State] フィールドに、ユーザーの市がある都道府県を入力します（例：神奈川）。
8. [2-Letter Country Code] フィールドに、ユーザーの都道府県がある国の 2 文字のコードを入力します。たとえば、米国の 2 文字の国コードは US です。
9. [Validity] をクリックして、証明書の有効期間を選択します。
10. 必要に応じて、[Subject Alternative Name (SAN) DNS Names] フィールドに、証明書の信頼を拡張する必要がある DNS サーバーの名前を入力します。複数の DNS サーバー名を入力する場合は、各名前をスペースまたはコンマで区切ります。

（注） Cisco Catalyst SD-WAN は、Cisco IOS XE SD-WAN リリース 16.11 および Cisco SD-WAN リリース 19.1 以降の SAN DNS 名をサポートしています。

11. 必要に応じて、[Subject Alternative Name (SAN) URIs] フィールドに、証明書の信頼を拡張する必要があるリソースの URI を入力します。複数の URI を入力する場合は、各 URI をスペースまたはコンマで区切ります。

    各 URI を schema:value 形式で入力します。ここで、scheme はリソースにアクセスするためのプロトコルで、value はリソースです。例：**`https://example.example.com`** または **`scp://example.example.com`**。

（注） Cisco Catalyst SD-WAN は、Cisco IOS XE SD-WAN リリース 16.11 および Cisco SD-WAN リリース 19.1 以降の SAN URI をサポートしています。

12. [Generate（生成）] をクリックして CSR を生成します。
13. CSR を CA サーバーに送信して、署名してもらいます。

14. 署名付き証明書を受け取ったら、[Web Server Certificate] バーの近くにある [Certificate] をクリックして、新しい証明書をインストールします。[View] ボックスに、Cisco SD-WAN Manager サーバー上の現在の証明書が表示されます。
15. 新しい証明書をコピーしてボックスに貼り付けます。または、[Import and Select a File] をクリックして、新しい証明書ファイルをダウンロードします。
16. アプリケーションサーバーを再起動して、Cisco SD-WAN Manager にログインします。

Web サーバー証明書期限日の表示

認証証明書を使用して Web ブラウザと Cisco SD-WAN Manager サーバー間のセキュアな接続を確立する場合は、証明書の有効期間を設定します（前のセクションのステップ 8）。この期間が終了すると、証明書が期限切れになります。[Web Server Certificate] バーに、期限の日時が表示されます。

証明書の有効期限が切れる 60 日前から、証明書の有効期限が近づいていることを示す通知が Cisco SD-WAN Manager ダッシュボードに表示されます。この通知は、期限日の 30 日前、15 日前、および 7 日前に再表示され、その後は毎日表示されます。

リバースプロキシの有効化

表 *5:* 機能の履歴

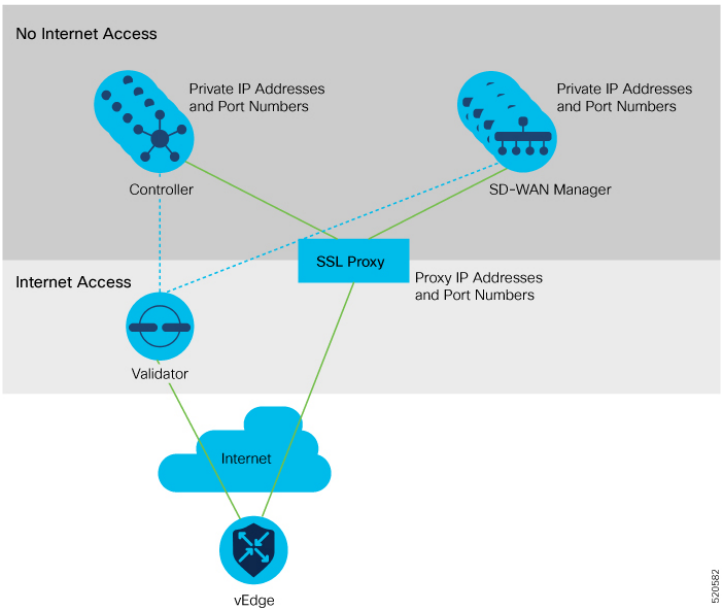
機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス および Cisco Catalyst SD-WAN マルチテナンシーを使用したリバースプロキシのサポート	Cisco IOS XE リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco SD-WAN Manager と Cisco SD-WAN コントローラ の間のオーバーレイネットワークにリバースプロキシを展開できます。また、この機能を使用すると、Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス を含むシングルテナント展開とマルチテナント展開の両方にリバースプロキシを展開できます。マルチテナント展開では、サービスプロバイダーがリバースプロキシおよび関連する設定を管理します。

標準のオーバーレイネットワークでは、Cisco Catalyst SD-WAN エッジデバイスが Cisco SD-WAN コントローラ（Cisco SD-WAN Manager および Cisco SD-WAN コントローラ）への直接接続を開始し、これらの接続を介してコントロールプレーン情報を交換します。WAN エッジデバイスは通常、ブランチサイトに配置され、インターネット経由で Cisco SD-WAN コントローラに接続します。その結果、Cisco SD-WAN Manager および Cisco SD-WAN コントローラもインターネットに直接接続されます。

セキュリティまたはその他の理由から、Cisco SD-WAN コントローラに直接インターネット接続をさせたくない場合があります。このようなシナリオでは、Cisco SD-WAN コントローラと

WAN エッジデバイスの間にリバースプロキシを展開できます。リバースプロキシは、Cisco SD-WAN コントローラと WAN エッジデバイスの間で制御トラフィックを渡す仲介役として機能します。WAN エッジデバイスは、Cisco SD-WAN Manager および Cisco SD-WAN コントローラと直接通信するのではなくリバースプロキシと通信し、リバースプロキシは Cisco SD-WAN Manager および Cisco SD-WAN コントローラとの間のトラフィックをリレーします。

次の図は、WAN エッジデバイスと Cisco SD-WAN Manager および Cisco SD-WAN コントローラの間に展開されたリバースプロキシを示しています。



Cisco Catalyst SD-WAN のシングルテナント展開とマルチテナント展開の両方でリバースプロキシを展開できます。TLOC は、パブリックまたはプライベート TLOC に関係なく、パブリック IP アドレスとポートでリバースプロキシと通信します。

リバースプロキシのサポートの有効化に関する制約事項

- マルチテナント Cisco Catalyst SD-WAN オーバーレイネットワークでは、3 ノード Cisco SD-WAN Manager クラスタのみでリバースプロキシデバイスを展開できます。
- リバースプロキシの展開は、Cisco SD-WAN Manager および Cisco SD-WAN コントローラの TLS ベースのコントロールプレーンでのみサポートされます。
- Cisco vEdge 5000 ルータではリバースプロキシを展開できません。
- IPv6 制御接続ではリバースプロキシを展開できません。

リバースプロキシでの証明書のプロビジョニング

トラフィックを交換する前に、リバースプロキシと WAN エッジデバイスの相互認証が必要です。

リバースプロキシでは、Cisco SD-WAN コントローラの証明書に署名した CA によって署名された証明書をプロビジョニングする必要があります。この証明書は、WAN エッジデバイスを検証するためにリバースプロキシによって使用されます。

リバースプロキシの証明書署名要求（CSR）を生成し、シスコが署名するようにするには、次の手順を実行します。

1. リバースプロキシで次のコマンドを実行します。

   ```
   proxy$ openssl req -new -days 365 -newkey rsa:2048 -nodes -keyout Proxy.key -out Proxy.csr
   ```

   プロンプトが表示されたら、次の表に示されている値を入力します。

プロパティ	説明
Country Name（2 文字コード）	任意の国コード。 例：US
州または都道府県	任意の州または都道府県。 例：CA
地域の名前	任意の地域。 例：San Jose
組織名	「vIPtela Inc」または「Viptela LLC」のいずれかを使用してください。 Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a から、エンタープライズ証明書の組織名として「Cisco Systems」文字列を使用できます。 例：Viptela LLC
組織単位の名前	オーバーレイで設定した「組織」の名前を使用します。 例：cisco-sdwan-12345
共通名	「.viptela.com」で終わるホスト名。 例：proxy.viptela.com
Email Address	任意の有効な電子メールアドレスを使用します。 例：someone@example.com

2. CSR がシスコによって署名されます。

   - Cisco SD-WAN コントローラの CA として Symantec/Digicert を使用する場合は、Cisco TAC で CSR の署名のためのケースを開きます。

- Cisco SD-WAN コントローラの CA として Cisco Public Key Infrastructure（PKI）を使用する場合は、Cisco ネットワーク プラグ アンド プレイ（PnP）アプリケーションで CSR を送信し、署名付き証明書を取得します。

リバースプロキシの有効化

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
2. [Reverse Proxy] 設定で、[Edit] をクリックします。
3. [Enable Reverse Proxy] で、[Enabled] をクリックします。
4. [Save] をクリックします。

Cisco SD-WAN コントローラでのリバースプロキシの設定

1. Cisco SD-WAN Manager のメニューから、**[Configure]** > **[Devices]** の順に選択します。
2. [Controllers] をクリックします。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

3. 目的の Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ で […] をクリックして、[Add Reverse Proxy] をクリックします。

   [Add Reverse Proxy] ダイアログボックスが表示されます。

4. プライベート IP アドレスとポート番号をプロキシ IP アドレスとポート番号にマッピングするには、次の手順を実行します。
   1. [Add Reverse Proxy] をクリックします。
   2. 次の詳細を入力します。

プライベート IP	プライベート IP アドレスは、VPN 0 のトランスポート インターフェイスの IP アドレスです。
プライベート ポート	これは、オーバーレイネットワークでトラフィックの制御と処理を行う接続を確立するために使用されるポートです。デフォルト ポート番号は、12346 です。
プロキシ IP	プライベート IP アドレスをマップする必要があるプロキシ IP アドレス。
プロキシポート	プライベートポートをマップする必要があるプロキシポート。

3. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ に複数のコアがある場合は、コアごとに手順 4a と手順 4b を繰り返します。

5. プライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除するには、マッピングを探してごみ箱アイコンをクリックします。
6. リバースプロキシ設定を保存するには、[Add] をクリックします。

   設定を破棄するには、[Cancel] をクリックします。
7. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ にアタッチされたセキュリティ機能テンプレートで、トランスポートプロトコルとして TLS を選択します。

Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ でリバースプロキシを設定すると、オーバーレイネットワーク内の WAN エッジデバイスは、リバースプロキシでの認証用の証明書を使用してプロビジョニングされます。

1. リバースプロキシが展開されると、Cisco Catalyst SD-WAN Validator はリバースプロキシの詳細を WAN エッジデバイスと共有します。
2. リバースプロキシについて学習した WAN エッジデバイスは、Cisco SD-WAN Manager から署名付き証明書のインストールを開始します。
3. 証明書がインストールされると、WAN エッジデバイスはその証明書を使用してリバースプロキシを認証し、リバースプロキシに接続します。

リバースプロキシの無効化

（注） リバースプロキシを無効にする前に、Cisco SD-WAN Manager インスタンスおよび Cisco SD-WAN コントローラ に対して設定したプライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除します。マッピングの削除については、「Configure Reverse Proxy Settings on Cisco Catalyst SD-WAN Controllers」を参照してください。

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
2. [Reverse Proxy] 設定で、[Edit] をクリックします。
3. [Enable Reverse Proxy] で、[Disabled] をクリックします。
4. [Save] をクリックします。

Cisco SD-WAN コントローラおよび WAN エッジデバイスのプライベートおよびプロキシ IP アドレスの監視

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. Cisco SD-WAN Manager インスタンス、Cisco SD-WAN コントローラ、または WAN エッジデバイスのホスト名をクリックします。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストから、[Control Connections] を選択します。

   表示されるテーブルの [Private IP] 列と [Private Port] 列のエントリが、VPN 0 のトランスポート インターフェイスのプライベート IP アドレスとポート番号となります。[Public IP] および [Public Port] 列のエントリは、プロキシ IP アドレスとポート番号です。

CLI を使用したリバースプロキシの監視

例：Cisco SD-WAN コントローラで WAN エッジデバイスのプライベートおよびプロキシ IP アドレスとポート番号を監視する

次に、Cisco SD-WAN コントローラ での **show control connections** コマンドの出力例を示します。WAN エッジデバイスの場合、コマンド出力の [PEER PRIVATE IP] および [PEER PRIV PORT] 列のエントリは、設定された TLOC IP アドレスと WAN エッジインターフェイスのポート番号です。[PEER PUBLIC IP] および [PEER PUB PORT] 列のエントリは、リバース プロキシ インターフェイスの対応する IP アドレスとポート番号です。同じコマンドを Cisco SD-WAN Manager インスタンスで実行した場合も、同様の出力が得られます。

```
vsmart1# show control connections
                                                                    PEER
PEER
      PEER    PEER PEER            SITE       DOMAIN PEER         PRIV    PEER
PUB
INDEX TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP   PORT    PUBLIC IP
PORT    ORGANIZATION   REMOTE COLOR     STATE UPTIME
------------------------------------------------------------------------------------
0     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
  12346   EXAMPLE-ORG    default         up     53:08:18:50
0     vmanage tls  172.16.1.6         1          0      10.2.100.6   45689   10.2.100.6
  45689   EXAMPLE-ORG    default         up     53:08:18:32
1     vedge   tls  1.1.100.1       100        1      10.3.1.2     57853   10.2.100.1
53624   EXAMPLE-ORG    biz-internet    up     53:08:18:44
1     vedge   tls  1.1.101.1       101        1      10.4.1.2     55411   10.2.100.1
53622   EXAMPLE-ORG    biz-internet    up     53:08:18:48
1     vbond   dtls 172.16.1.2         0          0      10.1.1.2     12346   10.1.1.2
  12346   EXAMPLE-ORG    default         up     53:08:18:51

vsmart1#
```

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から Cisco Catalyst SD-WAN Validator のプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco SD-WAN Validator での **show orchestrator reverse-proxy-mapping** コマンドの出力例を示します。コマンド出力の [PROXY IP] 列と [PROXY PORT] 列のエントリは、プロキシの IP アドレスとポート番号です。[PRIVATE IP] 列と [PRIVATE PORT] 列のエントリは、VPN 0 のトランスポート インターフェイスのプライベート IP アドレスとポート番号です。

```
vbond# show orchestrator reverse-proxy-mapping

                                                        PRIVATE             PROXY
UUID                                    PRIVATE IP      PORT     PROXY IP   PORT
------------------------------------------------------------------------------
14c35ae4-69e3-41c5-a62f-725c839d25df    10.2.100.4      23456    10.2.1.10  23458
14c35ae4-69e3-41c5-a62f-725c839d25df    10.2.100.4      23556    10.2.1.10  23558
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23456    10.2.1.10  23457
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23556    10.2.1.10  23557
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23656    10.2.1.10  23657
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23756    10.2.1.10  23757
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23856    10.2.1.10  23857
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      23956    10.2.1.10  23957
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      24056    10.2.1.10  24057
6c63e80a-8175-47de-a455-53a127ee70bd    10.2.100.6      24156    10.2.1.10  24157

vbond#
```

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から WAN エッジデバイスのプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan control connections** コマンドの出力例を示します。コマンド出力で、Cisco SD-WAN Managerインスタンスまたは Cisco SD-WAN コントローラ の [PROXY] 列のエントリを確認します。エントリが [Yes] の場合、[PEER PUBLIC IP] および [PEER PUBLIC PORT] のエントリはプロキシ IP アドレスとポート番号です。

```
Device# show sdwan control connections

                                                                    PEER              PEER
                                CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER              PRIV  PEER        PUB
                              GROUP

TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP        PORT  PUBLIC IP   PORT
ORGANIZATION    LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------------------------

vsmart  tls  172.16.1.4         1          1      10.2.100.4    23558 10.2.1.10   23558
 EXAMPLE-ORG     biz-internet    Yes   up     52:08:44:25 0

vbond   dtls 0.0.0.0         0          0      10.1.1.2      12346 10.1.1.2    12346
EXAMPLE-ORG     biz-internet    -     up     52:08:50:47 0
```

```
vmanage tls  172.16.1.6         1          0      10.2.100.6    23957 10.2.1.10   23957
 EXAMPLE-ORG     biz-internet    Yes   up     66:03:04:50 0
```

```
Device#
```

Cisco vEdge デバイス では、**show control connections** コマンドを実行して同様の出力を取得できます。

例：リバースプロキシとの認証のために WAN エッジデバイスにインストールされた署名付き証明書を表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan certificate reverse-proxy** コマンドの出力例を示します。

```
Device# show sdwan certificate reverse-proxy

Reverse proxy certificate

------------------


Certificate:

    Data:

        Version: 1 (0x0)

        Serial Number: 1 (0x1)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

        Validity

            Not Before: Jun  2 19:31:08 2021 GMT

            Not After : May 27 19:31:08 2051 GMT

       Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78,
 O = ViptelaClient
        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                RSA Public-Key: (2048 bit)

                Modulus:

                    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:

                    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:

                    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:

                    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:
```

```
                    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:
                    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
                    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:
                    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
                    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:
                    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:
                    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:
                    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:
                    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:
                    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:
                    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:
                    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
                    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:
                    34:9b
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
         b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:
         07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
         33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:
         c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:
         af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:
         7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:
         61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:
         0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:
         d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:
         3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:
         88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:
         19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:
         06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:
         2f:31:02:59

Device#
```

Cisco vEdge デバイス では、**show certificate reverse-proxy** コマンドを実行して同様の出力を取得できます。

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。