



期限切れのエンタープライズ証明書の表示と検疫

- [期限切れの証明書の表示と検疫（1 ページ）](#)
- [期限切れの証明書の表示と検疫について（2 ページ）](#)
- [証明書が期限切れのデバイスの検疫の有効化（3 ページ）](#)
- [期限切れ証明書の検疫におけるデバイスの表示と修復（3 ページ）](#)

期限切れの証明書の表示と検疫

表 1: 機能の履歴

機能名	リリース情報	機能説明
期限切れの証明書の表示と検疫	Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1	Cisco SD-WAN Manager は、デバイスまたは Cisco Catalyst SD-WAN 制御コンポーネントの証明書がいつ期限切れになったかを示します。 また、証明書が期限切れになったすべてのエッジデバイスを検疫できます。検疫により、デバイスはステージングステータスになります。検疫対象のデバイスは Cisco Catalyst SD-WAN 制御コンポーネントへの制御接続は維持しますが、データプレーントラフィックは処理しません。

期限切れの証明書の表示と検疫について

期限切れの証明書の表示

デジタル証明書は、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。認証後、デバイスと Cisco Catalyst SD-WAN 制御コンポーネントは相互にセキュアなセッションを確立できます。証明書は認証局（CA）によって発行され、有効期限があります。

Cisco SD-WAN Manager は数分ごとに、ネットワーク内のデバイスと Cisco Catalyst SD-WAN 制御コンポーネントに期限切れの証明書がないかチェックします。期限切れの証明書が検出された場合、Cisco SD-WAN Manager には、**[Configuration] > [Certificates] > [WAN Edges]** ページまたは **[Configuration] > [Certificates] > [Control Components]** ページへのリンク付きのバナーが表示され、証明書の更新が必要なデバイスまたはコンポーネントの詳細が示されます。

デバイス検疫

検疫とは、デバイスをステージング状態にすることを指します。検疫対象のデバイスは Cisco Catalyst SD-WAN 制御コンポーネントへの制御接続は維持しますが、データプレーントラフィックは処理しません。

証明書の期限が切れているデバイスを検疫できます。「[証明書が期限切れのデバイスの検疫の有効化（3 ページ）](#)」を参照してください。

証明書の期限が切れているデバイスを検疫すると、期限切れの証明書の更新が要求されます。組織のネットワークセキュリティ要件に準拠するために、証明書の期限が切れているネットワーク要素の削除が必要となる場合があります。

この表は、検疫機能が有効になっている場合に、自動検疫の対象となるデバイスを示しています。

表 2: 期限切れ証明書の自動検疫

デバイスまたは制御コンポーネント	検疫が有効な場合の自動検疫
証明書を使用するハードウェアデバイス	対応
オンボックスのトラステッドプラットフォーム モジュール（TPM）のセキュアな固有デバイス識別子（SUDI）証明書を使用するハードウェアデバイス	非対応
ソフトウェアデバイス	対応
Cisco Catalyst SD-WAN 制御コンポーネント	非対応

マルチテナント機能

マルチテナントのシナリオでは、期限切れ証明書の検疫の有効化はプロバイダーレベルでのみ可能であり、すべてのテナントに適用されます。

証明書が期限切れのデバイスの検疫の有効化

手順

ステップ 1 Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。

ステップ 2 **[Device Quarantine]** をクリックします。

ステップ 3 デバイス検疫を有効にします。

期限切れ証明書の検疫におけるデバイスの表示と修復

Cisco SD-WAN Manager は、証明書が期限切れのデバイスを検疫できます。「[期限切れの証明書の表示と検疫について（2 ページ）](#)」を参照してください。Cisco SD-WAN 制御コンポーネントは検疫しません。

始める前に

期限切れ証明書の検疫を有効にします。「[証明書が期限切れのデバイスの検疫の有効化（3 ページ）](#)」を参照してください。

手順

ステップ 1 **[Configuration] > [Certificates] > [WAN Edges]** ページを開き、証明書の更新が必要なデバイスはどれかの詳細を含むテーブルを表示します。

Cisco SD-WAN Manager に証明書の期限切れによって 1 つ以上のデバイスが検疫されていることを示すバナーメッセージが表示されている場合は、バナーメッセージ内のリンクをクリックしてページを開きます。

テーブルで、感嘆符アイコンはデバイスの問題を示しています。アイコンにカーソルを合わせると、証明書の期限切れなどの問題の詳細が表示されます。デバイスが検疫されている場合、そのデバイスの **[Validate]** 列に **[staging]** と表示されます。

ステップ 2 検疫からデバイスを削除するには、その証明書を更新します。「[WAN Edge デバイス証明書署名要求の生成](#)」を参照してください。

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。