Certificate Management

（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。

Web サーバー証明書

シスコは Cisco SD-WAN Manager の Web 証明書を発行しません。証明書署名要求（CSR）を生成し、ドメインネームシステム（DNS）名の認証局（CA）の署名を得ることをお勧めします。その後、IP の DNS サーバーに A エントリを追加するか、`.viptela.net` / `.sdwan.cisco.com` Cisco SD-WAN Manager DNS 名に CNAME を追加します。

（注） シスコが発行するコントローラ証明書は、コントローラが内部で使用するためのものです。これらの証明書を使用して Web サーバー証明書を発行することはできません。

詳細については、『Cisco Catalyst SD-WAN Getting Started Guide』の「Web Server Certificates」の項を参照してください。

コントローラの Cisco Catalyst SD-WAN SSL 証明書の更新

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。

（注） 証明書の更新プロセスは、専用のシングルテナントまたはマルチテナント コントローラ オーバーレイがある場合にのみ適用されます。共用テナントオーバーレイがある場合、このプロセスは適用されません。

Cisco SD-WAN Manager を使用して、証明書署名要求（CSR）を生成し、署名付き証明書をインストールできます。証明書ルート CA には、次の 3 つのオプションがあります。

1. Cisco Root CA バンドル（ソフトウェアバージョン 19.2.3 以降を搭載のコントローラ、ソフトウェアバージョン 19.2.3 以降を搭載の Cisco Catalyst SD-WAN デバイス、ソフトウェアバージョン 16.12.3+ または 16.10.4+ または 17.x+ 以降を搭載の Cisco IOS XE Catalyst SD-WAN デバイスに提供済み）
2. Symantec/Digicert Root CA（すべてのコントローラ、Cisco Catalyst SD-WAN デバイス、および Cisco IOS XE Catalyst SD-WAN デバイスに提供済み）
3. お客様自身の Enterprise Root CA

（注） 証明書生成方式を 1 回だけ選択します。選択した方法は、オーバーレイネットワークにデバイスを追加するたびに自動的に適用されます。

コントローラ証明書を更新するには、展開タイプと証明書タイプに基づく適切なプロセスに従う必要があります。

- コントローラの認定許可設定は、すべてのコントローラデバイスの認証生成プロセスを設定します。詳細については、『Cisco Catalyst SD-WAN Controller Certificates』[英語] を参照してください。
- 証明書の更新にはコントロールプレーンのフラップ全体が含まれるため、シスコのプロビジョニング済みのクラウドホスト型コントローラの場合でも、上記の手順に従う必要があります。
- Cisco CloudOps チームは、お客様の証明書を自動的に更新しません。
- [Cisco SD-WAN Manager Settings] ページには、[Symantec Automated] または [Cisco Automated] のオプションがあります。このオプションの「自動」とは、CSR の自動送信と証明書の自動取得を指します。このオプションには、手動オプションと比較すると、プロセスの特定のステップの自動化が含まれます。ただし、各コントローラの CSR の生成をトリガーするステップは手動のままで、更新プロセスはお客様自身で開始します。

- Cisco SD-WAN Manager ダッシュボードには、証明書の有効期限が近づいているという警告が 6 ヵ月前に表示されます。
- 有効期限は、Cisco SD-WAN Manager メニューから **[Configuration]** > **[Certificates]** > **[Controllers]** を選択していつでも確認できます。

（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。

- Cisco CloudOps チームは、有効期限の 30 日、15 日、5 日前に、システム内オーバーレイの登録済み電子メールアドレスの連絡先に電子メール通知を送信します。
- お客様は、現在の登録済み電子メールアドレスのリクエストや変更のために、いつでもケースをオープンできます。すべての Cisco CloudOps 通知について、所有者の電子メールアドレスを常に最新の状態に保つことをお勧めします。アラート通知用のお客様の連絡先電子メールアドレスを更新することをお勧めします。できれば、個人のユーザーではなく、チームのメールアドレスを使用してください。
- また、コントローラ証明書の有効期限に注意し、失効日の少なくとも 1 ヵ月前に更新を計画することをお勧めします。

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。