Cisco vManage のセットアップと設定

ネットワークの設定

このセクションのトピックでは、ネットワークの設定方法について説明します。

稼働イベントシーケンス

エッジデバイスの稼働プロセス（すべてのデバイスの認証と検証、機能するオーバーレイネットワークの確立など）は、最小限のユーザー入力のみで実行されます。概念的な観点から見ると、稼働プロセスを 2 つの部分に分けることができます。1 つはユーザー入力を必要とする部分で、もう一つは自動的に実行される部分です。

1. 最初の部分では、ネットワークを設計し、クラウドルータの仮想マシン（VM）インスタンスを作成し、ハードウェアルータを設置して起動します。次に、Cisco vManage で、ネットワークにルータを追加し、各ルータの設定を作成します。このプロセスについては、「稼働シーケンスのユーザー部分の概要」で説明します。

2. 稼働プロセスの 2 つ目の部分は、自動的に実行され、Cisco SD-WAN ソフトウェアによってオーケストレーションされます。ルーターは、オーバーレイネットワークに参加すると、それら自体の検証と認証を自動的に実行し、相互にセキュアな通信チャネルを確立します。Cisco vBond オーケストレーション と Cisco vSmart コントローラ については、ネッ

トワーク管理者が必要な認証関連ファイルを Cisco vManage からダウンロードする必要があり、その後、これらの Cisco vSmart コントローラ と Cisco vBond オーケストレーション が Cisco vManage からそれらの設定を自動的に受信します。シスコのハードウェアルータは、起動すると、ネットワーク上で認証され、ゼロタッチプロビジョニング（ZTP）と呼ばれるプロセスを通じて Cisco vManage から自動的に設定を受信します。このプロセスについては、「稼働シーケンスの自動部分」で説明します。

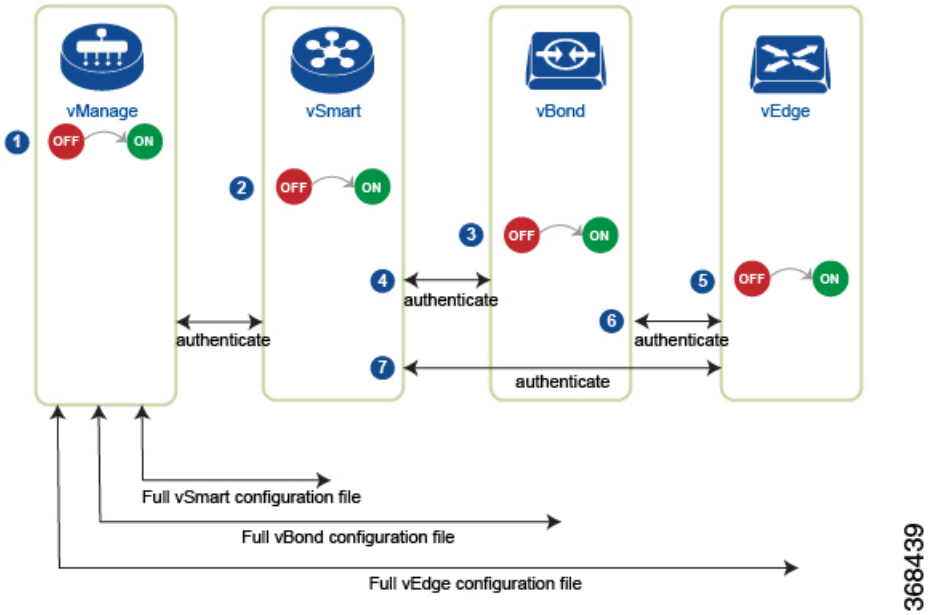
この 2 つの部分からなるプロセスの最終結果は、運用可能なオーバーレイネットワークです。

このトピックでは、稼働プロセスの実行中に発生するイベントシーケンスについて説明します。まずユーザー部分を説明し、次に自動認証およびデバイス検証の動作方法を説明します。

稼働プロセスのイベントシーケンス

機能的な観点から見ると、オーバーレイネットワークでルータを稼働させるタスクは、次の順序で実行されます。

図 *1*: 稼働イベントシーケンス



1. Cisco vManage ソフトウェアが、データセンター内のサーバーで起動します。
2. Cisco vBond オーケストレーション が、DMZ 内のサーバーで起動します。
3. Cisco vSmart コントローラ が、データセンター内のサーバーで起動します。
4. Cisco vManage と Cisco vBond オーケストレーション が相互に認証し、Cisco vManage と Cisco vSmart コントローラ が相互に認証し、Cisco vSmart コントローラ と Cisco vBond オーケストレーション が相互にセキュアに認証します。

5. Cisco vManage が、Cisco vSmart コントローラ と Cisco vBond オーケストレーション に設定を送信します。
6. ルータが、ネットワーク内で起動します。
7. ルータが、それ自体を Cisco vBond オーケストレーション で認証します。
8. ルータが、それ自体を Cisco vManage で認証します。
9. ルータが、それ自体を Cisco vSmart コントローラ で認証します。
10. Cisco vManage が、ルータに設定を送信します。

稼働プロセスを開始する前に、次の点に注意してください。

- 最高レベルのセキュリティを実現するために、認証および許可されたルータのみが Cisco SD-WAN オーバーレイネットワークにアクセスして参加することができます。この目的のために、Cisco vSmart コントローラ は、すべてのルータがネットワークを介してデータトラフィックを送信する前に、すべてのルータに対する自動認証を実行します。
- ルータが認証されると、ルータがプライベートアドレス空間（NAT ゲートウェイの後ろ）にあるかパブリックアドレス空間にあるかにかかわらず、データトラフィックフローが発生します。

Cisco SD-WAN オーバーレイネットワークでハードウェアおよびソフトウェアコンポーネントを稼働させるには、すべてのルータおよびその他のネットワーク ハードウェア コンポーネントを接続するトランスポートネットワーク（「トランスポートクラウド」とも呼ばれる）が使用可能である必要があります。通常、これらのコンポーネントは、データセンターおよびブランチオフィスにあります。トランスポートネットワークの唯一の目的は、ドメイン内のすべてのネットワークデバイスを接続することです。Cisco SD-WAN ソリューションは、トランスポートネットワークに依存しないため、任意のタイプ（インターネット、マルチプロトコルラベル スイッチング（MPLS）、レイヤ 2 スイッチング、レイヤ 3 ルーティング、ロングターム エボリューション（LTE）など）またはトランスポートの任意の組み合わせにすることができます。

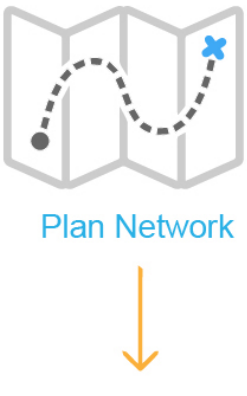
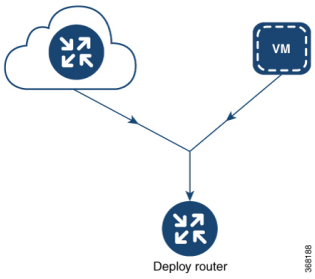
ハードウェアルータの場合は、Cisco SD-WAN ゼロタッチプロビジョニング（ZTP）SaaS を使用してルータを稼働させることができます。詳細については、「ZTP 用のルータの準備」を参照してください。

稼働シーケンスのユーザー部分の概要

一般的な意味では、Cisco SD-WAN オーバーレイネットワークを稼働させるために行うことは、任意のネットワークを稼働させるために行うことと同じです。つまり、ネットワークを計画し、デバイス設定を作成してから、ネットワークハードウェアおよびソフトウェアコンポーネントを展開します。これらのコンポーネントには、すべての Cisco IOS XE SD-WAN デバイス、オーバーレイネットワークに参加するすべての従来のルータ、およびオーバーレイネットワーク全体で共有サービス（ファイアウォール、ロードバランサ、ID プロバイダー（IdP）システムなど）を提供するすべてのネットワークデバイスが含まれます。

次の表に、Cisco SD-WAN オーバーレイネットワークの稼働シーケンスのユーザー部分における手順の概要を示します。各手順の詳細については、「**手順**」列に示されている手順のリンク先を参照してください。Cisco IOS XE SD-WAN デバイスは任意の順序で稼働させることができますが、表に記載されている順序で展開することをお勧めします。これは、デバイスがそれ自体を検証および認証する機能的な順序です。

表 *1*: 稼働シーケンスのワークフロー

	ワークフロー	手順
1		オーバーレイネットワークを計画します。
2		Cisco IOS XE SD-WAN デバイスをオーバーレイネットワークに展開します。 1. クラウドルータについては、AWS サーバー、ESXi、または KVM ハイパーバイザのいずれかで VM インスタンスを作成します。 2. Cisco vManage から、すべての Cisco IOS XE SD-WAN デバイスのシリアル番号をオーバーレイネットワーク内の Cisco vSmart コントローラ および Cisco vBond オーケストレーション に送信します。 3. Cisco vManage で設定テンプレートを作成することにより、Cisco IOS XE SD-WAN デバイスの完全な設定を作成します。Cisco vManage は、オーバーレイネットワーク内のデバイスを検出すると、適切な設定テンプレートをデバイスにプッシュします。

システムとインターフェイスの概要

ネットワークデバイスの基本的なシステム全体の機能のセットアップは、単純明快なプロセスです。基本パラメータには、ホストプロパティ（名前や IP アドレスなど）の定義、時間プロパティ（NTP など）の設定、デバイスへのユーザーアクセスのセットアップ、システムログ（Syslog）パラメータの定義が含まれます。

さらに、Cisco SD-WAN ソフトウェアは、オーバーレイネットワーク内の Cisco SD-WAN デバイスにアクセスするための多数の管理インターフェイスを提供します。

ホストプロパティ

すべてのデバイスには、ネットワークトポロジのビューを構築するために Cisco SD-WAN ソフトウェアが使用する情報を指定する基本的なシステム全体のプロパティがあります。各デバイスには、オーバーレイネットワーク内のデバイスの固定位置を提供するシステム IP アドレスがあります。このアドレスは、ルータのルータ ID と同じように機能しますが、デバイスのインターフェイスやインターフェイス IP アドレスには依存しません。システム IP アドレスは、各デバイスのトランスポートロケーション（TLOC）プロパティを構成する 4 つのコンポーネントの 1 つです。

すべてのデバイスで設定する必要がある 2 つ目のホストプロパティは、そのネットワークドメインの Cisco vBond オーケストレーション の IP アドレス、または Cisco vBond オーケストレーション の 1 つ以上の IP アドレスに解決されるドメインネームシステム（DNS）名です。Cisco vBond オーケストレーション は、オーバーレイネットワークを稼働させ、新しいデバイスのオーバーレイへの参加を許可し、デバイスと Cisco vSmart コントローラ が相互に見つけられるように紹介を提供するというプロセスを自動的にオーケストレーションします。

その他に、Cisco vBond オーケストレーション を除くすべてのデバイスに、ドメイン識別子とサイト識別子という 2 つのシステム全体のホストプロパティが必要です。これらは、Cisco SD-WAN ソフトウェアがトポロジのビューを構築することを可能にします。

ホストプロパティの設定方法については、「Cisco SD-WAN Overlay Network Bring-Up Process」を参照してください。

時刻と NTP

Cisco SD-WAN ソフトウェアは、Network Time Protocol（NTP）を実装して、Cisco SD-WAN オーバーレイネットワーク全体の時刻配信を同期および調整します。NTP は、交差アルゴリズムを使用して、適切なタイムサーバーを選択し、ネットワーク遅延に起因する問題を回避します。サーバーは、ローカル ルーティング アルゴリズムとタイムデーモンを使用して基準時刻を再配信することもできます。NTP は、RFC 5905『Network Time Protocol Version 4: Protocol and Algorithms Specification』で定義されています。

AAA、RADIUS、および TACACS+ によるユーザー認証とアクセス

Cisco SD-WAN ソフトウェアは、認証、許可、およびアカウンティング（AAA）を使用して、ネットワーク上のデバイスのセキュリティを提供します。AAA は、RADIUS および Terminal Access Controller Access-Control System（TACACS +）のユーザー認証との組み合わせによって、デバイスへのアクセスを許可するユーザーと、ユーザーがデバイスにログインまたは接続した後に実行を許可する操作を制御します。

「認証」とは、デバイスへのアクセスを試みるユーザーが認証されるプロセスを指します。ユーザーは、デバイスにアクセスするために、ユーザー名とパスワードを使用してログインします。ローカルデバイスはユーザーを認証できます。または、リモートデバイス（RADIUS サーバーと TACACS+ サーバーのいずれか、またはその両方を順番に使用）によって認証を実行することもできます。

「許可」は、ユーザーがデバイスで特定のアクティビティを実行することを許可されるかどうかを決定します。Cisco SD-WAN ソフトウェアでは、ロールベースのアクセスを使用して許可が実装されています。アクセスは、デバイスで設定されているグループに基づきます。ユーザーは、1 つ以上のグループのメンバーになることができます。許可の実行時にはユーザー定義のグループが考慮されます。つまり、Cisco SD-WAN ソフトウェアは、RADIUS サーバーまたはTACACS+ サーバーから受信したグループ名を使用してユーザーの許可レベルを確認します。各グループには、対応するデバイスで特定の機能を実行することをグループのメンバーに許可する権限が割り当てられます。これらの権限は、設定コマンドの特定の階層や、グループのメンバーが表示または変更できる操作コマンドの対応する階層に対応します。

Cisco IOS XE リリース 17.5.1a 以降では、「アカウンティング」で、ユーザーがデバイスで実行するコマンドのレコードが生成されます。アカウンティングは、TACACS+ サーバーによって実行されます。

詳細については、「Role-Based Access with AAA」を参照してください。

WAN と WLAN の認証

有線ネットワーク（WAN）の場合、Cisco SD-WAN デバイスは、IEEE 802.1X ソフトウェアを実行して、無許可のネットワークデバイスが WAN にアクセスすることを防止できます。IEEE 802.1X は、ポートベースのネットワーク アクセス コントロール（PNAC）プロトコルで、クライアント/サーバーメカニズムを使用して、ネットワークへの接続を希望するデバイスの認証を提供します。

IEEE 802.1X 認証には、次の 3 つのコンポーネントが必要です。

- リクエスト送信者：ワイドエリアネットワーク（WAN）へのアクセスをリクエストするクライアントデバイス（ラップトップなど）。Cisco SD-WAN オーバーレイネットワークでは、サプリカントは、802.1X 準拠のソフトウェアを実行しているサービス側デバイスです。これらのデバイスは、ネットワーク アクセス リクエストをルータに送信します。
- オーセンティケータ：WAN に防壁を提供するネットワークデバイス。オーバーレイネットワークでは、インターフェイスデバイスを、802.1X オーセンティケータとして機能するように設定できます。このデバイスは、制御ポートと非制御ポートの両方をサポートします。制御ポートの場合、Cisco SD-WAN デバイスは、802.1X ポートアクセスエンティティ（PAE）として機能し、許可されたネットワークトラフィックに対して制御ポートの出入りを許可し、無許可のネットワークトラフィックに対してはそれを拒否します。非制御ポートの場合、Cisco SD-WAN は、802.1X PAE として機能し、Extensible Authentication Protocol over IEEE 802（EAP over LAN または EAPOL）フレームを送受信します。
- 認証サーバー：WAN に接続するリクエスト送信者を検証および認証する認証ソフトウェアを実行しているホスト。オーバーレイネットワークでは、このホストは、外部RADIUS サーバーです。802.1X ポートインターフェイス Cisco SD-WAN デバイスに接続された各クライアントが、この RADIUS サーバーによって認証され、インターフェイスが仮想 LAN（VLAN）に割り当てられることにより、クライアントが、ルータまたは LAN によって提供されるサービスにアクセスできるようになります。

ワイヤレス LAN（WLAN）の場合、ルータは、IEEE 802.11i を実行することにより、無許可のネットワークデバイスが WLAN にアクセスすることを防止できます。IEEE 802.11i は、Wi-Fi

Protected Access（WPA）と Wi-Fi Protected Access II（WPA2）を実装して、WLAN に接続するデバイスに関する認証と暗号化を提供します。WPA は、ユーザー名とパスワードを使用して、WLAN 上の個別のユーザーを認証します。WPA は、RC4 暗号に基づく Temporal Key Integrity Protocol（TKIP）を使用します。WPA2 は、NIST FIPS 140-2 準拠の AES 暗号化アルゴリズムと IEEE 802.1X ベースの認証を実装し、WPA よりも強力なユーザー アクセス セキュリティを実現します。WPA2 は、AES 暗号に基づく Counter Mode Cipher Block Chaining Message Authentication Code Protocol（CCMP）を使用します。認証は、事前共有キーを使用するか RADIUS 認証によって行われます。

ネットワークのセグメント化

Cisco SD-WAN のレイヤ 3 ネットワーク セグメンテーションは、Cisco IOS XE SD-WAN デバイス 上の VRF によって実現されます。Cisco IOS XE SD-WAN デバイス で Cisco vManage を使用してネットワーク セグメンテーションを設定すると、システムによって自動的に VPN 設定が VRF 設定にマッピングされます。

ネットワーク インターフェイス

Cisco SD-WAN オーバーレイネットワークの設計では、インターフェイスは、VRF に変換される VPN に関連付けられます。VPN に参加するインターフェイスは、その VPN で設定および有効化されます。各インターフェイスは、単一の VPN にのみ存在できます。

（注） Cisco IOS XE SD-WAN デバイス は、VPN の代わりに VRF を使用します。Cisco vManage で設定を完了すると、システムは、VPN 設定を VRF 設定に自動的にマッピングします。

オーバーレイネットワークには、次のタイプの VPN/VRF があります。

- **VPN 0**：設定された WAN トランスポート インターフェイスを使用して制御トラフィックを伝送する**トランスポート VPN**。最初は、VPN 0 には管理インターフェイスを除くデバイスのすべてのインターフェイスが含まれており、すべてのインターフェイスが無効になっています。これは、Cisco IOS XE SD-WAN ソフトウェアのグローバル VRF です。
- **VPN 512**：オーバーレイネットワーク内の Cisco SD-WAN デバイス間でアウトオブバンドネットワーク管理トラフィックを伝送する**管理 VPN**。管理トラフィックに使用されるインターフェイスは、VPN 512 に存在します。デフォルトでは、VPN 512 が設定され、すべての Cisco SD-WAN デバイスで有効になっています。コントローラデバイスの場合は、デフォルトでは VPN 512 は設定されていません。Cisco IOS XE SD-WAN デバイス では、管理 VPN は VRF Mgmt-Intf に変換されます。

ネットワーク インターフェイスごとに、多数のインターフェイス固有のプロパティ（DHCP クライアントおよびサーバー、VRRP、インターフェイスの MTU および速度、Point-to-Point Protocol over Ethernet（PPPoE）など）を設定できます。大まかに言うと、インターフェイスを動作可能にするには、インターフェイスの IP アドレスを設定し、動作可能（シャットダウンなし）としてマークする必要があります。実際には、インターフェイスごとに常に追加のパラメータを設定します。

管理とモニタリングのオプション

ルータは、さまざまな方法で管理およびモニタリングできます。管理インターフェイスは、Cisco SD-WAN オーバーレイネットワーク内のデバイスへのアクセスを提供します。これにより、アウトオブバンド方式でデバイスから情報を収集し、デバイスの設定や再起動などの操作を実行することが可能になります。

次の管理インターフェイスを使用できます。

- CLI
- IPFIX（IP Flow Information Export）
- RESTful API
- SNMP
- システムロギング（Syslog）メッセージ
- Cisco vManage

CLI

各デバイスで CLI にアクセスして、CLI から、ローカルデバイスでオーバーレイネットワーク機能を設定し、そのデバイスに関する動作ステータスおよび情報を収集することができます。使用可能な CLI を使用して、Cisco vManage からすべての Cisco SD-WAN ネットワークデバイスを設定およびモニタリングすることを強く推奨します。これにより、詳細な動作データおよびステータスデータを含む、ネットワーク全体の動作とデバイスステータスを確認できます。さらに、Cisco vManage は、複数のデバイスを同時にセットアップするための一括操作など、オーバーレイネットワークデバイスを稼働させて設定するための簡単なツールを提供します。

Cisco SD-WAN デバイスへの SSH セッションを確立することにより、CLI にアクセスできます。

Cisco vManage によって管理されている Cisco SD-WAN デバイスの場合は、CLI から設定を作成または変更すると、その変更が、Cisco vManage 設定データベースに保存されている設定によって上書きされます。

IPFIX

IP Flow Information Export（IPFIX）プロトコル（「cflowd」とも呼ばれる）は、オーバーレイネットワーク内の Cisco SD-WAN デバイスを通過するトラフィックをモニタリングし、トラフィックに関する情報をフローコレクタにエクスポートするためのツールです。エクスポートされた情報は、フローに関する情報とフロー内のパケットの IP ヘッダーから抽出されたデータの両方を含むテンプレートレポートで送信されます。

Cisco SD-WAN cflowd は、1:1 トラフィックサンプリングを実行します。すべてのフローに関する情報が cflowd レコードに集約されます。フローはサンプリングされません。

（注） Cisco SD-WAN デバイスは、コレクタにエクスポートされるレコードをキャッシュしません。

Cisco SD-WAN cflowd ソフトウェアは、RFC 7011 および RFC 7012 で指定されている cflowd バージョン 10 を実装しています。

IPFIX によってエクスポートされる要素のリストについては、「Traffic Flow Monitoring with Cflowd」を参照してください。

トラフィックフロー情報の収集を有効にするには、対象となるトラフィックを識別するデータポリシーを作成し、そのトラフィックを cflowd コレクタに転送する必要があります。詳細については、「Traffic Flow Monitoring with Cflowd」を参照してください。

また、データポリシーを設定せずに Cisco SD-WAN デバイスで cflowd の可視性を直接有効にすることもできます。これにより、LAN 内のすべての VPN からデバイスに着信するトラフィックのトラフィックフローモニタリングを実行できます。その後、Cisco vManage の GUI またはデバイスの CLI からトラフィックをモニタリングできます。

RESTful API

Cisco SD-WAN ソフトウェアは、オーバーレイネットワークの Cisco SD-WAN デバイスを制御、設定、モニターするためのプログラムインターフェイスである RESTful API を提供します。Cisco vManage を介して RESTful API にアクセスできます。

Cisco SD-WAN の RESTful API コールにより、Cisco SD-WAN ソフトウェアおよびハードウェアの機能がアプリケーションプログラムに公開されます。このような機能には、デバイスとオーバーレイネットワーク自体を維持するために実行する通常の操作が含まれます。

SNMP

Simple Network Management Protocol（SNMP）を使用すると、オーバーレイネットワーク内のすべての Cisco SD-WAN デバイスを管理できます。Cisco SD-WAN ソフトウェアは SNMP v2c をサポートしています。

基本的な SNMP プロパティ（デバイス名、ロケーション、連絡先、コミュニティ）を設定すると、SNMP ネットワーク管理システム（NMS）によるデバイスのモニタリングが可能になります。

トラップを受信するようにトラップグループ および SNMP サーバーを設定できます。

SNMP MIB のインターネットポートのオブジェクト識別子（OID）は、1.3.6.1 です。

SNMP トラップは、Cisco SD-WAN デバイスが SNMP 管理サーバーに送信する非同期通知です。トラップにより、Cisco SD-WAN デバイスで発生するイベント（正常なものであっても重大なものであっても）が管理サーバーに通知されます。デフォルトでは、SNMP トラップは SNMP サーバーに送信されません。SNMPv3 の場合は、通知の PDU タイプが SNMPv2c inform（InformRequest-PDU）または trap（Trapv2-PDU）のいずれかであることに注意してください。

syslog メッセージ

システムロギング操作では、UNIX の **syslog** コマンドと同様のメカニズムを使用して、オーバーレイネットワーク内の Cisco SD-WAN デバイスで発生するシステム全体の高レベルの操作が記録されます。メッセージのログレベル（優先順位）は、標準の UNIX コマンドのログレベル（優先順位）と同じです。また、記録する Syslog メッセージの優先順位を設定できます。

メッセージのログは、Cisco SD-WAN デバイス上のファイルまたはリモートホストに記録できます。

Cisco vManage

Cisco vManage は、オーバーレイネットワーク内のすべての Cisco SD-WAN デバイスの設定と管理を可能にする中央集中型のネットワーク管理システムで、ネットワーク全体の動作とネットワーク内の個別のデバイスの動作を表示するダッシュボードを提供します。3 台以上の Cisco vManage サーバーが Cisco vManage クラスタに統合され、最大 6,000 台の Cisco SD-WAN デバイスに拡張性と管理サポートを提供し、複数のデバイスに Cisco vManage 機能を分散し、ネットワーク管理動作の冗長性を実現します。

Okta を使用したシングルサインオンの設定

Oktaは、シングルサインオン（SSO）を使用して任意のユーザーを任意のデバイスの任意のアプリケーションに接続できるセキュアな ID 管理サービスを提供します。

（注） Cisco vManage では MD5 または SHA-1 はサポートされなくなりました。Cisco vManage によって処理されるすべての x.509 証明書は、少なくとも SHA-256 以上の暗号化アルゴリズムを使用する必要があります。

SSO を設定するには、次の作業に従います。

Cisco vManage での ID プロバイダーの有効化

Okta SSO を設定するには、Cisco vManage を使用して ID プロバイダーを有効にし、セキュリティ アサーション マークアップ言語（SAML）メタデータファイルを生成します。

1. Cisco vManage の左側のペインで、**[Administration]** > **[Settings]** を選択します。
2. [Identity Provider Settings] をクリックし、[Edit] をクリックします。
3. [Enabled] をクリックします。
4. [Click here to download the SAML metadata] をクリックし、内容をテキストファイルに保存します。このデータは Okta の設定に使用されます。
5. 表示されるメタデータから、Cisco vManage で Okta を設定するために必要な次の情報をメモします。
   - Entity ID
   - 署名付き証明書
   - 暗号化証明書
   - ログアウト URL

- ログイン URL（Login URL）

Okta Web サイトでの SSO の設定

Okta Webサイトで SSO を設定するには、次の手順に従います。

1. Okta Web サイトにログインします。

（注） 各 IdP アプリケーションは、Okta Web サイトにログインするために、カスタマイズされた URL を Okta から取得します。

2. 電子メールアドレスを使用してユーザー名を作成します。
3. Cisco vManage を SSO アプリケーションとして追加するには、右上隅の [Admin] ボタンをクリックして次の画面に移動します。
4. 左上隅を確認して、Okta で**クラシック UI** ビューが表示されていることを確認します。
5. **開発者コンソール**が表示されている場合は、下向きの三角形をクリックして [Classic UI] を選択します。
6. 右側の [Shortcuts] で [Add Application] をクリックして次の画面に移動し、ポップアップウィンドウで [Create New Application] をクリックします。
7. プラットフォームとして [Web] を選択し、[Sign on Method] として [SAML 2.0] を選択します。
8. [作成（Create）] をクリックします。
9. [Application name] にアプリケーション名として文字列を入力します。
10. （任意）：ロゴをアップロードし、[Next] をクリックします。
11. [SAML Settings for Single sign on URL] セクションで、値を、Cisco vManage の GUI からダウンロードしたメタデータの **samlLoginResponse URL** に設定します。
12. [Use this this for Recipient URL and Destination URL] チェックボックスをオンにします。
13. [entityID] の文字列をコピーし、[Audience URI (SP Entity ID)] フィールドに貼り付けます。

    この値は、IP アドレスまたは Cisco vManage サイトの名前です。
14. [Default RelayState] は空のままにします。
15. [Name ID format] で、[EmailAddress] を選択します。
16. [Application username] で、[Okta username] を選択します。
17. [Show Advanced Settings] で、フィールドに次のように入力します。

表 *2 : [Show Advanced Settings]* のフィールド

コンポーネント	値	設定
応答	署名済み	N/A
アサーション署名	署名済み	N/A
Signature Algorithm	RSA-SHA256	N/A
Digest Algorithm	SHA256	N/A
アサーションの暗号化	暗号化	N/A
Encryption Algorithm	AES256-CBC	N/A
Key Transport Algorithm	RSA-OAEP	N/A
暗号化証明書	N/A	**1.** ダウンロードしたメタデータから暗号化証明書をコピーします。 **2.** www.samltool.com に移動し、[X.509 CERTS] をクリックして、そこに貼り付けます。[Format X.509 Certificate] をクリックします。 **3.** 最後の空の行を削除し、出力（**ヘッダー付きの X.509.cert**）をテキストファイル **encryption.cer** に保存します。 **4.** ファイルをアップロードします。Mozilla Firefox では、アップロードできない場合があります。代わりに、Google Chrome を使用できます。Okta にアップロードすると、証明書情報が表示されます。
シングルログアウトの有効化		これがオンになっていることを確認します。
シングル ログアウト URL		メタデータから取得します。
SP 発行者		メタデータの entityID を使用します。

コンポーネント	値	設定
署名証明書		1. メタデータから取得します。www.samltool.com を使用し、説明に従って、署名証明書をフォーマットします。 2. **signing.cer** などのファイルに保存してアップロードします。
Authentication context class	X.509 証明書	N/A
オナー強制認証	対応	該当なし
SAML issuer ID string	SAML 発行者 ID の文字列	N/A
Attribute Statements	フィールド：[Name]	値：*Username*
	フィールド：[Name format (optional)]	値：指定しない
	フィールド：[Value]	値：*user.login*
Group Attribute Statements	フィールド：[Name]	値：Groups
	フィールド：[Name format (optional)]	値：指定しない
	フィールド：[Matches regex]	値：**.***

（注） 上記のとおりに、Username と Groups という 2 つの文字列を使用する必要があります。それ以外の場合は、デフォルトグループの Basic でのログインになる可能性があります。

18. [Next] をクリックします。
19. [Application Type] で、[This is an internal app that we have created] をオンにします（任意）。
20. [Finish] をクリックします。これにより、Okta アプリケーションの画面が表示されます。
21. [View Setup Instructions] をクリックします。
22. IdP メタデータをコピーします。
23. Cisco vManage で、**[Identity Provider Settings]** > **[Upload Identity Provider Metadata]** に移動し、IdP メタデータを貼り付けて、[Save] をクリックします。

24. IdP メタデータが含まれたファイルの内容をコピーして貼り付けるだけでなく、[Select a file] オプションを使用してファイルを直接アップロードすることもできます。

Okta Web サイトでのアプリケーションへのユーザーの割り当て

Okta Web サイトでユーザーをアプリケーションに割り当てるには、次の手順に従います。

1. Okta アプリケーションの画面で、**[Assignments]** > **[People]** > **[Assign]** に移動します。
2. ドロップダウンリストから [Assign to people] を選択します。
3. 選択したユーザーの横にある [Assign] をクリックし、[Done] をクリックします。
4. ユーザーを追加するには、**[Directory]** > **[Add Person]** をクリックします。
5. [保存（Save）] をクリックします。

PingID の SSO の設定

Cisco vManage は、PingID を IdP としてサポートしています。PingID は、SSO 対応アプリケーションでユーザー ID を認証するための ID 管理サービスです。

PingID を IdP として使用するための Cisco vManage の設定には、次の手順が含まれます。

- PdID から Cisco vManage に IdP メタデータをインポート（アップロード）します。
- PingID にエクスポートする Cisco vManage の SAML メタデータファイルをダウンロードします。

前提条件：

1. Cisco vManage で、ID プロバイダーの設定（**[Administration Settings]** > **[Identity Provider Settings]**）が [Enabled] に設定されていることを確認します。
2. PingID にエクスポートする Cisco vManage の SAML メタデータファイルをダウンロードします。

   これらの手順の詳細については、「Cisco vManage での ID プロバイダーの有効化」を参照してください。この手順は、Okta を IdP として設定する場合と同じです。

PingID を設定するには、次の手順に従います。

PingID 管理ポータルでの SSO の設定

PingID を設定するには、次の手順に従います。

1. PingID 管理ポータルにログインします。
2. 電子メールアドレスを使用してユーザー名を作成します。

3. [アプリケーション（Applications）] タブをクリックします。
4. [Add Application] をクリックし、[New SAML Application] を選択します。

   [Application Details] セクションの [Application Name]、[Application Description]、および [Category] はすべて必須フィールドです。

   ロゴとアイコンについては、使用可能なグラフィック形式は PNG のみです。
5. [Continue to Next Step] をクリックします。

   [Application Configuration] セクションが表示されます。
6. [I have the SAML configuration] が選択されていることを確認します。
7. [You will need to download this SAML metadata to configure the application] セクションで、次のフィールドを設定します。
   1. [Signing Certificate] で、[PingOne Account Origination Certificate] ドロップダウンオプションを使用します。
   2. [SAML Metadata] の横にある [Download] をクリックして、PingOne IdP メタデータをファイルに保存します。
   3. SSO 設定を完了するには、後で、この PingOne IdP メタデータファイルを Cisco vManage にインポートする必要があります。
      1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します。
      2. **[Identity Provider Settings]** > **[Upload Identity Provider Metadata]** をクリックして、保存した PingOne IdP メタデータファイルを Cisco vManage にインポートします。
      3. [保存（Save）] をクリックします。
8. [Provide SAML details about the application you are connecting to] セクションで、次のフィールドを設定します。
   1. [Protocol Version] で、[SAMLv2.0] をクリックします。
   2. [Upload Metadata] で [Select File] をクリックして、保存した Cisco vManage SAML メタデータファイルを PingID にアップロードします。

      PingID は、メタデータファイルを復号化し、他のフィールドに入力できる必要があります。
   3. 次のフィールドと値が正しく入力されていることを確認します。

フィールド	値
Assertion Consumer Service（ACS）	<vManage_URL>/samlLoginResponse
Entity ID	Cisco vManage の IP アドレス

フィールド	値
Single Logout Endpoint	<vManage_URL>/samlLogoutResponse
Single Logout Binging Type	Redirect
Primary Verification Certificate	証明書の名前
Encrypt Assertion	（任意）アサーションを暗号化しないと、アサーションリプレイアタックなどの脆弱性が発生する可能性があります。
Encryption Certification	証明書の名前
Encryption Algorithm	（任意）AES_256
Transport Algorithm	RSA_OAEP
Signing Algorithm	RSA_SHA256
Force Re-authentication	[はい（True）]

9. [Continue to Next Step] をクリックします。
10. [SSO Attribute Mapping] セクションで、次のフィールドを設定します。
    1. [Add new attribute] をクリックして次の属性を追加します。
        1. [Application Attribute] でアプリケーション属性を「Username」として追加します。
        2. [Identity Bridge Attribute or Literal Value Value] を [Email] に設定します。
        3. [Required] チェックボックスをオンにします。
        4. [Application Attribute] で別のアプリケーション属性を「Groups」として追加します。
        5. [Required] チェックボックスをオンにして、[Advanced] をクリックします。
        6. [IDP Attribute Name or Literal Value] セクションで [memberOf] をクリックし、[Function] で [GetLocalPartFromEmail] をクリックします。
    2. [保存（Save）] をクリックします。
11. [Continue to Next Step] をクリックして、**グループアクセス**を設定します。
12. [Continue to Next Step] をクリックします。
13. [Finish] をクリックする前に、設定がすべて正しいことを確認します。

強化されたパスワードの設定

表 *3 :* 機能の履歴

機能名	リリース情報	説明
強化されたパスワード	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、Cisco vManage でパスワードポリシールールが有効になります。パスワードポリシールールが有効になると、Cisco vManage では強力なパスワードの使用が強制されます。

強力なパスワードの強制

強力なパスワードの使用を勧めします。強力なパスワードの使用を強制するには、Cisco vManage でパスワードポリシールールを有効にする必要があります。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します。
2. [Password Policy] で、[Edit] を選択します。
3. [Enabled] をクリックします。

   デフォルトでは、[Password Policy] は [Disabled] に設定されています。
4. [Password Expiration Time (Days)] フィールドで、パスワードが期限切れになるまでの日数を指定できます。

   デフォルトでは、パスワードの有効期限は 90 日です。

   パスワードの有効期限が切れる前に、有効期限の特定日数前にパスワードの変更を求めるバナーが表示されます。これは 30 日です。ただし、パスワードの有効期限フィールドが 60 日未満に設定されている場合は、指定した日数の半分が使用されます。パスワードを変更しないと、ログイン操作がブロックされます。ユーザーアカウントがロックされ、アカウントのロックを解除するには、管理者に連絡する必要があります。

（注） パスワード有効期限ポリシーは、admin ユーザーには適用されません。

パスワード要件

Cisco vManage では、パスワードポリシールールを有効にすると、次のパスワード要件が適用されます。

- 8 文字以上、32 文字以下。
- 少なくとも 1 つの大文字を含む。
- 少なくとも 1 つの小文字を含む。
- 少なくとも 1 つの数字を含む。
- 少なくとも 1 つの特殊文字（# ? ! @ $ % ^ & * -）を含む。
- フルネームまたはユーザー名を含まない。

許可されるパスワード試行回数

アカウントがロックされるまで、6 回連続してパスワードを試行できます。パスワード試行に 6 回失敗すると、15 分間ロックアウトされます。7 回目の試行で正しくないパスワードを入力すると、ログインが許可されず、15 分のロックタイマーが再び開始されます。

アカウントがロックされたら、アカウントが自動的にロック解除されるまで 15 分間待ってください。または、管理者に連絡してパスワードをリセットするか、管理者にアカウントのロック解除を依頼してください。

（注） パスワードを複数回入力しなかった場合も、アカウントはロックされます。パスワードフィールドに何も入力しない場合、パスワードは無効または正しくないと見なされます。

パスワード変更ポリシー

（注） 強力なパスワードを有効にするには、パスワードポリシールールが有効になっている必要があります。詳細については、強力なパスワードの強制 （17 ページ）を参照してください。

パスワードを再設定する場合、最近使用したの 5 つのパスワード（4 つの古いパスワードと 1 つの現在のパスワード）と同じパスワードは使用できません。

Cisco vManage では、パスワード内の少なくとも 4 つの位置の文字を変更する必要があります。

ロックされたユーザーのリセット

ユーザーがパスワードを複数回試行した後にロックされた場合、必要な権限を持つ管理者は、このユーザーのパスワードを更新できます。

ユーザーアカウントのロック解除には、パスワードの変更とユーザーアカウントのロック解除の 2 つの方法があります。

（注） この操作を実行できるのは、**netadmin** ユーザーまたは User Management Write ロールを持つユーザーだけです。

ロックされたユーザーのパスワードをリセットするには、次の手順に従います。

1. [Users] タブ（**[Administration]** > **[Manage Users]**）で、ロックを解除するアカウントを持つユーザーをリストから選択します。
2. [More Actions] オプションをクリックし、[Reset Locked User] をクリックします。
3. [OK] をクリックして、ロックされたユーザーのパスワードをリセットすることを確認します。この操作は取り消すことができないので、注意が必要です。

   または、[Cancel] をクリックして操作をキャンセルできます。

Cisco vManage を使用したユーザーの管理

Cisco vManage のユーザーおよびユーザーグループを追加、編集、表示、または削除するには、[Manage Users] ウィンドウを使用します。

（注） **admin** ユーザーとしてログインしているユーザー、または [Manage Users] 書き込み権限を持つユーザーだけが、Cisco vManage のユーザーおよびユーザーグループを追加、編集、または削除できます。

各ユーザグループには、このセクションに示されている機能の読み取りまたは書き込み権限を付与できます。書き込み権限には読み取り権限が含まれます。

（注） すべてのユーザーグループが、選択された読み取りまたは書き込み権限に関係なく、Cisco vManage ダッシュボードに表示される情報を確認できます。

表 *4:* ユーザ グループ

機能	読み取り権限	書き込み権限
アラーム	**[Monitor]** > **[Alarms]** 画面で、アラームフィルタを設定し、デバイスで生成されたアラームを表示します。	追加の権限はありません。
監査ログ	**[Monitor]** > **[Alarms]** 画面と **[Monitor]** > **[Audit Log]** 画面で、監査ログフィルタを設定し、デバイスのすべてのアクティビティに関するログを表示します。	追加の権限はありません。
証明書	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** で、オーバーレイネットワーク内のデバイスのリストを表示します。 **[Configuration]** > **[Certificates]** > **[Controllers]** 画面で、証明書署名要求（CSR）を表示します。	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** 画面で、デバイスを検証および無効化し、デバイスをステージングし、有効なコントローラデバイスのシリアル番号を Cisco vBond オーケストレーション に送信します。 **[Configuration]** > **[Certificates]** > **[Controllers]** 画面で、CSR を生成し、署名付き証明書をインストールし、RSA キーペアをリセットします。

機能	読み取り権限	書き込み権限
クラスタ	**[Administration]** > **[Cluster Management]** 画面で、Cisco vManage で動作中のサービス、Cisco vManage サーバーに接続されているデバイスのリスト、およびクラスタ内のすべての Cisco vManage サーバーで使用可能なサービスと動作中のサービスに関する情報を表示します。	**[Administration]** > **[Cluster Management]** 画面で、現在の Cisco vManage の IP アドレスを変更し、Cisco vManage サーバーをクラスタに追加し、統計データベースを設定し、クラスタの Cisco vManage サーバーを編集および削除します。
デバイス インベントリ	**[Configuration]** > **[Devices]** > **[WAN Edge List]** 画面で、デバイスの実行中の設定とローカル設定、テンプレートアクティビティのログ、およびデバイスへの設定テンプレート適用のステータスを表示します。 **[Configuration]** > **[Devices]** > **[Controllers]** 画面で、デバイスの実行中の設定とローカル設定や、コントローラデバイスへの設定テンプレート適用のステータスを表示します。	**[Configuration]** > **[Devices]** > **[WAN Edge List]** 画面で、デバイスの許可済みシリアル番号ファイルを Cisco vManage にアップロードし、デバイスを Cisco vManage 設定モードから CLI モードに切り替え、デバイス設定をコピーし、ネットワークからデバイスを削除します。 **[Configuration]** > **[Devices]** > **[Controllers]** 画面で、オーバーレイネットワークからコントローラデバイスを追加および削除し、コントローラデバイスの IP アドレスとログイン情報を編集します。

機能	読み取り権限	書き込み権限
デバイスのモニタリング	**[Monitor]** > **[Geography]** 画面で、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Events]** 画面で、デバイスで発生したイベントを表示します。 **[Monitor]** > **[Network]** 画面で（デバイスが選択されている場合のみ）、ネットワーク内のデバイスのリストを、デバイスステータスの概要、ディープパケットインスペクション（DPI）および Cflowd フロー情報、トランスポートロケーション（TLOC）ロス、遅延、およびジッター情報、制御およびトンネル接続、システムステータス、ならびにイベントとともに表示します。	**[Monitor]** > **[Network]** 画面で（デバイスが選択されている場合のみ）、デバイスを ping し、トレースルートを実行し、IP パケットのトラフィックパスを分析します。
デバイス リブート	**[Maintenance]** > **[Device Reboot]** 画面で、再起動操作を実行できるデバイスのリストを表示します。	**[Maintenance]** > **[Device Reboot]** 画面で、1 つ以上のデバイスを再起動します。
インターフェイス	**[Monitor]** > **[Network]** > **[Interface]** 画面で、デバイスのインターフェイスに関する情報を表示します。	**[Monitor]** > **[Network]** > **[Interface]** 画面で、**チャートオプション**を編集して、表示するデータのタイプを選択し、表示するデータの期間を編集します。
Manage Users	**[Administration]** > **[Manage Users]** 画面で、ユーザーとユーザーグループを表示します。	**[Administration]** > **[Manage Users]** 画面で、Cisco vManage のユーザーとユーザーグループの追加、編集、および削除し、ユーザーグループの権限を編集します。

機能	読み取り権限	書き込み権限
ポリシー（Policy）	**[Configuration]** > **[Policies]** 画面で、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを表示します。	**[Configuration]** > **[Policies]** 画面で、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを作成、編集、および削除します。
ポリシーの設定	**[Configuration]** > **[Policies]** 画面で、作成されたポリシーのリストとその詳細を表示します。	**[Configuration]** > **[Policies]** 画面で、ネットワーク内のすべての Cisco vSmart コントローラ およびデバイスの共通ポリシーを作成、編集、および削除します。
ポリシーの展開	**[Configuration]** > **[Policies]** 画面で、ポリシーが適用されている Cisco vSmart コントローラ の現在のステータスを表示します。	**[Configuration]** > **[Policies]** 画面で、ネットワーク内のすべての Cisco vManage サーバーの共通ポリシーをアクティブ化および非アクティブ化します。
ルーティング	**[Monitor]** > **[Network]** > **[Real-Time]** 画面で、デバイスのリアルタイムルーティング情報を表示します。	**[Monitor]** > **[Network]** > **[Real-Time]** 画面で、コマンドフィルタを追加して情報表示を迅速化させます。
Settings	**[Administration]** > **[Settings]** 画面で、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を表示します。	**[Administration]** > **[Settings]** 画面で、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、証明書認証設定、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を編集し、Web サーバー証明書の証明書署名要求（CSR）を生成し、証明書をインストールします。

機能	読み取り権限	書き込み権限
ソフトウェア アップグレード	**[Maintenance]** > **[Software Upgrade]** 画面で、デバイスのリスト、ソフトウェアアップグレードを実行できる Cisco vManage のカスタムバナー、およびデバイスで実行されているソフトウェアの現在のバージョンを表示します。	**[Maintenance]** > **[Software Upgrade]** 画面で、デバイスに新しいソフトウェアイメージをアップロードし、デバイスのソフトウェアイメージをアップグレード、アクティブ化、および削除し、ソフトウェアイメージをデバイスのデフォルトイメージに設定します。
システム	**[Configuration]** > **[Templates]** > **[Device]** 画面で、Cisco vManage テンプレートを使用して設定されたシステム全体のパラメータを表示します。	**[Configuration]** > **[Templates]** > **[Device]** 画面で、Cisco vManage テンプレートを使用してシステム全体のパラメータを設定します。
テンプレートの設定	**[Configuration]** > **[Templates]** 画面で、機能テンプレートとデバイステンプレートを表示します。	**[Configuration]** > **[Templates]** 画面で、機能テンプレートまたはデバイステンプレートを作成、編集、削除、およびコピーします。
テンプレートの展開	**[Configuration]** > **[Templates]** 画面で、デバイステンプレートが適用されているデバイスを表示します。	**[Configuration]** > **[Templates]** 画面で、デバイステンプレートをデバイスに適用します。

機能	読み取り権限	書き込み権限
ツール	**[Tools]** > **[Operational Commands]** 画面で、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集します。	**[Tools]** > **[Operational Commands]** 画面で、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集し、**interface reset** コマンドを使用して 1 回の操作でデバイスのインターフェイスをシャットダウンして再起動します。 **[Tools]** > **[Operational Commands]** 画面で、ネットワークを再検索して新しいデバイスを検出し、Cisco vManage と同期させます。 **[Tools]** > **[Operational Commands]** 画面で、デバイスへの SSH セッションを確立し、CLI コマンドを発行します。

次の表に、マルチテナント環境でのロールベースアクセスコントロール（RBAC）のユーザーグループ権限のリストを示します。

- R は読み取り権限を表します。
- W は書き込み権限を表します。

表 *5 :* マルチテナント環境の *RBAC* ユーザーグループ

機能	Provider Admin	Provider Operator	Tenant Admin	テナントのオペレータ
Cloud OnRamp	RW	R	RW	R
コロケーション	RW	R	RW	R
RBAC VPN	RW	R	RW	R
セキュリティ	RW	R	RW	R
セキュリティポリシー設定	RW	R	RW	R
vAnalytics	RW	R	RW	R

Add User

1. Cisco vManage で、**[Administration]** > **[Manage Users]** を選択します。[Manage Users] 画面が表示されます。
2. デフォルトでは、[Users] ペインが選択されています。テーブルに、デバイスで設定されているユーザーのリストが表示されます。
3. 既存のユーザーのパスワードを編集、削除、または変更するには、右側の [More Info (…)] 列で、[Edit]、[Delete]、または [Change Password] をクリックします。
4. [Add User] をクリックして新しいユーザーを追加します。
5. [Add New User] ページで、[Full Name]、[Username]、[Password]、および [Confirm Password] に詳細情報を入力します。
6. [User Groups] ドロップダウンで、ユーザーを追加するユーザーグループを選択します。
7. [Resource Group] ドロップダウンで、リソースグループを選択します。

（注） このフィールドは Cisco IOS XE リリース 17.5.1a 以降で利用できます。

8. ユーザーグループを追加するには、[Add User Group] ボタンをクリックします。
9. [Group Name] フィールドにユーザーグループ名を入力します。
10. ユーザーグループに割り当てる [Read] または [Write] チェックボックスをオンにします。

ユーザの削除

ユーザーがデバイスにアクセスする必要がなくなった場合は、そのユーザーを削除できます。ユーザーを削除すると、そのユーザーは対応するデバイスにアクセスできなくなります。ユーザーがログインしている場合、そのユーザーを削除してもログアウトされません。

ユーザを削除するには、次の手順を実行します。

1. [Users] タブで、削除するユーザーをクリックします。
2. テーブルの対応する行の横にある [More Actions] をクリックし、[Delete] をクリックします。
3. [OK] をクリックしてユーザーの削除を確認します。

ユーザの詳細の編集

ユーザーのログイン情報を更新したり、ユーザーグループのユーザーを追加または削除することができます。ログインしているユーザーの詳細情報を編集した場合、変更はそのユーザーがログアウトした後に有効になります。

ユーザの詳細情報を編集するには、次のようにします。

1. [Users] タブで、詳細情報を編集するユーザーをクリックします。
2. テーブルの対応する行の横にある [More Actions] をクリックし、[Edit] をクリックします。
3. ユーザの詳細を編集します。ユーザーグループのユーザーを追加または削除することもできます。
4. [Update] をクリックします。

ユーザ パスワードの変更

必要に応じて、ユーザーのパスワードを更新できます。強力なパスワードの使用を推奨します。

ユーザーのパスワードを変更するには、次の手順に従います。

1. [Users] タブで、パスワードを変更するユーザーをクリックします。
2. テーブルの対応する行の横にある [More Actions] をクリックし、[Change Password] をクリックします。
3. 新しいパスワードを入力し、それを確認します。対象のユーザーがログインしている場合はログアウトされます。
4. [Done] をクリックします。

SSH セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage のホームページで、**[Monitor]** > **[Network]** を選択します。
2. [Hostname] 列で、使用するデバイスを選択します。
3. ウィンドウの左側で、[Real Time] をクリックします。
4. [Device Options] で、[AAA users]（Cisco IOS XE SD-WAN デバイスの場合）を選択します。

   このデバイスにログインしているユーザーのリストが表示されます。

HTTP セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage のホームページで、**[Administration]** > **[Manage Users]** を選択します
2. [User Sessions] をクリックします。

   Cisco vManage 内のすべてのアクティブな HTTP セッションのリスト（ユーザー名、ドメイン、送信元 IP アドレスなどを含む）が表示されます。

CLI を使用したユーザーの設定

各デバイスでCLIを使用してユーザーログイン情報を設定できます。この方法により、追加のユーザーを作成し、それらのユーザーに特定のデバイスへのアクセス権を付与することが可能

です。CLIを使用してユーザーのための作成するログイン情報は、そのユーザーのCisco vManageログイン情報とは異なるものにすることができます。また、デバイスごとに同じユーザーの異なるログイン情報を作成できます。**netadmin** 権限を持つすべての Cisco IOS XE SD-WAN デバイス ユーザーが、新しいユーザーを作成できます。

ユーザーアカウントを作成するには、ユーザー名とパスワードを設定し、ユーザーをグループに追加します。

次の例は、既存のグループへのユーザー Bob の追加を示しています。

```
デバイス(config)# system aaa user bob group basic
```

次の例は、新しいグループ `test-group` へのユーザー Alice の追加を示しています。

```
デバイス(config)# system aaa user test-group
デバイス(config)# system aaa user alice group test-group
```

ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。一部のユーザー名は、予約されているために設定できません。予約済みユーザー名のリストについては、『Cisco SD-WAN Command Reference Guide 』で **aaa** コンフィギュレーション コマンドを参照してください。

パスワードは、ユーザーのパスワードです。各ユーザー名にはパスワードが必要であり、ユーザーは自分のパスワードを変更できます。CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。ユーザーには、 Cisco IOS XE SD-WAN デバイスにログインする際に、正しいパスワードの入力を 5 回試みることができます。5 回の試行で正しく入力できなかった場合、そのユーザーはデバイスからロックアウトされ、再度ログインを試みるまでに 15 分間待つ必要があります。

グループ名は、Cisco SD-WAN の標準グループの名前（**basic**、**netadmin**、または **operator**）か、 **usergroup** コマンド（後述）で設定されたグループの名前です。管理者ユーザーがグループを変更することによってユーザーの権限を変更する場合、そのユーザーは、そのときにデバイスにログインしているとログアウトされ、再度ログインする必要があります。

admin ユーザー名の工場出荷時のデフォルトパスワードは、admin です。 Cisco IOS XE SD-WAN デバイスを最初に設定するときに、このパスワードを変更することを強く推奨します。

```
デバイス(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

パスワードは、ASCII 文字列で設定します。次の例のように、CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。

```
デバイス(config)# show run
...
aaa authentication login default local
aaa authentication login user1 group basic
aaa authentication login user2 group operator
aaa authentication login user3 group netadmin
aaa authorization exec default local
```

RADIUS を使用して AAA 認証を実行している場合は、パスワードを確認するように特定の RADIUS サーバーを設定できます。

```
デバイス(config)#  radius server tag
```

タグは、**radius server tag** コマンドで定義した文字列です（『Cisco SD-WAN Command Reference Guide』を参照）。

Cisco vManage でのセッションの設定

表 *6 :* 機能の履歴

機能の履歴	リリース情報	説明
Cisco vManage でのセッションの設定	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、Cisco vManage の内部で開いているすべての HTTP セッションを確認できます。ユーザー名、送信元 IP アドレス、ユーザーのドメイン、およびその他の情報の詳細が表示されます。ユーザー管理書き込みアクセス権を持つユーザー（netadmin ユーザー）は、疑わしいユーザーのセッションのログアウトをトリガーできます。

Cisco vManage でのクライアント セッション タイムアウトの設定

Cisco vManage でクライアント セッション タイムアウトを設定できます。タイムアウトが設定されている場合（キーボードまたはキーストロークアクティビティがないときのタイムアウトなど）、クライアントはシステムから自動的にログアウトされます。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します。
2. [Client Session Timeout] をクリックします。
3. [Edit] をクリックします。
4. [Enabled] をクリックします。
5. タイムアウト値を分単位で指定します。
6. [保存（Save）] をクリックします。

Cisco vManage でのセッションライフタイムの設定

セッションライフタイムを分単位で設定することにより、セッションをアクティブにしておく時間を指定できます。セッションライフタイムは、セッションをアクティブにしておくことができる時間を示します。

デフォルトのセッションライフタイムは 1440 分間（24 時間）です。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します
2. [Session Life Time] をクリックします。
3. [Edit] をクリックします。
4. [SessionLifeTime] フィールドで、セッションタイムアウト値（分単位）をドロップダウンリストから指定します。
5. [保存（Save）] をクリックします。

Cisco vManage でのサーバー セッション タイムアウトの設定

Cisco vManage でサーバー セッション タイムアウトを設定できます。サーバー セッション タイムアウトは、非アクティブが原因で期限切れになるまでにサーバーがセッションの動作を維持する必要がある時間を示します。デフォルトのサーバー セッション タイムアウトは 30 分です。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します
2. [Server Session Timeout] をクリックします。
3. [Edit] をクリックします。
4. [Timeout(minutes)] フィールドで、タイムアウト値を分単位で指定します。
5. [保存（Save）] をクリックします。

ユーザーあたりの最大セッション数の有効化

ユーザー名ごとに許可される同時HTTPセッションの最大数を有効にすることができます。値として 2 を入力する場合、2 つの同時 HTTP セッションのみを開くことができます。同じユーザー名で 3 つ目の HTTP セッションを開こうとすると、3 つ目のセッションにアクセス権が付与され、最も古いセッションがログアウトされます。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します
2. [Max Sessions Per User] をクリックします。
3. [Edit] をクリックします。
4. [Enabled] をクリックします。

   デフォルトでは、[Max Sessions Per User] は [Disabled] に設定されています。
5. [Max Sessions Per User] フィールドで、ユーザーセッションの最大数の値を指定します。
6. [保存（Save）] をクリックします。

NTP アドレスの設定

このセクションのトピックでは、Network Time Protocol（NTP）アドレスの設定方法について説明します。

官公庁向け Cisco SD-WAN オーバーレイネットワークの NTP

Cisco SD-WAN セルフサービスポータル（SSP）が Cisco SD-WAN オーバーレイネットワークを作成すると、そのオーバーレイネットワークの NTP サーバーが自動的に設定されます。設定されるサーバーは、米国国立標準技術研究所認証済み（NIST 認証済み）NTP サーバーです。ログを表示する場合、ログのタイムスタンプは、これらの NTP サーバーに対応します。

Cisco SD-WAN SSP は、次のように、オーバーレイネットワークに関して選択した場所に基づいて NTP サーバーを決定します。

- [US Gov West (California)]：コロラド州の NTP サーバー
- [US Gov East (Maryland)]：メリーランド州の NTP サーバー

すべての管理仮想プライベートクラウド（VPC）は、**US Government Cloud West** でホストされます。そのため、これらの VPC に対して設定される NTP サーバーは、コロラド州の NTP サーバーです。

任意で、次のセクションの説明に従って、NTP サーバーを設定できます。

Cisco vManage を使用した NTP サーバーの設定

Cisco オーバーレイネットワーク内のすべてのデバイスで時刻を同期するために、デバイスで NTP サーバーを設定します。最大 4 つの NTP サーバーを設定できます。これらのサーバーはすべて、同じ VPN 内に配置されているか、同じ VPN 内で到達可能である必要があります。

他のデバイスは Cisco SD-WAN デバイスに時刻を問い合わせることはできますが、Cisco SD-WAN デバイスを NTP サーバーとして使用することはできません。

Cisco vManage テンプレートを使用して NTP サーバーを設定するには、次の手順に従います。

1. このセクションの説明に従って、NTP パラメータを設定する NTP 機能テンプレートを作成します。
2. システムテンプレートでタイムゾーンを設定します。

テンプレートの命名

1. Cisco vManage のホームページで、**[Configuration]** > **[Templates]** を選択します。
2. [Device] タブで、[Create Template] をクリックします。
3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。

4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Basic Information] タブをクリックします。
6. ウィンドウの右側にある [Additional Cisco System Templates] で、[NTP] をクリックします。
7. [NTP] ドロップダウンリストから、[Create Template] を選択します。

   [Cisco NTP] テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはNTPパラメータを定義するためのフィールドがあります。
8. [テンプレート名（Template Name）] フィールドに、テンプレートの名前を入力します。

   名前の最大長は 128 文字で、英数字のみを使用できます。
9. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある範囲のドロップダウンリストをクリックし、次のいずれかを選択します。

表 7: パラメータの範囲の設定

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。デバイステンプレートをデバイスに適用するときに、値を入力します。 [Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに1つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。デバイステンプレートをデバイスに適用するときに、この CSV ファイルをアップロードします。詳細については、「テンプレート変数のスプレッドシートの作成」を参照してください。 デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。 デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。

パラメータの範囲	範囲の説明
グローバル（地球のアイコンで示される）	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。

NTP サーバーの設定

NTP サーバーを設定するには、[Server] タブをクリックし、[Add New Server] をクリックして、次のパラメータを設定します。NTP サーバーを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *8 : NTP* サーバを設定するためのパラメータ

パラメータ名	説明
ホスト名/IP アドレス*	NTP サーバーの IP アドレスか、NTP サーバーへの到達方法を認識している DNS サーバーの IP アドレスを入力します。
認証キー ID*	MD5 認証を有効にするために、NTP サーバーに関連付けられた MD5 キーを指定します。キーを機能させるには、[Authentication] タブの [Trusted Keys] フィールドで、信頼できるものとしてマークする必要があります（後で説明します）。
VPN ID*	NTP サーバーに到達するために使用する必要がある VPN の番号か、NTP サーバーが配置されている VPN の番号を入力します。複数の NTP サーバーを設定している場合は、すべての NTP サーバーが、同じ VPN 内に配置されているか、同じ VPN 内で到達可能である必要があります。 有効な範囲は 0 ～ 65535 です。
バージョン*	NTP プロトコルソフトウェアのバージョン番号を入力します。範囲は 1 ～ 4 です。デフォルトは 4 です。
送信元インターフェイス	NTP パケットの発信に使用する特定のインターフェイスの名前を入力します。このインターフェイスは、NTP サーバーと同じ VPN 内にある必要があります。そうでない場合、設定は無視されます。
prefer	複数の NTP サーバーが同じストラタムレベルにあり、そのうちの 1 つを優先する場合は、[On] をクリックします。異なるストラタムレベルのサーバーについては、ソフトウェアは、最上位のストラタムレベルのサーバーを選択します。

NTP サーバーを追加するには、[Add] をクリックします。

別の NTP サーバーを追加するには、[Add NTP Server] をクリックします。最大 4 台の NTP サーバを設定できます。Cisco SD-WAN ソフトウェアは、最上位のストラタムレベルのサーバーを使用します。

NTP サーバーを編集するには、エントリの右側にある鉛筆のアイコンをクリックします。

NTP サーバーを削除するには、エントリの右側にあるゴミ箱のアイコンをクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

NTP 認証キーの設定

NTP サーバーの認証に使用する認証キーを設定するには、[Authentication] タブをクリックし、[Authentication Key] タブをクリックします。次に、[New Authentication Key] をクリックし、次のパラメータを設定します。認証キーを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *9 : NTP* 認証キーを設定するためのパラメータ

パラメータ名	説明
認証キー ID*	次の値を入力します。 • [Authentication Key]：MD5 認証キー ID を入力します。有効な範囲は 1 ～ 65535 です。 • [Authentication Value]：クリアテキストキーまたは AES 暗号化キーを入力します。
認証値*	MD5 認証キーを入力します。このキーを使用するには、信頼できるキーとして指定する必要があります。キーをサーバーに関連付けるには、[Server] タブの [Authentication Key ID] フィールドに入力したものと同じ値を入力します。

NTP サーバーの認証に使用する信頼できるキーを設定するには、[Authentication] タブで、[Trusted Key] タブをクリックし、次のパラメータを設定します。

表 *10 :* 信頼できるキーを設定するためのパラメータ

パラメータ名	説明
信頼できるキー*	キーを信頼できるものとして指定するには、MD5 認証キーを入力します。このキーをサーバーに関連付けるには、[Server] タブの [Authentication Key ID] フィールドに入力したものと同じ値を入力します。

ドメイン ネーム システム セキュリティ拡張の設定

このセクションのトピックでは、ドメイン ネーム システム セキュリティ拡張（DNSSEC）の設定方法について説明します。

ドメイン ネーム システム セキュリティ拡張の概要

Cisco vManage は、NLnet Labs が開発したオープンソースプロジェクトである Unbound を使用して DNSSEC 検証を実行します。Unbound は、簡単に使用および設定できるセキュアなドメインネームシステム（DNS）リゾルバです。

DNSSECは、ドメイン名をインターネットアドレスに変換するために使用されるセキュリティのレイヤを DNS に追加します。

Unboundは、デーモン化されたローカルDNSサーバーとしてCisco vManageに統合されます。

Unbound は、次のタスクを実行します。

- DNS クエリをローカルアプリケーションから DNS サーバーに転送します。
- DNS サーバーからの応答を検証し、アプリケーションからのクエリに応答します。
- DNS サーバーの解決の結果をキャッシュします。

DNSSEC の応答を検証するために、DNSSEC サーバー（Cisco vManage で動作しているローカル Unbound サーバー）は、信頼するための特定のキーで設定されている必要があります。

DNSエントリはDNSサーバーによって秘密キーを使用して署名され、公開キーはそのサーバーによってDNSKEY リソースレコード（RR）として返されます。DNSKEY RR はハッシュ化され、親ゾーンのDNSサーバーが、そのハッシュを保存し、委任署名者RRとして公開します。

デフォルトでは、Unbound ドメインネームシステムを、ルート委任署名者と DNSKEY RR を自動的にダウンロードして信頼するように設定できます。また、auto-trust-anchor-file 設定オプションを使用すると、ルート委任署名者とDNSKEY RR を最新の状態に保つように設定することができます。

（注） Cisco SD-WAN RESTful API を使用して DNSSEC 検証を設定します。

ドメイン ネーム システム セキュリティ拡張のユースケース

多くの官公庁機関は、Cisco vManage へのログインを試みるユーザーを認証するための独自の ID プロバイダー（IdP）またはシングルサインオン（SSO）メカニズムを保有しています。たとえば、社会保障のためにsso.ssa.govが使用されているとします。このドメイン名は、設定済みのプライベート DNS サーバー（DNSSEC にも対応）によって解決される必要があります。これにより、ネームサーバーリクエストのスプーフィングによる Cisco vManage の潜在的な

DDoS 攻撃が防御されます。プライベート DNS サーバーが侵害されると、応答署名が一致しないため、転送は行われません。

CLI を使用したドメイン ネーム システム セキュリティ拡張の設定

DNSSEC 検証を有効にするには、**request dnssec start** CLI コマンドを使用します。DNSSEC 検証を無効にするには、**request dnssec stop** CLI コマンドを使用します。

次のように、**restart** コマンドまたは **status** コマンドを使用して、DNSSEC サーバーを再起動したり、そのステータスを確認することもできます。

```
vmanage# request dnssec ?
Description: Enable or disable DNSSEC server
Possible completions:
  restart   restart the unbound server
  start     start the unbound server
  status    show unbound server status information
  stop      stop the unbound server
```

（注） すでに DNSSEC に対応している Amazon Web Services（AWS）などのクラウド環境では、DNSSEC を無効にする必要がある場合があります。

FIPS が有効になっていることの確認

連邦情報処理標準（FIPS）が有効になっていることを確認するには、Cisco vManage の vshell で次のコマンドを実行します。

```
openssl version -a
```

Cisco vManage の CLI から次のコマンドを実行して、FIPS が有効になっているかどうかを確認することもできます。

```
show system status
```

Web サーバ証明書

シスコは Cisco vManage 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 / .sdwa.cisco.com` vManage 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 SD-WAN の『スタートアップガイド』の「Web サーバー証明書」の項を参照してください。

Web サーバー証明書失効日の表示

認証証明書を使用して Web ブラウザと Cisco vManage サーバーの間のセキュアな接続を確立するときは、証明書の有効期間を設定します（前のセクションの手順 8）。この期間が終了すると、証明書が期限切れになります。ウィンドウの [Web Server Certificate] バーに、有効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 vManage ダッシュボードに表示されます。この通知は、有効期限の 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。

コントローラの Cisco 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。

Cisco vManage 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 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 SD-WAN に提供済み）
2. Symantec/Digicert Root CA（すべてのコントローラ、Cisco SD-WAN デバイス、および Cisco IOS XE 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 SD-WAN コントローラ証明書」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。
- クラウド インフラストラクチャ チームは、お客様の証明書を自動的に更新しません。

- [Cisco vManage 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 vManage 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 vManage]** > **[Configuration]** > **[Certificates]** > **[Controllers]** で、いつでも確認できます。
- シスコ クラウドインフラストラクチャ 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強くお勧めします。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。

Symantec プロセスの証明書の設定

各コントローラデバイスで証明書を自動的に生成、署名、およびインストールするように Symantec 署名サーバーを設定するには、次の手順に従います。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** 画面を選択します。
2. [Controller Certificate Authorization] バーの右側にある [Edit] をクリックします。
3. [Symantec Automated] をクリックします。これは、コントローラが署名した証明書の処理に推奨される方式です。
4. 証明書リクエスト送信者の姓と名を入力します。
5. 証明書リクエスト送信者の電子メールアドレスを入力します。このアドレスは、電子メールを使用して署名付き証明書と確認電子メールをリクエスト送信者に送信するために必要です。署名済み証明書と確認電子メールは、カスタマーポータルでも入手できます。
6. 証明書の有効期間を指定します。1 年、2 年、または 3 年を指定できます。
7. チャレンジフレーズを入力します。チャレンジフレーズは証明書のパスワードであり、証明書を更新するときや失効させるときに必要です。

（注） チャレンジフレーズは、証明書の暗号化に使用されます。証明書を紛失した場合は、チャレンジフレーズを使用して Symantec の DigiCert ポータルからその特定の証明書を取得できます。Symantec の自動または手動方式で証明書を更新できます。

自動方式の場合は、Cisco vManage の **[Administration]** > **[Settings]** 画面で、名前、電子メールアドレス、およびチャレンジフレーズを入力します。CSR が生成されると、この情報を使用して自動的に、Symantec ポータルに登録され、承認済み証明書が Symantec から受信され、インストールされます。

手動方式の場合は、Symantec の DigiCert ポータルで、名前、電子メールアドレス、およびチャレンジフレーズを入力します。

8. チャレンジフレーズを確認します。
9. [Certificate Retrieve Interval] フィールドで、Symantec 署名サーバーが証明書を送信したかどうかを Cisco vManage サーバーが確認する頻度を指定します。
10. [保存（Save）] をクリックします。

エンタープライズルート証明書のインストール

Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラ にエンタープライズルート証明書をインストールできます。

デフォルトでは、エンタープライズルート証明書には次のプロパティがあります。

- 国：United States
- 州：California
- 市：San Jose
- 組織単位：ENB
- 組織：CISCO
- ドメイン名：cisco.com
- 電子メール：cisco-cloudops-sdwan@cisco.com

この情報を表示するには、コントローラデバイスで **show certificate signing-request decoded** コマンドを使用し、Subject 行の出力を確認します。次に例を示します。

```
vSmart# show certificate signing-request decoded
.
.
.
Subject: C=US, ST=California, L=San Jose, OU=vIPtela Inc Regression, O=vIPtela Inc,
CN=vsmart-uuid.viptela.com/emailAddress=support@viptela.com
.
```

.
.

エンタープライズルート証明書をインストールするには、次の手順に従います。

1. Cisco vManage のホームページで、**[Administration]** > **[Settings]** を選択します。
2. [Controller Certificate Authorization] バーの右側にある [Edit] をクリックします。
3. [Enterprise Root Certificate] をクリックします。
4. [Certificate] フィールドで、エンタープライズルート証明書を貼り付けるか、[Select a file] をクリックして証明書を含むファイルをアップロードします。
5. 1 つ以上のデフォルト CSR プロパティを変更するには、次の手順に従います。
   1. [Set CSR Properties] をクリックします。
   2. CSR に含めるドメイン名を入力します。このドメイン名は、証明書番号（CN）に付加されます。
   3. CSR に含める組織単位（OU）を入力します。
   4. CSR に含める組織（O）を入力します。
   5. CSR に含める市（L）、州（ST）、および 2 文字の国コード（C）を入力します。
   6. 証明書リクエスト送信者の電子メールアドレス（emailAddress）を入力します。
   7. 証明書の有効期間を指定します。1 年、2 年、または 3 年を指定できます。
6. [Import & Save] をクリックします。

（注） シスコでは、現在、Cisco vManage の Web 証明書を発行していません。CSR を生成し、ドメインネームシステム（DNS）名の CA の署名を得ることをお勧めします。IP の DNS サーバーに A エントリを追加するか、Cisco vManage DNS 名に CNAME を追加する必要があります。

デバイスから Cisco vManage へのセキュアな接続

このセクションのトピックでは、デバイスから Cisco vManage への接続を保護する方法について説明します。

コントロール プレーン セキュリティの概要

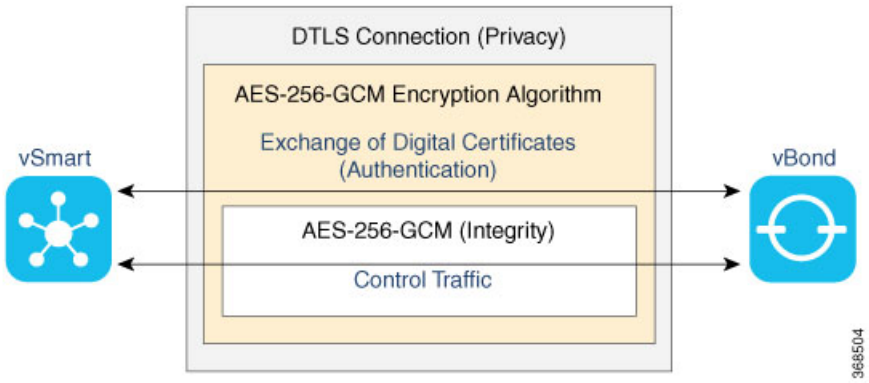
どのネットワークのコントロールプレーンも、ネットワークトポロジを決定し、パケットの転送方法を定義します。従来のネットワークでは、ルーティングテーブルと転送テーブルを構築および維持し、パケットを宛先に転送するコントロールプレーンの動作は、ルーティングプロトコルとスイッチングプロトコルによって処理されます。通常、これらのプロトコルは、デバ

イスの認証や、ルーティング更新またはその他の制御情報の暗号化に関するメカニズムをほとんど、またはまったく提供しません。さらに、セキュリティを提供する従来の方法は手動であり、拡張できません。たとえば、証明書は、通常、自動化された方法ではなく手動でインストールされます。また、事前共有キーを使用することは、デバイスのセキュリティを確保する上でセキュアなアプローチではありません。

Cisco SD-WAN コントロールプレーンは、ネットワークとデバイスのセキュリティを考慮して設計されています。コントロールプレーンの基盤となるのは、セキュアソケットレイヤ（SSL）から派生した 2 つのセキュリティプロトコルである Datagram Transport Layer Security（DTLS）プロトコルと Transport Layer Security（TLS）プロトコルのいずれかです。Cisco SD-WAN ソリューションの中核である Cisco vSmart コントローラ は、オーバーレイネットワーク内のすべての Cisco SD-WAN デバイス（ルータ、Cisco vBond オーケストレーション、Cisco vManage、およびその他の Cisco vSmart コントローラ）への DTLS または TLS 接続を確立し、維持します。これらの接続により、コントロールプレーン トラフィックが伝送されます。DTLS または TLS は、Advanced Encryption Standard（AES-256）暗号化アルゴリズムを使用して、接続を介して送信されるすべての制御トラフィックを暗号化することで、ネットワーク内の Cisco SD-WAN デバイス間の通信プライバシーを提供します。

DTLS および TLS によって提供されるコントロールプレーンのプライバシーと暗号化は、他の 2 つのセキュリティコンポーネントである認証と完全性に対して安全でセキュアな基盤を提供します。認証を実行するために、Cisco SD-WAN デバイスは、デジタル証明書を交換します。これらの証明書（デバイスに応じて、ソフトウェアによってインストールされるか、ハードウェアにハードコードされる）によってデバイスが識別され、ネットワークに属しているものと偽装しているものをデバイス自体が自動的に判別することが可能になります。完全性のために、DTLS または TLS 接続では AES-256-GCM が実行されます。これは、暗号化と完全性を提供する認証付き暗号（AEAD）であり、接続を介して送信されるすべての制御およびデータトラフィックが改ざんされていないことを保証します。

図 *2 : Cisco SD-WAN*コントロール プレーンの概要



DTLS または TLS 接続によって提供されるプライバシーで機能するコントロールプレーンのセキュリティコンポーネントは、次のとおりです。

- AES-256-GCM：このアルゴリズムは暗号化サービスを提供します。
- デジタル証明書：これらは認証に使用されます。

• AES-256-GCM：これは完全性の確保を担当します。

データプレーンセキュリティの概要

ネットワークのデータプレーンは、ネットワークを介して転送されるデータパケットを処理を担当します。データプレーンは「フォワーディングプレーン」とも呼ばれます。従来のネットワークでは、データパケットは、通常、インターネットまたは別のタイプのパブリック IP クラウドを介して直接送信されますが、MPLS トンネルを介して送信されることもあります。Cisco SD-WAN オーバーレイネットワークのルータがパブリック IP クラウドを介してトラフィックを送信する場合、その送信はセキュアではありません。誰でもトラフィックを傍受し、中間者（MITM）攻撃を含むさまざまなタイプの攻撃を実装できます。

Cisco SD-WAN データプレーンにおけるセキュリティの基盤は、コントロールプレーンのセキュリティです。コントロールプレーンは、すべてのデバイスが検証され、制御トラフィックが暗号化されて改ざんできないため、セキュアです。そのため、安心して、コントロールプレーンから学習したルートやその他の情報を使用して、ルータのネットワーク全体でセキュアなデータパスを作成および維持できます。

データプレーンは、Cisco SD-WAN オーバーレイネットワーク内のルータ間でデータトラフィックを送信するためのインフラストラクチャを提供します。データプレーントラフィックは、セキュアなインターネットセキュリティ（IPsec）接続内を移動します。Cisco SD-WAN のデータプレーンは、図に示すように、認証、暗号化、および完全性の主要なセキュリティコンポーネントを実装します。

図 *3 : Cisco SD-WAN* のデータプレーンの概要

• 認証：前述のように、Cisco SD-WAN のコントロールプレーンは、データプレーンセキュリティの基盤となるインフラストラクチャを提供します。さらに、認証は、別の 2 つのメカニズムによって実行されます。

  • 従来のキー交換モデルでは、Cisco vSmart コントローラ は、各エッジデバイスに IPsec 暗号キーを送信します。

    ペアワイズキーモデルでは、Cisco vSmart コントローラ は、エッジデバイスに Diffie-Hellman 公開値を送信し、楕円曲線 Diffie-Hellman（ECDH）と P-384 曲線を使用してペアワイズ IPsec 暗号キーを生成します。詳細については、ペアワイズキーを参照してください。

  • デフォルトでは、IPsec トンネル接続は、IPsec トンネルでの認証に Encapsulating Security Payload（ESP）プロトコルの修正バージョンを使用します。

• 暗号化：ESP の修正バージョンは、データパケットのペイロードを保護します。このバージョンのプロトコルは、外側の IP ヘッダーと UDP ヘッダーもチェックします。そのた

め、このオプションは、認証ヘッダー（AH）プロトコルと同様のパケットの完全性チェックをサポートします。データの暗号化は、AES-GCM-256 暗号を使用して行われます。

- 完全性：データトラフィックが改ざんされることなくネットワークを介して送信されることを保証するために、データプレーンは、IPsec セキュリティ プロトコル スイートのいくつかのメカニズムを実装します。
  - ESP プロトコルの修正バージョンは、データパケットのペイロードをカプセル化します。
  - ESP の修正バージョンは、AH のようなメカニズムを使用して、外側の IP ヘッダーと UDP ヘッダーの完全性をチェックします。各ルータでサポートされる完全性方式を設定できます。この情報は、ルータの TLOC プロパティで交換されます。2 つのピアが異なる認証タイプをアドバタイズする場合、それらのピアは、使用するタイプをネゴシエートし、最も強力な方式を選択します。
  - アンチリプレイスキームは、攻撃者が暗号化されたパケットを複製する攻撃を防御します。

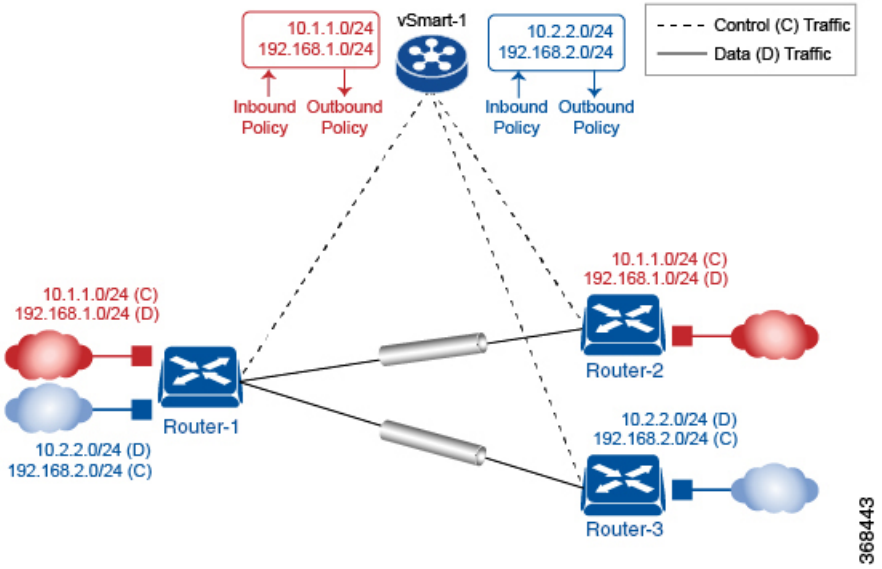
Cisco SD-WAN でのセグメンテーション

Cisco SD-WAN オーバーレイネットワークでは、 VRF が、ネットワークを異なるセグメントに分割します。

Cisco SD-WAN では、より一般的で拡張性に優れたセグメント作成モデルが採用されます。基本的に、セグメンテーションはルータのエッジで行われ、セグメンテーション情報は識別子の形式でパケットで伝送されます。

図は、 VRF 内のルーティング情報の伝播を示しています。

図 *4 : VRF* 内のルーティング情報の伝播



この図では次のようになっています。

- Router-1 は、2 つの VRF（赤色と青色）に登録します。
  - 赤色の VRF は、プレフィックス 10.1.1.0/24 に対応します（接続されたインターフェイスを介して直接、または IGP や BGP を使用して学習されます）。
  - 青色の VRF は、プレフィックス 10.2.2.0/24 に対応します（接続されたインターフェイスを介して直接、または IGP や BGP を使用して学習されます）。
- Router-2 は、赤色の VRF に登録します。
  - この VRF は、プレフィックス 192.168.1.0/24 に対応します（接続されたインターフェイスを介して直接、または IGP や BGP を使用して学習されます）。
- Router-3 は、青色の VRF に登録します。
  - この VRF は、プレフィックス 192.168.2.0/24 に対応します（接続されたインターフェイスを介して直接、または IGP や BGP を使用して学習されます）。

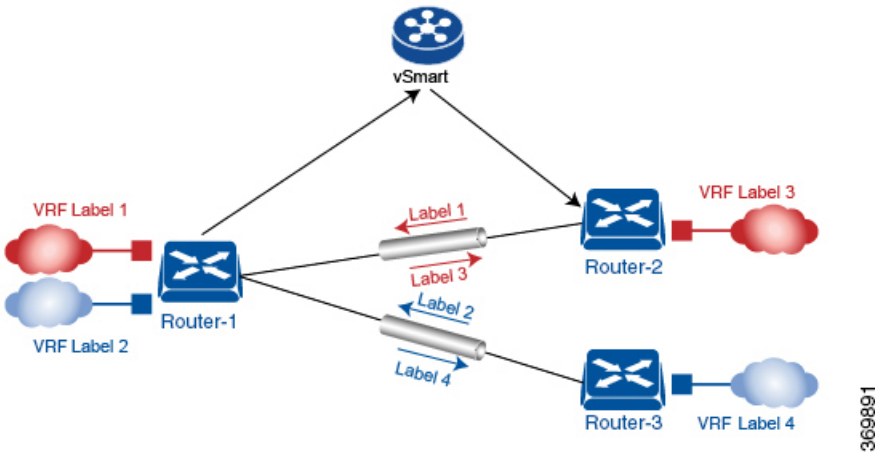
各ルータは、Cisco vSmart コントローラ への TLS トンネルを介した Overlay Management Protocol（OMP）接続を持つため、そのルーティング情報を Cisco vSmart コントローラ に伝播します。Cisco vSmart コントローラ で、ネットワーク管理者は、ポリシーを適用して、ルートをドロップしたり、トラフィックエンジニアリングまたはサービスチェーン構築のために、オーバーレイネクストホップである TLOC を変更することができます（詳細については、「ポリシーの概要」を参照）。ネットワーク管理者は、これらのポリシーをインバウンドポリシーおよびアウトバウンドポリシーとして Cisco vSmart コントローラ に適用できます。

単一の VRF に属しているすべてのプレフィックスは、別のルートテーブルに保持されます。これにより、ネットワーク内のさまざまなセグメントに必要なレイヤ 3 分離が実現されます。そのため、Router-1 には 2 つの VRF ルートテーブルがあり、Router-2 と Router-3 にはそれぞれ 1 つのルートテーブルがあります。さらに、Cisco vSmart コントローラ は、各プレフィックスの VRF コンテキストを維持します。

個別のルートテーブルにより、単一ノードの分離が実現されます。では、ルーティング情報はネットワーク全体にどのように伝播されるのでしょうか。

Cisco SD-WAN ソリューションでは、次の図に示すように、VRF 識別子を使用して、それが実行されます。パケットで伝送される VRF ID により、リンク上の各 VRF が識別されます。ルータで VRF を設定すると、 VRF にラベルが関連付けられます。ルータは、このラベルを VRF ID とともに Cisco vSmart コントローラ に送信します。Cisco vSmart コントローラ は、このルータと VRF ID のマッピング情報をドメイン内の他のルータに伝播します。その後、リモートルータは、このラベルを使用して、適切な VRF にトラフィックを送信します。ローカルルータは、VRF ID ラベルが付いたデータを受信すると、そのラベルを使用してデータトラフィックを逆多重化します。これは、MPLS ラベルの使用方法に似ています。この設計は標準 RFC に基づいており、PCI や HIPAA などの規制手順に準拠しています。

図 *5 : VRF* 識別子



（注） ルータを接続するトランスポートネットワークは、 VRF をまったく認識しません。ルータのみが VRF を認識します。ネットワークの残りの部分は、標準 IP ルーティングに従います。

Cisco SD-WAN セグメンテーションで使用される VRF

Cisco SD-WAN ソリューションでは、VRF を使用してトラフィックを分離します。

グローバル VRF

グローバル VRF はトランスポートに使用されます。サービス（企業に属するプレフィックスなど）とトランスポート（ルータを接続するネットワーク）を本質的に分離するために、すべてのトランスポート インターフェイス（つまり、すべての TLOC）がグローバル VRF で保持されます。これにより、デフォルトでは、トランスポートネットワークがサービスネットワークに到達できなくなります。複数のトランスポート インターフェイスが同じ VRF に属することができ、それらのトランスポート インターフェイス間でパケットを転送できます。

グローバル VPN には管理インターフェイスを除くデバイスのすべてのインターフェイスが含まれており、すべてのインターフェイスが無効になっています。オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、グローバル VRF でトンネルインターフェイスを設定する必要があります。グローバル VRF のインターフェイスごとに、IP アドレスを設定するとともに、WAN トランスポート接続の色とカプセル化を設定するトンネル接続を作成する必要があります（カプセル化はデータトラフィックの送信に使用されます）。これらの3つのパラメータ（IPアドレス、色、およびカプセル化）により、ルータ上の TLOC（トランスポートロケーション）が定義されます。各トンネルで動作する OMP セッションでは、オーバーレイ ネットワーク トポロジを学習できるようにCisco vSmart コントローラ に TLOC が送信されます。

トランスポート VPN でのデュアルスタックのサポート

グローバル VRF では、Cisco IOS XE SD-WAN デバイス および vSmart コントローラがデュアルスタックをサポートします。デュアルスタックを有効にするには、トンネルインターフェイスで IPv4 アドレスと IPv6 アドレスを設定します。ルータは、宛先が IPv4 アドレスまたは IPv6 アドレスをサポートしているかどうかを Cisco vSmart コントローラから学習します。トラフィックを転送する場合、ルータは、宛先アドレスに基づいて、IPv4 TLOC または IPv6 TLOC のいずれかを選択します。ただし、IPv4 が設定されている場合は、IPv4 が常に優先されます。

管理 VRF

Mgmt-Intf は Cisco IOS XE SD-WAN デバイス での管理 VRF です。これはデフォルトで設定されており、有効になっています。これにより、オーバーレイネットワーク内の Viptela デバイス間でアウトオブバンドネットワーク管理トラフィックが伝送されます。必要に応じて、この設定を変更できます。

Cisco vManage テンプレートを使用した VRF の設定

Cisco vManage では、CLI テンプレートを使用してデバイスの VRF を設定します。VRF ごとに、サブインターフェイスを設定し、そのサブインターフェイスを VRF にリンクさせます。最大 300 の VRF を設定できます。

CLI テンプレートをデバイスにプッシュすると、Cisco vManage は、デバイス上の既存の設定を上書きし、CLI テンプレートで定義された設定をロードします。そのため、テンプレートでは、設定している新しいコンテンツ（VRF など）だけを提供することはできません。CLI テンプレートには、デバイスに必要なすべての設定の詳細情報を含める必要があります。デバイスの関連する設定の詳細情報を表示するには、**show sdwan running-config** コマンドを使用します。

CLI テンプレートの作成と適用の詳細と、VRF の設定例については、『Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「CLI Templates for Cisco IOS XE SD-WAN Routers」の章を参照してください。

次のデバイスがサポートされています。

- Cisco ASR1001-HX
- ASR1002-HX