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 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。

- Cisco vManage の基本設定 （7 ページ）
- 基本システムパラメータの設定 （15 ページ）
- グローバルパラメータの設定 （22 ページ）
- Cisco vManage を使用した NTP サーバーの設定 （26 ページ）
- ルータの NTP プライマリとしての設定 （30 ページ）
- NTP の設定 （32 ページ）
- CLI を使用した時間の設定 （32 ページ）
- Cisco vManage を使用した GPS の設定 （32 ページ）
- 自動帯域幅検出の設定 （35 ページ）
- CLI を使用したシステムロギングの設定 （37 ページ）

Cisco vManage の基本設定

システムテンプレートは、システムレベルの Cisco vManage ワークフローを構成するために使用されます。

[Settings] 画面を使用して、現在の設定を表示し、組織名、vBond オーケストレータの DNS 名または IP アドレス、証明書の設定、統計情報の収集などの Cisco vManage パラメータの設定を構成します。

各項目の現在の設定は、各項目のバーの名前の直後に表示されます。

組織名の設定

証明書署名要求（CSR）を生成する前に、組織の名前を構成する必要があります。組織名は CSR に含まれます。

Public Key Infrastructure（PKI）システムでは、デジタル ID 証明書を申請するために CSR が認証局に送信されます。

組織名を設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Organization Name] で、[Edit] をクリックします。
3. [Organization Name] に、組織の名前を入力します。組織名は、vBond オーケストレータで構成されている名前と同じである必要があります。
4. [Confirm Organization Name] で、組織名を再入力して確認します。
5. **[Save]** をクリックします。

（注） 制御接続が起動して実行されると、組織名バーは編集できなくなります。

Cisco vBond のドメインネームシステム（DNS）名または IP アドレスの設定

1. [vBond] から、[Edit] をクリックします。

2. [vBond DNS/IP Address: Port] に、vBond オーケストレータを指す DNS 名とまたは Cisco vBond オーケストレータの IP アドレスと、それへの接続に使用するポート番号を入力します。
3. **[Save]** をクリックします。

（注） DNS キャッシュのタイムアウトは、DNS が解決する必要がある Cisco vBond オーケストレーション の IP アドレスの数に比例する必要があります。そうしないと、リンク障害中に Cisco vManage の制御接続が行われない可能性があります。これは、チェックする IP アドレスが 6 つ以上ある場合（デフォルトの DNS キャッシュタイムアウトは現在 2 分であるため、これは推奨数です）、最も優先されるインターフェイスがすべての vBond IP アドレスを試行しても、別の色にフェールオーバーする前に、DNS キャッシュタイマーが期限切れになるためです。たとえば、1 つの IP アドレスへの接続を試みるのに約 20 秒かかります。したがって、解決する IP アドレスが 8 つある場合、DNS キャッシュのタイムアウトは 20*8=160 秒、つまり 3 分になります。

コントローラ認証局の設定

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。これらの証明書の生成、およびコントローラデバイス（Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart コントローラ）へのインストールは、Cisco vManage から実行します。Symantec によって署名された証明書を使用することも、エンタープライズルート証明書を使用することもできます。

コントローラの認定許可設定では、すべてのコントローラデバイスの認証生成がどのように行われるのかを確立します。証明書は生成しません。

証明書生成方式を 1 回だけ選択する必要があります。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使用されます。

Symantec 署名サーバーが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するには、次の手順を実行します。

1. [Controller Certificate Authorization] から、[Edit] をクリックします。
2. [Symantec Automated] をクリックします（推奨）。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。
3. [Confirm Certificate Authorization Change] ダイアログボックスで、[Proceed] をクリックして、Symantec 署名サーバーが各コントローラデバイスに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することを確認します。
4. 証明書のリクエスト送信者の姓名を入力します。
5. 証明書の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。カスタマーポータルから利用できるようにすることもできます。

6. 証明書の有効期間を指定します。1 年、2 年、または 3 年に指定できます。
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。
8. チャレンジフレーズを確認します。
9. [Certificate Retrieve Interval] 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. **[Save]** をクリックします。

Symantec 署名サーバーが生成して署名した証明書を手動でインストールするには、次の手順を実行します。

1. [Controller Certificate Authorization] から、[Edit] をクリックします。
2. [Symantec Manual] をクリックします。
3. [Confirm Certificate Authorization Change] ダイアログボックスで、[Proceed] をクリックして、Symantec 署名サーバーが生成して署名した証明書を手動でインストールします。
4. **[Save]** をクリックします。

エンタープライズルート証明書を使用するには、次の手順を実行します。

1. [Controller Certificate Authorization] から、[Edit] をクリックします。
2. [Enterprise Root Certificate] をクリックします。
3. [Confirm Certificate Authorization Change] ダイアログボックスで、[Proceed] をクリックして、エンタープライズルート証明書を使用することを確認します。
4. [Certificate] ボックスで、証明書を貼り付けるか、[Select a file] をクリックしてエンタープライズルート証明書を含むファイルをアップロードします。
5. 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。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** コマンドを発行し、Subject 行の出力を確認します。次に例を示します。
   - 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

```
vSmart# show certificate signing-request decoded
    ...
    Subject: C=US, ST=California, L=San Jose, OU=ENB, O=CISCO, CN=vsmart-uuid
.cisco.com/emailAddress=cisco-cloudops-sdwan@cisco.com
    ...
```

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 年に指定できます。

6. [Import & Save] をクリックします。

デバイスでのソフトウェアバージョンの適用

Cisco SD-WAN ホストサービスを使用している場合は、ルータが最初にオーバーレイネットワークに参加するときに、そのバージョンの Cisco SD-WAN ソフトウェアを強制的にルータ上で実行できます。

ソフトウェアバージョンを強制するアップグレード後にテンプレートが同期されるようにするには、アップグレードを実行する前に次のことを確認してください。

- ルータのブートフラッシュとフラッシュには、アップグレードをサポートするのに十分な空き容量が必要です
- アップグレード前にデバイス上にある SD-WAN イメージのバージョンは、次の手順で指定する強制 SD-WAN バージョンよりも低いバージョンである必要があります

ルータが最初にオーバーレイネットワークに参加するときに、ルータ上で Cisco SD-WAN ソフトウェアのバージョンを強制的に実行するには、次の手順を実行します。

1. 目的のデバイス ソフトウェア バージョンのソフトウェアイメージが Cisco vManage ソフトウェア イメージ リポジトリに存在することを確認します。
   1. Cisco vManage のメニューから、**[Maintenance]** > **[Software Repository]**を選択します。

      [Software Repository] 画面が開き、ソフトウェアイメージのテーブルが表示されます。目的のソフトウェアイメージがリポジトリに存在する場合は、ステップ2に進みます。
   2. ソフトウェアイメージを追加する必要がある場合は、[Add New Software] をクリックします。

3. ソフトウェアイメージをダウンロードする場所として、Cisco vManage、[Remote Server] または [Remote Server - vManage] を選択します。
4. x86 ベースまたは MIPS ベースのソフトウェアイメージを選択します。
5. リポジトリにイメージを配置するには、[Add] をクリックします。

2. Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。
3. [Enforce Software Version (ZTP)] で、[Edit] をクリックします。
4. [Enforce Software Version] で、[Enabled] をクリックします。
5. [Version] ドロップダウンリストから、デバイスがネットワークに参加したときにデバイスに適用するソフトウェアのバージョンを選択します。
6. [Save] をクリックします。

バナー

Cisco vBond オーケストレーション、Cisco vManage、Cisco vSmart コントローラ、、および Cisco IOS XE SD-WAN デバイスのバナーテンプレートを使用します。

- Cisco vManage テンプレートを使用してログイン画面のバナーテキストを設定するには、このトピックの説明に従って、バナー機能テンプレートを作成して PIM パラメータを設定します。
- Cisco vManage システムのログインバナーを設定するには、Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。

バナーの設定

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックし、[Create Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

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. [Additional Templates] をクリックするか、[Additional Templates] セクションまでスクロールします。

6. [Banner] ドロップダウンリストから、[Create Template] をクリックします。[Banner] テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、バナーパラメータを定義するためのフィールドが含まれています。
7. [Template Name] 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。
8. [Template Description] 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、[Scope] ドロップダウンリストをクリックします。
9. バナーを設定するには、次のパラメータを設定します。

   表 *1:* バナーの設定時に設定するパラメータ：

パラメータ名	説明
MOTD Banner	Cisco IOS XE SD-WAN デバイスで、ログインバナーの前に表示する今日のメッセージのテキストを入力します。ストリングの長さは、最大 2048 文字まで可能です。改行を挿入するには、**\n** と入力します。
ログイン バナー	ログインプロンプトの前に表示するテキストを入力します。ストリングの長さは、最大 2048 文字まで可能です。改行を挿入するには、**\n** と入力します。

10. 機能テンプレートを保存するには、[Save] をクリックします。

CLI の同等の設定：

```
banner{login login-string | motd motd-string}
```

カスタムバナーの作成

Cisco vManage にログインした後に表示されるカスタムバナーを作成するには、次の手順を実行します。

1. [Banner] から、[Edit] をクリックします。
2. [Enable Banner] で、[Enabled] をクリックします。
3. [Banner Info] で、ログインバナーのテキスト文字列を入力するか、[Select a File] をクリックして、テキスト文字列を含むファイルをダウンロードします。
4. [Save] をクリックします。

デバイス統計の収集

オーバーレイネットワーク内のデバイス統計情報の収集を有効または無効にします。デフォルトでは、オーバーレイネットワーク内のすべてのデバイスで統計情報の収集が有効になっています。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. デバイス統計情報を収集するための設定を変更するには、[Statistics Setting] をクリックし、[Edit] をクリックします。

ヒント　構成された設定を表示するには、[View] をクリックします。

デフォルトでは、統計のすべてのグループ（**Aggregated DPI**、**AppHosting** など）について、すべてのデバイスの統計情報の収集が有効になっています。

3. すべてのデバイスの統計グループの収集を有効にするには、特定のグループの [Enable All] をクリックします。
4. すべてのデバイスの統計グループの収集を無効にするには、特定のグループの [Disable All] をクリックします。
5. Cisco vAnalytics でのみ使用するために、すべてのデバイスの統計グループの収集を有効にするには、特定のグループの [vAnalytics only] をクリックします。
6. オーバーレイネットワーク内の特定のデバイスの統計グループの収集を有効または無効にするには、特定のグループの [Custom] をクリックします。

   [Select Devices] ダイアログボックスでは、デバイスの統計収集が有効か無効かに応じて、デバイスは [Enabled Devices] または [Disabled Devices] にそれぞれ一覧表示されます。

   1. 1 つまたは複数のデバイスの統計収集を有効にするには、[Disabled Devices] でデバイスを選択し、[Enabled Devices] に移動します。

ヒント　[Disabled Devices] のすべてを選択するには、[Select All] をクリックします。

   2. 1 つまたは複数のデバイスの統計収集を無効にするには、[Enabled Devices] でデバイスを選択し、[Disabled Devices] に移動します。

ヒント　[Enabled Devices] のすべてを選択するには、[Select All] をクリックします。

   3. 選択内容を保存するには、[Done] をクリックします。

      選択内容を破棄するには、[Cancel] をクリックします。

7. 変更した設定を適用するには、[Save] をクリックします。

変更内容を破棄するには、[Cancel] をクリックします。

デフォルト設定に戻すには、[Restore Factory Default] をクリックします。

デバイス統計を収集する時間間隔の設定

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. デバイス統計が収集される時間間隔を変更するには、[Statistics Configuration] を見つけて [Edit] をクリックします。

ヒント　設定された時間間隔を表示するには、[View] をクリックします。

3. 目的の [Collection Interval] を分単位で入力します。
   - デフォルト値：30 分
   - 最小値：5 分
   - 最大値：180 分
4. 変更した設定を適用するには、[Save] をクリックします。

   変更内容を破棄するには、[Cancel] をクリックします。

   デフォルト設定に戻すには、[Restore Factory Default] をクリックします。

vManage サーバー メンテナンス ウィンドウの設定またはキャンセル

vManage サーバーのメンテナンスウィンドウの開始時刻と終了時刻、および期間を設定またはキャンセルできます。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Maintenance Window] から、[Edit] をクリックします。

   メンテナンスウィンドウをキャンセルするには、[Cancel] をクリックします。
3. [Start date and time] ドロップダウンリストをクリックし、[Maintenance Window] を開始する日時を選択します。
4. [End date and time] ドロップダウンリストをクリックし、[Maintenance Window] を終了する日時を選択します。
5. **[Save]** をクリックします。メンテナンスウィンドウの開始時刻と終了時刻、および期間は、[Maintenance Window] バーに表示されます。

ウィンドウの開始2日前に、Cisco vManage ダッシュボードにメンテナンスウィンドウのアラート通知が表示されます。

基本システムパラメータの設定

すべての Cisco SD-WAN デバイスにシステムテンプレートを使用します。

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するには、次の手順を実行します。

1. **システム**機能テンプレートを作成して、システムパラメータを設定します。
2. **NTP** 機能テンプレートを作成して、NTP サーバーと認証を設定します。
3. Cisco vManage で、組織名および Cisco vBond オーケストレーション IP アドレスを設定します。これらの設定は、テンプレートがデバイスにプッシュされるときにデバイステンプレートに追加されます。

システムテンプレートの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [デバイス テンプレート] をクリックし、[テンプレートの作成] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

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. システムのカスタムテンプレートを作成するには、[Factory_Default_System_Template] を選択し、[Create Template] をクリックします。

   [System] テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、システムパラメータを定義するためのフィールドが含まれています。
6. [Template Name] 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。
7. [Template Description] 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 [Scope] ドロップダウンをクリックし、次のいずれかを選択します。

表 *2:*

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。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、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。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。 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。
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。

システム全体の基本設定

Cisco SD-WAN デバイスにシステム全体の機能を設定するには、[Basic Configuration] タブを選択し、次のパラメータを設定します。アスタリスクの付いたパラメータは必須です。

表 *3:*

パラメータフィールド	**Description**
Site ID*（ルータ、vManage インスタンス、および vSmart コントローラ上）	ブランチ、キャンパス、データセンターなど、デバイスが存在する Cisco SD-WAN オーバーレイ ネットワーク ドメイン内のサイトの識別子を入力します。サイト ID は、同じサイトに存在するすべての Cisco SD-WAN デバイスで同じである必要があります。 範囲：1 ～ 4294967295（$2^{32} – 1$）

パラメータフィールド	Description
System IP*	Cisco SD-WAN デバイスのシステム IP アドレスを、10 進数の 4 分割ドット表記で入力します。システム IP アドレスは、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し、デバイスの TLOC アドレスのコンポーネントです。トランスポート VPN（VPN 0）でデバイスのループバックアドレスとして使用されます。この同じアドレスを VPN 0 の別のインターフェイスに使用することはできません。
Timezone*	デバイスで使用するタイムゾーンを選択します。
ホストネーム	Cisco SD-WAN デバイスの名前を入力します。32 文字以内です。
参照先	デバイスのロケーションの説明を入力します。最大 128 文字を使用できます。
デバイスグループ	デバイスが属する 1 つ以上のグループの名前をカンマで区切って入力します。
Controller Groups	ルータが属する Cisco vSmart コントローラ グループのリスト。
説明	デバイスに関する追加の説明情報を入力します。
Console Baud Rate	ルータのコンソール接続のボーレートを選択します。値：1200、2400、4800、9600、19200、38400、57600、115200 ボーまたはビット/秒（bps）。 Cisco vManage リリース 20.3.1 以降、Cisco IOS XE SD-WAN デバイスのデフォルト値は 9600 です。
Maximum OMP Sessions	ルータが Cisco vSmart コントローラに対して確立できる OMP セッションの最大数を設定します。範囲：0 ～ 100。デフォルト：2

機能テンプレートを保存するには、[Save] をクリックします。

オーバーレイネットワークの Cisco vBond オーケストレーション の DNS 名または IP アドレスを設定するには、**[Administration]** > **[Settings]** 画面に移動し、[vBond] をクリックします。

GPS 位置情報の設定

デバイスの位置情報を設定するには、[GPS] タブを選択し、次のパラメータを設定します。この位置情報は、デバイスを Cisco vManage ネットワークマップに配置するために使用されます。位置情報を設定すると、デバイスが別の場所に移動した場合に Cisco vManage から通知を送信することもできます。

表 *4:*

パラメータフィールド	Description
Latitude	デバイスの緯度を十進角の形式で入力します。
Longitude	デバイスの経度を十進角の形式で入力します。

機能テンプレートを保存するには、[Save] をクリックします。

NAT ダイレクト インターネット アクセス用のインターフェイストラッカーの設定

DIA トラッカーは、インターネットまたは外部ネットワークが使用できなくなったかどうかを判断するのに役立ちます。この機能は、VPN 0 のトランスポート インターフェイスで NAT が有効になっている場合に役立ち、ルータからのデータトラフィックが直接インターネットに送信されるようにします。

インターネットまたは外部ネットワークが使用できなくなった場合、ルータはサービス VPN の NAT ルートに基づいてトラフィックを転送し続けます。インターネットに転送されるトラフィックはドロップされます。インターネット バウンド トラフィックがドロップされないようにするには、エッジルータで DIA トラッカーを設定して、トランスポート インターフェイスのステータスをトラッキングします。トラッカーは、トンネルインターフェイスのエンドポイントのインターフェイス IP アドレスを定期的にプローブして、トランスポートインターフェイスのステータスを判断します。トラッカーはインターネットのステータスを判断し、トラッカーに関連付けられている接続ポイントにデータを返します。

トランスポート インターフェイスでトラッカーが設定されている場合、インターフェイスの IP アドレスは、プローブパケットの送信元 IP アドレスとして使用されます。

IP SLA は、プローブのステータスをモニタリングし、これらのプローブパケットの往復時間を測定し、その値をプローブで設定された遅延と比較します。遅延が設定されたしきい値を超えると、トラッカーはネットワークを使用不可と見なします。

トラッカーがローカルインターネットが利用できないと判断した場合、ルータは NAT ルートを取り消し、ローカルルーティング設定に基づいてトラフィックをオーバーレイに再ルーティングします。

ローカルルータは、インターフェイスへのパスのステータスを定期的にチェックし続けます。パスが再び機能していることを検出すると、ルータはインターネットへの NAT ルートを再インストールします。

Cisco IOS XE SD-WAN デバイスの NAT DIA トラッカーの詳細については、『*Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE* リリース *17.x*』の「NAT DIA Tracker」セクションを参照してください。

NAT DIA トラッカーの設定

インターネットに接続するトランスポートインターフェイス（ネットワークアドレス変換ダイレクト インターネット アクセス（NAT DIA））のステータスを追跡するには、**[Tracker]** > **[Add New Tracker]** をクリックして、次のパラメータを設定します。

表 *5:*

パラメータフィールド	説明
Name	トラッカーの名前。名前には 128 文字以内の英数字を使用できます。最大 8 つのトラッカーを設定できます。
[Tracker Type]	インターフェイス、スタティックルートを選択します。
しきい値	トランスポートインターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲：100 ～ 1000 ミリ秒。デフォルト：300 ミリ秒。
インターバル	トランスポート インターフェイスのステータスを判別するためにプローブが送信される頻度。範囲：10 ～ 600 秒。デフォルト：60 秒（1 秒）
Multiplier（乗数）	トランスポートインターフェイスがダウンしていることを宣言する前にプローブを再送信する回数。範囲：1 ～ 10。デフォルト：3
[End Point Type: IP Address]	トンネルインターフェイスのエンドポイントの IP アドレス。これは、ルータがプローブを送信してトランスポート インターフェイスのステータスを判断するインターネット内の宛先です。 （注） Cisco SD-WAN リリース 20.5.1 以降のリリースでは、トラッカーが 400 未満の HTTP レスポンスステータスコードを受信した場合、エンドポイントは到達可能です。 Cisco SD-WAN リリース 20.5.1 より前では、トラッカーが HTTP レスポンスステータスコード 200 を受信した場合、エンドポイントは到達可能です。
[End Point Type: DNS Name]	トンネルインターフェイスのエンドポイントの DNS 名。これは、ルータがプローブを送信してトランスポートインターフェイスのステータスを判断するインターネット内の宛先です。

トラッカーを保存するには、[Add] 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。

CLI を使用した NAT DIA トラッカーの設定

NAT DIA トラッカーの設定

```
Device(config)# endpoint-tracker tracker1
    Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
    Device(config-endpoint-tracker)# threshold 100
    Device(config-endpoint-tracker)# multiplier 5
    Device(config-endpoint-tracker)# interval 10

Device(config)# endpoint-tracker tracker1
    Device(config-endpoint-tracker)# endpoint-api-url https://ip-address:8443/apidocs
    Device(config-endpoint-tracker)# threshold 100
```

```
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 10
```

インターフェイスへのトラッカーの適用

インターフェイスにトラッカーを適用するには、[VPN Interface Cellular]、[VPN Interface Ethernet]、[VPN Interface NAT Pool]、または [VPN Interface PPP] 設定テンプレートでトラッカーを設定します。インターフェイスに適用できるトラッカーは 1 つだけです。

NAT DIA エンドポイントトラッカー設定のモニタリング

1. Cisco vManage 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 vManage メニューから**[Monitor]** > **[Network]**の順に選択します。

2. デバイスのリストからデバイスを選択します。
3. [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、[Endpoint Tracker Info] を選択します。

詳細オプションの設定

追加のシステムパラメータを設定するには、[Advanced] をクリックします。

表 6:

パラメータ名	説明
Control Session Policer Rate	制御トラフィックのフローをポリシングするための DTLS 制御セッショントラフィックの最大レートを指定します。範囲：1 ～ 65535 pps。デフォルト：300 pps
Port Hopping	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。Cisco SD-WAN デバイスが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号（ベースポートと呼ばれる）のプールを循環して、接続の試行が失敗したときに他の Cisco SD-WAN デバイスとの DTLS 接続を確立します。デフォルトのベース ポートは 12346、12366、12386、12406、および 12426 です。ベース ポートを変更するには、ポート オフセット値を設定します。個々の TLOC（トンネルインターフェイス）でポートホッピングを無効にするには、[VPN Interface Ethernet] 設定テンプレートを使用します。デフォルト：有効（ルータ）、無効（Cisco vManage デバイスおよび Cisco vSmart コントローラ）。
Port Offset	ベースポート番号をオフセットする番号を入力します。複数の Cisco SD-WAN デバイスが 1 つの NAT デバイスの背後にある場合は、このオプションを設定して、各デバイスが DTLS 接続に一意のベースポートを使用するようにします。値：0 ～ 19

パラメータ名	説明
Track Transport	[On] をクリックすると、デバイスと Cisco vBond オーケストレーションの間の DTLS 接続が稼働しているかどうかを定期的に確認します。[Off] をクリックすると、確認は無効になります。デフォルトでは、トランスポートの確認は有効になっています。
Track Interface	非動作インターフェイスに接続されているネットワークに関連付けられたルートに含めるタグ文字列を設定します。範囲：1 ～ 4294967295
Gateway Tracking	デフォルトゲートウェイの追跡を有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ゲートウェイトラッキングにより、スタティックルートの場合、そのルートをデバイスのルートテーブルに追加する前に、ネクストホップが到達可能かどうかを判断します。デフォルト：有効
Collect Admin Tech on Reboot	デバイスの再起動時に管理技術情報を収集するには、[On] をクリックします。
アイドル タイムアウト	デバイスで CLI が非アクティブであるとユーザーがログアウトされるまでの時間を設定します。ユーザーが SSH 接続を介してデバイスに接続している場合、この時間が経過すると SSH 接続が閉じられます。範囲：0 ～ 300 秒。デフォルト：CLI セッションはタイムアウトしません。

機能テンプレートを保存するには、[Save] をクリックします。

CLI の同等の設定：

```
system
   admin-tech-on-failure  allow-same-site-tunnels
   control-session-pps rate eco-friendly-mode
   host-policer-pps rate

   icmp-error-pps rate

   idle-timeout seconds multicast-buffer-percent percentage

   port-hop  port-offset number
   system-tunnel-mtu bytes timer
    dns-cache-timeout minutes track-default-gateway
    track-interface-tag number

   track-transport  upgrade-confirm minutes
```

グローバルパラメータの設定

表 7: 機能の履歴

機能名	リリース情報	説明
グローバルパラメータの設定	Cisco IOS XE リリース 17.2.1r	この機能を使用すると、HTTP および Telnet サーバー設定、およびその他のデバイス設定を Cisco vManage で構成できます。

グローバル設定テンプレートを使用して、次の項目を含む、すべての Cisco IOS XE SD-WAN デバイス のさまざまなグローバルパラメータを設定します。

- HTTP や Telnet などの各種サービス
- NAT64 タイムアウト
- HTTP 認証モード
- TCP キープアライブ
- TCP および UDP 小規模サーバー
- コンソール ロギング
- IP ソースルーティング
- VTY 回線のロギング
- SNMP IFINDEX パーシステンス
- BOOTP サーバ

グローバルパラメータをデバイスに適用する前に、デバイスの現在の設定を表示し、グローバル設定テンプレートで設定したパラメータ値とデバイスの現在の値の相違を表示できます。

Cisco vManage を使用してグローバル設定を構成するには、次の手順を実行します。

1. 機能テンプレートを作成してグローバル設定を構成します。
2. デバイステンプレートを作成して、グローバル設定機能テンプレートを含めます。
3. （推奨）デバイステンプレートをデバイスに適用する前に、デバイス設定のプレビューと設定の相違点の表示機能を使用して、デバイスの現在の設定とデバイスに送信される設定の相違を確認します。デバイステンプレートを適用すると、デバイスの既存の設定が上書きされるため、この手順をお勧めします。

制限事項

Cisco SD-WAN は、Cisco IOS XE リリース Amsterdam 17.2.x 以降が実行されているデバイスにのみグローバル設定機能テンプレートを適用できます。

グローバル設定機能テンプレートの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. 左側ペインで、デバイスタイプを選択します。
5. [Global Settings] テンプレートを選択します。
6. テンプレートの名前と説明を入力します。
7. 各パラメータについて、デフォルトを使用するか、必要に応じてカスタム値を設定します。

パラメータ	説明
Services	
HTTP サーバー	HTTP サーバーを有効または無効にします。
HTTPS サーバ（HTTPS Server）	セキュア HTTPS サーバーを有効または無効にします。
Passive FTP	パッシブ FTP を有効または無効にします。
IP Domain-Lookup	ドメインネームサーバー（DNS）ルックアップを有効または無効にします。
Arp Proxy	プロキシ ARP を有効または無効にします。
RSH/RCP	デバイスでリモートシェル（RSH）とリモートコピー（RCP）を有効または無効にします。
Telnet（アウトバウンド）	アウトバウンド Telnet を有効または無効にします。
CDP	Cisco Discovery Protocol を有効または無効にします。Cisco SD-WAN 17.3 リリース以降、Cisco ASR 1000 シリーズ デバイスでコマンドをグローバルに実行すると、インターフェイスの CDP が有効になります。cdp run
その他の設定	

パラメータ	説明
TCP Keepalives (In)	着信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Keepalives (Out)	発信ネットワーク接続がアイドル状態のときのキープアライブタイマーの生成を有効または無効にします。
TCP Small Servers	小規模なTCPサーバー（ECHOなど）を有効または無効にします。
UDP Small Servers	小規模な UDP サーバー（ECHO など）を有効または無効にします。
Console Logging	コンソールロギングを有効または無効にします。デフォルトでは、ルータはすべてのログメッセージをコンソールポートに送信します。
IP ソース ルーティング	IP ソースルーティングを有効または無効にします。IP ソースルーティングは、パケットの発信元が、パケットが宛先に到達するために使用するパスを指定できるようにする機能です。
VTY Line Logging	デバイスがログメッセージをリアルタイムでVTYセッションに表示することを有効または無効にします。
SNMP IFINDEX Persist	デバイスの再起動時に保持および使用されるインターフェイス インデックス（ifIndex）値を提供するSNMP IINDEXパーシステンスを有効または無効にします。
Ignore BOOTP	BOOTPサーバーを有効または無効にします。有効にすると、デバイスは 0.0.0.0 から送信される bootp パケットをリッスンします。無効にすると、デバイスはこれらのパケットを無視します。
NAT64	
[UDP Timeout]	UDP の NAT64 変換タイムアウト 範囲：1 ～ 65536（秒） デフォルト：300 秒（5 分） （注） Cisco IOS XE リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [UDP Timeout] 値は 300 秒（5 分）に変更されました。

パラメータ	説明
[TCP Timeout]	TCP の NAT64 変換タイムアウト 範囲：1 ～ 65536（秒） デフォルト：3600 秒（1 時間） （注） Cisco IOS XE リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [TCP Timeout] 値は 3600 秒（1 時間）に変更されました。
HTTP Authentication	
HTTP Authentication	HTTP 認証モード 許容値：Local、AAA デフォルト：Local
SSH Version	
SSH version	SSH バージョンを指定します。 デフォルト値：バージョン 2

8. テンプレートの名前を入力し、[Save] をクリックします。

CLI での同等コマンド

サービス（有効化）：

```
system
    ip http server
    ip http secure-server
    ip ftp passive
    ip domain lookup
    ip arp proxy disable
    ip rcmd rsh-enable
    ip rcmd rcp-enable
    cdp run enable
```

（注） Cisco SD-WAN 17.3 リリース以降、Cisco ASR 1000 シリーズ デバイスでコマンドをグローバルに実行すると、インターフェイスの CDP が有効になります。**cdp run**

Telnet アウトバウンド有効化：

```
system
    line vty 0 4
        transport input telnet ssh
```

サービス（無効化）：

```
system
    no ip http server
    no ip http secure-server
    no ip ftp passive
    no ip domain lookup
    no ip arp proxy disable
    no ip rcmd rsh-enable
    no ip rcmd rcp-enable
    no cdp run enable
```

Telnet アウトバウンド無効化：

```
system
    line vty 0 4
        transport input ssh
```

その他の設定（有効化）：

```
system
    service tcp-keepalives-in
    service tcp-keepalives-out
    service tcp-small-servers
    service udp-small-server
    logging console
    ip source-route
    logging monitor
    snmp-server ifindex persist
    ip bootp server
```

その他の設定（無効化）：

```
system
    no service tcp-keepalives-in
    no service tcp-keepalives-out
    no service tcp-small-servers
    no service udp-small-server
    no logging console
    no ip source-route
    no logging monitor
    no snmp-server ifindex persist
    no ip bootp server
```

NAT 64：

```
system
    nat64 translation timeout udp timeout
    nat64 translation timeout tcp timeout
```

HTTP 認証：

```
system
    ip http authentication {local | aaa}
```

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。

（注） Cisco IOS XE SD-WAN デバイス でグローバル VRF を使用するときに NTP が正しく機能するには、Cisco VPN インターフェイス イーサネット テンプレートのトンネルインターフェイスに **allow-service ntp** を設定する必要があります。

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 メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

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] をクリックします。
6. [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。このフォームには、テンプレートに名前を付けるためのフィールドと、NTP パラメータを定義するためのフィールドが含まれています。
8. [Template Name] 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] 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 *8:* 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。デバイスをデバイステンプレートに添付するときに、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。デバイスをデバイステンプレートに添付するときに、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。
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] 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 *9: NTP* サーバー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] 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）。

パラメータ名	説明
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 サーバーを設定できます。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ごみ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] をクリックし、[Authentication Key] 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 *10* : *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] の [Authentication Key ID] フィールドに入力した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] で、[Trusted Key] をクリックし、次のパラメータを設定します。

表 *11* : 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] の [Authentication Key ID] フィールドに入力したのと同じ値を入力します。

ルータの NTP プライマリとしての設定

表 *12* : 機能の履歴

機能名	リリース情報	説明
ルータの NTP プライマリとしての設定	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、サポートされているルータを NTP プライマリルータとして設定できます。Cisco SD-WAN 展開内の他のノードは、NTP プライマリルータにクロックを同期します。この設定は、展開内に NTP サーバーがない場合に役立ちます。

サポートされている 1 つまたは複数のルータを、Cisco SD-WAN 展開内の NTP プライマリルータとして設定できます。このように設定されたルータは、展開内の他のノードがクロックを同期する NTP サーバーとして機能します。

展開内に NTP サーバーがない場合は、ルータを NTP プライマリルータとして設定すると便利です。

ルータを NTP プライマリルータとして設定するには、NTP プライマリルータの設定パラメータを含むテンプレートを作成します。これを行うには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. 次のいずれかの操作を行います。
   - 新しいテンプレートを作成するには、[Feature Templates] で [Add Template] をクリックし、NTP プライマリルータにするデバイスのタイプを選択してから、[Basic Information] テンプレートのグループで [NTP] テンプレートを選択します。

（注） Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

   - 既存のテンプレートを更新するには、[...] をクリックし、[Edit] をクリックします。
3. 必要に応じてテンプレートのオプションを設定し、[Master] タブで次の操作を実行します。
   1. [Master] オプションで、ドロップダウンリストから [Global] を選択し、[On] を選択します。
   2. （オプション）[Stratum] フィールドに、NTP プライマリルータのストラタム値を入力します。

      ストラタム値は、基準クロックからのルータの階層的距離を定義します。

      有効な範囲：1 ～ 15 の整数値を入力しない場合、システムはルータの内部クロックのデフォルトストラタム値である 8 を使用します。
   3. （オプション）[Source] フィールドに NTP 通信の出口インターフェイスの名前を入力します。

      設定されている場合、システムは NTP トラフィックをこのインターフェイスに送信します。

      たとえば、**GigabitEthernet1** または **Loopback0** と入力します。
4. [Save]（新しいテンプレートの場合）または [Update]（既存のテンプレートの場合）をクリックします。

CLI の同等の設定：

```
ntp master [stratum-number]
ntp source source-interface
```

NTP の設定

NTP を使用したネットワーク全体の時刻の構成

Cisco SD-WAN オーバーレイネットワーク内のすべてのデバイス間で時間を調整および同期するには、各デバイスで NTP サーバーの IP アドレスまたは DNS サーバーアドレスを構成します。Cisco IOS XE リリース 17.9.1a で始まる NTP サーバーの IP アドレスは、ブロードキャストまたはマルチキャストアドレスにすることはできません。

```
config-terminal
   ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

CLI を使用した時間の設定

デバイスのネットワーク全体で時間を同期させる必要がない場合は、NTP を使用せずにローカルで時間を設定できます。NTP サーバーの設定に加えて、ネットワークに参加する任意のデバイスでローカルに時間を設定することもできます。デバイスが NTP サーバーに接続すると、ローカル時間は公式の NTP 時間で上書きされます。

```
clock set 12:00:00 31 May 2019
```

Cisco vManage を使用した GPS の設定

Cisco SD-WAN ソフトウェアを実行しているすべての Cisco セルラールータに GPS テンプレートを使用します。

Cisco SD-WAN ソフトウェアを実行しているシスコデバイスの場合、GPS および National Marine Electronics Association（NMEA）ストリーミングを設定できます。これらの両方の機能を有効にして、4G LTE ルータが GPS 座標を取得できるようにします。

（注） Cisco vManage リリース 20.6.1 以降の Cisco vManage を使用して GPS を設定できます。

CLI または CLI テンプレートを使用したデバイス設定は、Cisco IOS XE リリース 17.6.1a 以降のみ使用できます。

Cisco vManage 機能テンプレートを使用して GPS を設定できます。ジオフェンシングを機能させるには、GPS を設定する必要があります。GPS 機能テンプレートを設定するには、**[Configuration]** > **[Templates]** > **[Feature Templates]** > **[GPS]**に移動します。

Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

ジオフェンシングの詳細については、「Configure Geofencing」を参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]**を選択します。
2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [テンプレートの作成（Create Template）] をクリックします。
4. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
5. [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。
6. [Cellular] をクリックします。
7. [Additional Cellular Controller Templates] で、[GPS] をクリックします。
8. GPS のカスタムテンプレートを作成するには、[GPS] ドロップダウンリストをクリックし、[Create Template] をクリックします。GPS テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、GPS パラメータを定義するためのフィールドが含まれています。
9. [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。
10. [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 [Scope] ドロップダウンリストをクリックし、[Device Specific] または [Global] を選択します。

GPS の設定

セルラールータの GPS パラメータを設定するには、次のパラメータを設定します。GPS 機能を設定する場合、アスタリスクの付いたパラメータは必須です。

表 *13*：

パラメータ名	説明
GPS	[On] をクリックして、ルータの GPS 機能を有効にします。

パラメータ名	説明
GPS モード	GPS モードを選択します。 • [MS-based]：位置を決定するときに、モバイルステーションベースの支援（アシスト GPS モードとも呼ばれます）を使用します。このモードでは、ネットワーク データ セッションを使用して GPS 衛星の位置を取得するため、位置座標をより迅速に特定できます。 • [Standalone]：位置を決定するときに衛星情報を使用します。 （注） [Standalone] モードは現在、ジオフェンシングでサポートされていません。
NMEA	[On] をクリックして、位置の決定に役立つNMEA ストリームの使用を有効にします。NMEA は、ルータの 4G LTE Pluggable Interface Module（PIM）から、市販の GPS ベースのアプリケーションを実行している Windows ベースの PC などのデバイスにデータをストリーミングします。
送信元アドレス	（オプション）ルータの PIM に接続するインターフェイスの IP アドレスを入力します。 （注） このオプションは、ジオフェンシングの設定には使用されません。
宛先アドレス	（オプション）NMEA サーバーの IP アドレスを入力します。NMEA サーバーは、ローカルでもリモートでもかまいません。 （注） このオプションは、ジオフェンシングの設定には使用されません。
宛先ポート	（オプション）NMEA データをサーバーに送信するために使用するポートの番号を入力します。 （注） このオプションは、ジオフェンシングの設定には使用されません。

機能テンプレートを保存するには、[Save] をクリックします。

自動帯域幅検出の設定

表 *14 :* 機能の履歴

機能名	リリース情報	説明
Day 0 WAN インターフェイス自動帯域幅検出	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、iPerf3 サーバーを使用して速度テストを実行することにより、Day 0 オンボーディング中に VPN0 の WAN インターフェイスの帯域幅をデバイスが自動的に決定できます。

[Cisco VPN Interface Ethernet] テンプレートを設定して、Day 0 オンボーディング中に VPN0 の WAN インターフェイスの帯域幅をデバイスが自動的に検出するようにすることができます。この方法でテンプレートを設定すると、Cisco IOS XE SD-WAN デバイスは PnP プロセスの完了後に VPN0 の WAN インターフェイスの帯域幅を決定しようとします。

自動帯域幅検出は、結果に影響を与える可能性のあるユーザートラフィックが限られているため、手動設定よりも正確な Day 0 帯域幅設定を提供できます。

デバイスは、iPerf3 サーバーを使用して速度テストを実行することにより、帯域幅を決定します。iPerf3 は、IP ネットワークの帯域幅のアクティブな測定を提供するサードパーティ製ツールです。詳細については、Iperf.fr の Web サイトを参照してください。

デバイスがインターネットに接続されている場合、プライベート iPerf3 サーバーを指定しない限り、デバイスは自動帯域幅検出にパブリック iPerf3 サーバーを使用します。デバイスがプライベート回線に接続されていてインターネット接続がない場合は、自動帯域幅検出用にプライベート iPerf3 サーバーを指定する必要があります。

プライベート iPerf3 サーバーを指定することをお勧めします。プライベート iPerf3 サーバーが指定されていない場合、デバイスはシステム定義のパブリック iPerf3 サーバーのセットに ping し、速度テストのために最小ホップ値のパブリックサーバーを選択します。すべてのサーバーの最小ホップ値が同じ場合は、遅延値が最小のサーバーが選択されます。速度テストに失敗した場合、デバイスはリストから別のパブリックサーバーを選択します。デバイスは、速度テストが成功するか、すべてのサーバーを試すまで、他のパブリック iPerf3 サーバーを選択し続けます。したがって、パブリック iPerf3 サーバーでの速度テストでは、遠く離れたサーバーを使用する可能性があり、最小よりも遅延が長くなります。

システム定義のパブリック iPerf3 サーバーのセットには、以下が含まれます。

- iperf.scottlinux.com
- iperf.he.net
- bouygues.iperf.fr
- ping.online.net
- iperf.biznetnetworks.com

帯域幅検出は、Cisco vManage の [VPN Interface Ethernet] テンプレートの次の設定で制御されます。これらの設定は、VPN0 の WAN インターフェイスでのみサポートされています。

- [Auto Detect Bandwidth]：有効にすると、デバイスが帯域幅を検出します。
- [Iperf Server]：自動帯域幅検出にプライベート iPerf3 サーバーを使用するには、プライベートサーバーの IPv4 アドレスを入力します。自動帯域幅検出にパブリック iPerf3 サーバーを使用するには、このフィールドを空白のままにします。

  プライベート iPerf3 サーバーは、デフォルトの iPerf3 ポートであるポート 5201 で実行する必要があります。

また、自動帯域幅検出では、トンネルインターフェイスに allow-service all コマンドを設定する必要があります。「WAN および LAN インターフェイスの VPN、インターフェイス、およびトンネルの設定」を参照してください。

デバイスは、速度テストの結果をブートフラッシュ ディレクトリの auto_speedtest.json ファイルに書き込みます。結果は、Cisco vManage の **[Monitor]** > **[Devices]** > **[Interface]** ページの [Auto Upstream Bandwidth (bps)] および [Auto Downstream Bandwidth (Mbps)] 領域にも表示されます。

デバイスが iPerf3 サーバーからの応答を受信しない場合、エラーが auto_speedtest.json ファイルに記録され、Cisco vManage の **[Monitor]** > **[Devices]** > **[Interface]** ページに表示されます。

（注） Cisco vManage リリース 20.6.x 以前のリリースでは、速度テストの結果は **[Monitor]** > **[Network]** > **[Interface]** ページに表示されます。

CLI での同等コマンド

auto-bandwidth-detect

iperf-server *ipv4-address*

このコマンドには、no auto-bandwidth-detect の形式もあります。

例

```
Device# show sdwan running-config sdwan
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
```

```
 exit
 auto-bandwidth-detect
 iperf-server 192.0.2.255
exit
appqoe
 no tcpopt enable
 no dreopt enable
```

CLI を使用したシステムロギングの設定

次のコマンドを使用して、Cisco SDWAN でシステムロギングを設定します。

```
config-transaction [IP address | description | alarm | buffered | buginf | console |
discriminator
 esm | event | facility | file | history | host | origin-id | persistent | rate-limit |
 snmp-authfail | snmp-trap | source-interface
 trap | userinfo]
```

SSH ターミナル

ルータへのSSHセッションを確立するには、SSHターミナル画面を使用します。SSHセッションから、ルータで CLI コマンドを発行できます。

デバイスへの SSH セッションの確立

デバイスへの SSH セッションを確立するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Tools]** > **[SSH Terminal]** を選択します。
2. 統計を収集するデバイスを選択します。
    1. デバイスが属するデバイスグループを選択します。
    2. 必要に応じて、ステータス、ホスト名、システムIP、サイトID、またはデバイスタイプでデバイスリストを並べ替えます。
    3. デバイスをクリックして、選択します。
3. ユーザー名とパスワードを入力して、デバイスにログインします。

CLI コマンドを発行して、デバイスをモニタリングまたは設定できるようになりました。

Cisco vManage と外部サーバーが通信するための HTTP/HTTPS プロキシサーバー

表 *15 :* 機能の履歴

機能名	リリース情報	説明
Cisco vManage と外部サーバーが通信するための HTTP/HTTPS プロキシサーバー	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	Cisco vManage では HTTP/HTTPS を使用して一部の Web サービスへアクセスし、REST API コールを行います。この機能を使用すると、HTTP/HTTPS プロキシサーバーを介して HTTP/HTTPS 通信をチャネル化できます。

次は、Cisco vManage が外部サーバーへの HTTP/HTTPS 接続を使用する例です。

- 証明書の要求または更新
- Cisco プラグアンドプレイ統合
- ポリシーを使用したスマートライセンス
- Cloud OnRamp
- ソフトウェア イメージ ダウンロード
- Cisco SD-WAN vAnalytics へのデータアップロード

Cisco vManage リリース 20.4.1 以前のリリースでは、オンプレミス Cisco vManage インスタンスに設定されたファイアウォールでこの HTTP/HTTPS 通信を許可する必要があります。Cisco vManage 20.5.1 以降、HTTP/HTTPS プロキシサーバー経由で HTTP/HTTPS 通信をチャネル化できます。HTTP/HTTPS プロキシサーバーを設定すると、ファイアウォールの設定中に外部サーバーとの HTTP/HTTPS 通信を制限して、システムのセキュリティの向上が可能になります。

次の場合、トラフィックは HTTP/HTTPS プロキシサーバー経由で送信されます。

- シマンテックまたはシスコの自動証明書要求または更新のための HTTPS 接続
- 次のドメインの URL への REST API コール：
  - cisco.com
  - amazonaws.com
  - microsoft.com
  - office.com
  - microsoftonline.com

設定された HTTP/HTTPS プロキシサーバーに到達可能かどうかが Cisco vManage によって 24 時間ごとに確認されます。プロキシサーバーに到達できない場合、Cisco vManage で `HTTPS proxy server {IP} not reachable` アラームが発生します。

制約事項

- HTTP/HTTPS プロキシサーバーを介して外部サーバーと通信するように設定されている場合、Cisco vManage はローカルで、またはプロキシサーバーをバイパスして、設定されたドメインネームシステム（DNS）サーバーを介して FQDN を解決します。次に、Cisco vManage は、解決の結果として得られた HTTP/HTTPS 接続をプロキシサーバーに送信します。外部サーバーの FQDN を解決するための DNS クエリは、Cisco vManage が HTTP/HTTPS プロキシサーバーに結果の HTTP/HTTPS 接続を送信するまでに成功する必要があります。
- Cisco vManage の SD-AVC コンテナと外部サービス間の通信では、HTTP/HTTPS プロキシサーバーの使用はサポートされていません。

HTTP/HTTPS プロキシサーバーの設定

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [HTTP/HTTPS Proxy] 設定で、[Edit] をクリックします。
3. [Enable HTTP/HTTPS Proxy] 設定で、[Enabled] をクリックします。
4. [HTTP/HTTPS Proxy IP Address] と [Port number] を入力します。
5. **[Save]** をクリックします。

（注） Cisco vManage では TCP ポート 7 のエコー要求を使用して、プロキシサーバーの到達可能性が検証されます。エコー要求が宛先ホストポートにアクセスできるようにファイアウォールとプロキシサーバーを設定していることを確認してください。

Cisco vManage では、HTTP/HTTPS プロキシサーバーが到達可能であることが確認され、サーバーの詳細が構成データベースに保存されます。外部サーバーへの HTTP/HTTPS 接続および REST API コールは、プロキシサーバー経由で送信されます。

HTTP/HTTPS プロキシサーバーに到達できない場合、Cisco vManage に失敗の理由を示すエラーメッセージが GUI に表示されます。

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。