Cisco SD-WAN システムおよびインターフェイス コンフィギュレーション ガイド、Cisco IOS XE リリース 17.x

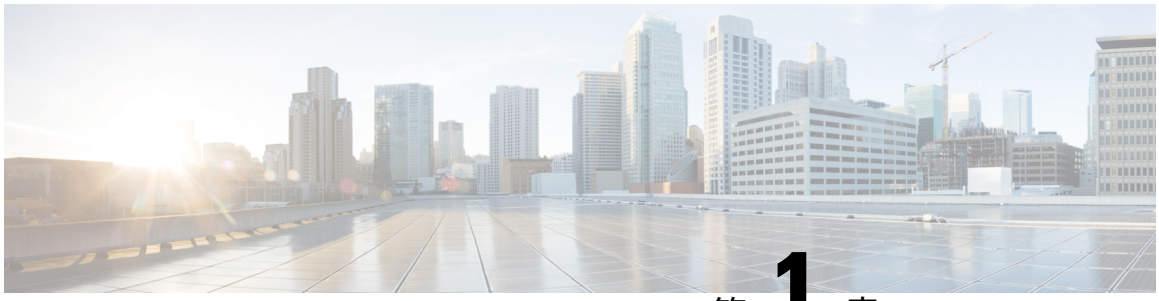
初版：2019 年 4 月 15 日

最終更新：2022 年 8 月 24 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

最初にお読みください

参考資料

- Release Notes[英語]
- Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations[英語]

ユーザマニュアル

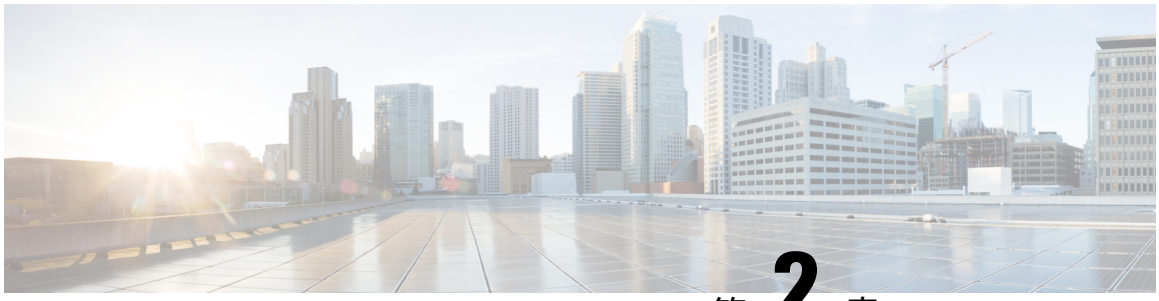
- Cisco IOS XE (Cisco IOS XE SD-WAN Devices)[英語]
- Cisco IOS XE (SD-WAN) Qualified Command Reference[英語]
- Cisco IOS XE（SD-WAN）リリース 17 のユーザーマニュアル

通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、CiscoDevnet にアクセスしてください。
- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Toolにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

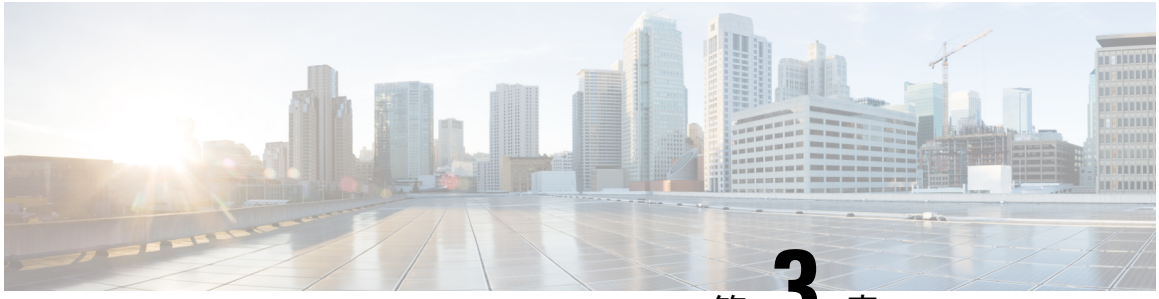


第 2 章

Cisco IOS XE（SD-WAN）の新機能

シスコでは、リリースごとに SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco SD-WAN ソリューションに関係する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

『What's New in Cisco IOS XE (SD-WAN) Release 17.x』[英語]



第 3 章

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 （11 ページ）
- 基本システムパラメータの設定 （19 ページ）
- グローバルパラメータの設定 （26 ページ）
- Cisco vManage を使用した NTP サーバーの設定 （30 ページ）
- ルータの NTP プライマリとしての設定 （34 ページ）
- NTP の設定 （36 ページ）
- CLI を使用した時間の設定 （36 ページ）
- Cisco vManage を使用した GPS の設定 （36 ページ）
- 自動帯域幅検出の設定 （39 ページ）
- CLI を使用したシステムロギングの設定 （41 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（213 ページ）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。

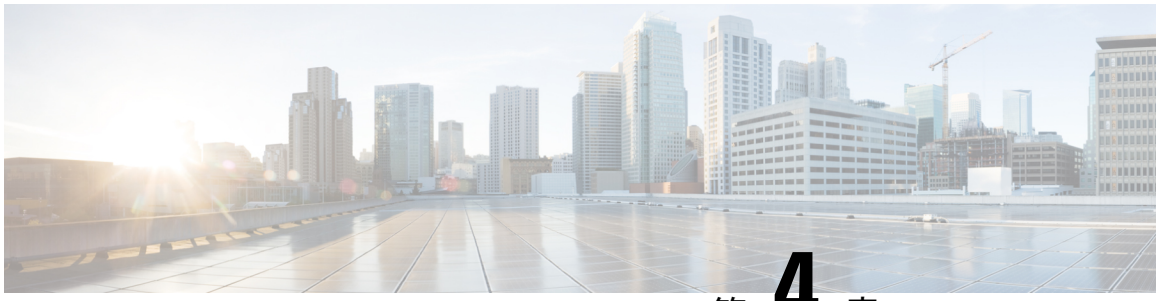
HTTP/HTTPS プロキシサーバーの設定

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。



第 4 章

システムロギングの設定

表 16 : 機能の履歴

機能名	リリース情報	説明
TLS 経由で Syslog メッセージを送信する機能	Cisco IOS XE リリース 17.2.1r	この機能を使用すると、Transport Layer Security（TLS）接続を確立することにより、syslog メッセージを外部の設定済みホストに転送できます。TLS プロトコルを使用すると、ホップごとに、syslog メッセージの内容の機密性、安全性を保ち、改ざんや変更を防ぐことができます。

システムロギング

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、syslogメッセージの優先順位を設定できます。Cisco SD-WANデバイスは、UNIX スタイルの syslog サービスにログメッセージを送信できます。

Cisco IOS XE SD-WAN デバイスは、TCP および UDP を使用して、構成された外部ホスト上の syslog サーバーに syslog メッセージを送信します。これらのデバイスが syslog メッセージを送信している場合、メッセージは出力先に到達するためにいくつかのホップを通過する場合があります。ホップ中の中間ネットワークは、信頼できないか、別のドメインにあるか、セキュリティレベルが異なる可能性があります。このためCisco IOS XE SD-WANデバイスでは、RFC5425に従って Transport Layer Security（TLS）を介した安全な syslog メッセージの送信をサポートするようになりました。潜在的な改ざんから syslogメッセージの内容を保護するために、証明書交換、相互認証、および暗号ネゴシエーションに TLS プロトコルが使用されます。

Cisco IOS XE SD-WAN デバイスは、TLS 経由で syslog メッセージを送信するための相互認証とサーバー認証の両方をサポートします。

Syslog メッセージの形式、Syslog メッセージのレベル、およびシステムログファイル

syslog メッセージ形式

Syslog メッセージはパーセント記号（%）で始まり、syslog メッセージの形式は次のとおりです。

- Syslog メッセージ形式

  seq no:timestamp: %facility-severity-MENEMONIC:description (hostname-n)
- RFC5424 に基づく Syslog メッセージ形式

  <pri>ver timestamp hostname appname procid msgid structured data description/msg

（注） RFC5424 に基づく syslog メッセージ形式では、hostname、appname、procId、msgId、structured data などのオプションフィールドは - で指定されます。

syslog メッセージのフィールドの説明は次のとおりです。

表 *17 : Syslog* メッセージ形式のフィールドの説明

フィールド	説明
facility	ロギングファシリティを20以外の値に設定します。これは、UNIXシステムで想定されています。

フィールド	説明
シビラティ（重大度）	メッセージの重要度または重大度は、0から7までの数値コードによって分類されます。この範囲で数値が小さいほど、システム状態の重大度が高いことを示します。
msg または description	syslog サーバーの状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、インターフェイス名、ポート番号、またはユーザー名が含まれていることがあります。 RFC5424 に基づく syslog メッセージ形式では、description は次を表します。*%facility-severity-MENEMONIC:description*

通常、syslog メッセージの前には余分なテキストが付きます。

- プライオリティ値、シーケンス番号、およびタイムスタンプが前に付いたシステムロギングメッセージの例を以下に示します。

  *<45>10: polaris-user1: *Jun 21 10:76:84.100: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down*

- RFC5424 に基づく、プライオリティ値、syslog プロトコル仕様のバージョン、およびタイムスタンプが前に付いたシステムロギングメッセージの例を次に示します。

  <45>1 2003-10-11T22:14:15.003Z 10.64.48.125 polaris-user1 - - - %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down

（注） タイムスタンプの形式は、両方の syslog メッセージ形式で同じではありません。RFC5424 に基づくメッセージ形式では、T と Z は必須で、T は区切りを表し、Z はゼロタイムゾーンを表します。

Syslog メッセージのレベル

すべての syslog メッセージは、保存する syslog メッセージの重大度を示す優先度に関連付けられています。デフォルトのプライオリティ値は「informational」であるため、デフォルトでは、すべての syslog メッセージが記録されます。優先度には、次のいずれかを指定でき、順に重大度が下がります。

- [Emergency]：システムは使用できません（syslog 重大度 0 に対応）。
- [Alert]：ただちに対応するようにします（syslog 重大度 1 に対応）。
- [Critical]：重大な状態（syslog 重大度 2 に対応）。
- [Error]：システムのユーザビリティを完全に損なわないエラー状態（syslog 重大度 3 に対応）。

- [Warning]：軽微なエラー状態（syslog 重大度 4 に対応）。
- [Notice]：正常だが重大な状態（syslog 重大度 5 に対応）。
- [Informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応）。
- [Debug]：syslog 重大度 7 に対応するデバッグメッセージを発行します。

システムのログファイル

デフォルトまたは設定されたプライオリティ値以上のすべての syslog メッセージは、syslog サーバーのローカルデバイスの `/var/log` ディレクトリ内にあるいくつかのファイルに記録されます。ログファイルの内容は次のとおりです。

- auth.log：ログイン、ログアウト、スーパーユーザーのアクセスイベント、および認可システムの使用状況
- kern.log：カーネルメッセージ
- messages.log：すべてのソースからの syslog メッセージが記録された統合ログファイル。
- vconfd.log：設定に関するすべての syslog メッセージ
- vdebug.log：デバッグ機能が有効になっているモジュールのすべてのデバッグメッセージ、およびデフォルトのプライオリティ値を超えるすべての syslog メッセージ。デバッグログメッセージは、モジュールに基づいてさまざまなレベルのロギングをサポートします。実装されているロギングレベルは、モジュールごとに異なります。たとえば、システムマネージャ（sysmgr）には 2 つのロギングレベル（オンとオフ）があり、シャーシマネージャ（chmgr）には 4 つの異なるロギングレベル（オフ、低、標準、高）があります。デバッグメッセージをリモートホストに送信することはできません。そのため、デバッグを有効にするには、**debug** 操作コマンドを使用します。
- vsyslog.log：設定されたプライオリティ値を超える Cisco SD-WAN プロセス（デーモン）からのすべての syslog メッセージ。デフォルトのプライオリティ値は「informational」であるため、デフォルトでは「notice」、「warning」、「error」、「critical」、「alert」、および「emergency」のすべての syslog メッセージが保存されます。
- vmanage-syslog.log：Cisco vManage NMS 監査ログメッセージ

以下は、Cisco SD-WAN が使用しない標準の LINUX ファイルであり、`/var/log` ディレクトリにあります。

- cron.log
- debug.log
- lpr.log
- mail.log
- syslog

syslog ファイルに送信されるメッセージはレート制限されていないため、次のようになります。

- 各 syslog ファイルには、最大 16 MB のサイズ容量で 10 個のログファイルのストレージ制限が設定されています。
  - ストレージ容量が 16 MB のサイズ制限を超えると、ログファイルは日付が付けられて .GZ ファイルとして保存されます。
  - ストレージの制限が 10 個のログファイルを超えると、最も古いログファイルがドロップされます。
- 短時間に多くの syslog メッセージが生成された場合、オーバーフローメッセージはバッファに入れられ、syslog ファイルに保存するためのキューに入れられます。

syslog メッセージが繰り返された場合、つまり連続して同一メッセージが複数回発生した場合、メッセージは 1 回だけ syslog ファイルに記録されます。メッセージには、メッセージの発生回数を示す注釈が付けられます。

ログメッセージの最大長は 1024 バイトです。それより長いメッセージは切り捨てられます。

Cisco vManage NMS 監査ログメッセージの最大長は 1024 バイトです。それより長いメッセージはより小さいフラグメントに切り捨てられ、これらの各フラグメントは識別子によって示されます。識別子は、フラグメント 1/2、フラグメント 2/2 などです。たとえば、長い監査ログメッセージがより小さなフラグメントに切り捨てられると、次のように表示されます。

```
local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-1/2: {“logid”:
“d9ed576a-43ae-49ce-921b-a51c1ed40698”, “entry_time”:
1576605512190, “statcycletime” 34542398334245, “logmodule”:”maintenance”, “logfeature”:
 “upgrade”, “loguser”: “admin”, “logusersrcip”:
“10.0.1.1”, “logmessage”: “Device validation Upgrade to version — Validation success”,
“logdeviceid”:”Validation”, “auditdetails” :
[“[18-Oct-2020 17:42:08 UTC] Published messages to vmanage(s)”,
“auditdetails”:[“[18-Oct-2020 17:42:07 UTC] Software image: vmanage-99.99.999-
x86_64.tar.gz”, “Software image download may take up to 60}

local6.info: 18-Oct-2020 17:42:07 vm10 maintenance-fragment-2/2: { minutes”,
“logprocessid”: “software_install-7de0ec44-d290-4429-b24532435324”, “tenant”:, “default”}
```

AAA 認証および Netconf CLI のアクセス状況と使用状況に関連する syslog メッセージは、auth.log および messages.log ファイルに記録されます。Cisco vManage NMS がルータにログインして統計情報とステータス情報を取得し、ファイルをルータにプッシュするたびに、ルータは AAA 認証と Netconf のログメッセージを生成します。したがって、時間の経過とともに、これらのメッセージでログファイルがいっぱいになる可能性があります。これらのメッセージでログファイルがいっぱいにならないようにするには、Cisco vManage NMS から次のコマンドを使用して、AAA 認証と Netconf の syslog メッセージのロギングを無効にします。

AAA および Netconf Syslog メッセージのロギングの無効化

1. `vManage# config`

   コンフィギュレーション モード端末を開始します。

2. `vManage(config)# system aaa logs`

AAA および Netconf システムロギング（syslog）メッセージのロギングを設定します。

3. `vManage(config-logs)# audit-disable`

   AAA イベントのロギングを無効にします。

4. `vManage(config-logs)# netconf-disable`

   Netconf イベントのロギングを無効にします。

5. `vManage(config-logs)# commit`

   Commit complete.

Syslog メッセージの送信に TLS を使用する利点

syslog メッセージの送信に TLS を使用する利点は次のとおりです。

- Cisco IOS XE SD-WAN デバイス と syslog サーバー間のハンドシェイクで各 TLS セッションが開始されるため、メッセージコンテンツの機密性が確保されます。Cisco IOS XE SD-WAN デバイス と syslog サーバーでは、そのセッションに使用される特定のセキュリティキーと暗号化アルゴリズムが一致します。TLS セッションでは、syslog メッセージの内容の開示が拒否されます。
- 各メッセージの内容の整合性チェックにより、ホップ単位での転送中のメッセージに対する変更が無効になります。
- Cisco IOS XE SD-WAN デバイス と syslog サーバー間の相互認証により、syslog サーバーは証明書交換を通じて許可されたクライアントからのみログメッセージを受け入れるようになります。

TLS のサーバー認証でのロギングの設定

サーバー認証では、Cisco IOS XE SD-WAN デバイス は syslog サーバーの ID を確認します。syslog サーバーと証明書が正当なエンティティである場合、デバイスはサーバーとの TLS 接続を確立します。サーバー認証を実装するために、syslog サーバーは公開証明書を Cisco IOS XE SD-WAN デバイスと共有します。

前提条件

Cisco IOS XE SD-WAN デバイスに、暗号化モジュール CLI を使用して設定するルート認証局（CA）が事前にインストールされていることを確認します。「サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール」を参照してください。

syslog サーバーの TLS プロファイルを設定するには、次の手順を実行します。

1. Cisco vManage を使用したロギング機能テンプレートの設定。
   1. ローカルディスクへのロギング属性の設定。

2. リモートサーバーへのロギングの設定。

2. ロギング機能テンプレートからデバイステンプレートを作成します。

TLS の相互認証でのロギングの設定

相互認証では、syslog サーバーと Cisco IOS XE SD-WAN デバイスの両方がお互いを同時に認証します。Cisco IOS XE SD-WAN デバイスには、TLS セッションの相互認証のために、ルート証明書または ID 証明書が必要です。syslog サーバーの TLS プロファイルを設定するには、次の手順を実行します。

1. 相互認証のために Cisco IOS XE SD-WAN デバイスに Syslog ルート証明書をインストール。
2. Cisco vManage を使用したロギング機能テンプレートの設定。
    1. ローカルディスクへのロギング属性の設定。
    2. 機能証明書署名要求の生成と機能証明書のインストール （63 ページ）
    3. リモートサーバーへのロギングの設定。
3. ロギング機能テンプレートからデバイステンプレートを作成します。
4. 機能証明書署名要求の生成と機能証明書のインストール （63 ページ）。
5. Cisco IOS XE SD-WAN デバイス でのトラストポイント設定の確認。

サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール

始める前に

エンコードされた CA 証明書を syslog サーバーで生成していることを確認します。サーバー認証のために Syslog サーバーにルート認証局をインストール （53 ページ）を参照してください。

ステップ 1 認証局の PKI トラストポイントを設定するには、次のコマンドを使用して、PKI での証明書の許可および失効を設定します。

a) **enable**

特権 EXEC モードを有効にします。

例：

```
Cisco XE SD-WAN> enable
```

b) **config-transaction**

コンフィギュレーション モードを開始します。

例：

```
Cisco XE SD-WAN# config-transaction
```

c) **crypto pki trustpoint** *name*

トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

例：

```
Cisco XE SD-WAN  (config)# crypto pki trustpoint Syslog-signing-CA
```

d) **enrollment [mode] [retry period** *minutes*] [**retry count** *number*] **url** url [**pem**]

CA の登録パラメータを指定します。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# enrollment terminal
```

e) **chain-validation [{stop | continue}[parent-trustpoint]]**

証明書チェーンが、すべての証明書で処理されるレベルを設定します。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# chain-validation stop
```

f) **revocation-check method**

（任意）証明書の失効ステータスをチェックします。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# revocation-check none
```

g) **exit**

グローバル コンフィギュレーション モードに戻ります。

例：

```
Cisco XE SD-WAN(ca-trustpoint)# exit
```

ステップ 2 Cisco IOS XE SD-WAN デバイスに証明書を発行して証明書の登録を行う前に、ルート CA を取得して認証します。

CA を認証するには、**crypto pki authenticate** コマンドを使用します。

例：

```
Cisco XE SD-WAN(config)# crypto pki authenticate root
```

ステップ 3 Base 64 でエンコードされた CA 証明書が含まれているテキスト部分をコピーし、プロンプトにペーストします。

エンコードされた CA 証明書を含むテキストを生成してコピーするには、サーバー認証のために Syslog サーバーにルート認証局をインストール （53 ページ）を参照してください。

例：

Base 64 でエンコードされた CA 証明書のサンプル：

```
-----BEGIN CERTIFICATE-----
MIID9jCCAt6gAwIBAgIJAM5b3nyjDAKIMA0GCSqGSIb3DQEBCwUAMIGPMQswCQYD
```

```
VQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWthMRIwEAYDVQQHDAlCYW5nYWxvcmUx
DjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANDU0cxGzAZBgNVBAMMEmVtYmQtbG54
LmNpc2NvLmNvbTEdMBsGCSqGSIb3DQEJARYOYW5idkBjaXNjby5jb20wHhcNMTkw
OTIwMTQ1NjAxWhcNMjIwOTE5MTQ1NjAxWjCBjzELMAkGA1UEBhMCSU4xEjAQBgNV
BAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVDaXNj
bzEMMAoGA1UECwwDQ1NHMRswGQYDVQQDDBJlbWJkLWxueC5jaXNjby5jb20xHTAb
BgkqhkiG9w0BCQEWDmFuYnZAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuof+Dh8EdAQ7bHJPdnXhy9ibTLAQ+OpQrMBoOqeAsU/Jru8y
3ht2Eqci35aNjlDcsTUlZyUHBNAMtL69t1HxTRVCOghOZmipzOS+q8rFykHa+bcA
FqmHyqxNwdQcW3cQFZ6rvWTFD9O46ONX3xewpdCR+s+0KFOHDd+RxpAb2NyDWIvn
/1/xwq2a4ZlwgM2d0G8sit0i0D/+6FbZuJjAf+PRTypo4IJyQjcOHpZuslLzPztM
HxLI7pOmR+8+WcInT0l0dyGdpKKHXi6lEbeiyubIym0z0Des5OckDYFejXgXpJDx
9jCVkz+r0bijqbT5PMpSAYYcjdnQ0kdH43sykwIDAQABo1MwUTAdBgNVHQ4EFgQU
OcOmN72TyBqD/Ud2qBLUwId1Yv0wHwYDVR0jBBgwFoAUOcOmN72TyBqD/Ud2qBLU
wId1Yv0wDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAUVVWJHWo
rKxfFV2w7jR7mLZSlVtEvZueMXWPvyYP+Qt09MrRqwNDUJEvggTxU7lvLwtnITPM
l/dOmpoer8GhDtnxUnjsVeVWGIR74SJCS0GU/03bEJ2sto/eAJEOzI7wDg7Fubgy
Pc3RHbk4JWTWs4JF8+E64p2UzJMuu0eLDPQWxl7p2wd3sr4DBHB3qlfbg31T3VHr
PCcuzJmOEdeZYGL1/LFvPx7NZS8lwFAohe6h8ptm3ENg7dzIeyZFZVfcq11Q1rer
+3RcM0VqjScIOZhp97dqfBlHEdqUE/QfKlBt12KU+0sj8yJJC+cuKlHQj5JGmGLI
Y6r7bMcn99Y6Rw==
-----END CERTIFICATE-----
```

ステップ 4 **yes** と入力して、証明書の受け入れを確認します。

ルート CA 証明書が正常にインポートされました。

次のタスク

Cisco vManage を使用したロギング機能テンプレートの設定 （55 ページ）

サーバー認証のために Syslog サーバーにルート認証局をインストール

このドキュメントでは、TLS をサポートする syslog-ng サーバーをセットアップする手順について説明します。

ステップ 1 サーバーに syslog-ng をインストールするには、次のコマンドを使用します。

例：

```
# apt-get install syslog-ng openssl
```

ステップ 2 ディレクトリを syslog-ng フォルダに変更し、ルート証明書を保存するフォルダを作成するには、次のコマンドを使用します。

例：

```
# cd /etc/syslog-ng
# mkdir cert.d
# mkdir key.d
# mkdir ca.d
# cd cert.d
```

```
# openssl req -new -x509 -out cacert.pem -days 1095 -nodes
# mv privkey.pem ../key.d
```

openssl コマンドを使用すると、`cacert.pem` ファイルでエンコードされたルート証明書を使用できます。このファイルは、`cd/etc/syslog-ng/cert.d` ディレクトリにあります。

ステップ 3 Cisco IOS XE SD-WAN デバイスでルート証明書をインストールするときに、`cacert.pem` ファイルからコンテンツをコピーします。サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール （51 ページ）のステップ 3 を参照してください。

次のタスク

サーバー認証のために Cisco IOS XE SD-WAN デバイスにルート認証局をインストール （51 ページ）

相互認証のために Cisco IOS XE SD-WAN デバイスに Syslog ルート証明書をインストール

Transport Layer Security（TLS）syslog プロトコルを使用して Cisco IOS XE SD-WAN デバイスを設定するには、デバイスに TLS セッションを相互認証するためのルート証明書またはアイデンティティ証明書が必要です。サードパーティの認証局（CA）を使用して Public Key Infrastructure（PKI）サービスを取得するか、Microsoft Active Directory 証明書サービス（AD CS）を使用できます。AD CS を使用すると、PKI を作成し、要件に応じて公開キー暗号、デジタル証明書、およびデジタル署名機能を提供できます。

ステップ 1 サードパーティの CA または Microsoft Active Directory 証明書サービスを使用して、エンタープライズルート証明書を生成します。

ステップ 2 ルート CA を Base 64 形式でダウンロードし、ルート CA の内容を選択してコピーします。

ステップ 3 Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。

ステップ 4 [Enterprise Feature Certificate Authorization] をクリックし、[Edit] をクリックします。

ステップ 5 [Enterprise Root Certificate] ボックスにルート CA の内容を貼り付けます。

ステップ 6 （オプション）証明書署名要求（CSR）を生成する場合は、[Set CSR Properties] チェックボックスをオンにします。

ステップ 7 [Close] をクリックします。

ルート CA は Cisco vManage にアップロードされ、Cisco vManage はルート証明書を Cisco IOS XE SD-WAN デバイス に保存します。

次のタスク

Cisco vManage を使用したロギング機能テンプレートの設定 （55 ページ）

Cisco vManage を使用したロギング機能テンプレートの設定

Cisco IOS XE SD-WAN デバイス では、Cisco vManage を使用してイベント通知システムログ（syslog）メッセージをローカルデバイス上またはリモートホスト上のファイルに記録できます。

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 2 [Feature Templates] をクリックして、[Add Template] をクリックします。

（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。

ステップ 3 [Select Devices] で、テンプレートを作成するデバイスを選択します。

ステップ 4 ロギング用のテンプレートを作成するには、[Cisco Logging] を選択します。

Cisco ロギング 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、ロギング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。タブまたはプラス記号（+）をクリックして、他のフィールドを表示します。

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の範囲は [Default] に設定されています。デフォルトの設定または値は、パラメータの横に表示されます。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ます。

ステップ 5 [Template Name] に、テンプレートの名前を入力します。

名前には、最大 128 文字の英数字を使用できます。

ステップ 6 [Template Description] に、テンプレートの説明を入力します。

説明には、最大 2048 文字の英数字を使用できます。

次のタスク

ローカルディスクへのロギング属性の設定 （55 ページ）

ローカルディスクへのロギング属性の設定

1. [Disk] をクリックし、次のパラメータを設定します。

表 *18* : パラメータ情報

パラメータ	説明
Enable Disk	ローカルハードディスク上のファイルに syslog メッセージを保存する場合は [On] を、保存を許可しない場合は [Off] をクリックします。デフォルトでは、すべてのデバイスでローカルディスクファイルへのロギングが有効になっています。
最大ファイル サイズ（Maximum File Size）	syslog ファイルの最大サイズを入力します。syslog ファイルは、ファイルサイズに基づいて 1 時間ごとにローテーションされます。ファイルサイズが設定値を超えると、ファイルがローテーションされ、*syslogd* プロセスに通知されます。 範囲：1 ～ 20 MB デフォルト：10 MB
Rotations	最も早く作成されたファイルを破棄するまでに作成できる syslog ファイルの数を入力します。 範囲：1 ～ 10 MB デフォルト：10 MB

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。
3. 機能テンプレートをデバイステンプレートに関連付けるには、機能テンプレートからのデバイス テンプレートの作成を参照してください。https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/System-Interface/systems-interfaces-book-xe-sdwan/configure-devices.html

次の作業

サーバー認証用 TLS プロファイルの設定 （56 ページ） または 相互認証用 TLS プロファイルの設定 （59 ページ）

サーバー認証用 TLS プロファイルの設定

1. [TLS Profile] をクリックします。
2. [New Profile] をクリックし、次のパラメータを設定します。

表 *19:* パラメータ情報

パラメータ名	説明
プロファイル名	TLS プロファイル名を入力します。
TLS バージョン	TLS バージョン v1.1 または v1.2 を選択します。
認証タイプ	認証タイプとして [Server] を選択します。

パラメータ名	説明
Ciphersuites	TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。 以下は、暗号スイートのリストです。 • aes-128-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha 暗号化タイプ tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2（TLS1.2 以上） • dhe-aes-gcm-sha2 暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2（TLS1.2 以上） • ecdhe-ecdsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2（TLS1.2 以上）SuiteB • ecdhe-rsa-aes-128-cbc-sha 暗号化タイプ tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2（TLS1.2 以上） • ecdhe-rsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2（TLS1.2 以上） • rsa-aes-cbc-sha2 暗号化タイプ tls_rsa_with_aes_cbc_sha2（TLS1.2 以上） • rsa-aes-gcm-sha2 暗号化タイプ tls_rsa_with_aes_gcm_sha2（TLS1.2 以上）

TLS バージョンごとに、次の暗号スイートを使用できます。

```
TLS v1.1
```

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

TLS v1.2 以降

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)

ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

TLS プロファイルが表に表示されます。

3. 別のプロファイルを作成するには、[Add] をクリックします。
4. TLS プロファイル情報を編集または削除するには、[Action] の下にある または をクリックします。
5. 機能テンプレートを保存するには、[Save] をクリックします。
6. 機能テンプレートをデバイステンプレートに関連付ける場合は、「機能テンプレートからのデバイステンプレートの作成」を参照してください。

認証タイプとして [Server] を選択すると、トラストポイント情報を除く、TLS プロファイルに関するすべての情報が保存されます。

次の作業

リモートサーバーへのロギングの設定 （61 ページ）

相互認証用 TLS プロファイルの設定

1. [TLS Profile] をクリックします。
2. [New Profile] をクリックし、次のパラメータを設定します。

表 *20* : パラメータ情報

パラメータ名	説明
プロファイル名	TLS プロファイル名を入力します。
TLS バージョン	TLS バージョン v1.1 または v1.2 を選択します。
認証タイプ	認証タイプとして [Mutual] を選択します。

パラメータ名	説明
Ciphersuites	暗号化に使用する必要がある TLS バージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。 以下は、暗号スイートのリストです。 • aes-128-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_128_sha • aes-256-cbc-sha 暗号化タイプ tls_rsa_with_aes_cbc_256_sha • dhe-aes-128-cbc-sha 暗号化タイプ tls_dhe_rsa_with_aes_128_cbc_sha • dhe-aes-cbc-sha2 暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2（TLS1.2 以上） • dhe-aes-gcm-sha2 暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2（TLS1.2 以上） • ecdhe-ecdsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2（TLS1.2 以上）SuiteB • ecdhe-rsa-aes-128-cbc-sha 暗号化タイプ tls_ecdhe_rsa_with_aes_128_cbc_sha • ecdhe-rsa-aes-cbc-sha2 暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2（TLS1.2 以上） • ecdhe-rsa-aes-gcm-sha2 暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2（TLS1.2 以上） • rsa-aes-cbc-sha2 暗号化タイプ tls_rsa_with_aes_cbc_sha2（TLS1.2 以上） • rsa-aes-gcm-sha2 暗号化タイプ tls_rsa_with_aes_gcm_sha2（TLS1.2 以上）

TLS バージョンごとに、次の暗号スイートを使用できます。

```
TLS v1.1
```

```
aes-128-cbc-sha Encryption type tls_rsa_with_aes_cbc_128_sha
aes-256-cbc-sha Encryption type tls_rsa_with_aes_cbc_256_sha
```

TLS v1.2 以降

```
dhe-aes-cbc-sha2 Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
dhe-aes-gcm-sha2 Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)

ecdhe-ecdsa-aes-gcm-sha2 Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ecdhe-rsa-aes-cbc-sha2 Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ecdhe-rsa-aes-gcm-sha2 Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)

rsa-aes-cbc-sha2 Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
rsa-aes-gcm-sha2 Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
```

TLS プロファイルが表に表示されます。

3. 別のプロファイルを作成するには、[Add] をクリックします。
4. TLS プロファイル情報を編集または削除するには、[Action] の下にある または をクリックします。
5. 機能テンプレートを保存するには、[Save] をクリックします。
6. 機能テンプレートをデバイステンプレートに関連付けます。「機能テンプレートからのデバイステンプレートの作成」を参照してください。

相互認証された機能テンプレートは Cisco IOS XE SD-WAN デバイスに保存され、SYSLOG-SIGNING-CA 証明書などのトラストポイントはデバイスに保存されます。これで、Cisco vManage は Cisco IOS XE SD-WAN デバイスから証明書をインストールできるようになりました。

次の作業

リモートサーバーへのロギングの設定 （61 ページ）

リモートサーバーへのロギングの設定

IPV6 または IPV4 サーバー設定に TLS プロファイルを追加し、イベント通知システムログメッセージのリモートサーバーへのロギングを設定するには、次の手順を実行します。

1. [Server] をクリックします。
2. [Add New Server] をクリックし、IPv4 または IPv6 の次のパラメータを設定します。

表 *21* : パラメータ情報

パラメータ名	説明
ホスト名/IP アドレス（Hostname/IP Address）	syslog メッセージを保存するシステムのドメインネームシステム（DNS）名、ホスト名、または IPv4/IPv6 アドレスを入力します。 別の syslog サーバーを追加するには、[+] をクリックします。 syslog サーバーを削除するには、 をクリックします。
VPN ID	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 VPN ID 範囲：0 ～ 65530
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、syslog サーバーの設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスはすべて同じにする必要があります。
プライオリティ	保存する syslog メッセージの重大度を選択します。重大度は、syslog メッセージを生成したイベントの深刻度を示します。Syslog メッセージのレベルを参照してください。
TLS	Cisco IOS XE SD-WAN デバイス の場合は、[On] をクリックして TLS 経由の syslog を有効にします。
カスタム プロファイル	Cisco IOS XE SD-WAN デバイス の場合、[On] をクリックして TLS プロファイルの選択を有効にするか、[Off] をクリックして TLS プロファイルの選択を無効にします。
TLS Profile	Cisco IOS XE SD-WAN デバイス の場合、IPv4 または IPv6 サーバー設定でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。

サーバーエントリがテーブルに表示されます。

3. サーバーの別のエントリを作成するには、[Add] をクリックします。
4. ロギングサーバーを編集するには、 をクリックします。
5. ロギングサーバーを削除するには、 をクリックします。
6. 機能テンプレートを保存するには、[Save] をクリックします。
7. 機能テンプレートをデバイステンプレートに関連付ける場合は、「機能テンプレートからのデバイステンプレートの作成」を参照してください。

機能証明書署名要求の生成と機能証明書のインストール

Cisco IOS XE SD-WAN デバイス および syslog サーバーを検証および認証するには、Cisco vManage の [Certificates] 画面で次の操作を実行します。エンタープライズ証明書については、『Cisco SD-WAN Getting Started Guide』を参照してください。

ステップ 1 Cisco vManage のメニューから**[Configuration]** > **[Certificates]**の順に選択します。

ステップ 2 [Certificates] から、Cisco IOS XE SD-WAN デバイス を選択します。

a) 機能証明書署名要求（CSR）を生成します。

機能 CSR を生成すると、[View Feature CSR] および [Install Feature certificate] オプションが使用できるようになります。

b) 機能 CSR を表示します。

c) 機能 CSR をダウンロードするには、[Download] をクリックします。

ステップ 3 証明書に署名するには、証明書をサードパーティの署名機関に送信します。

ステップ 4 Cisco IOS XE SD-WAN デバイス に証明書をインポートするには、機能証明書をインストールします。

[Install Feature Certificate] 画面では、署名された証明書を使用し、それを Cisco IOS XE SD-WAN デバイスにインストールします。

機能証明書のインストールが成功すると、[Revoke Feature Certificate] および [View Feature Certificate] オプションが Cisco vManage で使用できるようになります。https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c-Certificates-12278https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c-Certificates-12278

次のタスク

Cisco IOS XE SD-WAN デバイス でのトラストポイント設定の確認 （64 ページ）

Cisco IOS XE SD-WAN デバイス でのトラストポイント設定の確認

Cisco IOS XE SD-WAN デバイス のトラストポイント情報を含む syslog ファイルの内容を表示するには、**show crypto pki trustpoints status** コマンドを使用します。

例

サーバー認証

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

相互認証

```
Cisco XE SD-WAN# show crypto pki trustpoints status

crypto pki trustpoint SYSLOG-SIGNING-CA
  enrollment url bootflash:vmanage-admin/
  fqdn none
  fingerprint xxxxxx
  revocation-check none
  rsakeypair SYSLOG-SIGNING-CA 2048
  subject-name CN=CSR-cbc47d9d-45bf-433a-9816-1f12a8b48223_vManage Root CA
```

Syslog-signing-CA 証明書のデバイス上のトラストポイントを確認します

```
Cisco XE SD-WAN# show crypto pki trustpoints SYSLOG-SIGNING-CA status

Trustpoint SYSLOG-SIGNING-CA:

 Issuing CA certificate not configured.

State:

Keys generated ..... No

 Issuing CA authenticated ..... No

  Certificate request(s) ..... None
```

Cisco vManage NMS 監査ログの Syslog サーバーへのエクスポート

表 *22 :* 機能の履歴

機能名	リリース情報	説明
vManage 監査ログを Syslog としてエクスポート	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	Cisco vManage NMS は、監査ログを syslog メッセージ形式で、構成済みの外部 syslog サーバーにエクスポートします。この機能により、ネットワーク アクティビティ ログを一元的な場所に統合して保存できます。

Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス では、CLI を使用してイベント通知システムログ（syslog）メッセージをローカルデバイス上またはリモートホスト上のファイルに記録できます。これらのイベント通知ログは、システムログファイルに変換され、syslog サーバーにエクスポートされます。その後、syslog サーバーからシステムログ情報を取得できます。

CLI を使用したシステムロギングの設定

Syslog メッセージをローカルデバイスに記録する

デフォルトでは、ローカルデバイス上のファイルに syslog メッセージを記録するときには、「情報」の優先度レベルが有効になっています。次のコマンドを使用します。

1. **logging disk**

   ハードディスクに syslog メッセージを記録します

   例：

   ```
   vm01(config-system)# logging disk
   ```

2. **enable**

   ディスクへのロギングを有効にします

   例：

   ```
   vm01(config-logging-disk)# enable
   ```

3. **file size** *size*

   syslog ファイルのサイズをメガバイト（MB）で指定します。デフォルトでは、syslog ファイルは 10 MB です。syslog ファイルのサイズは 1 ～ 20 MB に設定できます。

   例：

   ```
   vm01(config-logging-disk)# file size 3
   ```

4. **file rotate** *number*

   ファイルのサイズに基づいて、1 時間ごとに syslog ファイルをローテーションします。デフォルトでは、10 個の syslog ファイルが作成されます。rotate コマンドは、1 ～ 10 の数値に設定できます。

   例：

   ```
   vm01(config-logging-disk)# file rotate 3
   ```

logging disk コマンドの詳細については、「logging disk」コマンドを参照してください。

Syslog メッセージをリモートデバイスに記録する

イベント通知システムログ（syslog）メッセージをリモートホストに記録するには、次のコマンドを使用します。

1. **logging server**

   syslog メッセージをリモートホストまたは syslog サーバーに記録します。サーバーの名前は、DNS 名、ホスト名、または IP アドレスで設定できます。最大 4 つの syslog サーバーを設定できます。

   例：

   ```
   vm01(config-system)# logging server 192.168.0.1
   ```

2. （オプション）**vpn** *vpn-id*

   syslog サーバーの VPN ID を指定します

3. （オプション）**source interface** *interface-name*

   syslog サーバーに到達するソースインターフェイスを指定します。インターフェイス名は、物理インターフェイスまたはサブインターフェイス（VLAN タグ付きインターフェイス）にすることができます。インターフェイスが syslog サーバーと同じ VPN にあることを確認します。それ以外の場合、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。

   例：

   ```
   vm01(config-server-192.168.0.1)# source interface eth0
   ```

4. **priority** *priority*

   保存する syslog メッセージの重大度を指定します。デフォルトのプライオリティ値は「情報」であり、デフォルトでは、すべての syslog メッセージが記録されます。

   例：

   次の例では、syslog の優先度をログアラート条件に設定します。

   ```
   vm01(config-server-192.168.0.1)# priority alert
   ```

syslog サーバーに到達できない場合、システムは syslog メッセージの送信を 180 秒間停止します。サーバーが到達可能になると、ロギングが再開されます。logging server コマンドの詳細については、「logging server」コマンドを参照してください。

システムロギング情報の表示

リモートホストに syslog メッセージを記録した後にシステムログ設定を表示するには、**show logging** コマンドを使用します。次に例を示します。

```
vm01(config-server-192.168.0.1)# show logging

System logging
    server 192.168.0.1
    source interface eth0
    exit
!
!
```

syslog ファイルの内容を表示するには、**show log** コマンドを使用します。次に例を示します。

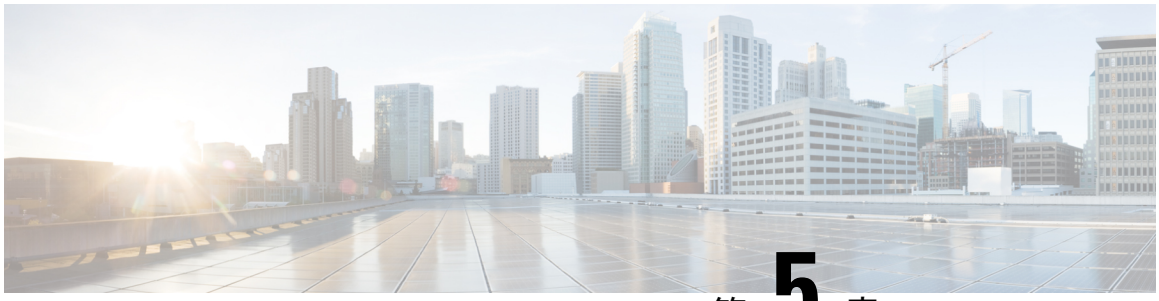
```
vm01(config-server-192.168.0.1)# show log nms/vmanage-syslog.log tail 10
```

Cisco vManage から設定されたシステムロギング設定を表示するには、監査ログを参照してください。

Cisco vManage からデバイス固有の syslog ファイルを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから **[Administration]** > **[Settings]** を選択し、[Data Stream] を有効にしていることを確認します。
2. Cisco vManage のメニューから **[Monitor]** > **[Devices]** を選択し、Cisco IOS XE SD-WAN デバイスを選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから **[Monitor]** > **[Network]** を選択し、Cisco IOS XE SD-WAN デバイスを選択します。
3. [Troubleshooting] をクリックします。
4. [Logs] で、[Debug Log] をクリックします。
5. [Log Files] から、ログファイルの名前を選択してログ情報を表示します。



第 5 章

ユーザーアクセスと認証の設定

vManage NMS 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] 画面を使用します。

[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、vManage NMS 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。

強化されたパスワードの設定

表 *23 :* 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。
	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、事前定義された中程度のセキュリティまたは高セキュリティのパスワード条件を適用するように Cisco vManage を設定できます。

強力なパスワードの強制

強力なパスワードの使用を推奨します。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。

パスワードポリシールールを有効にした後は、新しいユーザー用に作成されるパスワードはルールで定義されている要件を満たす必要があります。さらに、Cisco vManage リリース 20.9.1 以降のリリースでは、既存のパスワードがルールで定義されている要件を満たしていない場合、次回のログイン時にパスワードを変更するように求められます。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Password Policy] で、[Edit] を選択します。
3. Cisco vManage リリースに基づいて、次のいずれかのアクションを実行します。
   - Cisco vManage リリース 20.9.1 より前のリリースの場合は、[Enabled] をクリックします。
   - Cisco vManage リリース 20.9.1 以降のリリースの場合は、[Medium Security] または [High Security] をクリックしてパスワード条件を選択します。

   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、パスワードの変更を求めるバナーが表示されます。パスワードの有効期限が 60 日以上の場合、このバナーはパスワードの有効期限が切れる 30 日前に最初に表示されます。パスワードの有効期限が 60 日未満の場合、このバナーは、有効期限に設定されている日数の半分の時点で最初に表示されます。有効期限が切れる前にパスワードを変更しないと、ログインがブロックされます。このようなシナリオでは、管理者ユーザーがパスワードを変更してアクセスを復元できます。

（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。

5. [Save] をクリックします。

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。

- 次のパスワード要件は、Cisco vManage リリース 20.9.1 より前のリリースに適用されます。
  - 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。
  - 次の特殊文字のうち少なくとも 1 つを含む必要があります。# ? ! @ $ % ^ & * -。
  - ユーザーのフルネームまたはユーザー名を含まない。
  - 以前に使用したパスワードを再利用しない。
  - パスワード内の少なくとも 4 つの位置に異なる文字を含む。
- 最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1：

パスワード条件	要件
中レベルセキュリティ	• 最低 8 文字を含む • 32 文字以下にする • 少なくとも 1 つの小文字を含む • 少なくとも 1 つの大文字を含む • 少なくとも 1 つの数字を含む • 次の特殊文字を少なくとも 1 つ含む：# ? ! @ $ % ^ & * - • 最近使用した 5 つのパスワードのいずれかと同じではない • ユーザーのフルネームまたはユーザー名を含まない
高レベルセキュリティ	• 最低 15 文字を含む • 32 文字以下にする • 少なくとも 1 つの小文字を含む • 少なくとも 1 つの大文字を含む • 少なくとも 1 つの数字を含む • 次の特殊文字を少なくとも 1 つ含む：# ? ! @ $ % ^ & * - • 最近使用した 5 つのパスワードのいずれかと同じではない • ユーザーのフルネームまたはユーザー名を含まない • 少なくとも 8 文字が古いパスワードと同じ位置にない

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に、パスワード入力を連続して 5 回まで試行できます。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 （70 ページ）を参照してください。

パスワードをリセットするときは、新しいパスワードを設定する必要があります。古いパスワードを使用してパスワードをリセットすることはできません。

（注） Cisco vManage リリース 20.6.4、および Cisco vManage リリース 20.9.1 以降のリリースでは、ログアウトしたユーザー、またはローカルまたはリモート TACACS サーバーでパスワードが変更されたユーザーは、古いパスワードを使用してログインすることはできません。ユーザーは、新しいパスワードを使用してのみ、ログインできます。

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]（**[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. **[. . .]** をクリックし、[Reset Locked User] を選択します。
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。

CLI を使用したロックされたユーザーのリセット

次のように CLI を使用して、ロックされたユーザーをリセットできます。

1. admin ユーザーとしてデバイスにログインします。
2. 次のコマンドを実行します。

   デバイス# request aaa unlock-user *username*
3. プロンプトが表示されたら、ユーザーの新しいパスワードを入力します。

ユーザの管理

Cisco vManage のメニューで、**[Administration]** > **[Manage Users]** を選択し、ユーザーおよびユーザーグループを追加、編集、表示、または削除します。

次の点に注意してください。

- **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。
- 各ユーザーグループには、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。
- 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 *24 :* ユーザーグループ権限：*Cisco IOS XE SD-WAN* デバイス

機能	読み取り権限	書き込み権限
アラーム	**[Monitor]** > **[Logs]** > **[Alarms]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページで、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。

機能	読み取り権限	書き込み権限
監査ログ	**[Monitor]** > **[Logs]** > **[Alarms]** ページと **[Monitor]** > **[Logs]** > **[Audit Log]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページと **[Monitor]** > **[Audit Log]** ページで、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]** ウィンドウで、証明書署名要求（CSR）と証明書を表示します。	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** ウィンドウで、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]** ウィンドウで、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、コントローラデバイスを無効化します。

機能	読み取り権限	書き込み権限
CLI アドオンテンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで CLI アドオン機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、CLI アドオン機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。
Cloud OnRamp	**[Configuration]** > **[Cloud OnRamp for SaaS]** および **[Configuration]** > **[Cloud OnRamp for IaaS]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。
[Cluster]	**[Administration]** > **[Cluster Management]** ウィンドウで、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]** ウィンドウで、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。
コロケーション	**[Configuration]** > **[Cloud OnRamp for Colocation]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
[Config Group] > **[Device]** > **[Deploy]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	この権限では、機能は提供されません。	設定を Cisco IOS XE SD-WAN デバイス に展開します。 （注） 既存の機能設定を編集するには、[Template Configuration] の書き込み権限が必要です。
デバイス CLI テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウでデバイス CLI テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、デバイス CLI テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。

機能	読み取り権限	書き込み権限
デバイス インベントリ	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、オーバーレイネットワークの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]** ウィンドウで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 **[Monitor]** > **[Devices]** ページで（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、SD-WAN Application Intelligence Engine（SAIE）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。 （注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープパケットインスペクション（DPI）フローと呼ばれていました。 Cisco vManage リリース 20.6.x 以前のリリース：デバイス情報は **[Monitor]** > **[Network]** ページに表示されます。	**[Monitor]** > **[Devices]** ページで（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。

機能	読み取り権限	書き込み権限
デバイス リブート	**[Maintenance]** > **[Device Reboot]** ウィンドウで、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]** ウィンドウで、1 つまたは複数のデバイスを再起動します。
ディザスタ リカバリ	**[Administration]** > **[Disaster Recovery]** ウィンドウで、Cisco vManage 上で実行されているアクティブクラスタとスタンバイクラスタに関する情報を表示します。	追加の権限はありません。
[Event]	**[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Events]** ページで、デバイスの地理的な位置を表示します。	**[Monitor]** > **[Logs]** > **[Events]** ページで（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。
[Feature Profile] > **[Other]** > **[Thousandeyes]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Dhcp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [DHCP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [DHCP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Lan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Svi]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [SVI Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [SVI Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Service Profile] セクションで [Routing/BGP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Service Profile] セクションで [Routing/BGP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Routing/Ospf]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Service Profile] セクションで [Routing/OSPF] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Service Profile] セクションで [Routing/OSPF] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Switchport]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Service Profile] セクションで [Switchport] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Service Profile] セクションで [Switchport] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Wirelesslan]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Aaa]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [AAA] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [AAA] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Banner]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Banner] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Banner] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Basic]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Basic] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Basic] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Bfd]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [BFD] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [BFD] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Global]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Global] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Global] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Logging]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Logging] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Logging] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Ntp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [NTP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [NTP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Omp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [OMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [OMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Snmp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [SNMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [SNMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Controller]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Profile]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Management/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [Management VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Management VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Management/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [Management Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Management VPN and Management Internet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Tracker]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Tracker] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Tracker] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Cellular]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
統合管理	**[Administration]** > **[Integration Management]** ウィンドウで、Cisco vManage で実行中のコントローラに関する情報を表示します。	追加の権限はありません。
ライセンス管理	**[Administration]** > **[License Management]** ウィンドウで、Cisco vManage で実行中のデバイスのライセンス情報を表示します。	**[Administration]** > **[License Management]** ページで、Cisco スマートアカウントの使用を設定し、管理するライセンスを選択して、Cisco vManage とライセンスサーバー間でライセンス情報を同期します。
インターフェイス（**Interface**）	**[Monitor]** > **[Network]** > **[Interface]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのインターフェイスに関する情報は **[Monitor]** > **[Network]** > **[Interface]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Interface]** ページで、[Chart Options] を編集して、表示するデータのタイプを選択し、データを表示する期間を編集します。

機能	読み取り権限	書き込み権限
ユーザーの管理	**[Administration]** > **[Manage Users]** ウィンドウで、ユーザーとユーザーグループを表示します。	**[Administration]** > **[Manage Users]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、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。
その他の機能テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。
ポリシー	**[Configuration]** > **[Policies]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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。

機能	読み取り権限	書き込み権限
ポリシーの展開	**[Configuration]** > **[Policies]** ウィンドウで、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]** ウィンドウで、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。
RBAC VPN	**[Monitor]** > **[VPN]** ページで、ロールに基づいて VPN グループとセグメントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Dashboard]** > **[VPN Dashboard]** ページで、ロールに基づいて VPN グループとセグメントを表示します。	**[Administration]** > **[VPN Groups]** ウィンドウで、Cisco vManage の VPN と VPN グループを追加、編集、および削除し、VPN グループの権限を編集します。
ルーティング	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのリアルタイムルーティングに関する情報は **[Monitor]** > **[Network]** > **[Real-Time]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、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。
セキュリティ	**[Configuration]** > **[Security]** ウィンドウで、セキュリティ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]** > **[Security]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。
セキュリティポリシー設定	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、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。	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。

機能	読み取り権限	書き込み権限
セッション管理	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、ユーザーセッションを表示します。	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーセッションを編集します。
Settings	**[Administration]** > **[Settings]** ウィンドウで、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表示します。	**[Administration]** > **[Settings]** ウィンドウで、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。
SIG テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。

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]** ウィンドウで、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]** ウィンドウで、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 Template]** ウィンドウで、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。 （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。	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、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設定します。 （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。
テンプレートの設定	**[Configuration]** > **[Templates]** ウィンドウで、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]** ウィンドウで、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。 （注） Cisco vManage リリース 20.7.1 以降、デバイスにすでにアタッチされているテンプレートを作成、編集、または削除するには、ユーザーに [Template Deploy] オプションに対する書き込み権限が必要です。

機能	読み取り権限	書き込み権限
テンプレートの展開	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにアタッチされているデバイスを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにデバイスをアタッチします。
ツール	**[Tools]** > **[Operational Commands]** ウィンドウで、**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]** ウィンドウで、**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]** ウィンドウで、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]** ウィンドウで、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。
vAnalytics	**[Cisco vManage]** > **[vAnalytics]** ウィンドウで vAnalytics を起動します。	追加の権限はありません。
Workflows	**[Cisco vManage]** > **[Workflows]** ウィンドウからワークフローライブラリを起動します。	追加の権限はありません。

マルチテナント環境の RBAC ユーザーグループ

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 *25 :* 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 メニューから **[Administration]** > **[Manage Users]** を選択します。
2. デフォルトでは、[Users] 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、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、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] ドロップダウンリストで、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. [Add] をクリックします。

ユーザーの削除

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。

ユーザーを削除するには、次の手順を実行します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。

2. 削除するユーザーの [...] をクリックし、[Delete] をクリックします。
3. ユーザーの削除を確認するには、[OK] をクリックします。

ユーザーの詳細の編集

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。

ユーザーの詳細情報を編集するには、次のようにします。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. 編集するユーザーの [...] をクリックし、[Edit] をクリックします。
3. ユーザー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。

ユーザー 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。

はじめる前に

管理者ユーザーのパスワードを変更する場合は、この手順を実行する前に、クラスタ内のすべての Cisco vManage インスタンスからデバイステンプレートをアタッチ解除してください。この手順を完了した後、デバイステンプレートを再アタッチできます。

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. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. パスワードを変更するユーザーの [...] 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。

（注） 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 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. [Hostname] 列で、使用するデバイスを選択します。
3. [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 メニューから **[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。

（注） 特殊文字 ! を含むユーザーパスワードは二重引用符（" "）で囲みます。パスワード全体を二重引用符で囲まない場合、構成データベース（?）はこの特殊文字をスペースとして扱い、パスワードの残りの部分を無視します。

たとえば、パスワードが C!sc0 の場合は、"C!sc0" を使用します。

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）。

ユーザーグループの管理

ユーザーはグループに配置されます。グループは、ユーザーが表示および変更を許可されている特定の構成および操作コマンドを定義します。1 人のユーザーが 1 つ以上のグループに属することができます。Cisco SD-WAN ソフトウェアには標準ユーザーグループが用意されており、必要に応じてカスタムユーザーグループを作成できます。

- [basic]：インターフェイスおよびシステム情報を表示する権限を持つユーザーが含まれます。
- [netadmin]：Cisco vManage ですべての操作を実行できる管理者ユーザーがデフォルトで含まれます。このグループに他のユーザーを追加できます。

- [operator]：情報を表示する権限のみを持つユーザーを含みます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：非セキュリティポリシーの表示と変更、デバイステンプレートのアタッチとデタッチ、非セキュリティデータの監視など、セキュリティ以外の操作を Cisco vManage で実行できるユーザーが含まれます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：セキュリティポリシーの表示と変更、セキュリティデータの監視など、セキュリティ操作を Cisco vManage で実行できるユーザーが含まれます。

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。

ユーザーグループの削除

不要になったユーザーグループは削除できます。たとえば、特定のプロジェクト用に作成したユーザーグループを、そのプロジェクトの終了時に削除する場合があります。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 削除するユーザーグループの名前をクリックします。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）は削除できません。

4. [Trash] アイコンをクリックします。
5. ユーザーグループの削除を確認するには、[OK] をクリックします。

ユーザーグループ権限の編集

既存のユーザーグループのグループ権限を編集できます。この手順では、必要なユーザーグループの構成済み機能の読み取りおよび書き込みアクセス許可を変更できます。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 権限を編集するユーザーグループの名前を選択します。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）の権限は編集できません。

4. [Edit] をクリックし、必要に応じて権限を編集します。
5. **[Save]** をクリックします。

admin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。

CLI を使用したグループの作成

Cisco SD-WAN ソフトウェアには、デフォルトのユーザーグループ（**basic**、**netadmin**、**operator**、**network_operations**、**security_operations**）が用意されています。ユーザー名 **admin** は自動的に **netadmin** ユーザーグループに配置されます。

必要に応じて、追加のカスタムグループを作成し、グループメンバーが持つ権限ロールを設定できます。特定の権限を持つカスタムグループを作成するには、グループ名と権限を設定します。

```
デバイス(config)# aaa authentication login user1 group radius enable
デバイス(config)# aaa authentication login user2 group radius enable
デバイス(config)# aaa authentication login user3 group radius enable
デバイス(config)#
```

group-name 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。名前に大文字は使用できません。一部のグループ名は予約されているため、設定できません。それらのリストについては、aaa 設定コマンドを参照してください。

リモート RADIUS または TACACS+ サーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。リモートサーバーが認証を検証し、VSA Cisco SD-WAN-Group-Name を使用してユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがローカルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

task オプションでは、グループメンバーが持つ権限ロールを一覧表示します。ロールは、**インターフェイス**、**ポリシー**、**ルーティング**、**セキュリティ**、および**システム**の 1 つ以上にすることができます。

Cisco vManage でのセッションの設定

表 *26 :* 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。

（注） プロバイダーアクセスがある場合にのみ、マルチテナント環境でクライアント セッション タイムアウトを編集できます。

1. Cisco vManage のメニューから、**[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. [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。セッションを期限切れにせずにアクティブなままにすると、デフォルトのセッションタイムアウト値である 24 時間後にセッションからログアウトされます。

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。

（注） プロバイダーアクセスがある場合にのみ、マルチテナント環境でセッションライフタイムを編集できます。

1. Cisco vManage のメニューから、**[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. [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。

（注） サーバー セッション タイムアウトは、プロバイダーアクセス権またはテナントアクセス権がある場合でも、マルチテナント環境では使用できません。

1. Cisco vManage のメニューから、**[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. [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。

（注） ユーザーあたりの最大セッション数は、プロバイダーアクセス権またはテナントアクセス権がある場合でも、マルチテナント環境では使用できません。

1. Cisco vManage のメニューから、**[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. [Save] をクリックします。

CLI を使用した RADIUS 認証の設定

Remote Authentication Dial-In User Service（RADIUS）は、無許可のアクセスに対してネットワークを保護する分散型クライアント/サーバーシステムです。RADIUS クライアントは RADIUS をサポートするシスコデバイス上で動作し、中央RADIUSサーバーに認証要求を送信します。RADIUS サーバーには、ユーザー認証情報とネットワーク サービス アクセス情報がすべて格納されます。

Cisco IOS XE SD-WAN デバイス でユーザー認証に RADIUS サーバーを使用するには、1 つまたは最大 8 つのサーバーを設定します。

```
デバイスconfig-transaction
デバイス(config)# radius server test address ipv4 10.1.1.55 acct-port 110
デバイス(config-radius-server)# key 33
デバイス(config-radius-server)# exit
デバイス(config)# radius server test address ipv4 10.1.1.55 auth-port 330
デバイス(config-radius-server)# key 55
デバイス(config-radius-server)#
```

RADIUS サーバーごとに、少なくともその IP アドレスとパスワードまたはキーを設定する必要があります。キーには、最大 31 文字のクリアテキスト文字列、または AES 128 ビット暗号化キーを指定できます。ローカルデバイスはキーをRADIUSサーバーに渡します。パスワードは、サーバーで使用されているものと一致する必要があります。複数のRADIUSサーバーを設定するには、サーバーごとに **server** コマンドと **secret-key** コマンドを使用します。

残りの RADIUS 設定パラメータはオプションです。

RADIUS サーバーの優先順位を設定する場合、複数の RADIUS サーバー間での選択または負荷分散の手段として、サーバーのプライオリティ値を設定します。優先順位には、0 から 7 までの値を指定できます。優先順位番号が小さいサーバーは、番号が大きいサーバーよりも優先されます。

デフォルトでは、 Cisco IOS XE SD-WAN デバイス は RADIUS サーバーへの認証接続にポート 1812 を使用し、アカウンティング接続にポート 1813 を使用します。これらのポート番号を変更するには、**auth-port** および **acct-port** コマンドを使用します。

特定のインターフェイスを介して RADIUS サーバーに到達できる場合は、**source-interface** コマンドを使用してそのインターフェイスを設定します。

特定のサーバーを AAA、IEEE 802.1X、および IEEE 802.11i の認証とアカウンティングに使用できるように、RADIUS サーバーにタグを付けることができます。ここで、4 ～ 16 文字の文字列でタグを定義します。次に、AAA を設定するとき、および 802.1X および 802.11i のインターフェイスを設定するときに、タグを **radius-servers** コマンドに関連付けます。

RADIUS サーバーが Cisco IOS XE SD-WAN デバイス とは異なる VPN にある場合は、サーバーの VPN 番号を設定して、 Cisco IOS XE SD-WAN デバイス が検出できるようにします。複数の RADIUS サーバーを設定する場合は、すべてが同じ VPN 内にある必要があります。

RADIUS サーバーからの応答を待機する場合、 Cisco IOS XE SD-WAN デバイス は 3 秒間待機してから要求を再送信します。この時間間隔を変更するには、**timeout** コマンドを使用して、1 ～ 1000 秒の値を設定します。

```
デバイス# config-transaction
 デバイス(config)# aaa group server radius server-10.99.144.201
 デバイス(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5
retransmit 3
```

SSH 認証の設定

表 *27:* 機能の履歴

機能名	リリース情報	説明
RSA キーを使用したセキュアシェル認証	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能は、クライアントと Cisco SD-WAN サーバー間の通信を保護することにより、RSA キーを設定するのに役立ちます。

セキュアシェル（SSH）プロトコルは、ネットワークデバイスへの安全なリモートアクセス接続を提供します。

SSHは、公開鍵と秘密鍵を使用したユーザー認証をサポートしています。SSH認証を有効にするために、ユーザーの公開鍵は、次の場所にある認証ユーザーのホームディレクトリに保存されます。

```
~<user>/.ssh/authorized_keys
```

秘密鍵を所有するクライアントマシンで新しい鍵が生成されます。SSHサーバーの公開鍵を使用して暗号化されたメッセージは、クライアントの秘密鍵を使用して復号化されます。

Cisco SD-WAN での SSH 認証の制約事項

- Cisco IOS XE SD-WAN デバイス でサポートされる SSH RSA キーサイズの範囲は 2048 ～ 4096 です。1024 および 8192 の SSH RSA キーサイズはサポートされていません。
- Cisco IOS XE SD-WAN デバイス では、ユーザーごとに最大 2 つのキーを使用できます。

Cisco IOS XE SD-WAN デバイス での vManage を使用した SSH 認証

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。

（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。

3. [Select Devices] で、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。
4. [Basic Information] から、[CISCO AAA] テンプレートを選択します。
5. [Local] から、[New User] をクリックし、詳細を入力します。
6. [SSH RSA Key] を入力します。

（注） [SSH RSA Key] の id_rsa.pub ファイルから完全な公開キーを入力する必要があります。

Cisco IOS XE SD-WAN デバイスで CLI を使用して SSH 認証を設定する

SSH キーベースのログインは、IOS でサポートされています。ユーザーごとに最大 2 つのキーをサポートできます。また、IOS は RSA ベースのキーのみをサポートします。

従来の IOS CLI では、次のサポートが可能です。

•キー文字列

• キーハッシュ：キー文字列は base64 でデコードされ、MD5 ハッシュが実行されます。

ただし、トランザクションヤンモデルには、（キー文字列全体ではなく）キーハッシュのみをコピーする規定があります。vManageはこの変換を行い、構成をデバイスにプッシュします。

Cisco IOS XE SD-WAN デバイス でサポートされる公開鍵

- SSH-RSA

認証順序の設定

認証順序では、SSH セッションまたはコンソールポートを介して Cisco IOS XE SD-WAN デバイスに対するユーザーアクセスを確認するときに認証方式が試行される順序を指示します。デフォルトの認証順序は、**local**、**radius**、**tacacs** の順です。デフォルトの認証順序では、認証プロセスは次の順序で実行されます。

- 認証プロセスでは、まず、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在するかどうかがチェックされます。
- ローカル認証が失敗し、認証フォールバックを（**auth-fallback** コマンドで）設定していない場合、認証プロセスは停止します。しかし、認証フォールバックを設定している場合、認証プロセスは次に RADIUS サーバーをチェックします。この方法を機能させるには、**system radius server** コマンドを使用して 1 つ以上の RADIUS サーバーを設定する必要があります。RADIUS サーバーに到達できる場合、ユーザーはそのサーバーの RADIUS データベースに基づいて認証またはアクセス拒否されます。RADIUS サーバーに到達できず、複数の RADIUS サーバーを設定している場合、認証プロセスは各サーバーを順番にチェックし、そのうちの 1 つに到達できると停止します。その後、ユーザーは、そのサーバーの RADIUS データベースに基づいて認証またはアクセス拒否されます。
- RADIUS サーバーに到達できない（つまり、すべてのサーバーに到達できない）場合、認証プロセスは TACACS+ サーバーをチェックします。この方法を機能させるには、**system tacacs server** コマンドを使用して 1 つ以上の TACACS+ サーバーを設定する必要があります。TACACS+ サーバーに到達できる場合、ユーザーはそのサーバーの TACACS+ データベースに基づいて認証またはアクセス拒否されます。TACACS+ サーバーに到達できず、複数の TACACS+ サーバーを設定している場合、認証プロセスは各サーバーを順番にチェックし、そのうちの 1 つに到達できると停止します。その後、ユーザーは、そのサーバーの TACACS+ データベースに基づいて認証またはアクセス拒否されます。
- TACACS+ サーバーに到達できない場合（つまり、すべての TACACS+ サーバーに到達できない場合）、ローカル Cisco IOS XE SD-WAN デバイスへのユーザーアクセスは拒否されます。

最初に試行するものから優先順で、1 つ、2 つ、または 3 つの認証方法を指定します。認証方法を 1 つだけ設定する場合は、**ローカル**である必要があります。

このコマンドを含めない場合、「admin」ユーザーは常にローカルで認証されます。

第2または第3の認証メカニズムへのフォールバックは、ユーザーによって提供されたログイン情報が無効であるためか、サーバーに到達できないために、より優先度の高い認証サーバーがユーザーの認証に失敗したときに発生します。

次に、デフォルトの認証動作と、認証フォールバックが有効になっている場合の動作の例を示します。

- 認証順序が **radius local** として設定されている場合：
  - デフォルトの認証では、ローカル認証は、すべてのRADIUSサーバーに到達できない場合にのみ使用されます。RADIUS サーバーを介した認証の試行が失敗した場合、ユーザーは、ローカル認証に正しいログイン情報を提供した場合でも、ログインを許可されません。
  - 認証フォールバックを有効にすると、すべての RADIUS サーバーに到達できない場合、またはRADIUSサーバーがユーザーに対してアクセスを拒否した場合に、ローカル認証が使用されます。
- 認証順序が **local radius** として設定されている場合：
  - デフォルトの認証では、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在しない場合、RADIUS 認証が試行されます。
  - 認証フォールバックを有効にすると、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在しない場合に、RADIUS認証が試行されます。この場合、2 つの認証方式の動作は同じです。
- 認証順序が **radius tacacs local** として設定されている場合：
  - デフォルトの認証では、すべての RADIUS サーバーに到達できない場合にのみ TACACS+ が試行され、すべてのTACACS+サーバーに到達できない場合にのみ、ローカル認証が試行されます。RADIUS サーバーを介した認証の試行が失敗した場合、ユーザーは、TACACS+ サーバーに正しいログイン情報を提供した場合でも、ログインを許可されません。同様に、TACACS+ サーバーがアクセスを拒否した場合、ユーザーはローカル認証を介してログインできません。
  - 認証フォールバックを有効にすると、すべての RADIUS サーバーに到達できない場合、またはRADIUSサーバーがユーザーのアクセスを拒否した場合に、TACACS+認証が使用されます。続いて、すべてのTACACS+サーバーに到達できない場合、またはTACACS+サーバーがユーザーに対してアクセスを拒否した場合に、ローカル認証が使用されます。

リモートサーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。

リモートサーバーが認証を検証し、ユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがローカルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

リモートサーバーが認証を検証し、そのユーザーがローカルに設定されていない場合、ユーザーは、**basic** ユーザーとして vshell にログインし、ホームディレクトリは /home/basic になります。

リモートサーバーが認証を検証し、そのユーザーがローカルに設定されている場合、ユーザーはローカルユーザー名（たとえば、eve）で vshell にログインし、ホームディレクトリは /home/*username*（つまり、/home/eve）になります。

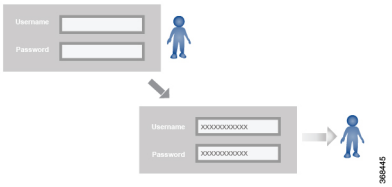
AAA を使用したロールベースアクセス

Cisco SD-WAN AAA ソフトウェアは、ロールベースのアクセスを実装して、Cisco IOS XE SD-WAN デバイス のユーザーの認可権限を制御します。ロールベースのアクセスは、次の 3 つのコンポーネントで構成されます。

- ユーザーは、Cisco IOS XE SD-WAN デバイス へのログインが許可されているユーザーです。
- ユーザーグループは、ユーザーのコレクションです。
- 権限は各グループに関連付けられています。これらは、グループのユーザーが発行を許可されているコマンドを定義します。

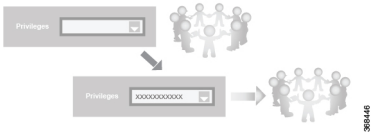
ユーザーとユーザーグループ

Cisco IOS XE SD-WAN デバイス での操作の実行が許可されているすべてのユーザーは、ログインアカウントを持っている必要があります。ログインアカウントについては、デバイス自体でユーザー名とパスワードを設定します。これらにより、ユーザーはそのデバイスにログインできます。ユーザーがアクセスを許可されている各デバイスで、ユーザー名とパスワードを設定する必要があります。



Cisco SD-WAN ソフトウェアは、UNIX スーパーユーザーと同様な、完全な管理者権限を持つユーザーである **admin** という 1 つの標準ユーザー名を提供します。デフォルトでは、**admin** ユーザー名のパスワードは**admin** です。このユーザー名を削除または変更することはできませんが、デフォルトのパスワードは変更できますし、変更する必要があります。

ユーザーグループは、Cisco IOS XE SD-WAN デバイス で共通のロールまたは権限を持つユーザーをプールします。ログインアカウント情報の構成の一環として、ユーザーがメンバーであるユーザーグループを指定します。**admin**ユーザーのグループを指定する必要はありません。このユーザーは自動的にユーザーグループ **netadmin** に属し、Cisco IOS XE SD-WAN デバイス でのすべての操作の実行が許可されるためです。



ユーザーグループ自体は、そのグループに関連付けられた権限を設定する場所です。これらの権限は、ユーザーが実行を許可されている特定のコマンドに対応し、Cisco SD-WAN ソフトウェア要素への役割ベースのアクセスを効果的に定義します。

Cisco SD-WAN ソフトウェアは、次の標準ユーザーグループを提供します。

- [basic]：[basic] グループは設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、デバイス上の情報を表示および変更する権限を持つユーザーを含むように設計されています。
- [operator]：[operator] グループも設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、情報を表示する権限のみを持つユーザーを含むように設計されています。
- [netadmin]：[netadmin] グループは設定不可能なグループです。デフォルトでは、このグループには**admin**ユーザーが含まれます。このグループに他のユーザーを追加できます。このグループのユーザーは、デバイスですべての操作を実行できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：[network_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上でセキュリティポリシー以外のすべての操作を実行でき、セキュリティポリシー情報は表示のみが可能です。たとえば、ユーザーはテンプレート設定を作成または変更し、災害復旧を管理し、アプリケーション対応ルーティングポリシーや CFlowD ポリシーなどの非セキュリティポリシーを作成できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：[security_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上ですべてのセキュリティ操作を実行でき、セキュリティポリシー以外の情報は表示のみが可能です。たとえば、ユーザーはUmbrellaキー、ライセンス、IPS 署名の自動更新、TLS/SSL プロキシ設定などを管理できます。

[network_operations] グループのユーザーは、デバイスへのポリシーの適用、適用されたポリシーの取り消し、およびデバイステンプレートの編集を許可されています。[security_operations] グループのユーザーは、デバイスにセキュリティポリシーを展開するために、[network_operations] ユーザーによる 0 日目の介入と、展開されたセキュリティポリシーを削除するために、N 日目の介入が必要です。ただし、セキュリティポリシーがデバイスに展開された後は、[security_operations] ユーザーは、[network_operations] ユーザーの介入を必要とせずにセキュリティポリシーを変更できます。

（注） 実行中の設定およびローカル設定を表示できるのは管理ユーザーのみです。事前定義された [operator] ユーザーグループに関連付けられたユーザーは、実行中の設定およびローカル設定にアクセスできません。事前定義されたユーザーグループ [operator] には、テンプレート設定の読み取りアクセスのみがあります。管理者ユーザー権限のサブセットのみが必要な場合は、機能リストから選択した機能を使用して、読み取りと書き込みの両方のアクセス権を持つ新しいユーザーグループを作成し、そのグループをカスタムユーザーに関連付ける必要があります。

ロールベースのアクセス権限

ロールベースのアクセス権限は、タスクと呼ばれる 5 つのカテゴリに分類されます。

- インターフェイス：Cisco IOS XE SD-WAN デバイス 上のインターフェイスを制御するための権限。
- ポリシー：コントロール プレーン ポリシー、OMP、およびデータプレーンポリシーを制御するための権限。
- ルーティング：BFD、BGP、OMP、OSPF などのルーティングプロトコルを制御するための権限。
- セキュリティ：ソフトウェアや証明書のインストールなど、デバイスのセキュリティを制御するための権限。[netadmin] グループに属するユーザーのみがシステムにソフトウェアをインストールできます。
- システム：一般的なシステム全体の権限。

次のセクションの表は、ユーザーおよびユーザーグループの AAA 認証ルールの詳細を示しています。これらの認証ルールは、CLI から発行されたコマンドと Netconf から発行されたコマンドに適用されます。

操作コマンドのユーザー認証ルール

操作コマンドのユーザー認証ルールは、ユーザー名のみに基づいています。Cisco IOS XE SD-WAN デバイス にログインできるユーザーは、ほとんどの操作コマンドを実行できます。ただし、ソフトウェアのインストールとアップグレード、デバイスのシャットダウンなど、デバイスの基本的な操作に影響を与えるコマンドを発行できるのは **admin** ユーザーだけです。

どのユーザーも **config** コマンドを発行して設定モードに入ることができ、設定モードに入ると、一般的な設定コマンドを発行できることに注意してください。また、すべてのユーザーは、**system aaa user** *self* **password** *password* コマンドを発行して、その設定変更をコミットすることにより、自分のパスワードを設定することができます。デバイスの動作を設定する実際のコマンドでは、ユーザーグループのメンバーシップに従って承認が定義されます。「設定コマンドのユーザーグループの認証ルール」を参照してください。

次の表に、一般的な CLI コマンドの AAA 認証ルールを示します。注記があるものを除き、すべてのコマンドは操作コマンドです。また、「admin」ユーザーが使用できる一部のコマンドは、そのユーザーが「netadmin」ユーザーグループに属している場合にのみ使用できます。

CLI コマンド	すべてのユーザー	管理者ユーザ
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X（netadmin グループのユーザーのみ）
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X
poweroff	—	X（netadmin グループのユーザーのみ）
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X（netadmin グループのユーザーのみ）
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X（netadmin グループのユーザーのみ）
request execute request download request upload	X	X
request（その他すべて）	—	×

CLI コマンド	すべてのユーザー	管理者ユーザ
rollback（設定モードコマンド）	—	X（netadmin グループのユーザーのみ）
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user self password password（設定モードコマンド）（注：ユーザーは自分自身を削除できません）		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X	X（netadmin グループのユーザーのみ）

操作コマンドのユーザーグループの認証ルール

操作コマンドのユーザーグループの認証ロールを次の表に示します。

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear app		X			
clear app-route		X			

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs：debug コマンドと同じ					
show dhcp					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

設定コマンドのユーザーグループの認証ルール

次の表に、設定コマンドのユーザーグループの認証ルールを示します。

コンフィギュレーション コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
[omp]		X	X		X
ポリシー		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn（作成、削除、命名を含むその他すべて）					X
wlan	X				

Cisco vManage テンプレートを使用した AAA の設定

表 *28 :* 機能の履歴

機能名	リリース情報	説明
許可とアカウンティング	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能では、許可（コマンドが実行される前に、ユーザーがデバイスに入力するコマンドを許可する）とアカウンティング（ユーザーがデバイスで実行するコマンドのレコードを生成する）を設定します。

Cisco vManage テンプレートを使用して AAA を設定すると、Cisco vManage で設定を行った後に、同じタイプの選択したデバイスにこの設定をプッシュできます。この手順は、同じタイプの複数のデバイスを一度に設定するのに便利な方法です。

Cisco vBond オーケストレーション、Cisco vManage インスタンス、Cisco vSmart コントローラ、および Cisco IOS XE SD-WAN デバイス には AAA テンプレートを使用します。

Cisco IOS XE SD-WAN デバイス では、RADIUS および TACACS+ と組み合わせた認証、許可、およびアカウンティング（AAA）の設定がサポートされます。

（注） PPP を使用している場合、または CHAP で MLPPP を使用している場合は、テンプレートを介して秘密鍵を使用してローカルユーザーを設定する必要があります。

[Template] 画面に移動しテンプレートを命名

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、[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] 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] を選択します。

6. AAA のカスタムテンプレートを作成するには、[Factory_Default_AAA_CISCO_Template] を選択し、[Create Template] をクリックします。AAA 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 AAA パラメータを定義するためのフィールドがあります。
7. [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。
8. [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、次のいずれかを選択します。

表 *29*：

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 IOS XE SD-WAN デバイス をデバイステンプレートにアタッチするときに、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 IOS XE SD-WAN デバイスをデバイステンプレートにアタッチするときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」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。

ユーザーとユーザーグループのローカルアクセスの設定

ユーザーおよびユーザーグループのデバイスへのローカルアクセスを設定できます。ローカルアクセスは、RADIUS または TACACS+ 認証が失敗した場合にデバイスへのアクセスを提供します。

個々のユーザーのローカルアクセスを構成するには、[Local] を選択します。

新しいユーザーを追加するには、[Local] から [+ New User] をクリックし、次のパラメータを設定します。

表 *30 :*

パラメータ名	説明
Name	ユーザの名前を入力します。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。 次のユーザー名は予約されているため、設定できません。backup、basic、bin、daemon、games、gnats、irc、list、lp、mail、man、news、nobody、proxy、quagga、root、sshd、sync、sys、uucp、および www-data。また、viptela-reserved で始まる名前は予約されています。
パスワード	ユーザーのパスワードを入力します。 各ユーザー名にはパスワードが必要です。ユーザーは自分のパスワードを変更できます。 管理ユーザーのデフォルトパスワードは admin です。このパスワードから変更することを強く推奨します。 （注） Cisco vManage AAA テンプレートを使用してローカルユーザーを設定する場合、Cisco vManage は Cisco タイプ 9 パスワードタイプを使用します。Cisco タイプ 9 パスワードタイプは、ローカルユーザーのパスワードをハッシュするために scrypt アルゴリズムを使用します。Cisco vManage AAA テンプレートは、ローカルユーザーのパスワードのハッシュに Cisco タイプ 9 パスワードタイプだけを使用します。 デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用してローカルユーザーを設定する場合、ローカルユーザーのパスワードのハッシュに他の Cisco パスワードタイプを選択できます。詳細については、「CLI アドオンテンプレートを使用したタイプ 6 パスワードの設定」を参照してください。

パラメータ名	説明
Privilege Level 1 OR 15	特権レベル 1 または 15 から選択します。 • [Level 1]：ユーザー EXEC モード。読み取り専用です。アクセスできるコマンドは `ping` などに限定されています。 • [Level 15]：特権 EXEC モード。`reload` コマンドなど、すべてのコマンドにアクセスできます。また設定の変更も可能です。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです
SSH RSA キー	[+ Add] ボタンをクリックして、SSH RSA キーを追加します。SSH RSA キーを貼り付けるための新しいフィールドが表示されます。キーを削除するには、[-] ボタンをクリックします。 デバイスは、最大 2 の SSH RSA キーをサポートします。

[Add] をクリックして、新しいユーザーを追加します。[+ New User] をもう一度クリックして、さらにユーザーを追加します。

ユーザーグループのローカルアクセスを設定するには、最初にユーザーを基本グループまたはオペレータグループのいずれかに配置します。admin は自動的に netadmin グループに配置されます。次に、ユーザーグループを設定します。この設定を行うには、[Local] から [User Group] を選択します。

[+ New User Group] をクリックし、次のパラメータを設定します。

表 *31 :*

パラメータ名	説明
Name	認証グループの名前。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。Cisco SD-WAN ソフトウェアには、basic、netadmin、および operator の 3 つの標準ユーザーグループが用意されています。ユーザー admin は自動的にグループ netadmin に配置され、このグループの唯一のユーザーです。RADIUS または TACACS+ サーバーから学習したすべてのユーザーは、グループ basic に配置されます。basic グループのすべてのユーザーは、operator グループのすべてのユーザーと同様の、タスクを実行するための同じ権限を持っています。次のグループ名は予約されているため、設定できません。adm、audio、backup、bin、cdrom、dialout、dip、disk、fax、floppy、games、gnats、input、irc、kmem、list、lp、mail、man、news、nogroup、plugdev、proxy、quagga、quaggavty、root、sasl、shadow、src、sshd、staff、sudo、sync、sys、tape、tty、uucp、users、utmp、video、voice、および www-data。また、文字列 viptela-reserved で始まるグループ名は予約されています。

パラメータ名	説明
機能タイプ	[Preset] をクリックして、ユーザーグループのプリセットロールのリストを表示します。[Custom] をクリックして、構成されている承認タスクのリストを表示します。
機能	機能テーブルには、ユーザーグループのロールが一覧表示されます。これらのロールは、インターフェイス、ポリシー、ルーティング、セキュリティ、およびシステムです。各ロールにより、ユーザーグループはデバイス構成の特定の部分の読み取りまたは書き込み、および特定のタイプの操作コマンドを実行できます。[Read]、[Write]、および [None] の適切なボックスをクリックして、各ロールのグループに権限を割り当てます。

[Add] をクリックして、新しいユーザーグループを追加します。

別のユーザーグループを追加するには、[+ New User Group] を再度クリックします。

ユーザーグループを削除するには、エントリの右側にあるごみ箱アイコンをクリックします。basic、netadmin、operator の 3 つの標準ユーザーグループは削除できません。

RADIUS 認証の設定

展開で RADIUS を使用している場合は、RADIUS 認証を設定します。

RADIUS サーバーへの接続を設定するには、[RADIUS] から [+ New Radius Server] をクリックし、次のパラメータを設定します。

表 *32:*

パラメータ名	説明
Address	RADIUS サーバーホストの IP アドレスを入力します。
Authentication Port	RADIUS サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。デフォルト：ポート 1812
Accounting Port	802.1X および 802.11i アカウンティング情報を RADIUS サーバーに送信するために使用する UDP ポートを入力します。 範囲：0 ～ 65535。デフォルト：1813。
タイムアウト	要求を再送信する前に、デバイスが RADIUS 要求への応答を待機する秒数を入力します。 デフォルト：5 秒。 範囲：1 ～ 1000

パラメータ名	説明
Retransmit Count	デバイスがRADIUS要求をサーバーに再送信する回数を入力します。デフォルト：5 秒。
[Key]（廃止）	認証および暗号化のために Cisco IOS XE SD-WAN デバイス が RADIUS サーバーに渡すキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、RADIUS サーバーで使用する AES 暗号化キーと一致させる必要があります。

[Add] をクリックして、新しい RADIUS サーバーを追加します。

別の RADIUS サーバーを追加するには、[+ New RADIUS Server] を再度クリックします。

サーバーを削除するには、ごみ箱アイコンをクリックします。

CLI の同等の設定：

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

TACACS+ 認証の設定

展開で TACACS+ を使用している場合は、TACACS+ 認証を設定します。

TACACS+ サーバーへの接続を設定するには、[TACACS] から [+ New TACACS Server] をクリックし、次のパラメータを設定します。

表 *33*：

パラメータ名	説明
Address	TACACS+ サーバーホストの IP アドレスを入力します。
Port	TACACS+ サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：ポート 49
タイムアウト	要求を再送信する前に、デバイスが TACACS+ 要求への応答を待機する秒数を入力します。デフォルト：5 秒。範囲：1 ～ 1000
Key	認証と暗号化のために Cisco IOS XE SD-WAN デバイス が TACACS+ サーバーに渡すキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、TACACS+ サーバーで使用する AES 暗号化キーと一致させる必要があります。

[Add] をクリックして、新しい TACACS サーバーを追加します。

別の TACACS サーバーを追加するには、[+ New TACACS Server] を再度クリックします。

サーバーを削除するには、ごみ箱アイコンをクリックします。

8021X の設定

802.1X の設定については、IEEE 802.1X 認証の設定 （127 ページ）を参照してください。

認証順序の設定

デバイスの認証順序と認証フォールバックを設定できます。認証順序では、システムがユーザーの認証を試みる順序を指定し、現在の認証方法が使用できない場合に認証を続行する方法を提供します。フォールバックでは、ユーザーを認証できない場合、またはRADUSやTACACS+サーバーに到達できない場合に、認証のメカニズムを提供します。

Cisco IOS XE SD-WAN デバイス で AAA 認証順序および認証フォールバックを設定するには、[Authentication] タブを選択し、次のパラメータを設定します。

表 34 :

パラメータ名	説明
サーバーグループの順序	AAA サーバーグループを使用するようにデバイスを設定すると、既存のサーバーホストをグループ化できます。既存のサーバーホストをグループ化すると、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます Cisco IOS XE SD-WAN デバイス へのユーザーアクセスを検証するときに、ソフトウェアが試行する認証方法のデフォルトの順序を変更するには、次の手順を実行します。 **1.** ServerGroups 優先順位フィールドをクリックして、サーバーグループのドロップダウンリストを表示します。リストには、ローカル、RADIUS、および TACACS 認証方式のグループが表示されます。 **2.** リストから、Cisco IOS XE SD-WAN デバイス へのアクセスを試みるユーザーをソフトウェアで検証する順序でグループを選択します。 リストから少なくとも 1 つのグループを選択する必要があります。

認可およびアカウンティングの設定

表 *35 :* 機能の履歴

機能名	リリース情報	説明
許可とアカウンティング	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能では、許可（コマンドが実行される前に、ユーザーがデバイスに入力するコマンドを許可する）とアカウンティング（ユーザーがデバイスで実行するコマンドのレコードを生成する）を設定します。

認可の設定

許可を設定できます。これにより、TACACS+サーバーは、コマンドを実行する前に、ユーザーがデバイスに入力するコマンドを許可します。許可は、TACACS+ サーバーで設定されたポリシーと、[Authorization] タブで設定したパラメータに基づいています。

前提条件

- [Authentication] タブで、TACACS+ サーバーとローカルサーバーを認証順序の最初に設定する必要があります。

許可を設定するには、[Authorization] タブを選択し、[+ New Authorization Rule] をクリックして、次のパラメータを設定します。

パラメータ名	説明
コンソール	コンソールアクセスコマンドの認証を実行するには、このオプションを有効にします。
コンフィギュレーション コマンド	コンフィギュレーション コマンドの認証を実行するには、このオプションを有効にします。
メソッド	[Command] を選択します。これにより、ユーザーが入力するコマンドが許可されます。
Privilege Level 1 or 15	許可するコマンドの権限レベル（1または15）を選択します。この権限レベルを持つユーザーが入力したコマンドが許可されます。
Groups	以前に設定した TACACS グループを選択します。この認証ルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

パラメータ名	説明
認証	このオプションを有効にすると、認証されたユーザーにのみ、この承認ルールが定義するパラメータが適用されます。このオプションを有効にしない場合、ルールはすべてのユーザーに適用されます。

[add] をクリックして、新しい認証ルールを追加します。

別の認証ルールを追加するには、[+ New Accounting Rule] を再度クリックします。

認証ルールを削除するには、行の右側にあるごみ箱アイコンをクリックします。

CLI の同等の設定：

```
system
   aaa
     aaa authorization console
     aaa authorization config-commands
     aaa authorization exec default list-name method
     aaa authorization commands level default list-name method
```

アカウンティングの設定

アカウンティングを設定できます。これにより、TACACS+ サーバーは、ユーザーがデバイスで実行するコマンドのレコードを生成します。

前提条件

- TACACS+ サーバーとローカルサーバーは、[Authentication] タブの認証順序で、それぞれ 1 番目と 2 番目に設定する必要があります。「認証順序の設定」を参照してください。

アカウンティングを設定するには、[Accounting] タブを選択し、[+ New Accounting Rule] をクリックして、次のパラメータを構成します。

表 *36 :*

パラメータ名	説明
[Method]	[Command] を選択すると、ユーザーが実行したコマンドがログに記録されます。
Privilege Level 1 or 15	特権レベル（1 または 15）を選択します。アカウンティングレコードは、この特権レベルのユーザーが入力したコマンドに対してのみ生成されます。
Enable Start-Stop	イベントの開始時に開始アカウンティング通知、イベントの終了時に停止レコード通知を送信する場合は、[On] をクリックします。
Groups	Choose a previously configured TACACS group. このアカウンティングルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

[Add] をクリックして新しいアカウンティングルールを追加します。

別のアカウンティングルールを追加するには、[+New Accounting Rule] を再度クリックします。

アカウンティングルールを削除するには、行の右側にあるごみ箱アイコンをクリックします。

CLI の同等の設定：

```
system
  aaa
    aaa accounting exec default start-stop group group-name
    aaa accounting commands level default start-stop group group-name
    aaa accounting network default start-stop group group-name
    aaa accounting system default start-stop group group-name
```

IEEE 802.1X 認証の設定

表 *37* : 機能の履歴

機能名	リリース情報	説明
SD-WAN の 802.1X サポート	Cisco IOS XE リリース 17.2.1r	この機能により、Cisco IOS XE SD-WAN デバイス で IEEE 802.1X 認証を有効にできます。Cisco vManage を使用してこの機能を設定できるようにするには、Cisco vManage で Cisco SD-WAN リリース 20.1.1 が実行されていることを確認してください。

Cisco IOS XE リリース 17.2.1r 以降、IEEE 802.1X は Identity-Based Networking Services（IBNS）1.0 IOS-XE CLI に基づいてサポートされます。この機能は、LAN インターフェイスと WAN インターフェイスの両方でサポートされています。

IEEE 802.1X オープン認証とホストモード

4 つのホストモード（単一ホストモード、複数ホストモード、複数ドメイン認証モード、および複数認証モード）のいずれかを設定して、認証前にデバイスがネットワークアクセスを取得できるようにすることができます。

オープン認証は、ホストモードの設定後に **authentication open** コマンドを入力することで有効になり、設定済みのホストモードの拡張として機能します。たとえば、シングルホストモードでオープン認証を有効にした場合、ポートでは 1 つの MAC アドレスだけが許可されます。認証前オープンアクセスが有効の場合、ポートの初期トラフィックは制限され、ポートに設定されている 802.1X とは無関係です。ポートに 802.1X 以外のアクセス制限が設定されていない場合、クライアントデバイスは設定されている VLAN 上でフルアクセスが可能です。オープン認証は、CLI テンプレートのみを使用して設定できます。Cisco vManage で dot1x 機能テンプレートを使用してオープン認証を設定することはできません。

前提条件

- IEEE 802.1x サービスを認証するように RADIUS 認証サーバーを有効にします。
- スイッチ ポート インターフェイスで IEEE 802.1X 構成を有効にします。
- 認証済みクライアントと非認証クライアントに対して、次の VLAN 設定を有効にします。
  - 制限 VLAN（または認証拒否 VLAN）
  - ゲスト VLAN
  - クリティカル VLAN（または認証失敗 VLAN）
  - クリティカル音声 VLAN
- 次のいずれかのホストモード認証を有効にします。
  - シングルホストモード
  - マルチホストモード
  - 複数認証モード
  - マルチドメインモード
- RADIUS アカウンティング属性の設定
- 必要に応じて、アドオンテンプレートで VLAN ID を使用した IEEE 802.1X 認証イベントを有効にする必要があります。

制約事項

- IEEE 802.1X 認証、許可、およびアカウンティング（AAA）は、複数のグループではサポートされていません。
- Cisco vManage によって認証順序 IEEE 802.1X MAB CLI を無効にすることはできません。この認証順序 CLI が存在すると、MAB クライアントがオンラインの場合、MAB 認証で 60 秒の遅延が発生します。
- 認証オープンは機能テンプレートではサポートされていませんが、CLI アドオンテンプレートで展開できます。

vManage を使用した IEEE 802.1X 認証の設定

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）プロトコルであり、有線ネットワークに接続するデバイスに認証を提供することにより、許可されていないネットワークデバイスが有線ネットワークにアクセスするのを防ぎます。

RADIUS 認証サーバーは、ネットワークが提供するサービスにクライアントがアクセスする前に、ポートに接続されている各クライアントを認証する必要があります。

インターフェイスで IEEE 802.1X 認証を設定するには、最初に [Cisco AAA] 機能テンプレートを作成します。

1. Cisco vManage で、**[Configuration]** > **[Templates]** を選択します
2. [Feature Templates] をクリックしてから、[Add Template] をクリックします。

（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。

3. 左側のパネルのリストからデバイスを選択します。
4. [Cisco AAA] テンプレートを選択します。
5. [Template Name] と [Description] に入力します。
6. [RADIUS] タブを選択し、[RADIUS SERVER] で [New RADIUS Server] をクリックします。
7. 次のパラメータを設定します。

パラメータ名	説明
[Mark as Optional Row]	設定をデバイス固有としてマークするには、[Mark as Optional Row] チェックボックスをオンにします。
アドレス	RADIUS サーバーの IP アドレスを入力します。
Authentication Port	[Authentication] をクリックし、[Add New Authentication Entry] をクリックして、IEEE 802.1X セッション中に RADIUS サーバーに送信する RADIUS 認証の属性と値（AV）のペアを構成します。 エントリを保存するには、[Add] をクリックします。
Accounting Port	[Accounting] をクリックし、[Add New Accounting Entry] をクリックして、IEEE 802.1X セッション中に RADIUS サーバーに送信する RADIUS アカウンティングの属性と値（AV）のペアを構成します。 エントリを保存するには、[Add] をクリックします。
タイムアウト	RADIUS サーバーからの応答を待機する時間を設定します
Retransmit Count	この RADIUS サーバーに接続する回数を設定します。
キー	RADIUS サーバーの共有キーを入力します。

8. [Add] をクリックします。
9. [RADIUS GROUP] を選択し、[New RADIUS Group] をクリックして、次のパラメータを設定します。

パラメータ名	説明
VPN-ID	RADIUS または他の認証サーバーに到達できる VPN を入力します。
Source Interface	RADIUS サーバーに到達するために使用されるインターフェイスを入力します。
RADIUS サーバ	RADIUS サーバーを設定します。

10. [Add] をクリックします。
11. [802.1X] タブを選択し、次のパラメータを入力します。

パラメータ名	説明
Authentication Param	認証パラメータを有効にするには、[On] をクリックします。
Accounting Param	アカウンティングパラメータを有効にするには、[On] をクリックします。

12. この機能テンプレートを保存するには、[Save] をクリックします。
13. デバイスでこの機能を有効にするには、これらの機能テンプレートをデバイステンプレートに追加してください。

（注） Cisco vManage リリース 20.5 より前に作成されたテンプレートはデバイスに接続すると失敗するため、AAA 機能テンプレートを再作成する必要があります。

次に、スイッチポートデバイスに使用できる [Switch Port] テンプレートを作成します。

1. [Switch Port] テンプレートを作成するには、上記の手順 1 ～ 3 を繰り返します。
2. [Switch Port] テンプレートを選択します。
3. [Template Name] と [Description] に入力します。
4. [Interface] タブを選択し、[New Interface] をクリックします。
5. 次のパラメータを設定します。

パラメータ名	説明
インターフェイス名	インターフェイス名を入力します。
速度	インターフェイス速度を入力します。
VLAN 名	VLAN 名を入力します。

パラメータ名	説明
VLAN ID	ブリッジングドメインに関連付けられた VLAN 識別子を入力します。
802.1X	このインターフェイスで IEEE 802.1X 認証を有効にします。[On] を選択します。 これにより、以下にリストされている追加のパラメータセットが提供されます。
Interface PAE Type	IEEE 802.1x インターフェイス PAE タイプを入力します。
Control Direction	単方向または双方向の認証モードを入力します。
Host Mode	IEEE 802.1X インターフェイスが単一のホスト（クライアント）または複数のホスト（クライアント）へのアクセスを許可するかどうかを選択します。 • [Multi Auth]：音声 VLAN 上の 1 つのホストとデータ VLAN 上の複数のホストへのアクセスを許可します。 • [Multi Host]：複数のホストへのアクセスを許可します • [Single Host]：最初に認証されたホストにのみアクセスを許可します。これがデフォルトです。 • [Multi-Domain]：ホストと音声デバイス（同じスイッチポート上の IP 電話など）の両方にアクセスを許可します。 （注） これらのオプションは、「Global」ホストモード設定でのみ使用できます。
定期再認証	IEEE 802.1X クライアントを再認証する頻度を入力します。デフォルトでは、最初の LAN アクセス要求の後、再認証は試行されません。 範囲：0 ～ 1440 分

6. [Advanced Options] をクリックし、次のように入力します。

パラメータ名	説明
Authentication Order	IEEE 802.1X インターフェイスに接続するデバイスを認証するときに使用する認証方法の順序を入力します。デフォルトの認証順序は RADIUS、次に MAC 認証バイパス（MAB）です。
MAC 認証バイパス	RADIUS サーバーで MAC 認証バイパス（MAB）を有効にし、RADIUS サーバーを使用して非 IEEE 802.1X 準拠のクライアントを認証する場合に選択します。

パラメータ名	説明
Port Control Mode	インターフェイスで IEEE 802.1X ポートベースの認証を有効にするには、ポート制御モードを入力します。 自動：IEEE 802.1X 認証を有効にし、ポートを未承認状態で起動するには、これを設定します。これにより、ポート経由で送受信できるのは EAPOL フレームのみです。
音声VLAN ID	音声 VLAN ID を設定します。
Critical VLAN	IEEE 802.1x 準拠クライアントのクリティカル VLAN（または認証失敗VLAN）を入力します。RADIUS認証またはRADIUSサーバーが失敗した場合のネットワークアクセスを構成します。
Critical Voice VLAN	クリティカル音声 VLAN を有効にします。
ゲスト VLAN	クライアントが MAB リストにない場合、ゲスト VLAN を設定して、IEEE 802.1X 対応でないクライアントをドロップします。
制限付き VLAN	IEEE 802.1x 準拠クライアントの制限付き VLAN（または認証失敗 VLAN）を入力します。RADIUS 認証に失敗した IEEE 802.1X 準拠クライアントへの限定サービスを設定します。

7. [Add] をクリックします。
8. この機能テンプレートを保存するには、[Save] をクリックします。
9. デバイスでこの機能を有効にするには、これらの機能テンプレートをデバイステンプレートに追加してください。

IEEE 802.1X オープン認証の設定

IEEE 802.1X オープン認証は、CLI アドオンテンプレートを使用して設定できます。

```
Device# config-transaction
Device(config)# interface GigabitEthernet2
Device(config-if)# authentication open
```

CLI を使用した IEEE 802.1X 認証の設定

設定

この機能には、次の 2 セットの設定が必要です。

1. **グローバル AAA コマンドを設定します。**
    1. IEEE 802.1X をグローバルに有効または無効にします

```
Device(config)# aaa authentication dot1x default group radius-0
Device(config)# aaa authorization network default group radius-0
Device(config)# dot1x system-auth-control
Device(config)# radius-server dead-criteria time 10 tries 3
Device(config)# radius-server deadtime 15
```

2. アカウンティングを有効にします

```
Device(config)# aaa accounting dot1x default start-stop group radius-0
```

2. インターフェイスレベルのコマンドを設定します。

1. ポート単位で IEEE 802.1X を有効または無効にします

```
Device(config-if)# dot1x pae authenticator
Device(config-if)# authentication port-control auto
```

2. ポート単位で MAB を有効または無効にします

```
Device(config-if)# mab
```

3. ホストモードを選択します

```
Device(config-if)# authentication host-mode  <multi-auth | multi-domain |
multi-host | single-host>
```

4. 音声 VLAN を設定します

```
Device(config-if)# switchport voice vlan <vlan-id>
```

5. IEEE 802.1X 制御方向を選択します

```
Device(config-if)# authentication control-direction <both | in>
```

6. 定期的な再認証と、対応する再認証間隔および非アクティブタイムアウト時間を有効にします

```
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate <internal-in-sec>
Device(config-if)# authentication timer inactivity <timeout-in-sec>
```

7. ポート単位で認証順序を設定します

```
Device(config-if)# authentication order dot1x mab
```

8. 制限 VLAN を指定します

```
Device(config-if)#  authentication event fail action authorize vlan <vlan-id>
```

9. ゲスト VLAN を指定します

```
Device(config-if)# authentication event no-response action authorize vlan
<vlan-id>
```

10. クリティカル VLAN を指定します

```
Device(config-if)# authentication event server dead action authorize vlan
<vlan-id>
```

11. クリティカル音声 VLAN 機能を有効にします

```
Device(config-if)# authentication event server dead action authorize voice
```

ポスチャアセスメントのサポート

表 *38* : 機能の履歴

機能名	リリース情報	説明
ポスチャアセスメントのサポート	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、ポスチャアセスメント機能を利用して、企業のセキュリティポリシーに従ってエンドポイントのコンプライアンスを検証できます。Identity Services Engine（ISE）のポスチャ機能は、Cisco 1100 サービス統合型ルータに統合されています。この機能は、Cisco vManage のアドオン機能テンプレートを使用してのみ設定できます。

ネットワークでは、企業のセキュリティポリシーへの準拠を保証するためにエンドポイントの検証が必要であり、ポスチャ評価によってこれを検証できます。ポスチャモジュールは、ネットワークに接続されているエンドポイントにセキュリティポリシーを適用します。Cisco 1100 サービス統合型ルータと ISE（アイデンティティ サービス エンジン）のエンドポイント間の接続では、それらの間の認証相互作用が必要です。IEEE 802.1X は、ポスチャアセスメントに推奨される標準認証プロセスです。MAC 認証バイパス（MAB）も使用できます。

これに使用されるポスチャ エージェント ソフトウェアは、Cisco AnyConnect ポスチャアセスメントです。Cisco AnyConnect ソフトウェアはエンドポイントにインストールされ、ポスチャと呼ばれるモジュールがあります。Cisco AnyConnect は、ISE サーバーからセキュリティポリシーをダウンロードし、エンドポイントの条件（マルウェア対策の条件、スパイウェア対策の条件、ウイルス対策の条件、アプリケーションの条件、USB の条件）をチェックします。すべての条件が満たされている場合、Cisco AnyConnect は ISE サーバーに「準拠」という結果を返します。そうでない場合、Cisco AnyConnect は「非準拠」という結果を返します。認証およびリダイレクト アクセス コントロール リスト（ACL）によるエンドポイントの認可と認証の後、クライアントエンドの Cisco AnyConnect ポスチャモジュールは、ポスチャポリシーサーバーでポスチャ評価を開始します。

ポスチャ評価が完了して認証されると、新しいポリシーを再認証または再許可するために、RADIUS サーバーから ISE で設定されたポリシーによって RADIUS CoA（許可変更）プロセスが開始されます。ポスチャ評価が成功すると、ネットワーク全体へのアクセスは、CoA 再認証コマンドによって Cisco ISR 1100 ルータおよびクライアントにプッシュされます。

ポスチャアセスメントの前提条件

- 基本的な IEEE 802.1x 認証プロセスが機能している必要があります。

- 認可変更（CoA）がサポートされている必要があります。
- リダイレクト ACL、ダウンロード可能な ACL（dACL）、およびクリティカル ACL が利用可能である必要があります。
- デバイス トラッキング ポリシー（アイデンティティ用）がサポートされている必要があります。
- URL リダイレクトがサポートされている必要があります。

ポスチャアセスメントの制約事項

- 8 ポートの Cisco 1100 サービス統合型ルータのみが、dACL やリダイレクト ACL などの ACL 機能をサポートします。
- ACL およびアクセス制御エントリ（ACE）ルールは、>、<、>=、<= などの比較操作をサポートしていません。
- 最大 120 の dACL ACE がサポートされ、64 のリダイレクト ACL ACE がサポートされます。
- ポート ACL および IPv6 ACL はサポートされていません。
- IP オプションと IP フラグメント ACL はサポートされていません。
- VLAN 単位のデバイストラッキングはサポートされていません。
- 収集やアドレストラッキングなど、制限されたポート単位のデバイストラッキング ポリシー オプションのみが許可されます。

Cisco SD-WAN でのポスチャ評価の設定

1. Cisco vManage の CLI アドオンテンプレートを使用して、AAA、IEEE 802.1x、ポスチャ評価を設定し、ACL とデバイストラッキングをリダイレクトします。

   設定例を以下に示します。

（注） `aaa new-model` はデフォルトで Cisco SD-WAN で有効になっており、ユーザーが設定することはできません。ただし、非 SD-WAN イメージ上に設定される必要があります。

1. AAA の設定

```
aaa new-model
radius server ISE1

address ipv4 198.51.100.255 auth-port 1812 acct-port 1813
key cisco

aaa group server radius ISE
 server name ISE1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

interface vlan 15
 ip address 198.51.100.1 198.51.100.254
```

```
interface GigabitEthernet0/1/0
 switchport mode access
 switchport access vlan 15

ip radius source-interface vlan 15
```

2. IEEE 802.1x 認証および許可の設定

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

（注） IEEE 802.1x エンドポイントは GigabitEthernet0/1/7 に接続されています。

3. ポスチャ評価の設定および ACL のリダイレクト

```
ip http server
ip http secure-server

ip access-list extended ACL-POSTAUTH-REDIRECT
10 deny tcp any host 192.0.2.255
20 deny tcp any any eq domain
30 deny udp any any eq domain
40 deny udp any any eq bootpc
50 deny udp any any eq bootps
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

4. デバイストラッキングの設定

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

（注） 上記の IP アドレスは ISE に属しています。

この設定を Cisco vManage の CLI アドオンテンプレートに追加するために実行する必要がある手順は、ここに記載されています。

2. ISE で CoA 再認証と dACL を設定するには、次の手順を実行します。
   1. ダウンロード可能な ACL を作成し、その中に ACE を定義します。

      ACL 名：TEST_IP_PERMIT_ALL

      ACE：permit ip any any
   2. 認証結果を作成し、ダウンロード可能な ACL を dACL として選択します。
   3. **[Administration]** > **[System]** > **[Settings]** > **[Policy Settings]** に移動し、[Policy Sets] 設定で、認証結果を認証ポリシーとして選択します。
3. CLI アドオンテンプレートを作成したら、それをデバイステンプレートにアタッチしてから、Cisco vManage はデバイステンプレートのすべての設定をデバイスにプッシュします。

Cisco IOS XE SD-WAN ルータのタイプ 6 パスワード

表 *39* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN ルータのタイプ 6 パスワード	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能により、安全な可逆暗号化を使用するタイプ 6 パスワードを使用できます。この暗号化は、より安全なアルゴリズムを使用してパスワードを暗号化することにより、セキュリティを強化します。これらのパスワードは、サポートされるテンプレート（138ページ）で詳しく説明されているテンプレートでサポートされています。

タイプ 6 パスワードの概要

タイプ 6 パスワード機能により、Advanced Encryption Scheme（AES）アルゴリズムに基づく認証、許可、およびアカウンティング（AAA）および Simple Network Management Protocol（SNMP）設定の安全な可逆暗号化が可能になります。

可逆暗号化は、可逆的な対称暗号化アルゴリズムを使用してパスワードを暗号化するプロセスです。ユーザーが入力したパスワードが有効かどうかを確認するために、パスワードが復号され、ユーザーが入力したパスワードと比較されます。この暗号化を実行するには、対称暗号化アルゴリズムにキーを指定する必要があります。使用する暗号化アルゴリズムは、PKCS#5 パ

ディングを使用した暗号ブロック連鎖（CBC）モードの Advanced Encryption Scheme（AES）アルゴリズムです。このアルゴリズムは、RADIUS、TACACS+、SNMP、TrustSec などの AAA 機能に使用されます。

Cisco vManage リリース 20.4.1 およびそれ以降のリリースでサポートされているテンプレートを作成すると、デフォルトでタイプ 6 パスワードが使用されます。Cisco vManage ではパスワードを暗号化し、そのパスワードを安全なトンネル経由でルータに送信します。次に、ルータはパスワードをタイプ 6 形式に暗号化し、それをデバイスに保存します。

（注） Cisco IOS XE SD-WAN デバイスでは、デバイスの 0 日目の起動時に、特権レベル 15 を持つ管理者ユーザーがデフォルトで作成されます。ユーザーがこの管理者ユーザーを削除しないことをお勧めします。

（注） パスワードの完全性に対する悪意のある攻撃の脆弱性を減らすために、タイプ 6 パスワードを使用することをお勧めします。デバイスを Cisco IOS XE リリース 17.4.1a にアップグレードすると、すべての AAA、RADIUS キー、および TACACS+ キーがタイプ 6 に暗号化されます。

サポートされるプラットフォーム

Cisco IOS XE SD-WAN デバイス。

サポートされるテンプレート

次のテンプレートは、タイプ 6 パスワードをサポートしています。

- Cisco AAA テンプレートを使用した RADIUS および TACACS 認証。
- SNMP テンプレート。
- CLI アドオンテンプレート。

機能制限

- SNMP テンプレートの場合、コミュニティ名はデフォルトで暗号化されます。したがって、既存の SNMP テンプレートをタイプ 6 のパスワードにアップグレードするには、コミュニティとトラップターゲットを削除して再作成します。
- **keychain key-string** コマンドでタイプ 6 パスワードを使用する場合、クリアテキストのパスワードの最大長は 38 文字です。

Cisco vManage を使用したタイプ 6 パスワードの設定

タイプ 6 パスワードへの既存のテンプレートのアップグレード

Cisco vManage で既存のテンプレートのパスワードをタイプ 6 のパスワードにアップグレードするには、次の手順を実行します。

（注） ルータを Cisco IOS XE リリース 17.4.1a にアップグレードすると、サポートされているすべてのパスワードがタイプ 6 のパスワードに自動的にアップグレードされます。

1. **[Configuration]** > **[Templates]** に移動します
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. タイプ 6 のパスワードにアップグレードするテンプレートに対し、[…] ボタンをクリックします。
4. [Edit] をクリックします。
5. **[Save]** をクリックします。

（注） パスワードを更新するために、テンプレートに他の変更を加える必要はありません。[Save] をクリックすると、Cisco vManage ではパスワードがタイプ 6 のパスワードに自動的にアップグレードされます。

CLI アドオンテンプレートを使用したタイプ 6 パスワードの設定

次の手順を実行して、CLI アドオン機能テンプレートを使用するときにタイプ 6 のパスワードを設定できます。

1. **[Configuration]** > **[Templates]** に移動します。
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. [Select Devices] ペインで、テンプレートを作成するデバイスを選択します。
5. [Select Template] ペインで、[Other Templates] セクションまで下にスクロールします。
6. [CLI Add-On Template] をクリックします。CLI アドオン機能テンプレートの詳細については、「CLI Add-on Feature Templates」を参照してください。
7. テンプレート名と説明を入力します。
8. デバイスで実行する CLI を入力するか貼り付けます。
9. CLI で平文パスワードを選択し、[Encrypt Type 6] ボタンをクリックします。
10. [Save] をクリックします。

タイプ6パスワードの確認

パスワードがタイプ6のパスワードにアップグレードされたことを確認するには、次のいずれかを実行します。

- Cisco vManage では、タイプ 6 パスワードをサポートする構成をデバイスにアタッチすると、構成プレビューに暗号化されたパスワードが表示されます。次に例を示します。

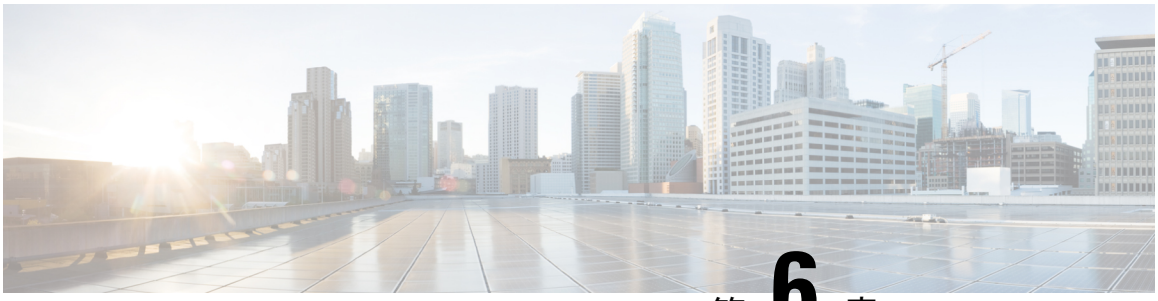
```
snmp-server community 0
$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ== ro
```

  コマンドでタイプが `0` と表示されているにもかかわらず、文字列 `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` は暗号化されたパスワードを表しています。パスワードが暗号化されている場合は、`$CRYPT_CLUSTER$` で始まります。

- デバイスで次のコマンドを実行して、暗号化されたパスワードを表示できます。

```
デバイス#show run | sec aaa
aaa new-model
aaa group server tacacs+ tacacs-0
server-private 10.0.0.1 key 6 BibgKcVeWF]^aK[XfEIICXMCbdScBYAAB
aaa group server radius radius-0
server-private 10.0.0.2 timeout 5 retransmit 3 key 6 CHd_VK[]NHEdcVCWGCaENGINQHLBEhDBe
```

  出力には、パスワードがタイプ6であることが表示され、暗号化されたパスワードも表示されます。



第 6 章

ロールベース アクセス コントロール

表 *40* : 機能の履歴

機能名	リリース情報	説明
リソースグループによるロールベースアクセス コントロール	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、サイトまたはリソースグループに基づいたロールベース アクセス コントロール（RBAC）が導入されます。これは、ユーザーグループとリソースグループの組み合わせに基づいて、ユーザーのシステムアクセスを承認する方法です。 複数の地理的な場所にまたがる大規模なCisco SD-WAN展開の場合、この機能は、ネットワーク管理を異なる地域管理者間で分割するのに役立ちます。
ポリシーに対する RBAC	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco vManage ポリシーに必要な読み取りおよび書き込み権限を持つユーザーおよびユーザーグループを作成できます。ポリシーに対する RBAC は、運用効率を最大化するのに役立つポリシーのすべての詳細へのアクセスをユーザーに提供します。これにより、構成要件を満たすことが容易になり、システム上の許可されたユーザーに必要なものへのアクセスのみが許可されることが保証されます。

機能名	リリース情報	説明
共同管理：機能テンプレートのきめ細かいロールベースアクセスコントロール	Cisco vManage リリース 20.7.1	この機能により、テンプレートの使用にあたって RBAC によるアクセス許可をより細分化して割り当てられるようになり、テナントに自己管理によるネットワーク構成タスクを与えることができます。ネットワーク管理者やマネージドサービスプロバイダーはこの機能を使ってエンドカスタマーにアクセス許可を割り当てることができます。
共同管理：きめ細かい構成タスクのアクセス許可の改善	Cisco vManage リリース 20.9.1	ユーザーが特定の構成タスクを自己管理できるようにするために、他のタスクを除外しながら、特定の構成タスクを実行する権限をユーザーに割り当てることができます。 この機能により、多数の新しいアクセス許可オプションが導入され、ユーザーに提供する構成タスクのアクセス許可をきめ細かく決定できます。
セキュリティ操作およびネットワーク操作のデフォルトのユーザーグループに対する RBAC	Cisco vManage リリース 20.9.1	この機能は、次のデフォルトのユーザーグループを提供します。 • 非セキュリティポリシー用の network_operations ユーザーグループ • セキュリティポリシー用の security_operations ユーザーグループ ポリシーに対する RBAC を使用すると、セキュリティポリシーと非セキュリティポリシーに必要な読み取りおよび書き込みアクセス許可を持つユーザーとユーザーグループを作成できます。ユーザーは、承認されたポリシータイプに対してのみ構成およびモニタリングアクションを実行できます。

- RBAC に関する情報 （143 ページ）
- RBAC の制約事項 （157 ページ）
- RBAC の設定 （158 ページ）
- CLI を使用した RBAC の設定 （187 ページ）
- RBAC の確認 （189 ページ）
- RBAC のモニタリング （189 ページ）

RBAC に関する情報

VPN によるロールベース アクセス コントロール

ロールベースアクセスコントロール（RBAC）は、ネットワーク設定およびリソースへのユーザーアクセスを制限するプロセスです。RBACでは、アクセスが必要なリソースに応じてユーザーにロールを割り当てます。VPN による RBAC 機能は、VPN に基づいてネットワークへのアクセスを管理および制御するのに役立ちます。これには、権限を持つユーザーがアクセスできるようにするアクセス許可と権限の設定が含まれます。

VPN による RBAC

VPNによるロールベースアクセスにより、ネットワーク管理者は1つ以上のネットワークセグメントを持つ VPN グループを定義できます。ネットワーク管理者は、ネットワーク内のデバイスおよびCisco vManageの機能へのユーザーアクセスを制限するVPNグループにユーザーを関連付けることができます。

VPN による RBAC は、VPN グループが設定されたユーザーに次の制限付きアクセスを提供します。

- VPN ダッシュボードへのアクセス
- VPNダッシュボードを介したデバイス、ネットワーク、およびアプリケーションのステータスのモニタリング
- VPN グループ内のセグメントを持つデバイスに制限された VPN ダッシュボード情報
- VPN グループ内のセグメントを持つデバイスに制限されたモニタリングオプション
- VPNグループ内のセグメントのインターフェイスに制限された各デバイスのインターフェイス モニタリング

VPN ダッシュボードの概要

VPN グループで設定されたユーザーは、VPN ダッシュボードにのみアクセスでき、読み取り専用アクセスになります。管理者アクセスのあるユーザーは、VPNグループを作成でき、管理ダッシュボードと VPN ダッシュボードの両方にアクセスできます。管理ユーザーは、Cisco vManage のメニューから [Dashboard] を選択して、これらのダッシュボードにアクセスできます。

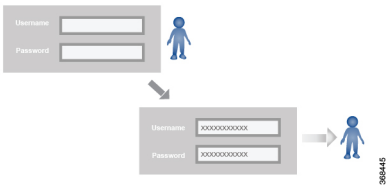
AAA を使用したロールベースアクセス

Cisco SD-WAN AAA ソフトウェアは、ロールベースのアクセスを実装して、Cisco IOS XE SD-WAN デバイス のユーザーの認可権限を制御します。ロールベースのアクセスは、次の 3 つのコンポーネントで構成されます。

- ユーザーは、Cisco IOS XE SD-WAN デバイス へのログインが許可されているユーザーです。
- ユーザーグループは、ユーザーのコレクションです。
- 権限は各グループに関連付けられています。これらは、グループのユーザーが発行を許可されているコマンドを定義します。

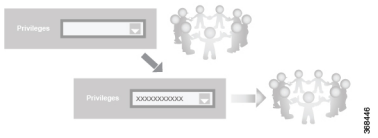
ユーザーとユーザーグループ

Cisco IOS XE SD-WAN デバイス での操作の実行が許可されているすべてのユーザーは、ログインアカウントを持っている必要があります。ログインアカウントについては、デバイス自体でユーザー名とパスワードを設定します。これらにより、ユーザーはそのデバイスにログインできます。ユーザーがアクセスを許可されている各デバイスで、ユーザー名とパスワードを設定する必要があります。



Cisco SD-WAN ソフトウェアは、UNIX スーパーユーザーと同様な、完全な管理者権限を持つユーザーである **admin** という 1 つの標準ユーザー名を提供します。デフォルトでは、**admin** ユーザー名のパスワードは**admin** です。このユーザー名を削除または変更することはできませんが、デフォルトのパスワードは変更できますし、変更する必要があります。

ユーザーグループは、Cisco IOS XE SD-WAN デバイス で共通のロールまたは権限を持つユーザーをプールします。ログインアカウント情報の構成の一環として、ユーザーがメンバーであるユーザーグループを指定します。**admin**ユーザーのグループを指定する必要はありません。このユーザーは自動的にユーザーグループ **netadmin** に属し、Cisco IOS XE SD-WAN デバイスでのすべての操作の実行が許可されるためです。



ユーザーグループ自体は、そのグループに関連付けられた権限を設定する場所です。これらの権限は、ユーザーが実行を許可されている特定のコマンドに対応し、Cisco SD-WAN ソフトウェア要素への役割ベースのアクセスを効果的に定義します。

Cisco SD-WAN ソフトウェアは、次の標準ユーザーグループを提供します。

- [basic]：[basic] グループは設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、デバイス上の情報を表示および変更する権限を持つユーザーを含むように設計されています。
- [operator]：[operator] グループも設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、情報を表示する権限のみを持つユーザーを含むように設計されています。
- [netadmin]：[netadmin] グループは設定不可能なグループです。デフォルトでは、このグループには**admin**ユーザーが含まれます。このグループに他のユーザーを追加できます。このグループのユーザーは、デバイスですべての操作を実行できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：[network_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上でセキュリティポリシー以外のすべての操作を実行でき、セキュリティポリシー情報は表示のみが可能です。たとえば、ユーザーはテンプレート設定を作成または変更し、災害復旧を管理し、アプリケーション対応ルーティングポリシーや CFlowD ポリシーなどの非セキュリティポリシーを作成できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：[security_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上ですべてのセキュリティ操作を実行でき、セキュリティポリシー以外の情報は表示のみが可能です。たとえば、ユーザーはUmbrellaキー、ライセンス、IPS 署名の自動更新、TLS/SSL プロキシ設定などを管理できます。

[network_operations] グループのユーザーは、デバイスへのポリシーの適用、適用されたポリシーの取り消し、およびデバイステンプレートの編集を許可されています。[security_operations] グループのユーザーは、デバイスにセキュリティポリシーを展開するために、[network_operations] ユーザーによる 0 日目の介入と、展開されたセキュリティポリシーを削除するために、N 日目の介入が必要です。ただし、セキュリティポリシーがデバイスに展開された後は、[security_operations] ユーザーは、[network_operations] ユーザーの介入を必要とせずにセキュリティポリシーを変更できます。

（注） 実行中の設定およびローカル設定を表示できるのは管理ユーザーのみです。事前定義された [operator] ユーザーグループに関連付けられたユーザーは、実行中の設定およびローカル設定にアクセスできません。事前定義されたユーザーグループ [operator] には、テンプレート設定の読み取りアクセスのみがあります。管理者ユーザー権限のサブセットのみが必要な場合は、機能リストから選択した機能を使用して、読み取りと書き込みの両方のアクセス権を持つ新しいユーザーグループを作成し、そのグループをカスタムユーザーに関連付ける必要があります。

ロールベースのアクセス権限

ロールベースのアクセス権限は、タスクと呼ばれる 5 つのカテゴリに分類されます。

- インターフェイス：Cisco IOS XE SD-WAN デバイス 上のインターフェイスを制御するための権限。
- ポリシー：コントロール プレーン ポリシー、OMP、およびデータプレーンポリシーを制御するための権限。
- ルーティング：BFD、BGP、OMP、OSPF などのルーティングプロトコルを制御するための権限。
- セキュリティ：ソフトウェアや証明書のインストールなど、デバイスのセキュリティを制御するための権限。[netadmin] グループに属するユーザーのみがシステムにソフトウェアをインストールできます。
- システム：一般的なシステム全体の権限。

次のセクションの表は、ユーザーおよびユーザーグループの AAA 認証ルールの詳細を示しています。これらの認証ルールは、CLI から発行されたコマンドと Netconf から発行されたコマンドに適用されます。

操作コマンドのユーザー認証ルール

操作コマンドのユーザー認証ルールは、ユーザー名のみに基づいています。Cisco IOS XE SD-WAN デバイス にログインできるユーザーは、ほとんどの操作コマンドを実行できます。ただし、ソフトウェアのインストールとアップグレード、デバイスのシャットダウンなど、デバイスの基本的な操作に影響を与えるコマンドを発行できるのは **admin** ユーザーだけです。

どのユーザーも **config** コマンドを発行して設定モードに入ることができ、設定モードに入ると、一般的な設定コマンドを発行できることに注意してください。また、すべてのユーザーは、**system aaa user** *self* **password** *password* コマンドを発行して、その設定変更をコミットすることにより、自分のパスワードを設定することができます。デバイスの動作を設定する実際のコマンドでは、ユーザーグループのメンバーシップに従って承認が定義されます。「設定コマンドのユーザーグループの認証ルール」を参照してください。

次の表に、一般的な CLI コマンドの AAA 認証ルールを示します。注記があるものを除き、すべてのコマンドは操作コマンドです。また、「admin」ユーザーが使用できる一部のコマンドは、そのユーザーが「netadmin」ユーザーグループに属している場合にのみ使用できます。

CLI コマンド	すべてのユーザー	管理者ユーザ
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X

CLI コマンド	すべてのユーザー	管理者ユーザ
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X（netadmin グループのユーザーのみ）
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X
poweroff	—	X（netadmin グループのユーザーのみ）
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X（netadmin グループのユーザーのみ）
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X（netadmin グループのユーザーのみ）
request execute request download request upload	X	X
request（その他すべて）	—	×
rollback（設定モードコマンド）	—	X（netadmin グループのユーザーのみ）
screen-length	X	X
screen-width	X	X
show cli	X	X

CLI コマンド	すべてのユーザー	管理者ユーザ
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user self password password（設定モードコマンド）（注：ユーザーは自分自身を削除できません）		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X	X（netadmin グループのユーザーのみ）

操作コマンドのユーザーグループの認証ルール

操作コマンドのユーザーグループの認証ロールを次の表に示します。

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs：debug コマンドと同じ					
show dhcp					X
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

設定コマンドのユーザーグループの認証ルール

次の表に、設定コマンドのユーザーグループの認証ルールを示します。

コンフィギュレーション コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
[omp]		X	X		X
ポリシー		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn（作成、削除、命名を含むその他すべて）					X
wlan	X				

リソースグループによる RBAC の概要

サポートされている最小リリース：Cisco IOS XE リリース 17.5.1a、Cisco vManage リリース 20.5.1

リソースグループによるRBACは、ユーザーグループとリソースグループに基づいてユーザーのシステムアクセスを制限または承認する方法です。ユーザーグループはシステム内のユーザーの権限を定義し、リソースグループはユーザーがアクセスできる組織（ドメイン）を定義します。権限がユーザーに直接割り当てられることはないため、個々のユーザー権限の管理では、適切なユーザーとリソースグループを割り当てることが主な作業になります。

複数の地理的な場所にまたがる大規模な Cisco SD-WAN 展開では、ネットワーク管理を異なる地域管理者間で分割できます。

ネットワーク管理者が割り当てられているユーザーグループとリソースグループに基づいて、それらをグローバル管理者と地域管理者として大まかに分類できます。グローバル管理者は、すべてのリソースグループのリソースにアクセスでき、すべての機能に対する完全な読み取り/書き込み特権を持っています。地域管理者グループには、すべての機能に対する完全な読み取り/書き込み権限がありますが、アクセスできるリソースは、割り当てられているリソースグループによって制御されます。

Global Admin

グローバルリソースグループのユーザーアカウントは、すべてのリソースにアクセスできます。グローバル管理者は、ネットワーク全体を監視する責任がありますが、毎日の個々のデバイスの操作には関与しません。グローバル管理者は、デバイスを対応する地域に割り当て、地域管理者アカウントを割り当て、コントローラを管理し、共有可能で一元化された構成を維持し、必要に応じて個々のデバイスを操作できます。

netadmin 権限を持ち、グローバルリソースグループの一部でもあるシングル テナント セットアップのユーザーは、グローバル管理者と見なされます。Cisco vManage のデフォルトの管理者ユーザーもグローバル管理者であり、そのユーザーはさらにグローバル管理者を割り当てることができます。グローバルリソースグループには、すべての WAN エッジ、単一ビューのコントローラが含まれます。

グローバル管理者は、特定のリソースグループのみを表示するように切り替え、テンプレートを作成できます。地域管理者とも呼ばれるローカルリソースグループ管理者は、グローバルテンプレートを複製して、リソースグループ内で再利用できます。

地域管理者

地域管理者は、対応する地域のデバイスの日常的な操作（構成、監視、オンボーディング、など）を担当します。地域外のデバイスにアクセスしたり、表示したりしてはなりません。次のユーザーグループを作成できます。

- リソースグループ管理者：対応するリソースグループ内のデバイスへの完全な読み取り/書き込みアクセス権。グループ内の WAN エッジのテンプレートのトラブルシューティング、監視、アタッチ、またはデタッチを行うことができます
- リソースグループオペレータ：リソースグループ内の WAN エッジへの読み取り専用アクセス
- リソースグループ基本：基本アクセス

リソースグループの管理者は、新しいテンプレートを作成し、グループ内の WAN エッジにアタッチまたはデタッチできます。また、グローバルテンプレートをコピーして再利用することもできます。

リソースグループは、ユーザーがアクセスできるリソースを決定します。ただし、アクセスレベルは既存のユーザーグループによって制御されます。

- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_admin** に属している場合、resource_group_a のすべてのリソースへの完全な読み取り/書き込みアクセス権があります。

- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_operator** に属している場合、**resource_group_a** のすべてのリソースへの読み取り専用アクセス権があります。
- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_basic** に属している場合、**resource_group_a** のインターフェイスおよびシステムリソースへの読み取り専用アクセス権があります。

グローバルリソースグループ

グローバルグループは、異なるアクセス制御ルールを持つ特別なシステム定義済みリソースグループです。

- このグループ内のユーザーはグローバル管理者と見なされ、システム内のすべてのリソース（デバイス、テンプレート、ポリシー）に完全にアクセスでき、リソースグループを管理し、リソースとユーザーをグループに割り当てることができます。
- 他のすべてのユーザーは、このグループ内のリソースへの読み取り専用アクセス権を持っています。
- システムのデフォルトの管理者アカウント（またはマルチテナント設定の tenantadmin アカウント）は、常にこのグループに属します。この権限は変更できません。ただし、管理者アカウントは、他のユーザーアカウントをこのグループに追加したり、このグループから削除したりできます。

IdP（SSO）管理グループ

ID プロバイダー（IdP）は、ユーザー ID を保存して検証するサービスです。IdP は通常、シングルサインオン（SSO）プロバイダーと連携してユーザーを認証します。ユーザーが IdP の SSO サービスで認証されている場合、グループ情報も IDP によって提供および管理されます。IdP は、ユーザー名やユーザーが属するすべてのグループ名など、ユーザーに関する情報を渡します。Cisco vManage は、グループ名をデータベースに保存されているグループ名と照合して、IdP から渡された特定のグループ名がユーザーグループ、リソースグループ、または VPN グループのものであるかどうかをさらに区別します。

マルチテナントサポート

Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。テナントは、Cisco vManage インスタンス、Cisco vBond Orchestrator、および Cisco vSmart Controller を共有します。サービスプロバイダーのドメイン名には、テナントごとにサブドメインがあります。Cisco vManage は、サービスプロバイダーによって展開および設定されます。プロバイダーは、マルチテナント機能を有効にし、テナントにサービスを提供する Cisco vManage クラスタを作成します。SSH 端末を介して Cisco vManage インスタンスにアクセスできるのはプロバイダーのみです。

プロバイダーには次の機能があります。

- プロバイダーはコントローラのみを管理するため、リソースグループは適用されません。

- プロバイダーが新しいテナントをプロビジョニングする場合、テナントのデフォルトのユーザーアカウントは tenantadmin です。
- プロバイダーによって作成された他のユーザーアカウントは、既定のグローバルリソースグループに含まれます。
- プロバイダーがテナント用のテンプレートを作成すると、そのテンプレートはグローバルリソースグループに含まれます。

ポリシーの RBAC の概要

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

ポリシーに対する RBAC により、ユーザーまたはユーザーグループは、Cisco vManage ポリシーへの選択的な読み取りおよび書き込み（RW）アクセスを行うことができます。次に例を示します。

- Cflowd ポリシーの RW アクセスを持つユーザーは、Cflowd ポリシーのみを構成でき、アプリケーション対応ルーティングポリシーを構成することはできません。
- アプリケーション対応ルーティングポリシーの RW アクセスを持つユーザーは、アプリケーション対応ルーティングポリシーのみを構成でき、他のポリシーを構成することはできません。

この機能は、集中化およびローカライズされたポリシーでのみサポートされており、セキュリティポリシーではサポートされていません。

機能テンプレートの詳細な RBAC に関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

ユーザーグループのアクセス権を設定する場合、次のテンプレート権限を使用して、さまざまなタイプのテンプレートへの特定のレベルのアクセス権を RBAC ユーザーに付与できます。これにより、RBAC ユーザーが適用できるデバイス設定のタイプを管理できます。

権限	説明
CLI アドオンテンプレート	CLI アドオン機能テンプレートへのアクセス権を付与します。
デバイス CLI テンプレート	デバイス CLI テンプレートへのアクセス権を付与します。
SIG テンプレート	SIG 機能テンプレートおよび SIG ログイン情報テンプレートへのアクセス権を付与します。
その他の機能テンプレート	SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートへのアクセス権を付与します。

シングルテナントとマルチテナントのシナリオ

シングルテナントおよびマルチテナント Cisco vManage のシナリオでは、機能テンプレートに詳細な RBAC を使用できます。

ユーザーグループを作成して、テナントのさまざまなチームに特定の権限を割り当てることができます。これにより、チームは、デバイス CLI テンプレートを使用する権限がなくても、特定のネットワークサービスのみを管理できます。デバイス CLI テンプレートは他のテンプレートやデバイス設定を上書きする可能性があるため、テナントにデバイス CLI テンプレートを適用する権限を与えることは望ましくない場合があります。

たとえば、テナントのセキュリティ運用グループ用のユーザーグループを作成して、SIG テンプレートオプションへの読み取り/書き込みアクセスのみを許可することができます。これにより、セキュリティ運用グループはセキュリティ設定を使用できるようになります。

きめ細かい設定タスク権限に関する情報

Cisco vManage リリース 20.9.1 からは多数のユーザー権限オプションが利用可能であり、設定グループと機能プロファイルに関連する特定の設定タスクの管理権限をユーザーに割り当てる際にきめ細かい対応が可能です。

RBAC の利点

機能テンプレートのきめ細かい RBAC の利点

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

共同管理のために追加する権限は、ネットワーク設定へのアクセスを詳細に制御するのに役立ちます。これらは、テナントで Cisco SD-WAN を使用する場合に便利で、特定のタイプのテンプレートへのテナントアクセスを提供できます。テナントの VPN 内でテナントに自己管理によるネットワーク構成タスクを与えることができます。

共同管理用に追加された権限については、機能テンプレートの詳細な RBAC に関する情報（156 ページ）を参照してください。

RBAC の制約事項

機能テンプレートの詳細な RBAC の制限

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

- 共同管理用の RBAC に提供されているテンプレート制限オプションのいずれかを使用するには、[Template Configuration] オプションの権限を指定します。特定のユーザーロールに [Template Configuration] オプションで権限が割り当てられていない場合、そのユーザーに

対して [Templates] メニューは Cisco vManage に表示されません。「Manage Users」を参照してください。

- RBACユーザーがテンプレートをデバイスに適用できるようにするには、[Template Deploy] オプションに [Write] 権限を提供します。

RBAC の設定

ユーザの管理

Cisco vManage のメニューで、**[Administration]** > **[Manage Users]** を選択し、ユーザーおよびユーザーグループを追加、編集、表示、または削除します。

次の点に注意してください。

- **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。
- 各ユーザーグループには、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。
- 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 *41* : ユーザーグループ権限：*Cisco IOS XE SD-WAN* デバイス

機能	読み取り権限	書き込み権限
アラーム	**[Monitor]** > **[Logs]** > **[Alarms]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページで、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。

機能	読み取り権限	書き込み権限
監査ログ	**[Monitor]** > **[Logs]** > **[Alarms]** ページと **[Monitor]** > **[Logs]** > **[Audit Log]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページと **[Monitor]** > **[Audit Log]** ページで、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]** ウィンドウで、証明書署名要求（CSR）と証明書を表示します。	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** ウィンドウで、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]** ウィンドウで、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、コントローラデバイスを無効化します。

機能	読み取り権限	書き込み権限
CLI アドオンテンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで CLI アドオン機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、CLI アドオン機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。
Cloud OnRamp	**[Configuration]** > **[Cloud OnRamp for SaaS]** および **[Configuration]** > **[Cloud OnRamp for IaaS]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。
[Cluster]	**[Administration]** > **[Cluster Management]** ウィンドウで、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]** ウィンドウで、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。
コロケーション	**[Configuration]** > **[Cloud OnRamp for Colocation]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
[Config Group] > **[Device]** > **[Deploy]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	この権限では、機能は提供されません。	設定を Cisco IOS XE SD-WAN デバイス に展開します。 （注） 既存の機能設定を編集するには、[Template Configuration] の書き込み権限が必要です。
デバイス CLI テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウでデバイス CLI テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、デバイス CLI テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。

機能	読み取り権限	書き込み権限
デバイス インベントリ	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、オーバーレイネットワークの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]** ウィンドウで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 **[Monitor]** > **[Devices]** ページで（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、SD-WAN Application Intelligence Engine（SAIE）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。 （注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープパケットインスペクション（DPI）フローと呼ばれていました。 Cisco vManage リリース 20.6.x 以前のリリース：デバイス情報は **[Monitor]** > **[Network]** ページに表示されます。	**[Monitor]** > **[Devices]** ページで（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。

機能	読み取り権限	書き込み権限
デバイス リブート	**[Maintenance]** > **[Device Reboot]** ウィンドウで、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]** ウィンドウで、1 つまたは複数のデバイスを再起動します。
ディザスタ リカバリ	**[Administration]** > **[Disaster Recovery]** ウィンドウで、Cisco vManage 上で実行されているアクティブクラスタとスタンバイクラスタに関する情報を表示します。	追加の権限はありません。
[Event]	**[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Events]** ページで、デバイスの地理的な位置を表示します。	**[Monitor]** > **[Logs]** > **[Events]** ページで（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。
[Feature Profile] > **[Other]** > **[Thousandeyes]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Dhcp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [DHCP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [DHCP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Lan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Svi]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [SVI Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [SVI Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Routing/Ospf]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Switchport]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Switchport] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Switchport] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Wirelesslan]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Aaa]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [AAA] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [AAA] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Banner]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Banner] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Banner] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Basic]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [System Profile] セクションで [Basic] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [System Profile] セクションで [Basic] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Bfd]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [System Profile] セクションで [BFD] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [System Profile] セクションで [BFD] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Global]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [System Profile] セクションで [Global] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [System Profile] セクションで [Global] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Logging]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Logging] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Logging] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Ntp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [NTP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [NTP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Omp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [OMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [OMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Snmp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [SNMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [SNMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Controller]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Profile]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Management/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Management VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Management VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Management/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Management Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Management VPN and Management Internet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Tracker]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Tracker] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Tracker] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Cellular]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** >（設定グループを表示する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** >（設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
統合管理	**[Administration]** > **[Integration Management]** ウィンドウで、Cisco vManage で実行中のコントローラに関する情報を表示します。	追加の権限はありません。
ライセンス管理	**[Administration]** > **[License Management]** ウィンドウで、Cisco vManage で実行中のデバイスのライセンス情報を表示します。	**[Administration]** > **[License Management]** ページで、Cisco スマートアカウントの使用を設定し、管理するライセンスを選択して、Cisco vManage とライセンスサーバー間でライセンス情報を同期します。
インターフェイス（Interface）	**[Monitor]** > **[Network]** > **[Interface]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのインターフェイスに関する情報は **[Monitor]** > **[Network]** > **[Interface]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Interface]** ページで、[Chart Options] を編集して、表示するデータのタイプを選択し、データを表示する期間を編集します。

機能	読み取り権限	書き込み権限
ユーザーの管理	**[Administration]** > **[Manage Users]** ウィンドウで、ユーザーとユーザーグループを表示します。	**[Administration]** > **[Manage Users]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、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。
その他の機能テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。
ポリシー	**[Configuration]** > **[Policies]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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]** ウィンドウで、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。

機能	読み取り権限	書き込み権限
ポリシーの展開	**[Configuration]** > **[Policies]** ウィンドウで、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]** ウィンドウで、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。
RBAC VPN	**[Monitor]** > **[VPN]** ページで、ロールに基づいて VPN グループとセグメントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Dashboard]** > **[VPN Dashboard]** ページで、ロールに基づいて VPN グループとセグメントを表示します。	**[Administration]** > **[VPN Groups]** ウィンドウで、Cisco vManage の VPN と VPN グループを追加、編集、および削除し、VPN グループの権限を編集します。
ルーティング	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、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。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのリアルタイムルーティングに関する情報は **[Monitor]** > **[Network]** > **[Real-Time]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、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。
セキュリティ	**[Configuration]** > **[Security]** ウィンドウで、セキュリティ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]** > **[Security]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。
セキュリティポリシー設定	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、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。	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。

機能	読み取り権限	書き込み権限
セッション管理	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、ユーザーセッションを表示します。	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーセッションを編集します。
Settings	**[Administration]** > **[Settings]** ウィンドウで、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表示します。	**[Administration]** > **[Settings]** ウィンドウで、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。
SIG テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。

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]** ウィンドウで、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]** ウィンドウで、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 Template]** ウィンドウで、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。 （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。	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、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設定します。 （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。
テンプレートの設定	**[Configuration]** > **[Templates]** ウィンドウで、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]** ウィンドウで、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。 （注） Cisco vManage リリース 20.7.1 以降、デバイスにすでにアタッチされているテンプレートを作成、編集、または削除するには、ユーザーに [Template Deploy] オプションに対する書き込み権限が必要です。

機能	読み取り権限	書き込み権限
テンプレートの展開	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにアタッチされているデバイスを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにデバイスをアタッチします。
ツール	**[Tools]** > **[Operational Commands]** ウィンドウで、**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]** ウィンドウで、**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]** ウィンドウで、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]** ウィンドウで、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。
vAnalytics	**[Cisco vManage]** > **[vAnalytics]** ウィンドウで vAnalytics を起動します。	追加の権限はありません。
Workflows	**[Cisco vManage]** > **[Workflows]** ウィンドウからワークフローライブラリを起動します。	追加の権限はありません。

マルチテナント環境の RBAC ユーザーグループ

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 *42 :* 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 メニューから **[Administration]** > **[Manage Users]** を選択します。
2. デフォルトでは、[Users] 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、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、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] ドロップダウンリストで、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. [Add] をクリックします。

ユーザーの削除

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。

ユーザーを削除するには、次の手順を実行します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。

2. 削除するユーザーの [...] をクリックし、[Delete] をクリックします。
3. ユーザーの削除を確認するには、[OK] をクリックします。

ユーザーの詳細の編集

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。

ユーザーの詳細情報を編集するには、次のようにします。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. 編集するユーザーの [...] をクリックし、[Edit] をクリックします。
3. ユーザー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。

ユーザー 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。

はじめる前に

管理者ユーザーのパスワードを変更する場合は、この手順を実行する前に、クラスタ内のすべての Cisco vManage インスタンスからデバイステンプレートをアタッチ解除してください。この手順を完了した後、デバイステンプレートを再アタッチできます。

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. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. パスワードを変更するユーザーの [...] 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。

（注） 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 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. [Hostname] 列で、使用するデバイスを選択します。
3. [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 メニューから **[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。

ユーザーグループの管理

ユーザーはグループに配置されます。グループは、ユーザーが表示および変更を許可されている特定の構成および操作コマンドを定義します。1 人のユーザーが 1 つ以上のグループに属することができます。Cisco SD-WAN ソフトウェアには標準ユーザーグループが用意されており、必要に応じてカスタムユーザーグループを作成できます。

- [basic]：インターフェイスおよびシステム情報を表示する権限を持つユーザーが含まれます。
- [netadmin]：Cisco vManage ですべての操作を実行できる管理者ユーザーがデフォルトで含まれます。このグループに他のユーザーを追加できます。
- [operator]：情報を表示する権限のみを持つユーザーを含みます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：非セキュリティポリシーの表示と変更、デバイステンプレートのアタッチとデタッチ、非セキュリティデータの監視など、セキュリティ以外の操作を Cisco vManage で実行できるユーザーが含まれます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：セキュリティポリシーの表示と変更、セキュリティデータの監視など、セキュリティ操作を Cisco vManage で実行できるユーザーが含まれます。

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。

ユーザーグループの削除

不要になったユーザーグループは削除できます。たとえば、特定のプロジェクト用に作成したユーザーグループを、そのプロジェクトの終了時に削除する場合があります。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 削除するユーザーグループの名前をクリックします。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）は削除できません。

4. [Trash] アイコンをクリックします。
5. ユーザーグループの削除を確認するには、[OK] をクリックします。

ユーザーグループ権限の編集

既存のユーザーグループのグループ権限を編集できます。この手順では、必要なユーザーグループの構成済み機能の読み取りおよび書き込みアクセス許可を変更できます。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 権限を編集するユーザーグループの名前を選択します。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）の権限は編集できません。

4. [Edit] をクリックし、必要に応じて権限を編集します。
5. **[Save]** をクリックします。

admin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。

ユーザーグループの作成

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. [Add a User Group] をクリックします。

4. [User Group Name] を入力します。
5. ユーザーグループに割り当てる機能に対して、[Read] または [Write] チェックボックスをオンにします。
6. [Add] をクリックします。
7. 左側のナビゲーションパスで、新しいユーザーグループを表示できます。[Edit] をクリックして、既存の読み取りまたは書き込みルールを編集します。
8. [Save] をクリックします。

VPN セグメントの設定と管理

VPN セグメントを設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Administration]** > **[VPN Segments]** を選択します。Web ページに、構成されているセグメントのリストが表示されます。
2. 既存のセグメントを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. 新しいセグメントを追加するには、[Add Segment] をクリックします。
4. [Segment Name] フィールドにセグメントの名前を入力します。
5. [VPN Number] フィールドに、設定する VPN の番号を入力します。
6. 新しいセグメントを追加するには、[Add] をクリックします。

VPN グループの設定と管理

VPN グループを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Administration]** > **[VPN Groups]** を選択します。Web ページに、構成されているセグメントのリストが表示されます。
2. VPN グループを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. ダッシュボードに既存の VPN を表示するには、[…] をクリックし、[View Dashboard] をクリックします。[VPN Dashboard] には、設定された VPN デバイスのデバイス詳細が表示されます。
4. 新規 VPN グループを追加するには、[Add Group] をクリックします。
5. [Create VPN Group] から、[VPN Group Name] フィールドに VPN グループ名を入力します。
6. [Description] フィールドに VPN の簡単な説明を入力します。

7. [Enable User Group access] チェックボックスをオンにして、ユーザーグループ名を入力します。
8. [Assign Segment] で、[Add Segment] ドロップダウンリストをクリックして、新規または既存のセグメントを VPN グループに追加します。
9. それぞれのフィールドに [Segment Name] と [VPN Number] を入力します。
10. 設定 VPN グループをデバイスに追加するには、[Add] をクリックします。

リソース グループの管理

サポートされている最小リリース：Cisco IOS XE リリース 17.5.1a、Cisco vManage リリース 20.5.1

リソースグループを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Administration]** > **[Resource Groups]** を選択します。テーブルには、Cisco vManage に設定されているリソースグループのリストが表示されます。
2. リソースグループを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. 新しいリソースグループを追加するには、[Add Resource Group] をクリックします。
4. [Resource Group Name] と [Description] を入力します。
5. [Site ID] で、ドロップダウンリストからリソースグループに含める [Range] または [Select ID(S)] を入力します。
6. リソースグループをデバイスに追加するには、[Add] をクリックします。

ユーザーを追加するには、次の手順を実行します。

1. Cisco vManage メニューから **[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] 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、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザーを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、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] ドロップダウンリストで、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. [Add] をクリックします。

ポリシーに RBAC を設定するためのワークフロー

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

ポリシーに RBAC を設定するには、次のワークフローを使用します。

1. 選択した制御またはデータポリシーへの必要な読み取りまたは書き込み（R/W）アクセス権を持つユーザーグループを作成します。ユーザーグループの作成については、「ユーザーグループの作成」を参照してください。
2. ユーザーを作成して必要なユーザーグループに割り当てます。「ユーザーの作成」を参照してください。
3. 必要に応じて、ポリシー設定を作成、変更、または表示します。ポリシー設定については、「Configure Centralized Policies Using Cisco vManage」を参照してください。

ポリシー設定の変更

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

1. 新しいユーザー詳細情報を使用して Cisco vManage にログインします。
2. 要件に基づいて設定を変更または更新できます。

新しいユーザー詳細情報を使用して Cisco vManage にログインすると、自分に割り当てられているユーザー グループ コンポーネントのみを表示できます。ポリシーの設定の詳細については、『Cisco SD-WAN Policies Configuration Guide』を参照してください。

ポリシーに RBAC を設定するためのユーザーの割り当て

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

CFlowd データポリシーを作成または変更するユーザーを割り当てるには

CFlowd ユーザーグループを作成するには、次の手順を実行します。

1. Cisco vManage から**[Administration]** > **[Manage Users]**の順に選択します。
2. [User Groups] と [Add User Group] をクリックします。
3. [User Group Name] を入力します。

たとえば、cflowd-policy-only などです。

4. ユーザーグループに割り当てる CFlowD ポリシー機能に対して、[Read] または [Write] チェックボックスをオンにします。
5. [Add] をクリックします。
6. 左側のナビゲーションパスで、新しいユーザーグループを表示できます。[Edit] をクリックして、既存の読み取りまたは書き込みルールを編集します。
7. **[Save]** をクリックします。

CFlowd ユーザーを作成するには、次の手順を実行します。

1. Cisco vManage で、**[Administration]** > **[Manage Users]** を選択します。
2. [ユーザー（Users）] をクリックします。
3. [ユーザの追加（Add User）] をクリックします。
4. [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。
5. [User Groups] ドロップダウンから [cflowd-policy-only] を選択します。

   [Resource Group] がデフォルトのリソースグループを選択できるようにします。
6. [Add] をクリックします。[Users] ウィンドウで新しいユーザーを表示できます。
7. ユーザーの既存の読み取りまたは書き込みルールを編集するには、[Edit] をクリックします。

Cflowd ポリシーを変更するには、次の手順を実行します。

1. 新しいユーザークレデンシャルを使用して Cisco vManage にログインします。

   ログインは [cflowd-policy-only] ユーザーグループに割り当てられるため、CFlowd ポリシーへのアクセスのみを表示できます。
2. 要件に基づいて構成を作成、変更、または更新できます。

機能テンプレートの詳細な RBAC の構成

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

特定のテンプレートアクセスを設定するには、ユーザーグループを作成し、共同管理の RBAC に関する情報で説明されているアクセス許可タイプを使用して、読み取りおよび書き込みアクセス許可を割り当てます。テンプレートアクセスを制限するためのアクセス許可オプションは、ユーザーグループを追加するときに選択した他のアクセス許可オプションとともに表示されます。

機能テンプレートの詳細な RBAC については、機能テンプレートの詳細な RBAC に関する情報 （156 ページ）を参照してください。

ユーザーグループの追加については、「ユーザーグループの作成」を参照してください。

アクセス許可のタイプと説明のリストについては、「ユーザーの管理」を参照してください。

CLI を使用した RBAC の設定

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。

（注） 特殊文字 ! を含むユーザーパスワードは二重引用符（" "）で囲みます。パスワード全体を二重引用符で囲まない場合、構成データベース（?）はこの特殊文字をスペースとして扱い、パスワードの残りの部分を無視します。

たとえば、パスワードが C!sc0 の場合は、"C!sc0" を使用します。

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）。

CLI を使用したグループの作成

Cisco SD-WAN ソフトウェアには、デフォルトのユーザーグループ（**basic**、**netadmin**、**operator**、**network_operations**、**security_operations**）が用意されています。ユーザー名 **admin** は自動的に **netadmin** ユーザーグループに配置されます。

必要に応じて、追加のカスタムグループを作成し、グループメンバーが持つ権限ロールを設定できます。特定の権限を持つカスタムグループを作成するには、グループ名と権限を設定します。

```
デバイス(config)# aaa authentication login user1 group radius enable
デバイス(config)# aaa authentication login user2 group radius enable
デバイス(config)# aaa authentication login user3 group radius enable
デバイス(config)#
```

group-name 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。名前に大文字は使用できません。一部のグループ名は予約されているため、設定できません。それらのリストについては、aaa 設定コマンドを参照してください。

リモート RADIUS または TACACS+ サーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。リモートサーバーが認証を検証し、VSA Cisco SD-WAN-Group-Name を使用してユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがロー

カルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

task オプションでは、グループメンバーが持つ権限ロールを一覧表示します。ロールは、**インターフェイス**、**ポリシー**、**ルーティング**、**セキュリティ**、および**システム**の 1 つ以上にすることができます。

RBAC の確認

詳細な RBAC アクセス許可を確認する

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

この手順を使用して、ユーザーグループに設定したアクセス許可を確認します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. ユーザーグループを表示するペインで、ユーザーグループを選択して、ユーザーグループに割り当てられている読み取りおよび書き込み権限を表示します。
4. テンプレートアクセスを制御する権限までスクロールして、ユーザーグループの設定を確認します。

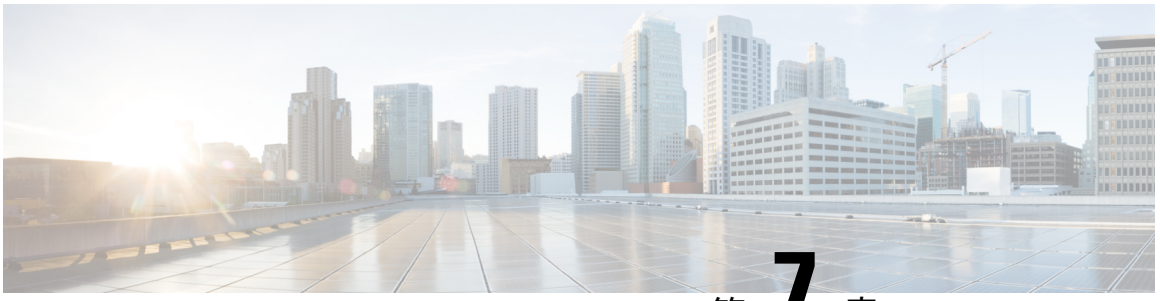
RBAC のモニタリング

VPN グループのデバイスのモニタリング

デバイスをモニタリングするには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。
2. [WAN - Edge] をクリックします。
3. ネットワークをモニタリングする [VPN Group] と [VPN Segment] を選択します。

   Web ページに、デバイスに設定されている VPN グループとセグメントのリストが表示されます。



第 7 章

デバイスの設定

Cisco vManage を使用して、すべてのデバイス（Cisco vManage システム自体、Cisco vSmart コントローラ、Cisco vBond オーケストレーション、およびルータ）の構成を作成して保存できます。デバイスが起動すると、Cisco vManage に接続し、デバイス構成がデバイスにダウンロードされます。（起動中のデバイスは最初に Cisco vBond オーケストレーション に接続し、デバイスを検証してから Cisco vManage の IP アドレスを送信します。）

すべてのデバイスの構成を作成する一般的な手順は同じです。このセクションでは、構成手順の概要を説明します。また、オーバーレイネットワークで構成を作成してデバイスを設定する前に実行する必要がある前提条件の手順についても説明します。

デバイス設定ワークフロー

Cisco vManage によって管理されるオーバーレイネットワーク内のデバイスは、Cisco vManage から設定する必要があります。基本的な設定手順は簡単です。

1. 機能テンプレートを作成します。
    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、[Add Templates] をクリックします。

（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。

2. デバイステンプレートを作成します。
   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 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. デバイステンプレートを個々のデバイスにアタッチします。
   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、テンプレートを選択します。

（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. [...] をクリックして、[Attach Devices] を選択します。

機能テンプレート

機能テンプレートは、デバイスの完全な設定の構成要素です。デバイスで有効にできる機能ごとに、Cisco vManage では、入力するテンプレートフォームが提供されます。このフォームでは、その機能の設定可能なすべてのパラメータの値を設定できます。

デバイス設定はデバイスタイプおよびルータタイプごとに異なるため、機能テンプレートはデバイスのタイプに固有です。

一部の機能はデバイスの操作に必須であるため、これらの機能のテンプレートを作成する必要があります。また、同じ機能について、同じデバイスタイプに対して複数のテンプレートを作成できます。

（注） Cisco IOS XE リリース 17.7.1a より前のリリースでは、Cisco vManage 機能テンプレートの定義または説明に特殊文字 [<] または [>] を入力すると、Cisco vManage で Cisco vManage 機能テンプレートをプレビューしようとしたときに 500 例外エラーが生成されました。

Cisco IOS XE リリース 17.7.1a 以降では、Cisco vManage 機能テンプレートの定義または説明に特殊文字 [<] または [>] を入力すると、その特殊文字は対応する HTML の [<] および [>] に変換されます。これは、すべての機能テンプレートに適用されます。Cisco vManage 機能テンプレートをプレビューするときに、500 例外エラーを受信しなくなりました。

デバイステンプレート

Cisco vManage を使用して、すべてのデバイス（Cisco vManage システム自体、Cisco vSmart コントローラ、Cisco vBond オーケストレーション、およびルータ）の設定を作成して保存します。デバイスが起動すると、Cisco vManage に接続し、デバイス構成がデバイスにダウンロードされます。（起動中のデバイスは最初に Cisco vBond オーケストレーション に接続し、デバイスを検証してから Cisco vManage の IP アドレスを送信します。）

デバイステンプレートには、デバイスの完全な運用設定が含まれます。デバイステンプレートは、個々の機能テンプレートを統合して作成します。

各デバイステンプレートは、デバイスのタイプに固有です。各デバイスタイプで、複数のデバイスの設定が同じ場合は、それらに同じデバイステンプレートを使用できます。たとえば、ネットワーク内のルータの多くが同じ基本設定である場合、同じテンプレートを使用してそれらを設定できます（以下で説明する設定変数を使用してテンプレートの違いを指定します）。同じデバイスタイプの設定が異なる場合は、個別のデバイステンプレートを作成します。

Cisco vManage で CLI テキスト形式の設定を直接入力してデバイステンプレートを作成することもできます。通常、設定テキストを含むテキストファイルをアップロードします（または、テキストファイルから設定テキストを切り取り、Cisco vManage に貼り付けます）。設定テキストを直接 Cisco vManage に入力することもできます。

Cisco IOS XE リリース 17.5.1a および Cisco vManage リリース 20.5.1 以降では、最新の設定がデバイスにプッシュされていない場合、最後に編集した設定を確認できます。詳細については、プッシュが失敗した場合のデバイステンプレートの編集 （211 ページ）を参照してください。

Cisco vManage リリース 20.5.1 以降では、デバイス変数ページにテキスト入力フィールドの代わりにテキストエリアが表示され、CLI デバイステンプレートを設定して容易に設定できるようになりました。

テンプレート変数

機能テンプレート内では、一部の設定コマンドとコマンドオプションはすべてのデバイスタイプで同じです。その他、デバイスシステムの IP アドレス、地理的な緯度と経度、タイムゾーン、オーバーレイ ネットワーク サイト識別子などは可変であり、デバイスごとに異なります。デバイステンプレートをデバイスにアタッチすると、これらのコマンド変数の実際の値を入力するように求められます。これは、各変数と各デバイスの値を入力して手動で行うか、各デバイスの値を含む CSV 形式の Excel ファイルをアップロードできます。

設定要件

セキュリティの前提条件

ネットワーク内のデバイスを設定する前に、そのデバイスを検証および認証して、Cisco vManage システム、Cisco vSmart コントローラ、および Cisco vBond オーケストレーションが、オーバーレイネットワークで許可されているデバイスとして認識できるようにする必要があります。

オーバーレイネットワーク内のコントローラ（Cisco vManage システム、vSmart コントローラ、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション）を検証および認証するには、これらのデバイスに署名付き証明書をインストールする必要があります。

ルータを検証および認証するには、シスコから認定シリアル番号ファイルを受け取ります。このファイルには、ネットワークで許可されているすべてのルータのシリアル番号とシャーシ番号がリストされています。それから、シリアル番号ファイルを Cisco vManage にアップロードします。

変数スプレッドシート

作成する機能テンプレートには、ほとんどの場合、変数が含まれます。デバイステンプレートをデバイスにアタッチするときに Cisco vManage で変数に実際の値を設定するには、各デバイスの変数値をリストした Excel ファイルを作成し、そのファイルを CSV 形式で保存します。

スプレッドシートでは、ヘッダー行に変数名が含まれ、後続の各行はデバイスに対応し、変数の値が定義されます。スプレッドシートの最初の 3 つの列は次の順番である必要があります。

- csv-deviceId：デバイスのシリアル番号（デバイスを一意に識別するために使用）。ルータの場合、シスコから送信された認定シリアル番号ファイルでシリアル番号を受け取ります。他のデバイスの場合、シリアル番号は、Symantec またはルート CA から受け取る署名付き証明書に含まれています。

  csv-deviceIP：デバイスのシステム IP アドレス（**system ip address** コマンドの入力に使用）。

- csv-host-name：デバイスのホスト名（**system hostname** コマンドの入力に使用）。

オーバーレイネットワーク内のすべてのデバイス（Cisco vSmart コントローラ、Cisco vBond オーケストレーション、およびルータ）に対して 1 つのスプレッドシートを作成できます。全デバイスのすべての変数に値を指定する必要はありません。

機能テンプレートからのデバイステンプレートの作成

デバイステンプレートは、デバイスの完全な運用構成を定義します。デバイステンプレートは、いくつかの機能テンプレートで構成されています。各機能テンプレートは、特定の Cisco SD-WAN ソフトウェア機能の構成を定義します。一部の機能テンプレートは必須であり、アスタリスク（*）で示され、一部はオプションです。必須の各機能テンプレートと一部のオプショ

ンのテンプレートには、工場出荷時のデフォルトテンプレートがあります。工場出荷時のデフォルトテンプレートを持つソフトウェア機能の場合、工場出荷時のデフォルトテンプレート（Factory_Default_ feature-name _Template という名前）を使用するか、カスタム機能テンプレートを作成できます。

機能テンプレートからのデバイステンプレートの作成

デバイステンプレートを作成するには、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. [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をクリックし、[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。

   vManage NMS は、そのデバイスタイプのすべての機能テンプレートを表示します。必須の機能テンプレートはアスタリスク（*）で示され、残りのテンプレートはオプションです。デフォルトでは、各機能の工場出荷時のデフォルトテンプレートが選択されています。
5. [Template Name] フィールドに、デバイステンプレートの名前を入力します。

   このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
6. [Description] フィールドにデバイステンプレートの説明を入力します。

   このフィールドは必須であり、任意の文字とスペースを含めることができます。
7. 機能テンプレートの工場出荷時のデフォルト設定を表示するには、目的の機能テンプレートを選択して、[View Template] をクリックします。
8. [Cancel] をクリックして [Configuration Template] 画面に戻ります。
9. 機能のカスタムテンプレートを作成するには、目的の工場出荷時のデフォルト機能テンプレートを選択し、[Create Template] をクリックします。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、機能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。
10. [Template Name] フィールドに、機能テンプレートの名前を入力します。

このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。

11. [Description] フィールドに機能テンプレートの説明を入力します。

    このフィールドは必須であり、任意の文字とスペースを含めることができます。

12. 各フィールドに、必要な値を入力します。その他のフィールドを表示するには、タブまたはプラス記号（+）をクリックする必要がある場合があります。

13. 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 [Scope] 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 *43*:

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、「設定テンプレートでの変数値の使用」を参照してください。 デフォルト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。

14. 一部のパラメータグループについては、グループ全体をデバイス固有としてマークできます。これを行うには、[Mark as Optional Row] チェックボックスをオンにします。

これらのパラメータはグレー表示されるため、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。

15. **[Save]** をクリックします。

16. 手順6～13を繰り返して、追加のソフトウェア機能ごとにカスタムテンプレートを作成します。特定の機能テンプレートの作成の詳細については、「**Available Feature Templates**」にリストされているテンプレートを参照してください。

17. [Create] をクリックします。新しい設定テンプレートが [Device Template] テーブルに表示されます。

    [Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。

機能テンプレートからデバイステンプレートを作成するもう1つの方法は、最初に1つ以上のカスタム機能テンプレートを作成してから、デバイステンプレートを作成することです。同じ機能に対して複数の機能テンプレートを作成できます。機能テンプレートのリストについては、「**Available Feature Templates**」を参照してください。

1. [Feature] をクリックします。

2. [Add template] をクリックします。

3. [Select Devices] で、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。

   複数のデバイスタイプで使用できる機能に対して、1つの機能テンプレートを作成できます。ただし、設定しているデバイスタイプでのみ使用できるソフトウェア機能については、別の機能テンプレートを作成する必要があります。

4. 機能テンプレートを選択します。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、必須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。機能にオプションのパラメータがある場合、テンプレートフォームでは必須パラメータの後にプラス記号（+）が表示されます。

5. [Template Name] フィールドに、機能テンプレートの名前を入力します。

   このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。

6. [Description] フィールドに機能テンプレートの説明を入力します。

   このフィールドは必須であり、任意の文字とスペースを含めることができます。

7. 必要な各パラメータについて、目的の値を選択し、該当する場合はパラメータの範囲を選択します。各パラメータの値ボックスのドロップダウンリストから範囲を選択します。

8. 必須パラメータのプラス記号（+）をクリックして、オプションのパラメータの値を設定します。

9. **[Save]** をクリックします。
10. 作成する追加の機能テンプレートごとに、手順 2 ～ 9 を繰り返します。
11. [デバイス（Device）] をクリックします。
12. [Create Template] ドロップダウンリストをクリックし、[From Feature Template] を選択します。
13. [Device Model] ドロップダウンリストから、デバイス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。

    vManage NMS に、選択したデバイスタイプの機能テンプレートが表示されます。必須の機能テンプレートはアスタリスク（*）で示されます。その他のテンプレートは省略可能です。
14. [Template Name] フィールドに、デバイステンプレートの名前を入力します。

    このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
15. [Description] フィールドにデバイステンプレートの説明を入力します。

    このフィールドは必須であり、任意の文字とスペースを含めることができます。
16. 機能テンプレートの工場出荷時のデフォルト設定を表示するには、目的の機能テンプレートを選択して、[View Template] をクリックします。
17. [Cancel] をクリックして [Configuration Template] 画面に戻ります。
18. 工場出荷時のデフォルト構成を使用するには、[Create] をクリックしてデバイステンプレートを作成します。新しいデバイステンプレートが [Device Template] テーブルに表示されます。[Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。
19. 工場出荷時の設定を変更するには、工場出荷時のデフォルトテンプレートを使用しない機能テンプレートを選択します。使用可能な機能テンプレートのドロップダウンリストから、作成した機能テンプレートを選択します。
20. 変更する工場出荷時のデフォルト機能テンプレートごとに、手順 19 を繰り返します。
21. [Create] をクリックします。新しい設定テンプレートが [Device Template] テーブルに表示されます。

    [Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが機能テンプレートのコレクションから作成されたことを示す「Feature」が表示されます。

デバイス CLI テンプレートの作成

Cisco vManage で直接 CLI テキスト形式の設定を入力してデバイステンプレートを作成するには、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. [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をクリックし、[CLI Template] を選択します。
4. [Device] 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. [Template Name] フィールドに、デバイステンプレートの名前を入力します。

   このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（–）、下線（_）のみです。スペースやその他の文字を含めることはできません。
6. [Description] フィールドにデバイステンプレートの説明を入力します。

   このフィールドは必須であり、任意の文字とスペースを含めることができます。
7. [CLI Configuration] ボックスで、手入力するか、カットアンドペーストするか、ファイルをアップロードして、構成を入力します。
8. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{*variable-name*}}; の形式で変数名を直接入力することもできます。たとえば、{{hostname}} です。
9. [Add] をクリックします。新しいデバイステンプレートが [Device Template] テーブルに表示されます。

   [Feature Templates] 列には、デバイステンプレートに含まれている機能テンプレートの数が表示され、[Type] 列には、デバイステンプレートが CLI テキストから作成されたことを示す「CLI」が表示されます。

デバイステンプレートの管理

表 *44 :* 機能の履歴

機能名	リリース情報	説明
デバイステンプレートでのドラフトモードのサポート	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、デバイステンプレート設定の変更を Cisco vManage に保存し、これらの設定変更を後で複数の Cisco IOS XE SD-WAN デバイス に適用できます。設定の変更を保存する機能により、より大きなデバイステンプレート設定の生成とデバイスへの適用が簡素化されます。

デバイステンプレートの編集

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] または [Feature Templates] をクリックし、テンプレートを選択します。

（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、[Feature Templates] のタイトルは [Feature] です。

3. [...] をクリックして、[Edit] をクリックします。

デバイスにアタッチされている場合、デバイスまたは機能テンプレートの名前を変更することはできません。

（注） テンプレートは、1 つ以上の vManage サーバーから同時に編集できます。テンプレートの同時編集操作には、次のルールが適用されます。

- 同じデバイスまたは機能テンプレートを同時に編集することはできません。
- デバイステンプレートを編集しているとき、そのデバイステンプレートにアタッチされている他のすべての機能テンプレートはロックされ、編集操作を実行することはできません。
- デバイステンプレートにアタッチされている機能テンプレートを編集しているとき、そのデバイステンプレートとそれにアタッチされている他のすべての機能テンプレートはロックされ、編集操作を実行することはできません。

テンプレートの削除

テンプレートを削除しても、関連する設定はデバイスから削除されません。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

2. [Device Templates] または [Feature Templates] をクリックし、テンプレートを選択します。

（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、[Feature Templates] のタイトルは [Feature] です。

3. [...] をクリックし、[Delete] をクリックします。
4. テンプレートの削除を確認するには、[OK] をクリックします。

テンプレートのコピー

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] または [Feature Templates] をクリックし、テンプレートを選択します。

（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、[Feature Templates] のタイトルは [Feature] です。

3. [...] をクリックして、[Copy] をクリックします。
4. 新しいテンプレート名と説明を入力します。
5. [コピー（**Copy**）] をクリックします。

CLI デバイステンプレートの編集

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、テンプレートを選択します。

（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. [...] をクリックして、[Edit] をクリックします。
4. [Device CLI Template] で、テンプレートを編集します。
5. [更新（Update）] をクリックします。

設定テンプレートでの変数値の使用

オーバーレイネットワークでは、構成がほぼ同じである同じタイプの複数のデバイスが存在する場合があります。この状況は、複数の店舗または支店の場所にあるルータが同一のサービス

を提供しているが、個々のルータが独自のホスト名、IPアドレス、GPSロケーション、およびその他のサイト固有のプロパティ（BGPネイバーなど）を持っている場合に、ルータで最も一般的に発生します。この状況は、すべてが同一のポリシーとCisco vManageシステムで構成されている必要がある、Cisco vSmartコントローラ などの冗長コントローラデバイスを備えたネットワークでも発生します。繰り返しますが、各コントローラには、ホスト名やIPアドレスなどの独自のパラメータがあります。

これらのデバイスの設定プロセスを簡素化するために、静的設定値と変数値の両方を含む単一の設定テンプレートを作成できます。静的な値はすべてのデバイスで共通であり、変数の値は個々のデバイスにのみ適用されます。個々のデバイスをデバイス設定テンプレートにアタッチするときに、変数の実際の値を指定します。

機能設定テンプレートのパラメータの変数値は、次の2つの方法で設定できます。

- パラメータの範囲を[Device Specific]にする：個々の設定パラメータについて、[Device Specific]を選択して、パラメータを変数としてマークします。各変数は、キーと呼ばれる一意のテキスト文字列で識別する必要があります。[Device Specific]を選択すると、[Enter Key]ボックスが開き、デフォルトのキーが表示されます。デフォルトキーを使用するか、また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て、デフォルトキーを変更できます。
- 関連パラメータのグループをオプションとしてマークする：一部の機能設定テンプレートの一部の機能については、機能全体をオプションとしてマークできます。この方法で機能をマークするには、機能設定テンプレートのセクションで[Mark as Optional Row]をクリックします。変数パラメータは淡色表示になり、機能設定テンプレートでそれらの値を構成することはできません。

デバイスを構成にアタッチするときに、次のいずれかの方法で、変数のデバイス固有の値を入力します。

- ファイルから：テンプレートをデバイスにアタッチする場合、ファイルをvManage NMSにロードします。これは、すべての変数をリストし、各デバイスの変数の値を定義するCSV形式のExcelファイルです。
- 手動：デバイステンプレートをデバイスにアタッチすると、Cisco vManageではデバイス固有の各パラメータの値を求めるプロンプトが表示され、各パラメータの値を入力します。

（注） Cisco SD-WANではテンプレートのプッシュ操作で最大500の変数をサポートします。

変数パラメータのファイルの使用

ファイルからデバイス固有の変数値をロードするには、テンプレート変数ファイルを作成します。このファイルは、デバイスの構成内のすべての変数をリストし、各変数の値を定義するCSV形式のExcelファイルです。このファイルをオフラインで作成し、デバイス構成をオー

バーレイネットワーク内の 1 つ以上のデバイスに接続するときに、Cisco vManage サーバーにインポートします。

オーバーレイネットワークの Cisco IOS XE SD-WAN デバイスの数が少なくない場合は、テンプレート変数 CSV ファイルを作成することをお勧めします。

CSV ファイル形式

CSV ファイルは、デバイスの構成に必要な変数ごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行には変数名（行ごとに 1 つの変数）が含まれます。その後の各行は、デバイスに対応し、そのデバイスの変数の値を定義します。

オーバーレイネットワーク内のすべてのデバイス（Cisco IOS XE SD-WAN デバイス、、Cisco vManage システム、Cisco vSmart コントローラ、および Cisco vBond オーケストレーション）に対して 1 つのスプレッドシートを作成することも、デバイスタイプごとに 1 つのスプレッドシートを作成することもできます。システムは、シリアル番号からデバイスタイプを判別します。

スプレッドシートでは、デバイスタイプごとおよび個々のデバイスごとに、必要な変数の値のみを指定します。変数の値を指定する必要がない場合は、そのセルを空白のままにします。

スプレッドシートの最初の 3 列は、次の項目であり、表示されている順序である必要があります。

カラム	カラムのヘッダー	説明
1	csv-deviceId	デバイスのシリアル番号（デバイスを一意に識別するために使用）。Cisco IOS XE SD-WAN デバイスの場合、シスコから送信された認定シリアル番号ファイルでシリアル番号を受け取ります。他のデバイスの場合、シリアル番号は、Symantec またはルート CA から受け取る署名付き証明書に含まれています。
2	csv-deviceIP	デバイスのシステム IP アドレス（**system ip address** コマンドの入力に使用）。
3	csv-host-name	デバイスのホスト名（**system hostname** コマンドの入力に使用）。

残りの列の見出しは、機能設定テンプレートの [Enter Key] ボックスで定義されている一意の変数キーである必要があります。これらの残りの列は、任意の順序にすることができます。

スケルトン CSV ファイルの生成

前のセクションで説明したフォーマットを使用して、テンプレート変数 CSV ファイルを手動で作成するか、Cisco vManage で必要なすべての列と列見出しを含むスケルトン CSV ファイル

を生成することができます。この生成されたCSVファイルには、Ciscoデバイスタイプごとに1つの行があり、デバイス設定に含まれるすべての機能テンプレートに必要な各変数の列見出しがあります。列見出しのテキストは、デバイス固有のパラメータを識別するキー文字列に対応します。次に、各変数の値を行に入力します。

Cisco vManage でスケルトン CSV ファイルを生成するには、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. [Feature Templates] をクリックし、[Add Template] をクリックします。

（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。

3. 1つの Cisco IOS XE SD-WAN デバイスルータ、1つの Cisco vSmart コントローラ、1つの Cisco vManage システム、および1つの Cisco vBond オーケストレーション に必要な機能テンプレートを作成します。

   機能テンプレートごとに、次の手順を実行します。

   1. デフォルト値を持つフィールドの場合、その値をすべてのデバイスに使用することを確認します。デフォルトを使用しない場合は、範囲を [Global] または [Device-specific] に変更します。
   2. すべてのデバイスに適用されるフィールドについては、フィールドの横にある [Global] アイコンを選択し、必要なグローバル値を設定します。
   3. デバイス固有のフィールドの場合は、フィールドの横にある [Device-specific] アイコンを選択し、フィールドを空白のままにします。

4. Cisco デバイスタイプごとに、デバイステンプレートを作成します。
5. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
6. [Device Templates] をクリックし、テンプレートリストテーブルから目的のデバイステンプレートを選択します。

（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。

7. [...] をクリックして、[Export CSV] をクリックします。
8. デバイステンプレートごとに手順 7 と 8 を繰り返します。

エクスポートされた CSV ファイルを編集して、オーバーレイネットワーク内の各デバイスの少なくともデバイスシリアル番号、デバイスシステム IP アドレス、およびデバイスホスト名を追加します。次に、各デバイスに必要なデバイス固有の変数の値を追加します。変数名に

は、スラッシュ（/）、バックスラッシュ（\）、または括弧（( )）を含めることができないことに注意してください。

必要に応じて、CSV ファイルを 1 つのファイルに結合できます。

CSV ファイルのインポート

CSV ファイルでデバイス固有の変数値を使用するには、デバイステンプレートを Viptela デバイスにアタッチするときにファイルをインポートします。

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. 目的のテンプレートについて、[...] をクリックし、[Attach Devices] を選択します。
4. [Attach Devices] ダイアログボックスで、[Available Devices] で目的のデバイスを選択し、矢印をクリックしてそれらを [Selected Devices] に移動します。
5. [Attach] をクリックします。
6. 上向き矢印をクリックします。[Upload CSV File] ボックスが表示されます。
7. アップロードする CSV ファイルを選択し、[Upload] をクリックします。

添付プロセス中に、[Import file] をクリックして Excel ファイルをロードします。Cisco vManage がオーバーレイネットワークでデバイスの重複するシステム IP アドレスを検出すると、警告メッセージまたはポップアップウィンドウが表示されます。デバイステンプレートを Viptela デバイスにアタッチするプロセスを続行する前に、システム IP アドレスを修正して重複を削除する必要があります。

デバイス固有の変数とオプション行の値の手動入力

デバイス固有として設定する機能テンプレートのパラメータの場合、デバイステンプレートをデバイスにアタッチすると、Cisco vManage でこれらのパラメータに使用する値の入力を求めるプロンプトが表示されます。この方法でデバイス固有の値を入力すると、テストネットワークやPOCネットワーク、または小規模なネットワークを展開する場合に役立ちます。一般に、この方法は、大規模なネットワークでは適切に拡張できません。

多くのデバイスの設定がいくつかのパラメータを除いて同じである場合、機能設定テンプレートで、そのパラメータが設定のオプションの行であることを指定できます。オプションの行を選択すると、機能テンプレートはパラメータをデバイス固有として自動的にマークし、これらのパラメータは淡色表示されるため、テンプレートで設定することはできません。パラメータをデバイス固有として個別にマークする必要はありません。デバイステンプレートをデバイスにアタッチすると、Cisco vManage でこれらのパラメータに使用する値の入力を求めるプロン

プトが表示されます。オプションの行を使用してデバイス固有の値を入力すると、多数のCisco IOS XE SD-WAN デバイス のグループがブランチまたはサイトで同一のサービスを提供しているが、個々のルータが独自のホスト名、IPアドレス、GPSロケーション、およびその他のサイトまたはストアプロパティ（BGP ネイバーなど）を持っている場合に便利です。

オプションの行は、一部の機能設定テンプレートの一部のパラメータで使用できます。パラメータまたはパラメータセットをオプションの行として扱うには、[Mark as Optional Row] ボックスをクリックします。これらのタイプのパラメータについては、機能設定テンプレートに、設定されたすべてのパラメータをリストした表があります。オプションの列は、オプションの行を示します。

テンプレートをデバイスにアタッチするときに、デバイス固有の変数またはオプションの行の変数の値を手動で入力するには、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. [Device Templates] をクリックし、目的のデバイステンプレートを選択します。

（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. [...] をクリックして、[Attach Devices] をクリックします。[Attach Devices] ダイアログボックスが開きます。
4. 1 台以上のデバイスを [Available Devices] から選択し、[Selected Devices] に移動します。
5. [Attach] をクリックします。
6. [Chassis Number] リストで、目的のデバイスを選択します。
7. [...] をクリックして、[Edit Device Template] をクリックします。[Update Device Templates] ダイアログボックスが開きます。
8. オプションのパラメータの値を入力します。オプションの行を使用しているときに、特定のデバイスのパラメータを含めない場合は、値を指定しないでください。
9. **Update** をクリックします。
10. [Next] をクリックします。

    同じシステム IP アドレスを持つデバイスがある場合、[Next] をクリックすると、ダイアログボックスが表示されるか、エラーメッセージが表示されます。重複しないようにシステムの IP アドレスを変更し、[Save] をクリックします。次に、もう一度 [Next] をクリックします。

（注） デバイスのシステム IP を変更する前に、デバイスの OMP をシャットダウンする必要があります。

11. 左側のペインで、デバイスを選択します。右側のペインにデバイス設定が表示され、右上隅の [Config Preview] タブが選択されています。
12. [Config Diff] をクリックして、この設定とデバイスで現在実行されている設定との相違をプレビューします（該当する場合）。前の画面で入力した変数値を編集するには、[Back] をクリックします。
13. [Configure Devices] をクリックして、設定をデバイスにプッシュします。

    [Status] 列には、設定が正常にプッシュされたかどうかが表示されます。行の左側にある右山括弧をクリックして、プッシュ操作の詳細を表示します。

デバイステンプレートの表示

テンプレートの表示

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] または [Feature Templates] をクリックし、表示するテンプレートを選択します。

（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、[Feature Templates] のタイトルは [Feature] です。

3. […] をクリックして、[View] をクリックします。

機能テンプレートにアタッチされたデバイステンプレートの表示

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、表示する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。

3. […] をクリックして、[Show Attached Device Templates] をクリックします。

   [Device Templates] ダイアログボックスが開き、機能テンプレートがアタッチされているデバイステンプレートの名前が表示されます。

デバイステンプレートにアタッチされたデバイスの表示

機能テンプレートから作成したデバイステンプレートの場合：

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、表示するテンプレートを選択します。

（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. [...] をクリックして、[Attach Devices] をクリックします。
4. [Attach Devices] で、[Attached Devices] をクリックします。

CLI テンプレートから作成したデバイステンプレートの場合：

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、表示するテンプレートを選択します。

（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. […] をクリックして、[Show Attached Devices] をクリックします。

デバイステンプレートのアタッチとアタッチ解除

ネットワーク上のデバイスを設定するには、デバイステンプレートをデバイスにアタッチします。デバイスにアタッチできるデバイステンプレートは1つだけなので、テンプレートには、個々の機能テンプレートを統合して作成したか、CLIテキスト形式の設定を入力して作成したかにかかわらず、デバイスの完全な設定が含まれている必要があります。機能テンプレートとCLI 形式の設定を組み合わせて対応させることはできません。

オーバーレイネットワークの Cisco IOS XE SD-WAN デバイスでは、1 つ以上の vManage サーバーから同じ操作を並行して実行できます。次のテンプレート操作を並行して実行できます。

- デバイスへのデバイステンプレートのアタッチ
- デバイスからのデバイステンプレートのデタッチ
- デバイスがアタッチされているデバイステンプレートの変数値の変更

テンプレート操作には、次のルールが適用されます。

- デバイステンプレートがデバイスにすでにアタッチされている場合は、その機能テンプレートの 1 つを変更できます。**[Update]** > **[Configure Devices]** をクリックすると、他のすべてのテンプレート操作（デバイスのアタッチ、デバイスのデタッチ、デバイス値の編集など）は、更新操作が完了するまで、すべての vManage サーバーでロックされます。つまり、更新が完了するまで、別の vManage サーバー上のユーザーはテンプレート操作を実行できません。

- 1 つまたは複数の vManage サーバーから、さまざまなデバイスでデバイステンプレートのアタッチおよびデタッチ操作を同時に実行できます。ただし、これらの操作のいずれかが 1 つの vManage サーバーで進行中の場合、アタッチまたはデタッチ操作が完了するまで、どのサーバーの機能テンプレートも編集できません。

（注） Cisco vManage リリース 20.5 より前に作成されたテンプレートはデバイスにアタッチされると失敗するため、機能テンプレートを再作成する必要があります。

設定中のデバイスがネットワーク上に存在し、動作中である場合、設定はすぐにデバイスに送信され、ただちに有効になります。デバイスがまだネットワークに参加していない場合は、デバイスへの設定のプッシュがスケジュールされます。デバイスがネットワークに参加すると、Cisco vManage はデバイスがネットワークに存在することを認識した直後に設定をプッシュします。

デバイスへのデバイステンプレートのアタッチ

同じテンプレートを複数のデバイスにアタッチすることができ、これは1回の操作で同時に実行できます。

デバイステンプレートを 1 つ以上のデバイスにアタッチするには、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. [Device Templates] をクリックし、目的のテンプレートを選択します。

（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. [...] をクリックして、[Attach Devices] をクリックします。[Select Devices] タブが選択された状態で [Attach Devices] ダイアログボックスが開きます。
4. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索し、リストからデバイスを選択するか、[Select All] をクリックします。
5. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。
6. [Attach] をクリックします。
7. テンプレートに変数が含まれている場合は、次のいずれかの方法で、選択した各デバイスの欠落している変数値を入力します。
   - 表の列で、または [...] をクリックして [Edit Device Template] をクリックして、各デバイスの値を手動で入力します。オプションの行を使用しているときに、特定のデバイスのパラメータを含めない場合は、値を指定しないでください。
   - [Import File] をクリックして、すべての変数をリストし、各デバイスの各変数の値を定義した CSV ファイルをアップロードします。

8. **[更新（Update）]** をクリックします。
9. [Next] をクリックします。

   同じシステム IP アドレスを持つデバイスがある場合、[Next] をクリックすると、ダイアログボックスが表示されるか、エラーメッセージが表示されます。重複しないようにシステムの IP アドレスを変更し、[Save] をクリックします。次に、もう一度 [Next] をクリックします。
10. 左ペインでデバイスを選択し、デバイスにプッシュする準備ができている設定をプレビューします。右側のペインにデバイスの設定が表示され、[Config Preview] タブが選択されています。[Config Diff] タブをクリックして、この設定とデバイスで現在実行されている設定との相違を表示します（該当する場合）。[Back] ボタンをクリックして、前の画面で入力した変数値を編集します。
11. Cisco IOS XE SD-WAN デバイスをアタッチしている場合は、[Configure Device Rollback Timer] をクリックして、ルータがオーバーレイネットワークへの制御接続を失った場合にデバイスが以前の設定にロールバックする時間間隔を設定します。[Configure Device Rollback Time] ダイアログボックスが表示されます。
    1. [Devices] ドロップダウンリストからデバイスを選択します。
    2. ロールバックタイマーを有効にするには、[Set Rollback] スライダでスライダを左にドラッグして、ロールバックタイマーを有効にします。この操作を行うと、スライダの色は灰色から緑色に変わります。
    3. ロールバックタイマーを無効にするには、[Enable Rollback] スライダをクリックします。タイマーを無効にすると、[Password] フィールド ダイアログボックスが開きます。vManage NMS へのログインに使用したパスワードを入力します。
    4. [Device Rollback Time] スライダで、スライダを目的の値までドラッグします。デフォルトの時間は 5 分です。6 ～ 15 分の時間を設定できます。
    5. ロールバックタイマー設定からデバイスを除外するには、[Add Exception] をクリックして、除外するデバイスを選択します。
    6. [Configure Device Rollback Time] ダイアログボックス下部の表には、テンプレートをアタッチするすべてのデバイスとそのロールバック時間が一覧表示されます。設定されたロールバック時間を削除するには、デバイス名の [Trash] アイコンをクリックします。
    7. **[Save]** をクリックします。
12. [Configure Devices] をクリックして、設定をデバイスにプッシュします。[ステータス] 列には、構成が正常にプッシュされたかどうかが表示されます。右山括弧をクリックして、プッシュ操作の詳細を表示します。

テンプレート用に変数スプレッドシートを CSV 形式でエクスポート

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、目的のテンプレートを選択します。

（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. [...] をクリックして、[Export CSV] をクリックします。

デバイスでテンプレートが拒否される理由の特定

画面を使用してテンプレートをデバイスに接続すると、デバイスがテンプレートを拒否する場合があります。これが発生する理由の1つは、デバイステンプレートに誤った変数値が含まれているためです。デバイスがテンプレートを拒否すると、以前の構成に戻ります。

デバイスがテンプレートを拒否した理由を特定するには、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. [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. デバイスの場所を特定します。[Template Status] 列には、デバイスがテンプレートを拒否した理由が示されます。

プッシュが失敗した場合のデバイステンプレートの編集

表 *45 :* 機能の履歴

機能名	リリース情報	説明
最後に編集された設定の取得	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、デバイスへの設定のプッシュが失敗したときに、最後に編集された設定を確認できます。最後に編集した設定のコピーが保存され、次のプッシュの前に設定を編集できるように取得できます。

設定をデバイスにプッシュし、プッシュが失敗した場合は、最後に編集した設定を確認して、デバイスへの設定のプッシュに失敗した原因を特定できます。

前提条件

最後に編集した設定を確認するには、デバイステンプレートをデバイスにアタッチする必要があります。

Cisco vManage で最後に編集された設定の確認

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、デバイステンプレートを選択します。

（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. [...] をクリックし、[Edit] を選択します。

   [CLI Configuration] ボックスにはデバイスで実行されている現在の設定が表示されます。
4. [Load Last Attempted Config] をクリックして、最後に編集された設定を表示します。
5. [Config Diff] をクリックして、現在の設定と最後に編集した設定の相違を表示します。設定を変更する、または [Load Last Attempted Config] をクリックすると、[Config Diff] オプションが使用可能になります。
6. [Config Preview] をクリックします。

（注） [Load Last Attempted Config] および [Config Diff] オプションは、設定がデバイスにプッシュされていない場合にのみ使用できます。

7. [更新（Update）] をクリックします。
8. [Configure Devices] をクリックして、設定をデバイスにプッシュします。[Status] 列には、設定が正常にプッシュされたかどうかが表示されます。[>] をクリックして、プッシュ操作の詳細を表示します。

デバイス ロールバック タイマーの変更

デフォルトでは、Cisco IOS XE SD-WAN デバイスを設定テンプレートにアタッチすると、ルータが 5 分後に正常に起動できない場合、前の設定に戻るか、前の設定にロールバックします。CLI から作成した設定では、デバイスのロールバックタイマーを変更できます。

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、デバイステンプレートを選択します。

（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. […] をクリックし、[Change Device Values] をクリックします。

   右側のペインにデバイスの構成が表示され、[Config Preview] タブが選択されています。

4. 左側ペインで、デバイスの名前をクリックします。

5. [Configure Device Rollback Timer] をクリックします。[Configure Device Rollback Time] ポップアップページが表示されます。

6. [Devices] ドロップダウンリストからデバイスを選択します。

7. ロールバックタイマーを有効にするには、[Set Rollback slider] でスライダを左にドラッグして、ロールバックタイマーを有効にします。この操作を行うと、スライダの色は灰色から緑色に変わります。

8. ロールバックタイマーを無効にするには、[Enable Rollback slider] をクリックします。タイマーを無効にすると、[Password] フィールド ダイアログ ボックスが表示されます。vManage NMS へのログインに使用したパスワードを入力します。

9. [Device Rollback Time] スライダで、スライダを目的の値までドラッグします。デフォルトの時間は 5 分です。6 ～ 15 分の時間を設定できます。

10. ロールバックタイマー設定からデバイスを除外するには、[Add Exception] をクリックして、除外するデバイスを選択します。

11. [Configure Device Rollback Time] ダイアログボックスの表には、テンプレートをアタッチするすべてのデバイスとそのロールバック時間が一覧表示されます。設定されたロールバック時間を削除するには、デバイス名の [Trash] アイコンをクリックします。

12. **[Save]** をクリックします。

13. [Configure Devices] をクリックして、設定をデバイスにプッシュします。[Status] 列には、構成が正常にプッシュされたかどうかが表示されます。[(+)] をクリックして、プッシュ操作の詳細を表示します。

デバイス設定のプレビューと設定の相違点の表示

CLI から作成した設定の場合、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. [Device Templates] をクリックし、目的のデバイステンプレートを選択します。

（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. […] をクリックし、[Change Device Values] をクリックします。

   右側のペインにデバイスの設定が表示され、[Config Preview] が選択されています。

4. デバイスの名前をクリックします。

5. [Config Diff] をクリックして、この設定とデバイスで現在実行されている設定との相違を表示します（該当する場合）。[Back] をクリックして、前の画面で入力した変数値を編集します。

6. [Configure Devices] をクリックして、設定をデバイスにプッシュします。[Status] 列には、設定が正常にプッシュされたかどうかが表示されます。右山括弧をクリックして、プッシュ操作の詳細を表示します。

デバイスの変数値の変更

デバイス設定テンプレートから作成した設定の場合、テンプレートに変数が含まれていると、vManage NMS は、テンプレートがデバイスにアタッチされるときに、変数に実際の値を自動的に入力できます。これを行うには、各デバイスの変数値をリストした Excel ファイルを作成し、そのファイルを CSV 形式で保存します。これらの変数の値を手動で入力することもできます。

設定をデバイスにプッシュした後、変数に割り当てられた値を変更できます。

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、目的のデバイステンプレートを選択します。

（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. […] をクリックし、[Change Device Values] をクリックします。

   画面には、そのデバイステンプレートにアタッチされているすべてのデバイスの表が表示されます。

4. 目的のデバイスで […] をクリックし、[Edit Device Template] をクリックします。

5. [Update Device Template] ダイアログボックスで、変数リストの項目の値を入力します。

6. **Update** をクリックします。

7. [Next] をクリックします。

8. [Configure Devices] をクリックして、設定をデバイスにプッシュします。[Status] 列には、設定が正常にプッシュされたかどうかが表示されます。右山括弧をクリックして、プッシュ操作の詳細を表示します。

デフォルトのデバイステンプレート

表 *46 :* 機能の履歴

機能名	リリース情報	説明
デフォルトのデバイステンプレート	Cisco IOS XE リリース 17.2.1r	デフォルトのデバイステンプレートは、展開でデバイスをすばやく起動するために使用できる基本情報を提供します。 この機能は、シスコ クラウド サービス ルータ 1000V シリーズ、Cisco C1111-8PLTELA サービス統合型ルータ、および Cisco 4331 サービス統合型ルータでサポートされます。

デフォルトのデバイステンプレートは、展開でデバイスを起動するために使用できる基本情報を提供します。これにより、ネットワークでの動作に必要な最小限の情報をデバイスにすばやくプロビジョニングできます。

デバイスのデフォルトテンプレートの情報を直接編集または更新することはできませんが、テンプレートをコピーしてから、そのコピーを編集できます。

デフォルトのデバイステンプレートを使用するには、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. [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. [Template Type] ドロップダウンリストから [Default] を選択します。

   デフォルトのデバイステンプレートのリストが表示されます。
4. 次のいずれかの操作を行います。
   - デフォルトのデバイステンプレートをデバイスにアタッチするには、[...] をクリックし、[Attach Devices] を選択します。

[Attach Devices] ダイアログボックスで、アタッチするデバイスを選択し、[Attach] をクリックします。

- デフォルトのデバイステンプレートの構成設定を表示するには、[...] をクリックし、[View] を選択します。
- デフォルトのデバイステンプレートをコピーするには、[...] をクリックし、[View] を選択します。

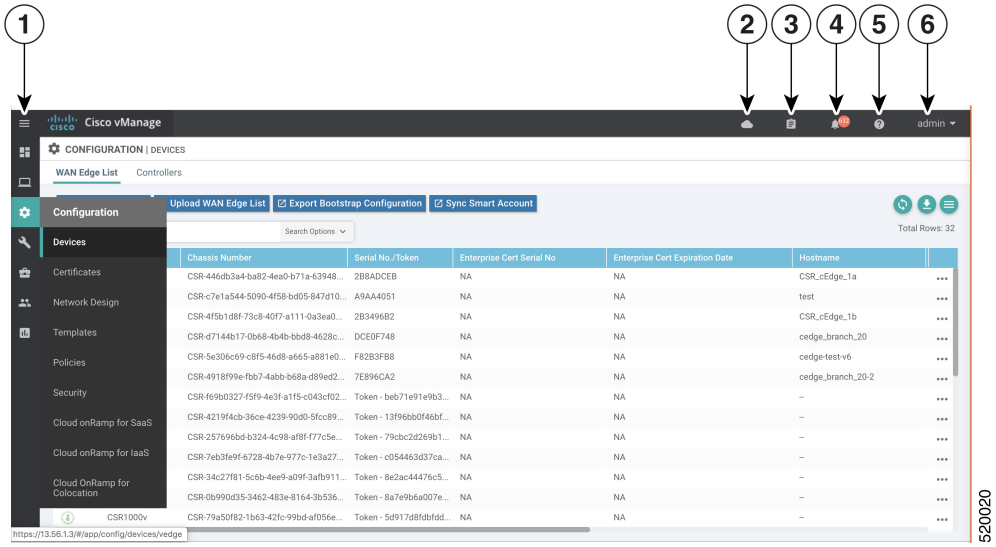
  [Template Copy] ダイアログボックスで、作成するコピーの一意の名前と説明を入力し、[Copy] をクリックします。

  コピーされたバージョンは、編集可能な機能テンプレートになります。
- デバイステンプレートからのデバイス固有の設定を含む Excel ファイルを CSV 形式で作成するには、[...] をクリックし、[Export CSV] を選択します。表示されるダイアログボックスを使用して、CSV ファイルを開くか保存します。

  この CSV ファイルは、他のデバイステンプレートを作成するときに、デバイス固有の設定の参照として使用できます。

vManage を使用してデバイスを構成する

[Devices] 画面を使用して、デバイスの追加と削除、CLI と vManage 間のデバイスのモードの切り替え、WAN エッジシリアル番号ファイルのアップロード、ブートストラップ構成のエクスポート、およびその他のデバイス関連のタスクを実行します。



1	メニュー
2	CloudExpress

3	タスク
4	アラーム
5	ヘルプ
6	ユーザー プロファイル

コンフィギュレーション モードの変更

デバイスは、次のいずれかの設定モードにできます。

- vManage モード：テンプレートがデバイスにアタッチされていて、CLI を使用してデバイスの設定を変更することはできません。
- CLI モード：テンプレートがデバイスにアタッチされておらず、デバイスは CLI を使用してローカルに設定できます。

vManage からテンプレートをデバイスにアタッチすると、デバイスは vManage モードになります。デバイスの構成をローカルで変更する必要がある場合は、デバイスを CLI モードに戻すことができます。

ルータを vManage モードから CLI モードに切り替えるには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] をクリックし、デバイスを選択します。
3. [Change Mode] ドロップダウンリストをクリックして、[CLI mode] を選択します。

SSH ウィンドウが開きます。デバイスにログインするには、ユーザー名とパスワードを入力します。その後、CLI コマンドを発行して、デバイスを構成または監視できます。

コントローラデバイスを vManage モードから CLI モードに切り替えるには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [Controllers] をクリックし、デバイスを選択します。
3. [Change Mode] ドロップダウンリストをクリックします。
4. [CLI mode] を選択し、デバイスタイプを選択します。[Change Mode - CLI] ウィンドウが開きます。
5. [vManage mode] ペインからデバイスを選択し、右矢印をクリックしてデバイスを [CLI mode] ペインに移動します。
6. [Update to CLI Mode] をクリックします。

SSH ウィンドウが開きます。デバイスにログインするには、ユーザー名とパスワードを入力します。その後、CLI コマンドを発行して、デバイスを構成または監視できます。

WAN エッジルータの認定シリアル番号ファイルのアップロード

表 *47 :* 機能の履歴

機能名	リリース情報	説明
証明書の SUDI 要件を削除する	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、証明書のシリアル番号の代わりにサブジェクトの SUDI シリアル番号を使用して、デバイスを Cisco SD-WAN オーバーレイネットワークに追加できます。

WAN eEdge ルータの認証済みシリアル番号ファイルには、該当する場合、対象の SUDI シリアル番号、シャーシ番号、およびオーバーレイネットワーク内のすべての有効な Cisco IOS XE SD-WAN デバイス の証明書シリアル番号が含まれています。Cisco Plug-and-Play（PnP）ポータルからシリアル番号ファイルを取得して Cisco vManage にアップロードします。（Cisco PnP の詳細については、『Cisco Plug and Play Support Guide for Cisco SD-WAN Products』を参照してください。）Cisco vManage から、ネットワーク内のコントローラにファイルを送信します。このファイルは、Cisco SD-WAN オーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにし、オーバーレイネットワークが動作できるようにするために必要です。

WAN エッジルータの認証済みシリアル番号ファイルを Cisco vManage にアップロードしてからネットワーク内のコントローラにダウンロードするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] をクリックし、[Upload WAN Edge List] をクリックします。
3. [Upload WAN Edge List] 画面で、次の手順を実行します。
    1. [Choose File] をクリックし、Cisco PnP から受信した WAN エッジルータの認証シリアル番号ファイルを選択します。
    2. ルータを自動的に検証してそのシャーシとシリアル番号をコントローラに送信するには、[Validate the uploaded vEdge List and send to controllers] チェックボックスを選択します。このオプションを選択しない場合は、**[Configuration]** > **[Certificates]** > **[WAN Edge List]**で各ルータを個別に検証する必要があります。
    3. [Upload] をクリックします。

ネットワーク内のルータのリストがルータテーブルに表示され、各ルータの詳細が表示されます。

Cisco vManage リリース 20.9.2 から、**[Monitor]** > **[Devices]**ページで、新しく追加された WAN エッジデバイスを監視できます。

Cisco スマートアカウントからの WAN エッジルータシリアル番号のアップロード

Cisco SD-WAN によりオーバーレイ ネットワーク コンポーネントが相互に検証および認証できるようにし、オーバーレイネットワークが動作できるようにするには、Cisco SD-WAN にオーバーレイネットワーク内のすべての有効な Cisco IOS XE SD-WAN デバイス のシャーシ番号が必要です。

さらに、証明書のシリアル番号、サブジェクト SUDI のシリアル番号、または両方の番号がすべてのデバイスに必要です。

WAN エッジルータの承認済みシリアル番号を Cisco Smart アカウントから vManage NMS にアップロードしてから、オーバーレイネットワーク内のすべてのコントローラにダウンロードするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] をクリックし、[Sync Smart Account] をクリックします。
3. [Sync with Smart Account] ウィンドウで、次の手順を実行します。
    1. スマートアカウントの [Username] および [Password] を入力します。
    2. ルータを自動的に検証し、そのシャーシ番号とシリアル番号をコントローラに送信するには、[Validate the Uploaded WAN Edge List and Send to Controllers] チェックボックスをオンにします。このオプションを選択しない場合は、**[Configuration]** > **[Certificates]** > **[WAN Edge List]**で各ルータを個別に検証する必要があります。
    3. [同期（Sync）] をクリックします。

ネットワーク内のルータのリストがルータテーブルに表示され、各ルータの詳細が表示されます。

Cisco vManage リリース 20.9.2 から、**[Monitor]** > **[Devices]**ページで、新しく追加された WAN エッジデバイスを監視できます。

CSV 形式でのデバイスデータのエクスポート

オーバーレイネットワークでは、同一または実質的に同一の構成を持つ同じタイプの複数のデバイスが存在する場合があります。たとえば、Cisco vSmart コントローラ が冗長なネットワークでは、各コントローラに同一のポリシーを設定する必要があります。別の例は、複数のサイトに Cisco IOS XE SD-WAN デバイス があり、それぞれの Cisco IOS XE SD-WAN デバイス が各サイトで同じサービスを提供しているネットワークです。

これらのデバイスの設定は基本的に同一であるため、1 セットの機能テンプレートを作成し、それを 1 つのデバイステンプレートに統合して、すべてのデバイスの設定に使用できます。変数をリストし、各デバイスの各デバイス固有の変数値を定義する CSV 形式の Excel ファイルを作成できます。すると、デバイステンプレートをデバイスにアタッチするときに、このファイルをロードできます。

すべてのデバイスのデータをCSV形式のファイルにエクスポートするには、[Export]アイコンをクリックします。下向きの矢印であるこのアイコンは、WAN エッジリストと [Controllers] タブの両方で、フィルタ基準の右側にあります。

vManage NMS はデバイステーブルのすべてのデータをCSV形式でExcelファイルにダウンロードします。

デバイス設定の表示とコピー

デバイスの実行コンフィギュレーションを表示する

実行コンフィギュレーションは、vManageがデバイスのメモリから取得する構成情報です。この情報は、トラブルシューティングに役立ちます。

デバイスの実行コンフィギュレーションを表示するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] または [Controllers] をクリックし、デバイスを選択します。
3. […] をクリックし、[Running configuration] をクリックします。

デバイスのローカル設定を表示する

ローカル設定は、vManage がデバイス用に保存した設定です。この情報は、トラブルシューティングや、デバイスにvManageから到達できない場合などにデバイスにアクセスする方法を決定するのに役立ちます。

[Configuration] ▶ [Templates] を使用して作成されたデバイスのローカル設定を表示するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] または [Controllers] をクリックし、デバイスを選択します。
3. […] をクリックし、[Local Configuration] をクリックします。

ルータ設定をコピーする

サイトの1つのルータを別のルータに置き換える場合は、古いルータの設定を新しいルータにコピーします。次に、古いルータをネットワークから削除し、新しいルータを追加します。

古いルータから新しいルータに設定をコピーするには、次の手順を実行します。

1. Cisco vManage のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. 新しい Cisco IOS XE SD-WAN デバイス を無効としてマークします。
3. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
4. [WAN Edge List] で、古いルータを選択します。

5. […] をクリックし、[Copy Configuration] をクリックします。
6. [Copy Configuration] ウィンドウで、新しいルータを選択します。
7. 設定のコピーを確認するには、[Update] をクリックします。

設定を新しいルータにコピーしたら、新しいルータをネットワークに追加できます。まず、以下で説明するように、古いルータをネットワークから削除します。次に、新しいルータをネットワークに追加します。

1. Cisco vManage のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. 新しいルータを有効としてマークします。
3. [Send to Controller] をクリックします。

WAN エッジルータの削除

ご使用の展開からルータを削除する必要がある場合は、ルータを削除します。これにより、WAN エッジルータのシリアル番号リストから、ルータに保存されている次の項目が削除されます。

- シャーシ番号
- 証明書シリアル番号
- サブジェクト SUDI シリアル番号

（注） ルータを削除すると、vManage NMS からもルータ設定が完全に削除されます。

ルータを削除するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
2. WAN エッジルータを無効とマークします。
3. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
4. [WAN Edge List] をクリックし、ルータを選択します。
5. [...] をクリックし、[Delete WAN Edge] をクリックします。
6. デバイスの削除を確認するには、[OK] をクリックします。
7. Cisco vManage のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
8. [Send to Controller] をクリックします。

クラウドルータの廃止

クラウドルータ（Cisco Cloud Services Router 1000V など）を廃止すると、デバイスのシリアル番号が Cisco vManage から削除され、デバイスの新しいトークンが生成されます。次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] をクリックし、クラウドルータを選択します。
3. […] をクリックし、[Decommission WAN Edge] をクリックします。
4. ルータの廃止を確定するには、[OK] をクリックします。

テンプレートログとデバイス起動の表示

テンプレートアクティビティのログの表示

テンプレートアクティビティのログには、設定テンプレートの作成、編集、削除、および設定テンプレートのデバイスへの接続ステータスに関する情報が含まれます。この情報は、トラブルシューティングに役立ちます。

テンプレートアクティビティのログを表示するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] または [Controllers] をクリックし、デバイスを選択します。
3. […] をクリックし、[Template Log] をクリックします。

デバイスの起動ステータスの表示

オーバーレイネットワークでのルータまたはコントローラの起動に関連する操作のステータスを表示できます。この情報は、これらの操作を監視するのに役立ちます。

デバイスの起動のステータスを表示するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] または [Controllers] をクリックし、デバイスを選択します。
3. […] をクリックし、[Device Bring Up] をクリックします。

Cisco vBond オーケストレーション の追加

Cisco vBond オーケストレーション は、Cisco IOS XE SD-WAN デバイス と vManage コントローラ間の接続を自動的に調整します。Cisco IOS XE SD-WAN デバイス または Cisco vSmart コントローラ が NAT の背後にある場合、Cisco vBond オーケストレーション は最初の NAT トラ

バーサル オーケストレータとしても機能します。Cisco vBond オーケストレーションの追加手順：

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [Controllers] をクリックします。
3. [Add Controller] ドロップダウンリストをクリックし、[vBond] を選択します。
4. [Add vBond] ウィンドウで、次の手順を実行します。
    1. vBond コントローラの [vBond Management IP Address] を入力します。
    2. vBond オーケストレータにアクセスにするための [Username] と [Password] を入力します。
    3. 証明書生成プロセスを自動的に実行できるようにするには、[Generate CSR] チェックボックスをオンにします。
    4. [Add] をクリックします。
5. Cisco vBond オーケストレーション を追加するには、手順 2、3、4 を繰り返します。

[Controllers] 画面のコントローラのリストに、新しい Cisco vBond オーケストレーション が追加されます。

Cisco vSmart コントローラ の設定

vSmart コントローラの追加

Cisco vBond オーケストレーション で Cisco IOS XE SD-WAN デバイス が認証されると、Cisco vSmart コントローラ への接続に必要な Cisco IOS XE SD-WAN デバイス 情報が Cisco vBond オーケストレーションから取得できます。Cisco vSmart コントローラ では、データポリシーおよびアプリケーション ルート ポリシーを介してネットワーク全体のデータトラフィックのフローが制御されます。Cisco vSmart コントローラ を設定するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [Controllers] をクリックします。
3. [Add Controller] ドロップダウンをクリックして、[vSmart] を選択します。
4. [Add vSmart] ウィンドウで、次の手順を実行します。
    1. Cisco vSmart コントローラ のシステム IP アドレスを入力します。
    2. Cisco vSmart コントローラ にアクセスにするためのユーザー名とパスワードを入力します。
    3. コントロールプレーン接続に使用するプロトコルを選択します。デフォルトは[DTLS]です。DTLS（Datagram Transport Layer Security）プロトコルは、UDP 通信のセキュリティを提供するように設計されています。

4. [TLS] を選択した場合は、TLS 接続に使用するポート番号を入力します。デフォルトは 23456 です。

   TLS（Transport Socket Layer）プロトコルは、ネットワーク上で通信セキュリティを提供します。
5. 証明書生成プロセスを自動的に実行できるように、[Generate CSR] チェックボックスをオンにします。
6. [Add] をクリックします。

5. Cisco vSmart コントローラ を追加する場合は、手順 2、3、4 を繰り返します。vManage NMS では、ネットワーク内で最大 20 の Cisco vSmart コントローラ をサポートできます。

[Controllers] 画面のコントローラのリストに、新しい Cisco vSmart コントローラ が追加されます。

コントローラ詳細の編集

コントローラ詳細を編集すると、コントローラデバイスの IP アドレスとログイン情報を更新できます。コントローラ詳細を編集するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [Controllers] をクリックして、コントローラを選択します。
3. [...] をクリックして、[Edit] をクリックします。
4. [Edit] ウィンドウで、IP アドレスとログイン情報を編集します。
5. **[Save]** をクリックします。

コントローラの削除

コントローラを削除すると、オーバーレイから削除されます。コントローラを交換する場合、またはネットワークで不要になった場合は、コントローラを削除します。

コントローラを削除するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [Controllers] をクリックして、コントローラを選択します。
3. […] をクリックし、[Invalidate] をクリックします。
4. デバイスとそのすべての制御接続の削除を確認するには、[OK] をクリックします。

コントローラでのリバースプロキシの設定

個々の vManage NMS および Cisco vSmart コントローラ でリバースプロキシを設定するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。

2. [Controllers] をクリックして、コントローラを選択します。
3. […] をクリックして、[Add Reverse Proxy] をクリックします。

   [Add Reverse Proxy] ダイアログボックスが表示されます。
4. [Add Reverse Proxy] をクリックします。
5. デバイスのプライベート IP アドレスとポート番号を設定します。プライベート IP アドレスは、VPN 0 のトランスポート インターフェイスの IP アドレスです。デフォルト ポート番号は、12346 です。これは、オーバーレイネットワークで制御とトラフィックを処理する接続を確立するために使用するポートです。
6. デバイスのプロキシ IP アドレスとポート番号を設定して、プライベートとパブリックの IP アドレスおよびポート番号の間のマッピングを作成します。
7. Cisco vManage NMS または Cisco vSmart コントローラ に複数のコアがある場合は、コアごとに手順 5 と 6 を繰り返します。
8. [Add] をクリックします。

オーバーレイネットワークでリバースプロキシを有効にするには、Cisco vManage のメニューから **[Administration]** > **[Settings]** を選択します。次に、[Reverse Proxy] バーで [Edit] をクリックします。[Enabled] をクリックして、[Save] をクリックします。

UCS-E テンプレートの作成

表 *48* : 機能の履歴

機能名	リリース情報	機能説明
UCS-E テンプレートの作成	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能を使用すると、インターフェイス機能テンプレートを介して UCS-E インターフェイスを UCS-E サーバーに接続できます。

Cisco Unified Computing System（UCS）E シリーズ サーバーの詳細については、『Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide』を参照してください。

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. リストから Cisco IOS XE SD-WAN デバイスを選択します。
5. [Other Templates] セクションで、[UCSE] をクリックします。

   UCSE 機能テンプレートが開きます。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、下部には統合管理コントローラ（IMC）を設定するためのフィールドがあります。
6. [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。
7. [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。

テンプレートのベイとスロットの設定

[Basic Configuration] タブをクリックして、テンプレートのベイおよびスロットを設定します。

パラメータ名	説明
ベイ	SAS ドライブベイの数を指定します。
スロット	メザニンアダプタのスロット番号を指定します。

IMC 設定

[IMC] タブをクリックして、テンプレートの IMC パラメータを設定します。

パラメータ名	説明
アクセス ポート	

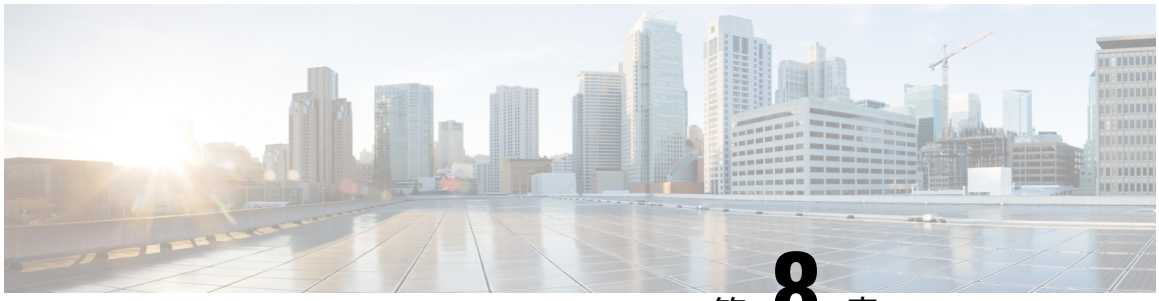
パラメータ名	説明

	インターフェイスをアクセス ポートとして設定します。アクセスポートでは VLAN を 1 つだけ設定でき、ポートは 1 つの VLAN のトラフィックだけを伝送できます。
	
	すべてのハードウェアモデルに専用のアクセスポートがあるわけではありません。サポートされているハードウェアについては、ご使用の Cisco SD-WAN リリースのリリースノートを参照してください。
	
	使用可能なオプション：
	
	• Dedicated
	
	• Shared
	
	ポートのタイプ（GE または TE）は、ハードウェアモデルによって異なります。
	
	次に例を示します。
	
	`Router(config-ucse)#imc access-port shared-lom ?`
	`GE1 GE1`
	`TE2 TE2`
	`TE3 TE3`
	`console Console`
	`failover Failover`
	
	一部のハードウェアモデルには GE ポートがあり、一部には TE ポートがあります。
	
	ハードウェアモジュールに応じて、適切なポート（GE または TE）を設定する必要があります。これを行わない場合、エラーが発生します。
	
	• 次のコマンドを使用して、UCS-Eモジュールのハードウェアモデルタイプを取得できます。
	
	show inventory
	
	show platform
	
	• Failover：Shared の下のサブオプション。
	
	次に例を示します。
	
	`Router(config)#`**`ucse subslot 1/0`**
	
	`Router(config-ucse)#`**`imc access-port ?`**
	`MGMT MGMT Interface`
	`shared-lom Shared LOM`

パラメータ名	説明
	Router(config-ucse)#**imc access-port shared-lom ?** **GE1 GE1** **TE2 TE2** **TE3 TE3** **console Console** **failover Failover**
IPv4 Address	UCS-E 管理ポートアドレスを指定します。
デフォルト ゲートウェイ	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。 デフォルトは Enabled です。
VLAN ID	1 ～ 4094 の値の VLAN 番号を指定します。
Assign Priority	優先順位を割り当てます。

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。

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。
デフォルト	[Default] が選択されている場合、このフィールドは有効になりません。



第 8 章

設定グループと機能プロファイル

表 *49 :* 機能の履歴

機能名	リリース情報	説明
設定グループと機能プロファイル	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能は、Cisco SD-WAN の構成にシンプルで再利用可能な構造化されたアプローチを提供します。構成グループ、つまり、Cisco SD-WAN によって管理されるネットワーク内の 1 つ以上のデバイスに適用できる機能または構成の論理グループを作成できます。また、必要な機能、推奨される機能、または独自に使用される機能に基づいてプロファイルを作成し、プロファイルを組み合わせてデバイス構成を完成させることもできます。 Cisco vManage の設定グループワークフローは、設定グループと機能プロファイルを作成するためのガイド付きの方法を提供します。

機能名	リリース情報	説明
設定グループと機能プロファイル（フェーズ II）	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	設定グループ機能には、次の拡張機能が導入されています。 • 次の機能のサポートを追加します。 • SNMP • セルラー インターフェイス • BGP ルーティング（トランスポートおよび管理プロファイル） • ワイヤレス LAN • Switch Port • SVI インターフェイス • DHCP サーバ • ThousandEyes • VPN、インターフェイス、および BGP 機能に IPv6 構成のサポートを追加します。 • システムプロファイルの一部であるグローバル設定に次のオプションを追加します。これらのオプションは、[Other Settings] タブに追加されました。 • 着信または発信ネットワーク接続がアイドル状態のときにキープアライブタイマーを生成する • 小規模な TCP および UDP サーバーを有効にする • コンソールロギングを有効にする • IP ソースルーティングを有効にする • ログメッセージを VTY セッションに表示する • SNMP IFINDEX パーシステンスを有効にする • BOOTP サーバーを有効にする

機能名	リリース情報	説明
単一ルータサイトの設定グループワークフローの作成	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、設定グループの作成ワークフローが導入されます。この簡素化されたワークフローでは、さまざまな設定ページが 1 つのページに統合されているため、構成を一度に簡単に確認できます。このワークフローでは、設定グループの作成時に、基本設定に加えて WAN および LAN ルーティングを設定することもできます。その結果、ワークフローから作成された設定をすぐに展開できるようになりました。

設定グループに関する情報

設定グループ機能を使用すると、次のことができます。

- ガイド付きワークフローのいずれかを使用して設定グループを作成します（設定グループ、高速サイト設定グループ、またはカスタム設定グループを作成します）

（注） [Rapid Site Configuration Group] および [Custom Configuration Group] ワークフローは、Cisco vManage リリース 20.8.x でのみ使用できます。

- [Deploy Configuration Group] ワークフローを使用して、設定グループを使用してデバイスを展開する

（注） Cisco vManage リリース 20.8.x では、[Deploy Configuration Group] ワークフローは、[Provision WAN Sites and Devices] ワークフローと呼ばれます。

設定グループの概要

設定グループ機能は、Cisco SD-WAN の設定にシンプルで再利用可能な構造化されたアプローチを提供します。

- **設定グループ**：設定グループは、Cisco SD-WAN によって管理されるネットワーク内の 1 つ以上のデバイスに適用できる機能または設定の論理グループです。このグループ化は、ビジネスニーズに基づいて定義およびカスタマイズできます。
- **機能プロファイル**：機能プロファイルは、さまざまな設定グループ間で再利用できる設定の柔軟な構成要素です。必要な機能、推奨される機能、または独自に使用される機能に基づいてプロファイルを作成し、プロファイルを組み合わせてデバイス設定を完成させることができます。
- **機能**：機能プロファイルは機能で構成されます。機能は、さまざまな設定グループ間で共有する個々の機能です。

設定グループのワークフローの概要

Cisco vManage リリース 20.9.1 以降では、簡素化された設定グループの作成ワークフローにより、単一ルータサイトの設定グループの作成を手順を追って実行できます。 ワークフローにより、設定とトラブルシューティングのエクスペリエンスが向上します。ワークフローには次の機能があります。

- 設定グループの名前と説明を指定し、ネットワークの実行を維持するための基本設定を構成できます。
- 基本設定に加えて、設定グループの作成時に詳細オプションを構成することもできます。たとえば、WAN および LAN ルーティングを設定できます。WAN トランスポート VPN に対して、BGP ルート、複数の静的 IPv4 ルート、またはその両方を構成できます。同様に、LAN サービス VPN に対して、BGP ルート、OSPF ルート、複数の静的 IPv4 ルート、またはこれらすべてのルートを構成できます。したがって、設定グループ自体の作成時に必要なすべてのオプションを構成でき、グループの作成後に機能を個別に変更する必要はありません。その結果、ワークフローから作成された設定をすぐに展開できます。
- ワークフロー内の 1 つのページでさまざまな構成設定を確認できます。
- 間違った設定を指定すると、赤で強調表示されます。その結果、エラーがあれば簡単に特定して修正できます。さらに、フィールド名の隣にあるアスタリスクは、ワークフロー内の必須設定を識別するのに役立ちます。

Cisco vManage の [Workflow Library] からワークフローにアクセスできます。

（注） Cisco vManage リリース 20.8.x では、[Rapid Site Configuration Group] および [Custom Configuration Group] ワークフローにより、設定グループを作成できました。ただし、Cisco vManage リリース 20.9.1 以降ではこれらのワークフローは廃止になっています。

構成グループの展開ワークフローの概要

設定グループの展開ワークフローを使用すると、デバイスを設定グループに関連付け、選択したデバイスに設定を展開できます。

（注） Cisco vManage リリース 20.8.x では、[Deploy Configuration Group] ワークフローは、[Provision WAN Sites and Devices] ワークフローと呼ばれます。

Cisco vManage の [Workflow Library] からワークフローにアクセスできます。

設定グループの利点

- シンプルさ：ワークフローベースの構成により、段階的な手順で利用できます。必須、オプション、および推奨されるシスコのネットワーキングのベストプラクティスを明確に識別できます。

  さらに、設定グループの基本設定と詳細設定が自動入力されるため、設定プロセスが簡素化されます。

- デイゼロ展開：設定グループのデイゼロセットアップにより、ブランチを簡単に作成し、デバイスを迅速に展開できます。

- 再利用性：1 つのデバイスモデルではなく、デバイスファミリ全体で構成コンポーネントを再利用できます。これにより、構成コンポーネントの管理が容易になります。

- 構造：Cisco vManage での共有構成に基づいてデバイスをグループ化できます。

- 可視性：設定グループに接続されている Cisco IOS XE SD-WAN デバイス に対して、サイトレベルのトポロジが生成されます。サイトのトポロジの表示の詳細については、「View Network Site Topology」を参照してください。

- 検索性：タグ付け機能により、設定グループ内の数百のデバイスからデバイスのサブセットを簡単に識別できます。デバイスへのタグの追加の詳細については、「Device Tagging」を参照してください。

設定グループでサポートされるデバイス

この機能は Cisco IOS XE SD-WAN デバイス でのみサポートされています。

設定グループの前提条件

Cisco IOS XE SD-WAN デバイス の最小ソフトウェアバージョン：Cisco IOS XE リリース 17.8.1a

（注） 下位互換サポートは Cisco IOS XE リリース 17.6.1a まで

Cisco vManage の最小ソフトウェアバージョン：Cisco vManage リリース 20.8.1

設定グループの制約事項

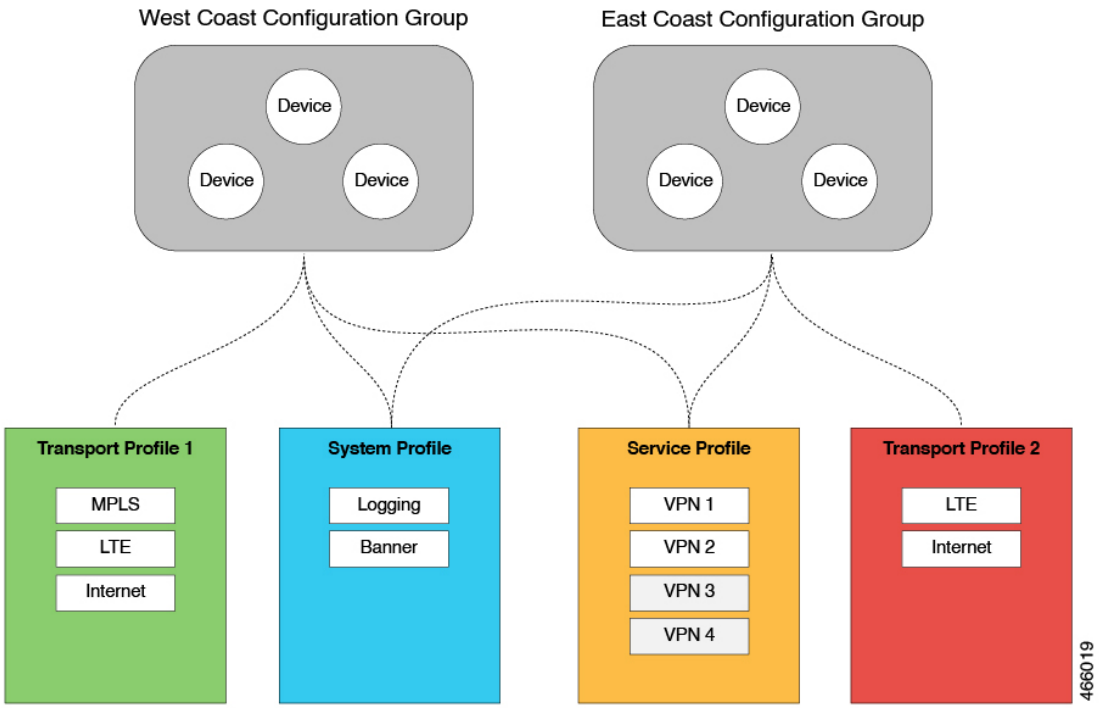
- デバイスは、設定グループまたはデバイステンプレートのいずれかに関連付けることができますが、両方に関連付けることはできません。
- デバイスは 1 つの設定グループにのみ追加できます。
- 設定グループに追加できるタグルールは 1 つだけです。

設定グループの使用例

ビジネスニーズに応じて設定グループを作成できます。たとえば、組織が北米で運営されており、西海岸と東海岸の両方にオフィスとネットワークインフラストラクチャがある場合、東海岸設定グループと西海岸設定グループの 2 つの設定グループを作成できます。

次の図は、東海岸設定グループと西海岸設定グループの両方が同じシステムプロファイルとサービスプロファイルを使用していることを示しています。トランスポートプロファイルは、両方のグループで異なります。

図 *1* : 設定グループの例



この図では次のようになっています。

- 東海岸設定グループと西海岸設定グループは、設定グループの例です。同様に、サプライチェーン組織は、小売店の設定グループや流通センターの設定グループなど、さまざまな施設の設定グループを作成できます。多国籍企業は、アメリカ地域設定グループやEMEA設定グループなど、さまざまな地域でのビジネスニーズに対応する設定グループを作成できます。
- システムプロファイル、トランスポートプロファイル、およびサービスプロファイルは、機能プロファイルの例です。
- ロギング、バナー、インターフェイス（MPLS、LTE、インターネットなど）、VPN1、VPN2、などが機能の例です。

設定グループワークフローの使用

はじめる前に

Cisco vBond オーケストレーション の IP アドレスが指定されていることを確認します。

1. Cisco vManage のメニューから、**[Administration]** > **[Settings]** > **[vBond]** を選択します。
2. Cisco vBond オーケストレーションの IP アドレスを入力します。

設定グループワークフローの作成の実行

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

Cisco vManage メニューから、**[Workflows]** > **[Create Configuration Group]** を選択します。 または、次の手順を実行します。

1. Cisco vManage のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Workflow Library] ページで、新しいワークフローを開始するか、既存のワークフローを再開します。
    1. 新しいワークフローを開始する：[Library] セクションで、[Create Configuration Group] をクリックします。または、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択し、[Add Configuration Group] をクリックします。
    2. 進行中のワークフローを再開する：[In-progress] セクションで、[Create Configuration Group] をクリックします。

ワークフローは、次のコンポーネントを生成します。

- 設定グループ
- 5 つの機能プロファイル：システムプロファイル、トランスポートおよび管理プロファイル、サービスプロファイル、CLI プロファイル（オプション）、およびその他のプロファイル（オプション）。もう 1 つのプロファイルには、オプションの ThousandEyes 機能が含まれています。

高速サイト設定グループワークフローの実行

（注） このワークフローは、Cisco vManage リリース 20.8.x でのみ使用できます。

1. Cisco vManage のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Workflow Library] ページで、新しいワークフローを開始するか、既存のワークフローを再開します。
    1. 新しいワークフローを開始する：[Library] セクションで、[Rapid Site Configuration Group] をクリックします。または、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択し、[Add Configuration Group] をクリックします。
    2. 進行中のワークフローを再開する：[In-progress] セクションで、[Rapid Site Configuration Group] をクリックします。

ワークフローは、次のコンポーネントを生成します。

- 設定グループ

- 4 つの機能プロファイル：システムプロファイル、トランスポートおよび管理プロファイル、サービスプロファイル、および CLI プロファイル（オプション）

カスタム設定グループワークフローの実行

（注） このワークフローは、Cisco vManage リリース 20.8.x でのみ使用できます。

1. Cisco vManage のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Workflow Library] ページで、新しいワークフローを開始するか、既存のワークフローを再開します。
   1. 新しいワークフローを開始する：[Library] セクションで、[Custom Configuration Group] をクリックします。または、**[Configuration]** > **[Templates]** > **[Configuration Groups]**を選択し、[Add Configuration Group] をクリックします。
   2. 進行中のワークフローを再開する：[In-progress] セクションで、[Custom Configuration Group] をクリックします。

ワークフローは、次のコンポーネントを生成します。

- A configuration group
- 3 つの機能プロファイル：システムプロファイル、トランスポートおよび管理プロファイル、およびサービスプロファイル

設定グループへのデバイスの追加

設定グループを作成したら、次のいずれかの方法でデバイスをグループに追加できます。

- デバイスを手動で追加します。
- ルールを使用して、デバイスをグループに自動的に追加します。

設定グループへのデバイスの手動追加

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. [Associated Devices] をクリックして、[Add Devices] をクリックします。

   [Add Devices to Configuration] ワークフローが開始されます。

4. ワークフローの指示に従ってください。

   選択したデバイスが [Devices] テーブルにリストされます。

ルールを使用した設定グループへのデバイスの追加

はじめる前に

デバイスにタグが追加されていることを確認します。タグ付けの詳細については、「デバイスのタグ付け」を参照してください。

ルールを使用した設定グループへのデバイスの追加

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. [Associated Devices] をクリックして、[Add and Edit Rules] をクリックします。

   [Automated Rules] サイドバーが表示されます。
4. [Rules] セクションで、次のオプションの値を選択します。
   - **Device Attribute**：[Tags] を選択します。
   - **Condition**：[Equal]、[Contains]、[Not contain]、[Not equal] のいずれかを選択します。これらの演算子の詳細については、「タグを使用したルールの適用例」を参照してください。
   - **Select Value**：使用可能なタグのリストからタグを選択します。

（注） デバイスがタグルールに一致する場合、デバイスは設定グループに追加されます。指定した値のいずれかを変更してタグルールを編集すると、デバイスはグループから削除されます。

5. [Apply] をクリックします。

   リストには、ルールに基づいて設定グループに追加またはグループから削除されるデバイスが表示されます。
6. [Confirm] をクリックして変更を適用します。

（注）

- 既存のルールと競合する場合、新しいルールは作成できません。
- デバイスがデバイステンプレートにすでにアタッチされている場合、デバイスにタグを追加できません。
- テンプレートをデバイスにアタッチし、タスクが進行中の場合は、デバイスにタグを追加できます。ただし、同じタグを使用して、このデバイスを設定グループに追加するルールを適用することはできません。これを行うには、デバイスをテンプレートからアタッチ解除するか、別のタグを使用する必要があります。

タスク詳細の確認

アクティブおよび完了したすべてのタスクのステータスを確認するには、次の手順を実行します。

1. [+] アイコンをクリックして、タスクの詳細を表示します。

   Cisco vManage にタスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

2. Cisco vManage のツールバーから [Task-list] アイコンをクリックします。

   Cisco vManage に、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。

タグを使用したルールの適用例

シナリオ：ネットワークに5つのデバイスがあり、タグ付けに基づいてデバイスを設定グループに追加します。

1. 各デバイスにタグを付けます。デバイスのタグ付けについては、「Cisco vManage を使用したデバイスへのタグの追加」を参照してください。

   次の例では、タグが 5 つの Cisco Catalyst 8000V デバイスに追加されています。

   表 *50* : デバイスのタグ付けの例

デバイス UUID	タグ
C8K-0001	CA1、CA2
C8K-0002	CA1、CA2、CA3
C8K-0003	CA1、CA4、CA5
C8K-0004	CA3、CA4
C8K-0005	CA3、CA5

2. ルールを使用して、各デバイスに追加したタグに基づいて、特定の設定グループにデバイスを追加します。

   ルールを適用するときは、次の演算子を使用できます。

   - Equal：この演算子は、一致するデータをチェックします。
   - Not equal：この演算子は、一致しないデータをチェックします。
   - Contain：この演算子は、データ内の任意の場所で値を検索します。
   - Not contain：この演算子は、指定された値をまったく含まないデータをフィルタリングします。

   ルールを使用してデバイスを設定グループに追加する方法については、「ルールを使用した設定グループへのデバイスの追加」を参照してください。

次の例は、デバイスのタグ付け方法に基づいて、ルールを適用するときにさまざまな演算子を使用した場合の影響を示しています。

ルール例 1

演算子：EQUAL

指定タグ：CA1、CA2

効果：これら 2 つのタグを含むすべてのデバイスに一致します。

設定グループ：A

結果：デバイス C8K-0001 および C8K-0002 が設定グループ A に追加されます。

ルール例 2

演算子：NOT EQUAL

指定タグ：CA1、CA2

効果：これらのタグの両方を含まないデバイスに一致します。

設定グループ：B

結果：デバイス C8K-0003、C8K-0004、および C8K-0005 が設定グループ B に追加されます。

ルール例 3

演算子：CONTAIN

指定タグ：CA1、CA2

効果：これらのタグのいずれかを含むすべてのデバイスに一致します。

設定グループ：C

結果：デバイス C8K-0001、C8K-0002、および C8K-0003 が設定グループ C に追加されます。

ルール例 4

演算子：NOT CONTAIN

指定タグ：CA1、CA2

効果：これらのタグのいずれも含まないデバイスに一致します。

設定グループ：D

結果：デバイス C8K-0004 および C8K-0005 が設定グループ D に追加されます。

デバイスの展開

設定グループにデバイスを追加した後、次のいずれかの方法でデバイスを展開できます。

手動でのデバイスの展開

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. [Associated Devices] をクリックします。
4. 1 つ以上のデバイスを選択し、[Deploy] をクリックします。

[Deploy Configuration Group] ワークフローを使用したデバイスの展開

はじめる前に

リストからグループを選択し、関連付けられたデバイスを展開できるように、1 つまたは複数の設定グループが作成されていることを確認します。

（注） Cisco vManage リリース 20.8.x では、[Deploy Configuration Group] ワークフローは、[Provision WAN Sites and Devices] ワークフローと呼ばれます。

デバイスの展開

1. Cisco vManage のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Deploy Configuration Group] ワークフローを開始します。
3. ワークフローの指示に従ってください。

設定グループからのデバイスの削除

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. [Associated Devices] をクリックします。
4. [Devices] テーブルで、設定グループから削除するデバイスを選択します。
5. [Remove Device] をクリックします。

（注） タグルールに基づいてデバイスが設定グループに自動的に追加された場合、上記の方法を使用してグループからデバイスを削除することはできません。これを行うには、タグルールを編集するか、ルールを削除する必要があります。タグルールの追加または編集の詳細については、「ルールを使用した設定グループへのデバイスの追加」を参照してください。

機能の管理

機能の追加

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. 目的の機能プロファイルをクリックします。
4. [Add Feature] をクリックします。
5. 機能ドロップダウンリストから機能を選択します。
6. [Name] フィールドに、機能の名前を入力します。
7. [Description] フィールドに機能の説明を入力します。説明には任意の文字とスペースを使用できます。
8. 必要に応じてオプションを設定します。
9. [Save] をクリックします。

サブ機能の追加

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. 目的の機能プロファイルをクリックします。
4. 機能の横にある […] をクリックし、[Add Sub-Feature] を選択します。
5. 機能ドロップダウンリストから機能を選択します。
6. [Name] フィールドに、機能の名前を入力します。
7. [Description] フィールドに機能の説明を入力します。説明には任意の文字とスペースを使用できます。
8. 必要に応じてオプションを設定します。
9. [Save] をクリックします。

機能の編集

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. 目的の機能プロファイルをクリックします。
4. 機能の横にある […] をクリックし、[Edit Feature] を選択します。
5. 必要に応じてオプションを設定します。
6. [Save] をクリックします。

機能の削除

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. 目的の機能プロファイルをクリックします。
4. 機能の横にある […] をクリックし、[Delete Feature] を選択します。

機能設定

設定グループのワークフローは、機能プロファイルを生成します。さまざまな機能は、これらのプロファイルのいずれかの一部です。

システム プロファイル

AAA

認証、許可、およびアカウンティング（AAA）機能は、デバイスがCisco SD-WANルータにログインしているユーザーを認証し、ユーザーに与える権限を決定して、アクションのアカウンティングを実行するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、AAA機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。

フィールド	説明
[Feature Name]*	機能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。
Description	機能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。

Local

フィールド	説明
Enable AAA Authentication	認証パラメータを有効にします。
Accounting Group	アカウンティングパラメータを有効にします。
Add AAA User	
Name	ユーザの名前を入力します。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。 次のユーザー名は予約されているため、設定できません。backup、basic、bin、daemon、games、gnats、irc、list、lp、mail、man、news、nobody、proxy、quagga、root、sshd、sync、sys、uucp、および www-data。また、viptela-reserved で始まる名前は予約されています。
Password	ユーザーのパスワードを入力します。パスワードは MD5 ダイジェスト文字列で、タブ、復帰、改行などの任意の文字を含めることができます。詳細については、RFC 7950「The YANG 1.1 Data Modeling Language」のセクション 9.4 を参照してください。 各ユーザー名にはパスワードが必要です。ユーザーは自分のパスワードを変更できます。 管理ユーザーのデフォルトパスワードは admin です。このパスワードから変更することを強く推奨します。
Confirm Password	ユーザーのパスワードをもう一度入力します。

フィールド	説明
特権	特権レベル 1 または 15 から選択します。 • [Level 1]：ユーザー EXEC モード。読み取り専用です。アクセスできるコマンドは ping などに限定されています。 • [Level 15]：特権 EXEC モード。reload コマンドなど、すべてのコマンドにアクセスできます。また設定の変更も可能です。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです。
Add Public Key Chain	
Key String*	キーの認証文字列を入力します。
キー タイプ	[ssh-rsa] を選択します。

RADIUS

フィールド	説明
Add Radius Server	
Address*	RADIUS サーバーホストの IP アドレスを入力します。
Acct Port	802.1X および 802.11i アカウンティング情報を RADIUS サーバーに送信するために使用する UDP ポートを入力します。 範囲：0 ～ 65535。 デフォルト：1813。
Auth Port	RADIUS サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：1812
Retransmit	デバイスが RADIUS 要求をサーバーに再送信する回数を入力します。 デフォルト：5 秒
Timeout	デバイスが RADIUS 要求への応答を待機してから、要求を再送信する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key*	認証および暗号化のために Cisco IOS XE SD-WAN デバイスが RADIUS サーバーに渡すキーを入力します。

フィールド	説明
キー タイプ	キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、RADIUS サーバーで使用する AES 暗号化キーと一致させる必要があります。

TACACS サーバー

フィールド	説明
Add TACACS Server	
Address*	TACACS+ サーバーホストの IP アドレスを入力します。
Port	TACACS+ サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：49
Timeout	デバイスが TACACS+ 要求への応答を待機してから、要求を再送信する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key*	認証と暗号化のために Cisco IOS XE SD-WAN デバイスが TACACS+ サーバーに渡すキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、TACACS+ サーバーで使用する AES 暗号化キーと一致させる必要があります。

アカウンティング

フィールド	説明
Add Accounting Rule	
Rule Id*	アカウンティングルール ID を入力します。

フィールド	説明
Method*	アカウンティング方式リストを指定します。次のいずれかを選択します。 • [commands]：特定の特権レベルに関連付けられた特定の個々の EXEC コマンドに関するアカウンティング情報を提供します。 • [exec]：ネットワーク アクセス サーバーでユーザー名、日付、開始および終了時間などのユーザー EXEC ターミナルセッションに関するアカウンティングレコードを提供します。 • [network]：ネットワークに関連するあらゆるサービス要求にアカウンティングを実行します。 • [system]：ユーザーに関連付けられていないすべてのシステムレベルのイベント（リロードなど）に対してアカウンティングを実行します。 （注） システム アカウンティングを使用しており、システムのスタートアップ時にアカウンティング サーバが到達不能である場合、システムに約 2 分間アクセスできません。
レベル	特権レベル（1 または 15）を選択します。アカウンティングレコードは、この特権レベルのユーザーが入力したコマンドに対してのみ生成されます。
Start Stop	イベントの開始時にアカウンティング開始通知を送信し、イベントの終了時にレコード停止通知を送信する場合は、このオプションを有効にします。
Use Server-group*	以前に設定した TACACS グループを選択します。このアカウンティングルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

許可

フィールド	説明
Server Auth Order*	認証順序を選択します。これにより、SSH セッションまたはコンソールポートを介して Cisco IOS XE SD-WAN デバイスに対するユーザーアクセスを確認するときに認証方式が試行される順序を指示します。
Authorization Console	コンソールアクセスコマンドの認証を実行するには、このオプションを有効にします。
Authorization Config Commands	コンフィギュレーション コマンドの認証を実行するには、このオプションを有効にします。
Add Authorization Rule	
Rule Id*	認証ルール ID を入力します。

フィールド	説明
Method*	[Commands] を選択します。これにより、ユーザーが入力するコマンドが許可されます。
レベル	許可するコマンドの権限レベル（1 または 15）を選択します。この権限レベルを持つユーザーが入力したコマンドが許可されます。
If Authenticated	認証されたユーザーにのみ認証ルールパラメータを適用するには、このオプションを有効にします。このオプションを有効にしない場合、ルールはすべてのユーザーに適用されます。
Use Server-group*	以前に設定した TACACS グループを選択します。この認証ルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

BFD

Bidirectional Forwarding Detection（BFD）は、Cisco SD-WAN 高可用性ソリューションの一部としてリンク障害を検出するプロトコルです。この機能は、色、DSCP 値、ポーリング間隔、検出の乗数などのオプションを構成するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、BFD 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
Poll Interval(In Millisecond)	BFD がルータ上のすべてのデータプレーントンネルをポーリングして、パケットの遅延、損失、およびアプリケーション認識ルーティングで使用されるその他の統計を収集する頻度を指定します。 範囲：1 ～ 4,294,967,296（$2^{32}-1$）ミリ秒 デフォルト：600,000 ミリ秒（10 分）
Multiplier（乗数）	ポーリング間隔に掛ける値を指定して、アプリケーション認識ルーティングがデータプレーントンネル統計に作用して損失と遅延を把握し、損失と遅延時間が設定された SLA を満たさない場合に新しいトンネルを計算する頻度を設定します。 範囲：1 ～ 6 デフォルト：6
DSCP Values for BFD Packets(decimal)	Differentiated Services Code Point（DSCP）制御トラフィックで使用される BFD パケットの DSCP 値を指定します。 範囲：0 ～ 63 デフォルト：48

色

フィールド	説明
色の追加	
Color*	デバイス間を移動するデータトラフィックのトランスポートトンネルの色を選択します。色は、特定のWANトランスポートプロバイダーを識別します。 値：3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1 ～ private6、public-internet、red、silver デフォルト：default
Hello Interval (milliseconds)*	BFDがトランスポートトンネルでHelloパケットを送信する頻度を指定します。BFDはこれらのパケットを使用して、トンネル接続の活性を検出し、トンネルの障害を検出します。 範囲：100 ～ 300000 ミリ秒 デフォルト：1000 ミリ秒（1 秒）
Multiplier*	トンネルに障害が発生したと宣言するまでにBFDが待機するHelloパケット間隔の数を指定します。これらすべての間隔中に、BFDがトンネルでHelloパケットを受信しなかった場合、BFDはトンネルに障害が発生したことを宣言します。この間隔は、Helloパケット間隔時間の乗数です。 範囲：1 ～ 60 デフォルト：7
Path MTU Discovery*	トランスポートトンネルのパスMTUディスカバリを有効または無効にします。パスMTUディスカバリが有効になっている場合、トンネル接続のパスMTUは定期的に（約1分に1回）チェックされ、動的に更新されます。パスMTUディスカバリが無効になっている場合、予想されるトンネルMTUは1472バイトですが、有効なトンネルMTUは1468バイトです。 デフォルト：有効
Default DSCP value for BFD packets*	Differentiated Services Code Point（DSCP）制御トラフィックで使用されるBFDパケットのDSCP値を指定します。 範囲：0 ～ 63 デフォルト：48

バナー

バナー機能は、システムログインバナーの設定に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、バナー機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
ログイン	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。

フィールド	説明
MOTD	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。

基本

基本機能を使用すると、ネットワークデバイスの基本的なシステム全体の機能（タイムゾーン、GPS 位置情報、ルータのコンソール接続のボーレートなど）を設定できます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、基本機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。

フィールド	説明
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
タイム ゾーン（**Time Zone**）	デバイスで使用するタイムゾーンを選択します。
デバイス グループ（**Device Groups**）	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。
Location	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。
Description	デバイスに関する追加の説明情報を入力します。
Console Baud Rate(bps)	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）。 デフォルト：9600
[Overlay ID]	Cisco SD-WAN オーバーレイネットワーク内のデバイスのオーバーレイ ID を指定します。 範囲：0 ～ 4294967295（$2^{32} – 1$） デフォルト：1
Controller Group	ルータが属する Cisco vSmart コントローラ グループのリスト。
Max 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：1 ～ 100

GPS

フィールド	説明
GPS Latitude	デバイスの緯度を十進角の形式で入力します。
GPS Longitude	デバイスの経度を十進角の形式で入力します。

Advanced

フィールド	説明
Port Hopping	ポートホッピングを有効または無効にします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。 デフォルト：有効
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
On Demand Tunnel	任意の 2 つの Cisco SD-WAN スポークデバイス間の動的オンデマンドトンネルを有効にします。
On Demand Tunnel Idle Timeout(In Minute)	オンデマンドトンネルのアイドルタイムアウト時間を入力します。設定された時間が経過すると、スポークデバイス間のトンネルが削除されます。 範囲：1 ー 65535 分 デフォルト：10 分
Control Session PPS	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入力します。 範囲：1 ～ 65535 pps デフォルト：300 pps
Track Transport	このオプションを有効にして、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。 デフォルト：有効
Track Default Gateway	デフォルトゲートウェイのトラッキングを有効または無効にします。ゲートウェイトラッキングにより、静的ルートの場合、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

フィールド	説明
Track Interface Tag	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
Multi Tenant	デバイスをマルチテナントとして指定するには、このオプションを有効にします。
Admin Tech On Failure	デバイスの再起動時に管理技術情報を収集するには、このオプションを有効にします。 デフォルト：有効

グローバル

グローバル機能は、HTTP、HTTPS、Telnet、IP ドメインルックアップ、およびその他のいくつかのデバイス設定など、デバイス上のさまざまなサービスを有効または無効にするのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、グローバル機能を構成するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

サービス

フィールド	説明
[HTTP Server]	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。
FTP パッシブ	パッシブ FTP を有効または無効にします。
Domain Lookup	ドメインネームシステム（DNS）ルックアップを有効または無効にします。
ARP プロキシ	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。
Line Virtual Teletype (Configure Outbound Telnet)	アウトバウンド Telnet を有効または無効にします。
Cisco Discovery Protocol（CDP）	Cisco Discovery Protocol（CDP）を有効または無効にします。
リンク層検出プロトコル（LLDP）	リンク層検出プロトコル（LLDP）を有効または無効にします。
Specify interface for source address	すべてのHTTPSクライアント接続に送信元インターフェイスのアドレスを入力します。

NAT 64

フィールド	説明
[UDP Timeout]	UDP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：300 秒（5 分）
[TCP Timeout]	TCP の NAT64 変換タイムアウトを指定します。 範囲：1 ～ 536870（秒） デフォルト：3600 秒（1 時間）

認証

フィールド	説明
HTTP Authentication	HTTP認証モードを選択します。 許容値：Local、AAA デフォルト：Local

SSH Version

フィールド	説明
SSH Version	SSHバージョンを選択します。 デフォルト：無効

Other Settings

フィールド	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。

フィールド	説明
IP Source Routing	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。

ロギング

ロギング機能は、ローカルハードドライブまたはリモートホストへのロギングを構成するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、ロギング機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

ディスク

フィールド	説明
Enable Disc	このオプションを有効にすると、syslog メッセージをローカルハードディスク上のファイルに保存できるようになり、このオプションを無効にすると保存できなくなります。デフォルトでは、すべての Cisco IOS XE SD-WAN デバイス でローカルディスクファイルへのロギングが有効になっています。
Max File Size(In Megabytes)	syslog ファイルの最大サイズを入力します。syslog ファイルは、ファイルサイズに基づいて 1 時間ごとにローテーションされます。ファイルサイズが設定値を超えると、ファイルがローテーションされ、syslog プロセスに通知されます。 範囲：1 ～ 20 MB デフォルト：10 MB
Rotations	最も古いファイルを破棄するまでに作成できる syslog ファイルの数を入力します。 範囲：1 ～ 10 デフォルト：10

TLS プロファイル

フィールド	説明
Add TLS Profile	

フィールド	説明
TLS Profile Name*	TLS プロファイル名を入力します。
TLS バージョン	TLS バージョンを選択します。 • TLSv1.1 • TLSv1.2
Authentication Type*	サーバーを選択します。
暗号スイート リスト	TLSバージョンに基づいて、暗号スイート（暗号化アルゴリズム）のグループを選択します。 暗号スイートのリストを以下に示します。 • [aes-128-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_128_sha • [aes-256-cbc-sha]：暗号化タイプ tls_rsa_with_aes_cbc_256_sha • [dhe-aes-cbc-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [dhe-aes-gcm-sha2]：暗号化タイプ tls_dhe_rsa_with_aes_gcm_sha2（TLS1.2 以上） • [ecdhe-ecdsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_ecdsa_aes_gcm_sha2（TLS1.2 以上）SuiteB • [ecdhe-rsa-aes-cbc-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_cbc_sha2（TLS1.2 以上） • [ecdhe-rsa-aes-gcm-sha2]：暗号化タイプ tls_ecdhe_rsa_aes_gcm_sha2（TLS1.2 以上） • [rsa-aes-cbc-sha2]：暗号化タイプ tls_rsa_with_aes_cbc_sha2（TLS1.2 以上） • [rsa-aes-gcm-sha2]：暗号化タイプ tls_rsa_with_aes_gcm_sha2（TLS1.2 以上）

サーバ

フィールド	説明
サーバの追加（Add Server）	

フィールド	説明
Hostname/IPv4 Address*	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog 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。
VPN*	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、構成は無視されます。複数の syslog サーバーを構成する場合、ソースインターフェイスはそれらすべてで同じである必要があります。
Priority	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重要性を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable*	このオプションを有効にすると、TLS を介した syslog が許可されます。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Custom Profile]：TLS プロファイルを選択するには、このオプションを有効にします。このオプションを有効にすると、次のフィールドが表示されます。 [TLS Properties Profile]：IPv4 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。

フィールド	説明
IPv6 サーバーの追加	
Hostname/IPv6 Address*	syslog メッセージを保存するシステムの DNS 名、ホスト名、または IP アドレスを入力します。 別の syslog サーバーを追加するには、プラス記号（+）をクリックします。syslog 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。
VPN*	syslog サーバーが配置されている VPN の識別子、または syslog サーバーに到達できる VPN の識別子を入力します。 範囲：0 ～ 65530
Source Interface	発信システムログメッセージに使用する特定のインターフェイスを入力します。このインターフェイスは、syslog サーバーと同じ VPN 内にある必要があります。それ以外の場合、構成は無視されます。複数の syslog サーバーを構成する場合、ソースインターフェイスはそれらすべてで同じである必要があります。
Priority	保存する syslog メッセージの重大度を選択します。重大度は、メッセージを生成したイベントの重大度を示します。優先順位は次のいずれかです。 • [informational]：ルーチンの状態（デフォルト）（syslog 重大度 6 に対応） • [debugging]：問題のデバッグに役立つ追加のログを出力します。 • [notice]：正常だが重大な状態（syslog 重大度 5 に対応） • [warn]：軽微なエラー状態（syslog 重大度 4 に対応） • [error]：システムの利便性を完全に損なわないエラー状態（syslog 重大度 3 に対応） • [critical]：重大な状態（syslog 重大度 2 に対応） • [alert]：すぐにアクションを実行する必要があります（syslog の重大度 1 に対応） • [emergency]：システムは使用できません（syslog 重大度 0 に対応）
TLS Enable*	このオプションを有効にすると、TLS を介した syslog が許可されます。
TLS Properties Custom Profile*	TLS プロファイルを選択するには、このオプションを有効にします。
TLS Properties Profile	IPv6 サーバー構成でサーバーまたは相互認証用に作成した TLS プロファイルを選択します。

NTP

Network Time Protocol（NTP）は、サーバーとクライアントの分散ネットワークがネットワーク全体で時刻を同期できるようにするプロトコルです。NTP 機能は、Cisco SD-WAN ネットワーク上で NTP 設定を行うのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、NTP 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

サーバ

フィールド	説明
サーバの追加（Add Server）	
Hostname/IP address*	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。
VPN to reach NTP Server*	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。 範囲：0 ～ 65530
Set authentication key for the server	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。 キーを有効にするには、[Authentication] の [Trusted Key] フィールドでキーを「trusted」とマークする必要があります。
Set NTP version*	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：1 ～ 4 デフォルト：4
Set interface to use to reach NTP server	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 this NTP server*	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、このオプションを有効にします。別のストラタムレベルのサーバーについては、Cisco SD-WAN は最上位のストラタムレベルのサーバーを選択します。

認証

フィールド	説明
Add Authentication Keys	
Key Id*	MD5 認証キー ID を入力します。 範囲：1 ～ 65535
MD5 Value*	MD5 認証キーを入力します。クリアテキストキーまたは AES 暗号化キーを入力します。

フィールド	説明
信頼済みキー	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 [Set authentication key for the server] フィールドに入力したものと同じ値を入力します。

正規の NTP サーバー

フィールド	説明
Authoritative NTP Server	サポートされている1つまたは複数のルータをプライマリNTPルータとして設定する場合は、ドロップダウンリストから [Global] を選択し、このオプションを有効にします。 このオプションを有効にすると、次のフィールドが表示されます。 **Stratum**：プライマリ NTP 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。
送信元	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。

OMP

この機能は、オーバーレイ管理プロトコル（OMP）パラメータを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、OMP 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能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。
Description	機能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。

基本設定

フィールド	説明
Graceful Restart Enable	グレースフル リスタートを有効にします。デフォルトでは、OMP のグレースフルリスタートは有効になっています。

フィールド	説明
Paths Advertised Per Prefix	プレフィックスごとにアドバタイズする等コストルートの最大数を指定します。Cisco IOS XE SD-WAN デバイス がルートを Cisco vSmart コントローラ にアドバタイズし、コントローラが学習したルートを再配布し、各ルート TLOC タプルをアドバタイズします。Cisco IOS XE SD-WAN デバイスは最大4つの TLOC を持つことができ、デフォルトでは各ルート TLOC タプルを Cisco vSmart コントローラにアドバタイズします。ローカルサイトに Cisco IOS XE SD-WAN デバイスが 2 つある場合、Cisco vSmart コントローラは同じルートに対して 8 つのルート TLOC タプルを学習する可能性があります。設定された制限がルート TLOC タプルの数よりも小さい場合は、最適なルートがアドバタイズされます。 範囲：1 ～ 16 デフォルト：4
ECMP Limit	Cisco IOS XE SD-WAN デバイス のローカルルートテーブルにインストールできる Cisco vSmart コントローラ から受信する OMP パスの最大数を指定します。デフォルトでは、Cisco IOS XE SD-WAN デバイスはルートテーブルに最大 4 つの一意の OMP パスをインストールします。 範囲：1 ～ 16 デフォルト：4
Advertisement Interval(In Second)	OMP 更新パケット間の時間を設定します。 範囲：0 ー 65535 秒 デフォルト：1 秒
Hold Time(In Second)	ピアへの OMP 接続を閉じるまでの待機時間を指定します。ピアがホールド時間内に 3 回連続してキープアライブメッセージを受信しない場合、ピアへの OMP 接続は閉じられます。 範囲：0 ー 65535 秒 デフォルト：60 秒
EOR Timer(In Second)	OMP セッションがダウンしてから復帰し、End-of-RIB（EOR）マーカーを送信するまでの待機時間を指定します。このマーカーが送信された後、OMP セッションの復帰後に更新されなかったルートは、古いルートと見なされ、ルートテーブルから削除されます。 範囲：1 ー 3600 秒（1 時間） デフォルト：300 秒（5 分）
Overlay AS	OMP がルータの BGP ネイバーにアドバタイズする BGP AS 番号を指定します。

フィールド	説明
Shutdown	このオプションを有効にすると OMP を無効にし、Cisco SD-WAN オーバーレイネットワークを無効にします。OMPはデフォルトで有効になっています。
OMP Admin Distance Ipv4	OMP 経由でルートをアドバタイズするには、リークされたルート アドミニストレーティブ ディスタンスよりも低い IPv4 アドレスの OMP アドミニストレーティブ ディスタンスを設定します。 範囲：1 ～ 255
OMP Admin Distance Ipv6	OMP 経由でルートをアドバタイズするには、リークされたルート アドミニストレーティブ ディスタンスよりも低い IPv6 アドレスの OMP アドミニストレーティブ ディスタンスを設定します。 範囲：1 ～ 255

タイマー

フィールド	説明
Graceful Restart(In Second)	OMP 情報キャッシュをフラッシュして更新する頻度を指定します。タイマー値を0にすると、OMPグレースフルリスタートが無効になります。 範囲：0 ー 604800 秒（168 時間、7 日） デフォルト：43200 秒（12 時間）

Advertise

フィールド	説明
Advertise Ipv4 BGP	BGP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、BGP ルートは OMP にアドバタイズされません。
Advertise Ipv4 OSPF	外部OSPFルートをOMPにアドバタイズする場合は、このオプションを有効にします。デフォルトでは、外部 OSPF ルートは OMP にアドバタイズされません。
Advertise Ipv4 OSPF v3	外部 OSPFv3 ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、外部 OSPFv3 ルートは OMP にアドバタイズされません。
Advertise Ipv4 Connected	接続ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、接続ルートは OMP にアドバタイズされません。

フィールド	説明
Advertise Ipv4 Static	スタティックルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、スタティックルートは OMP にアドバタイズされません。
Advertise Ipv4 LISP	LISP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、LISP ルートは OMP にアドバタイズされません。
Advertise Ipv4 ISIS	IS-IS ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、IS-IS ルートは OMP にアドバタイズされません。
Advertise Ipv4 EIGRP	EIGRP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、EIGRP ルートは OMP にアドバタイズされません。
Advertise Ipv6 BGP	BGP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、BGP ルートは OMP にアドバタイズされません。
Advertise Ipv6 OSPF	外部 OSPF ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、外部 OSPF ルートは OMP にアドバタイズされません。
Advertise Ipv6 Connected	接続ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、接続ルートは OMP にアドバタイズされません。
Advertise Ipv6 Static	スタティックルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、スタティックルートは OMP にアドバタイズされません。
Advertise Ipv6 LISP	LISP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、LISP ルートは OMP にアドバタイズされません。
Advertise Ipv6 ISIS	IS-IS ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、IS-IS ルートは OMP にアドバタイズされません。
Advertise Ipv6 EIGRP	EIGRP ルートを OMP にアドバタイズする場合は、このオプションを有効にします。デフォルトでは、EIGRP ルートは OMP にアドバタイズされません。

SNMP

アプリケーション層の簡易ネットワーク管理プロトコル（SNMP）は、SNMPマネージャとエージェント間の対話用の通信標準規格を提供します。このプロトコルは、ネットワークデバイスのモニタリングや管理に共通して使用される標準化された言語を定義します。SNMP機能は、Cisco IOS XE SD-WAN デバイス で SNMP 機能を設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、SNMP 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能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。
Description	機能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。

SNMP

フィールド	説明
Shutdown	デフォルトでは、SNMP は有効になっています。
連絡先担当者	Cisco IOS XE SD-WAN デバイス を管理するネットワーク管理連絡先担当者の名前を入力します。これには、最大 255 文字を使用できます。
Location of Device	デバイスのロケーションの説明を入力します。これには、最大 255 文字を使用できます。

SNMP バージョン（SNMP Version）

フィールド	説明
SNMP バージョン（SNMP Version）	次の SNMP バージョンのいずれかを選択します。 • SNMP v2 • **SNMP v3**
SNMP v2: Add View	
名前*	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id*]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にして OID をビューから除外します。
SNMP v2: Add Community	
名前*	コミュニティ名を入力します。名前は 1 ～ 32 文字で、山括弧（< および >）を含めることができます。

フィールド	説明
User Label*	（最小リリース：Cisco vManage リリース 20.9.2）コミュニティ名のラベルまたは識別子を入力します。SNMP ターゲットに複数のコミュニティ名がある場合に、コミュニティ名を区別または更新するのに役立ちます。
View*	コミュニティに適用するビューを選択します。ビューは、コミュニティがアクセスできる MIB ツリーの部分を指定します。
Authorization*	ドロップダウンリストから、[read-only] を選択します。Cisco SD-WAN でサポートされる MIB では書き込み操作が許可されないため、読み取り専用の許可のみを設定できます。
SNMP v2: Add Target	
VPN ID*	トラップサーバーに到達するために使用する VPN の番号を入力します。 範囲：0 ～ 65530
IPv4/IPv6 address of SNMP server*	SNMP サーバーの IP アドレスを入力します。
UDP port number to connect to SNMP server*	SNMP サーバーに接続するための UDP ポート番号を入力します。 範囲：1 ～ 65535
Community Name*	[Add Community] で構成されたコミュニティの名前を選択します。 このフィールドは、Cisco vManage リリース 20.9.1 以前のリリースにのみ適用されます。
User Label*	（最小リリース：Cisco vManage リリース 20.9.2）[Add Community] で構成されたユーザーラベルを選択します。
Source interface for outgoing SNMP trap*	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。
SNMP v3: Add View	
名前*	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。

フィールド	説明
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id*]：オブジェクトのOIDを入力します。たとえば、SNMP MIBのインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にしてOIDをビューから除外します。
SNMP v3: Add Group	
名前*	トラップグループの名前を入力します。1～32文字を使用できます。
Security Level*	グループに使用する認証を選択します。 • [no-auth-no-priv]：ユーザー名に基づいて認証します。この認証を構成する場合、認証またはプライバシー資格情報を構成する必要はありません。 [auth-no-priv]：選択した認証アルゴリズムを使用して認証します。この認証を構成する場合、このグループのユーザーに認証と認証パスワードを構成する必要があります。 [auth-priv]：選択した認証アルゴリズムを使用して認証します。この認証を構成する場合、このグループのユーザーに、認証と認証パスワード、およびプライバシーとプライバシーのパスワードを構成する必要があります。
View*	トラップグループがアクセスできる SNMP ビューを選択します。
SNMP v3: Add User	
名前*	SNMP ユーザーの名前を入力します。1 ～ 32 文字の英数字を使用できます。
Authentication Protocol	ユーザーの認証メカニズムを選択します。 • **md5** • **sha**
Authentication Password	認証パスワードをクリアテキストまたはAES暗号化キーとして入力します。

フィールド	説明
Privacy Protocol	ユーザーのプライバシータイプを選択します。 • [aes-cfb-128]：128 ビットキーで、暗号フィードバックモードで使用される Advanced Encryption Standard 暗号アルゴリズムを使用します。これは SHA-1 認証プロトコルです。 • [aes-256-cfb-128]：256 ビットキーで、暗号フィードバックモードで使用される Advanced Encryption Standard 暗号アルゴリズムを使用します。これは SHA-256 認証プロトコルです。
プライバシー パスワード（**Privacy Password**）	プライバシーパスワードをクリアテキストまたは AES 暗号化キーのいずれかで入力します。
Group*	SNMPv3 グループの名前を選択します。
SNMP v3: Add Target	
VPN ID*	トラップサーバーに到達するために使用する VPN の番号を入力します。 範囲：0 ～ 65530
IPv4/IPv6 address of SNMP server*	SNMP サーバーの IP アドレスを入力します。
UDP port number to connect to SNMP server*	SNMP サーバーに接続するための UDP ポート番号を入力します。 範囲：1 ～ 65535
User*	[Add User] で構成されたユーザーの名前を選択します。
Source interface for outgoing SNMP trap*	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

トランスポートおよび管理のプロファイル

トランスポート **VPN**

トランスポート VPN 機能は、VPN 0 または WAN VPN を設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、トランスポート VPN 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
VPN	VPN の数値識別子を入力します。
Enhance ECMP Keying	ECMP ハッシュキーとして、送信元 IP アドレス、宛先 IP アドレス、プロトコル、および DSCP フィールドの組み合わせの使用に加えて、レイヤ 4 の送信元ポートと宛先ポートの ECMP ハッシュキーでの使用を有効にします。 デフォルト：無効

DNS

フィールド	説明
Add DNS	
Primary DNS Address (IPv4)	この VPN のプライマリ IPv4 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv4)	この VPN のセカンダリ IPv4 DNS サーバーの IP アドレスを入力します。
Add DNS IPv6	
Primary DNS Address (IPv6)	この VPN のプライマリ IPv6 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv6)	この VPN のセカンダリ IPv6 DNS サーバーの IP アドレスを入力します。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname*	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
List of IP*	ホスト名に関連付ける IP アドレスを 8 つまで入力します。エントリをカンマで区切ります。

Route

フィールド	説明
IPv4スタティックルートの追加	
Network address*	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で設定する IPv4 スタティックルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。

フィールド	説明
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルートの追加	
Prefix*	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で設定する IPv6 スタティックルートのプレフィックス長を入力します。

フィールド	説明
Next Hop/Null 0/NAT	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv6 アドレスを入力します。 [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 Route Null 0]*：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [NAT]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 NAT]*：NAT64 または NAT66 を選択します。
Add BGP Routing	BGP ルートを選択します。

NAT

フィールド	説明
Add NAT64 v4 Pool	
NAT64 v4 Pool Name*	一元化されたデータポリシーで構成されている NAT プール番号を入力します。NAT プール名は、VPN および VRF 全体で一意である必要があります。ルータごとに最大 31（1 ～ 32）の NAT プールを設定できます。
NAT64 Pool Range Start*	NAT プールの開始 IP アドレスを入力します。
NAT64 Pool Range End*	NAT プールの終了 IP アドレスを入力します。
NAT64 Overload	ポートごとの変換を構成するには、このオプションを有効にします。このオプションを無効にすると、ダイナミック NAT のみがエンドデバイスに設定されます。ポートごとの NAT は設定されていません。 デフォルト：無効

Service

フィールド	説明
サービスの追加	
サービス タイプ	VPN で利用可能なサービスを選択します。 値：**TE**

イーサネット インターフェイス

この機能は、VPN 0 または WAN VPN でイーサネット インターフェイスを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、イーサネットインターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Associated VPN	VPN を選択します。
関連トラッカー	トラッカーを選択してください。

基本設定

フィールド	説明
Shutdown	インターフェイスを有効または無効にします。
[Interface Name]*	インターフェイスの名前を入力します。インターフェイス名を完全にスペルアウトします (たとえば、GigabitEthernet0/0/0)。 使用していない場合でも、ルータのすべてのインターフェイスを構成して、それらがシャットダウン状態で構成され、それらのすべてのデフォルト値が構成されるようにします。
Description	インターフェイスの説明を入力します。
Auto Detect Bandwidth	WAN インターフェイスの帯域幅を自動的に検出するには、このオプションを有効にします。デバイスは、iPerf3 サーバーに接続して速度テストを実行することにより、帯域幅を検出します。
IPv4 設定	IPv4 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。
Dynamic DHCP Distance	DHCP サーバーから学習したルートのアドミニストレーティブディスタンス値を入力します。このオプションは、[Dynamic] を選択した場合に使用できます。 デフォルト：1
IP Address	静的 IPv4 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。

フィールド	説明
[Subnet Mask]	サブネット マスクを入力します。
Configure Secondary IP Address	サービス側インターフェイスのセカンダリ IPv4 アドレスを最大 4 つ入力します。 • [IP Address]：IP アドレスを入力します。 • [Subnet Mask]：サブネットマスクを入力します。
DHCP Helper	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
IPv6 設定	IPv6 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。 • **None**
IPv6 Address Primary	静的 IPv6 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。
セカンダリ IPv6 を追加	
IP Address	サービス側インターフェイスのセカンダリ IPv6 アドレスを 2 つまで入力します。

トンネル

フィールド	説明
トンネルインターフェイス	トンネル インターフェイスを作成するには、このオプションを有効にします。
Per-tunnel QoS	個々のトンネルに Quality of Service（QoS）ポリシーを適用するには、このオプションを有効にします。
色	TLOC の色を選択します。

フィールド	説明
制限（Restrict）	ローカル TLOC が BFD セッションを確立できるリモート TLOC を制限するには、このオプションを有効にします。TLOC が制限付きとしてマークされている場合、ローカルルータの TLOC は、リモート TLOC が同じカラーである場合にのみ、リモート TLOC とのトンネル接続を確立します。
グループ	グループ番号を入力します。 範囲： 1 ～ 4294967295
Border	TLOC をボーダー TLOC として設定するには、このオプションを有効にします。
Maximum Control Connections	WAN トンネル インターフェイスが接続できる の最大数を指定します。Cisco vSmart コントローラトンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 100 デフォルト：2
vBond As Stun Server	Cisco IOS XE SD-WAN デバイス が NAT の背後にある場合に、トンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにするには、Session Traversal Utilities for NAT（STUN）を有効にします。
コントローラグループリストの除外	このトンネルが接続を許可されない 1 つ以上のグループの ID を設定します。Cisco vSmart コントローラ 範囲：0 ～ 100
vManage 接続設定	トンネルインターフェイスを使用して Cisco vManage と制御トラフィックを交換するための優先順位を設定します。 範囲：0 ～ 8 デフォルト：5
ポートホップ	Enable port hopping. ポートホッピングがグローバルに有効になっている場合は、個々の TLOC（トンネルインターフェイス）で無効にできます。 デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付けるには、このオプションを有効にします。

フィールド	説明
Tunnel TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネルMTUに基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし
Clear-Dont-Fragment	インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment（DF）ビットをクリアするには、このオプションを有効にします。DF ビットがクリアされると、インターフェイスのMTUより大きいパケットは送信前にフラグメント化されます。
CTS SGT Propagation	インターフェイスでの CTS SGT 伝達を有効にします。
Network Broadcast	このオプションを有効にして、ネットワークプレフィックス指向ブロードキャストを受け入れて応答します。
Allow Service	インターフェイスで次のサービスを許可または禁止します。 • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
カプセル化	

フィールド	説明
カプセル化*	カプセル化タイプを選択します。 • [gre]：トンネルインターフェイスで GRE カプセル化を使用します。 • [ipsec]：トンネルインターフェイスで IPsec カプセル化を使用します。 （注） IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。 [gre] を選択すると、次のフィールドが表示されます。 • [GRE Preference]：トラフィックをトンネルに送信するための優先値を入力します。高い値が低い値に優先します。 範囲：0 ～ 4294967295 デフォルト：0 • [GRE Weight]：複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255 デフォルト：1 [ipsec] を選択すると、次のフィールドが表示されます。 • [IPSEC Preference]：トラフィックをトンネルに送信するための優先値を入力します。高い値が低い値に優先します。 範囲：0 ～ 4294967295 デフォルト：0 • [IPSEC Weight]：複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255 デフォルト：1

NAT

フィールド	説明
IPv4 設定	
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
NAT Type	IPv4 の NAT 変換タイプを選択します。 • **interface** • **プール** • **loopback** デフォルト：[interface]。NAT64 でサポートされています。
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）
Configure New Static NAT	静的 NAT マッピングを追加します。
Source IP	変換される送信元アドレスを入力します。
Translate IP	変換された送信元 IP アドレスを入力します。
Direction	ネットワークアドレス変換を行う方向を選択します。 • [inside]：デバイスのサービス側から送信され、ルータのトランスポート側に向かうパケットの IP アドレスを変換します。 • [Outside]：トランスポート側デバイスからデバイスに到着し、サービス側デバイス宛てのパケットの IP アドレスを変換します。
Source VPN	送信元 VPN ID を入力します。
IPv6 設定	

フィールド	説明
IPv6 NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
Select NAT	NAT64 または NAT66 を選択します。NAT66 を選択すると、次のフィールドが表示されます。 • [Source Prefix]：送信元 IPv6 プレフィックスを入力します。 • [Translated Source Prefix]：変換された送信元プレフィックスを入力します。 • [Source VPN ID]：送信元 VPN ID を入力します。

ARP

フィールド	説明
IP Address	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
[MAC Address]	MAC アドレスをコロン区切りの 16 進表記で入力します。

Advanced

フィールド	説明
デュプレックス	インターフェイスが全二重または半二重のどちらのモードで実行されるかを指定します。 デフォルト：full
[MAC Address]	インターフェイスに関連付ける MAC アドレスを、コロン区切りの 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 9216 デフォルト：1500 バイト
インターフェイス **MTU**	インターフェイスで送受信されるフレームの最大伝送単位サイズを入力します。 範囲：1500 ～ 1518（GigabitEthernet0）、1500 ～ 9216（他の GigabitEthernet） デフォルト：1500 バイト

フィールド	説明
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネルMTUに基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし
速度	接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。 値：10、100、1000、2500、または 10000 Mbps
ARP Timeout	ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2147483 秒 デフォルト：1200 秒
自動ネゴシエーション	自動ネゴシエーションをオンにするには、このオプションを有効にします。
メディア タイプ	インターフェイスの物理メディア接続タイプを指定します。次のいずれかを選択します。 • [auto-select]：接続は自動的に選択されます。 • [rj45]：RJ-45 の物理接続を指定します。 • [sfp]：光ファイバメディアの Small Form Factor Pluggable（SFP）物理接続を指定します。
TLOC Extension	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。 （注） L3 を介した TLOC 拡張は、Cisco IOS XE SD-WAN デバイスでのみサポートされています。Cisco IOS XE SD-WAN デバイスに L3 を介した TLOC 拡張を設定する場合は、L3 インターフェイスの IP アドレスを入力します。

フィールド	説明
GRE tunnel source IP	拡張 WAN インターフェイスの IPv4 アドレスを入力します。
XConnect	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。
Load Interval	インターフェイス負荷計算の間隔値を入力します。
IP Directed Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。
ICMP Redirect Disable	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。

管理 VPN

この機能は、VPN 512 または管理 VPN の構成に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、管理 VPN 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
VPN	オーバーレイネットワーク内の Cisco IOS XE 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 IOS XE SD-WAN デバイス で有効になっています。

フィールド	説明
Name	インターフェイスの名前を入力します。

DNS

フィールド	説明
Add DNS	
Primary DNS Address (IPv4)	この VPN のプライマリ DNS サーバーの IPv4 アドレスを入力します。
Secondary DNS Address (IPv4)	この VPN のセカンダリ DNS サーバーの IPv4 アドレスを入力します。
DNS IPv6 を追加	
Primary DNS Address (IPv6)	この VPN のプライマリ DNS サーバーの IPv6 アドレスを入力します。
Secondary DNS Address (IPv6)	この VPN のセカンダリ DNS サーバーの IPv6 アドレスを入力します。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname*	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
List of IP Address*	ホスト名に関連付ける IP アドレスを入力します。エントリをカンマで区切ります。

IPv4/IPv6 スタティックルート

フィールド	説明
IPv4スタティックルートの追加	
IP Address*	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で構成する IPv4 スタティック ルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。

フィールド	説明
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。
IPv6 スタティックルートの追加	
Prefix*	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で構成する IPv6 スタティック ルートのプレフィックス長を入力します。

フィールド	説明
ネクストホップ/ヌル 0/NAT	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv6 アドレスを入力します。 [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [NULL0*]：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [NAT]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 NAT]：NAT64 または NAT66 を選択します。

管理イーサネット インターフェイス

この機能は、VPN 512 または管理 VPN でイーサネット インターフェイスを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、管理イーサネットインターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Associated VPN	管理 VPN または VPN 512。

基本設定

フィールド	説明
Shutdown	インターフェイスを有効または無効にします。
Interface Name	インターフェイスの名前を入力します。インターフェイス名を完全にスペルアウトします（例：GigabitEthernet1）。

フィールド	説明
Description	インターフェイスの説明を入力します。
IPv4 設定	IPv4 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。
Dynamic DHCP Distance	DHCP サーバーから学習したルートのアドミニストレーティブディスタンス値を入力します。このオプションは、[Dynamic] を選択した場合に使用できます。 デフォルト：1
DHCP Helper	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
Iperf server for auto bandwidth detect	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。
Auto Detect Bandwidth	このオプションを有効にして、デバイスが帯域幅を検出できるようにします。
IPv6 設定	IPv6 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。 • **None**
IPv6 Address Primary	静的 IPv6 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。

NAT

フィールド	説明
IPv4 設定	
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
NAT Type	IPv4 の NAT 変換タイプを選択します。 • **interface** • **プール** • **loopback** デフォルト：interface
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）
Configure New Static NAT	静的 NAT マッピングを追加します。
Source IP	変換される送信元アドレスを入力します。
Translate IP	変換された送信元 IP アドレスを入力します。
Direction	ネットワークアドレス変換を行う方向を選択します。 • [inside]：デバイスのサービス側から送信され、ルータのトランスポート側に向かうパケットの IP アドレスを変換します。 • [Outside]：トランスポート側デバイスからデバイスに到着し、サービス側デバイス宛てのパケットの IP アドレスを変換します。
Source VPN	送信元 VPN ID を入力します。
IPv6 設定	

フィールド	説明
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
Select NAT	NAT64 または NAT66 を選択します。NAT66 を選択すると、次のフィールドが表示されます。 • [Source Prefix]：送信元 IPv6 プレフィックスを入力します。 • [Translated Source Prefix]：変換された送信元プレフィックスを入力します。 • [Source VPN ID]：送信元 VPN ID を入力します。

ARP

フィールド	説明
IP Address	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
[MAC Address]	MAC アドレスをコロン区切りの 16 進表記で入力します。

Advanced

フィールド	説明
デュプレックス	インターフェイスが全二重または半二重のどちらのモードで実行されるかを指定します。
[MAC Address]	インターフェイスに関連付ける MAC アドレスを、コロン区切りの 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 9216 デフォルト：1500 バイト
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし

フィールド	説明
速度	接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。 値：10、100、1000、2500、または 10000 Mbps
ARP Timeout	ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2147483 秒 デフォルト：1200 秒
自動ネゴシエーション	自動ネゴシエーションをオンにするには、このオプションを有効にします。
メディア タイプ	インターフェイスの物理メディア接続タイプを指定します。次のいずれかを選択します。 • [auto-select]：接続は自動的に選択されます。 • [rj45]：RJ-45 の物理接続を指定します。 • [sfp]：光ファイバメディアの Small Form Factor Pluggable（SFP）物理接続を指定します。
XConnect	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。
Load Interval	インターフェイス負荷計算の間隔値を入力します。
ICMP/ICMPv6 Redirect Disable	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。

フィールド	説明
IP Directed Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。

セルラーコントローラ

この機能は、VPN 0 または WAN VPN でセルラーコントローラを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、セルラーコントローラ機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能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。
Description	機能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。
Cellular ID	セルラー NIM カードが取り付けられているインターフェイススロットとポート番号を入力します。現在、0/1/0 または 0/2/0 にすることができます。
Primary SIM slot	プライマリ SIM スロットの番号を入力します。0 または 1 にすることができます。もう一方のスロットは自動的にセカンダリに設定されます。SIM スロットが 1 つしかない場合、このパラメータは適用されません。

フィールド	説明
SIM Failover Retries	プライマリ SIM のサービスが利用できなくなった場合に、セカンダリ SIM への接続を再試行する最大回数を指定します。SIM スロットが 1 つしかない場合、このパラメータは適用されません。 範囲：0 ～ 65535 デフォルト：10
SIM Failover Timeout	プライマリ SIM のサービスが利用できなくなった場合に、プライマリ SIM からセカンダリ SIM に切り替えるまでの待機時間を指定します。SIM スロットが 1 つしかない場合、このパラメータは適用されません。 範囲：3 ～ 7 分 デフォルト：3 分
Firmware Auto Sim	デフォルトで、このオプションは有効になっています。AutoSIM は、アクティブな SIM カードを分析し、その SIM に関連付けられているサービス プロバイダー ネットワークを特定します。その分析に基づいて、AutoSIM は適切なファームウェアを自動的にロードします。

上記のパラメータを設定したら、セルラーコントローラに関連付けるセルラープロファイルを選択し、[Save] をクリックします。

セルラープロファイル

この機能は、VPN 0 または WAN VPN でセルラープロファイルを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、セルラープロファイル機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能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。
Description	機能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。
プロファイル ID	ルータで使用するプロファイルの識別番号を入力します。 範囲：1 ～ 15
アクセス ポイント名	サービス プロバイダー ネットワークとパブリックインターネット間のゲートウェイの名前を入力します。最大 32 文字を使用できます。
Authentication	セルラーネットワークへの接続に使用する認証方式を選択します。**none**、**pap**、**chap**、または **pap_chap** のいずれかに設定できます。

フィールド	説明
Profile Username	Web サービスのセルラー接続時に使用するユーザー名を入力します。1 ～ 32 文字の ID を使用できます。パスワードには、すべての英数字（スペースを含む）を使用できます。
プロファイル パスワード（**Profile Password**）	Web サービスのセルラー接続時に使用するユーザーパスワードを入力します。パスワードは大文字と小文字が区別され、クリアテキストまたは AES 暗号化キーを使用できます。
Packet Data Network Type	携帯電話ネットワークのパケットデータネットワーク（PDN）タイプを選択します。IPv4、IPv6、または IPv4v6 のいずれかに設定できます。
No Overwrite	セルラーモデムのプロファイルを上書きするには、このオプションを有効にします。デフォルトでは、このオプションは無効になっています。

トラッカー

この機能は、VPN インターフェイスのトラッカーを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、トラッカー機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Tracker 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。
Endpoint Tracker Type*	エンドポイントトラッカーを設定するトラッカータイプを選択します。 • **interface** • **static-route**
Endpoint	エンドポイントタイプを選択します。 • [Endpoint DNS Name]：このオプションを選択すると、次のフィールドが表示されます。 [Endpoint DNS Name]：エンドポイントの DNS 名。これは、エンドポイントのステータスを判断するためにプローブが送信されるインターネット上の宛先です。DNS 名には、最小 1 文字、最大 253 文字を含めることができます。 • [Endpoint IP]：このオプションを選択すると、次のフィールドが表示されます。 [Endpoint IP]：エンドポイントの IP アドレス。これは、エンドポイントのステータスを判断するためにプローブが送信されるインターネット上の宛先です。
インターバル（**Interval**）	構成されたエンドポイントのステータスを判断するためのプローブ間の時間間隔。 範囲：20 ー 600 秒 デフォルト：60 秒（1 秒）

フィールド	説明
Multiplier（乗数）	エンドポイントがダウンしていることを宣言する前にプローブを送信できる回数。 範囲：1 ～ 10 デフォルト：3
しきい値	構成されたエンドポイントがダウンしていることを宣言する前に、プローブが応答を返すまでの待機時間。 範囲： 100 ー 1000 ミリ秒 デフォルト： 300 ミリ秒
Tracker Type*	トラッカータイプを選択します。

セルラー インターフェイス

この機能は、VPN 0 または WAN VPN でセルラーインターフェイスを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、セルラーインターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Associated VPN	VPN 0 または WAN トランスポート VPN。
Associated Tracker	トラッカーを選択してください。

基本設定

フィールド	説明
Shutdown*	インターフェイスを有効または無効にします。
Interface Name*	インターフェイスの名前を入力します。
Description*	セルラーインターフェイスの説明を入力します。
DHCP Helper	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 4 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。

トンネル

フィールド	説明
トンネルインターフェイス	トンネル インターフェイスを作成するには、このオプションを有効にします。

フィールド	説明
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク ID を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default デフォルト：default
色	TLOC の色を選択します。
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。 範囲：100 ～ 600000 ミリ秒 デフォルト：1000 ミリ秒（1 秒）
Hello Tolerance	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 6000 秒 デフォルト：12 秒
Last-Resort Circuit	このオプションを有効にすると、トンネルインターフェイスを最終手段の回線として使用します。
制限（Restrict）	ローカル TLOC が BFD セッションを確立できるリモート TLOC を制限するには、このオプションを有効にします。TLOC が制限付きとしてマークされている場合、ローカルルータの TLOC は、リモート TLOC が同じカラーである場合にのみ、リモート TLOC とのトンネル接続を確立します。
グループ	Enter a group number. 範囲： 1 ～ 4294967295
Border	TLOC をボーダー TLOC として設定するには、このオプションを有効にします。
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラ の最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 100 デフォルト：2

フィールド	説明
NAT Refresh Interval	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。 範囲：1 ～ 60 秒 デフォルト：5 秒
vBond As Stun Server	Cisco IOS XE SD-WAN デバイス が NAT の背後にある場合に、トンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにするには、Session Traversal Utilities for NAT（STUN）を有効にします。
コントローラグループリストの除外	このトンネルが接続を許可されない 1 つ以上のグループの ID を設定します。Cisco vSmart コントローラ 範囲：1 ～ 100
vManage 接続設定	トンネルインターフェイスを使用して Cisco vManage と制御トラフィックを交換するための優先順位を設定します。 範囲：0 ～ 8 デフォルト：5
ポートホップ	Enable port hopping. ルータが 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ルータとの 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。 デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付けるには、このオプションを有効にします。
Tunnel TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし

フィールド	説明
Clear-Dont-Fragment	インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment（DF）ビットをクリアするには、このオプションを有効にします。DF ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
Network Broadcast	このオプションを有効にして、ネットワークプレフィックス指向ブロードキャストを受け入れて応答します。
Allow Service	インターフェイスで次のサービスを許可または禁止します。 • All • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
カプセル化	
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
GRE Preference	トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295 デフォルト：0

フィールド	説明
GRE Weight	複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255 デフォルト：1
IPSec	トンネルインターフェイスでIPsecカプセル化を使用します。デフォルトでは、IPsec は有効になっています。 IPsecカプセル化とGREカプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295 デフォルト：0
IPsec Weight	複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255 デフォルト：1

NAT

フィールド	説明
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
UDP Timeout*	UDPセッションを介したNAT変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：1 分
TCP Timeout*	TCPセッションを介したNAT変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）

ARP

フィールド	説明
IP Address*	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
[MAC アドレス（MAC Address）]*	MAC アドレスをコロン区切りの 16 進表記で入力します。

Advanced

フィールド	説明
[MAC Address]	インターフェイスに関連付ける MAC アドレスを、コロンで区切った 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 9216 デフォルト：1500 バイト
インターフェイス MTU	インターフェイスで送受信されるフレームの最大伝送単位サイズを入力します。 範囲：1500 ～ 9216 デフォルト：1500 バイト
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし

フィールド	説明
TLOC Extension	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。 （注） L3 を介した TLOC 拡張は、Cisco IOS XE SD-WAN デバイスでのみサポートされています。Cisco IOS XE SD-WAN デバイスに L3 を介した TLOC 拡張を設定する場合は、L3 インターフェイスの IP アドレスを入力します。
Tracker	インターフェイスステータスのトラッキングは、VPN 0 のトランスポート インターフェイスで NAT を有効にして、最初にデータセンターのルータにアクセスするのではなく、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出られるようにする場合に役立ちます。この状況では、トランスポート インターフェイスで NAT を有効にすると、ローカルルータとデータセンター間の TLOC が 2 つに分割され、1 つはリモートルータに、もう 1 つはインターネットに送られます。 トランスポート トンネル トラッキングを有効にすると、Cisco SD-WAN はインターネットへのパスを定期的に調べて、インターネットが稼働しているかどうかを判断します。このパスがダウンしていることを Cisco SD-WAN が検出すると、インターネットの宛先へのルートが撤回され、インターネットに向かうトラフィックはデータセンターのルータを介してルーティングされます。インターネットへのパスが再び機能していることを Cisco SD-WAN が検出すると、インターネットへのルートが再インストールされます。 インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

フィールド	説明
IP Directed-Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。

BGP ルーティング

この機能は、VPN 0 または WAN VPN でボーダー ゲートウェイ プロトコル（BGP）ルーティングを構成するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表は、BGP ルーティング機能を構成するためのオプションについて説明しています。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
AS Number	ローカル AS 番号を入力します。
Router ID	10 進数の 4 つの部分からなるドット付き表記で BGP ルータ ID を入力します。
Propagate AS Path	このオプションを有効にすると、BGP AS パス情報が OMP に伝達されます。

フィールド	説明
Propagate Community	このオプションを有効にすると、OMP 再配布を使用して VPN 全体で、Cisco SD-WAN サイト間で BGP コミュニティが伝播されます。
External Routes Distance	オーバーレイネットワーク内の他のサイトから学習したルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。 範囲：1 ～ 255 デフォルト：20
Internal Routes Distance	ある AS から別の AS に到達するルートの BGP ルート アドミニストレーティブ ディスタンスとして適用する値を入力します。 範囲：1 ～ 255 デフォルト：200
[Local Routes Distance]	ローカル AS 内のルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。デフォルトでは、BGP からローカルに受信したルートが OMP から受信したルートよりも優先されます。 範囲：1 ～ 255 デフォルト：20

ユニキャスト アドレス ファミリ

フィールド	説明
IPv4 設定	
Maximum Paths	内部 BGP マルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティングテーブルに存在するかどうかに関係なく、デフォルトルートが人為的に生成され、BGP ルート情報ベース（RIB）に挿入されます。新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	

フィールド	説明
Protocol*	すべてのBGPセッションに対して、ルートをBGPに再配布するプロトコルを選択します。オプションは、[static]、[connected]、[ospf]、[omp]、[eigrp]、および [nat] です。 少なくとも、[connected] を選択し、[Route Policy] で、BGPがループバック インターフェイス アドレスをネイバーにアドバタイズするルートポリシーを指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Network	
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。ネットワークプレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および 255.255.255.0 と入力します。
Aggregate Address	
Aggregate Prefix*	すべてのBGPセッションに対して集約するアドレスのプレフィックスを入力します。集約プレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および255.255.255.0 と入力します。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	
Policy Name	ルートのダウンロードを制御するルートマップを入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。

フィールド	説明
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIB にインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
IPv6 設定	
Maximum Paths	内部 BGP マルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティングテーブルに存在するかどうかに関係なく、デフォルトルートが人為的に生成され、BGP ルート情報ベース（RIB）に挿入されます。新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	
Protocol*	すべての BGP セッションに対して、ルートを BGP に再配布するプロトコルを選択します。オプションは、[static]、[connected]、[ospf]、[omp]、および [eigrp] です。 少なくとも、[connected] を選択し、[Route Policy] で、BGP がループバック インターフェイス アドレスをネイバーにアドバタイズするルートポリシーを指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Network	

フィールド	説明
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。IPv6 ネットワークプレフィックスは、IPv6 アドレスとプレフィックス長（1 ～ 128）で構成されます。たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
Aggregate Address	
Aggregate Prefix*	すべての BGP セッションに対して集約するアドレスのプレフィックスを入力します。IPv6 集約プレフィックスは、IPv6 アドレスとプレフィックス長（1 ～ 128）で構成されます。たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	
Policy Name	ルートのダウンロードを制御するルートマップを入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIB にインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。

MPLS インターフェイス

フィールド	説明
Interface Name*	MPLS インターフェイスの名前を入力します。

ネイバー

フィールド	説明
IPv4 設定	
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。
Allows in Number	プロバイダーエッジ（PE）デバイスの自律システム番号（ASN）のアドバタイズを許可する回数を入力します。指定できる範囲は 1 ～ 10 です。数値が指定されていない場合は、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。

フィールド	説明
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
Send Label	このオプションを有効にすると、ルータが相互にアドバタイズできるようになり、ルートとともに MPLS ラベルを送信できるようになります。ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。
ネイバーアドレスファミリの追加	
Family Type*	BGP IPv4 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Out Route Policy	ネイバーに送信するプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • [Policy Off]：ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • [Threshold (percentage)]：しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが過剰なピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰なプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。
IPv6 設定	
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。

フィールド	説明
Allowas in Number	プロバイダーエッジ（PE）デバイスの自律システム番号（ASN）のアドバタイズを許可する回数を入力します。指定できる範囲は 1 ～ 10 です。数値が指定されていない場合は、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）

フィールド	説明
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
IPv6 ネイバーアドレスファミリの追加	
Family Type*	BGP IPv6 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Out Route Policy	ネイバーに送信するプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • [Policy Off]：ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • [Threshold (percentage)]：しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが過剰なピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰なプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。

Advanced

フィールド	説明
Keepalive (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。このキープアライブ時間は、グローバルキープアライブ時間です。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）

フィールド	説明
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。このホールド時間は、グローバルホールド時間です。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
[Compare MED]	このオプションを有効にすると、BGP パス間でルータ ID を比較してアクティブパスを決定します。
[Deterministic MED]	このオプションを有効にすると、ルートがいつ受信されたかに関係なく、同じ AS から受信されたすべてのルートの MED が比較されます。
[Missing MED as Worst]	このオプションを有効にすると、パスに MED 属性がない場合にパスが最悪のパスと見なされます。
[Compare Router ID]	このオプションを有効にすると、比較されるルートのピア AS が同じであるかどうかにかかわらず、常に MED が比較されます。
[Multipath Relax]	このオプションを有効にすると、BGP ベストパスプロセスが異なる AS のルートから選択されます。デフォルトでは、BGP マルチパスを使用している場合、BGP ベストパスプロセスは同じ AS 内のルートから選択し、複数のパス間でロードバランシングを行います。

サービス プロファイル

サービス VPN

この機能は、サービス VPN（512 を除く 1 ～ 65527 の範囲）または LAN VPN の構成に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、サービス VPN 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
Feature Name*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
VPN*	VPN の数値識別子を入力します。
名前*	VPN の名前を入力します。
OMP Admin Distance IPv4	OMP ルートのアドミニストレーティブ ディスタンス。Cisco vSmart コントローラ は、オーバーレイネットワークのトポロジとネットワークで使用可能なサービスを OMP ルートを使用して学習します。距離には、1 ～ 255 の値を指定できます。

フィールド	説明
OMP Admin Distance IPv6	OMP ルートのアドミニストレーティブ ディスタンス。Cisco vSmart コントローラ は、オーバーレイネットワークのトポロジとネットワークで使用可能なサービスを OMP ルートを使用して学習します。距離には、1 ～ 255 の値を指定できます。

DNS

フィールド	説明
DNS IPv4 の追加	
Primary DNS Address (IPv4)	この VPN のプライマリ IPv4 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv4)	この VPN のセカンダリ IPv4 DNS サーバーの IP アドレスを入力します。
DNS IPv6 の追加	
Primary DNS Address (IPv6)	この VPN のプライマリ IPv6 DNS サーバーの IP アドレスを入力します。
Secondary DNS Address (IPv6)	この VPN のセカンダリ IPv6 DNS サーバーの IP アドレスを入力します。

ホストマッピング

フィールド	説明
新規ホストマッピングの追加	
Hostname*	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
List of IP*	ホスト名に関連付ける IP アドレスを 8 つまで入力します。エントリをカンマで区切ります。

OMP のアドバタイズ

フィールド	説明
OMP アドバタイズ IPv4 の追加	

フィールド	説明
Protocol	このVPNに対して、OMPへのルートアドバタイズメントを構成するプロトコルを選択します。 • **static** • **network** • **aggregate** • **eigrp** • **lisp** • **isis**
Select Route Policy	ルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
OMP アドバタイズ IPv6 の追加	
Protocol	このVPNに対して、OMPへのルートアドバタイズメントを構成するプロトコルを選択します。 • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate**
Select Route Policy	ルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Protocol Sub Type	OSPFプロトコルを選択する場合は、サブタイプを外部として指定します。

Route

フィールド	説明
IPv4スタティックルートの追加	

フィールド	説明
Network Address*	IPv4 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で設定する IPv4 スタティックルートのプレフィックス長を入力します。
Subnet Mask*	サブネット マスクを入力します。

フィールド	説明
Next Hop/Null 0/VPN/DHCP	

フィールド	説明
	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択すると、[IPv4 Route Gateway Next Hop] フィールドが表示されます。ネクストホップを追加するには、このオプションを有効にします。トラッカーの有無にかかわらずホップを追加できます。 [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative Distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 [Add Next Hop with Tracker] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv4 アドレスを入力します。 • [Administrative Distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Tracker]*：ゲートウェイトラッカーの名前を入力して、ネクストホップが到達可能かどうかを判断してから、そのルートをデバイスのルートテーブルに追加します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv4 Route Null 0]*：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [VPN]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv4 Route VPN]*：VPN をゲートウェイとして選択し、パケットを転送 VPN に転送します。 • [DHCP]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv4 Route Gateway DHCP]*：IP アドレスを取得するために DHCP サーバーにアクセスすると、デフォルトの

フィールド	説明
	ネクストホップルータのスタティックルートを割り当てます。
Add BGP Routing	BGP ルートを選択します。
Add OSPF Routing	OSPF ルートを選択します。
IPv6 スタティックルートの追加	
Prefix*	IPv6 アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、VPN で設定する IPv6 スタティックルートのプレフィックス長を入力します。
Next Hop/Null 0/NAT	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [Next Hop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]*：ネクストホップ IPv6 アドレスを入力します。 • [Administrative distance]*：ルートのアドミニストレーティブ ディスタンスを入力します。 • [Null 0]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 Route Null 0]*：このオプションを有効にして、ネクストホップを null インターフェイスに設定します。このインターフェイスに送信されたすべてのパケットは、ICMP メッセージを送信せずにドロップされます。 • [NAT]：このオプションを選択すると、次のフィールドが表示されます。 • [IPv6 NAT]*：NAT64 または NAT66 を選択します。

Service

フィールド	説明
サービスの追加	

フィールド	説明
サービス タイプ	ローカルサイトと VPN で利用可能なサービスを選択します。 値：[FW]、[IDS]、[IDP]、[netsvc1]、[netsvc2]、[netsvc3]、[netsvc4]、[TE]、[SIG]
IPv4 Addresses (Maximum: 4)*	カンマで区切って最大 4 つの IP アドレスを入力します。OMP を介して学習されたルート経由ではなく、ローカルサイトでアドレスの 1 つをローカルで解決できる場合にのみ、サービスが Cisco vSmart コントローラ にアドバタイズされます。最大 4 つの IP アドレスを設定できます。
Tracking*	Cisco SD-WAN は、各サービスデバイスを定期的にテストして、動作可能かどうかを確認します。トラッキングにより、定期テストの結果がサービスログに保存されます。 トラッキングはデフォルトで有効になっています。

サービスルート

フィールド	説明
サービスルートの追加	
Prefix*	GRE 固有のスタティックルートの IP アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、プレフィックス長を入力します。
サービス*	任意のサービスを指すルートを設定します。 値：[FW]、[IDS]、[IDP]、[netsvc1]、[netsvc2]、[netsvc3]、[netsvc4]。
VPN*	プレフィックスを解決する接続先 VPN。

GRE ルート

フィールド	説明
GRE ルートの追加	
Prefix*	GRE 固有のスタティックルートの IP アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、プレフィックス長を入力します。
Interface*	サービスに到達するために使用する 1 つまたは 2 つの GRE トンネルの名前を入力します。

フィールド	説明
VPN*	サービスに到達する VPN の番号を入力します。これは VPN 0 である必要があります。

IPSEC ルート

フィールド	説明
ipSec ルートの追加	
Prefix*	IPsec 固有のスタティックルートの IP アドレスまたはプレフィックスを 10 進数の 4 点ドット表記で入力し、プレフィックス長を入力します。
Interface*	1 つまたは 2 つの IPsec トンネルインターフェイスの名前を入力します。2 つのインターフェイスを構成する場合、1 つ目はプライマリ IPsec トンネルで、2 つ目はバックアップです。すべてのパケットは、プライマリトンネルにのみ送信されます。そのトンネルに障害が発生すると、すべてのパケットがセカンダリトンネルに送信されます。プライマリトンネルが復旧すると、すべてのトラフィックがプライマリ IPsec トンネルに戻されます。

NAT

フィールド	説明
NAT プール	
NatPool Name*	一元化されたデータポリシーで構成されている NAT プール番号を入力します。NAT プール名は、VPN および VRF 全体で一意である必要があります。ルータごとに最大 31（1 ～ 32）の NAT プールを設定できます。
Prefix Length*	NAT プールのプレフィックス長を入力します。
Range Start*	NAT プールの開始 IP アドレスを入力します。
Range End*	NAT プールの終了 IP アドレスを入力します。
Overload*	ポートごとの変換を構成するには、このオプションを有効にします。このオプションを無効にすると、ダイナミック NAT のみがエンドデバイスに設定されます。ポートごとの NAT は設定されていません。 デフォルト：有効
Direction*	NAT 方向を選択します。

フィールド	説明
NAT64 v4 プール	
Nat64 V4 Pool Name*	一元化されたデータポリシーで構成されている NAT プール番号を入力します。NAT プール名は、VPN および VRF 全体で一意である必要があります。ルータごとに最大 31（1 ～ 32）の NAT プールを設定できます。
Nat 64 V4 Pool Range Start*	NAT プールの開始 IP アドレスを入力します。
Nat 64 V4 Pool Range End*	NAT プールの終了 IP アドレスを入力します。
Overload*	ポートごとの変換を構成するには、このオプションを有効にします。このオプションを無効にすると、ダイナミック NAT のみがエンドデバイスに設定されます。ポートごとの NAT は設定されていません。 デフォルト：無効

ルートリーク

フィールド	説明
グローバル VPN からのルートリークを有効にする	
Route Protocol*	グローバル VRF からサービス VPN にルートをリークするプロトコルを選択します。 • **static** • **接続** • **bgp** • **ospf**
Route Policy	ルートポリシーの名前を入力します。
プロトコルへの再配布	
Protocol*	リークされたルートを再配布するプロトコルを選択します。 • **bgp** • **eigrp** • **ospf**
ポリシー	ルートポリシーの名前を入力します。
サービス VPN からのルートリークを有効にする	

フィールド	説明
Route Protocol*	サービス VPN からグローバル VRF にルートをリークするプロトコルを選択します。 • **static** • **接続** • **bgp** • **eigrp** • **ospf**
Route Policy	ルートポリシーの名前を入力します。
プロトコルへの再配布	
Protocol*	リークされたルートを再配布するプロトコルを選択します。 • **bgp** • **ospf**
ポリシー	ルートポリシーの名前を入力します。

ルートターゲット

フィールド	説明
IPv4 設定	
Import Route Target List: Route Target*	IPv4 インターフェイスのルートターゲットを設定します。ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
Export Route Target List: Route Target*	IPv4 インターフェイスのルートターゲットを設定します。ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。
IPv6 設定	
Import Route Target List: Route Target*	IPv6 インターフェイスのルートターゲットを設定します。ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
Export Route Target List: Route Target*	IPv6 インターフェイスのルートターゲットを設定します。ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。

BGP ルーティング

サービス側ルーティングにボーダー ゲートウェイ プロトコル（BGP）機能を使用して、ローカルサイトでネットワークへの到達可能性を提供します。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表は、BGP ルーティング機能を構成するためのオプションについて説明しています。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

BGP ルーティング（サービス）

表 *51 :* 基本設定

フィールド	説明
AS Number	ローカル AS 番号を入力します。
Router ID	10 進数の 4 つの部分からなるドット付き表記で BGP ルータ ID を入力します。
Propagate AS Path	このオプションを有効にすると、BGP AS パス情報が OMP に伝達されます。
Propagate Community	このオプションを有効にすると、OMP 再配布を使用して VPN 全体で、Cisco SD-WAN サイト間で BGP コミュニティが伝播されます。
External Routes Distance	オーバーレイネットワーク内の他のサイトから学習したルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。 範囲：1 ～ 255 デフォルト：20
Internal Routes Distance	ある AS から別の AS に到達するルートの BGP ルート アドミニストレーティブ ディスタンスとして適用する値を入力します。 範囲：1 ～ 255 デフォルト：200
[Local Routes Distance]	ローカル AS 内のルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。デフォルトでは、BGP からローカルに受信したルートが OMP から受信したルートよりも優先されます。 範囲：1 ～ 255 デフォルト：20

表 *52 :* ユニキャスト アドレス ファミリ

フィールド	説明
IPv4 設定	

フィールド	説明
Maximum Paths	内部BGPマルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティングテーブルに存在するかどうかに関係なく、デフォルトルートが人為的に生成され、BGP ルート情報ベース（RIB）に挿入されます。 新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	
Protocol*	すべてのBGPセッションに対して、ルートをBGPに再配布するプロトコルを選択します。オプションは、[static]、[connected]、[ospf]、[omp]、[eigrp]、および [nat] です。 少なくとも、[omp] を選択します。デフォルトでは、OMP ルートは BGP に再配布されません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Network	
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。ネットワークプレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および 255.255.255.0 と入力します。
Aggregate Address	
Aggregate Prefix*	すべてのBGPセッションに対して集約するアドレスのプレフィックスを入力します。集約プレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および 255.255.255.0 と入力します。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	

フィールド	説明
Policy Name	ルートのダウンロードを制御するルートマップを入力します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIBにインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
IPv6 設定	
Maximum Paths	内部BGPマルチパスロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティングテーブルに存在するかどうかに関係なく、デフォルトルートが人為的に生成され、BGP RIBに挿入されます。新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	
Protocol*	すべてのBGPセッションに対して、ルートをBGPに再配布するプロトコルを選択します。オプションは、[static]、[connected]、[ospf]、[omp]、および [eigrp] です。 少なくとも、[omp] を選択します。デフォルトでは、OMP ルートは BGP に再配布されません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Network	

フィールド	説明
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。IPv6 ネットワークプレフィックスは、IPv6 アドレスとプレフィックス長（1 ～ 128）で構成されます。 たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
Aggregate Address	
Aggregate Prefix*	すべてのBGPセッションに対して集約するアドレスのプレフィックスを入力します。IPv6 集約プレフィックスは、IPv6 アドレスとプレフィックス長（1 ～ 128）で構成されます。 たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	
Policy Name*	ルートのダウンロードを制御するルートマップを入力します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIB にインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。

表 *53 :* ネイバー

フィールド	説明
IPv4 設定	
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。

フィールド	説明
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。
Allowas in Number	プロバイダー エッジ (PE) デバイスの自律システム番号 (ASN) のアドバタイズを許可する回数を入力します。指定できる範囲は 1 ～ 10 です。数値が指定されていない場合は、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。

フィールド	説明
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
Send Label	このオプションを有効にすると、ルータが相互にアドバタイズできるようになり、ルートとともに MPLS ラベルを送信できるようになります。ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。
ネイバーアドレスファミリの追加	
Family Type*	BGP IPv4 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Out Route Policy	ネイバーに送信するプレフィックスに適用するルートポリシーの名前を指定します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • [Policy Off]：ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • [Threshold (percentage)]：しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが多すぎるピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰のプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。
IPv6 設定	
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。

フィールド	説明
Allowas in Number	プロバイダーエッジ(PE)デバイスの自律システム番号(ASN)のアドバタイズを許可する回数を入力します。指定できる範囲は1 ～ 10 です。数を指定しない場合、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータのBGPコミュニティ属性をBGPネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータのBGP拡張コミュニティ属性をBGPネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）

フィールド	説明
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
IPv6 ネイバーアドレスファミリの追加	
Family Type*	BGP IPv6 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1
Out Route Policy	ネイバーに送信されるプレフィックスに適用するルートポリシーの名前を指定します。 ではルートポリシーはサポートされていません。Cisco vManage リリース 20.9.1

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • ポリシー オフ : ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • しきい値 (パーセント) : しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが多すぎるピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰のプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。

BGP ルーティング（トランスポート）

表 *54* : 基本設定

フィールド	説明
AS Number	ローカル AS 番号を入力します。
Router ID	10 進数の 4 つの部分からなるドット付き表記で BGP ルータ ID を入力します。
Propagate AS Path	このオプションを有効にすると、BGP AS パス情報が OMP に伝達されます。

フィールド	説明
Propagate Community	このオプションを有効にして、OMP 再配布を使用して VPN 全体でサイト間で BGP コミュニティを伝播します。Cisco SD-WAN
External Routes Distance	オーバーレイネットワーク内の他のサイトから学習したルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。 範囲：1 ～ 255 デフォルト：20
Internal Routes Distance	ある AS から別の AS に到達するルートの BGP ルート アドミニストレーティブ ディスタンスとして適用する値を入力します。 範囲：1 ～ 255 デフォルト：200
[Local Routes Distance]	ローカル AS 内のルートの BGP ルート アドミニストレーティブ ディスタンスを指定します。デフォルトでは、BGP からローカルに受信したルートが OMP から受信したルートよりも優先されます。 範囲：1 ～ 255 デフォルト：20

表 *55:* ユニキャスト アドレス ファミリ

フィールド	説明
IPv4 設定	
Maximum Paths	内部 BGP マルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティング テーブルに存在するかどうかに関係なく、デフォルト ルートが人為的に生成され、BGP ルート情報ベース (RIB) に挿入されます。新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	

フィールド	説明
Protocol*	すべてのBGPセッションに対して、ルートをBGPに再配布するプロトコルを選択します。オプションは、静的、接続、ospf、omp、eigrp、および nat です。 少なくとも、[connected] を選択し、[Route Policy] で、BGP がループバック インターフェイス アドレスをネイバーにアドバタイズするルートポリシーを指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Network	
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。ネットワーク プレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および 255.255.255.0 と入力します。
Aggregate Address	
Aggregate Prefix*	すべてのBGPセッションに対して集約するアドレスのプレフィックスを入力します。集約プレフィックスは、IPv4 サブネットとマスクで構成されます。たとえば、192.0.2.0 および 255.255.255.0 と入力します。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	
Policy Name	ルートのダウンロードを制御するルートマップを入力します。

フィールド	説明
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIBにインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
IPv6 設定	
Maximum Paths	内部BGPマルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル内部 BGP パスの最大数を指定します。 範囲：0 ー 32
Originate	このオプションを有効にすると、ルーティング テーブルに存在するかどうかに関係なく、デフォルト ルートが人為的に生成され、BGP ルート情報ベース (RIB) に挿入されます。新しく挿入されたデフォルトは、すべての BGP ピアにアドバタイズされます。
Redistribute	
Protocol*	すべてのBGPセッションに対して、ルートをBGPに再配布するプロトコルを選択します。オプションは、[static]、[connected]、[ospf]、[omp]、および [eigrp] です。 少なくとも、[connected] を選択し、[Route Policy] で、BGPがループバック インターフェイス アドレスをネイバーにアドバタイズするルートポリシーを指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Route Policy	再配布されるルートに適用するルートポリシーの名前を入力します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Network	

フィールド	説明
Network Prefix*	BGP によってアドバタイズされるネットワークプレフィックスを入力します。IPv6 ネットワーク プレフィックスは、IPv6 アドレスとプレフィックス長 (1 ～ 128) で構成されます。たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
Aggregate Address	
Aggregate Prefix*	すべてのBGPセッションに対して集約するアドレスのプレフィックスを入力します。IPv6 集約プレフィックスは、IPv6 アドレスとプレフィックス長 (1 ～ 128) で構成されます。たとえば、IPv6 サブネットは 2001:DB8:0000:0000:: で、プレフィックス長は 64 です。
AS Set Path	集約されたプレフィックスの設定パス情報を生成するには、このオプションを有効にします。
Summary Only	BGP 更新から特定のルートを除外するには、このオプションを有効にします。
テーブル マップ	
Policy Name	ルートのダウンロードを制御するルートマップを入力します。
Filter	このオプションを有効にすると、[Policy Name] フィールドで指定されたルートマップによって、BGP ルートをルート情報ベース（RIB）にダウンロードするかどうかが制御されます。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。 このオプションを無効にすると、[Policy Name] フィールドで指定されたルートマップを使用して、トラフィックインデックスなど、RIBにインストールするルートの特定のプロパティが設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。

表 *56 : MPLS* インターフェイス

フィールド	説明
[Interface Name]*	MPLS インターフェイスの名前を入力します。

表 *57 :* ネイバー

フィールド	説明
IPv4 設定	

フィールド	説明
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。
Allowas in Number	プロバイダー エッジ (PE) デバイスの自律システム番号 (ASN) のアドバタイズを許可する回数を入力します。指定できる範囲は 1 ～ 10 です。数を指定しない場合、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。

フィールド	説明
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
Send Label	ルータが相互にアドバタイズできるようにするには、このオプションを有効にして、ルートとともに MPLS ラベルを送信できるようにします。ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。
ネイバーアドレスファミリの追加	
Family Type*	BGP IPv4 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Out Route Policy	ネイバーに送信されるプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • [Policy Off]：ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • [Threshold (percentage)]：しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが多すぎるピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰のプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。
IPv6 設定	
Address*	BGP ネイバーの IP アドレスを指定します。
[Description]	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Interface Name	インターフェイス名を入力します。このインターフェイスは、ネイバーシップを確立するときに TCP セッションのソースとして使用されます。ループバック インターフェイスを使用することを推奨します。

フィールド	説明
Allowas in Number	プロバイダーエッジ（PE）デバイスの自律システム番号（ASN）のアドバタイズを許可する回数を入力します。指定できる範囲は 1 ～ 10 です。数値が指定されていない場合は、デフォルト値の 3 回が使用されます。
AS Override	発信元ルータの AS 番号を送信 BGP ルータの AS 番号に置き換えるには、このオプションを有効にします。
Shutdown	VPN の BGP を有効にするには、このオプションを無効にします。
Advanced Options	
[Next-Hop Self]	BGP ネイバーにアドバタイズされるルートのネクストホップとしてルータを設定するには、このオプションを有効にします。
[Send Community]	ローカルルータの BGP コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[Send Extended Community]	ローカルルータの BGP 拡張コミュニティ属性を BGP ネイバーに送信するには、このオプションを有効にします。
[EBGP Multihop]	外部ピアへの BGP 接続の存続可能時間（TTL）を設定します。 範囲：1 ～ 255 デフォルトは 1 です。
Password	MD5 メッセージダイジェストの生成に使用するパスワードを入力します。パスワードを設定すると、BGP ピアとの TCP 接続で MD5 認証が有効になります。パスワードは、大文字と小文字が区別され最大 25 文字です。パスワードには、すべての英数字（スペースを含む）を使用できます。最初の文字を数値にはできません。
Keepalive Time (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。グローバルキープアライブ時間をオーバーライドするネイバーのキープアライブ時間を指定します。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）

フィールド	説明
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。グローバルホールド時間をオーバーライドするネイバーのホールド時間を指定します。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
IPv6 ネイバーアドレスファミリの追加	
Family Type*	BGP IPv6 ユニキャスト アドレス ファミリを選択します。
In Route Policy	ネイバーから受信したプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。
Out Route Policy	ネイバーに送信するプレフィックスに適用するルートポリシーの名前を指定します。 Cisco vManage リリース 20.9.1 ではルートポリシーはサポートされていません。

フィールド	説明
Maximum Prefix Reach Policy*	次のいずれかのオプションを選択します。 • [Policy Off]：ポリシーはオフです。 • [Policy On - Restart]：ピアから受信したプレフィックスの数が最大プレフィックス制限を超えた場合に、ピアリングセッションがデバイスによって再確立される時間間隔を設定します。 このオプションを選択すると、次のフィールドが表示されます。 • プレフィックスの最大数* : プレフィックスの最大数を入力します。 範囲：1 ～ 4294967295 • [Threshold (percentage)]：しきい値を入力します。 範囲：1 ～ 100 デフォルト：75 • [Restart Interval (minutes)]*：時間間隔を入力します。 範囲：1 ー 65535 分 • [Policy On - Warning message]：再起動機能を無効にするようにデバイスを構成して、送信するプレフィックスが多すぎるピアを調整できるようにします。 • [Policy On - Disable Peer Neighbor]：デバイスがピアデバイスから過剰のプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。

表 *58 : Advanced*

フィールド	説明
Keepalive (seconds)	キープアライブメッセージが BGP ピアにアドバタイズされる頻度を指定します。キープアライブメッセージは、ローカルルータがまだアクティブであり、使用可能だと見なされることをピアに示します。このキープアライブ時間は、グローバルキープアライブ時間です。 範囲：0 ー 65535 秒 デフォルト：60 秒（ホールド時間値の 3 分の 1）

フィールド	説明
Hold Time seconds	ローカル BGP セッションでそのピアが使用可能でないと見なされるキープアライブメッセージを受信しない間隔を指定します。ローカルルータは、そのピアへの BGP セッションを終了します。このホールド時間は、グローバルホールド時間です。 範囲：0 ー 65535 秒 デフォルト：180 秒（キープアライブ時間の 3 倍）
[Compare MED]	このオプションを有効にすると、BGP パス間でルータ ID を比較してアクティブパスを決定します。
[Deterministic MED]	このオプションを有効にすると、ルートがいつ受信されたかに関係なく、同じ AS から受信されたすべてのルートの MED が比較されます。
[Missing MED as Worst]	このオプションを有効にすると、パスに MED 属性がない場合にパスが最悪のパスと見なされます。
[Compare Router ID]	このオプションを有効にすると、比較されるルートのピア AS が同じであるかどうかにかかわらず、常に MED が比較されます。
[Multipath Relax]	このオプションを有効にすると、BGP ベストパスプロセスが異なる AS のルートから選択されます。デフォルトでは、BGP マルチパスを使用している場合、BGP ベストパスプロセスは同じ AS 内のルートから選択し、複数のパス間でロードバランシングを行います。

OSPF ルーティング

Open Shortest Path First（OSPF）は、IP ネットワークのルーティングプロトコルです。サービス側ルーティングに使用して、ローカルサイトでネットワークへの到達可能性を提供できます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、OSPF ルーティング機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
Router ID	10 進数の 4 つの部分からなるドット表記で OSPF ルータ ID を入力します。これは、OSPF 隣接関係のルータに関連付けられた IP アドレスです。

フィールド	説明
[Distance for External Routes]	他のドメインから学習したルートの OSPF ルート アドミニストレーティブ ディスタンスを指定します。 範囲：1 ～ 255 デフォルト：110
[Distance for Inter-Area Routes]	あるエリアから別のエリアに到達するルートの OSPF ルート アドミニストレーティブ ディスタンスを指定します。 範囲：1 ～ 255 デフォルト：110
[Distance for Intra-Area Routes]	エリア内のルートの OSPF ルート アドミニストレーティブ ディスタンスを指定します。 範囲：0 ー 255 デフォルト：110

Redistribute

フィールド	説明
Add Redistribute	
Protocol	OSPF にルートを再配布するプロトコルを選択します。 • スタティック • 接続されている状態 • BGP • OMP • NAT • EIGRP

最大メトリック（ルータ LSA）

フィールド	説明
Add Router LSA	

フィールド	説明
Type	OSPFが最大メトリックをアドバタイズするように設定して、他のルータがこのルータを最短パス優先（SPF）計算で中継ホップとして優先しないようにします。 タイプを選択します。 • [administrative]：オペレータの介入によって最大メトリックがただちに有効になるようにします。 • [on-startup]：指定した時間の最大メトリックをアドバタイズします。

エリア

フィールド	説明
Add Area	
Area Number*	OSPF エリアの番号を入力します。 範囲：32 ビットの数値
Set the area type	OSPF エリアのタイプを選択します。 • スタブ • NSSA
Add Interface	OSPF エリアのインターフェイスのプロパティを設定します。
名前*	インターフェイスの名前を **geslot/port** または **loopback number** の形式で入力します。
Hello Interval (seconds)*	ルータが OSPF hello パケットを送信する頻度を指定します。 範囲：1 ～ 65535 秒 デフォルト：10 秒
Dead Interval (seconds)*	ルータがネイバーから OSPF hello パケットを受信する頻度を指定します。パケットを受信しない場合、ルータはネイバーがダウンしていると見なします。 範囲：1 ～ 65535 秒 デフォルト：40 秒（デフォルト hello 間隔の 4 倍）

フィールド	説明
LSA Retransmission Interval (seconds)*	OSPF プロトコルが LSA をネイバーに再送信する頻度を指定します。 範囲：1 ～ 65535 秒 デフォルト：5 秒
[Interface Cost]	OSPF インターフェイスのコストを指定します。 範囲：1 ー 65535
Designated Router Priority*	ルータが代表ルータ（DR）として選択される優先順位を設定します。最大の優先順位を持つルータがDRになります。優先順位が等しい場合、ルータ ID が最も高いノードが DR またはバックアップ DR になります。 範囲：0 ー 255 デフォルト：1
OSPF ネットワーク タイプ	インターフェイスを接続するOSPFネットワークタイプを選択します。 • ブロードキャスト ネットワーク • ポイントツーポイント ネットワーク • ノンブロードキャスト ネットワーク • ポイントツーマルチポイント ネットワーク
Passive Interface*	OSPFインターフェイスをパッシブに設定するかどうかを指定します。パッシブインターフェイスはアドレスをアドバタイズしますが、OSPF プロトコルをアクティブに実行しません。 デフォルト：無効
認証タイプ	認証タイプを選択します。 • [simple]：パスワードはクリアテキストで送信されます。 • [message-digest]：MD5 アルゴリズムによりパスワードが生成されます。
Message Digest Key	クリアテキストで、または AES 暗号化キーとして、MD5 認証キーを入力します。1 ～ 255 文字のキーを使用できます。
md5	メッセージダイジェスト（MD5認証）のキーIDを入力します。1 ～ 32 文字の ID を使用できます。
範囲の追加（Add Range）	OSPF エリアのインターフェイスのエリア範囲を設定します。

フィールド	説明
IP Address*	IP アドレスを入力します。
Subnet Mask*	サブネット マスクを入力します。
Cost	タイプ 3 サマリー LSA の番号を指定します。OSPF は、SPF 計算時にこのメトリックを使用して、宛先への最短パスを決定します。 範囲：0 ー 16777214
No-advertise*	タイプ 3 サマリー LSA をアドバタイズしないようにするには、このオプションを有効にします。

Advanced

フィールド	説明
[Reference Bandwidth (Mbps)]	インターフェイスの OSPF 自動コスト計算の基準帯域幅を指定します。 範囲：1 ー 4294967 Mbps デフォルト：100 Mbps
RFC 1583 Compatible	デフォルトでは、OSPF 計算は RFC 1583 に従って行われます。RFC 2328 に基づいてサマリールートのコストを計算するには、このオプションを無効にします。
Originate	デフォルトの外部ルートを OSPF ルーティングドメインに生成するには、このオプションを有効にします。このオプションを有効にすると、次のフィールドが表示されます。 • [Always]：OSPF ルーティングドメインでデフォルトルートを常にアドバタイズするには、このオプションを有効にします。 • [Default Metric]：デフォルトルートの生成に使用されるメトリックを設定します。 範囲：0 ー 16777214 デフォルト：10 • [Metric Type]：デフォルトルートを OSPF タイプ 1 外部ルートまたは OSPF タイプ 2 外部ルートとしてアドバタイズする場合に選択します。

フィールド	説明
SPF Calculation Delay (milliseconds)	トポロジに対する最初の変更を受信してから SPF 計算を実行するまでの時間を指定します。 範囲：1 ー 600000 ミリ秒（60 秒） デフォルト：200 ミリ秒
Initial Hold Time (milliseconds)	連続する SPF 計算間の時間を指定します。 範囲：1 ー 600000 ミリ秒（60 秒） デフォルト：1000 ミリ秒
Maximum Hold Time (milliseconds)	連続する SPF 計算間の最長時間を指定します。 範囲：1 ～ 600000 デフォルト：10000 ミリ秒（60 秒）

ワイヤレス LAN

この機能は、ワイヤレスコントローラの設定に役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

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。

次の表では、ワイヤレス LAN 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。

基本設定

フィールド	説明
Enable 2.4G*	2.4 GHz の無線タイプをシャットダウンするには、このオプションを無効にします。 デフォルト：有効
Enable 5G*	5 GHz の無線タイプをシャットダウンするには、このオプションを無効にします。 デフォルト：有効
Country*	ルータが設置されている国を選択します。
Username*	Cisco Mobility Express のユーザー名を指定します。
パスワード*	Cisco Mobility Express のパスワードを指定します。

ME IP 設定

フィールド	説明
ME Dynamic IP*	インターフェイスが DHCP サーバーから動的に IP アドレスを受け取るようにするには、このオプションを有効にします。
ME IP Address	Cisco Mobility Express の IP アドレスを指定します。
[Subnet Mask]	Cisco Mobility Express のサブネットマスクを指定します。

フィールド	説明
デフォルト ゲートウェイ	Cisco Mobility Express のデフォルト ゲートウェイ アドレスを指定します。

SSID

フィールド	説明
SSID の追加	
SSID Name*	ワイヤレス SSID の名前を入力します。 4 ～ 32 文字の文字列を指定できます。SSID は一意である必要があります。
Admin State*	インターフェイスが設定されていることを示すには、このオプションを有効にします。
Broadcast SSID*	SSID をブロードキャストする場合は、このオプションを有効にします。SSID をすべてのワイヤレスクライアントに表示したくない場合は、このオプションを無効にします。
VLAN (Range 1-4094)*	ワイヤレス LAN トラフィックの VLAN ID を入力します。
Radio Type	次のいずれかの無線タイプを選択します。 • 2.4GHz • **5GHz** • All
Security Type*	セキュリティタイプを選択します。 • [WPA2 Enterprise]：リモート RADIUS サーバーでネットワークユーザーを認証および承認する企業では、このオプションを選択します。 • [WPA2 Personal]：パスフレーズを使用してワイヤレスネットワークにアクセスするユーザーを認証するには、このオプションを選択します。 • [Open]：認証なしでワイヤレスネットワークへのアクセスを許可するには、このオプションを選択します。
Passphrase*	このフィールドは、セキュリティタイプとして [WPA2 Personal] を選択する場合に使用できます。パスフレーズを設定します。このパスフレーズを使用して、ユーザーがワイヤレスネットワークにアクセスできます。

フィールド	説明
QoS プロファイル	QoS プロファイルを選択します。

Switch Port

スイッチポート機能を使用して、Cisco SD-WAN へのブリッジを設定します。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、スイッチポート機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能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。

フィールド	説明
Description	機能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。
Age Out Time	エントリが期限切れになるまでのMACテーブル内のエントリの長さを入力します。エントリがタイムアウトしないようにするには、値を 0 に設定します。 範囲：0、10 ～ 1000000 秒 デフォルト：300 秒
インターフェイスの設定	
Interface Name	ブリッジドメインに関連付けるインターフェイスの名前を **`geslot/port`** の形式で入力します。
Mode	スイッチポートモードを選択します。 • [access]：インターフェイスをアクセスポートとして設定します。アクセスポートではVLANを1つだけ設定でき、ポートは 1 つの VLAN のトラフィックだけを伝送できます。[access] を選択すると、次のフィールドが表示されます。 [Switchport Access Vlan]：VLAN 番号を入力します。値は 1 ～ 4094 です。 • [trunk]：インターフェイスをトランクポートとして設定します。トランクポートでは1つ以上のVLANを設定でき、ポートは複数の VLAN のトラフィックを伝送できます。[trunk] を選択すると、次のフィールドが表示されます。 • [Allowed Vlans]：トランクがトラフィックを伝送できる VLAN の数と VLAN の説明を入力します。 • [Switchport Trunk Native Vlan]：タグなしトラフィックを伝送できる VLAN の数を入力します。
Shutdown	インターフェイスをイネーブルにします。デフォルトでは、インターフェイスは無効です。
速度	インターフェイスの速度を入力します。
デュプレックス	[full] または [half] を選択して、インターフェイスが全二重または半二重のどちらのモードで動作するかを指定します。

フィールド	説明
Port Control	インターフェイスでIEEE 802.1Xポートベースの認証を有効にするには、ポート制御モードを選択します。 • [auto]：IEEE 802.1X認証を有効にし、ポートを無許可ステートで開始します。ポート経由で送受信できるのはEAPOLフレームだけです。ポートのリンクステートがダウンからアップに変更した際、またはEAPOL-Startフレームを受信した際に、認証プロセスが開始されます。デバイスはサプリカントの識別を要求し、サプリカントと認証サーバー間で認証メッセージのリレーを開始します。デバイスはサプリカントのMACアドレスを使用して、ネットワークアクセスを試みる各サプリカントを一意に識別します。 • [force unauthorized]：ポートが無許可ステートのままになり、サプリカントからの認証の試みをすべて無視します。デバイスは、このポートを介してサプリカントに認証サービスを提供することはできません。 • [force-authorized]：IEEE 802.1X認証を無効にし、その結果、認証の交換を必要とせずにポートが許可済みステートに変更されます。ポートは、クライアントのIEEE 802.1xベース認証を行わずに、通常のトラフィックを送受信します。
音声 VLAN	音声 VLAN ID を入力します。
Pae Enable	Cisco SD-WANデバイスは、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。
MAC 認証バイパス	RADIUS サーバーで MAC 認証バイパス（MAB）を許可し、RADIUSサーバーを使用して非IEEE 802.1X準拠のクライアントを認証するには、このオプションを有効にします。

フィールド	説明
Host Mode	IEEE 802.1Xインターフェイスが単一のホスト（クライアント）または複数のホスト（クライアント）へのアクセスを許可するかどうかを選択します。 • [single-host]：最初に認証されたホストにのみアクセスを許可します。これがデフォルトです。 • [multi-auth]：音声 VLAN 上の 1 つのホストとデータ VLAN 上の複数のホストへのアクセスを許可します。 • [multi-host]：複数のホストへのアクセスを許可します。 • [multi-domain]：ホストと音声デバイス（同じスイッチポート上の IP 電話など）の両方にアクセスを許可します。
Enable Periodic Reauth	定期的な再認証を有効にします。デフォルトで、このオプションは有効になっています。
Inactivity	非アクティブタイムアウト時間を秒単位で入力します。 デフォルト：60 秒
再認証（Reauthentication）	再認証間隔を秒で入力します。
Control Direction	[both]（双方向）または[in]（単方向）認証モードを選択します。
制限付き VLAN	IEEE 802.1x 準拠クライアントの制限付き VLAN（または認証失敗 VLAN）を入力します。RADIUS 認証に失敗した IEEE 802.1X 準拠クライアントへの限定サービスを設定します。
ゲスト VLAN	クライアントが MAB リストにない場合、ゲスト VLAN を入力して、IEEE 802.1X 対応でないクライアントをドロップします。
Critical VLAN	IEEE 802.1x 準拠クライアントのクリティカル VLAN（または認証失敗 VLAN）を入力します。RADIUS 認証または RADIUS サーバーが失敗した場合のネットワークアクセスを構成します。
Enable Voice	クリティカル音声 VLAN を有効にします。
Configure Static Mac Address	
[MAC Address]	スイッチ ポート インターフェイスにマッピングする静的 MAC アドレスを入力します。
Interface Name	スイッチ ポート インターフェイスの名前を入力します。
VLAN ID	スイッチポートの VLAN 番号を入力します。

イーサネット インターフェイス

この機能は、サービス VPN（512 を除く 1 ～ 65527 の範囲）でイーサネット インターフェイスを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、イーサネットインターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Associated VPN	サービス VPN。

基本設定

フィールド	説明
Shutdown	インターフェイスを有効または無効にします。
Interface Name	インターフェイスの名前を入力します。インターフェイス名を完全にスペルアウトします (たとえば、GigabitEthernet0/0/0)。 使用していない場合でも、ルータのすべてのインターフェイスを構成して、それらがシャットダウン状態で構成され、それらのすべてのデフォルト値が構成されるようにします。
Description	インターフェイスの説明を入力します。
IPv4 設定	IPv4 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。
Dynamic DHCP Distance	DHCP サーバーから学習したルートのアドミニストレーティブディスタンス値を入力します。このオプションは、[Dynamic] を選択した場合に使用できます。 デフォルト：1
IP Address	静的 IPv4 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。
[Subnet Mask]	サブネット マスクを入力します。
Add Secondary IP Address	サービス側インターフェイスのセカンダリ IPv4 アドレスを最大 4 つ入力します。 • [IP Address*]：IP アドレスを入力します。 • [Subnet Mask]：サブネットマスクを入力します。
DHCP Helper	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。

フィールド	説明
IPv6 設定	IPv6 VPN インターフェイスを設定します。 • [Dynamic]：インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。 • [Static]：変更されない IP アドレスを入力するには、[Static] を選択します。 • **None**
IPv6 Address Primary	静的 IPv6 アドレスを入力します。このオプションは、[Static] を選択した場合に使用できます。
Add Secondary Ipv6	サービス側インターフェイスのセカンダリ IPv6 アドレスを 2 つまで入力します。
Add DHCP Helper	
DHCPv6 Helper*	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスを 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
DHCPv6 Helper VPN	DHCP ヘルパーの VPN ソースインターフェイスの VPN ID を入力します。

NAT

フィールド	説明
IPv4 設定	
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。
NAT Type*	IPv4 の NAT 変換タイプを選択します。 • **プール** • **loopback** デフォルト：[pool]
範囲の開始	NAT プールの開始 IP アドレスを入力します。
範囲の終了	NAT プールの終了 IP アドレスを入力します。

フィールド	説明
Prefix Length	NAT プールのプレフィックス長を入力します。
Overload	ポートごとの変換を構成するには、このオプションを有効にします。このオプションを無効にすると、ダイナミック NAT のみがエンドデバイスに設定されます。ポートごとの NAT は設定されていません。 デフォルト：有効
NAT Loopback	ループバック インターフェイスの IP アドレスを入力します。
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）
Add New Static NAT	
Source IP*	変換される送信元アドレスを入力します。
Translate IP*	変換された送信元 IP アドレスを入力します。
Direction	ネットワークアドレス変換を行う方向を選択します。 • [inside]：デバイスのサービス側から送信され、ルータのトランスポート側に向かうパケットの IP アドレスを変換します。 • [Outside]：トランスポート側デバイスからデバイスに到着し、サービス側デバイス宛てのパケットの IP アドレスを変換します。
Source VPN*	送信元 VPN ID を入力します。
IPv6 設定	
NAT	インターフェイスを NAT デバイスとして機能させるには、このオプションを有効にします。

フィールド	説明
Select NAT	NAT64 または NAT66 を選択します。[NAT66] を選択し、[Add Static NAT66] をクリックすると、次のフィールドが表示されます。 • [Source Prefix*]：送信元 IPv6 プレフィックスを入力します。 • [Translated Source Prefix*]：変換された送信元プレフィックスを入力します。 • [Source VPN ID*]：送信元 VPN ID を入力します。

VRRP

フィールド	説明
IPv4 設定	
Add Vrrp Ipv4	
Group ID*	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ～ 255
Priority*	ルータの優先度を入力します。最も優先度が高いルータがプライマリルータとして選択されます。2 つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリルータとして選択されます。 範囲：1 ～ 254 デフォルト：100
Timer*	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。セカンダリルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。 範囲：100 ～ 40950 秒 デフォルト：100 秒
Track OMP*	このオプションを有効にすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションを追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。

フィールド	説明
プレフィックス リスト	OMP セッションと、ローカルルータで構成されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方を追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のプレフィックスの 1 つへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイス がプライマリ VRRP ルータを決定する間のオーバーレイトラフィックの量が最小限に抑えられます。
IP Address*	仮想ルータの IP アドレスを入力します。このアドレスは、ローカル ルータと VRRP を実行しているピアの両方の構成済みインターフェイス IP アドレスとは異なる必要があります。
Tloc Prefix Change*	このオプションを有効または無効にして、TLOC 設定を変更できるかどうかを設定します。
Tloc Prefix Change Value	TLOC 設定の変更値を入力します。 範囲：100 ～ 4294967295
VRRP セカンダリ IP アドレスの追加	
IP Address*	セカンダリ VRRP ルータの IP アドレスを入力します。
[Subnet Mask]	サブネット マスクを入力します。
VRRP トラッキングオブジェクトの追加	
Tracker ID*	インターフェイス オブジェクト ID またはオブジェクト グループ トラッカー ID を入力します。
Tracker Action*	次のいずれかのオプションを選択します。 • **decrement** • **shutdown**
Decrement Value*	減分値を入力します。 範囲：1 ～ 255
IPv6 設定	
Add Vrrp Ipv6	

フィールド	説明
Group ID*	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ～ 255
Priority*	ルータの優先度を入力します。最も優先度が高いルータがプライマリルータとして選択されます。2つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリルータとして選択されます。 範囲：1 ～ 254 デフォルト：100
Timer*	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。セカンダリルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。 範囲：100 ～ 40950 秒 デフォルト：100 秒
Track OMP*	このオプションを有効にすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションを追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。
Track Prefix List	OMP セッションと、ローカルルータで構成されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方を追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のプレフィックスの 1 つへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイス がプライマリ VRRP ルータを決定する間のオーバーレイトラフィックの量が最小限に抑えられます。
Link Local IPv6 Address*	グループのリンクローカルアドレスを表す仮想リンクローカル IPv6 アドレスを入力します。アドレスは、標準のリンクローカルアドレス形式になっている必要があります。たとえば、FE80::AB8 です。

フィールド	説明
Global IPv6 Prefix	グループのグローバルアドレスを表す仮想グローバルユニキャストIPv6アドレスを入力します。このアドレスは、VRRPグループが設定されているインターフェイス転送アドレスと同じマスクを持つIPv6グローバルプレフィックスアドレスである必要があります。たとえば、2001::2/124 です。 最大 3 つのグローバル IPv6 アドレスを設定できます。

ARP

フィールド	説明
ARPの追加	
IP Address*	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
[MAC アドレス（MAC Address）]*	MAC アドレスをコロン区切りの 16 進表記で入力します。

TrustSec

フィールド	説明
Enable SGTPropogation	Cisco TrustSec セキュリティグループタグ（SGT）の伝播機能を使用するには、このオプションを有効にします。
伝染する	Cisco SD-WAN で SGT を伝播するには、このオプションを有効にします。
セキュリティ グループタグ（**Security Group Tag**）	タグとして使用できる値を入力します。
Enable Enforced Propagation	インターフェイスで SGT 適用を開始するには、このオプションを有効にします。
Enforced Security Group Tag	適用のタグとして使用できる値を入力します。

Advanced

フィールド	説明
デュプレックス	インターフェイスが全二重または半二重のどちらのモードで実行されるかを指定します。 デフォルト：full

フィールド	説明
[MAC Address]	インターフェイスに関連付ける MAC アドレスを、コロンで区切った 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 9216 デフォルト：1500 バイト
インターフェイス MTU	インターフェイスで送受信されるフレームの最大伝送単位サイズを入力します。 範囲：1500 ～ 1518（GigabitEthernet0）、1500 ～ 9216（他の GigabitEthernet） デフォルト：1500 バイト
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし
速度	接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。 値：10、100、1000、2500、または 10000 Mbps
ARP Timeout	ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2147483 秒 デフォルト：1200 秒
自動ネゴシエーション	自動ネゴシエーションをオンにするには、このオプションを有効にします。
メディア タイプ	インターフェイスの物理メディア接続タイプを指定します。次のいずれかを選択します。 • [auto-select]：接続は自動的に選択されます。 • [rj45]：RJ-45 の物理接続を指定します。 • [sfp]：光ファイバメディアの Small Form Factor Pluggable（SFP）物理接続を指定します。

フィールド	説明
Load Interval	インターフェイス負荷計算の間隔値を入力します。
Tracker	サービス VPN の静的ルートトラッキングを使用すると、設定されたエンドポイントアドレスの可用性を追跡して、静的ルートをデバイスのルーティングテーブルに含めることができるかどうかを判断できます。ゲートウェイトラッカーの名前を入力して、ネクストホップが到達可能かどうかを判断してから、そのルートをデバイスのルートテーブルに追加します。
ICMP Redirect Disable	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。
XConnect	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。
IP Directed Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。

SVI インターフェイス

この機能は、スイッチ仮想インターフェイス（SVI）を設定して VLAN インターフェイスを設定するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、SVI インターフェイス機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
[Feature Name]*	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Associated VPN: VPN*	VPN を選択します。

基本設定

フィールド	説明
Shutdown	VLAN インターフェイスを有効または無効にします。
VLAN Interface Name*	VLAN インターフェイスの名前を入力します。 名前は 5 文字以上にする必要があります。名前は次の形式にする必要があります。 `^Vlan(([1-9]\d|\d)/){0,2}(0|[1-9]\d*)([:|\.][1-9]\d*)?`
インターフェイスの説明	インターフェイスの説明を入力します。
インターフェイス MTU	インターフェイスで送受信されるフレームの最大伝送単位サイズを入力します。 範囲：1500 ～ 9216 デフォルト：1500 バイト
IP MTU	各インターフェイスにおいて送信される IP パケットの最大伝送単位（MTU）サイズを入力します。 範囲：576 ～ 9216 デフォルト：1500 バイト
IPV4 アドレスの設定	
IPv4 Address Prefix*	インターフェイスの IPv4 アドレスを入力します。
List of DHCP helper addresses*	ネットワーク内の DHCP サーバーの IP アドレスを 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。各アドレスはカンマで区切ります。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
IPV4 セカンダリアドレスの設定	
Secondary IP Address*	セカンダリ IP アドレスを 4 つまで入力できます。
IPV6 アドレスの設定	
IPV6 address*	インターフェイスの IPv6 アドレスを入力します。
IPV6 セカンダリアドレスの設定	
Address*	セカンダリ IP アドレスを 4 つまで入力できます。
IPV6 DHCP ヘルパーの設定	

フィールド	説明
Address*	ネットワーク内の DHCP サーバーの IP アドレスを入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
VPN	DHCP ヘルパーアドレスの VPN ID。

ACL

フィールド	説明
アクセスリスト V4 の設定	
Direction*	ACL の方向（[in] または [out]）を選択します。
Name of ACL*	アクセスリストの名前を入力します。
アクセスリスト V6 の設定	
Direction*	ACL の方向（[in] または [out]）を選択します。
Name of ACL*	アクセスリストの名前を入力します。

VRRP

フィールド	説明
VRRP の設定	
Group ID*	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ～ 255
Priority*	ルータの優先度を入力します。最も優先度が高いルータがプライマリルータとして選択されます。2つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリルータとして選択されます。 範囲：1 ～ 254 デフォルト：100

フィールド	説明
Timer*	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。セカンダリルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。 範囲：100 ～ 40950 秒 デフォルト：100 秒
Track OMP	このオプションを有効にすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションを追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。
Prefix List*	OMP セッションと、ローカルルータで構成されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方を追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のプレフィックスの 1 つへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイス がプライマリ VRRP ルータを決定する間のオーバーレイトラフィックの量が最小限に抑えられます。
IP Address	仮想ルータの IP アドレスを入力します。このアドレスは、ローカルルータと VRRP を実行しているピアの両方の構成済みインターフェイス IP アドレスとは異なる必要があります。
VRRP セカンダリ IP アドレスの追加	
Address*	セカンダリ VRRP ルータの IP アドレスを入力します。
TLOC Preference Change	このオプションを有効または無効にして、TLOC 設定を変更できるかどうかを設定します。
VRRP トラッキングオブジェクトの追加	
Tracker Id*	インターフェイス オブジェクト ID またはオブジェクト グループ トラッカー ID を入力します。
Track Action*	次のいずれかのオプションを選択します。 • **decrement** • **shutdown**

フィールド	説明
Decrement Value	減分値を入力します。 範囲：1 ～ 255
VRRP IPv6 の設定	
Group ID*	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ～ 255
Priority*	ルータの優先度を入力します。最も優先度が高いルータがプライマリルータとして選択されます。2 つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリルータとして選択されます。 範囲：1 ～ 254 デフォルト：100
Timer*	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。セカンダリルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。 範囲：100 ～ 40950 秒 デフォルト：100 秒
Track OMP*	このオプションを有効にすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションを追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。
Track Prefix List	OMP セッションと、ローカルルータで構成されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方を追跡します。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のプレフィックスの 1 つへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイス がプライマリ VRRP ルータを決定する間のオーバーレイトラフィックの量が最小限に抑えられます。
VRRP IPv6 プライマリの追加	

フィールド	説明
IPv6 Link Local*	グループのリンクローカルアドレスを表す仮想リンクローカル IPv6 アドレスを入力します。アドレスは、標準のリンクローカルアドレス形式になっている必要があります。たとえば、FE80::AB8 です。
Prefix	プライマリ VRRP ルータの IPv6 アドレスを入力します。

ARP

フィールド	説明
ARP の設定	
IP Address*	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
[MAC アドレス（MAC Address）]*	MAC アドレスをコロン区切りの 16 進表記で入力します。

Advanced

フィールド	説明
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1960 バイト デフォルト：なし
ARP Timeout	動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2678400 秒（744 時間） デフォルト：1200（20 分）

フィールド	説明
IP Directed-Broadcast	IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。
ICMP/ICMPv6 Redirect Disable	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。

DHCP サーバ

この機能を使用すると、インターフェイスを DHCP ヘルパーとして設定して、DHCP サーバーから受信したブロードキャスト DHCP 要求を転送することができます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、DHCP サーバー機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
VPN	サービス VPN。このフィールドは編集できません。

基本設定

フィールド	説明
Address Pool*	ルータインターフェイスが DHCP サーバーとして機能するサービス側ネットワークのアドレスプールの IPv4 プレフィックス範囲を、**`prefix/length`** の形式で入力します。

フィールド	説明
Exclude	DHCP アドレスプールから除外する 1 つ以上の IP アドレスを入力します。複数の個別のアドレスを指定するには、それらをカンマで区切ってリストします。アドレスの範囲を指定するには、ハイフンで区切ります。
Lease Time(seconds)	DHCP によって割り当てられた IP アドレスが有効である時間を指定します 範囲：60 ～ 31536000 秒 デフォルト：86400

静的リース

フィールド	説明
Add Static Lease	
[MAC アドレス（MAC Address）]*	静的 IP アドレスが割り当てられるクライアントの MAC アドレスを入力します。
IP*	クライアントに割り当てる静的 IP アドレスを入力します。

DHCP オプション

フィールド	説明
Add Option Code	
Code*	オプションコードを設定します。 範囲：1 ～ 254
Type	次の 3 つのタイプのいずれかを選択します。 • [ASCII]：ASCII 値を指定します。 • [Hex]：16 進値を指定します。 • [IP]：IP アドレスを指定します。最大 8 つの IP アドレスを指定できます。

Advanced

フィールド	説明
インターフェイス MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：68 ～ 65535 バイト
ドメイン名	DHCP クライアントがホスト名を解決するために使用するドメイン名を指定します。
デフォルト ゲートウェイ	サービス側ネットワークのデフォルトゲートウェイの IP アドレスを入力します。
DNS Servers	サービス側ネットワークの DNS サーバーの IP アドレスを 1 つ以上入力します。複数のエントリがある場合は、カンマで区切ります。最大 8 つのアドレスを指定できます。
TFTP サーバ	サービス側ネットワークの TFTP サーバーの IP アドレスを入力します。1 つまたは 2 つのアドレスを指定できます。2 つの場合、アドレスはカンマで区切ってください

その他のプロファイル

ThousandEyes

Cisco ThousandEyes は、ビジネスに影響を与えるネットワークとサービス全体のエンドツーエンドのビューを提供する SaaS アプリケーションです。内部、外部、キャリアネットワーク、およびインターネット全体のネットワーク トラフィック パスをリアルタイムでモニターして、ネットワーク パフォーマンス データを提供します。Cisco ThousandEyes は、WAN とクラウドに関するインテリジェントな洞察を提供し、アプリケーション配信とエンドユーザー エクスペリエンスを最適化するのに役立ちます。

この機能のデフォルト値を持つ各パラメータでは、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。

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。

次の表では、ThousandEyes 機能を設定するためのオプションについて説明します。

フィールド	説明
Type	ドロップダウンリストから機能を選択します。
機能名	機能の名前を入力します。
Description	機能の説明を入力します。説明には任意の文字とスペースを使用できます。
Account Group Token	Cisco ThousandEyes アカウントグループトークンを入力します。
VPN	トランスポートまたはサービス VPN です。[Default] 設定は、トランスポート VPN（VPN 0）を示します。[Global] または [Device Specific] 設定は、サービス VPN を示します。 VPN 設定を [Global] または [Device Specific] 設定として設定する場合は、Cisco ThousandEyes Enterprise エージェントをプロビジョニングするサービス VPN の ID を入力します。
[Management IP]	Cisco ThousandEyes Enterprise エージェントの IP アドレスを入力します。このフィールドは、サービス VPN を指定した場合にのみ使用できます。

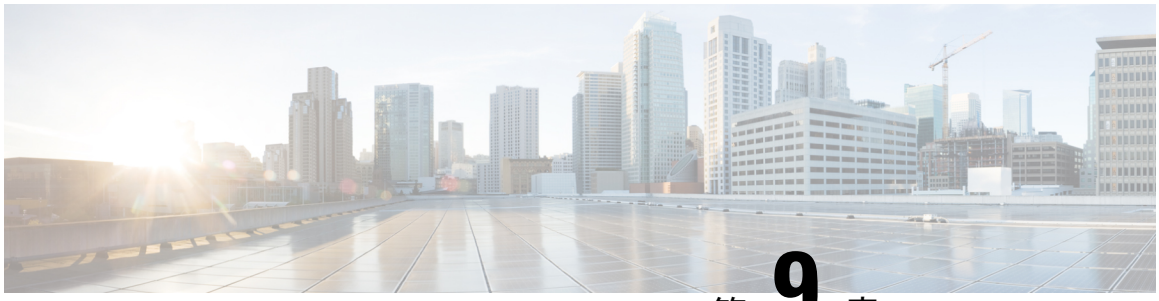
フィールド	説明
管理サブネット	Cisco ThousandEyes Enterprise エージェントのドロップダウンリストからサブネットマスクを選択します。このフィールドは、サービス VPN を指定した場合にのみ使用できます。 （注） この IP プレフィックスアドレス（[Management IP] および [Management Subnet]）は、ファブリック内で一意である必要があり、他のブランチエージェントの IP アドレスと重複してはなりません。
Agent Default Gateway	デフォルトゲートウェイのアドレスを入力します。この IP アドレスは、ルータの仮想ポートグループに割り当てられます。このフィールドは、サービス VPN を指定した場合にのみ使用できます。
Name Server IP	優先 DNS サーバーの IP アドレスを入力します。 このサーバーは、Cisco SD-WAN ファブリックの内部または外部に存在できますが、サービス VPN から到達可能である必要があります。
ホスト名（Host Name）	エージェントが Cisco ThousandEyes ポータルに登録するときに使用する必要があるホスト名を入力します。デフォルトでは、エージェントは Cisco IOS XE SD-WAN デバイスのホスト名を使用します。
Proxy Type	Cisco ThousandEyes Enterprise エージェントが外部アクセスにプロキシサーバーを使用する必要がある場合は、プロキシタイプとして次のいずれかを選択します。 • **static** • **pac** • **none** スタティックプロキシの設定： • [Proxy Host]：設定を [Global] 設定として設定し、プロキシサーバーのホスト名を入力します。 • [Proxy Port]：設定を [Global] 設定として設定し、プロキシサーバーのポート番号を入力します。 PAC の設定： • [PAC URL]：設定を [Global] 設定として設定し、プロキシ自動構成（PAC）ファイルの URL を入力します。

CLI プロファイル

CLI 機能プロファイルを使用すると、CLI 形式でデバイス設定を指定できます。

フィールド	説明
Choose existing	[Profiles] テーブルから既存のプロファイルを選択します。
Create new	このオプションを選択すると、次のフィールドが表示されます。 • [Name]：プロファイルの名前を入力します。 • [Description]：プロファイルの説明を入力します。説明には任意の文字とスペースを使用できます。

CLI 設定ウィンドウに設定を手動で入力するか、CLI 設定をコピーして貼り付けることができます。構成を保存するには、[Save] をクリックします。



第 9 章

デバイスのタグ付け

表 *59* : 機能の履歴

機能名	リリース情報	説明
ユーザー定義デバイスのタグ付け	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能は、デバイスにタグを追加するのに役立ちます。タグを使用して、デバイスのグループ化、説明、検索、または管理を行うことができます。

デバイスのタグ付けに関する情報

デバイスのタグ付け機能は、次のことを行うのに役立ちます。

- デバイスへのタグの追加：タグ付けを使用すると、デバイス管理がさらに効果的になります。タグを使用して、デバイスのグループ化、記述、または検索を行うことができます。1 つのデバイスに複数のタグを追加できます。
- タグ付けに基づいてデバイスを設定グループに追加：タグを使用すると、ルールを作成して、設定グループに自動的に追加する必要があるデバイスを定義できます。ルール作成の詳細については、「ルールを使用した設定グループへのデバイスの追加」を参照してください。

（注） この機能は、シングルテナント展開とマルチテナント展開の両方で使用できます。

デバイスのタグ付けでサポートされるデバイス

この機能は Cisco IOS XE SD-WAN デバイス でのみサポートされています。

デバイスのタグ付けの前提条件

Cisco IOS XE SD-WAN デバイスの最小ソフトウェアバージョン：Cisco IOS XE リリース 17.8.1a

Cisco vManage の最小ソフトウェアバージョン：Cisco vManage リリース 20.8.1

デバイスのタグ付けの制約事項

- Cisco vManage インスタンスには最大 25 個のタグを作成できます。
- デバイスごとに最大 25 個のタグを追加できます。
- タグの名前には、最長 25 文字を指定でき、英数字、ハイフン（-）、および下線（_）のみを使用できます。スペースや他の特殊文字は使用できません。
- タグの名前では、大文字と小文字が区別されます。
- 設定グループに追加できるタグルールは 1 つだけです。

Cisco vManage を使用したデバイスへのタグの追加

次の方法のいずれかを使用して、タグをデバイスに追加できます。

[Devices] ウィンドウを使用する

1. Cisco vManage メニューから、**[Configuration]** > **[Devices]**を選択します。
2. [WAN Edge List] をクリックし、デバイスを選択します。
3. [Add Tags] をクリックします
4. 既存のタグのリストからタグを選択するか、[Add New Tag] をクリックして新しいタグを作成します。
5. [Apply] をクリックします。

   指定したタグがデバイスに追加されます。

クイック接続ワークフローの使用

1. Cisco vManage メニューから、**[Workflows]** > **[Launch Workflows]** を選択します。

2. [Quick Connect] をクリックします。

   [Quick Connect] ワークフローが開始されます。

3. [Add Tags] をクリックします

4. ワークフローの指示に従ってください。

5. デバイスにタグ付けします。

   指定したタグがデバイスに追加されます。

（注） 現在デバイスに関連付けられているタグを編集するには、新しいタグを追加するか、不要なタグを削除します。

タグの削除

デバイスに追加されていないタグ、またはタグルールに含まれていないタグのみを削除できます。

1. Cisco vManage のメニューから、**[Tools]** > **[Tag Management]** を選択します。

2. 削除するタグを選択します。

3. [Delete Tags] をクリックします。

4. 確認のダイアログボックスで、[はい（Yes）] をクリックします。

第 10 章

ネットワーク階層とリソース管理

表 *60* : 機能の履歴

機能名	リリース情報	説明
ネットワーク階層とリソース管理	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、Cisco vManage でネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層と、リージョン ID とサイト ID を含む関連するリソース ID は、構成設定をデバイスに適用するのに役立ちます。さらに、リソースマネージャの Cisco vManage への導入により、これらのリソース ID が自動的に管理されるため、Cisco SD-WAN の全体的なユーザーエクスペリエンスが簡素化されます。 Cisco vManage で [Multi-Region Fabric] オプションを有効にした場合にのみ、リージョンを作成できることに注意してください。

ネットワーク階層とリソース管理に関する情報

ネットワーク階層の概要

Cisco vManage でネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層には、リージョン、エリア、サイトの 3 種類のノードを含めることができます。ノードに割り当てられたリソース ID は、後で構成設定をどこに適用するかを指定するのに役立ちます。

デフォルトでは、ネットワーク階層にグローバルと呼ばれるノードが 1 つあります。

ネットワーク階層には、次の 3 種類のノードを持つ 1 つの階層が事前定義されています。

- Region：マルチリージョン ファブリックベースの Cisco SD-WAN 展開におけるリージョンを表します。マルチリージョン ファブリック機能は、Cisco SD-WAN オーバーレイネットワークのアーキテクチャを、互いに区別して動作する複数のリージョンネットワークと、リージョン間のトラフィックを管理するための中央のコアリージョンネットワークに分割するオプションを提供します。

  Cisco vManage で [Multi-Region Fabric] オプションを有効にしている場合にのみ、リージョンを作成できます。マルチリージョンファブリック機能の詳細については、『*Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*』を参照してください。

- Area：エリアは、ネットワーク階層内のノードの論理グループです。サイト、リージョン、その他のエリア、またはこれらの組み合わせを 1 つのエリアにグループ化できます。

- Site：サイトは、ネットワーク階層の最下位レベルのノードまたはリーフノードです。サイトの下に子ノードを作成することはできません。デバイスはサイトにのみ関連付けることができます。

ネットワーク階層内のさまざまなノードの作成と管理の詳細については、「ネットワーク階層の管理」を参照してください。

リソース管理の概要

Cisco vManage のリソースマネージャは、リソース ID、つまりリージョン ID とサイト ID を管理します。**[Configuration]** > **[Network Hierarchy]** ページで作成したリージョンのリージョン ID が自動的に生成されます。指定しない場合は、同様にサイトのサイト ID が生成されます。

サイト ID とリージョン ID をデバイスに割り当てることができます。リソース ID をデバイスに割り当てる方法の詳細については、「デバイスへのリソース ID の割り当て」を参照してください。

Cisco vManage の以前のバージョンから Cisco vManage リリース 20.9.1 にアップグレードする場合、Cisco vManage のリソースマネージャは、セットアップ内の既存のデバイスのサイト ID に基づいてサイトを自動的に作成します。サイトの名前は SITE_<*id*> になります。Cisco vManage では [Network Hierarchy] ページのグローバルノードの下に、これらのサイトが表示されます。また、既存のデバイスをネットワーク階層内のサイトに関連付けます。

ネットワーク階層とリソース管理の利点

- リージョンとサイトの管理を自動化します。
- Cisco vManage が既存のすべてのサイトを検出してネットワーク階層に表示する場合、アップグレードシナリオでの手動の労力を省きます。
- デバイスの導入準備と構成を簡素化します。

ネットワーク階層とリソース管理でサポートされるデバイス

この機能は、Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス でサポートされています。

ネットワーク階層とリソース管理の制約事項

- 子ノードがない場合にのみ、ノードを削除できます。たとえば、デバイスが関連付けられていない場合にのみサイトを削除できます。
- サイトは、ネットワーク階層のノードの最下位レベルまたはリーフノードです。サイトの下に子ノードを作成することはできません。
- グローバルノードとサイトノードの間に複数のリージョンノードを作成することはできません。
- マルチテナント展開ではリージョンを作成できません。

ネットワーク階層の管理

ネットワーク階層とリソース管理機能を使用すると、次のことができます。

- リージョンの作成
- エリアの作成
- サイトの作成、編集、削除

ネットワーク階層でのリージョンの作成

はじめる前に

Cisco vManage の [Multi-Region Fabric] オプションが有効になっていることを確認します。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Multi-Region Fabric] オプションの横にある [Edit] をクリックします。
3. [Enabled] をクリックしてから、[Save] をクリックします。

リージョンの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. 左ペインのノード（グローバルまたはエリア）の隣にある […] をクリックし、[Add MRF Region] を選択します。

（注） Cisco vManage リリース 20.9.x では、[Add Node] オプションを使用して領域を追加することもできます。

3. [Name] フィールドに、領域の名前を入力します。名前は一意にする必要があり、使用できるのは、英字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。
4. [Description] フィールドに、領域の説明を入力します。
5. [Parent] ドロップダウンリストから、親ノードを選択します。
6. [Add] をクリックします。

ネットワーク階層でのエリアの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. 左ペインのノード（グローバル、リージョン、またはエリア）の隣にある […] をクリックし、[Add Area] を選択します。

（注） Cisco vManage リリース 20.9.x では、[Add Node] オプションを使用してエリアを追加することもできます。

3. [Name] フィールドに、エリアの名前を入力します。名前は一意にする必要があり、使用できるのは、英字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。
4. [Description] フィールドに、エリアの説明を入力します。
5. [Parent] ドロップダウンリストから、親ノードを選択します。
6. [Add] をクリックします。

ネットワーク階層のサイトの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. 左ペインのノード（グローバル、リージョン、またはエリア）の隣にある […] をクリックし、[Add Site] を選択します。

（注） Cisco vManage リリース 20.9.x では、[Add Node] オプションを使用してサイトを追加することもできます。

3. [Name] フィールドにサイトの名前を入力します。名前は一意にする必要があり、使用できるのは、英字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。
4. [Description] フィールドにサイトの説明を入力します。
5. [Parent] ドロップダウンリストから、親ノードを選択します。
6. [Site ID] フィールドに、サイト ID を入力します。

   サイト ID を入力しない場合、Cisco vManage によりサイトのサイト ID が生成されます。
7. [Add] をクリックします。

リージョンの編集

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. リージョン名の隣にある […] をクリックし、[Edit MRF Region] を選択します。
3. 必要に応じて、オプションを編集します。リージョンの名前、説明、および親を編集できます。
4. [Save] をクリックします。

リージョンの削除

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. リージョン名の隣にある […] をクリックし、[Delete MRF Region] を選択します。
3. 確認のダイアログボックスで、[はい（Yes）] をクリックします。

エリアの編集

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. エリア名の横にある […] をクリックし、[Edit Area] を選択します。
3. 必要に応じて、オプションを編集します。エリアの名前、説明、および親を編集できます。
4. [Save] をクリックします。

エリアの削除

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. エリア名の横にある […] をクリックし、[Delete Area] を選択します。
3. 確認のダイアログボックスで、[はい（Yes）] をクリックします。

サイトの編集

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. サイト名の横にある […] をクリックし、[Edit Site] を選択します。
3. 必要に応じて、オプションを編集します。サイトの名前、説明、および親のみを編集できます。
4. [Save] をクリックします。

サイトの削除

1. Cisco vManage メニューから、**[Configuration]** > **[Network Hierarchy]** を選択します。
2. サイト名の横にある […] をクリックし、[Delete Site] を選択します。
3. 確認のダイアログボックスで、[はい（Yes）] をクリックします。

デバイスへのリソース ID の割り当て

ネットワーク階層とリソース管理機能を使用すると、次のことができます。

- デバイスへのサイト ID の割り当て
- デバイスへのリージョン ID の割り当て

デバイスへのサイト ID の割り当て

次のいずれかの方法を使用して、デバイスにサイト ID を割り当てることができます。

クイック接続ワークフローの使用

1. Cisco vManage のメニューで **[Workflows]** > **[Workflow Library]** を選択します。
2. [Quick Connect] ワークフローを開始します。
3. ワークフローの指示に従ってください。

4. [Add and Review Device Configuration] ページで、デバイスのサイト ID を入力します。

（注）
- ネットワーク階層で使用可能な既存のサイト ID のいずれかを使用するか、新しいサイト ID を入力できます。ネットワーク階層にノードを作成せずに新しいサイト ID を入力すると、サイトが自動的に作成され、**[Configuration]** > **[Network Hierarchy]** ページに表示されます。

テンプレートの使用

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** > **[WAN Edge List]** を選択します。
2. デバイスがデバイステンプレートにアタッチされているかどうかを確認します。
3. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Feature Templates]** を選択します。
4. [System] 機能テンプレートの隣にある [...] をクリックし、[Edit] を選択します。
5. [Basic Configuration] タブをクリックし、[Site ID] フィールドの範囲を [Global] に設定して、サイト ID を入力します。
6. [更新（Update）] をクリックします。
7. [Configure Devices] をクリックして、設定をデバイスにプッシュします。

ステップ 5 で [Site ID] フィールドの範囲を [Device Specific] に設定した場合は、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Device Templates]** を選択します。
2. デバイステンプレートの隣にある [...] をクリックし、[Edit Device Template] を選択します。
3. [Site ID] フィールドに、サイト ID を入力します。

   ネットワーク階層で使用可能な既存のサイト ID のいずれかを使用するか、新しいサイト ID を入力できます。ネットワーク階層にノードを作成せずに新しいサイト ID を入力すると、サイトが自動的に作成され、[構成ネットワーク階層] ページに一覧表示されます。 >
4. [更新（Update）] をクリックします。
5. [Configure Devices] をクリックして、設定をデバイスにプッシュします。

設定グループの使用

設定グループフローは、Cisco IOS XE SD-WAN デバイス にのみ適用されます。

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある [...] をクリックし、[Edit] を選択します。
3. [Associated Devices] をクリックします。
4. 設定グループに関連付けられているデバイスを選択し、[Deploy] をクリックします。

   [Deploy Configuration Group] ワークフローが開始されます。
5. ワークフローの指示に従ってください。
6. [Add and Review Device Configuration] ページで、デバイスのサイト ID を入力します。

   ネットワーク階層で使用可能な既存のサイト ID のいずれかを使用するか、新しいサイト ID を入力できます。ネットワーク階層にノードを作成せずに新しいサイト ID を入力すると、サイトが自動的に作成され、**[Configuration]** > **[Network Hierarchy]** ページに表示されます。

デバイスへのリージョン ID の割り当て

はじめる前に

- [Multi-Region Fabric] 機能にアクセスできる必要があります。
- ネットワーク階層でリージョンが使用可能であることを確認します。

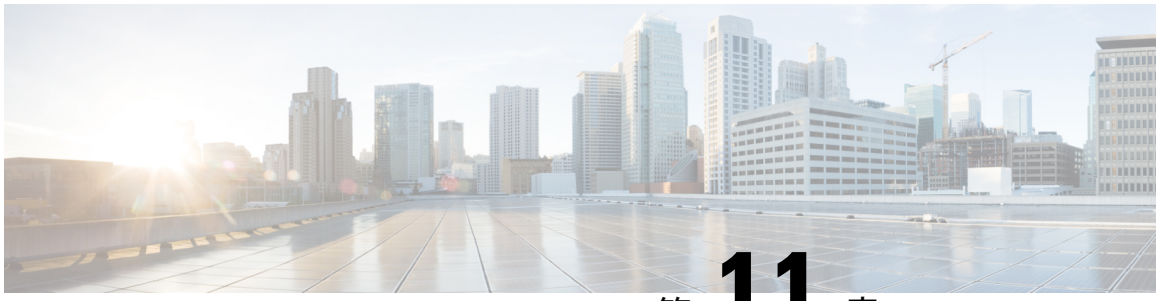
リージョン ID の割り当て

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** > **[WAN Edge List]** を選択します。
2. 対応するデバイスがデバイステンプレートにアタッチされているかどうかを確認します。
3. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Feature Templates]** を選択します。
4. [System] 機能テンプレートの隣にある [...] をクリックし、[Edit] を選択します。
5. [Basic Configuration] タブをクリックし、[Region ID] フィールドの範囲を [Global] に設定して、リージョン ID を入力します。

   ネットワーク階層で使用可能な既存のリージョン ID のいずれかを使用できます。指定されたリージョン ID がネットワーク階層で使用できない場合、デバイスへのテンプレートのプッシュ操作は失敗します。
6. [更新（Update）] をクリックします。
7. [Configure Devices] をクリックして、設定をデバイスにプッシュします。

ステップ 5 で [Region ID] フィールドの範囲を [Device Specific] に設定した場合は、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Templates]** > **[Device Templates]** を選択します。
2. デバイステンプレートの隣にある […] をクリックし、[Edit Device Template] を選択します。
3. [Region ID] フィールドに、リージョン ID を入力します。
4. [更新（Update）] をクリックします。
5. [Configure Devices] をクリックして、設定をデバイスにプッシュします。



第 11 章

Cisco Unified Communications 音声サービス

表 *61* : 機能の履歴

機能名	リリース情報	説明
Cisco Unified Communications との統合	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	このリリースでは、機能テンプレートを使用してシスコの IP ベースのメディアサービスを有効にするためのサポートが追加されています。
	Cisco IOS XE リリース 17.2.1r	この機能により、機能テンプレートと音声ポリシーを使用して、サポートされているルータで Cisco Unified Communications（UC）音声サービスを有効にすることができます。Cisco UC 音声サービスが有効になっている場合、ルータは、音声ポート、POTS ダイヤルピア、SIP ダイヤルピア、Cisco Unified SRST モードの電話プロファイルなどのさまざまなエンドポイントへのコールを処理できます。 UC 音声サービスの項目は、サポートされているデバイスの [Feature] タブと [Voice Policy] ページから設定できます。 Cisco Unified Communications の UC 音声サービスを設定するには、Cisco vManage が Cisco SD-WAN リリース 20.1.1 を実行している必要があります。 この機能は、Cisco 4000 シリーズサービス統合ルータでサポートされています。

機能テンプレートと音声ポリシーを設定して、サポートされているルータで Cisco Unified Communications（UC）音声サービスを有効にすることができます。これらのテンプレートとポリシーは、これらのルータの FXO、FXS、および FXS/DID インターフェイスのパラメータを設定します。Cisco IOS XE リリース 17.3.1a 以降では、PRI ISDN のパラメータも設定できます。また、DSPFarm 機能テンプレートを使用して、シスコの IP ベースのメディアサービスを有効にすることができます。

Cisco UC 音声サービスが有効になっている場合、ルータは、アナログインターフェイスとデジタルインターフェイスの音声ポート、POTS ダイヤルピア、SIP ダイヤルピア、Cisco Unified SRST モードの電話プロファイルなどのさまざまなエンドポイントへのコールを処理できます。

Cisco Unified Communications の UC 音声サービスを設定するには、Cisco vManage が Cisco SD-WAN リリース 20.3 を実行している必要があります。

Cisco IOS 音声アプリケーションを設定および保守するためのコマンドの詳細については、『Cisco IOS Master Command List』を参照してください。

次に、さまざまなシナリオで Cisco Unified Communications の音声サービスを設定するために実行する一般的な手順について説明します。

- Cisco Unified Communications の Cisco SD-WAN の初期設定ワークフロー

  ステップ 1：音声カード機能テンプレートを追加します。

  ステップ 2：コールルーティング機能テンプレートを追加します。

  ステップ 3：（オプション）SRST 機能テンプレートを追加します。

  ステップ 4：（オプション）DSPFarm 機能テンプレートを追加します。

  ステップ 5：（オプション）音声ポリシーを追加します。

  ステップ 6：Unified Communications 用のデバイステンプレートをプロビジョニングします。

- 音声ポート、POTS ダイヤルピア、SIP ダイヤルピア、または SRST 電話プロファイルサブポリシーを音声ポリシーに追加するワークフロー

  ステップ 1：UC 音声ポリシーと UC 固有の機能テンプレートを含むデバイステンプレートをアタッチ解除します。

  ステップ 2：サブポリシーを音声ポリシーに追加します。

  ステップ 3：必要に応じて、更新された音声ポリシーをエンドポイントにマッピングします。

  ステップ 4：機能テンプレートをデバイステンプレートにアタッチします。

- UC エンドポイントを追加または削除するために機能テンプレートを更新するワークフロー

  ステップ 1：音声カードの UC 固有の機能テンプレートと音声ポリシーを含むデバイステンプレートをアタッチ解除します。

  ステップ 2：必要に応じて、音声カード機能テンプレートを更新します。

ステップ 3：必要に応じて、更新された音声ポリシーをエンドポイントにマッピングします。

ステップ 4：機能テンプレートをデバイステンプレートにアタッチします。

- 音声ポートの機能が変更されたときに設定パラメータを更新するワークフロー

  ステップ 1：音声カードの UC 固有の機能テンプレートと関連する音声ポリシーマッピングを含むデバイステンプレートをアタッチ解除します。

  ステップ 2：必要に応じて、音声カード機能テンプレートと音声ポリシーを更新します。

  ステップ 3：必要に応じて、更新された音声ポリシーをエンドポイントにマッピングします。

  ステップ 4：機能テンプレートと音声ポリシーをデバイステンプレートにアタッチします。

- T1/E1 音声モジュールのインターフェイスタイプを変更するワークフロー

  ステップ 1：T1/E1 音声モジュールを定義する音声カード機能テンプレートを含むデバイステンプレートをアタッチ解除し、関連付けられたマッピングされた音声ポリシーをアタッチ解除します。

  ステップ 2：T1/E1 音声モジュール用に設定されている PRI ISDN 音声ポートからすべての音声ポリシーのマッピングを解除し、それらのポートの POTS ダイヤルピアをマッピング解除します。

  ステップ 3：音声カード機能テンプレートで、T1/E1 音声モジュール用に設定されている PRI ISDN 音声ポートを削除します。

  ステップ 4：デバイステンプレートをデバイスに再アタッチします。

  ステップ 5：デバイスをリロードします。

  ステップ 6：デバイステンプレートをデバイスからアタッチ解除します。

  ステップ 7：音声カード機能テンプレートで、必要に応じて T1/E1 音声モジュール用の新しい PRI ISDN 音声ポートを作成します。

  ステップ 8：音声カード機能テンプレートと音声ポリシーをデバイステンプレートにマッピングします。

  ステップ 9：必要に応じて、更新された音声ポリシーを新しく作成された PRI ISDN 音声ポートにマッピングします。

  ステップ 10：デバイステンプレートをデバイスに再アタッチします。

- T1/E1 音声モジュールのクロックソース設定を更新してプライマリおよびセカンダリクロックソースを変更するワークフロー

  ステップ 1：更新する T1/E1 音声モジュールの音声カード機能テンプレートで、各 PRI ISDN 音声ポートのクロックソースを [Line] に設定し、設定をデバイスにプッシュします。

  ステップ 2：設定が正常にプッシュされたら、音声カード機能テンプレートで、T1/E1 音声モジュールの各 PRI ISDN 音声ポートのクロックソースを目的の値に設定し、設定をデバイスにプッシュします。

音声カード機能テンプレートの追加

音声カード機能テンプレートは、アナログおよび PRI ISDN デジタルインターフェイスを設定します。これらは、ルータの音声カードのポートの設定を提供します。

アナログインターフェイスの音声カード機能テンプレートを追加する場合、設定する音声カードのタイプ、カードのポート情報、およびサービスプロバイダーから受け取るサービスのパラメータを設定します。 デジタルインターフェイスの場合、音声カードのタイプ、T1 または E1 コントローラ、および関連パラメータを設定します。

音声カードのモジュールを追加する場合、Cisco vManage は、モジュールの使用可能なスロットとサブスロットを表示することにより、モジュールの配置を支援します。Cisco vManage は、デバイスモデルに基づいて使用可能なスロットとサブスロットを決定します。

次の表では、アナログインターフェイスを設定するためのオプションについて説明します。

表 *62 :* アナログインターフェイス設定オプション

オプション	説明	Cisco IOS CLI での同等コマンド
モジュール	ルータにインストールされている音声モジュールのタイプを選択します。	—
モジュールのスロット/サブスロット	音声モジュールのスロットとサブスロットを入力します。	**voice-card** *slot/subslot*
Use DSP	TDM コール用のネットワークインターフェイス モジュールの組み込み DSP を使用する場合は、このオプションを有効にします。	**no local-bypass**

オプション	説明	Cisco IOS CLI での同等コマンド
ポート タイプ	このインターフェイス用に設定している音声モジュールのポートのタイプ（[FXS] または [FXO]）を選択します。[All] を選択して、選択したタイプのすべてのポートのポートタイプを定義するか、または [Port Range] を選択して、指定した範囲のポートのポートタイプを定義できます。 [Port Range] を使用すると、この手順の後半で説明するようにアナログインターフェイスを作成して、さまざまな範囲のポートを設定できます。	—
説明	選択したポートの説明を入力します。たとえば、Fax マシンやページングシステムなどです。	**description** *string*
Secondary Dialtone	[Port Type] ドロップダウンリストから [FXO] を選択した場合に使用できます。 発信者が外線にアクセスしたときに、選択したポートでセカンダリダイヤルトーンを生成する場合は、[On] に設定します。	**secondary dialtone**
Connection PLAR	選択したポートが着信コールを転送する専用線の自動リングダウン内線を入力します。	**connection plar** *digits*
OPX	[Port Type] ドロップダウンリストから [FXO] を選択した場合に使用できます。 PLAR 拡張機能のオフプレミス拡張機能を有効にする場合は、このオプションをオンにします。	**connection plar opx** *digits*
Signal Type	ポートが受信するコールのオンフックまたはオフフック状態を示す信号タイプを選択します。オプションは、[Loopstart]、[Groundstart]、または [DID] です。[DID] オプションは、[Port Type] ドロップダウンリストから [FXS] を選択した場合に使用できます。	**signal** {groundstart | loopstart} **signal did** {delay-dial | immediate | wink-start}

オプション	説明	Cisco IOS CLI での同等コマンド
Caller-ID Enable	[Loopstart] または [Groundstart] の信号タイプを選択した場合に使用できます。 着信コールの発信者 ID 情報を有効にする場合は、[ON] に設定します。	**caller-id enable**
DID Signal Mode	[DID] の信号タイプを選択した場合に使用できます。 DID 信号タイプのモードを選択します（[Delay Dial]、[Immediate]、または [Wink Start]）。 デフォルト：[Wink Start]。	**signal did** {delay-dial | immediate | wink-start}
シャットダウン	使用していないポートをシャットダウンする場合は、[ON] に設定します。 デフォルトは Off です。	**shutdown**

次の表では、デジタルインターフェイスを設定するためのオプションについて説明します。

表 *63 :* デジタルインターフェイスの設定オプション

オプション	説明	Cisco IOS CLI での同等コマンド
[Digital Interface] タブ T1/E1 音声モジュールのパラメータおよびモジュールポートのクロックソースを設定するためのオプションを提供します。これらのオプションを設定する前に、T1/E1 音声モジュールごとに適切な DSP モジュールがインストールされていることを確認してください。		
モジュール	ルータにインストールされている T1/E1 音声モジュールのタイプを選択します。	—
インターフェイスタイプ	音声モジュールのインターフェイスのタイプを選択します。 • [T1 PRI]：AMI または B8ZS コーディングを使用して、電話交換ネットワークを介した 1.544 Mbps の T1 接続を指定します • [E1 PRI]：主として欧州で使われている 2.048Mbps の速度でデータを伝送する広域デジタル伝送方式を指定します	**card type** {**t1** | **e1**} *slot sub-slot*

オプション	説明	Cisco IOS CLI での同等コマンド
Slot/Sub-slot	音声モジュールのスロットとサブスロットを入力します。	**voice-card** *slot*/*sub-slot*
Use DSP	TDM コール用のネットワーク インターフェイス モジュールの組み込み DSP を使用する場合は、このオプションを有効にします。	**no local-bypass**

オプション	説明	Cisco IOS CLI での同等コマンド
インターフェイス		**controller** {**t1** | **e1**} *slot*/*sub-slot*/*number* **clock source** {**network** | **line** | **line primary** | **line secondary**}

オプション	説明	Cisco IOS CLI での同等コマンド
	次のアクションを実行して、モジュールにプロビジョニングされる T1/E1 ポートの数と、各ポートのクロックソースを設定します。 **1.** [Add] をクリックします。[Port and Clock Selector] ウィンドウが表示されます。 **2.** 設定する各ポートに対応するチェックボックスをオンにします。設定できるポートの数は、選択したモジュールタイプによって異なります。 **3.** ポートごとに、クロックソースを選択します。 • [Line]：回線クロックをプライマリクロックソースとして設定します。このオプションを使用すると、ポートは、回線受信データストリームから復元されたクロックから送信データのクロックを生成します。 • [Primary Clock]：ポートをプライマリクロックソースに設定します。 • [Secondary Clock]：ポートをセカンダリクロックソースとして設定します。 • [Network]：バックプレーンクロックまたはシステムオシレータクロックをモジュールクロックソースとして設定します。 1つのポートをプライマリクロックとして設定し、同じネットワークに接続する別のポートを、バックアップとして機能するセカンダリクロックソースとして設定することをお勧めします。	

オプション	説明	Cisco IOS CLI での同等コマンド
	4. [Add] をクリックします。	
ネットワーク参加	このチェックボックスは、インターフェイスを追加した後に表示されます。 T1/E1 モジュールがバックプレーンクロックに参加するように設定するには、このチェックボックスをオンにします。 モジュールのバックプレーンクロックとのクロック同期を削除するには、このチェックボックスをオフにします。 デフォルトでは、このチェックボックスはオンになっています。	**network-clock synchronization participate** *slot*/*sub-slot*
シャットダウン	インターフェイスポートに関連付けられているコントローラ、シリアルインターフェイス、または音声ポートを無効または有効にするには、次のアクションを実行します。 **1.** [Shutdown Selected] をクリックします。[Shutdown] ウィンドウが表示されます。 **2.** ポートごとに、有効にする項目（[Controller]、[Serial]、または [Voice Port]）を選択します。項目を選択しない場合、有効になります。 **3.** [Add] をクリックします。	**controller e1/t1** *slot*/*sub-slot*/*port* **shutdown** **interface serial** *slot*/*sub-slot*/**port:**{**15** | **23**} **shutdown** **voice-port** *slot*/*sub-slot*/**port:**{**15** | **23**} **shutdown**
Time Slots	インターフェイスタイプのタイムスロット数を選択します。 有効な範囲： • T1 PRI の場合：タイムスロット 1 ～ 24。24 番目のタイムスロットは D チャネルです。 • E1 PRI の場合：タイムスロット 1 ～ 31。16 番目のタイムスロットは D チャネルです。	**controller e1/t1** *slot*/*sub-slot*/*port* **pri-group timeslots** *timeslot-range* [**voice-dsp**]

オプション	説明	Cisco IOS CLI での同等コマンド
フレーミング（Framing）	インターフェイスタイプのフレームタイプを選択します。 T1 PRI インターフェイスタイプの場合、オプションは次のとおりです。 • [esf]：拡張スーパーフレーム（デフォルト） • [sf]：スーパーフレーム E1 PRI インターフェイスタイプの場合、オプションは次のとおりです。 • [crc4]：CRC4 フレーミングタイプ（デフォルト） • [no-crc4]：CRC4 フレーミングタイプなし	**controller t1** *slot/sub-slot/port* **framing** [**esf** | **sf**] **controller e1** *slot/sub-slot/port* **framing** [**crc4** | **no-crc4**] [**australia**]
オーストラリア	このチェックボックスは、インターフェイスタイプとして E1 PRI を選択した場合に表示されます。 [australia] フレーミングタイプを使用するには、このチェックボックスをオンにします。	**controller e1** *slot/sub-slot/port* **framing** [**crc4** | **no-crc4**] **australia**

オプション	説明	Cisco IOS CLI での同等コマンド
Line Code	インターフェイスタイプの回線コードタイプを選択します。 T1 PRI インターフェイスタイプの場合、オプションは次のとおりです。 • [ami]：回線コードタイプとして Alternate Mark Inversion を使用します • [b8zs]：回線コードタイプとして binary 8-zero substitution を使用します（デフォルト） E1 PRI インターフェイスタイプの場合、オプションは次のとおりです。 • [ami]：回線コードタイプとして Alternate Mark Inversion を使用します • [hdb3]：回線コードタイプとして high-density binary 3 を使用します（デフォルト）	**controller t1** *slot*/*sub-slot*/*port* **linecode** [**ami** | **b8zs**] **controller e1** *slot*/*sub-slot*/*port* **linecode** [**ami** | **hdb3**]
Line Termination	このチェックボックスは、インターフェイスタイプが E1 PRI の場合にのみ表示されます。 E1 コントローラの回線終端タイプを選択します。 • [75-ohm]：75 Ω の不平衡型終端 • [120-ohm]：120 Ω の平衡型終端（デフォルト）	**controller e1** *slot*/*sub-slot*/*port* **line-termination** {**75-ohm** | **120-ohm**}
Cable Length Type	このチェックボックスは、インターフェイスタイプが T1 PRI の場合にのみ表示されます。 T1 PRI インターフェイスタイプのケーブル長タイプを選択します。 • [long]：長いケーブル長 • [short]：短いケーブル長	**controller t1** *slot*/*sub-slot*/*port* **cablelength** {**short** | **long**}

オプション	説明	Cisco IOS CLI での同等コマンド
ケーブル長	このチェックボックスは、インターフェイスタイプが T1 PRI の場合にのみ表示されます。 T1 PRI インターフェイスタイプのケーブル長を選択します。このオプションを使用して、T1 ケーブルの受信機で信号のパルスを微調整します。 デフォルト値は [0db] です。	**controller t1** *slot*/*sub-slot*/*port* **cablelength** {**[short** [**110ft** | **220ft** | **330ft** | **440ft** | **550ft** | **660ft**]] [**long** [**-15db** | **-22.5db** | **-7.5db** | **0db**]]}
Network Side	このオプションを有効にすると、デバイスは標準の PRI ネットワーク側インターフェイスを使用します。 デフォルトでは、このオプションは無効になっています（[No] に設定されています）。	**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn protocol-emulate** [**network**| **user**]

オプション	説明	Cisco IOS CLI での同等コマンド
スイッチ タイプ	このインターフェイスの ISDN スイッチタイプを選択します。 • [primary-qsig]：Q.931 プロトコルに従って QSIG シグナリングをサポートします。ネットワーク側の機能は、isdn protocol-emulate コマンドで割り当てられます。 • [primary-net5]：アジア、オーストラリア、およびニュージーランドの NET5 ISDN PRI スイッチタイプ。Euro-ISDN E-DSS1 シグナリングシステム用 ETSI 準拠スイッチ。 • [primary-ntt]：日本 NTT ISDN PRI スイッチ。 • [primary-4ess]：Lucent（AT&T）4ESS スイッチタイプ（米国向け）。 • [primary-5ess]：Lucent（AT&T）5ESS スイッチタイプ（米国向け）。 • [primary-dms100]：Nortel DMS-100 スイッチタイプ（米国向け）。 • [primary-ni]：National ISDN スイッチタイプ。	**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn switch-type** [**primary-4ess**	**primary-5ess** |**primary-dms100**	**primary-net5**	**primary-ni**	**primary-ntt**	**primary-qsig**]

オプション	説明	Cisco IOS CLI での同等コマンド
ISDN Timer		**interface serial** *slot*/*sub-slot*/**port:**{**15**| **23**} **isdn timer T200** *value* **isdn timer T203** *value* **isdn timer T301** *value* **isdn timer T303** *value* **isdn timer T306** *value* **isdn timer T309** *value* **isdn timer T310** *value* **isdn timer T321** *value*

オプション	説明	Cisco IOS CLI での同等コマンド
	インターフェイスの ISDN タイマーを設定するには、次のアクションを実行します。 **1.** [Add] をクリックします。ISDN タイマーウィンドウが表示されます。 **2.** 必要に応じて、以下のタイマーの設定を行います。値はミリ秒単位です。 • [T200]。有効な範囲：400 ～ 400000 の整数。デフォルト：1000。 • [T203]。有効な範囲：400 ～ 400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。 • [T301]。有効な範囲：180000 ～ 86400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。 • [T303]。有効な範囲：400 ～ 86400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。 • [T306]。有効な範囲：400 ～ 86400000 の整数。デフォルトは 30000 です。 • [T309]。有効な範囲：0 ～ 86400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。 • [T310]。有効な範囲：400 ～ 400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。	

オプション	説明	Cisco IOS CLI での同等コマンド
	• [T321]。有効な範囲：0 ～ 86400000 の整数。デフォルト値は、スイッチタイプとネットワーク側の設定に基づいています。 **3.** [Add] をクリックします。	
Delay Connect Timer	PRI ISDN へアピンコールを遅延接続する期間をミリ秒単位で選択します。 有効な範囲：0 ～ 200 の整数。デフォルトは 20 です。	**voice-port** *slot*/*sub-slot*/**port:**{**15**| **23**} **timing delay-connect** *value*
[Clock] タブ モジュールごとに選択したプライマリおよびセカンダリクロックソースの優先順位を設定するには、このタブを使用します。 このタブは、PRI ISDN デジタルインターフェイスを設定し、[Add] をクリックすると有効になります。		
Clock Priority Sorting	最大 6 つのクロックソースの優先順位を設定します。 ドロップダウンリストには、プライマリまたはセカンダリクロックソースが定義されていて、ネットワーク参加用に設定されているインターフェイスポートが表示されます。 チェックボックスをオンにして優先順位リストに含めるポートを選択し、ポートの横にある上矢印を使用して優先順位を変更します。リストには、優先順位の高い順にポートが表示され、最も優先順位の高いポートがリストの先頭に表示されます。 優先順位を設定すると、このフィールドには選択したポートが優先順位順に表示されます。 優先順位リストのすべてのポートは、E1-PRI または T1-PRI のいずれかの同じタイプにすることをお勧めします。	**network-clock input-source** priority **controller** [**t1**| **e1**] *slot*/*sub-slot*/*port*

オプション	説明	Cisco IOS CLI での同等コマンド
Automatically Sync	[Add] を選択して、すべてのモジュールとルータ間のネットワーク同期を有効にします。 デフォルト：[On]。	network-clock synchronization automatic
Wait to restore clock	クロック選択プロセスにプライマリクロックソースを含める前にルータが待機する時間をミリ秒単位で入力します。 有効な範囲：0～86400。デフォルトは 300 です。	network-clock wait-to-restore *milliseconds*

音声カード機能テンプレートを追加するには、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. [Feature Templates] をクリックし、[Add 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、[Feature Templates] は [Feature] と呼ばれます。

3. 音声サービスを追加するサポートされているデバイスを選択します。
4. [Unified Communications] テンプレートから [Voice Card] を選択します。
5. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
6. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
7. アナログインターフェイスを設定するには、[New Analog Interface] をクリックし、「アナログ設定オプション」の表の説明に従ってインターフェイスオプションを設定します。

   Cisco IOS XE リリース 17.3.1a 以降では、[Interface] 領域の [Analog Interface] をクリックして、[New Analog Interface] にアクセスします。

   モジュールがサポートするインターフェイスの数に基づいて、必要な数のアナログインターフェイスを追加できます。

   各アナログインターフェイスを設定したら、[Add] をクリックします。

   アナログインターフェイスがすでに設定されている場合は、このページのインターフェイステーブルに表示されます。既存のインターフェイスを編集するには、[...] をクリッ

クし、その鉛筆アイコンをクリックして、ポップアップウィンドウでオプションを編集し（「アナログ設定オプション」の表を参照）、[Save Changes] をクリックします。インターフェイスを削除するには、[…] をクリックし、ごみ箱アイコンをクリックします。

8. PRI ISDN デジタルインターフェイスを設定するには、[Interface] 領域で [Digital Interface] をクリックし、[New Digital Interface] をクリックして、「デジタルインターフェイス設定オプション」の表の説明に従ってインターフェイスオプションを設定します。

   各 PRI ISDN デジタルインターフェイスを設定したら、[Add] をクリックします。

   モジュールがサポートするインターフェイスの数に基づいて、必要な数の PRI ISDN デジタルインターフェイスを追加できます。

   デジタルインターフェイスがすでに設定されている場合は、このページのインターフェイステーブルに表示されます。既存のインターフェイスを編集するには、[…] をクリックし、その鉛筆アイコンをクリックして、ポップアップウィンドウでオプションを編集し（「デジタルインターフェイス設定オプション」の表を参照）、[Save Changes] をクリックします。インターフェイスを削除するには、[…] をクリックし、ごみ箱アイコンをクリックします。

   インターフェイス設定を保存した後は、モジュールタイプ、インターフェイスタイプ、スロットまたはサブスロット、またはタイムスロットを変更できません。

   タイムスロットを変更する場合は、インターフェイスを削除して新しいインターフェイスを作成する必要があります。

   モジュールタイプ、インターフェイスタイプ、およびスロットまたはサブスロットを変更する場合は、デバイスからテンプレートを切り離し、インターフェイスに関連付けられている音声ポリシーのマッピングを解除し、モジュールとスロットまたはサブスロットに関連付けられているすべてのインターフェイスを削除します。次に、テンプレートをデバイスにプッシュし、デバイスをリロードして、必要な新しいインターフェイスを作成します。最後に、新しいテンプレートをデバイスにプッシュし、テンプレートをデバイスに再アタッチします。

9. **[Save]** をクリックします。

10. （オプション）このテンプレートにさらに多くのアナログまたは PRI ISDN デジタルインターフェイスを設定する場合は、次のようにします。

    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] は [Feature] と呼ばれます。

    3. 設定するテンプレートの [...] をクリックし、[Edit] をクリックします。
    4. ステップ 7、またはステップ 8、およびステップ 9 を繰り返します。

コールルーティング機能テンプレートの追加

コールルーティング機能テンプレートは、電話料金詐欺を防止するための信頼できる IP アドレスやダイヤルプランなど、TDM-SIP トランキングのパラメータを設定します。ダイヤルプランは、ダイヤルピアで構成され、ルータが音声ポートから PSTN または別のブランチへのトラフィック、およびその逆方向のトラフィックをルーティングする方法を定義します。

次の表では、コールルーティングを設定するためのグローバルオプションについて説明します。

表 *64 :* グローバル コール ルーティング オプション

オプション	説明	Cisco IOS CLI での同等コマンド
Trusted IPv4 Prefix List	ルータが SIP 経由で通信できる IPv4 アドレスを入力します。 各 IPv4 アドレス形式を CIDR 形式で入力します。たとえば、10.1.2.3/32 です。カンマ（,）で各アドレスを区切ります。 ルータは他の IPv4 アドレスと通信しないため、ルータを介した不正コールが防止されます。 TDM から IP へのコールには、信頼できる IPv4 プレフィックスが必要です。	**voice service voip** **ip address trusted list** **ipv4** *ipv4-address*/*ipv4-network-mask*
Trusted IPv6 Prefix List	ルータが SIP 経由で通信できる IPv6 アドレスを入力します。 カンマ（,）で各 IPv6 アドレスを区切ります。 ルータは他の IPv6 アドレスと通信しないため、ルータを介した不正コールが防止されます。 TDM から IP へのコールには、信頼できる IPv6 プレフィックスが必要です。	**voice service voip** **ip address trusted list** **ipv6** *ipv6-prefix*//*prefix-length*
Source Interface	ルータが SIP 制御およびメディアトラフィックを開始する送信元インターフェイスの名前を入力します。 この情報で、このトラフィックへの返信や応答の送信方法を定義します。	**voice service voip** **sip** **bind control source-interface** *interface-id* **bind media source-interface** *interface-id*

次の表に、ダイヤルピアの設定オプションを示します。

表 *65*：ダイヤルピアオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Voice Dial Peer Tag	ダイヤルピアの参照に使用する番号を入力します。	**dial-peer voice** *number* {**pots** | **voip**}
Dial Peer Type	作成するダイヤルピアのタイプを選択します（[POTS] または [SIP]）。	**dial-peer voice** *number* {**pots** | **voip**}
方向	このダイヤルピアのトラフィックの方向を選択します（[Incoming] または [Outgoing]）。	Incoming： dial-peer voice *number* {pots | voip} **incoming called-number** *string* Outgoing： dial-peer voice *number* {pots | voip} **destination-pattern** *string*
説明	このダイヤルピアの説明を入力します。	**description**
Numbering Pattern	ダイヤルピアへの着信コールを照合するためにルータが使用する文字列を入力します。 [0-9,A-F#*.?+%()-]*T? の形式で、E.164 形式の正規表現として文字列を入力します。	Incoming： dial-peer voice *number* {pots | voip} **incoming called-number***string* Outgoing： dial-peer voice *number* {pots | voip} **destination-pattern** *string*

オプション	説明	Cisco IOS CLI での同等コマンド
Forward Digits Type	[POTS] ダイヤルピアタイプと [Outgoing] 方向を選択した場合に使用できます。 ダイヤルピアが発信番号内の番号を送信する方法を選択します。 • **All**：ダイヤルピアはすべての番号を送信します • **None**：ダイヤルピアは、宛先パターンに一致しない番号を送信しません • **Some**：ダイヤルピアは、右端から指定された数の桁だけ番号を送信します デフォルト：[None]。	すべて dial-peer voice *number* pots **forward-digits all** [なし（None）]： dial-peer voice *number* pots **forward-digits 0** Some： dial-peer voice *number* pots **forward-digits** *number*
Forward Digits	[Forward Digits Type] で [Some] を選択した場合に使用できます。 送信する発信番号の右端からの桁数を入力します。 たとえば、この値を 7 に設定し、発信番号が 1112223333 の場合、ダイヤルピアは 2223333 を送信します。	dial-peer voice *number* pots **forward-digits** *number*
Prefix	[POTS] ダイヤルピアタイプと [Outgoing] 方向を選択した場合に使用できます。 発信コールのダイヤル文字列に付加する番号を入力します。	dial-peer voice *number* pots **prefix** *string*
トランスポートプロトコル	[Dial Peer Type] で [SIP] を選択した場合に使用できます。 SIP 制御シグナリングのトランスポートプロトコル（[TCP] または [UDP]）を選択します。	dial-peer voice *number* voip **session transport** {**tcp** | **udp**}

オプション	説明	Cisco IOS CLI での同等コマンド
[優先順位（Preference）]	[Dial Peer Type] で [POTS] または [SIP] を選択した場合に使用できます。 0 ～ 10 の整数を選択します。数値が小さいほど優先順位が高くなります。 ダイヤルピアの一致基準が同じ場合、システムは優先順位の値が最も高いものを使用します。 デフォルト：0（優先順位が最も高い）	dial-peer voice *number* voip **preference** *value* dial-peer voice *number* pots **preference** *value*
Voice Port	[POTS] ダイヤルピアタイプを選択した場合に使用できます。 ダイヤルピアへのコールを照合するためにルータが使用する音声ポートを入力します。アナログポートの場合は、必要なポートを入力します。デジタル **T1** PRI ISDN ポートの場合は、サフィックス **23** の付いたポートを入力します。デジタル E1 PRI ISDN ポートの場合は、サフィックス **15** のポートを入力します。 発信ダイヤルピアの場合、ルータはダイヤルピアに一致するコールをこのポートに送信します。 着信ダイヤルピアの場合、このポートは追加の一致基準として機能します。ダイヤルピアは、コールがこのポートに着信した場合にのみ一致します。	dial-peer voice *number* pots アナログポートの場合： **port** *slot*/*subslot*/*port* デジタルポートの場合： **port** *slot*/*subslot*/*port***:15** **port** *slot*/*subslot*/*port***:23**

オプション	説明	Cisco IOS CLI での同等コマンド
宛先アドレス	[SIP] ダイヤルピアタイプと [Outgoing] 方向を選択した場合に使用できます。 ローカル発信 SIP ダイヤルピアが一致した後にコールが送信されるリモート音声ゲートウェイのネットワークアドレスを入力します。 次のいずれかの形式でアドレスを入力します。 • dns:*hostname.domain* • *sip-server* ipv4:*destination-address* ipv6:*destination-address*	**session target** {**ipv4:***destination-address* | **ipv6:***destination-address*| **sip-server** | **dns:***hostname.domain*}

コールルーティング機能テンプレートを追加するには、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. [Feature Templates] をクリックして、[Add 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、[Feature Templates] は [Feature] と呼ばれます。

3. コールルーティング機能を追加するサポート対象デバイスを選択します。
4. [Unified Communications] テンプレートから [Call Routing] をクリックします。
5. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
6. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
7. [Global] で、「グローバル コール ルーティング オプション」の表の説明に従ってオプションを設定します。
8. [Dial Plan] で次の操作のいずれかを実行します。
   - ダイヤルピアを直接設定する場合は、「ダイヤルピアオプション」の表の説明に従ってオプションを設定します。

- ダイヤルピア CSV ファイルを作成または編集する場合は、[Download Dial Peer List] をクリックして、Dial-Peers.csv という名前のシステム提供ファイルをダウンロードします。このファイルを初めてダウンロードしたときは、フィールド名は含まれていますが、レコードは含まれていません。Microsoft Excel などのアプリケーションを使用して、必要に応じてこのファイルを更新します。このファイルの詳細については、「ダイヤルピア CSV ファイル （507 ページ）」を参照してください。
- 作成したダイヤルピア CSV ファイルから設定情報をインポートするには、[Upload Dial Peer List] をクリックします。

ダイヤルピアは必要な数だけ追加できます。各ダイヤルピアを設定したら、[Add] をクリックします。

ダイヤルピアがすでに設定されている場合、それらはこのページのダイヤルピアテーブルに表示されます。設定済みのダイヤルピアを編集するには、[...] をクリックし、鉛筆アイコンをクリックします。表の説明に従ってポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。ダイヤルピアを削除するには、[...] をクリックし、ごみ箱アイコンをクリックします。

9. [Save] をクリックします。

SRST 機能テンプレートの追加

SRST 機能テンプレートは、SIP の Cisco Unified Survivable Remote Site Telephony（SRST）のパラメータを設定します。Cisco Unified SRST を使用すると、WAN がダウンまたは性能低下した場合、ブランチサイトの SIP IP 電話機はローカルゲートウェイに登録できるため、使用できなくなった WAN リソースを必要とせずに、緊急サービスのために引き続き機能できます。

次の表に、Cisco Unified SRST を設定するためのグローバルオプションを示します。

表 *66 : Cisco Unified SRST* のグローバルオプション

オプション	説明	Cisco IOS CLI での同等コマンド
システム メッセージ	Cisco Unified SRST モードが有効なときにエンドポイントに表示されるメッセージを入力します。	**voice register global** **system message** *string*

オプション	説明	Cisco IOS CLI での同等コマンド
Max Phones	Cisco Unified SRST モードのときに、システムがローカルゲートウェイに登録できる電話機の数を入力します。 このフィールドに入力できる使用可能な値と最大値は、設定するデバイスによって異なります。このフィールドの横にある情報アイコンにマウスポインターを合わせると、サポートされているデバイスの最大値が表示されます。	**voice register global** **max-pool** *max-voice-register-pools*
最大電話番号数（Max Directory Numbers）	Cisco Unified SRST モードのときにゲートウェイがサポートする DN の数を入力します。 このフィールドに入力できる使用可能な値と最大値は、設定するデバイスによって異なります。[Max phones to support] フィールドの横にある情報アイコンにマウスポインターを合わせると、サポートされているデバイスの最大値が表示されます。	**voice register global** **max-dn** *max-directory-numbers*
保留音（Music On Hold）	[Yes] を選択すると、Cisco Unified SRST モードで発信者が保留になっているときに、エンドポイントで保留音が再生されます。そうしない場合は、[いいえ（No）] を選択します。	—
Music on Hold file	保留音のオーディオファイルのパスとファイル名を入力します。 ファイルはシステムフラッシュ内にあり、.au または .wav 形式である必要があります。また、このファイル形式には 8 ビット 8 kHz データ（CCITT a-law または u-law データ形式など）が含まれている必要があります。	**call-manager-fallback** **moh** *filename*

次の表に、Cisco Unified SRST 電話機プロファイルを設定するためのオプションを示します。

表 *67 : SRST* 電話機プロファイルオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Voice Register Pool Tag	設定する IP 電話機の一意のシーケンス番号を入力します。 最大値は、SRST 機能テンプレートの [Global] タブにある [Max phones to support] オプションによって定義されます。	**voice register pool** *pool-tag*
Device Network IPv6 Prefix	サポートする IP 電話機を含むネットワークの IPv6 プレフィックスを入力します。 たとえば、a.b.c.d/24 です。	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]
Device Network IPv4 Prefix	サポートする IP 電話機を含むネットワークの IPv4 プレフィックスを入力します。	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]

SRST 機能テンプレートを追加するには、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. [Feature Templates] をクリックして、[Add 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、[Feature Templates] は [Feature] と呼ばれます。

3. Cisco Unified SRST 機能を追加するサポート対象デバイスを選択します。
4. Unified Communications テンプレートで [SRST] をクリックします。
5. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
6. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
7. [Global Settings] で、「グローバル SRST オプション」の表の説明に従ってオプションを設定します。
8. [Phone Profile] で、[New Phone Profile] をクリックして電話機プロファイルを作成し、「SRST 電話機プロファイルオプション」の表の説明に従ってオプションを設定します。

電話機プロファイルには、SIP 電話機のプールタグとデバイスネットワーク情報を指定します。

電話機プロファイルは必要な数だけ追加できます。各電話機プロファイルを設定したら、[Add] をクリックします。

電話機プロファイルがすでに設定されている場合は、このページの電話機プロファイルテーブルに表示されます。設定済みの電話機プロファイルを編集するには、[…] をクリックして、鉛筆アイコンをクリックします。表の説明に従ってポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。電話機プロファイルを削除するには、[…] をクリックし、ごみ箱アイコンをクリックします。

9. [Save] をクリックします。

DSPFarm 機能テンプレートの追加

DSP ファームは、ルータ上の DSP リソースのプールです。Cisco SD-WAN は、Cisco Unified Communications Manager が制御するトランスコーディング、会議（非セキュアのみ）、およびメディア ターミネーション ポイント（MTP）サービスのために Cisco Unified Communications Manager で使用可能な DSP ファームリソースを使用します。Cisco Unified Communications Manager は、コールパスで必要に応じてこれらのリソースを動的に呼び出します。

DSPFarm 機能テンプレートは、DSP ファームのセットアップとプロビジョニングに使用されます。テンプレートは、専用 DSP モジュールのみをサポートします。T1/E1 モジュールはサポートされていません。

DSPFarm 機能テンプレートを追加するときは、次の項目のオプションを構成します。

- メディアリソースモジュール：DSP モジュールとルータ上のそれらの配置。メディアリソースモジュールに基づいて DSP ファームプロファイルを決定および構築します。
- DSP ファームプロファイル：各プロファイルは、特定の DSP ファームサービスタイプをプロビジョニングするためのパラメータを定義します。プロファイルには、トランスコーディング、会議（非セキュアな会議のみがサポートされます）、または MTP サービスに使用される DSP リソースのグループをプロビジョニングするためのオプションが含まれています。Cisco Unified Communications Manager が必要に応じてサービスのリソースを呼び出すことができるように、プロファイルは Cisco Unified Communications Manager に登録されます。
- SCCP 設定：最大 4 つの Cisco Unified Communications Manager サーバーとの通信に使用されるローカルインターフェイスを設定し、DSP ファームプロファイルを Cisco Unified Communications Manager に登録するために必要な関連情報を設定します。また、1 つ以上の Cisco Unified Communications Manager グループを設定します。各グループには、サーバーに関連付けられている DSP ファームサービスを制御する最大 4 つの Cisco Unified Communications Manager サーバーが含まれます。

メディアリソースモジュールを追加すると、Cisco vManage はモジュールの使用可能なスロットとサブスロットを表示することにより、モジュールの配置を支援します。Cisco vManage は、デバイスモデルに基づいて使用可能なスロットとサブスロットを決定します。

次の表に、メディアリソースの設定オプションを示します。

表 *68 :* メディアリソースのオプション

オプション	説明	Cisco IOS CLI での同等コマンド
モジュール	DSPFarm プロファイルで使用される DSP リソースを伝送するルータリソースモジュールを選択します。	—
スロット/サブスロット ID	選択したリソースモジュールが存在するスロットとサブスロットを選択します。	**voice-card** *slot*/*subslot* **dsp service dspfarm**

次の表に、DSP ファームサービスの設定オプションを示します。

表 *69 : DSP* ファームサービスのオプション

オプション	説明	Cisco IOS CLI での同等コマンド
プロファイルタイプ	このプロファイルの対象となる DSP ファームサービスのタイプを選択します。オプションは、[Transcoder]、[Conference] および [MTP] です	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**}
プロファイル ID	プロファイルのシステム生成の一意の識別子。	—
Universal	[Profile Type] で [Transcoder] を選択した場合に使用可能 このチェックボックスがオフの場合、トランスコーディングは G.711 コーデックと他のコーデックの間でのみ許可されます。 このチェックボックスがオンの場合、トランスコーディングは任意のタイプのコーデック間で許可されます。	**dspfarm profile** *profile-identifier* **transcode** [**universal**]

オプション	説明	Cisco IOS CLI での同等コマンド
リストコーデック		**codec** *codec-name*

オプション	説明	Cisco IOS CLI での同等コマンド

	このプロファイルが定義する DSP ファームサービスで使用できるコーデックを選択します。
	
	次のコーデックがサポートされています。[MTP] プロファイルタイプの場合、1つのオプションを選択するか、[pass-through] と他の 1 つのオプションを選択できます。コーデックを変更する場合は、現在のコーデックの選択を解除してから、新しいコーデックを選択してください。
	
	• [Transcoder] プロファイルタイプの場合：
	  • g711alaw
	  • g711ulaw
	  • g729abr8
	  • g729ar8
	  • g729br8
	  • g729r8
	  • g722-64
	  • ilbc
	  • iSAC
	  • pass-through
	
	• [Conference] プロファイルタイプの場合：
	  • g711alaw
	  • g711ulaw
	  • g722r-64
	  • g729abr8
	  • g729ar8
	  • g729br8	

オプション	説明	Cisco IOS CLI での同等コマンド
	• g729r8 • ソフトウェア MTP 専用の [MTP] プロファイルタイプの場合： • g711ulaw • g711alaw • g722-64 • g729abr8 • g729ar8 • g729br8 • g729r8 • ilbc • iSAC • pass-through • ハードウェア MTP 専用、またはハードウェアおよびソフトウェア MTP 用の [MTP] プロファイルタイプの場合： • g711ulaw • g711alaw • pass-through	
会議の最大参加者数	[Profile Type] で [Conference] を選択した場合に使用できます。 会議ブリッジに参加できる最大パーティ数を選択します（[8]、[16]、または [32]）。	**maximum conference-participants** *number*

オプション	説明	Cisco IOS CLI での同等コマンド
Maximum Sessions	[Profile Type] で [Transcoder] または [Conference] を選択した場合に使用できます。 このプロファイルでサポートされる最大セッション数を指定します。 この値は、ルータで使用可能な DSP リソースで設定できる最大セッション数によって異なります。これらのリソースは、ルータのモジュールのタイプに基づいています。これらのリソースを決定するには、DSP 計算機を使用できます。	**maximum sessions** *number*
MTP タイプ	[Profile Type] で [MTP] を選択した場合に使用できます。 ルータが G.711alaw から G.711ulaw へのマイナー MTP トランスレーション、および DTMF 変換を実行する方法を選択します。 次のオプションがあります。 • [Hardware]：MTP トランスレーションおよび変換は、ハードウェア DSP リソースによって実行されます • [Software]：MTP トランスレーションおよび変換は、ルータ CPU によって実行されます	**maximum session** {**hardware** | **software**}

オプション	説明	Cisco IOS CLI での同等コマンド
MTP 最大ハードウェアセッション	[MTP Type] で [Hardware] を選択した場合に使用できます。 MTP トランスレーションおよび変換に使用できるハードウェアセッションの最大数を選択します。 最大値：4000	**maximum session hardware** *number*
MTP 最大ソフトウェアセッション	[MTP Type] で [Software] を選択した場合に使用できます。 MTP トランスレーションおよび変換に使用できる CPU セッションの最大数を選択します。 最大値：6000	**maximum session software** *number*
アプリケーション	デバイスにプロビジョニングされている DSP ファームサービスが関連付けられているアプリケーションのタイプを選択します。	**associate application sccp**
シャットダウン	このオプションを有効にすると、このプロファイルのサービスが停止します。	**shutdown**

次の表に、SCCP の設定オプションを示します。

表 *70 : SCCP* のオプション

オプション	説明	Cisco IOS CLI での同等コマンド
[CUCM] タブ [Profile] タブで定義したプロファイルが登録される最大 12 の Cisco Unified Communications Manager サーバーを設定します。		

オプション	説明	Cisco IOS CLI での同等コマンド
Local Interface	SCCP アプリケーションに関連付けられた DSP サービスが Cisco Unified Communications Manager に登録するために使用するローカルインターフェイスを入力します。 次の形式でインターフェイスを入力します。 ***interface-type/interface-number/port*** 引数の説明 • interface-type：Cisco Unified Communications Manager に登録するためにサービスが使用するインターフェイスのタイプ。タイプは、ギガビットイーサネット インターフェイスまたはポートチャネル インターフェイスです。 • interface-number：Cisco Unified Communications Manager に登録するためにサービスが使用するインターフェイスの番号。 • port：（オプション）インターフェイスが Cisco Unified Communications Manager と通信するポート。ポートを指定しない場合、デフォルト値の 2000 が使用されます。 例：**GigabitEthernet0/0/0**	**sccp local** *interface-type interface-number* [**port** *port-number*]

オプション	説明	Cisco IOS CLI での同等コマンド
サーバーリスト - x	[Profile] タブで定義したプロファイルが登録される Cisco Unified Communications Manager サーバーを指定します。 このフィールドに、Cisco Unified Communications Manager サーバーの IP アドレスまたは DNS 名を入力します。 2 番目のフィールドに、Cisco Unified Communications Manager サーバーの数値識別子を入力します。 プラス記号アイコン（+）をクリックして、最大 11 の追加サーバーを構成します。サーバーを削除するには、対応するマイナス記号アイコン（–）をクリックします。	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* **version 7.0+**
[CUCM Groups] タブ このタブは、[Cisco Unified Communications Manager] タブで少なくとも 1 つの Cisco Unified Communications Manager サーバーが設定されている場合に使用できます。 Cisco Unified Communications Manager グループを設定します。これには、サーバーに関連付けられている DSP ファームサービスを制御する最大 4 つの Cisco Unified Communications Manager サーバーが含まれます。 いずれかの Cisco Unified Communications Manager グループがすでに設定されている場合、それらはこのタブのテーブルに表示されます。設定済みの Cisco Unified Communications Manager グループを編集するには、[Action] 列でそのグループの鉛筆アイコンをクリックし、次の行の説明に従ってポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。Cisco Unified Communications Manager グループを削除するには、[Action] 列でそのグループのごみ箱アイコンをクリックします。		
新しい CUCM グループの追加	クリックして、新しい Cisco Unified Communications Manager グループを追加します。	**sccp ccm group** *group-id*

オプション	説明	Cisco IOS CLI での同等コマンド
サーバーグループの優先順位	この Cisco Unified Communications Manager グループ内の Cisco Unified Communications Manager サーバーが使用される優先順位を選択します。 次の手順を実行します。 **1.** このフィールドをクリックして、[Cisco Unified Communications Manager] タブで設定した Cisco Unified Communications Manager サーバーのリストを表示します。 **2.** プライマリサーバーにするサーバーを選択します。このサーバーの優先度は最高です。 **3.** フィールドをもう一度クリックして、次に優先順位の高い冗長サーバーにするサーバーを選択します。この手順を繰り返して、他の冗長サーバーを選択します。 サーバーは、優先順にこのフィールドに表示されます。 グループからサーバーを削除するには、そのサーバーの [X] アイコンをクリックします。サーバーの優先順位を変更するには、サーバーを削除し、必要な順序でサーバーを追加し直します。	**associate ccm** *cisco-unified-communications-manager-id* **priority** *priority*

オプション	説明	Cisco IOS CLI での同等コマンド
CUCM メディアリソース名 関連付けるプロファイル		**associate ccm** *profile-identifier* **register** *device-name*

オプション	説明	Cisco IOS CLI での同等コマンド
	[Cisco Unified Communications Manager Media Resource Name] フィールドに、DSP ファームプロファイルを Cisco Unified Communications Manager サーバーに登録するために使用される一意の名前を入力します。 名前は 6 ～ 15 文字にする必要があります。文字には、文字、数字、スラッシュ（/）、ハイフン（-）、およびアンダースコア（_）を使用できます。スペースは使用できません。 対応する [Profile to be Associated] フィールドで、入力した名前を使用して、この Cisco Unified Communications Manager グループに登録する DSP ファームプロファイルを選択します。 プロファイルを選択するには、このフィールドをクリックして [Profile] タブで構成したプロファイル ID のリストを表示し、目的のプロファイルの ID をクリックします。 別の Cisco Unified Communications Manager メディアリソース名とプロファイルを追加するには、プラス記号（+）をクリックします。最大 4 つの Cisco Unified Communications Manager メディアリソースとプロファイルを追加できます。 Cisco Unified Communications Manager メディアリソース名とプロファイルを削除するには、それに対応するマイナス記号（–）をクリックします。	

オプション	説明	Cisco IOS CLI での同等コマンド
CUCM スイッチバック	この Cisco Unified Communications Manager グループ内の Cisco Unified Communications Manager サーバーがフェールオーバー後にスイッチバックするために使用するスイッチバック方式を選択します。 • [graceful]：すべてのアクティブセッションが正常に終了した後にスイッチバックが発生します。 • [guard]：アクティブセッションの正常終了、または保護タイマーの時間切れの、どちらかが先に発生したときにスイッチバックが発生します。 • [immediate]：アクティブな接続があるかどうかに関係なく、タイマーが時間切れになるとすぐに、Cisco Unified Communications Manager が優先順位の高い Cisco Unified Communications Manager にスイッチバックします。 デフォルト：[graceful]。	**switchback method** {**graceful** | **guard** [*timeout-guard-value*] | **immediate**}

オプション	説明	Cisco IOS CLI での同等コマンド
CUCM スイッチオーバー	この Cisco Unified Communications Manager グループ内の Cisco Unified Communications Manager サーバーがフェールオーバー時に使用するスイッチオーバー方法を選択します。 • [graceful]：すべてのアクティブセッションが正常に終了した後にスイッチバックが発生します。 • [immediate]：アクティブな接続があるかどうかにかかわらず、スイッチオーバーはすぐに発生します。 デフォルト：[graceful]。	**switchover method** {**graceful** | **immediate**}

DSPFarm 機能テンプレートを追加するには、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. [Feature Templates] をクリックし、[Add 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、[Feature Templates] は [Feature] と呼ばれます。

3. DSP ファームを追加するサポートされているデバイスを選択します。
4. [Unified Communications] テンプレートから [DSPFarm] をクリックします。
5. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
6. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
7. [Media Resources Modules] で、[Add Media Resources] をクリックし、「メディアリソースのオプション」の表の説明に従ってオプションを構成します。

メディアリソースモジュールは、DSP ファームプロファイルによって使用される DSP モジュールです。

必要なだけメディア リソース インターフェイスを追加できます。

各メディアリソースを構成したら、[Add] をクリックします。他の構成アイテムはモジュールとその配置に基づいているため、メディアリソースを構成した後、それを変更または削除することはできません。メディアリソース構成を変更する必要がある場合は、DSPFarm 機能テンプレートを削除して、新しいテンプレートを作成する必要があります。

メディアリソースがすでに構成されている場合は、このタブのテーブルに表示されます。構成されたメディアリソースを編集するには、[…] をクリックし、その鉛筆アイコンをクリックします。「メディアリソースのオプション」の表の説明に従って、ポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。メディアリソースを削除するには、[…] をクリックし、そのごみ箱アイコンをクリックします。

8. [Profile] で、[Add New Profile] をクリックしてルータに DSP ファームサービスのプロファイルを追加し、「DSP ファームサービスのオプション」の表の説明に従って、プロファイルのオプションを構成します。

プロファイルを構成したら、[Add] をクリックします。機能テンプレートごとに最大 10 個の DSP ファームプロファイルを追加できます。

プロファイルを作成する前に、ルータで使用可能な DSP リソースで構成できるセッションの最大数を知っておく必要があります。これらのリソースは、ルータのモジュールのタイプに基づいています。これらのリソースを決定するには、DSP 計算機を使用できます。

プロファイルを追加した後、リストコーデック、最大セッション数、最大会議参加者、およびシャットダウンオプションを変更できます。プロファイルタイプを変更することはできません。プロファイルタイプを変更する場合は、プロファイルを削除して新しいプロファイルを作成する必要があります。

プロファイルがすでに構成されている場合は、このタブのテーブルに表示されます。構成されたプロファイルを編集するには、[…] をクリックし、その鉛筆アイコンをクリックします。「DSP ファームサービスのオプション」の表の説明に従って、ポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。プロファイルを削除するには、[…] をクリックし、そのごみ箱アイコンをクリックします。

9. [SCCP Config] で、「SCCP のオプション」の表の説明に従ってオプションを設定します。

10. [Save] をクリックします。

音声ポリシーの追加

音声ポリシーは、システムがさまざまなエンドポイントタイプのコールを拡張および操作する方法を定義します。エンドポイントには、音声ポート、POTS ダイヤルピア、SIP ダイヤルピ

ア、および Cisco Unified SRST 電話機プロファイルが含まれます。音声ポリシーには、設定する各エンドポイントのサブポリシーが含まれます。

音声ポリシーを追加するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Configuration]** > **[Unified Communications]** を選択します。
2. [Add Voice Policy] をクリックします。
3. [Voice Policy Name] に、ポリシーの名前を入力します。
4. 必要に応じて以下を設定します。
   - [Voice Ports]：音声ポリシーの音声ポートの設定 （453 ページ）を参照してください。
   - [POTS Dial Peers]：音声ポリシーの POTS ダイヤルピアの設定 （474 ページ）を参照してください。
   - [SIP Dial Peers]：音声ポリシーの SIP ダイヤルピアの設定 （484 ページ）を参照してください。
   - [SRST Phones]：音声ポリシーの SRST 電話機の設定 （502 ページ）を参照してください。
5. [Save Policy] をクリックします。

音声ポリシーの音声ポートの設定

音声ポリシーの音声ポートを設定するときは、システムが音声ポートのエンドポイントタイプのコールを拡張および操作する方法を定義するオプションを設定します。

使用している音声カードのタイプに応じて、次のコール機能ポリシーオプションを設定できます。

- **Trunk Group**：次のオプションを使用して、カードのトランクグループのメンバーとして音声ポートを設定します。音声カードに 1 つのトランクグループを設定できます。このオプションについて、次の表で説明します。

表 *71* : 音声ポートのトランクグループオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Trunk Group	クリックして、選択したカードのトランクグループを追加します。 音声ポートごとに 1 つのトランクグループを追加できます。	—

オプション	説明	Cisco IOS CLI での同等コマンド
Copy from Existing	クリックして、既存のトランクグループを新しいトランクグループにコピーします。表示されるボックスで、必要に応じて名前を変更し、トランクグループを選択して、[Copy] をクリックします。	—
名前	トランクグループの名前。 名前には最大 32 文字を使用できます。	**trunk group** *name*

オプション	説明	Cisco IOS CLI での同等コマンド
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

オプション	説明	Cisco IOS CLI での同等コマンド
	発信コールのトランクグループで次のハントスキームを選択します。 • **least-idle both**：アイドル時間が最短のアイドルチャネルを検索します • **least-idle even**：アイドル時間が最短の偶数番号のアイドルチャネルを検索します • **least-idle odd**：アイドル時間が最短の奇数番号のアイドルチャネルを検索します • **least-used both**：使用可能なチャネルの数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **least-used even**：使用可能な偶数番号のチャネル数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **least-used odd**：使用可能な奇数番号のチャネル数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **longest-idle both**：アイドル時間が最長の奇数番号のアイドルチャネルを検索します • **longest-idle even**：使用可能な偶数番号のチャネル数が最も多いアイドルチャネルを検索します • **longest-idle odd**：使用可能な奇数番号のチャネル数が最も多いアイドルチャネルを検索します • **round-robin both**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、ア	

オプション	説明	Cisco IOS CLI での同等コマンド
	イドルチャネルのトランクグループメンバーを順番に検索します • **round-robin even**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、偶数番号のアイドルチャネルのトランクグループメンバーを順番に検索します • **round-robin odd**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、奇数番号のアイドルチャネルのトランクグループメンバーを順番に検索します • **sequential-both**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、アイドルチャネルを検索します • **sequential-even**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、偶数番号のアイドルチャネルを検索します • **sequential-odd**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、奇数番号のアイドルチャネルを検索します • **random**：トランクグループメンバーをランダムに検索し、メンバーからランダムにチャネルを選択します デフォルト：**least-used both**	

オプション	説明	Cisco IOS CLI での同等コマンド
コールの最大数（Max Calls）	トランクグループに許可されるコールの最大数を入力します。値を入力しない場合、コール回数に制限はありません。 コールの最大数に達すると、トランクグループはそれ以上のコールに使用できなくなります。 • [In] フィールド：このトランクグループに許可される着信コールの最大数を入力します • [Out] フィールド：このトランクグループに許可される発信コールの最大数を入力します 両方のフィールドの有効な範囲：0 ～ 1000 の整数。	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]
Max-Retry	発信コールが失敗した場合にトランクグループが行う発信コールの最大試行回数を選択します。 値を入力しないでコールが失敗した場合、システムはコールを再試行しません。 有効な範囲：1 ～ 5 の整数	**trunk group** *name* **max-retry** *attempts*
Save Trunk Group	クリックして、設定したトランクグループを保存します。	—

- **Translation Profile**：次のオプションを使用して、発信番号と着信番号の変換ルールを設定します。このオプションについて、次の表で説明します。

表 *72*：発信者番号と着信者番号の変換プロファイルオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Translation Profile	クリックして、選択したカードの変換プロファイルを追加します。 このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。	**voice translation-profile** *name*

オプション	説明	Cisco IOS CLI での同等コマンド
Copy from Existing	クリックして、既存の変換プロファイルを新しい変換プロファイルにコピーします。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。	—
発信	クリックして、発信元の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate calling** *translation-rule-number*
コール済み	クリックして、着信側の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate called** *translation-rule-number*

オプション	説明	Cisco IOS CLI での同等コマンド
[Translation Rules] ペイン		**voice translation-rule** *number* 一致および置換ルール： **rule** *precedence /match-pattern/ / replace-pattern/* 拒否ルール： **rule** *precedence* **reject** */match-pattern/*

オプション	説明	Cisco IOS CLI での同等コマンド
	1. [Add New] をクリックして、変換ルールを作成します。 または、[Copy From Existing] をクリックして、既存の変換ルールを新しい変換ルールにコピーすることもできます。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。 2. [Translation Rule Number] フィールドに、このルールの優先順位を指定する一意の番号を入力します。有効な範囲：1 ～ 100 の整数 3. （オプション）CSV ファイルから既存の変換ルールをコピーするには、[Import] をクリックします。ルールの追加を続行するか、[Finish] をクリックします。このファイルの詳細については、「変換ルール CSV ファイル（508 ページ）」を参照してください。 4. [Add Rule] をクリックします。 5. [Match] フィールドに、変換ルールを適用する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で文字列を入力します。たとえば、/^9/。 一致文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 6. [Action] ドロップダウンリストから、[Match] フィールドの文字列に一致するコールに対してシステムが実行するアクション	

オプション	説明	Cisco IOS CLI での同等コマンド
	を選択します。[Reject] オプションを使用すると、システムはコールを拒否します。[Replace] オプションを使用すると、システムは一致番号を指定した値に置き換えます。 **7.** [Replace] アクションを選択した場合は、表示される [Replace] フィールドに、一致した文字列を変換する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で数値を入力します。たとえば、//は、文字列なしに置換することを意味します。 置換文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 たとえば、一致文字列として /^9/ を、置換文字列として // を指定すると、システムは、9 で始まる番号を持つコールから先頭の 9 を削除します。この場合、システムは 914085551212 を 14085551212 に変換します。 **8.** **[Save]** をクリックします。 **9.** 必要に応じて、さらに変換ルールを追加します。 **10.** （オプション）[Export] をクリックして、作成した変換ルールを CSV ファイルに保存します。 **11.** ペインの下部にある [Finish] をクリックします。	

- **Station ID**：次のオプションを使用して、発信者 ID 表示の名前と番号を設定します。このオプションについて、次の表で説明します。

表 *73* : ステーション *ID* オプション

オプション	説明	Cisco IOS CLI での同等コマンド
ステーション名（Station Name）	ステーション名を入力します。 ステーション名には、英字、数字、スペース、ダッシュ（-）、下線（_）を使用して最大50文字を入力できます。	**station-id name** *name*
Station Number	ステーションの電話番号を E.164 形式で入力します。 ステーション番号には、最大15文字の数字を使用できます。	**station-id number** *number*

- **Line Params**：次のオプションを使用して、音声品質に関する回線パラメータをカードに設定します。このオプションについて、次の表で説明します。

表 *74* : 回線パラメータオプション

オプション	説明	Cisco IOS CLI での同等コマンド
利得	音声入力のゲインをdB単位で入力します。 有効な範囲：–6 ～ 14。デフォルト：0	**input gain** *decibels*
Attenuation	送信音声出力の減衰量をdB単位で入力します。 有効な範囲：–6 ～ 14。デフォルトは3です。	**output attenuation** *decibels*
エコー キャンセラ	[Enable] を選択すると、エコーキャンセルを音声トラフィックに適用します。 デフォルトで、このオプションは有効になっています。	**echo-cancel** *enable*
音声アクティビティ検出（VAD）	[Enable] を選択すると、VAD を音声トラフィックに適用します。 デフォルトで、このオプションは有効になっています。	**vad**

オプション	説明	Cisco IOS CLI での同等コマンド
Compand Type	PCM システムのアナログ/デジタル信号間の変換に使用されるコンパンディング標準を選択します（**U-law** または **A-law**）。 デフォルト：U-Law。	**compand-type** {**u-law** | **a-law**}
インピーダンス	このフィールドは、PRI ISDN カードには適用されません。 コールの終端インピーダンスを選択します。 デフォルト：600r。	**impedance** {**600c** | **600r 900c** | **900r** | **complex1** | **complex2** | **complex3** | **complex4** | **complex5** | **complex6**}
コール プログレス トーン（Call Progress Tone）	コールプログレストーンのロケールを選択します。	**cptone** *locale*

- **Tuning Params**：次のオプションを使用して、音声ポートと別の機器間のシグナリングのパラメータを設定します。このオプションについて、次の表で説明します。

表 *75:* チューニング パラメータ オプション

オプション	説明	Cisco IOS CLI での同等コマンド
FXO カードのチューニング パラメータ オプション		
Pre Dial Delay	オフフック状態の開始から DTMF シグナリングの開始までの FXO インターフェイスでの遅延を秒単位で入力します。 有効な範囲：0 ～ 10。デフォルト：1。	**pre-dial-delay** *seconds*

オプション	説明	Cisco IOS CLI での同等コマンド
監視式のコール切断	コールが解放され、接続を切断する必要があることを示すトーンの種類を選択します。 • **Anytone**：任意のトーンで監視式のコール切断を示します • **Signal**：切断信号で監視式のコール切断を示します • **Dualtone**：デュアルトーンで監視式のコール切断を示します デフォルト：Signal。	Anytone： supervisory disconnect **anytone** Signal： supervisory disconnect Dualtone： supervisory disconnect **dualtone** {**mid-call** | **pre-connect**}
ダイヤル タイプ（Dial Type）	発信コールのダイヤル方式を選択します。 • **pulse**：パルスのダイヤラ • **dtmf**：デュアルトーン多重周波数ダイヤラ • **mf**：多重周波数ダイヤラ デフォルト：dtmf。	**dial-type** {**dtmf** | **pulse** | **mf**}
Timing Sup-Disconnect	（PSTN または PBX によって通知された電力拒否に基づいて）監視式のコール切断が発生する前に、オンフック指示が意図的なものであり、回線上の電気的過渡現象ではないことの確認に必要な最小時間をミリ秒単位で入力します。 有効な範囲：50 ～ 1500。デフォルト：350。	**timing sup-disconnect** *milliseconds*

オプション	説明	Cisco IOS CLI での同等コマンド
Battery Reversal	バッテリ反転では、コールが接続されたときにPBXのバッテリの極性が逆になり、遠端が切断されたときにバッテリの極性が通常に戻ります。 [Answer] を選択して、バッテリ反転の検出による応答監視をサポートするようにポートを設定します。 [Detection Delay] を選択して、カードでバッテリ反転信号が確認されるまでの遅延時間を設定し、ミリ秒単位で遅延時間を入力します。有効な範囲：0 ～ 800。デフォルト：0（遅延なし）。 FXOポートまたはそのピアFXSポートがバッテリ反転をサポートしていない場合は、予期しない動作を避けるためにバッテリ反転オプションを設定しないでください。	**battery-reversal** [**answer**] **battery-reversal-detection-delay** *milliseconds*
Timing Hookflash out	ゲートウェイがFXOインターフェイスで生成するフックフラッシュ通知の期間をミリ秒単位で入力します。 有効な範囲：50 ～ 1550。デフォルト：400。	**timing hookflash-out** *milliseconds*
Timing Guard out	コールが切断されてから別の発信コールが許可されるまでの期間をミリ秒単位で入力します。 有効な範囲：300 ～ 3000。デフォルトは 2000 です。	**timing guard-out** *milliseconds*
FXS カードのチューニング パラメータ オプション		

オプション	説明	Cisco IOS CLI での同等コマンド
Timing Hookflash In	FXS カードによってフックフラッシュと解釈されるオンフック状態の最小および最大期間をミリ秒単位で入力します。 最小期間の有効な範囲：0 ～ 400。デフォルトの最小値：50。 最大期間の有効な範囲：50 ～ 1500。デフォルトの最大値：1000。	**timing hookflash-in** *maximum-milliseconds minimum-milliseconds*
Pulse Digit Detection	コールの開始時にパルス桁検出を有効にするには、[Yes] を選択します。 デフォルト：[はい（Yes）]。	**pulse-digit-detection**
Loop Length	FXS ポートでのシグナリングの長さを選択します（**Long** または **Short**）。 デフォルト：Short。	**loop-length** [**long** | **short**]
リング	• **Frequency**：適用時に接続デバイスを鳴らす交流周波数（Hz 単位）を選択します。デフォルト：25。 • **DC Offset**：[Loop Length] が [Long] に設定されている場合にのみ適用されます。電圧のしきい値を選択します。これを下回るとデバイスで呼び出し音がなりません。有効な値：10 ボルト、20 ボルト、24 ボルト、30 ボルト、および 35 ボルト。	**ring frequency** *number* **ring dc-offset** *number*
リンガー等価番号（REN）	このカードが処理するコールの REN を選択します。この数値で、回線上の電話呼び出し音の負荷効果を指定します。 有効な範囲：1 ～ 5。デフォルト：1。	**ren** *number*

- **Supervisory Disconnect**：次のオプションを使用して、監視式のコール切断イベントのパラメータを設定します。このオプションについて、次の表で説明します。

表 *76*：監視式のコール切断オプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Supervisory Disconnect	クリックして監視式のコール切断イベントを追加します。	—
Mode	監視式のコール切断イベントのモードを選択します。 • **Custom CPTone**：監視式のコール切断イベントの cptone 検出パラメータを設定するためのオプションを指定します • **Dual Tone Detection Params**：監視式のコール切断イベントのデュアルトーン検出パラメータを設定するためのオプションを指定します	**voice class custom-cptone** *cptone-name* **voice class dualtone-detect-params** *tag*
Supervisory Name	カスタム CPTone モードに適用されます。監視式のコール切断イベントの名前を入力します。 名前には最大 32 文字を使用できます。有効な文字は、英字、数字、ダッシュ（-）、および下線（_）です。	**voice class custom-cptone** *cptone-name*
Dualtone	カスタム CPTone モードに適用されます。コール切断を発生させるデュアルトーンのタイプを選択します。次のオプションがあります。 • ビジー • Disconnect • Number Unobtainable • サービス停止中（Out of service） • リオーダー • リングバック	**dualtone** {**ringback** |**busy** | **reorder** | **out-of-service** | **number-unobtainable** | **disconnect**}

オプション	説明	Cisco IOS CLI での同等コマンド
Cadence	カスタム CPTone モードに適用されます。コール切断を発生させるデュアルトーンのパルス間隔をミリ秒単位で入力します。オン/オフ値のペアとしてパルスをスペースで区切って入力します。最大 4 つのオン/オフ値のペアをスペースで区切って入力できます。	**cadence** *cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time* [*cycle-3-on-time cycle-3-off-time* [*cycle-4-on-time cycle-4-off-time*]]]
Dualtone Frequency	カスタム CPTone モードに適用されます。デュアルトーンの各トーンの周波数（Hz 単位）を入力します。 各トーンの有効な範囲は 300 ～ 3600 です。	**frequency** *frequency-1* [*frequency-2*]
Supervisory Number	カスタムデュアルトーン検出パラメータモードに適用されます。 デュアルトーン検出パラメータを識別する一意の番号を入力します。 有効な範囲：1 ～ 10000。	**voice class dualtone-detect-params** *tag-number*
Cadence-Variation	カスタムデュアルトーン検出パラメータモードに適用されます。トーンの開始が指定した開始時間と異なっていても検出できる最大時間（ミリ秒単位）を入力します。入力した値に 10 が乗算されます。 有効な範囲：0 ～ 200（単位は 10 ミリ秒）。デフォルト：10。	**cadence-variation** *time*

オプション	説明	Cisco IOS CLI での同等コマンド
周波数	カスタムデュアルトーン検出パラメータモードに適用されます。 • Max Delay：デュアルトーンが検出された後、監視式のコール切断が実行されるまでの最大遅延（ミリ秒単位）を入力します。入力した値に 10 が乗算されます。有効な範囲：0 ～ 100（単位は 10 ミリ秒）。デフォルト：10。 • Max Deviation：各トーンが、設定された周波数とは異なっていても検出される最大偏差（Hz 単位）を入力します。有効な範囲：10 ～ 125。デフォルト：10。 • Max Power：デュアルトーンの電力（dBm0 単位）を入力します。これを上回ると監視式のコール切断が検出されません。有効範囲：0 ～ 20。デフォルト：10。 • Min Power：デュアルトーンの電力（dBm0 単位）を入力します。これを下回ると監視式のコール切断が検出されません。有効な範囲：10 ～ 35。デフォルトは 30 です。 • Power Twist：デュアルトーンの最小電力と最大電力の差（dBm0 単位）を入力します。これを上回ると監視式のコール切断が検出されません。有効な範囲：0 ～ 15。デフォルト：6。	**freq-max-delay** *time* **freq-max-deviation** *hertz* **freq-max-power** *dBm0* **freq-min-power** *dBm0* **freq-power-twist** *dBm0*
Save	クリックして、設定した監視式のコール切断情報を保存します。	—

- **DID Timers**：次のオプションを使用して、DID コールのタイマーを設定します。このオプションについて、次の表で説明します。

表 *77 : DID* タイマーのオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Wait Before Wink	カードがコールを受信した後、DNIS 情報を送信できることをリモート側に通知するためのウィンク信号を送信するまで待機する時間（ミリ秒単位）を入力します。 有効な範囲：100 ～ 6500。デフォルト：550。	**timing wait-wink** *milliseconds*
Wink Duration	カードのウィンク信号の最大時間（ミリ秒単位）を入力します。 有効な範囲：50 ～ 3000。デフォルト：200。	**timing wait-duration** *milliseconds*
Clear Wait	非アクティブな捕捉信号から、カードのコールがクリアされるまでの最小時間（ミリ秒単位）を入力します。 有効な範囲：200 ～ 2000。デフォルト：400。	**timing clear-wait** *milliseconds*
Dial Pulse Min Delay	カードのウィンクと同様のパルス間の時間（ミリ秒単位）を入力します。 有効な範囲：0 または 140 ～ 5000。デフォルト：140。	**timing dial-pulse min-delay** *milliseconds*
Answer Winkwidth	着信捕捉の開始からウィンク信号までの最小遅延時間（ミリ秒単位）を入力します。 有効範囲：110～290。デフォルト：210。	**timing answer-winkwidth** *milliseconds*

音声ポリシーに音声ポートを設定するには、次の手順に従います。

1. Cisco vManage のメニューで、**[Configuration]** > **[Unified Communications]** を選択します。
2. [Add Voice Policy] をクリックし、左側のペインで [Voice Ports] を選択します。
3. [Add Voice Ports Policy Profile] ドロップダウンリストから、[Create New] を選択します。

または、[Copy from Existing] を選択して、既存の音声ポリシーを新しい音声ポリシーにコピーすることもできます。表示されるボックスで、コピーするポリシープロファイルの名前を選択し、必要に応じてプロファイルの新しい名前を入力して、[Copy] をクリックします。

4. ポリシーの対象となる音声ポートのタイプを指定するには、[FXO]、[FXS]、[PRI ISDN]、または [FXS DID] を選択します。

5. 表示されるオプションのリストから、設定するコール機能ポリシーオプションのタイプを選択し、[Next] をクリックします。これらのオプションタイプには、次のものがあります。

   - **Trunk Group**：FXO、FXS、FXS DID、および PRI ISDN カードで使用できます。

     これらのオプションを使用して、カードのトランクグループのメンバーとして音声ポートを設定します。

   - **Translation Profile**：FXO、FXS、PRI ISDN、および FXS DID カードで使用できます。

     これらのオプションを使用して、発信番号と着信番号の変換ルールを設定します。

   - **Station ID**：FXO、FXS、および FXS DID カードで使用できます。

     これらのオプションを使用して、発信者 ID 表示の名前と番号を設定します。

   - **Line Params**：FXO、FXS、PRI ISDN、および FXS DID カードで使用できます。

     これらのオプションを使用して、カードの音声品質に関する回線パラメータを設定します。

   - **Tuning Params**：FXO および FXS カードで使用できます。

     これらのオプションを使用して、音声ポートと別の機器間のシグナリングのパラメータを設定します。

   - **Supervisory Disconnect**：FXO カードで使用できます。

     これらのオプションを使用して、監視式のコール切断イベントのパラメータを設定します。このイベントは、コールが切断されたことを示します。

   - **DID Timers**：FXS DID カードで使用できます。

     これらのオプションを使用して、DID コールのタイマーを設定します。

6. 表示されるページで、必要に応じてタブのオプションを設定します。

   使用できるタブは、選択した音声ポートとコール機能ポリシーオプションのタイプによって異なります。

   - [Trunk Group] オプション：これらのオプションの説明については、「音声ポートのトランクグループオプション」の表を参照してください。

     他の音声カード用にトランクグループがすでに設定されている場合、トランクグループはこのページのトランクグループテーブルに表示されます。設定されたトランク

グループを編集するには、[…] をクリックして、鉛筆アイコンをクリックします。「音声ポートのトランクグループオプション」の表の説明に従って、ポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。トランクグループを削除するには、[…] をクリックして、ごみ箱アイコンをクリックします。

トランクグループオプションを保存するときに [Save Trunk Group] をクリックした後、トランクグループの優先順位を設定するには、[Trunk Group] テーブルでトランクグループの [Priority] フィールドをダブルクリックし、優先順位番号を入力したら **Enter** キーを押すか、または [Priority] フィールドの外側をクリックします。有効な優先順位番号は、1 ～ 64 の整数です。入力する番号は、着信コールと発信コールのトランクグループにおける POTS ダイヤルピアの優先順位です。

- [Translation Profile] オプション：これらのオプションの説明については、「発信者番号と着信者番号の変換プロファイルオプション」の表を参照してください。

  変換プロファイルオプションの設定時に [Finish] をクリックした後、次のアクションを実行します。

  1. 必要に応じて、別の変換プロファイルを追加します。このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。
  2. [Save Translation Profile] をクリックします。
  3. 作成する変換プロファイルごとに、変換ルールテーブルの [Direction] 列に表示されるダッシュ（-）をダブルクリックし、表示されるドロップダウンリストから [Incoming] または [Outgoing] を選択します。[Incoming] を選択すると、対応する変換ルールがこのエンドポイントに着信するトラフィックに適用されます。[Outgoing] を選択すると、対応する変換ルールがこのエンドポイントから発信されるトラフィックに適用されます。

- [Station ID] オプション：これらのオプションの説明については、「ステーション ID オプション」の表を参照してください。
- [Line Params] オプション：これらのオプションの説明については、「回線パラメータオプション」の表を参照してください。
- [Tuning Params] オプション：これらのオプションの説明については、「チューニング パラメータ オプション」の表を参照してください。
- [Supervisory Disconnect] オプション：これらのオプションの説明については、「監視式のコール切断オプション」の表を参照してください。

  監視式のコール切断イベントは、必要な数だけ設定できます。
- [DID Timers] オプション：これらのオプションの説明については、「DID タイマー オプション」の表を参照してください。

7. [Next] をクリックします。
8. [Policy Profile Name] に、この子ポリシーの名前を入力します。

9. [Policy Profile Description] に、この子ポリシーの説明を入力します。
10. [Save] をクリックします。

音声ポリシーの POTS ダイヤルピアの設定

音声ポリシーに POTS ダイヤルピアを設定するときは、システムが POTS ダイヤルピアのエンドポイントタイプのコールを拡張および操作する方法を定義するオプションを設定します。

次のオプションを設定できます。

- [Trunk Groups]：以下の表で、それらのオプションについて説明しています。

表 *78 : POTS* ダイヤルピアのトランクグループオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Trunk Group	クリックして、選択したカードのトランクグループを追加します。 音声ポートごとに 1 つのトランクグループを追加できます。	—
Copy from Existing	クリックして、既存のトランクグループを新しいトランクグループにコピーします。表示されるボックスで、必要に応じて名前を変更し、トランクグループを選択して、[Copy] をクリックします。 名前の前に「{Master}」が付いているトランクグループ名は、すでにこの音声ポリシーに関連付けられています。このタイプのトランクグループをコピーすると、システムはトランクグループ定義の別のインスタンスを作成せずに、既存のトランクグループを再利用します。この場合、名前を変更することはできません。	—
名前	トランクグループの名前。 名前には最大 32 文字を使用できます。	**trunk group** *name*

オプション	説明	Cisco IOS CLI での同等コマンド
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle** [**both** | **even** | **odd**] **hunt-scheme least-used** [**both** | **even** | **odd**] **hunt-scheme longest-idle** [**both** | **even** | **odd**] **hunt-scheme round-robin** [**both** | **even** | **odd**] **hunt-scheme sequential** [**both** | **even** | **odd**] **hunt-scheme random**

オプション	説明	Cisco IOS CLI での同等コマンド
	発信コールのトランクグループで次のハントスキームを選択します。 • **least-idle both**：アイドル時間が最短のアイドルチャネルを検索します • **least-idle even**：アイドル時間が最短の偶数番号のアイドルチャネルを検索します • **least-idle odd**：アイドル時間が最短の奇数番号のアイドルチャネルを検索します • **least-used both**：使用可能なチャネルの数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **least-used even**：使用可能な偶数番号のチャネル数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **least-used odd**：使用可能な奇数番号のチャネル数が最も多いトランクグループメンバーを検索します（PRI ISDN カードのみに適用） • **longest-idle both**：アイドル時間が最長の奇数番号のアイドルチャネルを検索します • **longest-idle even**：使用可能な偶数番号のチャネル数が最も多いアイドルチャネルを検索します • **longest-idle odd**：使用可能な奇数番号のチャネル数が最も多いアイドルチャネルを検索します • **round-robin both**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、ア	

オプション	説明	Cisco IOS CLI での同等コマンド
	イドルチャネルのトランクグループメンバーを順番に検索します • **round-robin even**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、偶数番号のアイドルチャネルのトランクグループメンバーを順番に検索します • **round-robin odd**：最後に使用されたメンバーに続くトランクグループメンバーから始めて、奇数番号のアイドルチャネルのトランクグループメンバーを順番に検索します • **sequential-both**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、アイドルチャネルを検索します • **sequential-even**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、偶数番号のアイドルチャネルを検索します • **sequential-odd**：トランクグループ内で最も優先度の高いトランクグループメンバーから始めて、奇数番号のアイドルチャネルを検索します • **random**：トランクグループメンバーをランダムに検索し、メンバーからランダムにチャネルを選択します デフォルト：**least-used both**	

オプション	説明	Cisco IOS CLI での同等コマンド
コールの最大数（Max Calls）	トランクグループに許可されるコールの最大数を入力します。値を入力しない場合、コール回数に制限はありません。 コールの最大数に達すると、トランクグループはそれ以上のコールに使用できなくなります。 • [In] フィールド：このトランクグループに許可される着信コールの最大数を入力します。 • [Out] フィールド：このトランクグループに許可される発信コールの最大数を入力します。 両方のフィールドの有効な範囲：0 ～ 1000 の整数。	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]
Max-Retry	発信コールが失敗した場合にトランクグループが行う発信コールの最大試行回数を選択します。 値を入力しないでコールが失敗した場合、システムはコールを再試行しません。 有効な範囲：1 ～ 5 の整数	**trunk group** *name* **max-retry** *attempts*

• [Translation Profiles]：以下の表は、それらのオプションを示しています。

表 *79 : POTS* ダイヤルピアのトランスレーション プロファイルのオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Translation Profile	クリックして、選択した POTS ダイヤルピアの変換プロファイルを追加します。 このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。	—

オプション	説明	Cisco IOS CLI での同等コマンド
Copy from Existing	クリックして、既存の変換プロファイルを新しい変換プロファイルにコピーします。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。	—
名前	トランスレーション プロファイルの名前。 名前には最大 32 文字を使用できます。	**voice translation-profile** *name*
発信	クリックして、発信元の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate calling** *translation-rule-number*
コール済み	クリックして、着信側の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate called** *translation-rule-number*

オプション	説明	Cisco IOS CLI での同等コマンド
[Translation Rules] ペイン		**voice translation-rule** *number* 一致および置換ルール： **rule** *precedence /match-pattern/ / replace-pattern/* 拒否ルール： **rule** *precedence* **reject** */match-pattern/*

オプション	説明	Cisco IOS CLI での同等コマンド
	1. [Add New] をクリックして、変換ルールを作成します。 または、[Copy From Existing] をクリックして、既存の変換ルールを新しい変換ルールにコピーすることもできます。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。 2. [Translation Rule Number] フィールドに、このルールの優先順位を指定する一意の番号を入力します。有効な範囲：1 ～ 100 の整数 3. （オプション）CSV ファイルから既存の変換ルールをコピーするには、[Import] をクリックします。ルールの追加を続行するか、[Finish] をクリックします。このファイルの詳細については、「変換ルール CSV ファイル（508 ページ）」を参照してください。 4. [Add Rule] をクリックします。 5. [Match] フィールドに、変換ルールを適用する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で文字列を入力します。たとえば、/^9/。 一致文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 6. [Action] ドロップダウンリストから、[Match] フィールドの文字列に一致するコールに対してシステムが実行するアクション	

オプション	説明	Cisco IOS CLI での同等コマンド
	を選択します。[Reject] オプションを使用すると、システムはコールを拒否します。[Replace] オプションを使用すると、システムは一致番号を指定した値に置き換えます。 **7.** [Replace] アクションを選択した場合は、表示される [Replace] フィールドに、一致した文字列を変換する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で数値を入力します。たとえば、//は、置換する文字列がないことを示します。 置換文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 例として、/^9/ の一致文字列と // の置換文字列を指定すると、システムは、9 で始まる番号を持つ呼び出しから先頭の 9 を削除します。この場合、システムは 914085551212 を 14085551212 に変換します。 **8.** **[Save]** をクリックします。 **9.** 必要に応じて、さらに変換ルールを追加します。 **10.** （オプション）[Export] をクリックして、作成した変換ルールを CSV ファイルに保存します。 **11.** ページの下部にある [Finish] をクリックします。	

音声ポリシーの POTS ダイヤルピアを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Configuration]** > **[Unified Communications]** を選択します

2. [Add Voice Policy] をクリックし、左側のペインで [POTS Dial Peer] を選択します。
3. [Add POTS Dial Peer Policy Profile] ドロップダウンリストから、[Create New] を選択します。

   または、[Copy from Existing] を選択して、既存の POTS ダイヤルピアポリシーを新しいポリシーにコピーすることもできます。表示されるボックスで、コピーするポリシープロファイルの名前を選択し、必要に応じてプロファイルの新しい名前を入力して、[Copy] をクリックします。
4. 表示されるオプションのリストから、設定する POTS ダイヤルピアのタイプを選択し、[next] をクリックします。

   オプションは、[Trunk Group]（Cisco IOS XE リリース 17.3.1a で始まる）と [Translation Profile] です。
5. トランクグループを設定するには、次の操作を実行します。

   トランクグループがすでに設定されている場合、トランクグループはこのページのトランクグループテーブルに表示されます。設定されたトランクグループを編集するには、[…] をクリックして、鉛筆アイコンをクリックします。「POTS ダイヤルピアオプションのトランクグループ」の表の説明に従って、ポップアップウィンドウでオプションを編集し、[Save Changes] をクリックします。トランクグループを削除するには、[…] をクリックして、ごみ箱アイコンをクリックします。

   1. 「POTS ダイヤルピアのトランクグループオプション」の表の説明に従って、トランクグループオプションを設定します。
   2. 必要に応じて、別のトランクグループを追加します。

      このエンドポイントに対して最大 64 のトランクグループを作成できます。
   3. [Save Trunk Group] をクリックします。
   4. トランクグループの優先順位を設定するには、[Trunk Group] テーブルでトランクグループの [Priority] フィールドをダブルクリックし、優先順位番号を入力したら Enter キーを押すか、または [Priority] フィールドの外側をクリックします。有効な優先順位番号は、1 ～ 64 の整数です。テーブル内の他のトランクグループについて、このプロセスを繰り返します。入力する番号は、着信コールと発信コールのトランクグループにおける POTS ダイヤルピアの優先順位です。
6. トランスレーション プロファイルを設定するには、次のアクションを実行します。

   1. 「POTS ダイヤルピアのトランスレーション プロファイルのオプション」の表の説明に従って、トランスレーション プロファイルのオプションを設定します。
   2. 必要に応じて、別の変換プロファイルを追加します。

      このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。
   3. [Save Translation Profile] をクリックします。

4. 作成する変換プロファイルごとに、変換ルールテーブルの [Direction] 列に表示されるダッシュ（-）をダブルクリックし、表示されるドロップダウンリストから[Incoming] または [Outgoing] を選択します。

   [Incoming] を選択すると、対応する変換ルールがこのエンドポイントに着信するトラフィックに適用されます。[Outgoing] を選択すると、対応する変換ルールがこのエンドポイントから発信されるトラフィックに適用されます。

7. [Next] をクリックします。
8. [Policy Profile Name] に、この子ポリシーの名前を入力します。
9. [Policy Profile Description] に、この子ポリシーの説明を入力します。
10. [Save] をクリックします。

音声ポリシーの SIP ダイヤルピアの設定

音声ポリシーに SIP ダイヤルピアを設定するときは、システムが SIP ダイヤルピアのエンドポイントタイプのコールを拡張および操作する方法を定義するオプションを設定します。

SIP ダイヤルピアを設定するポリシータイプに応じて、次のオプションを設定できます。

- **Translation Profile**：次のオプションを使用して、SIP ダイヤルピアの着信番号と発信番号の変換ルールを設定します。このオプションについて、次の表で説明します。

表 *80 : SIP* ダイヤルピアの発信番号の変換プロファイルオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Translation Profile	クリックして、選択した SIP ダイヤルピアの変換プロファイルを追加します。 このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。	**voice translation-profile** *name*
Copy from Existing	クリックして、既存の変換プロファイルを新しい変換プロファイルにコピーします。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。	—

オプション	説明	Cisco IOS CLI での同等コマンド
発信	クリックして、発信元の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate calling** *translation-rule-number*
コール済み	クリックして、着信側の番号の変換ルールを設定します。 [Translation Rules] ペインが表示されます。	**translate called** *translation-rule-number*

オプション	説明	Cisco IOS CLI での同等コマンド
[Translation Rules] ペイン		**voice translation-rule** *number* 一致および置換ルール： **rule** *precedence /match-pattern/ / replace-pattern/* 拒否ルール： **rule** *precedence* **reject** */match-pattern/*

オプション	説明	Cisco IOS CLI での同等コマンド
	1. [Add New] をクリックして、変換ルールを作成します。 または、[Copy From Existing] をクリックして、既存の変換ルールを新しい変換ルールにコピーすることもできます。表示されるボックスで、必要に応じて名前を変更し、着信側の変換ルールと発信側の変換ルールを選択して、[Copy] をクリックします。 2. [Translation Rule Number] フィールドに、このルールの優先順位を指定する一意の番号を入力します。有効な範囲：1 ～ 100 の整数 3. （オプション）CSV ファイルから既存の変換ルールをコピーするには、[Import] をクリックします。ルールの追加を続行するか、[Finish] をクリックします。このファイルの詳細については、「変換ルール CSV ファイル（508 ページ）」を参照してください。 4. [Add Rule] をクリックします。 5. [Match] フィールドに、変換ルールを適用する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で文字列を入力します。たとえば、/^9/。 一致文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 6. [Action] ドロップダウンリストから、[Match] フィールドの文字列に一致するコールに対してシステムが実行するアクション	

オプション	説明	Cisco IOS CLI での同等コマンド
	を選択します。[Reject] オプションを使用すると、システムはコールを拒否します。[Replace] オプションを使用すると、システムは一致番号を指定した値に置き換えます。 **7.** [Replace] アクションを選択した場合は、表示される [Replace] フィールドに、一致した文字列を変換する文字列を入力します。スラッシュ（/）で囲んだ正規表現形式で数値を入力します。たとえば、//は、置換する文字列がないことを示します。 置換文字列にバックスラッシュ文字（\）を含めるには、バックスラッシュの前にバックスラッシュを置きます。 たとえば、一致文字列として /^9/ を、置換文字列として // を指定すると、システムは、9 で始まる番号を持つコールから先頭の 9 を削除します。この場合、システムは 914085551212 を 14085551212 に変換します。 **8.** **[Save]** をクリックします。 **9.** 必要に応じて、さらに変換ルールを追加します。 **10.** （オプション）[Export] をクリックして、作成した変換ルールを CSV ファイルに保存します。 **11.** ペインの下部にある [Finish] をクリックします。	

- **Media Profile**：次のオプションを使用して、リモートダイヤルピアとの SIP トランク通信に使用できるコーデックと、SIP コールに使用する DTMF リレーオプションを設定できます。このオプションについて、次の表で説明します。

表 *81* : メディア プロファイル オプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Media Profile	クリックして、ダイヤルピアの変換プロファイルを追加します。	—
Copy from Existing	クリックして、既存のメディアプロファイルを新しいメディアプロファイルにコピーします。表示されるボックスに、プロファイルのメディアプロファイル番号を入力し、[Copy] をクリックします。	—
Media Profile Number	この SIP メディアプロファイルの番号を入力します。 有効な範囲：1 ～ 10000 の整数。	**voice class codec** *tag-number*
コーデック	リモートダイヤルピアとの通信時に SIP トランクが使用できるようにするコーデックを、[Source] リストから [Target] リストに移動します。 ターゲットリストのコーデックは、優先順位の降順に並べられており、リストの一番上にあるものが優先順位が最も高くなります。このリスト内の項目をドラッグアンドドロップして、並べ替えます。	**voice class codec** *tag-number* **codec preference** *value codec-type*

オプション	説明	Cisco IOS CLI での同等コマンド
DTMF	システムで SIP コールに使用する DTMF リレーオプションを [Source] リストから [Target] リストに移動します。 [Target] リストの項目は、優先順位の高い順であり、リストの一番上にあるものが優先順位が最も高くなります。このリスト内の項目をドラッグアンドドロップして、並べ替えます。 [Target] リストに [Inband] オプションを含める場合は、そのリストの唯一のオプションになります。[Target] リストに他のオプションを含める場合は、メディアプロファイルを保存する前に、[Inband] オプションを [Source] リストに移動します。	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	クリックすると、入力した設定値が保存されます。	—

- **Modem Pass-through**：次のオプションを使用して、SIP ダイヤルピアエンドポイントのモデムパススルー機能を設定します。このオプションについて、次の表で説明します。

表 *82 :* モデムパススルーオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Modem Pass-through	クリックして、この SIP ダイヤルピアエンドポイントのモデムパススルーを追加します。	—
Copy from Existing	クリックして、既存のモデムパススルーを新しいモデムパススループロファイルにコピーします。表示されるボックスで、既存のモデムパススルーを選択し、必要に応じて新しい名前を入力して、[Copy] をクリックします。	—

オプション	説明	Cisco IOS CLI での同等コマンド
名前	モデムパススルーの名前。 この名前は、既存のモデム パススルー プロファイルを新しいものにコピーするときに使用されます。	—
プロトコル	モデムパススルーのプロトコルを選択します。 • **None**：デバイスでモデムパススルーが無効になります • **NSE G.711ulaw**：名前付きシグナリングイベント（NSE）を使用して、ゲートウェイ間の G.711ulaw コーデックスイッチオーバーを通信します • **NSE G.711alaw**：名前付きシグナリングイベント（NSE）を使用して、ゲートウェイ間の G.711alaw コーデックスイッチオーバーを通信します	[なし（None）]： **no modem passthrough** NSE G.711 ulaw： **modem passthrough nse codec g711ulaw** NSE G.711 alaw： **modem passthrough nse codec g711alaw**
Save Modem Pass-Through	クリックすると、入力した設定値が保存されます。	—

- **Fax Protocol**：次のオプションを使用して、SIP ダイヤルピアエンドポイントの Fax プロトコル機能を設定します。このオプションについて、次の表で説明します。

表 *83 : Fax* プロトコルオプション

オプション	説明	Cisco IOS CLI での同等コマンド
Add New Fax Protocol	クリックして、ダイヤルピアの Fax プロトコルを追加します。	—
Copy from Existing	クリックして、既存の Fax プロトコルを新しい Fax プロトコルにコピーします。表示されるボックスで、既存の Fax プロトコルを選択し、必要に応じて新しい名前を入力して、[Copy] をクリックします。	—

オプション	説明	Cisco IOS CLI での同等コマンド
名前	Fax プロトコルの名前。 この名前は、既存の Fax プロファイルを新しいFaxプロファイルにコピーするときに使用されます。	—

オプション	説明	Cisco IOS CLI での同等コマンド

プライマリ	一連の Fax プロトコル オプションから選択します。各オプションは、関連する Fax コマンドのバンドルセットです。
	各バンドルの詳細については、「プライマリ Fax プロトコルコマンドバンドル」の表を参照してください。
	バンドルの説明には、次のコンポーネントが含まれます。
	• **nse**：NSE を使用して T.38 Fax リレーモードに切り替えます
	• **force**：無条件に、Cisco Network Services Engine（NSE）を使用して T.38 Fax リレーに切り替えます
	• **version**：Fax 速度を設定するためのバージョンを指定します。
	  • **0**：T.38 バージョン 0（1998 - G3 Fax）を使用するバージョン 0 を設定します
	  • **3**：T.38 バージョン 3（2004 - V.34 または SG3 Fax）を使用するバージョン 3 を設定します
	• **none**：Fax パススルーまたは T.38 Fax リレーは試行されません
	• **Pass-through**：ファクスストリームは、次のいずれかの広帯域幅コーデックを使用します。
	  • **g711ulaw**：G.711 ulaw コーデックを使用します
	  • **g711alaw**：G.711 alaw コーデックを使用します
		fax protocol { **none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**]| **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

オプション	説明	Cisco IOS CLI での同等コマンド
フォールバック	[Primary] フィールドで選択したプライマリ プロトコル バンドル名が「T.38」または「Fax Pass-through」で始まる場合に使用できます。 Fax 送信のフォールバックモードを選択します。このフォールバックモードは、デバイスエンドポイント間でプライマリ Fax プロトコルをネゴシエートできない場合に使用されます。 各オプションの詳細については、「フォールバック プロトコル オプション」の表を参照してください。	**fax protocol** {none | pass-through {g711ulaw | g711alaw} [**fallback none**] | t38 [nse [force]] [version {0 | 3}] [ls-redundancy value [hs-redundancy value]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}
Low Speed	[Primary] フィールドで選択したプライマリ プロトコル バンドル名が「T.38」で始まる場合に使用できます。 低速 V.21 ベースの T.30 Fax マシンプロトコルに送信される冗長 T.38 Fax パケット数を指定します。 範囲：0（冗長性なし）～ 5。デフォルト：0。	**ls-redundancy** *value*
High Speed	[Primary] フィールドで選択したプライマリ プロトコル バンドル名が「T.38」で始まる場合に使用できます。 高速 V.17、V.27、V.29 T.4 または T.6 Fax マシン イメージ データに送信される冗長 T.38 Fax パケット数を指定します。 範囲：0（冗長性なし）～ 2。デフォルト：0	**hs-redundancy** *value*
Save Fax Protocol	クリックすると、入力した設定値が保存されます。	—

次の表では、SIP ダイヤルピアエンドポイントの Fax プロトコル機能を設定するときに、[Primary] オプションで使用できる Fax コマンドのバンドルセットについて説明します。

低速（ls）冗長性の場合、範囲は 0（冗長性なし）～ 5 です。高速（HS）冗長性の場合、範囲は 0（冗長性なし）～ 2 です。

表 *84 :* プライマリ *Fax* プロトコルコマンドバンドル

Fax コマンドプロトコルバンドル	説明	**Cisco IOS CLI** での同等コマンド
T.38 Fax Relay Version 3	プライマリ Fax プロトコルは、T.38 Fax リレーバージョン 3 です。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 3 ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0	プライマリ Fax プロトコルは、T.38 Fax リレーバージョン 0 です。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 3 NSE	プライマリ Fax プロトコルは、NSE ベースの T.38 Fax リレーバージョン 3 です。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 3 nse ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 3 NSE force	プライマリ Fax プロトコルは、T.38 Fax リレーバージョン 3 の NSE 強制オプションです。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 3 nse force ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0 NSE	プライマリ Fax プロトコルは、T.38 Fax リレーバージョン 0 の NSE オプションです。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value*

Fax コマンドプロトコルバンドル	説明	Cisco IOS CLI での同等コマンド
T.38 Fax Relay Version 0 NSE force	プライマリ Fax プロトコルは、T.38 Fax リレーバージョン 0 の NSE 強制オプションです。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 No ECM	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 で、ECM は無効になっています。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE No ECM	プライマリ Fax プロトコルは NSE ベースの T.38 Fax リレーバージョン 0 で、ECM は無効になっています。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE force No ECM	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 の NSE 強制オプションで、ECM は無効になっています。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 Rate 14.4 No ECM	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 で、ECM は無効、Fax 速度は 14,400 bps です。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**

Fax コマンドプロトコルバンドル	説明	Cisco IOS CLI での同等コマンド
T.38 Fax Relay Version 0 NSE Rate 14.4 No ECM	プライマリ Fax プロトコルは NSE ベースの T.38 Fax リレーバージョン 0 で、ECM は無効、Fax 速度は 14,400 bps です。 低速および高速の冗長性値を選択するオプションが使用できます。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4 No ECM	プライマリ Fax プロトコルは NSE フォースオプション T.38 Fax リレーバージョン 0 で、ECM は無効、Fax レートは 14,400 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax リレーバージョン 0 レート 9.6 非 ECM	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 で、ECM は無効、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax リレーバージョン 0 NSE レート 9.6 非 ECM	プライマリ Fax プロトコルは NSE ベースの T.38 Fax リレーバージョン 0 で、ECM は無効、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**

Fax コマンドプロトコルバンドル	説明	Cisco IOS CLI での同等コマンド
T.38 Fax リレーバージョン 0 NSE フォースレート 9.6 非 ECM	プライマリ Fax プロトコルは NSE フォースオプション T.38 Fax リレーバージョン 0 で、ECM は無効、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax リレーバージョン 0 レート 14.4	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 14,400 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax リレーバージョン 0 NSE レート 14.4	プライマリ Fax プロトコルは NSE ベースの T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 14,400 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax リレーバージョン 0 NSE フォースレート 14.4	プライマリ Fax プロトコルは NSE フォースオプション T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 14,400 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**

Fax コマンドプロトコルバンドル	説明	Cisco IOS CLI での同等コマンド
T.38 Fax リレーバージョン 0 レート 9.6	プライマリ Fax プロトコルは T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax リレーバージョン 0 NSE レート 9.6	プライマリ Fax プロトコルは NSE ベースの T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax リレーバージョン 0 NSE フォースレート 9.6	プライマリ Fax プロトコルは NSE フォースオプション T.38 Fax リレーバージョン 0 で、ECM があり、Fax レートは 9,600 bps です。 低速および高速の冗長性値を選択するオプションが利用可能です。	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
なし	Fax プロトコルは無効です。	**fax protocol none**
Fax パススルー G711ulaw	プライマリ Fax プロトコルは Fax パススルーで、パススルーコーデックは g711ulaw に設定されます。	**fax protocol pass-through g711ulaw**
Fax パススルー G711ulaw 非 ECM	プライマリ Fax プロトコルは Fax パススルーで、パススルーコーデックは g711ulaw に設定され、ECM は無効です。	**fax protocol pass-through g711ulaw** **fax-relay ecm disable**
Fax パススルー G711alaw	プライマリ Fax プロトコルは Fax パススルーで、パススルーコーデックは g711alaw に設定されます。	**fax protocol pass-through g711alaw**

Fax コマンドプロトコルバンドル	説明	Cisco IOS CLI での同等コマンド
Fax パススルー G711alaw 非 ECM	プライマリ Fax プロトコルは Fax パススルーで、パススルーコーデックは g711alaw に設定され、ECM は無効です。	**fax protocol pass-through g711alaw** **fax-relay ecm disable**

次の表では、SIP ダイヤルピアエンドポイントの Fax プロトコル機能を設定するとき、フォールバックオプションで使用できる選択肢について説明します。

表 *85 :* フォールバック プロトコル オプション

フォールバック Fax プロトコル オプション	説明	Cisco IOS CLI での同等コマンド
なし	フォールバック Fax プロトコルはなしです。すべての特殊な Fax 処理は無効化されます。	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback none** **fax protocol pass-through** {**g711ulaw** | **g711alaw** } **fallback none**
Fax パススルー G711ulaw	フォールバック Fax プロトコルは Fax パススルーで、パススルーコーデックは g711ulaw に設定されます。	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711ulaw**
Fax パススルー G711alaw	フォールバック Fax プロトコルは Fax パススルーで、パススルーコーデックは g711alaw に設定されます。	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711alaw**

音声ポリシーの SIP ダイヤルピアを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Configuration]** > **[Unified Communications]** を選択します。
2. [SIP Dial Peer] をクリックします。
3. [Add SIP Dial Peer Policy Profile] ドロップダウンリストから、[Create New] を選択します。

   または、[Copy from Existing] を選択して、既存の SIP ダイヤルピアポリシーを新しいポリシーにコピーすることもできます。表示されるボックスで、コピーするポリシープロファイルの名前を選択し、必要に応じてプロファイルの新しい名前を入力して、[Copy] をクリックします。
4. 作成するポリシータイプを選択し、[Next] をクリックします。
   - [Translation Profile]：発信番号と着信番号の変換ルールを設定できます。

- [Media Profile]：リモートダイヤルピアとの SIPtrunk 通信に使用できるコーデックと、SIP コールに使用する DTMF リレーオプションを設定できます。
- [Modem Pass-through]：SIP ダイヤルピアエンドポイントのモデムパススルー機能を設定できます。
- [Fax Protocol]：SIP ダイヤルピアエンドポイントの Fax プロトコル機能を設定できます。この機能は、リモートダイヤルピアとの機能のネゴシエーション時にアドバタイズされ、使用されます。

5. 表示されるページで、必要に応じて、以下の表で説明されているタブのオプションを設定します。

使用できるタブは、選択したポリシータイプによって異なります。

- [Translation Profile] オプション：これらのオプションの説明については、「SIP ダイヤルピアの発信者番号の変換プロファイルオプション」の表を参照してください。

  変換プロファイルの設定時に [Finish] をクリックした後、次のアクションを実行します。

  1. 必要に応じて、別の変換プロファイルを追加します。このエンドポイントに対して最大 2 つの変換プロファイルを作成できます。

  2. [Save Translation Profile] をクリックします。

  3. 作成する変換プロファイルごとに、変換ルールテーブルの [Direction] 列に表示されるダッシュ（-）をダブルクリックし、表示されるドロップダウンリストから [Incoming] または [Outgoing] を選択します。[Incoming] を選択すると、対応する変換ルールがこのエンドポイントに着信するトラフィックに適用されます。[Outgoing] を選択すると、対応する変換ルールがこのエンドポイントから発信されるトラフィックに適用されます。

- [Media Profile] オプション：これらのオプションの説明については、「メディア プロファイル オプション」の表を参照してください。
- [Modem Pass-through] オプション：これらのオプションの説明については、「モデムパススルーオプション」の表を参照してください。
- [Fax Protocol] オプション：これらのオプションの説明については、「Fax プロトコル オプション」の表を参照してください。

6. [Next] をクリックします。

7. [Policy Profile Name] に、この子ポリシーの名前を入力します。

8. [Policy Profile Description] に、この子ポリシーの説明を入力します。

9. [Save] をクリックします。

音声ポリシーの SRST 電話機の設定

音声ポリシーに SRST 電話機を設定するときは、システムが Cisco Unified SRST 電話機エンドポイントタイプのコールを拡張および操作する方法を定義するオプションを設定します。

次の表に、音声ポリシーに SRST 電話機を設定するためのオプションを示します。

表 *86 : SRST* 電話機の設定オプション

オプション	説明	Cisco IOS CLI での同等コマンド
Medial Profile Number	この Cisco Unified SRST メディアプロファイルの番号を入力します。 有効な範囲：1 ～ 10000 の整数。	**voice class codec** *tag-number*
コーデック	電話機が Cisco Unified SRST モードであり、同じサイトにあって同じゲートウェイに登録されている他の電話機と通信しているときに電話機で使用できるようにするコーデックを、ソースリストからターゲットリストに移動します。 ターゲットリストのコーデックは、優先順位の降順に並べられており、リストの一番上にあるものが優先順位が最も高くなります。このリスト内の項目をドラッグアンドドロップして、並べ替えます。	**voice class codec** *tag-number* **codec preference** *value codec-type*
DTMF field	Cisco Unified SRST モードのときにシステムで使用する DTMF リレーオプションをソースリストからターゲットリストに移動します。 ターゲットリストの項目は、優先順位の高い順であり、リストの一番上にあるものが優先順位が最も高くなります。このリスト内の項目をドラッグアンドドロップして、並べ替えます。 [Target] リストに [Inband] オプションを含める場合は、そのリストの唯一のオプションになります。[Target] リストに他のオプションを含める場合は、メディアプロファイルを保存する前に、[Inband] オプションを [Source] リストに移動します。	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}

オプション	説明	Cisco IOS CLI での同等コマンド
Save	Click to save the configuration settings that you made.	—

音声ポリシーに SRST 電話機を設定するには、次の手順に従います。

1. Cisco vManage のメニューで、**[Configuration]** > **[Unified Communications]** を選択します
2. [Add Voice Policy] をクリックし、[SRST Phone] を選択します。
3. [Add SRST Phone Policy Profile] ドロップダウンリストから、[Create New] を選択します。

   または、[Copy from Existing] を選択して、既存のポリシーを新しいポリシーにコピーすることもできます。表示されるボックスで、コピーするポリシープロファイルの名前を選択し、必要に応じてプロファイルの新しい名前を入力して、[Copy] をクリックします。
4. [Media Profile] をクリックし、[Next] をクリックします。
5. [Add New Media Profile] をクリックします。
6. 表示されるページで、「SRST 電話機の設定オプション」の表の説明に従ってオプションを設定します。
7. [Next] をクリックします。
8. [Policy Profile Name] に、この子ポリシーの名前を入力します。
9. [Policy Profile Description] に、この子ポリシーの説明を入力します。
10. [Save] をクリックします。

Unified Communications のデバイステンプレートのプロビジョニング

Unified Communications 用のデバイステンプレートをプロビジョニングするときは、UC 固有の機能テンプレートを選択し、デバイステンプレートに含める音声ポリシーを設定します。

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、UC 固有の機能テンプレートをアタッチし、音声ポリシーをマッピングする、サポートされているデバイスのタイプを選択します。
5. **[Unified Communications]** をクリックします。
6. デバイステンプレートに含める UC 固有の機能テンプレートを選択するには、次のアクションを実行します。
   1. [Voice Card] ドロップダウンリストから、デバイスにアタッチする音声カード機能テンプレートを選択します。
   2. [Call Routing] ドロップダウンリストから、デバイスにアタッチするコールルーティング機能テンプレートを選択します。
   3. [SRST] ドロップダウンリストから、デバイスにアタッチする SRST 機能テンプレートを選択します。
   4. [DSPFarm] ドロップダウンリストから、デバイスにアタッチする DSPFarm テンプレートを選択します。
7. デバイステンプレートに含める音声ポリシーを設定するには、次のアクションを実行します。
   1. [Voice Policy] ドロップダウンリストから、エンドポイントにマッピングする音声ポリシーを選択します。
   2. [Mapping] をクリックします。
   3. 表示される画面の左ペインにあるエンドポイントタイプのリストから、特定のエンドポイントにマッピングするサブポリシーを含むエンドポイントのタイプを選択します。
   4. 表示されるサブポリシーのリストから、[…] をクリックし、特定のエンドポイントにマッピングするサブポリシーの [Mapping] をクリックします。
   5. 表示されるエンドポイントのリストで、サブポリシーをマッピングする各エンドポイントを選択します。
   6. [**マップ**] をクリックします。
   7. **[Save]** をクリックします。
8. デバイステンプレートを作成するには、[Create] をクリックします。

   サブポリシーをエンドポイントにマッピングすると、システムは次の表に示す CLI コマンドを生成します。

表 *87* : サブポリシーからエンドポイントへのマッピングに対して生成された *CLI* コマンド

エンドポイント	サブポリシー	Cisco IOS CLI アプリケーションマッピング	備考
音声ポート FXO 音声ポート FXS 音声ポート FXS DID 音声ポート PRI ISDN POTS ダイヤル ピア SIP ダイヤルピア	トランスレーションプロファイル	**translation-profile incoming** *profile-name* **translation-profile outgoing** *profile-name*	トランスレーションプロファイル ポリシーは、ダイヤルピアまたは音声プロファイルに適用されます。
SRST 電話 SIP ダイヤルピア	メディアプロファイル	voice register pool *number* **voice-class codec** *number* **dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}	メディアプロファイル ポリシーには、音声クラスコーデックと DTMF リレー設定が含まれます。このポリシーは、着信 SIP ダイヤルピア、発信 SIP ダイヤルピア、または SRST 電話プロファイルに適用されます。
音声ポート FXO	監視式のコール切断	voice port *number* **supervisory custom-cptone** *cptone-name* **supervisory dualtone-detect=params** *tag*	custom-cptone または dualtone-detect-params などの監視式のコール切断ポリシーは、FXO 音声インターフェイスに適用されます。

エンドポイント	サブポリシー	Cisco IOS CLI アプリケーションマッピング	備考
音声ポート FXO 音声ポート FXS 音声ポート FXS DID 音声ポート PRI ISDN POTS ダイヤル ピア	トランク グループ	**trunk-group name** [*preference-num*] **voice-port** *number* *trunk-group name* [*preference-num*] **interface serial** *slot*/*sub-slot*/**port:**{**15** | **23**} **dial-peer voice** *tag* **pots** **trunkgroup name** *preference-num*	複数のインターフェイスが同じトランクグループに割り当てられている場合、preference-num 値によって、トランクグループがインターフェイスを使用する順序が決まります。 preference-num 値 1 は最も高い優先度であるため、その値を持つインターフェイスが最初に使用されます。値64は最も低い優先度であるため、その値を持つインターフェイスが最後に使用されます。
SIP ダイヤルピア	モデム パススルー	[なし（None）]： **no modem passthrough** G.711 ulaw： **modem passthrough nse codec g711ulaw** G.711 a-law： **modem passthrough nse codec g711alaw**	—
SIP ダイヤルピア	Fax protocol	**fax protocol** {**none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}	—

ダイヤルピア CSV ファイル

ダイヤルピア CSV ファイルには、1 つ以上の着信および発信 SIP および POTS ダイヤルピアに関する情報が含まれています。ファイルはカンマで区切る必要があり、ファイル内の各レコードには、次の表に示す各フィールドが示されている順序で含まれている必要があります。

表 *88* : ダイヤルピア *CSV* ファイルのフィールド

フィールド	説明
Dial Peer Tag	ダイヤルピアを参照するために使用される番号。
Dial Peer Type	作成するダイヤルピアのタイプ（[pots] または [voip]）。
方向	ダイヤルピアのトラフィックの方向（[Incoming] または [Outgoing]）。
説明	ダイヤルピアの説明。
Forward Digits	ダイヤルピアが発信番号内の番号を送信する方法。 • [All]：ダイヤルピアは番号内のすべての番号を送信します。 • [None]：ダイヤルピアは、宛先パターンに一致しない番号内の番号を送信しません。 • *n*：ダイヤルピアは、整数 *n* が表す番号内の右端からの桁数の番号を送信します。たとえば、*n* が 7 で発信番号が 1112223333 の場合、ダイヤルピアは 2223333 を送信します。
[優先順位（Preference）]	POTS ダイヤルピアの場合、ダイヤルピアの一意の数値。ダイヤルピアの一致基準が同じ場合、システムは優先順位の値が最も高いものを使用します。
Prefix	発信 POTS ダイヤルピアコールに付加される数字。
Numbering Pattern	ダイヤルピアへの着信コールを照合するためにルータが使用する文字列。

フィールド	説明
Dest. アドレス	ローカル発信 SIP ダイヤルピアが一致した後にコールが送信されるリモート音声ゲートウェイのネットワークアドレス。
Voice Port	ダイヤルピアへのコールを照合するためにルータが使用する音声ポート。 発信ダイヤルピアの場合、ルータはダイヤルピアに一致するコールをこのポートに送信します。 着信ダイヤルピアの場合、このポートは追加の一致基準として機能します。ダイヤルピアは、コールがこのポートに着信した場合にのみ一致します。
トランスポートプロトコル	SIP ダイヤルピアの場合、SIP 制御シグナリングのトランスポートプロトコル（[TCP] または [UDP]）。

ダイヤルピア CSV ファイルの例：

```
Tag,type,Direction,Description,Forward Digits,Preference,Prefix,Pattern,Dest. Address,Voice
 Port,Transport
6545,voip,Outgoing,description To Voice Gateway,,1,,23456,ipv4:166.2.121.17,,udp
6756,voip,Outgoing,description ***Fax Number 6362-6362***,,0,,34567,ipv4:166.2.121.16,,tcp
768,voip,Outgoing, description Fire Alarm Dialer,,8,,5678,ipv4:166.2.121.19,,udp
10,pots,Incoming,,,5,,0115T,,1/0/1,
54,pots,Outgoing,,,6,,.T,,1/0/3,
23,pots,Incoming,,all,0,,76..,,1/0/4,
26,pots,Incoming,,5,1,55,9800........,,1/0/5,
27,pots,Incoming,,5,1,55,9800........,,0/1/5:15,
```

変換ルール CSV ファイル

変換プロファイル、POTS ダイヤルピア、または SIP ダイヤルピアの変換ルールを設定する場合、新しい変換ルールを作成するか、CSV ファイルから既存の変換ルール情報をインポートすることができます。

ファイルはカンマで区切る必要があり、ファイル内の各レコードには、次の表に示す各フィールドが示されている順序で含まれている必要があります。

表 *89* : 変換ルール *CSV* ファイルのフィールド

フィールド	説明
一致（Match）	変換ルールを適用する文字列。文字列は、スラッシュ（/）で始まり、スラッシュで終わる正規表現形式である必要があります。たとえば、/^9/。
操作	Match フィールドの文字列に一致する呼び出しに対してシステムが実行するアクション。有効な値は次のとおりです。 • [reject]：システムがコールを拒否します • [replace]：システムが一致文字列を [Replace] フィールドの値に置き換えます
Replace	[Action] フィールドに [replace] が含まれている場合、このフィールドには、一致した文字列の変換先の文字列が含まれます。スラッシュ（/）で囲んだ正規表現形式で数値を入力します。たとえば、// は、置換する文字列がないことを示します。 例として、/^9/ の一致文字列と // の置換文字列を指定すると、システムは、9 で始まる番号を持つ呼び出しから先頭の 9 を削除します。この場合、システムは 914085551212 を 14085551212 に変換します。

変換ルール CSV ファイルの例：

```
Match,Action,Replace
/34/,replace,/34/
/23/,reject,
/56/,replace,/100/
/16083652563/,replace,/6083652563/
```

UC 操作のモニタリング

サポートされているルータの UC 音声サービスを有効にすると、デバイスが処理する回線、コール、インターフェイス、および関連項目のリアルタイムステータスをモニタリングできます。

UC 操作をモニタリングするには、次の手順を実行します。

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. デバイスの表で、UC 操作をモニタリングするデバイスを選択します。
3. [Security Monitoring] から、[Real Time] をクリックします。
4. [Device Options] で、次のいずれかのオプションを選択します。
   - [Voice Calls]：アクティブな音声コールの情報を表示します。「音声コールのモニタリング情報」の表を参照してください。
   - [Voice VOIP Calls]：アクティブな VOIP コールの情報を表示します。「音声 VoIP コールのモニタリング情報」の表を参照してください。
   - [Voice Phone Info]：Cisco Unified SRST 登録に関する情報を表示します。「音声電話情報のモニタリング情報」の表を参照してください。
   - [Voice Controller T1 E1 Current 15 mins Stats]：過去 15 分間にコンパイルされた、デバイスにインストールされている T1/E1 音声モジュールの設定およびステータス情報を表示します。「音声コントローラ T1 E1 直近 15 分間の統計情報のモニタリング情報」の表を参照してください。
   - [Voice Controller T1 E1 Total Stats]：モジュールの最後の起動以後にコンパイルされた、デバイスにインストールされている T1/E1 音声モジュールの設定およびステータス情報を表示します。「音声コントローラ T1 E1 合計の統計情報」の表を参照してください。
   - [Voice ISDN Status]：ISDN コントローラのレイヤ 1 およびレイヤ 2 ステータスに関する情報、およびアクティブコールに関する情報を表示します。「音声 ISDN ステータス情報」の表を参照してください。
   - [Voice DSPFarm SCCP CUCM Groups]：デバイスの DSP ファームサービス用に設定されている Cisco Unified Communications Manager グループに関する詳細情報を表示します。「音声 DSPFarm SCCP CUCM グループ」の表を参照してください。
   - [Voice DSPFarm Profile]：デバイスに設定されている DSP ファーム サービス プロファイルおよびメディアリソースに関する詳細情報を表示します。「音声 DSPFarm プロファイルのモニタリング情報」の表を参照してください。
   - [Voice DSP Farm SCCP Connections]：デバイスと Cisco Unified Communications Manager 間の SCCP 接続に関する詳細情報を表示します。「音声 DSPFarm SCCP 接続」の表を参照してください。
   - [Voice DSPFarm Active]：デバイスでアクティブな DSP ファームリソースに関する動作とステータスの情報を表示します。「音声 DSPFarm アクティブ」の表を参照してください。

   次のオプションを選択して、UC 操作を含む操作をモニタリングすることもできます。

   - [Interface Detail]：ルータに設定されているインターフェイスのステータスと統計情報を表示します。

- [Interface Statistics]：ルータに設定されているインターフェイスの統計情報を表示します。
- [Interface T1/E1]：デバイスにインストールされている T1/E1 音声モジュールの情報を表示します。

次の表では、音声コールをモニタリングするときに表示される情報について説明します。

表 *90*：音声コールのモニタリング情報

フィールド	説明
コール ID	テレフォニーコールレッグのシステム割り当て識別子
Voice Port	コールに使用された音声ポート
コーデック	コールに使用されたネゴシエートされたコーデック
VAD	コールに対して VAD が有効か無効かを示します。
DSP Cannel	コールに使用された DSP チャネル
DSP Type	コールに使用された DSP のタイプ
Aborted Packets	コール中に中断されたパケット数
TX Packets	コール中に送信されたパケット数
RX Packets	コール中に受信されたパケット数
最終更新日	このページの情報が最後に更新された日時

次の表では、音声 VoIP コールをモニタリングするときに表示される情報について説明します。

表 *91*：音声 *VoIP* コールのモニタリング情報

フィールド	説明
コール ID	コールレッグの RTP 接続のシステム割り当て識別子
コーデック	コールに使用されたネゴシエートされたコーデック
宛先アドレス	コールの宛先の IP アドレス
宛先ポート	コールの宛先の RTP ポート
TX Packets	コール中に送信されたパケット数
RX Packets	コール中に受信されたパケット数
Duration (ms)	コールの時間（ミリ秒単位）

フィールド	説明
最終更新日	このページの情報が最後に更新された日時

次の表では、音声電話情報をモニタリングするときに表示される情報について説明します。

表 *92*：音声電話情報のモニタリング情報

フィールド	説明
Pool Tag	デバイスの Cisco Unified SRST 電話プールに割り当てられているタグ番号
ID Network	Cisco Unified Communications Manager からこのデバイスにフォールバックする電話を登録するためにデバイスが使用するネットワークサブネットの識別子
登録の状態（Registration State）	Cisco Unified SRST モードの電話機がこのデバイスに登録されているかどうかを示します。
Dialpeer Tag	Cisco Unified SRST モードで、このデバイスに登録されている電話機の電話番号に割り当てられているダイヤルピアによって使用されるシステム割り当てのタグ
アドレス	電話機がフェールオーバーするときに SIP SRST 呼制御に使用されるデバイスインターフェイスの IP アドレス
[電話番号（Directory Number）]	Cisco Unified SRST モードの各電話機の電話番号
最終更新日	このページの情報が最後に更新された日時

次の表では、過去 15 分間の音声コントローラ T1/E1 情報をモニタリングしたときに表示される情報について説明します。

表 *93*：音声コントローラ *T1 E1* 直近 *15* 分間の統計情報のモニタリング情報

フィールド	説明
Interface-slot-num	コントローラのスロット番号。
Insterface-subslot-num	コントローラのサブスロット番号。
Interface-port-num	コントローラのポート番号。
ステータス	コントローラのステータス。
タイプ	コントローラの種類。
Clock Source	コントローラに使用されたクロックソース。
Line Code Violations	発生した回線コード違反の数。

フィールド	説明
Path Code Violations	発生したパスコード違反の数。
Slip Seconds	発生したスリップ秒数。同期受信側端末と受信された信号のタイミングに差がある場合、スリップが生じることがあります。
Frame Loss Seconds	フレーム同期外れ（OOF）エラーが発生した秒数。
Line Err. seconds	回線エラー秒数（LES）が発生した秒数。LES は、1 秒間に 1 つ以上の回線コード違反エラーが検出されたことを意味します。
低下分数	発生した低下分数。低下分数は、推定エラー率が 1E-6 を超えているが、1E-3 を超えない 1 分間の数を意味します。
エラー秒数	発生したエラー秒数。
バースト エラー秒数	発生したバーストエラー秒数。バーストエラー秒数は、1 秒間に 2 つ以上 320 個未満のパス符号違反エラーが検出され、重大エラーフレーム障害と着信 AIS 障害は検出されなかった秒の数を意味します。
重大エラー秒数	発生した重大エラー秒数。
使用不可能秒数	発生した使用不可秒数。この値は、インターフェイスが使用できない秒数をカウントして算出されます。
最終更新日	このページの情報が最後に更新された日時。

次の表では、デバイスが最後に起動してからの期間において音声コントローラ T1/E1 情報をモニタリングしたときに表示される情報について説明します。

表 *94 :* 音声コントローラ *T1 E1* 合計の統計情報

フィールド	説明
Interface-slot-num	コントローラのスロット番号。
Insterface-subslot-num	コントローラのサブスロット番号。
Interface-port-num	コントローラのポート番号。
ステータス	コントローラのステータス。
タイプ	コントローラの種類。
Clock Source	コントローラに使用されたクロック ソース。
Line Code Violations	発生した回線コード違反の数。

フィールド	説明
Path Code Violations	発生したパスコード違反の数。
Slip Seconds	発生したスリップ秒数。同期受信側端末と受信された信号のタイミングに差がある場合、スリップが生じることがあります。
Frame Loss Seconds	フレーム同期外れ（OOF）エラーが発生した秒数
Line Err. seconds	回線エラー秒数（LES）が発生した秒数。LES は、1 秒間に 1 つ以上の回線コード違反エラーが検出されたことを意味します。
低下分数	発生した低下分数。低下分数は、推定エラー率が 1E-6 を超えているが、1E-3 を超えない 1 分間の数を意味します。
エラー秒数	発生したエラー秒数。
バースト エラー秒数	発生したバーストエラー秒数。バーストエラー秒数は、1 秒間に 2 つ以上 320 個未満のパス符号違反エラーが検出され、重大エラーフレーム障害と着信 AIS 障害は検出されなかった秒の数を意味します。
重大エラー秒数	発生した重大エラー秒数。
使用不可能秒数	発生した使用不可秒数。この値は、インターフェイスが使用できない秒数をカウントして算出されます。
最終更新日	このページの情報が最後に更新された日時。

次の表では、音声 ISDN ステータスをモニタリングするときに表示される情報について説明します。

表 *95 :* 音声 *ISDN* ステータス情報

フィールド	説明
キー ID	表の行の識別子
インターフェイス	PRI ISDN デジタルインターフェイスの名前
スイッチ タイプ	PRI ISDN デジタルインターフェイスに使用されたスイッチ タイプ
Layer 1 Status	PRI ISDN デジタルインターフェイスのレイヤ 1 ステータス
Layer 2 Status	PRI ISDN デジタルインターフェイスのレイヤ 2 ステータス
Active Calls	PRI ISDN デジタルインターフェイスのアクティブコール数

フィールド	説明
最終更新日	このページの情報が最後に更新された日時

次の表では、デバイスで DSP ファームサービス用に設定された Cisco Unified Communications Manager グループをモニタリングするときに表示される情報について説明します。

表 *96* : 音声 *DSPFarm SCCP CUCM* グループのモニタリング情報

フィールド	説明
CUCM Group ID	Cisco Unified Communications Manager グループの識別子
説明	Cisco Unified Communications Manager グループの説明
スイッチオーバー方式（Switchover Method）	この Cisco Unified Communications Manager グループ内のプライマリ Cisco Unified Communications Manager サーバーがフェールオーバーに使用する方法
スイッチバック方式（Switchback Method）	この Cisco Unified Communications Manager グループ内のセカンダリ Cisco Unified Communications Manager サーバーがフェールオーバー後にスイッチバックするために使用する方法
CUCM ID	Cisco Unified Communications Manager グループ内の各 Cisco Unified Communications Manager サーバーの識別子
CUCM Priority	この Cisco Unified Communications Manager グループ内の Cisco Unified Communications Manager サーバーが使用されるプライオリティ
プロファイル ID	Cisco Unified Communications Manager グループ内の各 Cisco Unified Communications Manager サーバーに登録されている DSP ファームプロファイルの識別子
Reg. Name	Cisco Unified Communications Manager グループ内の各 Cisco Unified Communications Manager サーバーに登録されている DSP ファームプロファイルの名前
最終更新日	このページの情報が最後に更新された日時

次の表では、デバイスに設定されている DSP ファーム サービス プロファイルとメディアリソースをモニタリングするときに表示される情報について説明します。

表 *97* : 音声 *DSPFarm* プロファイルのモニタリング情報

フィールド	説明
プロファイル ID	DSP ファームプロファイルの識別子。

フィールド	説明
Service ID	この DSP ファームプロファイル用に設定されている DSP ファームサービスのタイプ。
Service Mode	この DSP ファームプロファイルのサービスモード。
リソース ID（Resource ID）	この DSP ファームプロファイル内の DSP リソースグループのリソース識別子。
Admin	この DSP ファームプロファイルのステータス。このフィールドに [DOWN] と表示されている場合は、この DSP ファームを定義する DSPFarm 機能テンプレートの [Profile] タブで [Shutdown] オプションが有効になっていないことを確認してください。
動作	Cisco Unified Communications Manager でのプロファイルの登録ステータス： • [ACTIVE IN PROGRESS]：プロファイルは Cisco Unified Communications Manager に登録中です。 • [DOWN]：プロファイルは Cisco Unified Communications Manager に登録できません。 • [ACTIVE]：プロファイルは Cisco Unified Communications Manager に登録されています。
アプリケーションタイプ	デバイスにプロビジョニングされている DSP ファームサービスが関連付けられているアプリケーションのタイプ。
アプリケーションステータス	このプロファイルと Cisco Unified Communications Manager の関連付けのステータス： • [app-assoc-done]：プロファイルは Cisco Unified Communications Manager に関連付けられています。 • [app-assoc-not-done]：プロファイルは Cisco Unified Communications Manager に関連付けられていません。
Resource Provider	プロファイルに関連するメディアリソースファミリに関する情報。
Provider Status	プロファイルに関連するメディアリソースのステータス。
最終更新日	このページの情報が最後に更新された日時。

次の表では、デバイスと Cisco Unified Communications Manager 間の SCCP 接続をモニタリングするときに表示される情報について説明します。

表 *98* : 音声 *DSPFarm SCCP* 接続

フィールド	説明
Connection ID	この DSP ファームサービスを使用するアクティブコールの SCCP 接続の識別子
Session ID	この DSP ファームサービスを使用するアクティブコールの SCCP セッションの識別子
Session Type	この SCCP 接続の DSP ファームサービスのタイプ
モード	この SCCP 接続のトラフィック方向のモード
コーデック	この SCCP 接続用にプロビジョニングされたコーデック
Remote IP	この SCCP 接続のリモートエンドポイントの IP アドレス
リモートポート	この SCCP 接続のリモートエンドポイントのポート番号
Source Port	この SCCP 接続のローカルエンドポイントのポート番号
最終更新日	このページの情報が最後に更新された日時

次の表では、デバイスでアクティブな DSP ファームリソースをモニタリングするときに表示される情報について説明します。

表 *99* : 音声 *DSPFarm* アクティブのモニタリング情報

フィールド	説明
DSP	この DSP ファームサービスを使用するアクティブコールの DSP の識別子
ステータス	この DSP ファームサービスを使用するアクティブコールの DSP のステータス
リソース ID（Resource ID）	この接続が使用する DSP に関連付けられたリソース識別子
ブリッジ ID	この接続が使用する DSP に関連付けられたブリッジ識別子
Transmit Packets	この接続が送信したパケット数
Received Packets	この接続が受信したパケット数
最終更新日	このページの情報が最後に更新された日時

Cisco Unified Communications FXS および FXO 発信者 ID のサポート

表 *100 :* 機能の履歴

機能名	リリース情報	説明
Cisco Unified Communications FXS および FXO 発信者 ID のサポート	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能により、Cisco vManage CLI アドオン機能テンプレートを使用して、Foreign Exchange Station（FXS）および Foreign Exchange Office（FXO）の発信者 ID 機能を設定できます。

CLI アドオン機能テンプレートを使用した音声機能の追加に関する情報

CLI アドオン機能テンプレートを使用して、Cisco IOS XE SD-WAN デバイス で FXS および FXO 発信者 ID 機能を設定できます。CLI アドオン機能テンプレートの詳細については、「CLI Add-On-Feature Templates」を参照してください。

発信者 ID は、電話局の交換機が着信コールに関するデジタル情報を送信するアナログサービスです。アナログ FXS ポートの発信者 ID 機能は、アナログ FXS 音声ポートに接続された電話機に対してポートごとに設定できます。発信者 ID は、アナログ FXO ポートでも使用できます。発信者 ID 関連の機能は、発信者の ID に基づいています。

FXS 音声ポートに caller-id コマンドが設定されている場合は、シグナリングタイプを loop-start または ground-start から Direct Inward Dialing（DID）に変更する前に、すべての caller-id 設定を削除します。

発信者 ID コマンドを設定した後でデバイスから音声ポートを削除する場合は、発信者 ID 設定をデバイスから削除します。そうしないと、Cisco IOS 設定と Cisco SD-WAN 設定の間で音声ポート設定の不一致が発生します。

CLI アドオン機能テンプレートを使用した音声機能の追加でサポートされるデバイス

- Cisco NIM-2FXO ネットワーク インターフェイス モジュール
- Cisco NIM-4FXO ネットワーク インターフェイス モジュール
- Cisco NIM-2FXSP ネットワーク インターフェイス モジュール

- Cisco NIM-4FXSP ネットワーク インターフェイス モジュール
- Cisco NIM-2FXS/4FXOP ネットワーク インターフェイス モジュール
- Cisco SM-X-72FXS ダブル幅サービスモジュール
- Cisco SM-X-24FXS/4FXO シングル幅サービスモジュール
- Cisco SM-X-16FXS/2FXO シングル幅サービスモジュール
- Cisco SM-X-8FXS/12FXO シングル幅サービスモジュール

CLI アドオン機能テンプレートを使用した音声機能の追加に関する制約事項

- **caller-id** コマンドを使用する前に、**caller-id enable** コマンドで発信者 ID を有効にする必要があります。
- **caller-id alerting dsp-pre-allocate** コマンドを使用するか無効にすると、FXO ポートがアイドル状態の場合、FXO 音声ポートは自動的にシャットダウンされてから、DSP 音声チャネルの割り当てまたは割り当て解除を行うために起動されます。

CLI アドオン機能テンプレートを使用した音声機能の設定

次のコマンドは、発信者 ID 機能の設定オプションを提供します。

- **caller-id alerting dsp-pre-allocate**：受信側 FXO 音声ポートでオンフック（タイプ 1）発信者 ID の発信者 ID 情報を受信するために、デジタルシグナルプロセッサ（DSP）音声チャネルを静的に割り当てます。
- **caller-id alerting line-reversal**：送信側 FXS 音声ポートのオンフック（タイプ 1）発信者 ID および受信側 FXO 音声ポートのオンフック発信者 ID の発信者 ID 情報に対する回線反転アラート方式を設定します。
- **caller-id alerting pre-ring**：送信側 FXS および受信側 FXO 音声ポートのオンフック（タイプ 1）発信者 ID の発信者 ID 情報に対する 250 ミリ秒の呼び出し前アラート方式を設定します。
- **caller-id alerting ring**：受信側 FXO または送信側 FXS 音声ポートのオンフック（タイプ 1）発信者 ID の発信者 ID 情報を受信するためのリングサイクル方式を設定します。
- **caller-id block**：FXS ポートから発信されたコールの遠端での発信者 ID 情報の表示のブロックを要求します。
- **caller-id format e911**：FXS 音声ポートで送信されるコールに対し拡張 911 形式である必要がある発信者 ID メッセージタイプを指定します。
- **caller-id mode**：受信側 FXO または送信側 FXS 音声ポートに対し国外の標準発信者 ID モードを指定します。

- **clid dtmf-codes**：グローバル発信者 ID の DTMF 開始、リダイレクト、および終了コードを指定します。

CLI アドオン機能テンプレートを使用して音声機能を追加する例

次の例は、FXS ポートの発信者 ID 設定を示しています。

```
voice service pots
    clid dtmf-codes ABC
!
voice-port 1/0/0
   caller-id enable
   caller-id alerting ring 3
    station name West Wing
   station number 4085550100
!
voice-port 1/0/1
   caller-id enable
    caller-id mode DTMF start * end #
    caller-id alerting line-reversal
    station name East Wing
    station number 4085550101
!
voice-port 1/0/2
   caller-id enable
    caller-id mode BT
    caller-id alerting pre-ring
    station name Jose
    station number 4085550102
!
voice-port 1/0/3
    caller-id enable
    caller-id block
    station name a-sample
    station number 4085552000
!
voice-port 1/0/4
    caller-id enable
    caller-id format e911
    station name sample-2
    station number 4085552222
```

次の例は、FXO ポートの発信者 ID 設定を示しています。

```
voice service pots
    clid dtmf-codes ABC
!
voice-port 2/0/0
    cptone BR
    caller-id enable
    caller-id alerting line-reversal
    caller-id alerting dsp-pre-allocate
!
voice-port 2/0/1
    caller-id enable
    caller-id alerting ring 2
!
voice-port 2/0/2
    caller-id enable
    caller-id BT FSK
```

```
caller-id alerting pre-ring
```

第 12 章

CUBE の設定

表 *101* : 機能の履歴

機能名	リリース情報	説明
Cisco Unified Border Element の設定	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、Cisco IOS XE SD-WAN デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを使用して、Cisco Unified Border Element（CUBE）機能を設定できます。

この章では、Cisco Unified Border Element（CUBE）のデバイスの設定について説明します。

CUBE に関する情報

CUBE は、2 つの VoIP ネットワーク間で音声およびビデオ接続をブリッジします。これは、IP ベースの音声トランクによる物理的な音声トランクの置換を除き、従来の音声ゲートウェイに類似しています。従来のゲートウェイは、PRI などの回線交換接続を使用して VoIP ネットワークを電話会社に接続します。CUBE は、VoIP ネットワークを他の VoIP ネットワークに接続し、インターネット電話サービスプロバイダー（ITSP）にエンタープライズ ネットワークを接続します。

CUBE は、従来のセッション ボーダー コントローラ（SBC）機能と、さまざまな高度な機能を提供します。

デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを使用して、CUBE の Cisco IOS XE SD-WAN デバイスを設定できます。

CUBE のセットアップ、機能、使用法、設定、および関連トピックの詳細については、『*Cisco Unified Border Element Configuration Guide*』を参照してください。

CUBE 構成でサポートされるデバイス

- Cisco 1000 シリーズ サービス統合型ルータ
- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8000v ソフトウェアルータ
- Cisco ASR 1001-X ルータ
- Cisco ASR 1002-X ルータ
- Cisco ASR1000-RP3 モジュール、および Cisco ASR1000-ESP100 または ASR1000-ESP100-X エンベデッド サービス プロセッサを搭載した Cisco ASR 1006-X ルータ
- RP2 ルートプロセッサおよび Cisco ASR 1000-ESP40 エンベデッド サービス プロセッサを搭載した Cisco ASR 1004 ルータ
- RP2 ルートプロセッサおよび Cisco ASR 1000-ESP40 エンベデッド サービス プロセッサを搭載した Cisco ASR 1006 ルータ
- RP2 ルートプロセッサおよび Cisco ASR 1000-ESP40 エンベデッド サービス プロセッサを搭載した Cisco ASR 1006-X ルータ

CUBE 設定の制約事項

CUBE では、可用性の高い構成はサポートされていません。

CUBE の使用例

CUBE を使用して、次のようなさまざまなアプリケーションのセッション ボーダー コントローラ要素を設定できます。

- 集中型またはローカルの PSTN ブレークアウトを備えた Cisco Unified Communications Manager（または別の呼制御アプリケーション）を使用した、企業のオンプレミスベースのコラボレーション機能

- 大企業向けのシスコがホストするクラウドサービスである Cisco Unified Communications Manager Cloud のローカル ブレークアウト ゲートウェイ
- Cisco Webex Calling の企業内の PSTN 接続（BYoPSTN; Bring Your Own PSTN）オプションを有効にするローカルゲートウェイ
- Cisco Webex Cloud への直接の VoIP ルーティング、または既存の PSTN サービスを介した Cisco Webex Meetings の Edge Audio

CUBE の設定

CUBE 機能を使用するようにデバイスを設定するには、デバイスの Cisco IOS XE SD-WAN デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを作成します。

デバイス CLI テンプレートの詳細については、「Cisco IOS XE SD-WAN デバイスルータの CLI テンプレート」を参照してください。

CLI アドオン機能テンプレートの詳細については、「CLI アドオン機能テンプレート」を参照してください。

CUBE の設定および使用法の詳細については、『*Cisco Unified Border Element Configuration Guide*』を参照してください。

CLI テンプレートでの使用が Cisco SD-WAN でサポートされる CUBE コマンドの詳細については、「CUBE コマンド」を参照してください。

次に、CLI アドオンテンプレートを使用した基本的な CUBE 設定の例を示します。

```
voice service voip
 ip address trusted list
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
  !
 allow-connections sip to sip
 sip
  no call service stop
  !
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
  session protocol sipv2
  incoming called number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 101 voip
  description Outbound LAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:10.10.10.1
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 200 voip
  description Inbound WAN side dial-peer
  session protocol sipv2
  incoming called-number .T
```

```
 voice-class codec 1
 dtmf-relay rtp-nte
 !
dial-peer voice 201 voip
 description Outbound WAN side dial-peer
 destination pattern [2-9].........
 session protocol sipv2
 session target ipv4:20.20.20.1
 voice-class codec 1
 dtmf-relay rtp-nte
```

CUBE コマンド

次の表に、CUBE 設定用に Cisco SD-WAN CLI テンプレートでサポートされているコマンドを示します。[Command]列のコマンドをクリックして、コマンド、その構文、および使用法に関する情報を表示します。

表 *102 : CUBE* 設定用の *Cisco SD-WAN CLI* テンプレートコマンド

コマンド	説明
address-hiding	ゲートウェイ以外のエンドポイントからのシグナリングおよびメディアピアアドレスを非表示にします。
anat	SIP トランク上で代替ネットワークアドレスタイプ（ANAT）を有効にします。
answer-address	着信コールのダイヤルピアを識別するために使用される完全な形式の E.164 電話番号を指定します。
application (global)	アプリケーション コンフィギュレーション モードを開始して、アプリケーションを設定します。
asserted-id	着信 SIP 要求または応答メッセージでアサートされた ID ヘッダーのサポートを有効にし、発信 SIP 要求または応答メッセージでアサートされた ID プライバシー情報を送信します。
asymmetric payload	SIP 非対称ペイロードサポートを設定します。
audio forced	音声と画像（T.38 Fax の場合）メディアタイプのみを許可し、他のすべてのメディアタイプをドロップします。
authentication	SIP ダイジェスト認証を有効にします。
bind	特定のインターフェイスの IPv4 または IPv6 アドレスに対するシグナリングおよびメディアパケットの送信元アドレスをバインドします。

コマンド	説明
block	CUBE で特定の着信 SIP 暫定応答メッセージをドロップする（渡さない）ようにグローバル設定を構成します。
call spike	短期間に受信する着信コール数（コールスパイク）の制限を設定します。
call threshold global	ゲートウェイのグローバルリソースを有効にします。
call treatment action	ローカルリソースが使用できない場合にルータが実行するアクションを設定します。
call treatment cause-code	ローカルリソースが使用できない場合の発信者に対する切断の理由を指定します。
call treatment isdn-reject	すべての ISDN トランクがビジーアウトになっているが、スイッチがビジーアウトトランクを無視し、ISDN コールをゲートウェイに送信する場合の ISDN コールの拒否原因コードを指定します。
call treatment on	ローカルリソースが利用できない場合にコールを処理するためのコール処理を有効にします。
callmonitor	VoIP ネットワークの SIP エンドポイントでコール モニタリング メッセージング機能を有効にします。
call-route	グローバル設定レベルでヘッダーベースのルーティングを有効にします。
clid	ネットワーク提供の ISDN 番号を ISDN 発信側情報要素スクリーニング インジケータ フィールドに渡し、音声サービス VoIP 設定モードで発信側の名前と番号を発信者回線識別子から削除します。または、Remote-Party-ID および From ヘッダーで欠落している [Display Name] フィールドを置き換えることにより、発信者番号の表示を許可します。
codec preference	ダイヤル ピアで使用するコーデックのリストを優先順位を付けて指定します。
codec profile	ビデオエンドポイントに必要なオーディオおよびビデオ機能を定義します。
codec transparent	CUBE のエンドポイント間で透過的に配信できるように、コーデック機能を有効にします。

コマンド	説明
conn-reuse	サポートされている最小リリース：Cisco vManage リリース 20.10.1 および Cisco IOS XE リリース 17.10.1a。ファイアウォールの背後にあるエンドポイントの SIP 登録の TCP 接続を再利用します。
connection-reuse	UDP経由で要求を送信するためにグローバルリスナーポートを使用します。
contact-passing	302 パススルーの場合にレッグから別のレッグへの Contact ヘッダーのパススルーを設定します。
cpa	アウトバウンド VoIP コールのコールプログレス分析（CPA）アルゴリズムを有効にし、CPA パラメータを設定します。
ログイン情報	UP 状態のときに SIP 登録メッセージを送信するように SIP TDM ゲートウェイまたは CUBE を設定します。
crypto signaling	リモートデバイスアドレスに対応する Transport Layer Security（TLS）ハンドシェイク中に使用される **trustpoint** *trustpoint-name* キーワードおよび引数を指定します。
dial-peer cor custom	ダイヤルピアに適用する名前付き制限クラス（COR）を指定します。
dial-peer cor list	制限クラス（COR）リスト名を定義します。
dspfarm profile	DSP ファーム プロファイル コンフィギュレーション モードを開始し、DSP ファーム サービス用のプロファイルを定義します。
dtmf-interworking	CUBE から送信される RFC 2833 パケットの dtmf-digit begin イベントと dtmf-digit end イベント間の遅延を有効にし、CUBE から RFC 4733 準拠の RTP Named Telephony Event（NTE）パケットを生成します。
early-media update block	Early Dialog で Session Description Protocol（SDP）を使用して UPDATE 要求をブロックします。
early-offer	アウトレッグでアーリーオファーを使用して SIP Invite を送信するように CUBE に強制します。
Emergency（致命的）	緊急電話番号のリストを設定します。
error-code-override	ダイヤルピアで使用される SIP エラーコードを設定します。

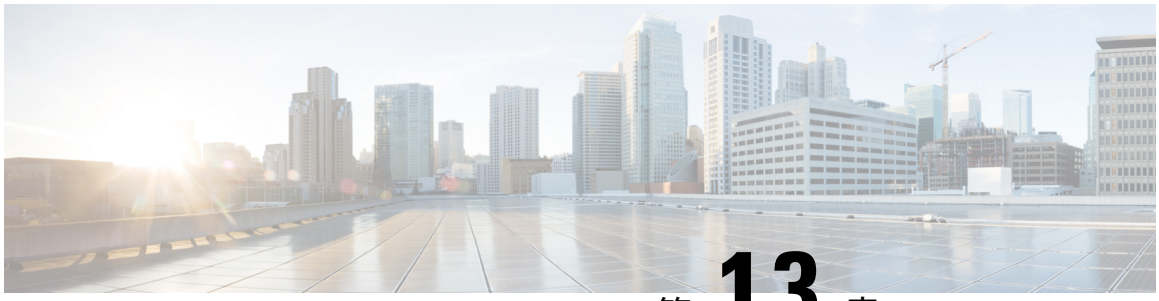
コマンド	説明
error-passthru	着信 SIP レッグから発信 SIP レッグへのエラーメッセージの通過を有効にします。
g729-annexb override	G.729 コーデックの相互運用性の設定を構成し、annexb 属性が存在しない場合にデフォルト値をオーバーライドします。
gcid	SIP エンドポイントの VoIP ダイヤルピアのアウトバウンドレッグで、すべてのコールに対してグローバルコール ID（GCID）を有効にします。
header-passing	SIP INVITE、SUBSCRIBE、および NOTIFY メッセージとの間でのヘッダーの受け渡しを有効にします。
host-registrar	Diversion ヘッダーのホスト部分に sip-ua レジストラドメイン名または IP アドレス値を入力し、302 応答の Contact ヘッダーをリダイレクトします。
http client connection idle timeout	アイドル状態の接続を終了する前に HTTP クライアントが待機する秒数を設定します。
http client connection persistent	同じ接続を使用して複数のファイルをロードできるように、HTTP 持続接続を有効にします。
http client connection timeout	接続の試行を中止するまでに、HTTP クライアントがサーバーによる接続の確立を待機する秒数を設定します。
ip qos dscp	QoS の DSCP 値を設定します。
localhost	発信メッセージの From、Call-ID、および Remote-Party-ID ヘッダーの物理 IP アドレスの代わりに、DNS ホスト名またはドメインを localhost 名として使用するように CUBE をグローバルに設定します。
max-conn	特定の VoIP ダイヤルピアの着信接続または発信接続の最大数を指定します。
メディア	CUBE の介在なしにメディアパケットがエンドポイント間を直接通過できるようにします。シグナリングサービスも有効にします。
media disable-detailed-stats	詳細なコール統計の収集を無効にします。
media profile asp	メディアプロファイルを作成して、音響衝撃保護パラメータを設定します。

コマンド	説明
media profile nr	メディアプロファイルを作成して、ノイズリダクションパラメータを設定します。
media profile stream-service	CUBE でストリームサービスを有効にします。
media profile video	メディアプロファイルビデオを作成します。
media-address voice-vrf	RTP ポート範囲を VRF と関連付けます。
media-inactivity-criteria	音声コールでメディアの非アクティブ（無音）を検出するメカニズムを指定します。
midcall-signaling	シグナリングメッセージに使用される方法を設定します。
min-se	SIP セッションタイマーを使用するすべてのコールの最小セッション有効期限（Min-SE）ヘッダーの値を変更します。
notify redirect	すべての VoIP ダイヤルピアに対するリダイレクト要求のアプリケーション処理を有効にします。
num-exp	内線電話番号を特定の宛先パターンに拡張する方法を定義します。
options-ping	ダイアログ内オプションを有効にします。
outbound-proxy	発信 SIP メッセージの SIP アウトバウンドプロキシをグローバルに設定します。
pass-thru content	内部レッグから外部レッグへの SDP のパススルーを有効にします。
privacy	RFC 3323 で定義されるプライバシーサポートをグローバルレベルで 設定します。
privacy-policy	グローバルレベルでプライバシー ヘッダー ポリシー オプションを設定します。
Progress_ind	指定したコールメッセージのデフォルトの進行状況インジケータを上書きして削除する（置き換える）ようにCUBE でアウトバウンドダイヤルピアを設定します。
protocol mode	Cisco IOS SIP スタックを設定します。
reason-header override	SIP レッグ間の原因コードの受け渡しを有効にします。
redirect ip2ip	ゲートウェイ上で SIP 電話コールを SIP 電話コールにグローバルにリダイレクトします。

コマンド	説明
redirection	3*xx* リダイレクトメッセージの処理を有効にします。
referto-passing	CUBE がコール転送中に REFER メッセージを渡すときに、ダイヤルピアルックアップと Refer-To ヘッダーの変更を無効にします。
registrar	SIP ゲートウェイが、アナログ電話の音声ポート（FXS）、IP Phone 仮想音声ポート（EFXS）、SCCP 電話に代わって、E.164 番号を外部 SIP プロキシまたは SIP レジストラに登録できるようにします。
rel1xx	SIP 暫定応答（100 Trying 以外）がリモート SIP エンドポイントに確実に送信されるようにします。
remote-party-id	Remote-Party-ID SIP ヘッダーの変換を有効にします。
requri-passing	Request-URI および To SIP ヘッダーのホスト部分のパススルーを有効にします。
retry bye	Bye 要求がもう一方のユーザーエージェントに再送信される回数を設定します。
rtcp all-pass-through	データパス内のすべての RTCP パケットを渡します。
rtcp keepalive	RTCP キープアライブレポート生成を設定し、RTCP キープアライブパケットを生成します。
rtp payload-type	RTP パケットのペイロードタイプを指定します。
rtp-media-loop count	RTP 音声およびビデオメディアパケットがドロップされるまでのメディアループの数を設定します。
rtp-port	リアルタイムプロトコル範囲を設定します。
rtp-ssrc multiplex	RTCP パケットを RTP パケットと多重化し、RTP セッションの RTP ヘッダー（SSRC）で複数の同期ソースを送信します。
session refresh（SIP UPDATE セッション更新）	SIP セッションの更新をグローバルに有効にします。
session transport	TCP または UDP を SIP メッセージの基礎となるトランスポート層プロトコルとして使用するように VoIP ダイヤルピアを設定します。
set pstn-cause	着信 PSTN 原因コードを SIP エラー ステータス コードにマッピングします。

コマンド	説明
set sip-status	着信 SIP エラーステータスコードを PSTN 原因コードにマッピングします。
signaling forward	QSIG、Q.931、H.225、および ISUP メッセージの透過トンネリングのグローバル設定を構成します。
silent discard untrusted	着信 SIP トランク内の信頼できないソースからの SIP 要求を破棄します。
sip-server	SIP サーバ インターフェイスのネットワーク アドレスを設定します。
srtp	SRTP を使用してセキュアなコールとコール フォールバックを有効にするよう指定します。
stun	ファイアウォール トラバーサル パラメータを設定するための STUN コンフィギュレーション モードを開始します。
stun usage firewall-traversal flowdata	STUN を使用したファイアウォール トラバーサルを有効にします。
supplementary-service media-renegotiate	補足サービスの通話中のメディア再ネゴシエーションをグローバルに有効にします。
timers	SIP シグナリングタイマーを設定します。
transport	SIP TCP、TLS over TCP、または UDP ソケットを介したインバウンドコールの SIP シグナリングメッセージに SIP ユーザーエージェント（ゲートウェイ）を設定します。
uc secure-wsapi	特定のアプリケーションにセキュア Cisco Unified Communication IOS サービス環境を設定します。
uc wsapi	特定のアプリケーションに非セキュア Cisco Unified Communication IOS サービス環境を設定します。
update-callerid	発信者 ID の更新の送信を有効にします。
url (SIP)	VoIP SIP コールに SIP、SIP secure（SIPS）、または telephone（TEL）形式の URL を設定します。
vad	特定のダイヤルピアを使用して、コールに対して VAD を有効にします。
voice cause code	音声の内部 Q850 原因コードマッピングを設定し、音声原因コンフィギュレーション モードを開始します。

コマンド	説明
voice class codec	音声クラスコンフィギュレーションモードを開始し、コーデック音声クラスに識別タグ番号を割り当てます。
voice class dpg	複数のアウトバウンドダイヤルピアのグループ化のためにダイヤルピアグループを作成します。
voice class e164-pattern-map	ダイヤルピアの複数の宛先E.164パターンを指定するE.164パターンマップを作成します。
voice class media	音声のメディア コントロール パラメータを設定します。
voice class server-group	音声クラス コンフィギュレーション モードを開始し、アウトバウンドSIPダイヤルピアから参照可能なサーバーグループ（IPv4 および IPv6 アドレスのグループ）を設定します。
voice-class sip options-keepalive	CUBE VoIP ダイヤルピアと SIP サーバー間の接続をモニタリングします。
voice class sip-copylist	ピアコールレッグに送信されるエンティティのリストを設定します。
voice class sip-event-list	渡される SIP イベントのリストを設定します。
voice class sip-hdr-passthrulist	ルート文字列を介して渡されるヘッダーのリストを設定します。
voice class sip-profiles	音声クラス用の SIP プロファイルを設定します。
voice class srtp-crypto	音声クラス コンフィギュレーション モードを開始し、**srtp-crypto voice class** コマンドに ID タグを割り当てます。
voice class uri	ダイヤルピアを SIP URI または TEL URI に一致させるための音声クラスを作成または変更します。
voice iec syslog	発生した内部エラーコードをリアルタイムで表示できます。
voice statistics iec	内部エラーコード統計の収集を有効にします。



第 13 章

ネットワーク インターフェイスの設定

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、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。

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（[no shutdown]）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。

Cisco IOS XE SD-WAN デバイスでは、最大 512 のインターフェイスを設定できます。この数には、物理インターフェイス、ループバック インターフェイス、およびサブインターフェイスが含まれます。

（注） Cisco vSmart コントローラ 間のロードバランシングの効率を最大化するには、ドメイン内の Cisco IOS XE SD-WAN デバイスにシステム IP アドレスを割り当てるときに連番を使用します。連番付与スキームの例は、172.16.1.1、172.16.1.2、172.16.1.3 などです。

（注） デバイスに構成されているネットワーク インターフェイスに一意の IP アドレスがあることを確認します。

VPN の設定

VPN

Cisco SD-WAN ソフトウェアを実行しているすべての Cisco SD-WAN デバイスに VPN 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 VPN を設定するには、次の一般的なワークフローに従います。

1. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN ごとに個別の VPN 機能テンプレートを作成します。たとえば、VPN 0 用に 1 つの機能テンプレート、VPN 1 用に 2 つ目、VPN 512 用に 3 つ目の機能テンプレートを作成します。

   Cisco vManage ネットワーク管理システムおよび Cisco vSmart コントローラ の場合、VPN 0 および 512 のみを構成できます。VPN のデフォルト設定を変更する場合にのみ、これらの VPN のテンプレートを作成します。Cisco IOS XE SD-WAN デバイス の場合、これら 2 つの VPN のテンプレートと、サービス側のユーザーネットワークをセグメント化するための追加の VPN 機能テンプレートを作成できます。

   - **VPN 0**：設定された WAN トランスポート インターフェイスを介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いて、すべてのインターフェイスが無効になっています。

   - **VPN 512**：オーバーレイネットワーク内の Cisco IOS XE 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 はすべての Cisco IOS XE SD-WAN デバイス で設定され、有効になっています。コントローラデバイスの場合、デフォルトでは、VPN 512 は設定されていません。

- **VPN 1** ～ **511**、**513** ～ **65530**：Cisco IOS XE SD-WAN デバイス のサービス側データトラフィック用の**サービス VPN**。

2. インターフェイス機能テンプレートを作成して、VPNのインターフェイスを設定します。

VPN テンプレートの作成

（注） Cisco IOS XE SD-WAN デバイスは、セグメンテーションとネットワーク分離に VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスのセグメンテーションを設定する場合は、引き続き次の手順が適用されます。設定が完了すると、システムは VPN を Cisco IOS XE SD-WAN デバイスの VRF に自動的に変換します。

（注） VPN テンプレートを使用して静的ルートを設定できます。

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 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。

ステップ 3 [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。

ステップ 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。

ステップ 5 VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
2. [VPN 0] または [VPN 512] ドロップダウンリストから、[Create Template] をクリックします。[VPN] 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、VPN 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。

ステップ 6 VPN 1 ～ 511、および 513 ～ 65527 のテンプレートを作成するには：

1. [Service VPN] をクリックするか、[Service VPN] までスクロールします。
2. [Service VPN] ドロップダウンリストをクリックします。
3. [VPN] ドロップダウンリストから、[Create Template] をクリックします。[VPN] 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、VPN 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。

ステップ 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。

ステップ 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。

パラメータ値の範囲を変更する

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、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、次のいずれかを選択します。

パラメータ名	説明
 [Device Specific]	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、「Create a Template Variables Spreadsheet」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。

パラメータ名	説明
グローバル	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。

テンプレートを作成して名前を付けたら、次の値を入力します。アスタリスクの付いたパラメータは必須です。

基本的な VPN パラメータの設定

基本的な VPN パラメータを設定するには、[Basic Configuration] を選択してから、次のパラメータを設定します。VPN 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。

パラメータ名	説明
VPN	VPN の数値識別子を入力します。 Cisco IOS XE SD-WAN デバイス の範囲：0 ～ 65527 Cisco vSmart コントローラ および Cisco vManage のデバイスの値：0、512
名前	VPN の名前を入力します。 （注） Cisco IOS XE SD-WAN デバイス には、VPN のデバイス固有の名前を入力できません。
Enhance ECMP keying	[On] をクリックして、ECMP ハッシュキーとして、送信元と宛先の IP アドレスの組み合わせに加えて、レイヤ 4 の送信元ポートと宛先ポートの ECMP ハッシュキーでの使用を有効にします。 ECMP キーイングはデフォルトで [Off] です。

（注） ルータでトランスポート VPN の設定を完了するには、VPN 0 で少なくとも 1 つのインターフェイスを設定する必要があります。

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 を使用する負荷分散アルゴリズムの設定

（注） Cisco IOS XE リリース 17.8.1a 以降、IPv4 および IPv6 SD-WAN および非 SD-WAN トラフィックの **src-only** 負荷分散アルゴリズムを設定するには、CLI テンプレートが必要です。負荷分散アルゴリズム CLI の詳細については、「IP Commands」リストを参照してください。

これは、非 SD-WAN IPv4 および IPv6 トラフィックの Cisco Express Forwarding 負荷分散アルゴリズムを選択するための CLI 設定を提供します。ECMP キーイングを有効にして、IPv4 と IPv6 の両方の設定を送信できます。

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source
[id] | destination [id]] |
src-only [id]}

Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source
 [id] | destination [id]] |
src-only [id]}
```

これは、SD-WAN IPv4 および IPv6 トラフィックのインターフェイスで負荷分散アルゴリズムを有効にするための CLI 設定を提供します。ECMP キーイングを有効にして、IPv4 と IPv6 の両方の設定を送信できます。

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}

Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

ドメインネームシステム（DNS）および静的ホスト名マッピングの設定

DNS アドレスと静的ホスト名マッピングを設定するには、[DNS] をクリックして、次のパラメータを設定します。

パラメータ名	オプション	Description
Primary DNS Address	[IPv4] または [IPv6] をクリックし、この VPN のプライマリ DNS サーバーの IP アドレスを入力します。	

パラメータ名	オプション	Description
New DNS Address	[New DNS Address] をクリックし、この VPN のセカンダリ DNS サーバーの IP アドレスを入力します。このフィールドは、プライマリ DNS アドレスを指定した場合にのみ表示されます。	
	[Mark as Optional Row]	この設定をデバイス固有としてマークするには、[Mark as Optional Row] チェックボックスをオンにします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
	Hostname	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
	List of IP Addresses	ホスト名に関連付ける IP アドレスを 8 つまで入力します。エントリをカンマで区切ります。
DNS サーバー設定を保存するには、[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。

ホスト名の IP アドレスへのマッピング

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

WAN トランスポート VPN（VPN 0）でのインターフェイスの設定

このトピックでは、WAN トランスポートとサービス側のネットワーク インターフェイスの一般的なプロパティを設定する方法について説明します。セルラーインターフェイス、DHCP、PPPoE、VRRP、WLAN インターフェイスなど、特定のインターフェイスタイプとプロパティを設定する方法に関する情報を提供します。

VPN 0 は WAN トランスポート VPN です。この VPN は、オーバーレイネットワークで OMP セッションを介して伝送されるすべてのコントロール プレーン トラフィックを処理します。Cisco IOS XE SD-WAN デバイス デバイスがオーバーレイネットワークに参加するには、少なくとも 1 つのインターフェイスが VPN 0 で設定されている必要があり、少なくとも 1 つのインターフェイスが WAN トランスポートネットワーク（インターネット、MPLS、メトロ イーサネット ネットワークなど）に接続されている必要があります。この WAN トランスポート インターフェイスは、トンネルインターフェイスと呼ばれます。少なくとも、このインターフェ

イスでは、IPアドレスを設定し、インターフェイスを有効にして、トンネルインターフェイスとして設定する必要があります。

Cisco vSmart コントローラ または Cisco vManage NMS でトンネルインターフェイスを設定するには、VPN 0 にインターフェイスを作成した後、IP アドレスを割り当てるか、DHCP から IP アドレスを受信するようにインターフェイスを設定して、トンネルインターフェイスとしてマークします。IPアドレスは、IPv4またはIPv6アドレスのどちらにすることもできます。デュアルスタックを有効にするには、両方のアドレスタイプを設定します。オプションで、カラーをトンネルに関連付けることができます。

（注） IPv6 アドレスは、トランスポート インターフェイスでのみ、つまり VPN 0 でのみ設定できます。

Cisco IOS XE SD-WAN デバイス のトンネルインターフェイスには、IP アドレス、カラー、およびカプセル化タイプを設定する必要があります。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。Cisco IOS XE リリース 17.3.2 より前のリリースでデュアルスタックを有効にするには、両方のアドレスタイプを設定します。

Cisco IOS XE リリース 17.3.2 の Cisco IOS XE SD-WAN デバイス でデュアルスタックを使用するには、すべてのコントローラに IPv4 アドレスと IPv6 アドレスの両方を設定します。さらに、IPv4 および IPv6 アドレスタイプを解決するように Cisco vBond オーケストレーション インターフェイス用のドメインネームシステム（DNS）を設定します。これにより、コントローラは、どちらの IP アドレスタイプを介しても Cisco vBond オーケストレーション に到達できます。

（注） Cisco vManage リリース 20.6.1 以降では、デュアルスタックを設定した際に、IPv4 アドレスや完全修飾ドメイン名（FQDN）は使用できず、IPv6アドレスは使用できる場合は、IPv6アドレスを使用して Cisco vBond オーケストレーション に接続します。

トンネルインターフェイスの場合、固定 IPv4 または IPv6 アドレスを設定するか、DHCP サーバーからアドレスを受信するようにインターフェイスを設定できます。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 アドレスの両方を設定します。

Cisco IOS XE リリース 17.3.2 以降、Cisco IOS XE SD-WAN デバイス では同じ TLOC またはインターフェイスでのデュアルスタックはサポートされません。TLOC またはインターフェイスにプロビジョニングできるアドレスタイプは 1 つだけです。2 つ目のアドレスタイプを使用する場合、それをプロビジョニングできる 2 つ目の TLOC またはインターフェイスが必要です。

Cisco vSmart コントローラ および Cisco vSmart コントローラ NMS では、*interface-name* は **eth** *number* または **loopback** *number* のいずれかになります。Cisco vSmart コントローラ と Cisco vSmart コントローラ NMS はオーバーレイネットワークのコントロールプレーンにのみ参加するため、これらのデバイスで設定できる VPN は VPN 0 と VPN 512 です。したがって、すべてのインターフェイスはこれらの VPN にのみ存在します。

インターフェイスを有効にするには、**no shutdown** コマンドを使用します。

カラーは、トランスポートトンネルを識別する Cisco SD-WAN ソフトウェア構造です。これは、**3g**、**biz-internet**、**blue**、**bronze**、**custom1**、**custom2**、**custom3**、**default**、**gold**、**green**、**lte**、**metro-ethernet**、**mpls**、**private1** ～ **private6**、**public-internet**、**red**、および **silver** のいずれかです。**metro-ethernet**、**mpls**、および **private1** ～ **private6** の各カラーは、プライベートアドレスを使用してプライベートネットワークのリモート側 Cisco IOS XE SD-WAN デバイス に接続するため、プライベートカラーと呼ばれます。ローカルとリモートの Cisco IOS XE SD-WAN デバイス 間に NAT デバイスがない場合は、パブリックネットワークでこれらのカラーを使用できます。

ローカル TLOC が BFD セッションを確立できるリモート TLOC を制限するには、[restrict] オプションで TLOC をマークします。TLOC が制限付きとしてマークされている場合、ローカルルータの TLOC は、リモート TLOC が同じカラーである場合にのみ、リモート TLOC とのトンネル接続を確立します。

Cisco vSmart コントローラ または Cisco vSmart コントローラ NMS では、1 つのトンネルインターフェイスを設定できます。Cisco IOS XE SD-WAN デバイス では、最大 8 つのトンネルインターフェイスを設定できます。

Cisco IOS XE SD-WAN デバイス では、トンネルのカプセル化を設定する必要があります。カプセル化は、IPsec または GRE のいずれかです。IPsec カプセル化の場合、デフォルトの MTU は 1442 バイトであり、GRE の場合は 1468 バイトです。これらの値は、すべての TLOC でデフォルトで有効になっている BFD パス MTU ディスカバリに必要なオーバーヘッドに基づいて決定されます。（詳細については、「Configuring Control Plane and Data Plane High Availability Parameters」を参照してください。）同じ **tunnel-interface** コマンドの下に 2 つの **encapsulation** コマンドを含めることにより、IPsec と GRE の両方のカプセル化を設定できます。リモート Cisco IOS XE SD-WAN デバイス では、2 つのルータがデータトラフィックを交換できるように、同じトンネルカプセル化タイプを設定する必要があります。IPsec トンネルから送信されたデータは IPsec トンネルでのみ受信でき、GRE トンネルで送信されたデータは GRE トンネルでのみ受信できます。Cisco SD-WAN ソフトウェアは、宛先 Cisco IOS XE SD-WAN デバイスの正しいトンネルを自動的に選択します。

トンネルインターフェイスでは、DTLS、TLS、および（Cisco IOS XE SD-WAN デバイス の場合）IPsec トラフィックのみがトンネルを通過できます。明示的なポリシーまたはアクセスリストを作成せずに追加のトラフィックが通過できるようにするには、サービスごとに 1 つの **allow-service** コマンドを追加することで有効にできます。**no allow-service** コマンドを追加することで、サービスを明示的に禁止することもできます。サービスは物理インターフェイスにのみ影響することに注意してください。トンネルインターフェイスで次のサービスを許可または禁止できます。

Service	Cisco vSmart コントローラ	Cisco vSmart コントローラ
all（個々のサービスを許可または禁止するコマンドをオーバーライドします）	X	X
bgp	—	—

Service	Cisco vSmart コントローラ	Cisco vSmart コントローラ
dhcp（DHCPv4 および DHCPv6 の場合）	—	—
dns	—	—
https	×	—
icmp	X	X
netconf	×	—
ntp	—	—
ospf	—	—
sshd	X	X
stun	X	X

allow-service stun コマンドを使用すると、Cisco IOS XE SD-WAN デバイス が汎用 STUN サーバーへの要求を生成することを許可または禁止して、このデバイスが NAT の背後にあるかどうかを判別し、NAT の背後にある場合は、NAT の種類とデバイスのパブリック IP アドレスとパブリックポート番号を判別できます。NAT の背後にある Cisco IOS XE SD-WAN デバイス では、そのパブリック IP アドレスとポート番号を Cisco vBond オーケストレーション から検出するトンネルインターフェイスを設定することもできます。

この設定では、Cisco IOS XE SD-WAN デバイス は Cisco vBond オーケストレーション を STUN サーバーとして使用するため、ルータはそのパブリック IP アドレスとパブリックポート番号を判別できます。（この設定では、ルータは自身の前にある NAT の種類を学習できません。）オーバーレイネットワーク制御トラフィックは送信されず、Cisco vBond オーケストレーション に STUN サーバーとして設定されたトンネルインターフェイスを介してキーが交換されることもありません。ただし、BFD はトンネルで起動し、データトラフィックはトンネルで送信できます。Cisco vBond オーケストレーション を STUN サーバーとして使用するように設定されたトンネルインターフェイスを介して制御トラフィックは送信されないため、Cisco IOS XE SD-WAN デバイス で少なくとも 1 つの他のトンネルインターフェイスを設定して、Cisco vSmart コントローラ および Cisco vSmart コントローラ NMS と制御トラフィックを交換できるようにする必要があります。

allow-service コマンドで設定されたサービスと一致しないためにドロップされたすべてのパケットのヘッダーをログに記録できます。これらのログをセキュリティの目的で使用できます。たとえば、WAN インターフェイスに送信されるフローをモニタリングし、DDoS 攻撃の場合にブロックする IP アドレスを決定できます。

システムインターフェイスの設定

各 Cisco IOS XE SD-WAN デバイス に対し、system system-ip コマンドを使用してシステムインターフェイスを設定します。システムインターフェイスの IP アドレスは、Cisco IOS XE SD-WAN

デバイス を識別する永続的なアドレスです。これは通常のルータのルータ ID に似ていて、パケットの発信元のルータを識別するために使用されるアドレスです。

システムの IP アドレスを 10 進 4 部ドット表記の IPv4 アドレスとして指定します。アドレスだけを指定してください。プレフィックス長（/32）は暗黙的です。

システム IP アドレスには、0.0.0.0/8、127.0.0.0/8、224.0.0.0/4、および 240.0.0.0/4 以降を除く任意の IPv4 アドレスを使用できます。オーバーレイネットワーク内の各デバイスには、一意のシステム IP アドレスが必要です。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。

システムインターフェイスは、[system] という名前のループバック インターフェイスとして VPN 0 に配置されます。これは、インターフェイスに設定するループバックアドレスと同じではないことに注意してください。

システムインターフェイスに関する情報を表示するには、**show interface** コマンドを使用します。次に例を示します。

システム IP アドレスは、OMP TLOC の属性の 1 つとして使用されます。各 TLOC は、システム IP アドレス、色、およびカプセル化で構成される 3 つのタプルによって一意に識別されます。TLOC 情報を表示するには、**show omp tlocs** コマンドを使用します。

デバイス管理の目的で、ベストプラクティスとして、管理目的に適した VPN であるサービス側 VPN にあるループバック インターフェイスにも同じシステム IP アドレスを設定することをお勧めします。ループバック インターフェイスを使用する理由は、ルータが動作していて、オーバーレイネットワークが稼働しているときに常に到達できるためです。物理インターフェイスでシステム IP アドレスを設定する場合、ルータが到達可能であるためには、ルータとインターフェイスの両方が稼働している必要があります。データセンターから到達できるため、サービス側 VPN を使用します。サービス側 VPN は、VPN 0（WAN トランスポート VPN）および VPN 512（管理 VPN）以外の VPN であり、データトラフィックのルーティングに使用されます。

コントロールプレーンの高可用性の設定

可用性の高い Cisco SD-WAN ネットワークには、各ドメインに 2 つ以上の Cisco vSmart コントローラ が含まれています。Cisco SD-WAN ドメインには、最大 8 つの Cisco vSmart コントローラ を含めることができ、デフォルトでは、それぞれの Cisco IOS XE SD-WAN デバイス がそのうちの 2 つに接続します。この値は、トンネルごとに変更します。

その他のインターフェイスの設定

管理でのインターフェイスの構成（VRF mgmt-intf）

すべての Cisco SD-WAN デバイスで、工場出荷時のデフォルト設定の一部として、デフォルトで VPN 512 が帯域外管理に使用されます。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。

Cisco XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。

```
デバイス# show sdwan running-config | sec vrf definition Mgmt-intf

vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
============
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 negotiation auto
exit
============
config-t
ip route vrf Mgmt-intf 10.0.0.1 10.0.0.1
```

設定された管理インターフェイスに関する情報を表示するには、**show interface** コマンドを使用します。次に例を示します。

```
デバイス# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 12 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     4839793 packets input, 415574814 bytes, 0 no buffer
     Received 3060073 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     82246 packets output, 41970224 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

（注） VPN 512 はオーバーレイでアドバタイズされません。デバイスに対してローカルです。オーバーレイ経由で到達可能な管理 VPN が必要な場合は、512 以外の番号で VPN を作成します。

ループバック インターフェイスの設定

インターフェイス名形式 **loopback** *string* を使用します。*string* には任意の英数字を使用でき、下線（_）とハイフン（–）を含めることができます。文字列「loopback」を含むインターフェイス名の合計の長さは、最長16文字です（CLIでのインターフェイスの命名の柔軟性のため、インターフェイス **lo0** と **loopback0** は異なる文字列として解析され、互換性がないことに注意してください。CLIがインターフェイスをループバック インターフェイスとして認識するためには、その名前が完全な文字列 **loopback** で始まる必要があります）。

ループバック インターフェイスの特別な用途の 1 つは、MPLS やメトロ イーサネット ネットワークなどのプライベート WAN でのデータトラフィック交換を設定することです。プライベートネットワークの背後にあるルータがプライベート WAN を介して他のエッジルータと直接通信できるようにするには、実際の物理 WAN インターフェイスではなく、トンネルインターフェイスとして設定されているループバック インターフェイスにデータトラフィックを送信します。

ループバック インターフェイスの暗黙的な ACL

表 *103 :* 機能の履歴

機能名	リリース情報	説明
ループバック インターフェイスの暗黙的な ACL	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、ループバック TLOC インターフェイスで暗黙的な ACL を有効にできます。 ループバック TLOC インターフェイスに独自の暗黙的な ACL がある場合、そのインターフェイス宛てのトラフィックに ACL ルールが適用されます。ループバック TLOC インターフェイスで暗黙的な ACL を有効にすると、制限されたサービスのみが許可されるため、ネットワークセキュリティが強化されます。 ループバック TLOC インターフェイスが Cisco IOS XE SD-WAN デバイスの物理インターフェイスにバインドされている場合、物理インターフェイスは物理 TLOC インターフェイスのように扱われます。

ループバック インターフェイスの暗黙的な ACL に関する情報

ローカライズされたデータポリシーを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。ルータ トンネル インターフェイスには、サービスとも呼ばれる暗黙的な ACL もあります。これらの一部はデフォルトでトンネルインターフェイスに存在し、無効にするまで有効になっています。設定によって、その他の暗黙的な ACL を有効にすることもできます。Cisco IOS XE SD-WAN デバイス では、DHCP、ドメインネームシステム（DNS）、および ICMP サービスがデフォルトで有効になっています。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。

サービスを許可するには、**allow-service** コマンドを使用して暗黙的な ACL を設定および変更します。サービスを禁止するには、**no allow-service** コマンドを使用します。暗黙的な ACL と明示的な ACL の両方が設定されている場合、明示的な ACL は暗黙的な ACL よりも優先されます。

Cisco IOS XE SD-WAN デバイス ループバック インターフェイスにトランスポートロケーション（TLOC）が設定されている場合、暗黙的なACLルールが宛先へのトラフィックに適用されます。ループバックインターフェイスの暗黙的なACLは、バインドモードとアンバインドモードの両方で適用されます。バインドモードは、ループバック インターフェイスがCisco IOS XE SD-WAN デバイス の物理インターフェイスにバインドされてデータを送信するモードです。アンバインドモードでは、ループバックインターフェイスはどの物理インターフェイスにもバインドされません。

物理 WAN インターフェイスにバインドされたループバック TLOC インターフェイス

ループバック インターフェイスがTLOCであり、物理WANインターフェイスにバインドされている場合、トラフィックの宛先に基づいて、対応する暗黙的なACLルールが適用されます。

- ループバック TLOC インターフェイス宛てのトラフィックが物理 WAN インターフェイスで受信された場合、ループバック TLOCインターフェイスで設定された暗黙的なACLルールが適用されます。
- トラフィックの宛先がループバック TLOC インターフェイスではない場合、物理 WAN インターフェイスがTLOC用に設定されているかどうかに応じて、次のルールが適用されます。
  - 物理 WAN インターフェイスに TLOC が設定されていない場合、ルーティングの決定が適用されます。

    TLOCが設定されていない物理インターフェイスにバインドされたループバックTLOCインターフェイスは、物理インターフェイス自体にTLOCが設定されているかのように扱われます。違いは、トラフィックの宛先がデバイスのその他のインターフェイスである場合、そのようなトラフィックはループバックバインドモードで許可されることです。ただし、物理 TLOC の暗黙的な ACL ルールの対象となります。

（注） 物理インターフェイスに TLOC が設定されておらず、ループバック TLOC インターフェイスにバインドされている場合、**implicit-acl-on-bind-intf** コマンドを使用して、物理インターフェイスでの暗黙的な ACL 保護を有効にします。

ループバック TLOC インターフェイスが物理 WAN インターフェイスにバインドされている場合、転送パケットまたはパススルーパケットはドロップされます。これは、物理インターフェイスが TLOC として設定されている場合と同じ動作です。したがって、パケットを転送するには、バインドされた物理インターフェイスで明示的な ACL を設定する必要があります。

次のサンプルシナリオでパススルーパケットを許可するには、明示的な ACL が必要です。

- **オンプレミスデータセンターでホストされているコントローラにアクセスするブランチエッジルータ**：このシナリオでは、物理WANインターフェイスにバインドされたループバックインターフェイスで設定されているデータセンターハブを介して、ブランチエッジルータがコントローラにアクセスすると想定しています。
- **データセンターのインターネット回線を介してクラウドでホストされているコントローラにアクセスするブランチルータ**：このシナリオでは、ブランチルータが MPLS ネットワークを使用してデータセンターエッジに接続されていると想定しています。このようなブランチルータは、物理 WAN インターフェイスにバインドされたループバック インターフェイスで設定されたデータセンターエッジルータを介して、クラウドでホストされているコントローラにアクセスします。

- 物理 WAN インターフェイスに TLOC が設定されている場合、物理 TLOC インターフェイスの暗黙的なACLルールが適用されます。どちらのシナリオでも、パススルートラフィックを許可するには、バインドされた物理 WAN インターフェイスに明示的な ACL が必要です。

物理 WAN インターフェイスにバインドされていないループバック TLOC インターフェイス

ループバック インターフェイスが TLOC であり、物理 WAN インターフェイスにバインドされていない場合、トラフィックの宛先に基づいて、次のように暗黙的な ACL ルールが適用されます。

- ループバック TLOC インターフェイス宛てのトラフィックが物理 WAN インターフェイスで受信された場合、ループバック TLOC の暗黙的な ACL ルールが適用されます。

- トラフィックの宛先がループバック TLOC インターフェイスではない場合、入力物理 WAN インターフェイスが TLOC 用に設定されているかどうかに応じて、次のルールが適用されます。
  - 物理 WAN インターフェイスが TLOC 用に設定されていない場合、ルーティングの決定が適用されます。
  - 物理 WAN インターフェイスが TLOC 用に設定されている場合、設定された暗黙的な ACL ルールが適用されます。

ループバック TLOC のバインドモードとアンバインドモードの違いは、バインドモードでは、バインドされた物理インターフェイスがそれ自体で TLOC として扱われるため、パススルートラフィックがドロップされることです。アンバインドモードでは、パススルートラフィックは許可されます。

バインドモードとアンバインドモードの使用例

バインド モード（Bind Mode）

Cisco IOS XE SD-WAN デバイス には、TLOC として設定され、物理インターフェイス GigabitEthernet1 にバインドされた Loopback1 および Loopback2 があります。このデバイスには、TLOC として設定されていない別のインターフェイスである Loopback3 もあります。

物理インターフェイス GigabitEthernet1 は、着信 VPN 0 の TLOC インターフェイスとして扱われます。

着信 VPN 0 トラフィックの物理インターフェイス GigabitEthernet1 で暗黙的な ACL 保護を有効にするには、**implicit-acl-on-bind-intf** コマンドを使用します。

この例では、次のようになります。

- トラフィックの宛先が Loopback1 である場合、Loopback1 の暗黙の ACL ルールが適用されます。
- トラフィックの宛先が Loopback2 である場合、Loopback2 の暗黙の ACL ルールが適用されます。
- トラフィックの宛先が GigabitEthernet1 の Loopback3 である場合、トラフィックは許可されます。
- トラフィックの宛先が GigabitEthernet1 を通過する別のデバイスである場合、そのトラフィックはドロップされます。

バインドされたインターフェイスである GigabitEthernet1 も TLOC として設定されている場合、Loopback3 へのトラフィックは、GigabitEthernet1 の暗黙的な ACL ルールに従います。

アンバインドモード

Cisco IOS XE SD-WAN デバイス には、TLOC として設定された Loopback1 があり、アンバインドモードになっています。Loopback2 は TLOC として設定されていません。このデバイスには、TLOC として設定されている GigabitEthernet1 インターフェイスと、TLOC として設定されていない GigabitEthernet4 インターフェイスもあります。

この例では、次のようになります。

- Loopback1 宛てのトラフィックが GigabitEthernet1 に到着すると、Loopback1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet1 の場合、GigabitEthernet1 の暗黙的な ACL ルールが適用されます。
- Loopback1 宛てのトラフィックが GigabitEthernet4 に到着すると、Loopback1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet4 の場合、トラフィックは許可されます。
- Loopback2 宛てのトラフィックが GigabitEthernet1 に到着すると、GigabitEthernet1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet1 を通過する別のデバイスである場合、そのトラフィックはドロップされます。

  トラフィックの宛先が GigabitEthernet4 を通過する別のデバイスである場合、トラフィックは転送されます。

ループバック インターフェイスの暗黙的な ACL の利点

ループバック TLOC インターフェイスの暗黙的な ACL は、限定されたサービスのみを許可することにより、サービス妨害（DoS）攻撃から保護します。これによって、ネットワークのセキュリティが強化されます。

ループバック インターフェイスでの暗黙的な ACL の設定

物理 WAN インターフェイスの設定と同様に、機能テンプレートまたは CLI アドオンテンプレートを Cisco vManage で使用して、ループバック インターフェイスに暗黙的な ACL を設定できます。

機能テンプレートを使用してループバック インターフェイスに暗黙的な ACL を設定する方法については、「Configure VPN Ethernet Interface」を参照してください。

CLI アドオンテンプレートの詳細については、「Create a CLI Add-On Feature Template」を参照してください。

CLI を使用したループバック インターフェイスでの暗黙的な ACL の設定

デフォルトでは、DNS、DHCP、ICMP、および HTTPS サービスは許可され、他のサービスは拒否されます。

すべてのサービスを許可するには、**allow-service** *all* コマンドを使用します。

特定のサービスを許可するには、**allow-service** *service name* コマンドを使用します。

サービスを拒否するには、**no allow-service** *service name* コマンドを使用します。

例

次に、ループバック インターフェイスに設定された暗黙の ACL の例を示します。

```
sdwan interface Loopback100
  tunnel-interface
```

```
 no allow-service bgp
 allow-service dhcp
 allow-service dns
 allow-service icmp
 no allow-service sshd
 no allow-service netconf
 no allow-service ntp
 no allow-service ospf
 no allow-service stun
 allow-service https
exit
```

TLOC が設定されたバインドモードのループバック インターフェイスに設定された暗黙的な ACL の設定例

次の例は、TLOC が設定されたバインドモードのループバック インターフェイスに設定された暗黙的な ACL を示しています。

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

TLOC が設定されたアンバインドモードのループバック インターフェイスに設定された暗黙的な ACL の設定例

次の例は、TLOC が設定されたアンバインドモードのループバック インターフェイスに設定された暗黙的な ACL を示しています。

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
```

```
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

ループバック インターフェイスの暗黙的な ACL のモニタリング

show platform hardware qfp active statistics drop コマンドを使用して、ループバック インターフェイスの暗黙的な ACL 設定を監視します。

例

次に、**show platform hardware qfp active statistics drop** コマンドの出力例を示します。

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-------------------------------------------------------------------------
Global Drop Stats                          Packets              Octets
-------------------------------------------------------------------------
Disabled                                         4                 266
Ipv4EgressIntfEnforce                           15               10968
Ipv6NoRoute                                      6                 336
Nat64v6tov4                                      6                 480
SVIInputInvalidMac                             244               15886
SdwanImplicitAclDrop                           160               27163
UnconfiguredIpv4Fia                         942525            58524580
UnconfiguredIpv6Fia                          77521             9587636
```

サブインターフェイスの設定

IP MTU 値を指定しないサブインターフェイスを作成すると、そのサブインターフェイスは親インターフェイスから IP MTU 値を継承します。サブインターフェイスに異なる IP MTU 値を設定する場合は、サブインターフェイスの設定で **ip mtu** コマンドを使用して、サブインターフェイスの IP MTU を設定します。

次に例を示します。

```
interface GigabitEthernet0/0/0
 mtu 1504
 no ip address
!
interface GigabitEthernet0/0/0.9
 encapsulation dot1Q 9
 no shutdown
 ip address 192.168.9.32 255.255.255.0
!
```

```
interface Tunnel9
 no shutdown
 ip unnumbered GigabitEthernet0/0/0.9
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0.9
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0.9
 tunnel mode sdwan
!
sdwan
 interface GigabitEthernet0/0/0.9
  tunnel-interface
   encapsulation ipsec
   color private1
  !
 !
```

インターフェイスプロパティの設定

インターフェイス速度の設定

Cisco IOS XE SD-WAN デバイス が起動すると、Cisco SD-WAN ソフトウェアはルータに存在する SFP を自動検出し、それに応じてインターフェイス速度を設定します。次に、ソフトウェアは、接続のリモートエンドにあるデバイスとインターフェイス速度をネゴシエートして、インターフェイスの実際の速度を確立します。ルータに存在するハードウェアを表示するには、**show hardware inventory** コマンドを使用します。

各インターフェイスの実際の速度を表示するには、**show interface** コマンドを使用します。ここで、WAN クラウドに接続するインターフェイス [ge0/0] は 1000 Mbps（1Gbps、上記の出力で強調表示されている 1GE PIM）で実行されており、ローカルサイトのデバイスに接続するインターフェイス [ge0/1] は、100 Mbps の速度をネゴシエートしました。

システム IP アドレスやループバック インターフェイスなどの非物理インターフェイスの場合、インターフェイス速度はデフォルトで 10 Mbps に設定されます。

インターフェイス上の 2 つのデバイスによってネゴシエートされた速度を無効にするには、自動ネゴシエーションを無効にして、目的の速度を設定します。

Cisco vSmart コントローラ および Cisco vManage システムの場合、初期インターフェイス速度は 1000 Mbps であり、動作速度はインターフェイスのリモートエンドにあるデバイスとネゴシエートされます。コントローラインターフェイスの速度は、仮想化プラットフォーム、使用される NIC、およびソフトウェアに存在するドライバによって異なる場合があります。

インターフェイス MTU の設定

デフォルトでは、すべてのインターフェイスの MTU は 1500 バイトです。これはインターフェイスで変更できます。

Cisco IOS XE リリース 17.4.1a より前のリリースでは、MTU の範囲は 576 ～ 2000 バイトです。

Cisco IOS XE リリース 17.4.1a 以降のリリースでは、MTU の範囲は 1 GE インターフェイスで 576 ～ 9216 バイトです。この MTU 範囲は、Cisco IOS XE リリース 17.5.1a 以降の 10 GE および 100 GE インターフェイスでもサポートされています。

インターフェイスの MTU を表示するには、**show interface** コマンドを入力します。

Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラデバイスでは、ICMP を使用して Path MTU（PMTU）ディスカバリを実行するようにインターフェイスを設定できます。PMTU ディスカバリが有効になっている場合、デバイスは、パケット フラグメンテーションを排除または最小限に抑えるために、インターフェイスでサポートされる最大 MTU サイズを自動的にネゴシエートします。

Cisco IOS XE SD-WAN デバイス デバイスの Cisco SD-WAN BFD ソフトウェアは、各トランスポート接続（つまり、各TLOCまたは色）でPMTUディスカバリを自動的に実行します。BFD PMTUディスカバリはデフォルトで有効になっていて、無効にせずに使用することをお勧めします。PMTU ディスカバリを実行するように BFD を明示的に設定するには、**bfd color pmtu-discovery** コンフィギュレーション コマンドを使用します。ただし、代わりに ICMP を使用して PMTU ディスカバリを実行することも選択できます。vEdge クラウドルータ

BFD はデータプレーンプロトコルであるため、Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラデバイスでは実行されません。

TCP MSS と [Clear Dont Fragment] の設定

表 *104 :* 機能の履歴

機能名	リリース情報	説明
TCP MSS の設定	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、Cisco SD-WAN トンネルインターフェイスの両方向で Cisco IOS XE SD-WAN デバイス の TCP MSS 調整サポートが追加されます。
[Clear Dont Fragment] オプションの設定	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、Cisco SD-WAN トンネルで送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアするオプションを提供します。[Don't Fragment] 設定をクリアすると、インターフェイス MTU より大きいパケットは送信前にフラグメント化されます。

TCP 最大セグメントサイズ（MSS）は、TCP ヘッダーまたは IP ヘッダーをカウントせずに、通信デバイスが単一の TCP セグメントで受信できるデータの最大量をバイト単位で指定する

パラメータです。MSS は、TCP ハンドシェイク中の TCP SYN パケットで最初に TCP MSS として指定されます。MSS 値が小さいと、IP フラグメンテーションが減少するかまたは排除され、オーバーヘッドが大きくなります。

デバイスを通過する TCP SYN パケットの MSS を設定できます。デフォルトでは、MSS は、TCP SYN パケットが決してフラグメント化されないように、インターフェイスまたはトンネルの最大伝送ユニット（MTU）に基づいて動的に調整されます。インターフェイスを介して送信されるデータの場合、MSS は、インターフェイス MTU、IP ヘッダー長、および最大 TCP ヘッダー長を加算して計算されます。

制限事項

- TCP MSS 値は、Cisco SD-WAN トンネルインターフェイスに対してのみ調整できます。

（注） Cisco IOS XE リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降、サービス VPN の場合、またはネットワークアドレス変換（NAT）ダイレクトインターネットアクセス（DIA）を使用する場合に TCP MSS 値を調整できます。TCP MSS 値を調整すると、TCP セッションのドロップを防ぐことができます。

NAT DIA の詳細については、『*Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE リリース 17.x*』を参照してください。

- [Clear Dont Fragment] オプションは、Cisco SD-WAN トンネルインターフェイスでのみ使用できます。

TCP MSS と [Clear Dont Fragment] の設定

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. 新しい CLI アドオン機能テンプレートを作成するか、次のいずれかのテンプレートを編集します。次の機能テンプレートのいずれかを使用して、TCP MSS を構成し、Dont Fragment をクリアできます。
   - VPN Ethernet インターフェイス
   - VPN インターフェイス DSL IPoE
   - VPN インターフェイス DSL PPoA
   - VPN インターフェイス DSL PPPoE

- VPN インターフェイス マルチリンク
- VPN インターフェイス T1/E1
- セルラーインターフェイス

新しい CLI アドオン機能テンプレートの作成の詳細については、「Create a CLI Add-on Feature Templates」を参照してください。

4. [Tunnel] をクリックします。
5. TCP MSS を設定するには、[Tunnel TCP MSS] で、Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

   TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダーの値がすでに TCP MSS よりも低い場合は、変更されずに通過します。トンネルの最後にあるホストは、2 つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。
6. [Clear-Dont-Fragment] オプションをクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Don't Fragment ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。

（注） フラグメンテーションが必要で、Dont Fragment ビットが設定されている場合に、[Clear-Dont-Fragment] は Dont Fragment ビットをクリアします。フラグメンテーションを必要としないパケットの場合、Don't Fragment ビットは影響を受けません。

7. [Save] または [Update] をクリックします。

CLI を使用した TCP MSS の設定

次のコマンドを使用して、CLI で TCP MSS を構成します。

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

TCP MSS 構成の確認

次に、**show platform hardware qfp active feature sdwan datapath session summary** コマンドのサンプル出力を示します。

```
Device#show platform hardware qfp active feature sdwan datapath session summary
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU
```

```
------          ------          -------- -------    ------   -------  ----------- -----
10.1.15.25      10.1.14.14      12347    12346      IPSEC    65526    10007       1446
10.1.15.25      10.0.5.21       12347    12357      IPSEC    65526    10009       1446
10.1.15.25      10.0.5.11       12347    12347      IPSEC    65526    10008       1446
10.1.15.25      10.1.16.16      12347    12366      IPSEC    65526    10006       1446
```

CLI での [Clear Dont Fragment] の設定

次のコマンドを使用して、CLI を使用して [Clear Dont Fragment] オプションを設定します。

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
```

CLI での Dont Fragment 設定の確認

次に、[Clear-dont-fragment] が有効かどうかを確認する **show platform software interface rp active name Tunnel1** コマンドの出力例を示します。

```
Device# show platform software interface rp active name Tunnel1 | include dont
IP Clear-dont-fragment: TRUE
```

次に、[Clear-dont-fragment] が有効な場合の実行コンフィギュレーションを表示する **show running-config interface Tunnel1** コマンドの出力例を示します。

```
Device# show running-config interface Tunnel1
Building configuration...

Current configuration : 132 bytes
!
interface Tunnel1
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end
```

トランスポート回線の帯域幅のモニタリング

トランスポート回線の帯域幅使用量をモニタリングして、帯域幅使用量の傾向を判断できます。帯域幅使用量が最大値に近づき始めた場合、通知を送信するようにソフトウェアを設定できます。通知は、Cisco vManage NMS、SNMP トラップ、および syslog メッセージに送信される Netconf 通知として送信されます。回線のキャパシティプランを行うときや、帯域幅使用量に関する傾向情報を収集するときなど、帯域幅のモニタリングのためにこの機能を有効にすることができます。また、この機能を有効にして、帯域幅使用量に関するアラートを受信することもできます。たとえば、トランスポートインターフェイスがトラフィックで飽和状態になって顧客のトラフィックに影響を与える時期を判断する必要がある場合や、顧客が LTE トランスポートのケースのように従量課金プランを利用している場合などです。

インターフェイス帯域幅をモニタリングするには、トランスポート回線で送受信されるトラフィックの最大帯域幅を設定します。最大帯域幅は、通常、回線プロバイダーとネゴシエート

された帯域幅です。帯域幅使用量が受信または送信トラフィックの設定値の85%を超えると、SNMPトラップの形式で通知が生成されます。具体的には、インターフェイストラフィックは10秒ごとにサンプリングされます。受信または送信された帯域幅が、連続する5分間にサンプリングされた間隔の 85% で設定値の 85% を超えると、SNMP トラップが生成されます。最初のトラップが生成された後、サンプリングは同じ頻度で続行されますが、通知は1時間に1回に制限されます。次の1時間に10秒のサンプリング間隔の 85% で帯域幅が値の 85% を超えると、2つ目（およびそれ以降）のトラップが送信されます。1時間後にもう1つのトラップが送信されない場合、通知間隔は5分に戻ります。

Cisco IOS XE SD-WAN デバイスおよび Cisco vManage NMS でトランスポート回線の帯域幅をモニタリングできます。

物理インターフェイスで受信したトラフィックの帯域幅が特定の帯域幅の 85% を超えたときに通知を生成するには、ダウンストリーム帯域幅を設定します。

物理インターフェイスで送信されるトラフィックの帯域幅が特定の帯域幅の 85% を超えたときに通知を生成するには、アップストリーム帯域幅を設定します。

どちらの設定コマンドでも、帯域幅は 1 ～ 2147483647（2^{32} / 2）– 1 kbps の範囲で指定できます。

設定された帯域幅を表示するには、**show interface detail** コマンドの出力で、bandwidth-downstream フィールドと bandwidth-upstream フィールドを確認します。このコマンドの rx-kbps および tx-kbps フィールドには、インターフェイスの現在の帯域幅使用量が表示されます。

Cisco vManage を使用した DHCP サーバーの有効化

表 *105 :* 機能の履歴

機能名	リリース情報	機能説明
DHCP オプションのサポート	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能により、DHCP サーバーオプション 43 および 191 は、クライアントとサーバーの交換でベンダー固有の情報を設定できます。

すべての Cisco SD-WAN に DHCP サーバーテンプレートを使用します。

Cisco SD-WAN デバイスインターフェイスで DHCP サーバー機能を有効にして、サービス側ネットワーク内のホストに IP アドレスを割り当てることができるようにします。

Cisco vManage テンプレートを使用して DHCP サーバーとして機能するように Cisco SD-WAN デバイスを設定するには、次の手順を実行します。

1. このトピックの説明に従って、DHCPサーバー機能テンプレートを作成し、DHCPサーバーパラメータを設定します。

2. VPN-Interface-Ethernet および VPN-Interface-PPP-Ethernet のヘルプトピックの説明に従って、1 つ以上のインターフェイス機能テンプレートを作成します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

Cisco IOS XE SD-WAN デバイスインターフェイスを DHCP ヘルパーとして設定して、DHCP サーバーから受信したブロードキャスト DHCP 要求を転送するようにするには、該当するインターフェイス テンプレートの [DHCP Helper] フィールドに、DHCP サーバーのアドレスを入力します。

[Template] 画面に移動し、テンプレートに命名する

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] 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. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
6. [Service VPN] ドロップダウンリストをクリックします。
7. [Additional VPN Templates] から、[VPN Interface] をクリックします。
8. [Sub-Templates] ドロップダウンリストから、[DHCP Server] を選択します。
9. [DHCP Server] ドロップダウンリストから、[Create Template] をクリックします。[DHCP-Server] 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、DHCP サーバ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。
10. [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。
11. [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。

DHCP サーバーの最小限の設定

DHCP サーバー機能を設定するには、[Basic Configuration] を選択して、次のパラメータを設定します。DHCP 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 *106*:

パラメータ名	説明
Address Pool*	ルータインターフェイスが DHCP サーバーとして機能するサービス側ネットワークのアドレスプールの IPv4 プレフィックス範囲を、*prefix/length* の形式で入力します。
Exclude Addresses	DHCP アドレスプールから除外する 1 つ以上の IP アドレスを入力します。複数の個別のアドレスを指定するには、それらをカンマで区切ってリストします。アドレスの範囲を指定するには、ハイフンで区切ります。
Maximum Leases	このインターフェイスに割り当てることができる IP アドレスの数を指定します。範囲：0 ～ 4294967295
リース時間	DHCP によって割り当てられた IP アドレスが有効である時間を指定します範囲：0 ～ 4294967295 秒
Offer Time	DHCP クライアントに提供された IP アドレスがそのクライアントのために予約される期間を指定します。デフォルトでは、提供された IP アドレスは、DHCP サーバーがアドレスを使い果たすまで無期限に予約されます。その時点で、アドレスは別のクライアントに提供されます。範囲：0 ～ 4294967295 秒、デフォルト：600 秒
管理ステート	インターフェイスで DHCP 機能を有効にする場合は [Up]、無効にする場合は [Down] を選択します。デフォルトでは、DHCP サーバー機能はインターフェイスで無効になっています。

機能テンプレートを保存するには、[Save] をクリックします。

静的リースの設定

静的リースを設定し、サービス側ネットワーク上のクライアントデバイスに静的 IP アドレスを割り当てるには、[Static Lease] をクリックし、[Add New Static Lease] をクリックして、次のパラメータを設定します。

表 *107 :*

パラメータ名	説明
MACアドレス（MAC Address）	静的IPアドレスが割り当てられるクライアントのMACアドレスを入力します。
IP アドレス	クライアントに割り当てる静的 IP アドレスを入力します。
ホストネーム	クライアントデバイスのホスト名を入力します。

静的リースを編集するには、鉛筆アイコンをクリックします。

静的リースを削除するには、ごみ箱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。

詳細オプションの設定

DHCP サーバーの詳細オプションを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 *108 :*

パラメータ名	説明
インターフェイス MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：68 ～ 65535 バイト
ドメイン名	DHCP クライアントがホスト名を解決するために使用するドメイン名を指定します。
デフォルト ゲートウェイ	サービス側ネットワークのデフォルトゲートウェイの IP アドレスを入力します。
DNS サーバー	サービス側ネットワークの DNS サーバーの IP アドレスを 1 つ以上入力します。複数のエントリがある場合は、カンマで区切ります。最大 8 つのアドレスを指定できます。
TFTP サーバ	サービス側ネットワークの TFTP サーバーの IP アドレスを入力します。1 つまたは 2 つのアドレスを指定できます。2 つの場合、アドレスはカンマで区切ってください

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 DHCP サーバーの設定

```
Device# config-transaction
Device(dhcp-config)# ip dhcp pool DHCP-POOL
Device(dhcp-config)# network 10.1.1.1 255.255.255.0
Device(dhcp-config)# default-router 10.1.1.2
Device(dhcp-config)# dns-server 172.16.0.1
```

```
Device(dhcp-config)# domain-name DHCP-DOMAIN
Device(dhcp-config)# exit
Device(config)ip dhcp excluded-address 10.1.1.2 10.1.1.10
Device(
```

リリース情報

リリース 15.2 の Cisco vManage で導入されました。

PPPoE の設定

Point-to-Point Protocol over Ethernet（PPPoE）は、一般的な顧客宅内機器を介して、イーサネットローカルエリアネットワーク経由で複数のユーザーをリモートサイトに接続します。PPPoE は一般的に、デジタル加入者線（DSL）などのブロードバンドアグリゲーションで使用されます。PPPoE は、CHAP または PAP プロトコルによる認証を提供します。Cisco SD-WAN オーバーレイネットワークでは、Cisco SD-WAN デバイスが PPPoE クライアントを実行できます。PPPoE サーバーコンポーネントはサポートされていません。

Cisco SD-WAN デバイスで PPPoE クライアントを設定するには、PPP 論理インターフェイスを作成し、それを物理インターフェイスにリンクします。物理インターフェイスが起動すると、PPPoE 接続が起動します。PPP インターフェイスは Cisco SD-WAN デバイス上の 1 つの物理インターフェイスのみにリンクでき、物理インターフェイスは 1 つの PPP インターフェイスのみにリンクできます。Cisco SD-WAN デバイスで複数の PPPoE インターフェイスをイネーブルにするには、複数の PPP インターフェイスを設定します。

Quality of Service（QoS）とシェーピングレートは、PPP インターフェイスではなく、PPPoE 対応の物理インターフェイスで設定することをお勧めします。

PPPoE 対応の物理インターフェイスでは、以下はサポートされていません。

- 802.1Q
- サブインターフェイス
- NAT、PMTU、およびトンネルインターフェイス。これらは PPP インターフェイスで設定されているため、PPPoE 対応のインターフェイスでは使用できません。

PPPoE の Cisco SD-WAN 実装では、RFC 1962 で定義されている Compression Control Protocol（CCP）オプションはサポートされていません。

vManage テンプレートからの PPPoE の設定

vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイスで PPPoE を設定するには、3 つの機能テンプレートと 1 つのデバイステンプレートを作成します。

- VPN-Interface-PPP 機能テンプレートを作成して、PPP 仮想インターフェイスの PPP パラメータを設定します。
- VPN-Interface-PPP-Ethernet 機能テンプレートを作成して、PPPoE 対応インターフェイスを設定します。

- 必要に応じて、VPN 機能テンプレートを作成して、VPN 0 の既定の構成を変更します。
- VPN-Interface-PPP、VPN-Interface-PPP-Ethernet、および VPN 機能テンプレートを組み込んだデバイステンプレートを作成します。

VPN-Interface-PPP 機能テンプレートを作成して、PPP 仮想インターフェイスの PPP パラメータを設定します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。

（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。

3. Cisco IOS XE SD-WAN デバイスクラウドまたはルータモデルを選択します。
4. [VPN-Interface-PPP] テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

表 109：

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
シャットダウン	[No] をクリックして、PPP 仮想インターフェイスを有効にします。
Interface Name	PPP インターフェイスの番号を入力します。1 ～ 31 で指定できます。
説明（Description）（任意）	PPP 仮想インターフェイスの説明を入力します。
認証プロトコル（Authentication Protocol）	CHAP または PAP のいずれかを選択して 1 つの認証プロトコルを設定するか、PAP と CHAP を選択して両方を設定します。CHAP の場合は、ISP から提供されたホスト名とパスワードを入力します。PAP の場合は、ISP から提供されたユーザー名とパスワードを入力します。PAP と CHAP の両方を設定する場合、両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] をクリックします。
AC Name（オプション）	[PPP] タブを選択し、[AC Name] フィールドに、インターネットへの接続をルーティングするために PPPoE が使用するアクセスコンセントレータの名前を入力します。

パラメータフィールド	手順
IP MTU	[Advanced] をクリックし、[IP MTU] フィールドで、IP MTU が物理インターフェイスの MTU よりも少なくとも 8 バイト少ないことを確認します。PPP インターフェイスの最大 MTU は 1492 バイトです。PPPoE サーバーで Maximum Receive Unit（MRU）が指定されていない場合、PPP インターフェイスの MTU 値が MRU として使用されます。 Cisco vManage リリース 20.9.1 以降では、設定がデバイスにプッシュされるときに、指定された IP MTU 値に基づいて 8 バイトのオーバーヘッドが推定されます。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN-Interface-PPP-Ethernet 機能テンプレートを作成して物理インターフェイスで PPPoE クライアントを有効にするには、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. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。

（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。

3. クラウドまたはルータモデルを選択します。
4. [VPN-Interface-PPP-Ethernet] テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
シャットダウン	[No] をクリックして、PPPoE 対応インターフェイスを有効にします。
Interface Name	PPP インターフェイスに関連付ける VPN 0 の物理インターフェイスの名前を入力します。
説明（Description）（任意）	PPPoE 対応インターフェイスの説明を入力します。

パラメータフィールド	手順
IP Configuration	物理インターフェイスに IP アドレスを割り当てます。 • DHCP を使用するには、[Dynamic] を選択します。DHCP から学習したルートのデフォルトのアドミニストレーティブディスタンスは 1 です。 • IP アドレスを直接設定するには、インターフェイスの IPv4 アドレスを入力します。
DHCP Helper（オプション）	ネットワーク内の DHCP サーバーの IP アドレスを 4 つまで入力します。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN 機能テンプレートを作成して、VPN 0、トランスポート VPN で PPPoE 対応インターフェイスを設定するには、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. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。

（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。

3. クラウドまたはルータモデルを選択します。
4. [VPN] テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
VPN 識別子	VPN 識別子 0 を入力します。
名前	VPN の名前を入力します。
Other interface parameters	必要なインターフェイスプロパティを設定します。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN-Interface-PPP、VPN-Interface-PPP-Ethernet、およびVPN機能テンプレートを組み込んだデバイステンプレートを作成するには、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. [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] 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、デバイス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。

   vManage NMS に、選択したデバイスタイプの機能テンプレートが表示されます。必須のテンプレートはアスタリスク（*）で示されます。
5. デバイステンプレートの名前と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字は使用できません。
6. [Transport & Management VPN] の [VPN 0] で、使用可能なテンプレートのドロップダウンリストから、目的の機能テンプレートを選択します。使用可能なテンプレートのリストは、以前に作成したテンプレートです。
7. [Additional VPN 0 Templates] で、[VPN Interface PPP] の横にあるプラス記号（+）をクリックします。
8. [VPN-Interface-PPP] および [VPN-Interface-PPP-Ethernet] フィールドから、使用する機能テンプレートを選択します。
9. VPN 0 で複数の PPPoE 対応インターフェイスを設定するには、[Sub-Templates] の横にあるプラス記号（+）をクリックします。
10. デバイステンプレートに追加の機能テンプレートを含めるには、残りのセクションで機能テンプレートを順に選択し、使用可能なテンプレートのドロップダウンリストから目的のテンプレートを選択します。使用可能なテンプレートのリストは、以前に作成したテンプレートです。すべての必須機能テンプレート、および目的の任意の機能テンプレートのテンプレートを選択していることを確認してください。
11. デバイステンプレートを作成するには、[Create] をクリックします。

デバイステンプレートをデバイスにアタッチするには、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. [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. テンプレートを選択します。
4. [...] をクリックして、[Attach Device] をクリックします。
5. デバイスを検索するか、左側の [Available Device(s)] 列からデバイスを選択します。
6. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。
7. [Attach] をクリックします。

PPPoE Over ATM の設定

表 *110*：機能の履歴

機能名	リリース情報	説明
PPPoE over ATM の設定	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、Cisco IOS XE SD-WAN デバイスでの PPPoEoA の設定をサポートします。PPPoEoA は AAL5MUX カプセル化を使用しており、他のカプセル化方法と比較して効率が優れています。

ADSL をサポートする Cisco IOS XE SD-WAN デバイスで PPPoE over ATM インターフェイス（PPPoEoA）を設定できます。PPPoEoA は、ATM Adaptation Layer 5 Multiplexed Encapsulation（AAL5MUX）カプセル化を使用して、ATM 相手先固定接続（PVC）上で PPPoE を伝送し、AAL5 LLC/SNAP カプセル化よりも効率が向上します。

PPPoEoA over AAL5MUX は、多重化（MUX）カプセル化を使用して、音声パケットの伝送に必要なセルの数を減らすことにより、サブネットワークアクセスプロトコル（SNAP）カプセル化の帯域幅使用量を削減します。PPPoEoA over ATM AAL5MUX 機能を VoIP 環境に導入すると、スループットと帯域幅の使用率が向上します。

PPPoE Over ATM でサポートされるプラットフォーム

次のプラットフォームは、PPPoE over ATM をサポートしています。

- Cisco 1100 4G/6G シリーズ サービス統合型ルータ。
- Cisco 1100 シリーズ サービス統合型ルータ。

- Cisco 1109 シリーズ サービス統合型ルータ。
- Cisco111x シリーズ サービス統合型ルータ。
- Cisco1111x シリーズ サービス統合型ルータ。
- Cisco 1120 シリーズ サービス統合型ルータ。
- Cisco 1160 シリーズ サービス統合型ルータ。

Cisco vManage を使用した PPPoE Over ATM の設定

デバイス CLI テンプレートを使用して、Cisco vManage で PPPoE を設定できます。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] から、[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] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[CLI 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. [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。
6. [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。
7. [Device configuration] を選択します。このオプションを使用すると、`show sdwan running-config` コマンドの出力に表示される IOS-XE 設定コマンドを指定できます。
8. （オプション）接続されたデバイスの実行構成をロードするには、[Load Running config from reachable device] リストからそのデバイスを選択し、[Search] をクリックします。
9. [CLI Configuration] で、手入力するか、カットアンドペーストするか、ファイルをアップロードして、設定を入力します。PPPoEoA の設定は、「CLI での PPPoE Over ATM の設定」セクションにあります。
10. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{*variable-name*}}; の形式で変数名を直接入力することもできます。たとえば、{{hostname}} です。
11. [Add] をクリックします。新しいデバイステンプレートが [Device Template] テーブルに表示されます。[Type] 列には、デバイステンプレートが CLI テキストから作成されたことを示す「CLI」が表示されます。

CLI での PPPoE Over ATM の設定

このセクションでは、CLI で PPPoE over ATM を設定するための CLI 設定例を示します。

```
Device(config)# interface atm number
Device(config)# no ip address
Device(config)# interface atm number point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# encapsulation aal5mux  pppoe-client
Device(config)# pppoe-client dial-pool-number number
Device(config)# interface Dialer dialer-rotary-group-number
Device(config)# mtu bytes
Device(config)# ip address negotiated
Device(config-if)# encapsulation encapsulation-type
Device(config)# load-interval seconds
Device(config)# dialer pool number
Device(config)# dialer-group group-number
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname hostname
Device(config)# ppp chap password secret
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
```

PPPoE Over ATM インターフェイスの設定例

次に、ATM インターフェイスでの PPPoE の設定例を示します。

```
Device(config)# interface ATM0/1/0
Device(config)# no ip address
Device(config)# no atm enable-ilmi-trap
!
Device(config)# interface ATM0/1/0.10 point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# cdp enable
Device(config)# pvc 22/62
Device(config)# ubr 1045
Device(config-if)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number 120
!
!
Device(config)# interface Dialer 120
Device(config)# mtu 1492
Device(config)# ip address negotiated
Device(config)# ip nat outside
Device(config-if)# encapsulation ppp
Device(config)# load-interval 30
Device(config)# dialer pool 120
Device(config)# dialer-group 1
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname test@cisco.com
Device(config)# ppp chap password 0 cisco
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
!
```

VRRP の設定

（注） VRRP が機能するには、x710 NIC に **t->system-> vrrp-advt-with-phymac** コマンドが設定されている必要があります。

Virtual Router Redundancy Protocol（VRRP）は、スイッチおよび他の IP エンドステーションに冗長ゲートウェイサービスを提供する LAN 側のプロトコルです。Cisco SD-WAN ソフトウェアでは、VPN内のインターフェイス（通常はサブインターフェイス）でVRRPを設定します。

VRRP はサービス側 VPN（VPN 0 および 512 が予約済み）でのみサポートされており、サブインターフェイスを使用する場合は、VPN 0 で VRRP 物理インターフェイスを設定する必要があります。

VRRPインターフェイス（またはサブインターフェイス）ごとに、IPアドレスを割り当て、そのインターフェイスを VRRP グループに配置します。

グループ番号は仮想ルータを識別します。ルータには最大512のグループを設定できます。一般的な VRRP トポロジでは、2 つの物理ルータが単一の仮想ルータとして機能するように構成するため、これら両方のルータのインターフェイスに同じグループ番号を設定します。

各仮想ルータ ID に対して 1 つの IP アドレスを設定する必要があります。

各 VRRP グループ内では、プライオリティ値の高いルータ がプライマリ VRRP として選択されます。デフォルトでは、各仮想ルータの IP アドレスのデフォルトプライマリ選択プライオリティは 100 であるため、より高い IP アドレスのルータがプライマリとして選択されます。プライオリティ値は、1 ～ 254 の値に設定して変更できます。

プライマリ VRRP は、まだ動作していることを示すアドバタイズメント メッセージを定期的に送信します。バックアップルータが 3 つの連続した VRRP アドバタイズメントを失うと、プライマリ VRRP がダウンしていると見なされ、新しいプライマリ VRRP が選択されます。デフォルトでは、これらのメッセージは 1 秒ごとに送信されます。VRRP アドバタイズメントの時間は、1 ～ 3600 秒の値に変更できます。

デフォルトでは、VRRP は、どのルータがプライマリ仮想ルータであるかを判別するために、VRRP が実行されているインターフェイスの状態を使用します。このインターフェイスは、ルータのサービス（LAN）側にあります。プライマリ VRRP のインターフェイスがダウンすると、VRRP プライオリティ値に基づいて新しいプライマリ VRRP 仮想ルータが選択されます。VRRP は LAN インターフェイスで実行されるため、ルータがすべての WAN 制御接続を失った場合、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを設定します。

- プライマリ VRRP 仮想ルータを決定するときに、WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションを追跡します。

プライマリ VRRP ルータですべての OMP セッションが失われた場合、VRRP は 1 つ以上のアクティブな OMP セッションを持つすべてのゲートウェイの中から新しいデフォルトゲートウェイを選択します。これは、選択されたゲートウェイの VRRP プライオリティが現在のプライマリ VRRP ルータよりも低い場合にも実行されます。このオプションでは、OMP 状態がアップからダウンに変化すると、VRRP フェールオーバーが発生します。この変化は、OMP ホールドタイマーが期限切れになったときに発生します（デフォルトの OMP ホールドタイマー間隔は 60 秒です）。ホールドタイマーが期限切れになり、新しいプライマリ VRRP が選択されるまでは、すべてのオーバーレイトラフィックがドロップされます。OMP セッションが回復すると、ローカル VRRP インターフェイスは 、Cisco vSmart コントローラから OMP ルートを学習およびインストールする前でも、自身をプライマリ VRRP として主張します。ルータが学習されるまでは、トラフィックもドロップされます。

- OMP セッションとリモートプレフィックスのリストの両方を追跡します。

すべての OMP セッションが失われた場合、**track-omp** オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、 ルータがプライマリ VRRP を決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。

先ほど説明したように、IEEE 802.1Q プロトコルは各パケットの長さに 4 バイトを追加します。したがって、パケットを送信するには、VPN 0 の物理インターフェイスの MTU サイズを増やすか（デフォルトの MTU は 1500 バイトです）、VRRP インターフェイスの MTU サイズを減らします。

動的インターフェイスの設定

表 *111 :* 機能の履歴

機能名	リリース情報	説明
動的インターフェイスの設定	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.2	この機能を使用すると、サポートされているデバイスの動的インターフェイスを設定できます。動的インターフェイスにより、デバイスはリアルタイムで最適なパスを選択できます。 この機能は、Cisco C8500-12X4QC ルータにのみ適用されます。

サポートされているデバイスの動的インターフェイスを設定できます。動的インターフェイスにより、デバイスはリアルタイムで最適なパスを選択できます。

動的インターフェイスの設定は、次の一般的な手順で構成されます。

1. 動的インターフェイスモード機能テンプレートを作成します。この手順の一部として、デバイスのベイのモードを定義します。
2. 制御接続のインターフェイスを設定します。
3. 動的インターフェイスモード機能テンプレートをデバイステンプレートに関連付けます。

動的インターフェイスモード機能テンプレートの作成

動的インターフェイスモード機能テンプレートを作成するときは、デバイスのベイのモードを定義するテンプレートを作成します。

ベイ 1、ベイ 2、またはその両方のモードを設定できます。

ベイ 0 のモードは自動的に設定され、変更できません。ベイ 1 のモードを 100G に設定すると、ベイ 0 の 10G インターフェイスは適用されないため、ベイ 0 は無効になります。

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をクリックし、[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を選択します。
5. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
6. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
7. [Additional Templates] から、[Dynamic Interface Mode] ドロップダウンリストを選択し、[Create Template] をクリックします。
8. [Template Name] に、テンプレートの名前を入力します。

   このフィールドには、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）を使用できます。
9. [Description] にテンプレートの説明を入力します。

   このフィールドには任意の文字とスペースを使用できます。
10. [Bay 1]、[Bay 2]、または両方のフィールドで目的の値を選択して、ベイ 1、ベイ 2、または両方のベイのモードを設定します。

ベイ 0 のデフォルト値は変更できません。

11. **[Save]** をクリックします。

制御接続のインターフェイスを構成する

このセクションでは、「動的インターフェイスモード機能テンプレートの作成」で設定したベイで動作するように、既存の制御接続用の新しいVPN 0インターフェイスを設定する方法について説明します。また、インターフェイスの IPv4 ルートを設定する方法についても説明します。

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. インターフェイスを設定するテンプレートの [...] をクリックし、[Edit] を選選択します。
4. [Transport & Management VPN] をクリックし、次のアクションを実行してベイのインターフェイスを作成します。
   1. [Additional VPN 0 Template] で [VPN Interface] をクリックします。
   2. 表示される新しい [VPN Interface Ethernet] メニューを選択し、[Create Template] をクリックします。
   3. [Template Name] に、テンプレートの名前を入力します。

      このフィールドには、英大文字と小文字、0～9の数字、ハイフン（-）、下線（_）を使用できます。
   4. [Description] にテンプレートの説明を入力します。

      このフィールドには任意の文字とスペースを使用できます。
   5. 「動的インターフェイスモード機能テンプレートの作成」の説明に従って、設定したベイに制御接続を追加します。
5. [Basic Configuration] を選択し、次のアクションを実行します。
   1. [Interface Name] にインターフェイスの名前を入力します。

      この例に示す形式で名前を入力します。「FortyGigabitEthernet0/1/0」。
   2. 必要に応じてこのタブの他のオプションを設定します。
6. [Tunnel] から、[Tunnel Interface] を [On] に設定します。
7. **[Save]** をクリックします。

8. [IPv4 Route] を選択し、次のアクションを実行して、VPN0 テンプレートの IPv4 ルートを設定します。
   1. [New IPv4 Route] をクリックします。
   2. [Prefix] に、IPv4 ルートのプレフィックスを入力します。
   3. [Gateway] で、[Next Hop] を選択します。
   4. [Next Hop] で必要に応じて項目を構成し、[Add] をクリックします。
   5. **[Save]** をクリックします。
9. [更新（Update）] をクリックします。

動的インターフェイスモード機能テンプレートとデバイステンプレートの関連付け

動的インターフェイスモード機能テンプレートを作成したら、それをデバイステンプレートに関連付け、デバイステンプレートをデバイスに接続します。手順については、「機能テンプレートからのデバイステンプレートの作成」を参照してください。

VPN イーサネット インターフェイスの設定

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 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] のタイトルは [Device] です。

ステップ 3 [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。

ステップ 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。

ステップ 5 VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
2. [Additional VPN 0 Templates] で、**[Cisco VPN Interface Ethernet]** をクリックします。
3. From the **VPN Interface** drop-down list, click **Create Template**.**[Cisco VPN Interface Ethernet]** 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、VPN インターフェイス イーサネット 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。

ステップ 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。

ステップ 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。

基本的なインターフェイス機能の設定

VPN で基本的なインターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。

（注） インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	IPv4 または IPv6	オプション	Description
[Shutdown] *	インターフェイスを有効にするには [No] をクリックします。		
Interface name*	インターフェイスの名前を入力します。 Cisco IOS XE SD-WAN デバイス については、次のことを行う必要があります。 • インターフェイス名を完全にスペルアウトします (たとえば、GigabitEthernet0/0/0)。 • 使用していない場合でも、すべてのルータのインターフェイスを設定して、それらがシャットダウン状態で設定され、それらのすべてのデフォルト値が設定されるようにします。		
Description	インターフェイスの説明を入力します。		
[IPv4 / IPv6]	[IPv4] をクリックして、IPv4 VPN インターフェイスを設定します。[IPv6] をクリックして、IPv6 インターフェイスを設定します。		

パラメータ名	IPv4 または IPv6	オプション	Description
Dynamic	インターフェイスを Dynamic Host Configuration Protocol（DHCP）クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。		
	両方	**DHCP Distance**	必要に応じて、DHCP サーバーから学習したルートのアドミニストレーティブ ディスタンス値を入力します。デフォルトは 1 です。
	IPv6	DHCP Rapid Commit	必要に応じて、DHCP Rapid Commit をサポートするように DHCP IPv6 ローカルサーバーを設定して、ビジーな環境でクライアントの設定と確認を高速化できるようにします。 [On] をクリックして、DHCP 高速コミットを有効にします。 [Off] をクリックして、通常のコミットプロセスの使用を続行します。
[Static]	[Static] をクリックして、変更しない IP アドレスを入力します。		
	IPv4	**IPv4 アドレス（IPv4 Address）**	静的 IPv4 アドレスを入力します。
	IPv6	[IPv6 アドレス（IPv6 Address）]	静的 IPv6 アドレスを入力します。
Secondary IP Address	**IPv4**	[Add] をクリックして、サービス側インターフェイスのセカンダリ IPv4 アドレスを最大 4 つ入力します。	
[IPv6 アドレス（IPv6 Address）]	**IPv6**	[Add] をクリックして、サービス側インターフェイスのセカンダリ IPv6 アドレスを 2 つまで入力します。	
DHCP Helper	**両方**	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BootP（ブロードキャスト）DHCP 要求を転送します。	
Block Non-Source IP	**Yes** / **No**	[Yes] をクリックして、トラフィックのソース IP アドレスがインターフェイスの IP プレフィックス範囲と一致する場合にのみ、インターフェイスにトラフィックを転送させます。他のトラフィックを許可するには、[No] 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。

トンネルインターフェイスの作成

Cisco IOS XE SD-WAN デバイス では、最大 8 つのトンネルインターフェイスを設定できます。つまり、各 Cisco IOS XE SD-WAN デバイス ルータに最大 8 つの TLOC を設定できます。Cisco vSmart コントローラ および Cisco vManage では、1 つのトンネルインターフェイスを設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。WAN インターフェイスは、オーバーレイへのトンネルトラフィックのフローを有効にします。WAN インターフェイスをトンネルインターフェイスとして設定しないと、次の表に示されている他のパラメータを追加できません。

トンネルインターフェイスを設定するには、[Interface Tunnel] を選択し、次のパラメータを設定します。

パラメータ名	説明
トンネル インターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。
ポートホップ	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。ポートホッピングがグローバルに有効になっている場合は、個々の TLOC（トンネルインターフェイス）で無効にできます。ポートホッピングをグローバルレベルで制御するには、[System] 設定テンプレートを使用します。https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/System デフォルト：有効 vManage NMS と Cisco vSmart コントローラ のデフォルト：無効
TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2 つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックします。

パラメータ名	説明
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default デフォルト：default
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。 範囲：1 ～ 60 秒 デフォルト：5 秒
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。 範囲：100 ～ 10000 ミリ秒 デフォルト：1000 ミリ秒（1 秒）

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒 デフォルト：12 秒

キャリア名とトンネルインターフェイスの関連付け

キャリア名またはプライベートネットワーク識別子をトンネルインターフェイスに関連付けるには、**carrier** コマンドを使用します。*carrier-name* には **default** および、**carrier1** ～ **carrier8** を指定できます。

```
Device(config)# interface Tunnel 0
Device(config-if)# ip unnumbered GigabitEthernet1
Device(config-if)# ipv6 unnumbered GigabitEthernet2
Device(config-if)# tunnel source GigabitEthernet1
Device(config-if)# tunnel mode sdwan
Device(config-if)# exit
Device(config)# sdwan
Device(config-sdwan)# int GigabitEthernet1
Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# carrier default
```

トンネルグループの作成

デフォルトでは、WAN エッジルータは色に関係なく、ネットワーク内の他のすべての TLOC とのトンネルを構築しようとします。トンネル設定の下で色を指定して restrict オプションを使用すると、TLOC は同じ色の TLOC へのトンネルの構築のみに制限されます。restrict オプションの詳細については、「Configure Interfaces in the WAN Transport VPN(VPN0)」を参照してください。

トンネルグループ機能は restrict オプションに似ていますが、トンネルグループ ID がトンネルの下で割り当てられると、同じトンネルグループ ID を持つ TLOC のみが色に関係なく相互にトンネルを形成できるため、柔軟性が向上します。

TLOC がトンネルグループ ID に関連付けられている場合、トンネルグループ ID に関連付けられていないネットワーク内の他の TLOC とのトンネルを引き続き形成します。

（注） restrict オプションは、この機能と組み合わせて使用できます。使用すると、インターフェイスで定義されたトンネルグループ ID と restrict オプションを持つインターフェイスは、同じトンネルグループ ID とカラーを持つ他のインターフェイスとだけトンネルを形成します。

CLI を使用した Cisco IOS XE SD-WAN デバイス でのトンネルグループの設定

Cisco IOS XE SD-WAN デバイス でトンネルグループを設定するには、次の手順を実行します。

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet2

Device(config-interface-GigabitEthernet2)# tunnel-interface
Device(config-tunnel-interface)#group Group ID
```

トンネルインターフェイスでのキープアライブトラフィックの制限

デフォルトでは、Cisco IOS XE SD-WAN デバイス は 1 秒に 1 回、Hello パケットを送信して、2 つのデバイス間のトンネルインターフェイスがまだ動作しているかどうかを判断し、トンネルを維持します。hello 間隔と hello 許容度の組み合わせによって、DTLS または TLS トンネルのダウンを宣言するまでの待機時間が決まります。デフォルトの hello 間隔は 1 秒で、デフォルトの許容値は 12 秒です。これらのデフォルト値では、Hello パケットが 11 秒以内に受信されない場合、トンネルは 12 秒時点でダウンが宣言されます。

DTLS または TLS トンネルの両端で hello 間隔、hello 許容度、またはその両方が異なる場合、トンネルは次のように間隔と許容度を選択します。

- 2 つのコントローラデバイス間のトンネル接続の場合、トンネルは 2 つのデバイス間の接続に対して、小さい方の hello 間隔と大きい方の許容間隔を使用します。（コントローラデバイスは、vBond コントローラ、vManage NMS、および vSmart コントローラです。）この選択は、コントローラのいずれかに低速の WAN 接続がある場合に行われます。hello 間隔と許容時間は、コントローラデバイスのペアごとに個別に選択されます。
- Cisco IOS XE SD-WAN デバイス と任意のコントローラデバイス間のトンネル接続の場合、トンネルはルータに設定されている hello 間隔と許容時間を使用します。この選択は、トンネルを介して送信されるトラフィックの量を最小限に抑え、リンクのコストがリンクを通過するトラフィックの量の関数である状況を可能にするために行われます。hello 間隔と許容時間は、Cisco IOS XE SD-WAN デバイス とコントローラデバイス間のトンネルごとに個別に選択されます。

トンネルインターフェイスのキープアライブトラフィックの量を最小限に抑えるには、トンネルインターフェイスの Hello パケット間隔と許容度を増やします。

```
Device(config-tunnel-interface)#  hello-interval milliseconds
Device(config-tunnel-interface)#  hello-tolerance seconds
```

デフォルトの hello 間隔は 1000 ミリ秒で、100 ～ 600000 ミリ秒（10 分）の範囲の時間にすることができます。デフォルトの hello 許容度は 12 秒で、12 ～ 600 秒（10 分）の範囲の時間にすることができます。hello 許容間隔は、OMP ホールド時間の半分以下にする必要があります。デフォルトの OMP ホールド時間は 60 秒で、**omp timers holdtime** コマンドで設定します。

インターフェイスの NAT デバイスとしての設定

NAT の設定方法については、『*Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE リリース 17.x*』を参照してください。

アクセスリストと QoS パラメータの適用

サービスの品質（QoS）は、サービスの実行方法を決定するのに役立ちます。QoS を設定することにより、WAN 上のアプリケーションのパフォーマンスを向上させます。インターフェイスのシェーピングレートを設定し、QoSマップ、書き換えルール、アクセスリスト、およびポリサーをインターフェイスに適用するには、[ACL/QoS] をクリックして、次のパラメータを設定します。

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ（QoS Map）	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[オン] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセス リストの名前を指定します。
出力 ACL – IPv6	[オン] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセス リストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[オン]をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

ARP テーブルエントリの追加

アドレス解決プロトコル（ARP）は、リンク層アドレス（デバイスの MAC アドレスなど）を割り当てられたインターネット層アドレスに関連付けるのに役立ちます。動的マッピングが機能していない場合は、静的 ARP アドレスを設定します。インターフェイスで静的 ARP テーブルエントリを設定するには、ARP を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

パラメータ名	Description
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。

パラメータ名	Description
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[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。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol（VRRP）をインターフェイスで実行するには、[VRRP] タブを選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

パラメータ名	説明
グループ ID（Group ID）	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ～ 255
プライオリティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリ VRRP ルータとして選択されます。2 つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリ VRRP ルータとして選択されます。 範囲：1 ～ 254 デフォルト：100
Timer（ミリ秒）	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリ VRRP ルータが選択されます。 範囲：100 ～ 40950 ミリ秒 デフォルト：100 ミリ秒 （注） Cisco IOS XE SD-WAN デバイスの VRRP 機能テンプレートのタイマーが 100 ミリ秒の場合、LAN インターフェイスのトラフィックが多いと VRRP は失敗します。

パラメータ名	説明
Track OMP Track Prefix List	デフォルトでは、VRRP は、どのルータがプライマリ仮想ルータであるかを判別するのに、実行されているサービス（LAN）インターフェイスの状態を使用します。ルータがすべての WAN 制御接続を失った場合、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを構成します。 [Track OMP]：[On] をクリックすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションをトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。 [Track Prefix List]：OMP セッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、ルータがプライマリ VRRP ルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。
IP アドレス	仮想ルータの IP アドレスを入力します。このアドレスは、ローカルルータと VRRP を実行しているピアの両方の構成済みインターフェイス IP アドレスとは異なる必要があります。

VRRP のプレフィックスリストを設定する

デバイスおよび機能テンプレートを使用して、VRRP のプレフィックス リスト トラッキングを設定できます。プレフィックスリストを設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Policy]** の順に選択します。
2. [Localized Policy] をクリックします。
3. [Custom Options] ドロップダウンリストから、[Lists] をクリックします。
4. 左ペインで [Prefix] をクリックし、[New Prefix List] をクリックします。
5. [Prefix List Name] に、プレフィックスリストの名前を入力します。
6. [Internet Protocol] として [IPv4] を選択します。
7. [Add Prefix] で、プレフィックスエントリをカンマで区切って入力します。
8. [Add] をクリックします。

9. [Next] をクリックし、[Forwarding Classes/QoS] を設定します。
10. [Next] をクリックし、[Access Control Lists] を設定します。
11. [Next] をクリックし、[Route Policy] ペインで、関連するルートポリシーを選択して […] をクリックし、[Edit] をクリックして、新しく追加されたプレフィックスリストを追加します。
12. [Match] ペインで [AS Path List] をクリックし、[Address] で新しく追加されたプレフィックスリストを選択します。
13. [Save Match and Actions] をクリックします。
14. [Next] をクリックし、[Policy Overview] 画面で [Policy Name] と [Policy Description] を入力します。
15. [Save Policy] をクリックします。

デバイステンプレートでの VRRP のプレフィックスリストの設定

デバイステンプレートの VRRP およびローカライズされたポリシーにプレフィックスリストを設定するには、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. [Device 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] のタイトルは [Device] です。

3. 関連するデバイステンプレートを選択して […] をクリックし、[Edit] をクリックしてテンプレートの詳細を編集します。
4. [Policy] から、新しく追加されたプレフィックスリストを持つポリシーを選択します。
5. [更新（Update）] をクリックします。
6. [Feature Templates] をクリックします。
7. 関連するデバイステンプレートを選択して […] をクリックし、[Edit] をクリックしてテンプレートの詳細を編集します。
8. [VRRP] をクリックします。
9. 関連するグループ ID を選択し、ペンアイコンをクリックして、新しいプレフィックスリストを VRRP の詳細に関連付けます。
10. [Track Prefix List] ドロップダウンリストをクリックし、新しく追加されたプレフィックスリスト名を入力します。
11. [Save Changes] をクリックします。

12. [Update] をクリックして変更を保存します。
13. [Device Templates] をクリックし、新しく追加されたプレフィックスリストを持つポリシーを選択します。
14. [...] をクリックして、[Attach Devices] をクリックします。
15. [Available Devices] で、関連するデバイスをダブルクリックして [Selected Devices] に移動し、[Attach] をクリックします。

詳細プロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のパラメータを設定します。

パラメータ名	説明
デュプレックス	[full] または [half] を選択して、インターフェイスが全二重または半二重のどちらのモードで動作するかを指定します。 デフォルト：full
MAC アドレス	インターフェイスに関連付ける MAC アドレスを、コロン区切りの 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 1804 デフォルト：1500 バイト
PMTU ディスカバリ	[On] をクリックして、インターフェイスで Path MTU Discovery を有効にします。PMTU は、パケットフラグメンテーションが発生しないように、インターフェイスがサポートする最大の MTU サイズを決定します。
Flow Control	インターフェイス上のデータの送信を一時的に停止するメカニズムである双方向フロー制御の設定を選択します。 値：autonet、both、egress、ingress、none デフォルト：autoneg
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1460 バイト デフォルト：なし

パラメータ名	説明
速度	接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。 値：10、100、1000、または 10000 Mbps
Clear-Dont-Fragment	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment（DF）ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） フラグメンテーションが必要で、DF ビットが設定されている場合に、Clear-Dont-Fragment は DF ビットをクリアします。フラグメンテーションを必要としないパケットの場合、DF ビットは影響を受けません。
自動ネゴシエーション	（注） Cisco vManage リリース 20.6.1 より前のリリースでは、フィールドのデフォルト値は [On] です。自動ネゴシエーションをオフにするには、[Off] をクリックします。 Cisco vManage リリース 20.6.1 以降、フィールドのデフォルトの動作は次のとおりです。 • ギガビット イーサネット インターフェイス タイプの場合、[Autonegotiation] フィールドはデフォルトで空白になっています。ただし、フィールドが空白の場合、自動ネゴシエーションは [On] に設定されます。 • 10 ギガビットイーサネットや 100 ギガビットイーサネットなどの他のインターフェイスタイプの場合、[Autonegotiation] フィールドはデフォルトで空白になっています。自動ネゴシエーションをオンまたはオフにするには、それぞれ [On] または [Off] をクリックします。
TLOC Extension	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。 L3 を介した TLOC 拡張は、Cisco IOS XE ルータでのみサポートされることに注意してください。Cisco IOS XE ルータに L3 を介した TLOC 拡張を設定する場合は、L3 インターフェイスの IP アドレスを入力します。
GRE Tunnel Source IP	拡張 WAN インターフェイスの IPv4 アドレスを入力します。

パラメータ名	説明
Xconnect（IOS XE ルータ）	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイスブリッジ

すべての Cisco IOS XE SD-WAN デバイス クラウドおよび Cisco IOS XE SD-WAN デバイス に VPN インターフェイス ブリッジ テンプレートを使用します。

統合ルーティングおよびブリッジング（IRB）により、異なるブリッジドメイン内の Cisco IOS XE SD-WAN デバイス が相互に通信できます。IRB を有効にするには、ブリッジドメインを VPN に接続する論理 IRB インターフェイスを作成します。VPN は、異なる VLAN 間でトラフィックを交換できるようにするために必要なレイヤ 3 ルーティングサービスを提供します。各ブリッジドメインは 1 つの IRB インターフェイスを持つことができ、1 つの VPN に接続できます。また、1 つの VPN は、Cisco IOS XE SD-WAN デバイス 上の複数のブリッジに接続できます。

Cisco vManage テンプレートを使用してブリッジインターフェイスを構成するには、次の手順を実行します。

1. この記事で説明されているように、論理 IRB インターフェイスのパラメータを構成する VPN インターフェイスブリッジ機能テンプレートを作成します。
2. ブリッジングドメインのパラメータを設定するには、ブリッジングドメインごとにブリッジ機能テンプレートを作成します。ブリッジのヘルプトピック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 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. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
6. [Service VPN] ドロップダウンリストをクリックします。

7. [Additional VPN Templates] から、[VPN Interface Bridge] をクリックします。
8. [VPN Interface Bridge] ドロップダウンリストから、[Create Template] をクリックします。

   VPN インターフェイス ブリッジ 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 VPN インターフェイス ブリッジ パラメータを定義するためのフィールドがあります。
9. [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。
10. [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 *112*:

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。Viptela 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。Viptela 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、「Create a Template Variables Spreadsheet」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。

リリース情報

リリース 15.3 の Cisco vManage NMS で導入されました。リリース 18.2 では、ICMP リダイレクト メッセージを無効にするためのサポートを追加します。

ブリッジング インターフェイスの作成

ブリッジサーバーに使用するインターフェイスを設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。ブリッジを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *113 :*

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface name*	インターフェイスの名前を **irb** *number* の形式で入力します。IRB インターフェイス番号は 1 ～ 63 で、IRB が接続されているブリッジドメインのブリッジ機能テンプレートで設定された VPN 識別子と同じである必要があります。
説明	インターフェイスの説明を入力します。
IPv4 Address*	ルータの IPv4 アドレスを入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
Block Non-Source IP	[Yes] をクリックして、トラフィックのソース IP アドレスがインターフェイスの IP プレフィックス範囲と一致する場合にのみ、インターフェイスにトラフィックを転送させます。
セカンダリ IP アドレス（Cisco IOS XE SD-WAN デバイス 上）	[Add] をクリックして、サービス側インターフェイスに最大 4 つのセカンダリ IPv4 アドレスを設定します。

テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

アクセスリストの適用

アクセスリストをIRBインターフェイスに適用するには、[ACL]タブを選択し、次のパラメータを設定します。ACL フィルタは、ブリッジドメインの内外で何が許可されるかを決定します。

表 *114*:

パラメータ名	説明
入力 ACL – IPv4	[On] をクリックし、インターフェイスで受信されるパケットへの IPv4 アクセスリストの名前を指定します。
Egress ACL– IPv4	[On] をクリックして、インターフェイスで送信されるパケットへの IPv4 アクセスリストの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol（VRRP）をインターフェイスで実行するには、[VRRP] を選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

表 *115*:

パラメータ名	説明
グループ ID（Group ID）	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。範囲：1 ～ 255
プライオリティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリ VRRP ルータとして選択されます。2 つの Cisco IOS XE SD-WAN デバイス の優先順位が同じ場合、IPアドレスが大きい方がプライマリ VRRPルータとして選択されます。範囲：1 ～ 254、デフォルト：100

パラメータ名	説明
Timer（ミリ秒）	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリ VRRP ルータが選択されます。 範囲：100 ～ 40950 ミリ秒 デフォルト：100 ミリ秒 （注） Cisco IOS XE SD-WAN デバイス の VRRP 機能テンプレートのタイマーが 100 ミリ秒の場合、LAN インターフェイスのトラフィックが多いと VRRP は失敗します。
Track OMP Track Prefix List	デフォルトでは、VRRP は、どの Cisco IOS XE SD-WAN デバイス がプライマリ仮想ルータであるかを判別するために、VRRP が実行されているサービス（LAN）インターフェイスの状態を使用します。Cisco IOS XE SD-WAN デバイス がすべての WAN 制御接続を失うと、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを設定します。 Track OMP：[On] をクリックすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションをトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。 Track Prefix List：OMP セッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイス がプライマリ VRRP ルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。
IP アドレス	仮想ルータの IP アドレスを入力します。このアドレスは、ローカル Cisco IOS XE SD-WAN デバイス と VRRP を実行しているピアの両方の設定済みインターフェイス IP アドレスとは異なる必要があります。

VRRP 設定を保存するには、[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。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル（ARP）テーブルエントリを構成するには、[ARP] を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

表 *116*：

パラメータ名	Description
IPアドレス	ARPエントリのIPアドレスをドット付き10進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[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。

詳細プロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 *117*：

パラメータ名	説明
MAC アドレス（MAC Address）	MAC アドレスは、静的または動的に設定できます。静的 MAC アドレスは、ARP要求を介して学習された動的MACアドレスとは対照的に、手動で構成されます。ルータのインターフェイスに静的MACを構成するか、ルータのインターフェイスを識別する静的 MAC を指定できます。 インターフェイスに関連付ける MAC アドレスを、コロンで区切った 16 進表記で指定します。
IP MTU	MTU と同様に、IP MTU は IP パケットにのみ影響します。IP パケットが IP MTU を超過すると、パケットはフラグメント化されます。 インターフェイス上のパケットの最大MTUサイズを指定します。範囲：576 ～ 1804、デフォルト：1500 バイト

パラメータ名	説明
TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。ヘッダー値がすでに低い場合は、変更されずにそのまま通過します。エンドホストは、2 つのホストの低い方の設定を使用します。TCP MSS を構成する場合は、最小パス MTU より 40 バイト低く設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし
Clear-Dont-Fragment	DF ビットが設定されたインターフェイスにパケットが到着する場合は、Clear-Dont-Fragment を設定します。これらのパケットが MTU が許可するサイズよりも大きい場合、それらはドロップされます。DF ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment（DF）ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） フラグメンテーションが必要で、DF ビットが設定されている場合に、Clear-Dont-Fragment は DF ビットをクリアします。フラグメンテーションを必要としないパケットの場合、DF ビットは影響を受けません。
ARP Timeout	ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。 動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。 範囲：0 ～ 2678400 秒（744 時間）デフォルト：1200 秒（20 分）
ICMP Redirect	ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。 ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。 インターフェイスで ICMP リダイレクトメッセージを無効にするには、[Disable] をクリックします。デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイス DSL IPoE

Cisco IOS XE SD-WAN デバイス の IPoE テンプレートを使用します。

サービスプロバイダーのデジタル加入者線（DSL）機能をサポートするには、DSL インターフェイスを備えたルータに IPoE を設定します。

Cisco vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイス に DSL インターフェイスを設定するには、次の手順を実行します。

1. この記事の説明に従って、IP-over-Ethernetインターフェイスのパラメータを設定する VPN インターフェイス DSL IPoE 機能テンプレートを作成します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピック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 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] 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. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional VPN 0 Templates] で、[VPN Interface DSL IPoE] をクリックします。
7. [VPN Interface DSL IPoE] ドロップダウンリストから、[Create Template] を選択します。**VPN インターフェイス DSL IPoE** 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、IPoEインターフェイスの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、[Scope] 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 *118*：

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。Viptela 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。Viptela 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、「Create a Template Variables Spreadsheet」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。

IPoE 機能の設定

基本的な IPoE 機能を設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 *119*：

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、*slot*/*subslot*/*port* の形式で入力します（たとえば、0/2/0）。

パラメータ名	説明
Mode*	ドロップダウンから VDSL コントローラの動作モードを選択します。 • Auto：デフォルトのモード。 • ADSL1：ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • ADSL2：ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • ADSL2+：ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • ANSI：ITU G.991.1、G.992.3、および G992.5（Annex A および Annex M）で定義されている ADSL2/2+ モード、および ITU-T G993.2 で定義されている VDSL2 モードで動作します。 • VDSL2：ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL モデムの設定	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	[Yes] をクリックして、インターフェイスでのシームレスなレート調整を有効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[Save] をクリックします。

イーサネット インターフェイスの設定

PPPoE を使用してイーサネット インターフェイスを設定すると、LAN 上の複数のユーザーをリモートサイトに接続できます。VDSL コントローラでイーサネットインターフェイスを設定するには、[Ethernet] をクリックして、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 *120 :*

パラメータ名	説明
Ethernet Interface Name	イーサネット インターフェイスの名前を *subslot/port* の形式で入力します（例：2/0）。スロット番号は常に 0 であるため、入力する必要はありません。

パラメータ名	説明
VLAN ID	イーサネット インターフェイスの VLAN 識別子を入力します。
説明	インターフェイスの説明を入力します。
Dynamic/Static	動的または静的IPv4アドレスをイーサネットインターフェイスに割り当てます。
IPv4 Address	イーサネット インターフェイスの静的 IPv4 アドレスを入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力して、インターフェイスをDHCPヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 *121 :*

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。 （注） 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 10 ミリ秒の hello-interval と 12 秒の hello-tolerance パラメータを設定して、650 ～ 700 Kbps 以上の帯域幅を設定することをお勧めします。 BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。 双方向BFDパケットフローに必要な帯域幅の計算例を以下に示します。 • 制御接続用にデバイスごとに 650 ～ 700 Kbps。 • デバイス上の BFD セッション（要求）ごとに 175 バイト（または 1.4 Kbps） • デバイス上の BFD セッション（応答）ごとに 175 バイト（または 1.4 Kbps） パス MTU ディスカバリ（PMTUD）が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅： 1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。 1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps（要求） 147 バイトの BFD パケットが応答として送信されます。 147 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 40 bps（応答） したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。 700k +（1.4k*775）+（400 *775）+（1.4k*775）+（40 *775）= ～ 3.5 MBps
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8。デフォルト：2

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT（STUN）のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0 ～ 8。デフォルト：5
ポートホップ	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。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2 つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *122：*

パラメータ名	説明
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295、デフォルト：0

パラメータ名	説明
IPsec Weight	複数のTLOC間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ー 255、デフォルト：1
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default、デフォルト：default
ループバックトンネルのバインド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。
ラストリゾート回線	トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。 （注） ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスでBFD TLOC ダウンアラームと制御TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1 ～ 60 秒、デフォルト：5 秒
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒、デフォルト：1000 ミリ秒（1 秒）

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒、デフォルト：12 秒

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT] をクリックし、[On] をクリックして、次のパラメータを設定します。

表 *123*：

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：60 分（1 時間）
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 *124*：

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を 1 つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535

パラメータ名	説明
プロトコル	ポート転送ルールを適用するプロトコル（[TCP] または [UDP]）を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ～ 65530
プライベート IP	ポート転送ルールに一致するトラフィックの転送先となる内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[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。

アクセスリストの適用

ACL を設定して、どのトラフィックが QoS を利用するかを選択します。ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL]タブを選択し、次のパラメータを設定します。

表 *125*：

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On]をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On]をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。

パラメータ名	説明
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のプロパティを設定します。

表 *126 :*

パラメータ名	説明
Bandwidth Upstream	WAN トランスポート VPN（VPN 0）の物理インターフェイスで送信されるトラフィックの帯域幅が特定の制限を 85% 超えると（Cisco IOS XE SD-WAN デバイス および Cisco vManage NMS のみ）、Bandwidth Upstream により通知が発行されます 送信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
Bandwidth Downstream	WAN トランスポート VPN（VPN 0）の物理インターフェイスで受信されるトラフィックの帯域幅が特定の制限を 85% 超えると（Cisco IOS XE SD-WAN デバイス および Cisco vManage NMS のみ）、Bandwidth Downstream により通知が発行されます 受信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
IP MTU	IP MTU は IP パケットに影響します。IP パケットが IP MTU を超過すると、パケットはフラグメント化されます。 インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ～ 1804、デフォルト：1500 バイト
TCP MSS	単一の TCP/IPv4 データグラムでは、TCP の最大セグメントサイズ（MSS）は、ホストが受け入れる最大データを定義します。この TCP/IPv4 データグラムは、IPv4 レイヤでフラグメント化されている可能性があります。MSS 値は、TCP SYN セグメント内でのみ TCP ヘッダー オプションとして送信されます。 ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
TLOC Extension	TLOC拡張機能を使用してインターフェイスをバインドし、同じ物理サイトにある別の Cisco IOS XE SD-WAN デバイス をローカルルータの WAN トランスポート インターフェイスに接続します（Cisco IOS XE SD-WAN デバイス のみ）。 WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
Tracker	インターフェイスステータスのトラッキングは、VPN 0 のトランスポートインターフェイスで NAT を有効にして、最初にデータセンターのルータにアクセスするのではなく、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出られるようにする場合に役立ちます。この状況では、トランスポートインターフェイスで NAT を有効にすると、ローカルルータとデータセンター間の TLOC が 2 つに分割され、1 つはリモートルータに、もう 1 つはインターネットに送られます。 トランスポート トンネル トラッキングを有効にすると、ソフトウェアはインターネットへのパスを定期的に調べて、インターネットが稼働しているかどうかを判断します。このパスがダウンしていることをソフトウェアが検出すると、インターネットの宛先へのルートが撤回され、インターネットに向かうトラフィックはデータセンターのルータを介してルーティングされます。インターネットへのパスが再び機能していることをソフトウェアが検出すると、インターネットへのルートが再インストールされます。 インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

パラメータ名	説明
IP Directed-Broadcast	IP ダイレクトブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。 宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクトブロードキャストを転送します。ダイレクトブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。 あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.4.1 の Cisco vManage NMS で導入されました。

VPN インターフェイス DSL PPPoA

サービスプロバイダーのデジタル加入者線（DSL）機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-ATM インターフェイスを設定します。

Cisco IOS XE SD-WAN デバイス の VPN インターフェイス DSL PPPoA テンプレートを使用します。

サービスプロバイダーのデジタル加入者線（DSL）機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-ATM インターフェイスを設定します。

Cisco vManage テンプレートを使用して Cisco ルータに DSL インターフェイスを設定するには、次の手順を実行します。

1. この記事の説明に従って、VPN インターフェイス DSL PPPoA 機能テンプレートを作成して、ATM インターフェイスパラメータを設定します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピック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 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. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional VPN 0 Templates] で、[VPN Interface DSL PPPoA] をクリックします。
7. [VPN Interface DSL PPPoA] ドロップダウンリストから、[Create Template] をクリックします。VPN インターフェイス DSL PPPoA 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、VPN インターフェイス PPP の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 [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 *127*:

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。Viptela 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。Viptela 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、「Create a Template Variables Spreadsheet」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。

VDSL コントローラ機能の構成

VPN の基本的な VDSL コントローラ機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 *128*:

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、*slot*/*subslot*/*port* の形式で入力します（たとえば、0/2/0）。

パラメータ名	説明
Mode*	ドロップダウンから VDSL コントローラの動作モードを選択します。 • [Auto]：デフォルトのモード。 • [ADSL1]：ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • [ADSL2]：ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • [ADSL2+]：ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • **ANSI**：ITU G.991.1、G.992.3、および G992.5（Annex A および Annex M）で定義されている ADSL2/2+ モード、および ITU-T G993.2 で定義されている VDSL2 モードで動作します。 • **VDSL2**：ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL モデムの設定	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	デフォルトでは有効になっています。[No] をクリックして、インターフェイスでのシームレスなレート調整を無効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[Save] をクリックします。

ATM インターフェイスの設定

VDSL コントローラで ATM インターフェイスを設定するには、[ATM] を選択し、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 *129 :*

パラメータ名	説明
ATM Interface Name	ATM インターフェイスの名前を *subslot*/*port* の形式で入力します（例：2/0）。スロット番号は常に 0 であるため、入力する必要はありません。
説明	インターフェイスの説明を入力します。

パラメータ名	説明
VPI and VCI	ATM 相手先固定接続（PVC）を *vpi*/*vci* の形式で作成します。仮想パス識別子（VPI）および仮想チャネル識別子（VCI）の値を入力します。
カプセル化	ATM PVC で使用する ATM アダプテーション層（AAL）およびカプセル化のタイプをドロップダウンから選択します。 • AAL5 MUX：PVC を単一のプロトコル専用にします。 • AAL5 NLPID：NLPID 多重化を使用します。 • AAL5 SNAP：同じ PVC で 2 つ以上のプロトコルを多重化します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。1 ～ 255 の値を指定できます。
VBR-NRT	可変ビットレート非リアルタイムパラメータを設定します。 • Peak Cell Rate：48 ～ 25000 Kbps の値を入力します。 • Sustainable Cell Rate：持続可能なセルレートを Kbps で入力します。 • Maximum Burst Size：このサイズは 1 セルです。
VBR-RT	可変ビット レート リアルタイム パラメータを設定します。 • Peak Cell Rate：48 ～ 25000 Kbps の値を入力します。 • Average Cell Rate：平均セルレートを Kbps で入力します。 • Maximum Burst Size：このサイズは 1 セルです。

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 *130 :*

パラメータ名	説明
認証プロトコル（Authentication Protocol）	MLP で使用される認証プロトコルを選択します。 • **CHAP**：インターネット サービス プロバイダー（ISP）から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • **PAP**：ISPから提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • **PAP**および**CHAP**：両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] 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。

トンネルインターフェイスの作成

Cisco IOS XE SD-WAN デバイス では、最大 4 つのトンネルインターフェイスを設定できます。つまり、各 Cisco IOS XE SD-WAN デバイス に最大 4 つの TLOC を設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] を選択し、次のパラメータを設定します。

表 *131 :*

パラメータ名	説明
トンネル インターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。
制御接続	Cisco IOS XE SD-WAN デバイス に複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC を確立しないようにします。デフォルトは [On] で、TLOC の制御接続を確立します。 （注） データをドロップしない制御接続トラフィックの場合、hello-interval（10）および hello-tolerance（12）にデフォルトのパラメータを設定した、650 ～ 700 kbps 以上の帯域幅をお勧めします。

パラメータ名	説明
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8、デフォルト：2
Cisco vBond オーケストレーション As STUN Server	Session Traversal Utilities for NAT（STUN）を有効にし、Cisco IOS XE SD-WAN デバイス が NAT の背後にある場合に、トンネルインターフェイスでそのパブリック IP アドレスとポート番号を検出できるようにする場合は、[On] をクリックします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラ を設定します。範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0～8、デフォルト：5
ポートホップ	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。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2 つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *132*：

パラメータ名	説明
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295。デフォルト：0

パラメータ名	説明
IPsec Weight	複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255。デフォルト：1
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト
ループバック トンネルのバインド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。
ラストリゾート回線	トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。 （注） ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1 つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1 ～ 60 秒。デフォルト：5 秒。
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒（1 秒）

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 *133:*

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] を選択し、次のプロパティを設定します。

表 *134*:

パラメータ名	説明
PMTUディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト。デフォルト：なし。
Dont Fragment のクリア	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0 ～ 7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目の Cisco IOS XE SD-WAN デバイス には、WAN への接続が提供されます。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.3 の Cisco vManage NMS で導入されました。

VPN インターフェイス DSL PPPoE

Cisco IOS XE SD-WAN デバイス の VPN インターフェイス DSL PPPoE テンプレートを使用します。

サービスプロバイダーのデジタル加入者線（DSL）機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-Ethernet インターフェイスを構成します。

Cisco vManageテンプレートを使用してCiscoルータにDSLインターフェイスを設定するには、次の手順を実行します。

1. この記事で説明されているように、PPP-over-Ethernet インターフェイスのパラメータを構成する VPN インターフェイス DSL PPPoE 機能テンプレートを作成します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピック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 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. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional VPN 0 Templates] で、[VPN Interface DSL PPPoE] をクリックします。
7. [VPN Interface DSL PPPoE] ドロップダウンリストから、[Create Template] をクリックします。VPNインターフェイスDSL PPPoE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、PPPoEインターフェイスの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 [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 *135*:

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。Viptela 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。Viptela 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、「Create a Template Variables Spreadsheet」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。

VDSL コントローラ機能の構成

VPN の基本的な VDSL コントローラ機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

（注） 展開に DSL を備えたデバイスが含まれている場合は、これらのテンプレートが使用されていない場合でも、DSL インターフェイス テンプレートを Cisco vManage に含める必要があります。

表 *136*:

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。

パラメータ名	説明
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、*slot*/*subslot*/*port* の形式で入力します（たとえば、0/2/0）。
Mode*	ドロップダウンから VDSL コントローラの動作モードを選択します。 • [Auto]：デフォルトのモード。 • [ADSL1]：ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • [ADSL2]：ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • [ADSL2+]：ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • [ANSI]：ITU G.991.1、G.992.3、および G992.5（Annex A および Annex M）で定義されている ADSL2/2+ モード、および ITU-T G993.2 で定義されている VDSL2 モードで動作します。 • [VDSL2]：ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL Modem Configuration	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	[Yes] をクリックして、インターフェイスでのシームレスなレート調整を有効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[Save] をクリックします。

VDSL コントローラのイーサネット インターフェイスを設定する

VDSL コントローラでイーサネット インターフェイスを設定するには、[Ethernet] を選択し、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 *137* : 機能の履歴

機能名	リリース情報	説明
DSL でのダイヤラインターフェイスのサポート	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.1	この機能により、Cisco IOS XE SD-WAN デバイスのダイヤラインターフェイスを介した Point-to-Point Protocol（PPP）セッションの追跡が可能になります。 ダイヤラインターフェイスは、Point-to-Point Protocol over Ethernet（PPPoE）、Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）の展開におけるデジタル加入者線（DSL）で使用されます。ダイヤラインターフェイスは、PPP セッションのステータスに関係なく、常に稼働しています。これにより、ダイヤラインターフェイスの使用中に、IP SLA やルーティング フェールオーバーが機能するための追跡などの追加設定の必要性を回避できます。 次のコマンドを追加して、PPP セッションがダウンしたときにダイヤラインターフェイスをダウンさせる、dialer down-with-vInterface を設定します。

表 *138* :

パラメータ名	説明
Ethernet Interface Name	イーサネット インターフェイスの名前を *subslot*/*port* の形式で入力します（例：2/0）。スロット番号は常に 0 であるため、入力する必要はありません。
VLAN ID	イーサネット インターフェイスの VLAN 識別子を入力します。
説明	インターフェイスの説明を入力します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。1 ～ 255 の値を指定できます。
PPP Max Payload	PPP リンク制御プロトコル（LCP）ネゴシエーション中にネゴシエートされる最大受信ユニット（MRU）値を入力します。範囲：64 ～ 1792 バイト
Dialer IP	ダイヤラインターフェイスの IP プレフィックスを設定します。このプレフィックスは、インターフェイスが呼び出す宛先のノードのプレフィックスです。 • [Negotiated]：IPCP ネゴシエーション中に取得されたアドレスを使用します。

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 *139*：

パラメータ名	説明
認証プロトコル（Authentication Protocol）	MLP で使用される認証プロトコルを選択します。 • **CHAP**：インターネット サービス プロバイダー（ISP）から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • [PAP]：ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • **PAP** および **CHAP**：両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[PAP と CHAP に同じ資格情報] 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。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 *140*：

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	デフォルトでは、制御接続はオンに設定されており、TLOCの制御接続を確立します。ルータに複数の TLOC がある場合は、[いいえ] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。 （注） 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランス パラメータを設定して、最低 650 ～ 700 Kbps の帯域幅を設定することをお勧めします。 BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。 双方向 BFD パケット フローに必要な帯域幅の計算例を以下に示します。 • 制御接続用にデバイスごとに 650 – 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) パス MTU ディスカバリ (PMTUD) が有効になっている場合、30 秒ごとにトンネルごとに BFD パケットを送受信するための帯域幅: 1500 バイトの BFD 要求パケットは、トンネルごとに 30 秒ごとに送信されます。 1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps (リクエスト) 147 バイトの BFD パケットが応答として送信されます。 147バイト×8ビット/1バイト×1パケット/30秒 = 40bps（レスポンス） したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3.5 MBps
最大制御接続数	WAN トンネル インターフェイスが接続できる の最大数を指定します。Cisco vSmart コントローラトンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8、デフォルト：2

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT（STUN）のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネル インターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネル インターフェイスの接続を許可しない Cisco vSmart コントローラ を設定します。 範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0 ～ 8、デフォルト：5
ポートホップ	[On] をクリックしてポートホッピングを有効にするか、[Off] をクリックして無効にします。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された TCP MSS 設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2 つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [On] または [On] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *141 :*

パラメータ名	説明
GRE	トンネル インターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec は有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295、デフォルト：0

パラメータ名	説明
IPsec の重み	複数のTLOC間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ー 255、デフォルト：1
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default、デフォルト：default
ループバックトンネルのバインド	ループバックインターフェイスにバインドする物理インターフェイスの名前を入力します。
ラストリゾート回線	トンネルインターフェイスを最終手段の回線として使用する場合に選択します。 （注） ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1つ以上のプライマリインターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスでBFD TLOCダウンアラームと制御TLOCダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。 範囲：1 ～ 60 秒。デフォルト：5 秒。
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒（1 秒）

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒。

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT] を選択し、[On] をクリックして、次のパラメータを設定します。

表 *142：*

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：60 分（1 時間）
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NATデバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 *143：*

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を 1 つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535

パラメータ名	説明
プロトコル	ポート転送ルールを適用するプロトコル（[TCP] または [UDP]）を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ～ 65530
プライベート IP	ポート転送ルールに一致するトラフィックを転送する内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[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。

アクセスリストの適用

ルータ インターフェイスに書き換えルール、アクセス リスト、およびポリサーを適用するには、ACL を選択し、次のパラメータを設定します。

表 *144 :*

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[オン] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセス リストの名前を指定します。
出力 ACL – IPv6	[オン] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセス リストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。

パラメータ名	説明
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のプロパティを設定します。

表 *145*:

パラメータ名	説明
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（$2^{32}/2$）– 1 kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（$2^{32}/2$）– 1 kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ～ 1804。デフォルト：1500 バイト。
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1460 バイト。デフォルト：なし。
Dont Fragment のクリア	[オン] をクリックして、インターフェイスから送信されるパケットの IPv4 パケット ヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
トラッカー	インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.3 の Cisco vManage NMS で導入されました。

VPN インターフェイス イーサネット PPPoE

Cisco IOS XE SD-WAN デバイス の PPPoE テンプレートを使用します。

Cisco IOS XE ルータで PPPoE over GigabitEthernet インターフェイスを設定して、PPPoE クライアントをサポートします。

Cisco vManage テンプレートを使用して Cisco ルータにインターフェイスを設定するには、次の手順を実行します。

1. このセクションの説明に従って、VPN インターフェイス イーサネット PPPoE 機能テンプレートを作成して、イーサネット PPPoE インターフェイスパラメータを設定します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピック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 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] 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. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional VPN 0 Templates] で、[VPN Interface Ethernet PPPoE] をクリックします。
7. [VPN Interface Ethernet PPPoE] ドロップダウンリストから、[Create Template] をクリックします。VPN インターフェイス イーサネット PPPoE 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、イーサネット PPPoE 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、[Scope] 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 *146*：

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。詳細については、「Create a Template Variables Spreadsheet」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。

PPPoE 機能の設定

基本的な PPPoE 機能を設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 *147*:

パラメータ名	説明
Shutdown*	[No] をクリックして、GigabitEthernet インターフェイスを有効にします。
Ethernet Interface Name	GigabitEthernet インターフェイスの名前を入力します。 IOS XE ルータの場合、インターフェイス名を完全に入力する必要があります（たとえば、**GigabitEthernet0/0/0**）。
VLAN ID	サブインターフェイスの VLAN タグ。
説明	Ethernet-PPPoE 対応インターフェイスの説明を入力します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。 範囲：100 ～ 255。
PPP Maximum Payload	PPP リンク制御プロトコル（LCP）ネゴシエーション中にネゴシエートされる最大受信ユニット（MRU）値を入力します。範囲：64 ～ 1792 バイト

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの設定

PPP 認証プロトコルを設定するには、[PPP] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 *148*:

パラメータ名	説明
PPP Authentication Protocol	MLP で使用される認証プロトコルを選択します。 • **CHAP**：インターネット サービス プロバイダー（ISP）から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • **PAP**：ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • **PAP** および **CHAP**：両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] 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。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] を選択し、次のパラメータを設定します。

表 *149 :*

パラメータ名	説明
トンネル インターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。 （注） 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランスパラメータを設定して、最低 650 ～ 700 Kbps の帯域幅を設定することをお勧めします。 BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。 双方向 BFD パケットフローに必要な帯域幅の計算例を以下に示します。 • 制御接続用にデバイスごとに 650 ～ 700 Kbps。 • デバイス上の BFD セッション（要求）ごとに 175 バイト（または 1.4 Kbps） • デバイス上の BFD セッション（応答）ごとに 175 バイト（または 1.4 Kbps） パス MTU ディスカバリ（PMTUD）が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅： 1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。 1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps（要求） 147 バイトの BFD パケットが応答として送信されます。 147 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 40 bps（応答） したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。 700k +（1.4k*775）+（400 *775）+（1.4k*775）+（40 *775）= ～ 3.5 MBps
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラ の最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8、デフォルト：2

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT（STUN）のセッショントラバーサルユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラ を設定します。範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0～8、デフォルト：5
ポートホップ	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。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *150*：

パラメータ名	説明
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。

パラメータ名	説明
IPsec Preference	トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295。デフォルト：0
IPsec Weight	複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255。デフォルト：1
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト
ループバック トンネルのバインド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。
ラストリゾート回線	トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。 （注） ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1 つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。 （注） プライマリ インターフェイス ルートでのアドミニストレーティブ ディスタンス値の設定はサポートされていません。

パラメータ名	説明
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1 ～ 60 秒。デフォルト： 5 秒
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒（1 秒）
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT] を選択し、[On] をクリックして、次のパラメータを設定します。

表 *151 :*

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：60 分（1 時間）
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 *152*:

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を 1 つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535
プロトコル	ポート転送ルールを適用するプロトコル（[TCP] または [UDP]）を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ～ 65530
プライベート IP	ポート転送ルールに一致するトラフィックの転送先となる内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[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。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] をクリックし、次のパラメータを設定します。

表 *153*:

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。

パラメータ名	説明
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のプロパティを設定します。

表 *154*:

パラメータ名	説明
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
IP MTU	インターフェイス上のパケットの最大MTUサイズを指定します。範囲：576 ～ 1804。デフォルト：1500 バイト
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト。デフォルト：なし
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
Tracker	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のステータスをトラッキングするトラッカーの名前を入力します。

パラメータ名	説明
IP Directed-Broadcast	ダイレクトブロードキャストの物理ブロードキャストへの変換を有効にします。IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.4.1 の Cisco vManage NMS で導入されました。

Cisco VPN インターフェイス GRE

ファイアウォールなどのサービスが、GRE トンネルのみをサポートするデバイスで使用できる場合、論理 GRE インターフェイスを設定することにより、デバイスに GRE トンネルを設定して、リモートデバイスに接続できます。これにより、サービスが GRE トンネルを介して利用可能であることをアドバタイズし、適切なトラフィックをトンネルに送信するデータポリシーを作成できます。GRE インターフェイスは、設定されるとすぐに起動し、物理トンネルインターフェイスが起動している限り起動し続けます。

Cisco vManage テンプレートを使用して GRE インターフェイスを設定するには、次の手順を実行します。

1. Cisco VPN インターフェイス GRE 機能テンプレートを作成して、GRE インターフェイスを設定します。
2. GRE トンネル経由で到達可能なサービスをアドバタイズし、GRE 固有の静的ルートを設定し、他の VPN パラメータを設定する Cisco VPN 機能テンプレートを作成します。
3. **set-service** *service-name* **local** コマンドを含む、サービス VPN に適用されるデータポリシーを Cisco vSmart コントローラ で作成します。

[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、[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] 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. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。
    1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
    2. [Additional VPN 0 Templates] で、[VPN Interface GRE] をクリックします。
    3. [VPN Interface GRE] ドロップダウンリストから、[Create Template] をクリックします。VPN インターフェイス GRE 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、VPNインターフェイス GRE 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、パラメータ範囲を選択します。

基本的な GRE インターフェイスの設定

基本的な GRE インターフェイスを設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。GREインターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *155*：

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [Off] をクリックします。
Interface Name*	GREインターフェイスの名前を入力します。形式は **gre** *number* です。*number* には 1 ～ 255 を指定できます。
説明	GRE インターフェイスの説明を入力します。

パラメータ名	説明
Source*	GRE インターフェイスの送信元を入力します。 • GRE Source IP Address：GRE トンネルインターフェイスの送信元 IP アドレスを入力します。このアドレスはローカルルータ上にあります。 • Tunnel Source Interface：GRE トンネルの送信元である物理インターフェイスを入力します。
Destination*	GRE トンネルインターフェイスの宛先 IP アドレスを入力します。このアドレスはリモートデバイス上にあります。
GRE Destination IP Address*	GRE トンネルインターフェイスの宛先 IP アドレスを入力します。このアドレスはリモートデバイス上にあります
IPv4 Address	GRE トンネルの IPv4 アドレスを入力します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ～ 1804、デフォルト：1500 バイト
Clear-Dont-Fragment	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。
TCP MSS	Cisco vEdge デバイス を通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

機能テンプレートを保存するには、[Save] をクリックします。

インターフェイス アクセス リストの設定

GRE インターフェイスでアクセスリストを設定するには、[ACL] をクリックして、次のパラメータを設定します。

表 *156 :*

パラメータ名	説明
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。

パラメータ名	説明
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。

トラッカーインターフェイスの設定

GREインターフェイスのステータスをトラッキングするようにトラッカーインターフェイスを設定するには、[Advanced] を選択し、次のパラメータを設定します。

表 *157:*

パラメータ名	説明
Tracker	インターネットに接続するGREインターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

VPN インターフェイス IPsec

VPN インターフェイス IPsec 機能テンプレートを使用して、インターネット キー エクスチェンジ（IKE）セッションに使用されている Cisco IOS XE サービス VPN で IPsec トンネルを設定します。512 を除く、VPN 1 から 65530 までのトンネルで IPsec を構成できます。

Cisco Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。Cisco vManage では、システムが VPN 設定を VRF 設定に自動的にマッピングします。

VPN IPsec インターフェイス テンプレートの作成

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 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。

ステップ 3 [Add template] をクリックします。

ステップ 4 リストから Cisco IOS XE SD-WAN デバイス を選択します。

ステップ 5 [VPN] セクションで、[VPN Interface IPsec] をクリックします。Cisco VPN インターフェイス IPsec テンプレートが表示されます。

ステップ 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。

ステップ 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。

基本設定

基本的な IPsec トンネルインターフェイスを設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。

パラメータ名	オプション/フォーマット	説明
Shutdown*	**Yes** / **No**	インターフェイスを有効にするには [No] をクリックし、無効にするには [Yes] をクリックします。
Interface Name*	**ipsec** *number*（1…255）	IPsec インターフェイスの名前を入力します。*Number* は 1 ～ 255 を指定できます。
説明	IPsec インターフェイスの説明を入力します。	
IPv4 Address*	*ipv4-prefix/length*	IPsec インターフェイスの IPv4 アドレスを入力します。アドレスには **/30** サブネットが必要です。
Source *	IKE キー交換に使用されている IPsec トンネルの送信元を設定します。	
	IP Address	クリックして、送信元トンネルインターフェイスである IPv4 アドレスを入力します。このアドレスは、**VPN 0** で設定する必要があります。
	インターフェイス（**Interface**）	クリックして、IPsec トンネルの送信元である物理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、**VPN 0** で設定する必要があります。 • [Source] にインターフェイスを選択した場合は、送信元インターフェイスの名前を入力します。ループバック インターフェイスを入力すると、[Tunnel Route-via Interface] フィールドが表示されます。ここには出力インターフェイスの名前を入力します。

パラメータ名	オプション/フォーマット	説明
Destination*	IKE キー交換に使用されている IPsec トンネルの宛先を設定します。	
	IPsec Destination IP Address	宛先をポイントするIPv4アドレスを入力します。
	TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1960 バイト デフォルト：なし
	IP MTU	インターフェイス上のパケットの最大伝送ユニット（MTU）サイズを指定します。 範囲：576 ～ 2000 デフォルト：1500 バイト

CLI での同等コマンド

```
crypto
   interface tunnel ifnum
      no shutdown
      vrf forwarding vrf_id
      ip address ip_address[mask]
      tunnel source wanif_ip
      tunnel mode {ipsec ipv4 | gre ip}
      tunnel destination gateway_ip
      tunnel protection ipsec profile ipsec_profile_name
```

デッドピア検出の設定

インターネット キー エクスチェンジ（IKE）の Dead Peer Detection（DPD; デッドピア検出）を設定して、IKE ピアへの接続が機能していて到達可能かどうかを判別するには、[DPD] をクリックして、次のパラメータを設定します。

パラメータ名	説明
DPD Interval	IKEが接続でHelloパケットを送信する間隔を指定します。 範囲：10 ～ 3600 秒 デフォルト：無効

パラメータ名	説明
DPD Retries	IKE ピアがデッド状態であると宣言してピアへのトンネルを切断するまでに許容する、確認応答のないパケットの数を指定します。 範囲：2 ～ 60 デフォルト：3

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 での同等コマンド

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

IKE の設定

表 *158 :* 機能の履歴

機能名	リリース情報	説明
IPSec トンネルの SHA256 サポート	Cisco IOS XE リリース 17.2.1r	この機能により、セキュリティを強化するための HMAC_SHA256 アルゴリズムのサポートが追加されます。

IKE を設定するには、[IKE] をクリックして、次のパラメータを設定します。

（注） Cisco IOS XE SD-WAN デバイス で IPsec トンネルを作成すると、トンネルインターフェイスで IKE バージョン 1 がデフォルトで有効になります。

IKE バージョン 1 および IKE バージョン 2

IKEv1 および IKEv2 トラフィックを伝送する IPsec トンネルを設定するには、[IPSEC] をクリックして、次のパラメータを設定します。

パラメータ名	オプション	Description
IKE Version	[1] IKEv1 [2] IKEv2	[1] を入力して IKEv1 を選択します。 [2] を入力して IKEv2 を選択します。 デフォルト：IKEv1

パラメータ名	オプション	Description
IKE Mode	**Aggressive mode** Main mode	IKEv1 の場合のみ、次のいずれかのモードを指定します。 • [Aggressive mode]：ネゴシエーションが速くなり、イニシエータとレスポンダの ID が平文で渡されます。 • IPsec ネゴシエーションを開始する前に、IKE SA セッションを確立します。 （注） IKEv2 の場合、モードはありません。 （注） 事前共有キーを使用した IKE アグレッシブモードは、可能な限り避ける必要があります。それ以外の場合は、強力な事前共有キーを選択する必要があります。 デフォルト：[Main mode]
IPsec Rekey Interval	3600 ～ 1209600 秒	IKE キーを更新する間隔を指定します。 範囲：1 時間から 14 日 デフォルト：14400 秒（4 時間）
IKE Cipher Suite	**3DES** **192-AES** **256-AES** **[AES]** **[DES]**	IKE キー交換中に使用する認証と暗号化のタイプを指定します。 デフォルト：256-AES
IKE Diffie-Hellman Group	**2** **14** **15** **16**	IKEv1 または IKEv2 のいずれかで、IKE キー交換で使用する Diffie-Hellman グループを指定します。 • 1024 ビットの係数 • 2048 ビットの係数 • 3072 ビットの係数 • 4096 ビットの係数 デフォルト：4096 ビットの係数

パラメータ名	オプション	Description
IKE 認証	IKE 認証を設定します。	
	Preshared Key	事前共有キーで使用するパスワードを入力します。
	IKE ID for Local End Point	リモート IKE ピアがローカルエンドポイント識別子を必要とする場合は、それを指定します。 範囲：1 ～ 64 文字 デフォルト：トンネルのソース IP アドレス
	IKE ID for Remote End Point	リモート IKE ピアがリモートエンドポイント識別子を必要とする場合は、それを指定します。 範囲：1 ～ 64 文字 デフォルト：トンネルの宛先 IP アドレス

機能テンプレートを保存するには、[Save] をクリックします。

IKE バージョンを IKEv1 から IKEv2 に変更する

IKE バージョンを変更するには、次の手順を実行します。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックしてから、[Add 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、[Feature Templates] は [Feature] と呼ばれます。

3. テンプレートを作成するデバイスを選択します。
4. [Basic Configuration] をクリックします。
5. トンネルをシャットダウンするには、[shutdown] パラメータを [yes] オプション（[yes shutdown]）とともに使用します。
6. IPsec プロファイルから ISAKMP プロファイルを削除します。
7. IKEv2 プロファイルを IPsec プロファイルにアタッチします。

（注） IKEv2プロファイルがすでにある場合は、この手順を実行します。それ以外の場合は、最初にIKEv2 プロファイルを作成します。

8. トンネルを開始するには、[no] オプション（[no shutdown]）を指定して shutdown パラメータを使用します。

（注） [shutdown] 操作は、2 つの別個の操作で発行する必要があります。

（注） IKE バージョンを変更するための単一の CLI はありません。「IKE バージョンを IKEv1 から IKEv2 に変更する」セクションに記載されている一連の手順に従う必要があります。

IKEv1 の場合の CLI での 同等コマンド

IKEv1 の場合の ISAKMP CLI 設定

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

IKEv1 の場合の IPsec CLI 設定

```
profile ipsec_profile_name
         set transform-set transform_set_name
         set isakmp-profile ikev1_profile_name
         set security-association
            lifetime {kilobytes disable | seconds 120-2592000}
            replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
         set pfs group {14 | 16 | 19 | 20 | 21}
   keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
   ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
 esp-sha256-hmac] mode tunnel
```

手順の概要

1. enable
2. configure terminal
3. crypto isakmp policy *priority*
4. encryption {des | 3des | aes | aes 192 | aes 256 }
5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }

7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

IKE2 の場合の CLI での同等コマンド

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

IPsec トンネルパラメータの設定

IKE トラフィックを伝送する IPsec トンネルを設定するには、[IPSEC] をクリックして、次のパラメータを設定します。

パラメータ名	[オプション（Options）]	Description
IPsec Rekey Interval	3600 ～ 1209600 秒	IKE キーを更新する間隔を指定します。 範囲：1 時間から 14 日 デフォルト：3600 秒
IKE Replay Window	64、128、256、512、1024、2048、4096、8192	IPsec トンネルのリプレイウィンドウサイズを指定します。 デフォルト：512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	IPsec トンネルで使用する認証と暗号化を指定します。 デフォルト：aes256-gcm

パラメータ名	[オプション（Options）]	Description
Perfect Forward Secrecy	**2** 1024 ビットの係数 **14** 2048 ビットの係数 **15** 3072 ビットの係数 **16** 4096 ビットの係数 **none**	IPsec トンネルで使用する PFS 設定を指定します。 次の Diffie-Hellman 素数係数グループのいずれかを選択します。 1024 ビット：グループ 2 2048 ビット：グループ 14 3072 ビット：グループ 15 4096 ビット：グループ 16 なし：PFS を無効にします。 デフォルト：グループ 16

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 での同等コマンド

```
crypto
   ipsec
      profile ipsec_profile_name
         set ikev2-profile ikev2_profile_name
         set security-association
            lifetime {seconds 120-2592000 | kilobytes disable}
            replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}
         set pfs group {2 | 14 | 15 | 16 | none}
         set transform-set transform_set_name
```

リリース情報

Cisco IOS XE SD-WAN リリース 16.11.x の Cisco vManage で導入されました。

VPN インターフェイス マルチリンク

Cisco SD-WAN ソフトウェアを実行している Cisco IOS XE SD-WAN デバイスには、VPN インターフェイス マルチリンク テンプレートを使用します。

（注） Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

マルチリンク ポイント ツー ポイント プロトコル（MLP）は、複数の物理リンクを、MLP バンドルと呼ばれる単一の論理接続に結合するために使用されます。

Cisco vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイスでマルチリンクを構成するには、次の手順を実行します。

1. VPNインターフェイスマルチリンク機能テンプレートを作成して、マルチリンク インターフェイスのプロパティを構成します。
2. 必要に応じて、VPN 機能テンプレートを作成して、VPN 0 の既定の構成を変更します。

[Template] 画面に移動し、テンプレートに命名する

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. トランスポート VPN（VPN 0）でマルチリンク インターフェイスを構成している場合は、次の手順を実行します。
   1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
   2. 画面の右側にある [Additional VPN 0 Templates] の下で、[VPN Interface Multilink Controller] をクリックします。
6. サービス VPN（VPN 0 以外の VPN）でマルチリンク インターフェイスを構成している場合は、次の手順を実行します。
   1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
   2. [Service VPN] ドロップダウンリストで、サービス VPN の番号を入力します。
   3. 画面の右側にある [Additional VPN Templates] の下で、[VPN Interface Multilink Controller] をクリックします。
7. [VPN Interface Multilink Controller] ドロップダウンリストから、[Create Template] をクリックします。[VPN Multilink] 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、マルチリンク インターフェイス 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 [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 *159*：

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。Viptela 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。Viptela 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、「Create a Template Variables Spreadsheet」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。

マルチリンク インターフェイスの構成

マルチリンク インターフェイスを構成するには、[Basic Configuration] を選択し、次のパラメータを構成します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

（注） VPN インターフェイス マルチリンク テンプレートを作成する場合は、T1/E1 コントローラ テンプレートまたは VPN インターフェイス T1/E1 テンプレートを作成する必要はありません。

表 *160 :*

パラメータ名	説明
Shutdown*	[No] をクリックして、マルチリンク インターフェイスを有効にします。
Interface Name*	MLP インターフェイスの番号を入力します。1 から 65,535 までの数値を指定できます。
説明	マルチリンク インターフェイスの説明を入力します。
Multilink Group Number*	マルチリンクグループの番号を入力します。1 ～ 65,535 の数値を指定できますが、Multilink Interface Name パラメータに入力する数値と同じである必要があります。
IPv4 Address*	静的アドレスを構成するには、[Static] をクリックして、IPv4 アドレスを入力します。 インターフェイスを DHCP クライアントとして設定して、インターフェイスが DHCP サーバーから IP アドレスを受け取るようにするには、[Dynamic] をクリックします。オプションで、DHCP ディスタンスを設定して、DHCP サーバーから学習したルートのアドミニストレーティブディスタンスを指定できます。デフォルトの DHCP ディスタンスは 1 です。
IPv6 Address*	VPN 0 のインターフェイスに静的アドレスを設定するには、[Static] をクリックして、IPv6 アドレスを入力します。 インターフェイスを DHCP クライアントとして設定して、インターフェイスが DHCP サーバーから IP アドレスを受け取るようにするには、[Dynamic] をクリックします。オプションで、DHCP ディスタンスを設定して、DHCP サーバーから学習したルートのアドミニストレーティブディスタンスを指定できます。デフォルトの DHCP ディスタンスは 1 です。オプションで DHCP 高速コミットを有効にして、IP アドレスの割り当てを高速化できます。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（2^{32} / 2）– 1 kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（2^{32} / 2）– 1 kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。MLP のカプセル化は、アウトバウンドパケットのそれぞれに 6 バイト（4 バイトのヘッダーと 2 バイトのチェックサム）を追加します。これらのオーバーヘッドバイトは、実質的な接続の帯域幅を減少させます。そのため、MLP バンドルのスループットは、MLP を使用しない同等の帯域幅接続よりもわずかに少なくなっています。範囲：576 ～ 1804、デフォルト：1500 バイト

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 *161 :*

パラメータ名	説明
認証プロトコル（Authentication Protocol）	MLP で使用される認証プロトコルを選択します。 • **CHAP**：インターネット サービス プロバイダー（ISP）から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • **PAP**：ISPから提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • **PAP**および**CHAP**：両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] 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。

トンネルインターフェイスの作成

最大4つのトンネルインターフェイスを設定できます。つまり、各デバイスに最大4つのTLOCを設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 *162 :*

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。 （注） 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランスパラメータを設定して、最低 650 ～ 700 Kbps の帯域幅を設定することをお勧めします。 BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。 双方向 BFD パケットフローに必要な帯域幅の計算例を以下に示します。 • 制御接続用にデバイスごとに 650 ～ 700 Kbps。 • デバイス上の BFD セッション（要求）ごとに 175 バイト（または 1.4 Kbps） • デバイス上の BFD セッション（応答）ごとに 175 バイト（または 1.4 Kbps） パス MTU ディスカバリ（PMTUD）が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅： 1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。 1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps（要求） 147 バイトの BFD パケットが応答として送信されます。 147 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 40 bps（応答） したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。 700k +（1.4k*775）+（400 *775）+（1.4k*775）+（40 *775）= ～ 3.5 MBps
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8、デフォルト：2

パラメータ名	説明
vBond As STUN Server	[On] をクリックして NAT（STUN）のセッション トラバーサル ユーティリティを有効にし、デバイスが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスが接続できない Cisco vSmart コントローラ を設定します。範囲：0 ～ 100
vManage 接続設定	トンネルインターフェイスを使用して制御トラフィックを vManage NMS と交換するための優先順位を設定します。範囲：0 ～ 8、デフォルト：5
ポートホップ	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。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2 つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *163 :*

パラメータ名	説明
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec は有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。 範囲：0 ～ 4294967295。デフォルト：0

パラメータ名	説明
IPsec の重み	複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255。デフォルト：1
通信事業者	トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。 値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト
ループバック トンネルのバインド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。
ラストリゾート回線	トンネルインターフェイスを最終手段の回線として使用する場合に選択します。 （注） ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1 つ以上のプライマリインターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。 範囲：1 ～ 60 秒。デフォルト：5 秒
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒（1 秒）

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 *164 :*

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のプロパティを設定します。

表 *165*:

パラメータ名	説明
PMTUディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	Cisco SD-WAN デバイスを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1460 バイト。デフォルト：なし
Dont Fragment のクリア	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0 ー 7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目の Cisco SD-WAN デバイスには、WAN への接続が提供されます。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.3 で Cisco vManage に導入されました。

vManage を使用した VPN インターフェイス SVI の設定

Cisco IOS XE SD-WAN デバイスの SVI を設定するには、VPN インターフェイス SVI テンプレートを使用します。VLAN インターフェイスを設定するには、スイッチ仮想インターフェイス（SVI）を設定します。

Cisco vManage テンプレートを使用して Cisco ルータに DSL インターフェイスを設定するには、VPN インターフェイス SVI 機能テンプレートを作成して、VLAN インターフェイスパラメータを設定します。

VPN インターフェイス SVI 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. [Device Templates] で、[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] のタイトルは [Device] です。

3. [Create Template] ドロップダウンから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンから、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. トランスポート VPN（VPN 0）で SVI を構成している場合は、次の手順を実行します。
   1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
   2. [Additional VPN 0 Templates] で、[VPN Interface SVI] をクリックします。
6. サービス VPN（VPN 0 以外の VPN）で SVI を構成している場合は、次の手順を実行します。
   1. [Service VPN] をクリックするか、[Service VPN] までスクロールします。
   2. [Service VPN] ドロップダウンリストで、サービス VPN の番号を入力します。
   3. [Additional VPN Templates] で、[VPN Interface SVI] をクリックします。
7. [VPN Interface SVI] ドロップダウンから、[Create Template] をクリックします。VPN インターフェイス SVI 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、VLAN インターフェイス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横にある [scope] ドロップダウンをクリックします。

（注） SVIインターフェイスを起動して機能させるには、適切なVLANがスイッチポートアクセスまたはトランクインターフェイスで明示的に設定されていることを確認します。

基本的なインターフェイス機能の設定

表 *166 :* 機能の履歴

機能名	リリース情報	説明
セカンダリ IP アドレスの構成のサポート	Cisco IOS XE リリース 17.2.1r	最大 4 つのセカンダリ IPv4 または IPv6 アドレス、および最大 4 つの DHCP ヘルパーを構成できます。セカンダリ IP アドレスは、異なるインターフェイス間で不均等なロードシェアリングを強制する場合、サブネットから使用できる IP がなくなったときに LAN 内の IP アドレスの数を増やす場合、および不連続なサブネットとクラスフル ルーティング プロトコルに関する問題を解決する場合に役立ちます。

VPN で基本的な VLAN インターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *167 :*

パラメータ名	説明
Shutdown*	VLAN インターフェイスを有効にするには [No] をクリックします。
VLAN Interface Name*	インターフェイスの VLAN ID を入力します。範囲：1 ～ 1094。
説明	インターフェイスの説明を入力します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ～ 1500。デフォルト：2000 バイト

パラメータ名	説明
IPv4* or IPv6	クリックして、インターフェイスの IPv4 または IPv6 アドレスを 1 つ以上構成します。（Cisco IOS XE SD-WAN リリース 17.2 以降。）
IPv4 Address* IPv6 Address	インターフェイスの IPv4 アドレスを入力します。
Secondary IP Address	[Add] をクリックして、最大 4 つのセカンダリ IP アドレスを入力します。（Cisco IOS XE SD-WAN リリース 17.2 以降。）
DHCP Helper*	ネットワーク内の DHCP サーバーの IP アドレスを 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。各アドレスはカンマで区切ります。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。 [Add] をクリックして、最大 4 つの DHCP ヘルパーを設定します。（IPv6 については、Cisco IOS XE SD-WAN リリース 17.2 以降。）

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 *168 :*

パラメータ名	説明
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックして、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol（VRRP）をインターフェイスで実行するには、

[VRRP] を選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

表 *169*：

パラメータ名	説明
グループ ID（Group ID）	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。範囲：1 ～ 255
プライオリティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリルータとして選択されます。2 つの Cisco IOS XE SD-WAN デバイスの優先順位が同じ場合、IP アドレスの高い方がプライマリとして選択されます。範囲：1 ～ 254、デフォルト：100
Timer	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。範囲：1 ～ 3600 秒、デフォルト：1 秒
Track OMP Track Prefix List	デフォルトでは、VRRP は、どの Cisco IOS XE SD-WAN デバイス がプライマリ仮想ルータであるかを判別するために、VRRP が実行されているサービス（LAN）インターフェイスの状態を使用します。Cisco IOS XE SD-WAN デバイス がすべての WAN 制御接続を失うと、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを構成します。 Track OMP：[On] をクリックすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションをトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。 Track Prefix List：OMP セッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイスがプライマリ VRRP ルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。
IP アドレス	仮想ルータの IP アドレスを入力します。このアドレスは、ローカル Cisco IOS XE SD-WAN デバイスと VRRP を実行しているピアの両方の設定済みインターフェイス IP アドレスとは異なる必要があります。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル（ARP）テーブルエントリを構成するには、[ARP] を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

表 *170 :*

パラメータ名	Description
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[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。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] を選択し、次のプロパティを設定します。

表 *171 :*

パラメータ名	説明
TCP MSS	Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし
ARP Timeout	動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。範囲：0 ～ 2678400 秒（744 時間）デフォルト：1200（20 分）

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイス T1/E1

Cisco SD-WAN ソフトウェアを実行している Cisco SD-WAN には、VPN インターフェイス T1/E1 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 VPN の T1/E1 インターフェイスを設定するには、次の手順を実行します。

1. この記事の説明に従って、VPN インターフェイス T1/E1 機能テンプレートを作成して、T1/E1 インターフェイスパラメータを設定します。

2. T1/E1 コントローラテンプレートを作成して、T1 または E1 ネットワーク インターフェイス モジュール（NIM）パラメータを設定します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。

[Template] 画面に移動し、テンプレートに命名する

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. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

（注） **注**：Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

   1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
   2. [Additional VPN 0 Templates] で、[VPN Interface T1/E1 Serial] をクリックします。
   3. [VPN Interface T1/E1 Serial] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface T1/E1] 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、VPN インターフェイス イーサネット 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. VPN 1 ー 511 および 513 ー 65530 のテンプレートを作成するには、次の手順を実行します。
   1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
   2. [Service VPN] ドロップダウンリストをクリックします。
   3. [Additional VPN] テンプレートで、[VPN Interface] をクリックします。
   4. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface Ethernet] 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、VPN インターフェイス イーサネット 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、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ます。

基本的なインターフェイス機能の設定

VPN で基本的なインターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *172 :*

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface name*	インターフェイスの名前を入力します。名前は、**serial** *slot* **/** *subslot* **/** *port* **:** *channel-group* の形式にする必要があります。 また、T1/E1 コントローラ機能設定テンプレートでチャネルグループの番号も設定する必要があります。
説明	インターフェイスの説明を入力します。
IPv4 Address*	IPv4 アドレスを入力します。
IPv6 Address*	IPv6 アドレスを入力します。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。 範囲：1 ～（2^{32} / 2）– 1 kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ～ 1804、デフォルト：1500 バイト

トンネルインターフェイスの作成

Cisco IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

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、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[トンネルインターフェイス] を選択し、次のパラメータを設定します。

表 *173*:

パラメータ名	説明
トンネルインターフェイス	[オン] をクリックして、トンネル インターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	デフォルトでは、制御接続はオンに設定されており、TLOCの制御接続を確立します。ルータに複数の TLOC がある場合は、[いいえ] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。 （注） 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランス パラメータを設定して、最低 650 ～ 700 Kbps の帯域幅を設定することをお勧めします。 BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。 双方向 BFD パケット フローに必要な帯域幅の計算例を以下に示します。 • 制御接続用にデバイスごとに 650 ～ 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) パス MTU ディスカバリ（PMTUD）が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅： 1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。 1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps (リクエスト) 147 バイトの BFD パケットが応答として送信されます。 147バイト×8ビット/1バイト×1パケット/30秒 = 40bps（レスポンス） したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3.5 MBps
最大制御接続数	WAN トンネル インターフェイスが接続できる の最大数を指定します。Cisco vSmart コントローラトンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0 ～ 8、デフォルト：2

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[オン] をクリックして NAT (STUN) のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネル インターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネル インターフェイスの接続を許可しない Cisco vSmart コントローラ を設定します。 範囲：0 ～ 100
Cisco vManage Connection Preference	トンネル インターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0 ～ 8、デフォルト：5
ポートホップ	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。ルータが 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ルータとの 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。デフォルト：有効
低帯域幅リンク	トンネル インターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイ ハンドシェイクで交換される MSS に対して検査されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2 つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 を通過する TPC SYN パケットの MSS を指定します。Cisco IOS XE SD-WAN デバイスデフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Dont Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
サービスの許可	サービスごとに [オン] または [オフ] を選択して、インターフェイスでサービスを許可または禁止します。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

Cisco vManage リリース 18.2 で導入されました。

T1/E1 コントローラ

Cisco SD-WAN ソフトウェアを実行する Cisco IOS XE SD-WAN デバイス の場合、T1/E1 コントローラ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 VPN の T1/E1 インターフェイスを設定するには、次の手順を実行します。

1. この記事の説明に従って、T1/E1 コントローラテンプレートを作成して、T1 または E1 ネットワーク インターフェイス モジュール（NIM）パラメータを設定します。
2. VPN インターフェイス T1/E1 機能テンプレートを作成して、T1/E1 インターフェイスパラメータを設定します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。

[Template] 画面に移動し、テンプレートに命名する

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. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。
   1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
   2. [Additional VPN 0 Templates] で、[VPN Interface] をクリックします。
   3. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface T1/E1] 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、VPN インターフェイス イーサネット 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. VPN 1 ー 511 および 513 ー 65530 のテンプレートを作成するには、次の手順を実行します。
   1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
   2. [Service VPN] ドロップダウンリストをクリックします。
   3. [Additional VPN] テンプレートで、[VPN Interface] をクリックします。
   4. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface Ethernet] テンプレートフォームが表示されます。This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
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、次のいずれかを選択します。

- デバイス固有（ホストのアイコンで示される）
- グローバル（地球のアイコンで示される）

T1 コントローラの設定

T1 コントローラを設定するには、[T1] をクリックして、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 *174*:

パラメータ名	説明
Slot*	T1 NIM がインストールされているスロットの番号を、slot/subslot/port の形式で入力します。たとえば、0/1/0 と入力できます。
Framing*	T1 フレームタイプを入力します。 • [esf]：T1 フレームを拡張スーパーフレームとして送信します。これがデフォルトです。 • [sf]：T1 フレームをスーパーフレームとして送信します。スーパーフレーミングは、D4 フレーミングと呼ばれることもあります。
Line Code	T1 フレームの送信に使用する回線エンコーディングを選択します。 • [ami]：回線コードとして Alternate Mark Inversion（AMI）を指定します。AMI シグナリングは、スーパーフレームにグループ化されたフレームを使用します。 • [b8zs]：回線コードとして Bipolar 8-Zeros Substitution を使用します。これがデフォルトです。B8ZS は、拡張スーパーフレームにグループ化されたフレームを使用します
Clock Source	クロックソースを選択します。 • [internal]：コントローラフレーマをプライマリクロックとして使用します。 • [line]：インターフェイスでフェーズロックループ（PLL）を使用します。これがデフォルトです。両方の T1 ポートが回線クロッキングを使用し、どちらのポートもプライマリとして設定されていない場合、デフォルトでは、ポート 0 がプライマリクロックソースで、ポート 1 がセカンダリクロックソースです。
Line Mode	回線クロックソースを選択した場合は、回線がプライマリまたはセカンダリ回線のどちらであるかを選択します。
説明	コントローラの説明を入力します。
Channel Group	チャネルグループの番号を入力します。その場合は、[Time Slot] フィールドにタイムスロットを入力する必要があります。範囲：0 ～ 30

パラメータ名	説明
タイム スロット（Time Slot）	チャネルグループの一部であるタイムスロットを入力します。範囲：1 ～ 24
ケーブル長	減衰を設定するケーブル長を選択します • [long]：パルスイコライゼーションと回線ビルドアウトを使用して、トランスミッタからのパルスを減衰させます。660 フィートを超えるケーブルには、長いケーブル長を設定できます。 • [short]：660 フィート以下のケーブルの伝送減衰を設定します。 デフォルトのケーブル長はありません。
長さ	[Cable Length Field] に値を指定する場合は、ケーブルの長さを入力します。 短いケーブルの場合、長さの値は次のとおりです。 • [110]：0 ～ 110 フィートの長さ • [220]：111 ～ 220 フィートの長さ • [330]：221 ～ 330 フィートの長さ • [440]：331 ～ 440 フィートの長さ • [550]：441 ～ 550 フィートの長さ • [660]：551 ～ 660 フィートの長さ 長いケーブルの場合、長さの値は次のとおりです。 • 0 dB • –7.5 dB • –15 dB • –22.5 dB

機能テンプレートを保存するには、[Save] をクリックします。

E1 コントローラの設定

E1 コントローラを設定するには、[E1] をクリックして、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 175：

パラメータ名	説明
Slot*	E1 NIM がインストールされているスロットの番号を、slot/subslot/port の形式で入力します。たとえば、0/1/0 と入力できます。

パラメータ名	説明
Framing*	E1 フレームタイプを入力します。 • [crc4]：巡回冗長検査 4（CRC4）を使用します。これがデフォルトです。 • [no-crc4]：CRC4 を使用しません。
Line Code*	E1 フレームの送信に使用する回線エンコーディングを選択します。 • [ami]：回線コードとして Alternate Mark Inversion（AMI）を指定します。 • [hdb3]：回線コードとして High-Density Bipolar 3 を使用します。これがデフォルトです。
Clock Source	クロックソースを選択します。 • [internal]：コントローラフレーマをプライマリクロックとして使用します。 • [line]：インターフェイスでフェーズロックループ（PLL）を使用します。これがデフォルトです。
Line Mode	回線クロックソースを選択した場合は、回線がプライマリまたはセカンダリ回線のどちらであるかを選択します。プライマリ回線とセカンダリ回線の両方を設定した場合、プライマリ回線に障害が発生すると、PLL は自動的にセカンダリ回線に切り替わります。プライマリ回線の PLL が再びアクティブになると、PLL は自動的にプライマリ回線に戻ります。
説明	コントローラの説明を入力します。
Channel Group	E1インターフェイスでシリアルWANを設定するには、チャネルグループ番号を入力します。範囲：0 ～ 30
タイム スロット（Time Slot）	チャネルグループの場合、タイムスロットを設定します。範囲：1～31

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

Cisco vManage リリース 18.1.1 で導入されました。

セルラーインターフェイス

LTE接続を有効にするには、セルラーモジュールを備えたルータでセルラーインターフェイスを設定します。セルラーモジュールにより、サービスプロバイダーのセルラーネットワーク上でワイヤレス接続ができます。使用例の1つとしては、分散拠点にワイヤレス接続を提供することがあります。

セルラーネットワークは、ルータのすべての有線 WAN トンネルインターフェイスが使用できなくなった場合にネットワーク接続を提供するために、バックアップ WAN リンクとして一般的に使用されます。分散拠点内での使用パターンと、サービスプロバイダーのセルラーネットワークのコアによってサポートされるデータレートに応じて、セルラーネットワークを分散拠点のプライマリ WAN リンクとして使用することもできます。

デバイスでセルラーインターフェイスを設定すると、デバイスの電源ケーブルを差し込むことで、デバイスをインターネットまたは別の WAN に接続できます。これにより、Cisco vBond オーケストレーション、Cisco vSmart コントローラ、および Cisco vManage システムと接続して認証することで、デバイスはオーバーレイネットワークへの参加プロセスを自動的に開始します。

Cisco vManage を使用したセルラーインターフェイスの設定

Cisco vManage テンプレートを使用してセルラーインターフェイスを構成するには、次の手順を実行します。

1. このセクションの説明に従って、VPNインターフェイスセルラー機能テンプレートを作成して、セルラー モジュール パラメータを設定します。
2. セルラー プロファイル テンプレートを作成して、セルラーモデムが使用するプロファイルを構成します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。

（注） 展開にセルラーインターフェイスを備えたデバイスが含まれている場合は、これらのテンプレートが使用されていない場合でも、セルラー コントローラ テンプレートを Cisco vManage に含める必要があります。

デバイスに LTE またはセルラー コントローラ モジュールが構成されていて、セルラーコントローラ機能テンプレートが存在しない場合、デバイスはセルラー コントローラ テンプレートの削除を試みます。Cisco IOS XE リリース 17.4.2 より前のリリースでは、次のエラーメッセージが表示されます。

```
bad-cli - No controller Cellular 0/2/0, parser-context - No controller Cellular 0/2/0,
parser-response % Cannot remove controllers this way
```

Cisco IOS XE リリース 17.4.2 以降で実行されているデバイスの場合、デバイスは access-denied エラーメッセージを返します。

VPN インターフェイスセルラーの作成

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. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional Cisco VPN 0 Templates] で、[VPN Interface Cellular] をクリックします。
7. [VPN Interface Cellular] ドロップダウンリストから、[Create Template] をクリックします。VPN インターフェイス セルラー 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、VPNインターフェイス セルラー 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。
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、[scope] ドロップダウンリストをクリックします。

基本的なセルラーインターフェイス機能の設定

基本的なセルラーインターフェイス機能を設定するには、[Basic Configuration] をクリックして、次のパラメータを構成します。Parameters marked with an asterisk are required to configure an interface. セルラーインターフェイスのトンネルインターフェイスも設定する必要があります。

表 *176 :*

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface Name*	インターフェイスの名前を入力します。それは [cellular0] でなければなりません。

パラメータ名	説明
説明	セルラーインターフェイスの説明を入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 4 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP（ブロードキャスト）DHCP 要求を転送します。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（$2^{32}/2$）– 1 kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ～（$2^{32}/2$）– 1 kbps
IP MTU*	MTU サイズに 1428 と入力します（バイト単位）。この値は 1428 である必要があります。別の値を使用することはできません。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

VPN 0 のインターフェイスを WAN トランスポート接続として構成するには、セルラーインターフェイスでトンネルインターフェイスを構成する必要があります。攻撃に対するセキュリティを提供するトンネルは、電話番号の送信に使用されます。前のセクションで説明したように、少なくとも、[On] を選択し、インターフェイスの色を選択します。通常、トンネルインターフェイス設定のリマインダについては、システムのデフォルトを受け入れることができます。

トンネルインターフェイスを構成するには、[Tunnel] をクリックし、次のパラメータを構成します。セルラーインターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	説明
Tunnel Interface*	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスを作成します。
Per-tunnel QoS	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルごとの QoS を作成します。 個々のトンネルにサービス品質（QoS）ポリシーを適用でき、ハブツースポーク ネットワーク トポロジでのみサポートされます。

パラメータ名	説明
Per-tunnel QoS Aggregrator	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルごとの QoS を作成します。 （注） 「帯域幅ダウンストリーム」は、トンネルごとの QoS 機能がスポークの役割として有効になるために必要です。
Color*	ドロップダウンから、[Global] を選択します。TLOC の色を選択します。セルラーインターフェイス トンネルに通常使用される色は [lte] です。
Groups	ドロップダウンから、[Global] を選択します。フィールドにグループのリストを入力します。
Border	ドロップダウンから、[Global] を選択します。[On] をクリックして、TLOC をボーダー TLOC として設定します。
最大制御接続数	WAN トンネルインターフェイスが接続できる vSmart コントローラの最大数を設定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。範囲：0 ～ 8 デフォルト：2
vBond As STUN Server	[On] をクリックして NAT（STUN）のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントロールグループリストの除外	このトンネルが制御接続の確立を許可しない 1 つ以上の vSmart コントローラグループの識別子を設定します。 範囲：0 ～ 100

パラメータ名	説明
vManage 接続設定	トンネルを使用して制御トラフィックを Cisco vManage と交換するための優先順位を設定します。 範囲：0 ～ 9 デフォルト：5 エッジデバイスに 2 つ以上のセルラーインターフェイスがある場合、Cisco vManage とセルラーインターフェイスの間のトラフィックの量を最小限に抑えるには、インターフェイスの 1 つを、Cisco vManage へのアップデートの送信時および Cisco vManage からの設定の受信時に使用する優先インターフェイスとして設定します。 トンネルインターフェイスが Cisco vManage に接続されないようにするには、数を 0 に設定します。エッジデバイスの少なくとも 1 つのトンネルインターフェイスには、ゼロ以外の Cisco vManage 接続プリファレンスが必要です。
ポートホップ	ドロップダウンから、[Global] を選択します。[Control Group List] をクリックして、トンネルインターフェイスでのポートホッピングを許可します。 デフォルト：[On]。トンネルインターフェイスでのポートホッピングを禁止します。
低帯域幅リンク	[On] をクリックして、トンネルインターフェイスを低帯域幅リンクとして設定します。 デフォルトは **Off** です。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイ ハンドシェイクで交換される MSS に対して検査されます。構成された TCP MSS 設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2 つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト。デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。 [On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。 （注） [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
Network Broadcast	ドロップダウンから、[Global] を選択します。[On] をクリックして、ネットワークプレフィックス宛てのブロードキャストを受け入れて応答します。LAN インターフェイス機能テンプレートで [Directed Broadcast] が有効になっている場合にのみ、これを [On] にします。 デフォルトは **Off** です。
Allow Service	サービスごとに [On] または [Off] をクリックして、セルラーインターフェイスでサービスを許可または禁止します。

追加のトンネル インターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 *177:*

パラメータ名	説明
GRE	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
GRE Preference	ドロップダウンから、[Global] を選択します。値を入力して、TLOC の GRE プリファレンスを設定します。 範囲：0 ～ 4294967295

パラメータ名	説明
GRE Weight	ドロップダウンから、[Global] を選択します。値を入力して、TLOC の GRE 重み付けを設定します。 デフォルト：1
IPSec	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec は有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	ドロップダウンから、[Global] を選択します。トラフィックをトンネルに誘導するための優先順位を設定する値を入力します。高い値が低い値に優先します。 範囲：0 ～ 4294967295。デフォルト：0
IPsec の重み	ドロップダウンから、[Global] を選択します。複数の TLOC 間でトラフィックのバランスをとるための重み付けを設定する値を入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲：1 ～ 255。デフォルト：1
通信事業者	ドロップダウンから、[Global] を選択します。[Carrier] ドロップダウンから、トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト
ループバックトンネルのバインド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。インターフェイス名の形式は、**ge** slot/port です。

パラメータ名	説明
ラストリゾート回線	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスを最終手段の回線として使用します。デフォルトでは、無効になっています。 （注） ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。 セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1 つ以上のプライマリインターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。 すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラスト リゾート インターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュ パケットの間隔を設定します。範囲：1 ～ 60 秒。デフォルト：5 秒。
Hello 間隔（Hello Interval）	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒（1 秒）。

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒。 デフォルトの hello 間隔は 1000 ミリ秒で、100 ～ 600000 ミリ秒 (10 分) の範囲の時間にすることができます。デフォルトの hello トレランスは 12 秒で、12 ～ 600 秒 (10 分) の範囲の時間にすることができます。TLOC での発信制御パケットを減らすには、トンネルインターフェイスで hello インターフェイスを 60000 ミリ秒（10 分）に設定し、hello 許容時間を 600 秒（10 分）に設定し、エッジデバイスとコントローラ間の DTLS 接続の [no track-transport disable] 定期チェックを含めることをお勧めします。エッジデバイスと任意のコントローラデバイス間のトンネル接続の場合、トンネルはエッジデバイスで構成された hello 間隔と許容時間を使用します。この選択は、トンネルを介して送信されるトラフィックを最小限に抑え、リンクのコストがリンクを通過するトラフィックの量の関数である状況を可能にするために行われます。hello 間隔と許容時間は、エッジデバイスとコントローラデバイス間のトンネルごとに個別に選択されます。コントロールプレーン トラフィックの量を最小限に抑えるために実行されるもう 1 つの手順は、他のインターフェイスが使用可能なときに、セルラーインターフェイスを介して OMP コントロールトラフィックを送受信しないようにすることです。この動作はソフトウェアに固有のものであり、構成することはできません。

機能テンプレートを保存するには、[Save] をクリックします。

セルラーインターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにセルラーインターフェイスを設定するには、[NAT] をクリックして、次のパラメータを設定します。

表 *178*：

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：60 分（1 時間）

パラメータ名	説明
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NATデバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：[オフ（Off）]
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 *179 :*

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を 1 つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535
プロトコル	ポート転送ルールを適用するプロトコル（[TCP] または [UDP]）を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ～ 65530
プライベート IP	ポート転送ルールに一致するトラフィックを転送する内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[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。

アクセスリストの適用

セルラーインターフェイスのシェーピングレートを設定し、QoS マップ、書き換えルール、アクセスリスト、およびポリサーをルータインターフェイスに適用するには、[ACL/QoS] をクリックして、次のパラメータを設定します。

表 *180 :* アクセスリストパラメータ

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。

パラメータ名	説明
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
書き換えルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックし、インターフェイスで受信されるパケットへの IPv4 アクセスリストの名前を指定します。
Egress ACL– IPv4	[On] をクリックして、インターフェイスで送信されるパケットへの IPv4 アクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックし、インターフェイスで受信されるパケットへの IPv6 アクセスリストの名前を指定します。
Egress ACL– IPv6	[On] をクリックして、インターフェイスで送信されるパケットへの IPv6 アクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
Egress policer	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル（ARP）テーブルエントリを構成するには、[ARP] をクリックします。Then click **Add New ARP** and configure the following parameters:

表 *181 :*

パラメータ名	**Description**
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

To save the ARP configuration, click **Add**.

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 *182 :* セルラーインターフェイスの高度なパラメータ

パラメータ名	説明
PMTU ディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	ルータを通過する TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト。デフォルト：[None]。
Clear-Dont-Fragment	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment（DF）ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0 ー 7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
トラッカー	インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。
IP Directed-Broadcast	ドロップダウンから、[Global] を選択します。IP directed-broadcast の場合、[On] をクリックします。 デフォルトは **Off** です。

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 を使用したセルラーインターフェイスの設定

次の例では、セルラーインターフェイスを有効にします。

```
interface Cellular0/2/0
   description Cellular interface
   no shutdown
   ip address negotiated
   ip mtu 1428
   mtu 1500
  exit

  controller Cellular 0/2/0
   lte sim max-retry 1
   lte failovertimer 7
   profile id 1 apn Broadband authentication none pdn-type ipv4
```

Data Profile

表 *183 :* 機能の履歴

機能名	リリース情報	説明
シングルおよびデュアル SIM の実行設定で APN を設定する機能	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能を使用すると、セルラーデバイスのデータプロファイルを作成できます。

セルラーデバイスのデータプロファイルでは、次のパラメータを定義します。デバイスでこれらのパラメータを使用して、サービスプロバイダーと通信します。セルラー コンフィギュレーション モードで **profile id** コマンドを使用して、次のパラメータを設定できます。次のパラメータの詳細については、profile id を参照してください。

- データプロファイルの識別番号
- サービスプロバイダーのアクセス ポイント ネットワーク名
- APN アクセスに使用される認証タイプ：認証なし、CHAP 認証のみ、PAP 認証のみ、または CHAP または PAP 認証のいずれか
- 認証が使用される場合、APN アクセス認証のためにサービスプロバイダーによって提供されるユーザー名とパスワード
- APN アクセスに使用されるパケットデータマッチングのタイプ：IPv4 タイプベアラー、IPv6 タイプベアラー、または IPv4v6 タイプベアラー
- 設定する SIM が挿入されている SIM スロット

セルラーインターフェイス設定のベストプラクティス

エッジデバイスのセルラーテクノロジーは、さまざまな方法で使用できます。

- ラストリゾート回線：ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。

  セルラー インターフェイスを備えたエッジ デバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1つ以上のプライマリ インターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。

  すべてのプライマリ インターフェイスがリモート エッジへの接続を失った場合にのみ、ラスト リゾート サーキットがアクティブになり、エッジ デバイスで BFD TLOC ダウン アラームと制御 TLOC ダウン アラームがトリガーされます。ラスト リゾート インターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンクBFDセッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。

  セルラーインターフェイスをラストリゾート回線として設定するには、**last-resort-circuit** コマンドを使用します。

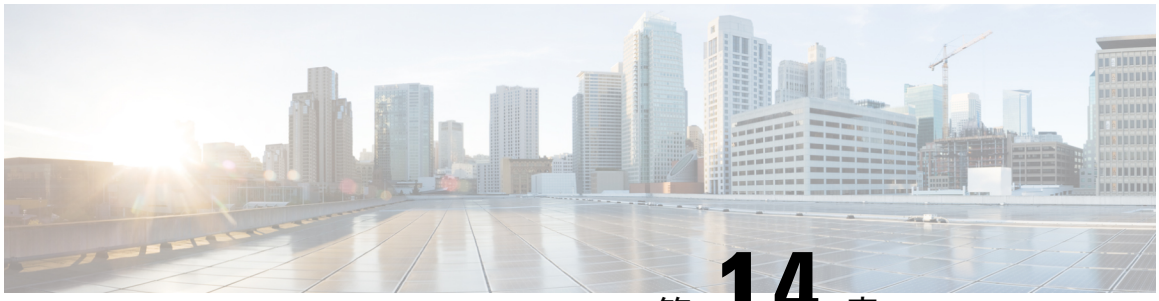
- アクティブ回線：セルラーインターフェイスをアクティブ回線として使用することを選択できます。そうする理由は、おそらく、唯一のラストマイル回線であるためか、または回線のパフォーマンスを測定できるようにセルラーインターフェイスを常にアクティブにしておくためです。このシナリオでは、セルラーインターフェイスを介して制御接続とデータ接続を維持するために使用される帯域幅の量が問題になる可能性があります。セルラーインターフェイスを介した帯域幅の使用量を最小限に抑えるためのベストプラクティスを次に示します。

  - セルラーインターフェイスを備えたデバイスがスポークとして展開され、データトンネルがハブアンドスポーク方式で確立されている場合、セルラーインターフェイスを低帯域幅インターフェイスとして設定できます。これを行うには、セルラーインターフェイスのトンネルインターフェイスを設定するときに、**low-bandwidth-link** コマンドを含めます。セルラーインターフェイスが低帯域幅インターフェイスとして動作している場合、デバイススポークサイトはすべての発信制御パケットを同期できます。スポークサイトはまた、プロアクティブに、ルーティングアップデート以外の制御トラフィックがいずれかのリモートハブノードから生成されないようにすることもできます。ルーティングアップデートは重要なアップデートと見なされるため、引き続き送信されます。

  - 制御パケットタイマーを増やす。セルラーインターフェイスの制御トラフィックを最小限に抑えるために、インターフェイスでプロトコル アップデート メッセージが送信される頻度を減らすことができます。デフォルトでは、OMPはアップデートパケットを毎秒送信します。**omp timers advertisement-interval** 設定コマンドを含めることで、この間隔を最大 65535 秒（約 18 時間）に増やすことができます。デフォルトでは、BFD は Hello パケットを毎秒送信します。**bfd color hello-interval** 設定コマンドを含めることで、この間隔を最大5分（300000ミリ秒）に増やすことができます（OMP アップデートパケットの間隔は秒単位で指定し、BFD Hello パケットの間隔はミリ秒単位で指定することに注意してください）。

- 非セルラーインターフェイスを介した Cisco vManage 制御トラフィックの優先順位付け：エッジデバイスにセルラー トランスポート インターフェイスと非セルラー トランスポートインターフェイスの両方がある場合、デフォルトでは、エッジデバイスはどちらかのインターフェイスを選択して、Cisco vManage と制御トラフィックを交換するために使用します。Cisco vManage とのトラフィック交換にセルラーインターフェイスを使用しないようにエッジデバイスを設定することも、このトラフィックにセルラーインターフェイスを使用するために低いプリファレンスを設定することもできます。トンネルインターフェイスを設定するときに **vmanage-connection-preference** コマンドを含めることで、プリファレンスを設定します。デフォルトでは、すべてのトンネルインターフェイスの Cisco vManage 接続プリファレンス値は 5 です。値の範囲は 0 ～ 8 で、値が大きいほど優先されます。プリファレンス値が 0 のトンネルは、Cisco vManageと制御トラフィックを交換することはできません。

（注） エッジデバイスの少なくとも 1 つのトンネルインターフェイスには、0 以外の Cisco vManage 接続プリファレンス値が必要です。そうでない場合、デバイスには制御接続がありません。



第 14 章

ホットスタンバイ ルータ プロトコル（HSRP）

表 *184 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス での HSRP および HSRP 認証のサポート	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1 Cisco SD-WAN リリース 20.7.1	この機能により、CLI テンプレートを介して Cisco IOS XE SD-WAN プラットフォームで HSRPv2 および HSRP 認証を設定できます。HSRP は、プロトコルと認証のバージョン 2 をサポートする、長年にわたるシスコ独自の First Hop Redundancy Protocol（FHRP）です。

HSRP に関する情報

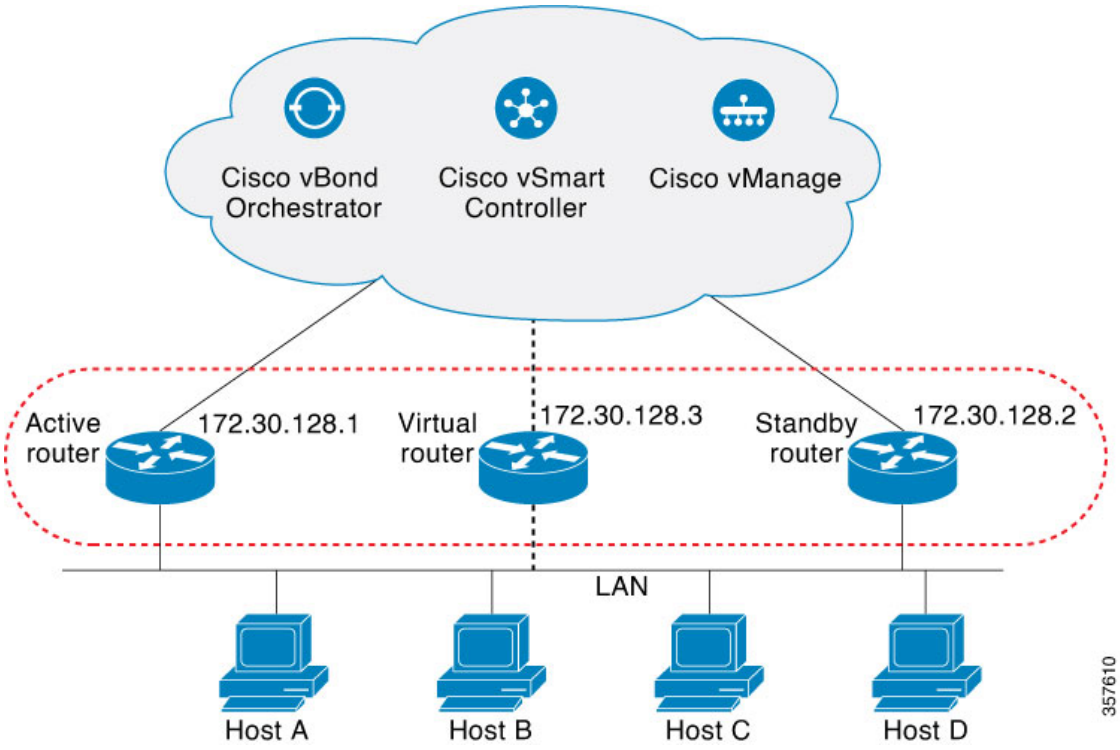
Hot Standby Router Protocol（HSRP）は、ファーストホップ IP デバイスのフェールオーバーを透過的に実行できるように作成された First Hop Redundancy Protocol（FHRP）です。デフォルト ゲートウェイの IP アドレスが設定されたネットワーク上の IP ホストにファーストホップのルーティング冗長性を確保することによって、高いネットワーク アベイラビリティを提供します。ルータ グループ内のアクティブデバイスとスタンバイデバイスを識別する場合は、HSRP を使用します。デバイスインターフェイスのグループでは、アクティブデバイスは、パケットをルーティングするために選択されるデバイスです。スタンバイデバイスはアクティブデバイ

スで障害が発生するか、事前設定された条件が満たされた場合に処理を引き継ぐデバイスです。

複数のホットスタンバイグループをインターフェイスに設定できるので、冗長デバイスおよびロードシェアリングを最大限に活用できるようになっています。

次の図に、HSRP 用に設定されたネットワークのセグメントを示します。仮想 MAC アドレスおよび IP アドレスを共有することによって、複数台のデバイスが 1 台の仮想ルータとして機能します。仮想デバイスは、互いのバックアップになるように設定されている複数のデバイスの共有のデフォルトゲートウェイになります。アクティブデバイスの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。その代わりに、仮想デバイスの IP アドレス（仮想 IP アドレス）をデフォルトゲートウェイとして使用して設定できます。設定した時間内にアクティブデバイスが hello メッセージを送信できない場合、スタンバイデバイスが処理を引き継いで仮想アドレスに対応するアクティブデバイスになり、アクティブデバイスの役割を引き受けます。

図 *2 : HSRP* のトポロジ



HSRP バージョン 2 のサポート

HSRP バージョン 2（HSRPv2）の機能は次のとおりです。

- HSRPv2 では、ミリ秒のタイマー値がアドバタイズおよび検出されます。この変更により、あらゆる状況での HSRP グループの安定性が確保されています。
- HSRPv2 では、グループ番号の範囲が 0 ～ 4095 に拡張されています。

- HSRPv2 では、管理性とトラブルシューティング機能が向上しています。HSRPv2 のパケット形式には、メッセージの送信元を一意に特定するための 6 バイトの識別子フィールドが組み込まれています。通常は、インターフェイスの MAC アドレスがこのフィールドに格納されます。
- HSRPv2 は 224.0.0.102 の IP マルチキャストアドレスを使用して hello パケットを送信します。このマルチキャストアドレスにより、シスコ グループ管理プロトコル（CGMP）の脱退処理を HSRP と同時に有効にできます。
- HSRPv2 のパケット形式は、Type-Length-Value（TLV）を使用する別の形式です。

HSRP MD5 認証

HSRP では、プロトコルパケット認証に単純なプレーンテキスト文字列と Message Digest 5（MD5）スキームを使用できます。HSRP MD5 認証は、マルチキャスト HSRP プロトコルパケットの HSRP 部分の MD5 ダイジェストを生成する、拡張タイプの認証方式です。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。

MD5 認証を使用すると、別のプレーンテキスト認証方式よりもセキュリティを強化できます。HSRP グループの各メンバーは秘密キーを使用して、発信パケットの一部となるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キーストリングを使用して設定で直接指定するか、またはキーチェーンを使用して間接的に指定できます。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

HSRP のオブジェクト トラッキング

オブジェクトトラッキングにより、HSRP からトラッキングメカニズムが分離され、他のプロセスおよび HSRP で使用可能な独立したトラッキングプロセスが別に生成されます。デバイスがオブジェクトトラッキング対応として設定されていて、トラッキング対象のオブジェクトがダウンした場合、デバイスの優先順位はダイナミックに変更されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。

HSRP 静的 NAT 冗長性の概要

Cisco IOS XE リリース 17.9.1a リリース以降、HSRP 静的 NAT 冗長性は Cisco IOS XE SD-WAN でサポートされます。HSRP で静的マッピングがサポートされるため、NAT アドレスが設定されたアクティブルータで着信 ARP に応答できます。この機能により、以前のアクティブルー

タからのARPエントリがタイムアウトするのを待たずに、HSRPアクティブルータからスタンバイルータにフェールオーバーするトラフィックで NAT の冗長性を利用できます。

静的 NAT 設定はアクティブルータとスタンバイルータでミラーリングされ、アクティブルータがトラフィックを処理します。

ルータには仮想 IP アドレスが割り当てられます。エッジデバイスは、仮想 IP アドレスにトラフィックを送信し、そのトラフィックはアクティブルータによって処理されます。スタンバイルータはアクティブルータをモニタリングします。フェールオーバーが発生すると、新しい HSRP アクティブエッジルータは、ARP がタイムアウトするのを待たずに、静的 NAT マッピングの所有権を自動的に再開します。静的 NAT マッピングエントリの Gratuitous ARP を送信して、同じ LAN セグメント内の独自の MAC アドレスを持つようにデバイスを更新します。

（注） HSRP NAT 冗長構成では、静的 NAT のみがサポートされます。

アクティブルータとスタンバイルータで次のタスクを実行し、HSRP に NAT の静的マッピングを設定します。

- 送信元と宛先の NAT が機能していることを確認します。
- NAT インターフェイスの HSRP を有効にします。
- HSRP 冗長性グループ名を設定します。
- 設定されている HSRP 冗長性グループ名を参照して、アクティブエッジとスタンバイエッジの両方で静的 NAT マッピングを手動で設定します。

HSRP 環境の高可用性で静的 NAT 冗長性を有効にする場合は、「Static NAT mapping support with HSRP」を参照してください。

HSRP の利点

- 冗長性：HSRP には、実績があり、大規模ネットワークで広範に導入されている冗長性方式が採用されています。
- 高速なフェールオーバー：HSRPはファーストホップデバイスの透過的な高速フェールオーバーを提供します。
- プリエンプション：プリエンプションにより、スタンバイデバイスがアクティブになるのを一定時間遅らせることができます（この時間は設定可能です）。
- 認証：HSRP の MD5 アルゴリズム認証は、HSRP スプーフィングソフトウェアからの保護に対応し、業界標準の MD5 アルゴリズムを使用して信頼性とセキュリティを向上させます。

HSRP でサポートされるデバイス

Cisco Catalyst 8500 シリーズ エッジ プラットフォーム

Cisco Catalyst 8300 シリーズ エッジ プラットフォーム

Cisco Catalyst 8200 シリーズ エッジ プラットフォーム

Cisco Catalyst 8200 uCPE シリーズ エッジ プラットフォーム

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ

Cisco ISR 1000 および ISR 4000 シリーズ サービス統合型ルータ（ISR）

Cisco ISR 1100 および ISR 1100X シリーズ サービス統合型ルータ（ISR）

Cisco IR1101 耐環境性能 サービス統合型ルータ

Cisco Catalyst 8000v シリーズ クラウドサービスルータ

これらの各デバイスファミリでサポートされるモデルの詳細については、「Cisco SD-WAN Device Compatibility」のページを参照してください。

CLI を使用した HSRP の設定

Cisco vManage CLI アドオン機能テンプレートおよび CLI デバイステンプレートを使用して、HSRP を設定できます。CLIテンプレートを使用した構成の詳細については、「CLIテンプレート」を参照してください。

（注） 次のコマンドはどの順序で実行してもかまいません。

次のリストに、Cisco IOS XE SD-WAN デバイス での HSRP 設定に関する情報を示します。

- HSRP を有効にします。

  HSRP グループの番号および仮想 IP アドレスを使用して、IPv4 で HSRP グループを作成（または有効に）します。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

  IPv6 の HSRP をアクティブにします。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ipv6 {link-local-address | autoconfig }
```

- バージョン 2 に変更します。

  HSRP バージョンを変更します。インターフェイスに IPv6 グループがある場合、**nostandby** または **nostandby version 2** コマンドは拒否されることに注意してください。

（注） インターフェイスに IPv6 グループがある場合、**nostandby** または **nostandby version 2** コマンドは拒否されます。

```
Device(config)# interface interface-type
Device(config-if)# standby version {1|2}
```

- HSRP のプライオリティとプリエンプションを設定します。

  アクティブルータの選択に使用されるプライオリティ値を設定し、HSRP プリエンプションとプリエンプション遅延を設定します。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
Device(config-if)# standby group-number priority [priority]
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
 seconds] [ sync seconds]}]
```

- HSRP 認証を設定します。

  キーチェーンを使用した HSRP MD5 認証を設定します。

  キー チェーンを使用すると、キー チェーン設定に従って異なる時点で異なるキー ストリングを使用できます。HSRP は、適切なキーチェーンを照会して、指定されたキーチェーンの現在アクティブなキーとキー ID を取得します。

```
Device(config)# interface interface-type
Device(config-if)# ip address ip-address mask [secondary ]
Device(config-if)# standby group-number priority [priority]
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
 seconds] [ sync seconds]}]
Device(config-if)# standby group-number authentication md5 key-chain key-chain-name
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

  HSRP テキスト認証を設定します。

  認証文字列には 8 文字までを指定できます。デフォルトの文字列は Cisco です。

```
Device(config)# interface interface-type
Device(config-if)# ip address ip-address mask [secondary ]
Device(config-if)# standby group-number priority [priority]
Device(config-if)# standby group-number preempt [ delay{ [ minimum seconds] [ reload
 seconds] [ sync seconds]}]
Device(config-if)# standby group-number authentication text string
Device(config-if)# standby group-number ip [ip-address [secondary]]
```

- HSRP タイマーを設定します。

  helloパケット間隔、およびアクティブルータを非アクティブであると他のルータが宣言するまでの時間を設定します。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number ip [ip-address [secondary]]
Device(config-if)# standby group-number timers hellotime holdtime
```

- HSRP オブジェクトトラッキングを設定します。

  オブジェクトを追跡し、オブジェクトの状態に基づいてHSRPのプライオリティを変更するように HSRP を設定します。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number track object-number [decrement
priority-decrement] [shutdown]
```

- HSRP 複数グループ最適化により CPU およびネットワークのパフォーマンスを向上します。

  HSRP グループをクライアントグループとして設定します。

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number follow group-name
  ```

  HSRP クライアントグループの更新間隔を設定します。

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number mac-refresh seconds
  ```

- HSRP の仮想 MAC アドレスを設定します。

  HSRP の仮想 MAC アドレスを指定します。

  ```
  Device(config)# interface interface-type
  Device(config-if)# standby group-number mac-address mac-address
  ```

- HSRP グループへ IP 冗長性クライアントをリンクします。

  スタンバイグループ名を設定します。

（注） Cisco IOS XE リリース 17.9.1a 以降、HSRP を使用した静的 NAT マッピング設定がサポートされます。冗長性命名規則にはスペースは含まれません。**standby group-number name***[redundancy-name]* コマンドを設定するときは、スペースを含む冗長名を使用しないことをお勧めします。

```
Device(config)# interface interface-type
Device(config-if)# standby group-number name [redundancy-name]
```

次に、CLI を使用した Cisco IOS XE SD-WAN デバイスでの HSRP の完全な設定例を示します。

```
config-transaction
!
    interface GigabitEthernet0/0/1.94
    encapsulation dot1Q 94
    vrf forwarding 509
    ip address 10.96.194.2 255.255.255.0
    ip directed-broadcast
    ip mtu 1500
    ip nbar protocol-discovery
    standby version 2
    standby 1 preempt
    standby 94 ip 10.96.194.1
    standby 94 timers 1 4
    standby 94 priority 110
    standby 94 preempt delay minimum 180
    standby 94 authentication md5 key-string 7 094F471A1A0A
    standby 94 track 8 shutdown
    standby 194 ipv6 2001:10:96:194::1/64
    standby 194 timers 1 4
```

```
  standby 194 priority 110
  standby 194 preempt delay minimum 180
  standby 194 authentication md5 key-string 7 094F471A1A0A
  standby 194 track 80 shutdown
  ip policy route-map clear-df
  ipv6 address 2001:10:96:194::2/64
  ipv6 mtu 1500
  arp timeout 1200
  end
```

CLI を使用した HSRP 設定の確認

次に、スタンバイルータの情報を表示する **show standby** コマンドの出力例を示します。

```
Device# show standby
GigabitEthernet0/0/1.94 - Group 94 (version 2)
  State is Standby
    1 state change, last state change 01:06:09
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.688 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is 10.96.194.2, priority 110 (expires in 4.272 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
  FLAGS: 0/1
GigabitEthernet0/0/1.94 - Group 194 (version 2)
  State is Standby
    1 state change, last state change 01:06:07
    Track object 80 state Up
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:C2 (impl auto EUI64)
    Virtual IPv6 address 2001:10:96:194::1/64
  Active virtual MAC address is 0005.73a0.00c2 (MAC Not In Use)
    Local virtual MAC address is 0005.73a0.00c2 (v2 IPv6 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.480 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is FE80::CE16:7EFF:FE8C:6DD1, priority 110 (expires in 4.032 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-194" (default)
  FLAGS: 0/1
```

次に、HSRP バージョン 2 が設定されている場合に HSRP バージョン 2 の情報を表示する **show standby** コマンドの出力例を示します。

```
Device# show standby
Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
   Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
```

```
   Next hello sent in 1.804 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  Group name is "hsrp-Et0/1-1" (default)
Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)
    Track interface Serial2/0 state Down decrement 10
  Group name is "hsrp-Et0/2-1" (default)
```

次に、HSRP MD5 認証が設定されている場合に HSRP 認証情報を表示する **show standby** コマンドの出力例を示します。

```
Device# show standby
Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

次に、特定のインターフェイスの HSRP 情報を表示する **show standby brief** コマンドの出力例を示します。

```
Device# show standby brief
Interface   Grp  Pri P State   Active                    Standby   Virtual IP
Gi0/0/1.94  94   105 P Standby 10.96.194.2                 local    10.96.194.1
Gi0/0/1.94  194  105 P Standby FE80::CE16:7EFF:FE8C:6DD1   local    FE80::5:73FF:FEA0:C2
```

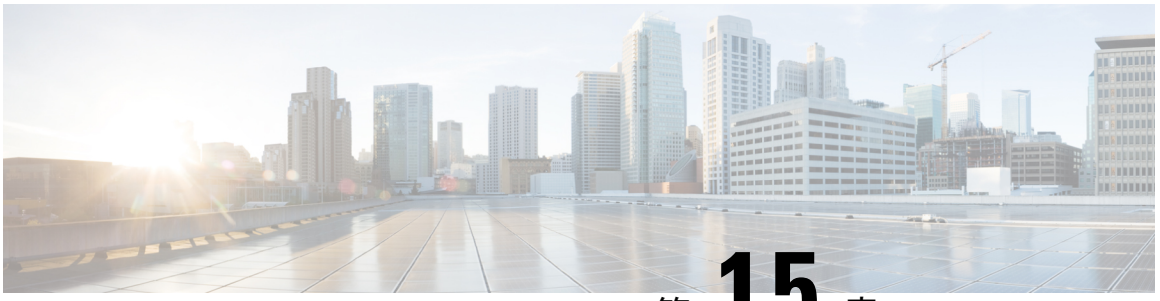
次に、イーサネットインターフェイス 0/0 の HSRP ネイバーを表示する **show standby neighbors** コマンドの出力例を示します。ネイバー 10.0.0.250 は、グループ 2 に対してアクティブ、グループ 1 および 8 に対してスタンバイであり、BFD に登録されています。

```
Device# show standby neighbors Ethernet0/0
HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
```

```
    No Active groups
    No Standby groups
    BFD enabled
```

次に、すべての HSRP ネイバーの情報を表示する **show standby neighbors** コマンドの出力例を示します。

```
Device# show standby neighbors
HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled
HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```



第 15 章

セルラーゲートウェイの設定

表 *185 :* 機能の履歴

機能名	リリース情報	機能説明
セルラーゲートウェイの設定	Cisco vManage リリース 20.4.1	この機能では、サポートされているセルラーゲートウェイを IP パススルーデバイスとして設定するためのテンプレートを使用できます。このリリースでは、Cisco セルラーゲートウェイ CG418-E がサポートされます。

サポートされているセルラーゲートウェイを IP パススルーデバイスとして設定できます。設定されたデバイスをLTE信号が強い施設内のエリアに配置することにより、信号をイーサネット接続を介して、LTE 信号が弱い場所にあるルーティング インフラストラクチャに拡張できます。

Cisco vManage でセルラーゲートウェイを設定するには、次の手順を実行します。

1. **Cisco セルラーゲートウェイ CG418-E** デバイスのデバイステンプレートを作成します。

   『*Systems and Interfaces Configuration Guide*』の「機能テンプレートからのデバイステンプレートの作成」を参照してください。

   機能テンプレートの説明を入力したら、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. [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. **[Cellular Gateway]** > **[Cellular Gateway Platform]** > **[Create Template]** を選択します。次に、以下の表に示すように、セルラー ゲートウェイ プラットフォーム機能テンプレートを設定します。

表 *186* : セルラー ゲートウェイ プラットフォーム テンプレート パラメータ

パラメータ名	説明
[Basic Configuration] タブ	
タイム ゾーン	デバイスで使用するタイムゾーンを選択します。NTP が設定されている場合、デバイスはこのタイムゾーンをクロック同期に使用します。
管理インターフェイス	デバイスにアクセスするための管理インターフェイスの IPv4 アドレスを入力します。
Admin-Password	SSH クライアントまたはコンソールポートを使用してデバイスにログインするための管理者ユーザーパスワードを入力します。
NTP-Servers	デバイスがクロックを同期する 1 つまたは複数の NTP サーバーを設定します。
[Cellular Configuration] タブ	
IP-Src-Violation	対応する IP アドレスタイプの IP ソース違反機能を有効にするには、[v4 only]、[v6 only]、または [v4 and v6] を選択します。この機能を有効にしない場合は、[None] を選択します。
Auto-SIM	[On] を選択して、自動 SIM 機能を有効にします。この機能を有効にすると、デバイスは、デバイス内の SIM が属するサービスプロバイダーを自動的に検出し、そのプロバイダーに適したファームウェアを自動的にロードします。

パラメータ名	説明
Primary SIM Slot	デバイスのプライマリ SIM カードが挿入されるスロットを選択します。デバイスがこのスロットへのサービスを失った場合、セカンダリスロットにフェールオーバーします。
Failover-Timer（分）	デバイスがプライマリ SIM スロットへのサービス消失を検出してから、プライマリ SIM スロットとの通信を試行するまでデバイスが待機する分数を入力します。
Max-Retry	連続試行回数を入力します。デバイスがプライマリ SIM との通信にこの回数連続して失敗すると、セカンダリスロットにフェールオーバーします。

6. **[Cellular Gateway]** > **[Cellular Gateway Profile]** を選択し、[Cellular Gateway Profile] ドロップダウンリストから [Create Template] を選択します。次にセルラー ゲートウェイ プロファイル機能テンプレートを以下の表に示すように設定します。

表 *187:* セルラー ゲートウェイ プロファイル テンプレート パラメータ

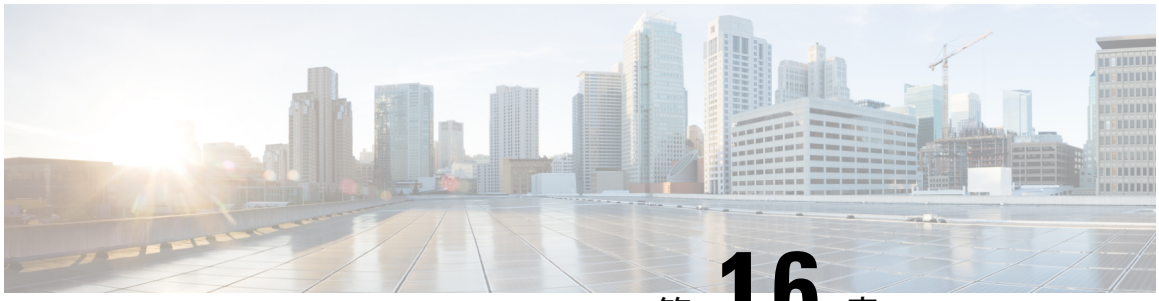
パラメータ名	説明
[Basic Configuration] タブ	

パラメータ名	説明
SIM	SIM スロットを選択し、次のオプションを設定して、このスロットの SIM のプロファイルを作成します。このプロファイルによって、SIMを接続するセルラーネットワークをサービスプロバイダーに示します。 • Profile ID：プロファイルの一意の ID を入力します • Access Point Name：このプロファイルのアクセスポイントの名前を入力します • Packet Data Network Type：このプロファイルのデータサービスのネットワークタイプを選択します（[IPv4]、[IPv6] または [IPv4v6]） • Authentication：このプロファイルがデータに使用する認証方法を選択し、表示される [Profile Username] および [Profile Password] フィールドに、この方法のユーザー名とパスワードを入力します デバイスの SIM スロットごとに 1 つのプロファイルを設定できます。
Add Profile	クリックして、セルラーデバイスがセルラーネットワークに接続するために使用するアクセスポイント名（APN）プロファイルを追加します。 最大 16 個のプロファイルを追加できます。
プロファイル ID	プロファイルの一意の識別子を入力します。 有効な値：1 ～ 16 の整数
アクセス ポイント名	セルラーアクセスポイントを識別する名前を入力します。

パラメータ名	説明
Packet Data Network Type	セルラーネットワークのパケットデータネットワーク（PDN）タイプ（[IPv4]、[IPv6] または [IPv46]）を選択します。
認証	セルラーアクセスポイントへの接続に使用する認証方法（[none]、[pap]、[chap]、[pap_chap]）を選択します。
Profile Username	[none] 以外の認証方法を選択した場合は、セルラーアクセスポイントに接続するときに認証に使用するユーザー名を入力します。
パスワード	[none] 以外の認証方法を選択した場合は、セルラーアクセスポイントに接続するときに認証に使用するパスワードを入力します。
[Add	クリックして、設定するプロファイルを追加します。
[Advanced Configuration] タブ	
Attach Profile	デバイスがセルラーネットワークに接続するために使用するプロファイルを選択します。
Cellular 1/1 Profile	デバイスがセルラーネットワーク経由のデータ接続に使用するプロファイルを選択します。

2. デバイステンプレートをデバイスに添付します。

   『*Systems and Interfaces Configuration Guide*』の「デバイステンプレートのアタッチとアタッチ解除」を参照してください。



第 16 章

ジオフェンシングの設定

表 *188* : 機能の履歴

機能名	リリース情報	説明
[Geofencing（ジオフェンシング）]	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能は、デバイスの場所を運用上の地理的境界に制限し、デバイスの場所を特定して、設定された境界の違反を報告する方法を提供します。デバイスが違反していると識別された場合は、Cisco vManage の操作コマンドを使用してデバイスへのネットワークアクセスを制限できます。 CLI または CLI テンプレートで、デバイスの場所を確立するためのジオフェンシング座標を設定します。SMS アラートに登録することもできます。
Cisco システム機能テンプレートを使用したジオフェンシングの設定のサポートを追加	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、シスコ システムの機能テンプレートを使用してデバイスの地理的境界を設定するためのサポートが追加されます。 この機能を使用すると、ジオフェンシングの構成中に、デバイスが自身の位置を特定する自動ジオロケーション検出を構成することもできます。新しいパラメータ **auto-detect-geofencing-location** が **geolocation (system)** コマンドに追加されました。
LTE Advanced NIM モジュールのサポートの追加	Cisco IOS XE リリース 17.8.1a	Cisco ISR 4000 ルータの Long-Term Evolution（LTE）Advanced Network Interface Modules（NIM）のサポートが追加されました。

ジオフェンシングに関する情報

ジオフェンシングを使用すると、デバイスを展開できる地理的境界を定義できます。デバイスが境界の外で検出されると、Cisco vManage に対し、SMS アラートとクリティカルイベントアラームが生成されます。

Long-Term Evolution プラガブル インターフェイス モジュール（PIM）内のグローバル ポジショニング システム（GPS）は、Cisco IOS XE SD-WAN デバイス でのデバイスの検出と監視に使用されます。

デバイス CLI または Cisco vManage CLI テンプレートを使用して、次の設定を構成できます。

- ベース位置（緯度と経度）とデバイス検出用のジオフェンス範囲
- SMS メッセージを携帯電話番号に送信するためのショートメッセージサービス（SMS）アラート登録
- コントローラセルラー 0/x/0 セクションの Long-Term Evolution PIM での GPS の有効化

（注） 機能テンプレートを使用して、Long-Term Evolution PIM で GPS を有効にすることもできます。

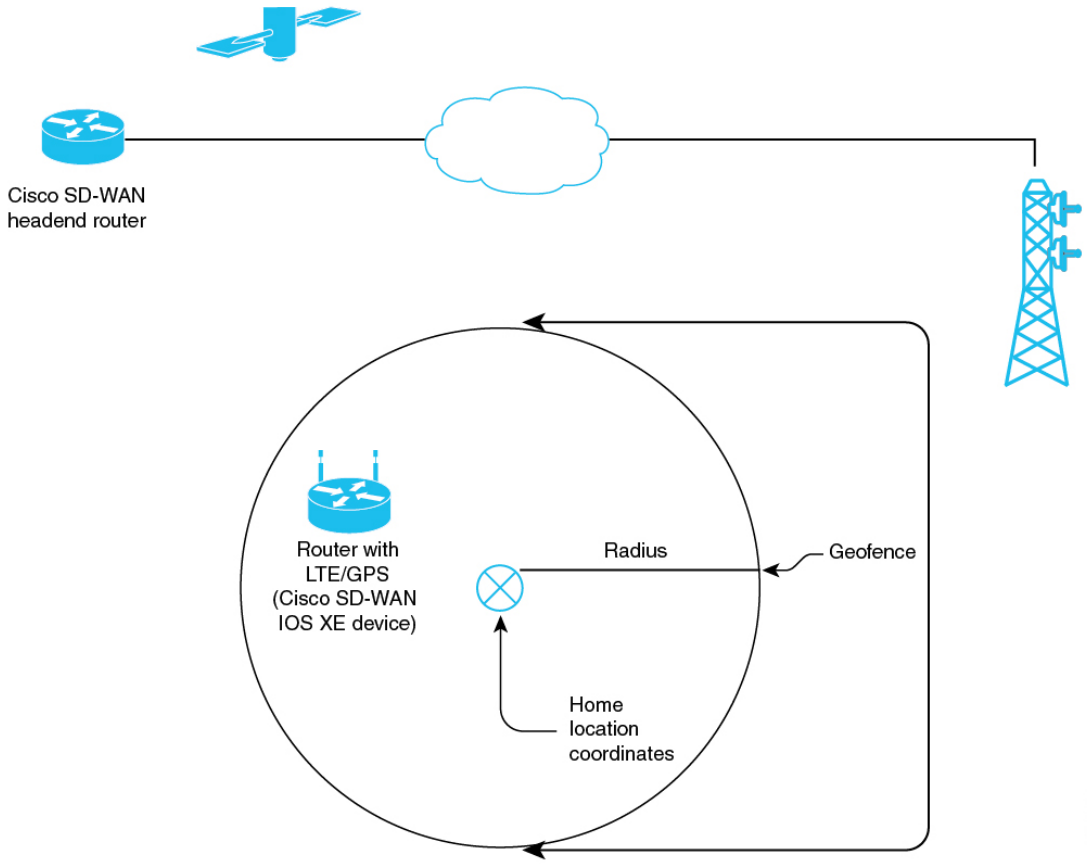
Cisco vManage リリース 20.7.1 から、[Cisco System] 機能テンプレートを使用してジオフェンシングを設定できます。デバイスが独自のベース位置を決定するデバイスの自動位置情報検出を有効にすることもできます。

Cisco vManage では、デバイスが地理的境界を越えた場合にネットワークアクセスを制限するための操作コマンドを使用できます。

ネットワークアクセスを制限する操作コマンドの詳細については、『Cisco SD-WAN Monitor and Maintain Configuration Guide』を参照してください。

デバイスの境界違反が検出されると、ジオフェンシング ステータス アラートが Cisco vManage に送信されます。

図 *3 :* ジオフェンシングの概要



ジオフェンシングの利点

- デバイスが地理的境界を越えている場合に、組織のネットワークへの不適切なアクセスから保護
- 移動したデバイスをエンドユーザーに通知
- デバイスのターゲット位置を指定するためのジオフェンス半径をサポート
- 携帯電話アラートの SMS アラートをサポート

ジオフェンシングでサポートされるデバイス

サポートされるデバイス：

- Long-Term Evolution（固定およびプラガブル）を備えた Cisco ISR 1000
- Long-Term Evolution Pluggable Interface Module（PIM）を備えた Cisco Catalyst 8K

- Long-Term Evolution Advanced Network Interface Module（NIM）を備えた Cisco ISR 4000

サポートされている Long-Term Evolution PIM：

- P-LTE-VZ（WP7601）
- P-LTE-US（WP7603）
- P-LTE-JN（WP7605）
- P-LTE-MNA（WP7610）
- P-LTE-GB（WP7607）
- P-LTE-IN（WP7608）
- P-LTE-AU（WP7609）
- P-LTEA-EA（EM7455）
- P-LTEA-LA（EM7430）

サポートされている Long-Term Evolution Advanced NIM：

- NIM-LTEA-EA（EM7455）
- NIM-LTEA-LA（EM7430）

ジオフェンシングの前提条件

- Cisco IOS XE SD-WAN C1100 シリーズ ルータにロングターム エボリューション インターフェイスが組み込まれていることを確認します。
- CLI または CLI テンプレートを使用してジオフェンシングを有効にします。Cisco vManage リリース 20.7.1 以降では、機能テンプレートを使用してジオフェンシングを有効にすることもできます。

  詳細については、『*Cisco IOS XE SD-WAN Qualified Command Reference Guide*』を参照してください。
- ロングターム エボリューション PIM では、SMS アラートを受信するために SIM カードが必須です。

ジオフェンシングの制約事項

- ジオフェンシングは、Cisco SD-WAN コントローラモードでのみ使用できます。

Cisco システムテンプレートを使用したジオフェンシングの設定

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. デバイスを選択します。
5. **[Select Template]** > **[Basic Information]** セクションで、**[Cisco System]** をクリックします。
6. [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。
7. [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。
8. [Cisco System] テンプレートの [Basic Configuration] セクションで、[Console Baud Rate (bps)] のドロップダウンリストから値を選択します。

   [Console Baud Rate (bps)] は、ジオフェンシングを設定するための必須フィールドです。
9. [GPS] をクリックするか、[Cisco System] テンプレートの [GPS] セクションに移動します。
10. [Latitude] フィールドで、デバイスの自動検出のためにフィールドを [Default] に設定したままにします。

    使用可能な値は、-90.0 ～ 90.0 です。
11. [Longitude] フィールドで、デバイスの自動検出のためにフィールドを [Default] に設定したままにします。

    使用可能な値は、-180.0 ～ 180.0 です。

注意 [Latitude] と [Longitude] の座標を手動で指定すると、デバイスの自動検出が無効になります。

デバイスに最後に認識された有効な場所がない場合、デバイスの自動検出は失敗する可能性があります。

12. [Geo Fencing Enable] フィールドで、範囲を [Default] から [Global] に変更し、[Yes] をクリックしてジオフェンシングを有効にします。

    [Geo Fencing Enable] フィールドは、デフォルトでは有効になっていません。

13. （オプション）[Geo Fencing Range in meters] フィールドで、メートル単位のジオフェンシング範囲の単位を指定します。

    ジオフェンシング範囲は、基本のターゲットの場所からの半径をメートル単位で指定します。

    デフォルトのジオフェンシング範囲は 100 m です。100 ～ 10,000 メートルのジオフェンシング範囲を設定できます。

14. （オプション）[Enable SMS] ドロップダウンリストで、範囲を [Global] に変更し、[Yes] をクリックして SMS アラートを有効にします。

    SMS アラートは、デバイスがターゲットの場所の設定されたジオフェンシング半径の外にあると判断された場合に配信されます。

（注） ロングターム エボリューション PIM では、SMS アラートを受信するために SIM カードの存在が必須です。

15. （オプション）[Mobile Number 1] フィールドに、SMS アラートを受信するための携帯電話番号を追加します。

（注） 携帯電話番号は、+ 記号で始まり、国コード、エリアコードを含み、国コードとエリアコードの間にスペースを入れず、残りの数字を含める必要があります。

    携帯電話番号の例は、+12344567236 です。

    その他の携帯電話番号を設定するには、[+] アイコンをクリックします。

    最大 4 つの携帯電話番号を設定できます。

16. [Save] をクリックします。

CLI を使用したジオフェンシングの設定

緯度、経度、ジオフェンス範囲の設定および SMS アラートの有効化

ここでは、次の CLI 設定の例を示します。

- ベースの位置、緯度と経度を設定します。
- デバイスが自身の位置を特定するデバイスの自動検出を有効にします。

• ジオフェンス範囲を有効化、設定、および指定します。

（注）
- ジオフェンシング範囲の単位はメートルです。
- ジオフェンシング範囲はオプションの設定パラメータであり、設定しない場合、デフォルト値の 100 m が使用されます。

• SMS アラートを受信するための携帯電話番号を追加します。

1. ベースの位置を設定します。

```
Device(config)# system
Device(config-system)# gps-location latitude 37.317342 longitude -122.218170
```

2. デバイスの自動検出を有効にします。

```
Router(config)# system
Router(config-system)# no gps-location latitude
Router(config-system)# no gps-location longitude
Router(config-system)# gps-location auto-detect-geofencing-location
```

（注） auto-detect-geofencing-location パラメータを使用する場合は、緯度と経度の座標を設定しないでください。

緯度と経度の座標を使用してベースの位置を設定するか、デバイスの自動検出を有効にするかを選択できます。

3. ジオフェンス範囲を有効化、設定、および指定します。

```
Device(config-system)# gps-location geo-fencing-enable
Device(config-system)# gps-location geo-fencing-config
Device(conf-geo-fencing-config)# geo-fencing-range 1000
```

4. デバイスのユーザーの携帯電話番号を追加して、SMS アラートを設定します。

```
Device(config-geo-fencing-config)# sms

Device(config-sms)# sms-enable
Device(config-sms)# mobile-number +12344567234
Device(config-mobile-number-+12344567234)# exit
Device(config-mobile-number-+12344567234)# mobile-number +12344567235
Device(config-mobile-number-+12344567235)# exit
Device(config-mobile-number-+12344567235)# mobile-number +12344567236
Device(config-mobile-number-+12344567236)# exit
Device(config-mobile-number-+12344567236)# mobile-number +12344567237
Device(config-mobile-number-+12344567237)# exit
Device(config-sms)# commit
```

5. 変更を保存します。

コントローラ セルラー セクションでのロングターム エボリューション PIM の GPS の有効化

ここでは、設定の 0/x/0 セクションでロングターム エボリューション PIM の GPS を有効にするための CLI 設定の例を示します。

1. コントローラ セルラー セクションでロングターム エボリューション PIM の GPS を有効にします。

```
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte gps enable
```

2. ロングターム エボリューション PIM に存在する SIM カードで ms-based モードを有効にします。SIM カードが存在する状態で ms-based を使用することをお勧めします。

   モバイルステーションベースのアシスタンスとは、グローバルナビゲーション衛星システム（GNSS 対応）モバイルデバイスが自身の位置をローカルで計算する場合を指します。

```
Device(config-Cellular-0/2/0)# lte gps mode ms-based
```

3. 米国海洋電子機器協会（NMEA）のストリーミングを有効にします。

```
Device(config-Cellular-0/2/0)# lte gps nmea
```

4. 変更を保存します。

ジオフェンシング設定の確認

次に、**show sdwan geofence-status** コマンドの出力例を示します。

```
Device# show sdwan geofence-status
geofence-status
 Geofence Config Status =                  Geofencing-Enabled
 Target Latitude =                         37.317342
 Target Longitude =                        -122.218170
 Geofence Range(in m) =                    100
 Current Device Location Status =          Location-Valid
 Current Latitude =                        37.317567
 Current Longitude =                        -122.218170
 Current Device Status =                   Within-defined-fence
 Distance from target location(in m) =     30
 Last updated device location timestamp =  2021-05-06T22:58:34+00:00
 Auto-Detect Geofencing Enabled =          true
```

この出力では、`Geofence Config Status = Geofencing-Enabled` なので、ジオフェンシングが有効になっています。

この出力では、`Auto-Detect Geofencing Enabled = true` です。したがって、デバイスの自動検出が有効になります。デバイスの自動検出が有効になっていない場合、`Auto-Detect Geofencing Enabled = false` が出力に表示されます。

次に、**show cellular 0/x/0 gps** コマンドの出力例を示します。

```
Device# show cellular 0/2/0 gps
GPS Feature =  enabled
GPS Mode Configured =  ms-based
GPS Port Selected =  Dedicated GPS port
GPS Status =  GPS coordinates acquired
Last Location Fix Error =  Offline [0x0]
```

```
==============================
GPS Error Count =  0
NMEA packet count =  17899
NMEA unknown packet count =  0


Per talker traffic count =
        US-GPS =  5982
        GLONASS =  2560
        GALILEO =  3505
        BEIDOU =  0
        GNSS =  3409
        Unknown talker =  2443
==============================
Speed over ground in km/hr =  0
==============================

Latitude =  31 Deg 19 Min 14.6203 Sec North
Longitude =  122 Deg 58 Min 32.8164 Sec West
*Apr 15 23:58:45.298: GPS Mode Configured =Timestamp (GMT) =  Thu Apr 15 23:57:21 2021

Fix type index =  0, Height =  18 m
Satellite Info
----------------
Satellite #2, elevation 51, azimuth 42, SNR 24 *
Satellite #5, elevation 36, azimuth 144, SNR 34 *
Satellite #6, elevation 14, azimuth 45, SNR 24 *
Satellite #12, elevation 72, azimuth 146, SNR 33 *
Satellite #25, elevation 60, azimuth 305, SNR 25 *
==============================
 Total Satellites in view =  5
 Total Active Satellites =  5
 GPS Quality Indicator =  1
 Total satellites from each constellation:
         US-GPS =  3
         GLONASS =  1
         GALILEO =  1
         BEIDOU =  0
==============================
```

この出力では、`GPS Feature = enabled` および `GPS Mode Configured = ms-based` です。したがって、コントローラセルラーの GPS が有効になっており、`ms-based` が設定されています。

次に、**show sdwan notification stream viptela** コマンドの出力例を示します。

```
Device# show sdwan notification stream viptela
notification
 eventTime 2021-04-13T23:05:02.881093+00:00
 system-logout-change
  severity-level minor
  host-name pm5
  system-ip 172.16.255.15
  user-name admin
  user-id 0
 !
!
notification
 eventTime 2021-04-14T00:36:31.344117+00:00
 geo-fence-alert-status
  severity-level major
  host-name pm5
  system-ip 172.16.255.15
  alert-type device-location-inside
  alert-msg Device Locking started for Geofencing Mode and device is within range
```

ジオフェンシングアラームの監視

重大度または時間に基づいてジオフェンシングアラームを監視できます。

ジオフェンシングアラームのタイプは次のとおりです。

表 *189 :* ジオフェンシングアラームのタイプ

タイプ	シビラティ（重大度）	説明
Device Location Outside	**[Critical]**	この通知は、デバイスの場所が定義されたジオフェンシング範囲外にある場合に送信されます。
Device Location Inside	**[Major]**	この通知は、以前にデバイスの位置が定義されたジオフェンスの範囲外にあると判断された場合、または GPS 信号の停止のためにデバイスの位置を取得できなかった場合、定義されたジオフェンスの範囲内にあると判断されると送信されます。
Device Location Lost	**[Major]**	この通知は、GPS の停止によりデバイスの位置を特定できない場合に送信されます。
Device Location Update	**[Major]**	この通知は、ジオフェンシングが有効になっているかどうかにかかわらず、デバイスの位置が 20 メートル以上変化すると送信されます。ジオフェンシングが有効になっていない場合、この通知はデバイスの場所が利用可能な場合にのみ送信されます。

Cisco vManage を使用してジオフェンシングアラームを監視できます。

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

   Cisco vManage リリース 20.6.1 以前：Cisco vManage メニューから**[Monitor]** > **[Alarms]**の順に選択します。

2. ジオフェンシングアラームがある場合、アラームはグラフの形式で表示され、その後に表が続きます。

指定した時間範囲（1 時間、3 時間、6 時間など）のデータをフィルタリングするか、[Custom] をクリックして時間範囲を定義できます。

3. アラームの詳細を表示するには、[...] をクリックし、 **[Alarm Details]** を選択して、デバイスに関する情報を表示します。

ジオフェンシングの構成例

ジオフェンシングとコントローラセルラーのエンドツーエンド構成

以下は、デバイスの自動検出を設定する際のジオフェンシングとコントローラセルラーの構成プロセスを示すエンドツーエンドのサンプル出力です。

```
system
  gps-location auto-detect-geofencing-location
  gps-location geo-fencing-enable
  gps-location geo-fencing
    geo-fencing-range 1000
    sms
      sms-enable
      mobile-number +112312345676
      !
      mobile-number +112312345677
      !
      mobile-number +112312345678
      !
      mobile-number +112312345679
      !
     !
    !
  system-ip             10.1.1.35
  site-id               273
  admin-tech-on-failure
  organization-name     LTE-Test
  vbond vbond-dummy.test.info port 12346
  !
  controller Cellular 0/2/0
  lte gps enable
  lte gps mode ms-based
  lte gps nmea
  !
```

以下は、緯度と経度の座標を手動で設定する場合のジオフェンシングとコントローラセルラーの構成プロセスを示すエンドツーエンドのサンプル出力です。

```
system
   gps-location latitude 37.317342
   gps-location longitude -122.218170
   gps-location geo-fencing-enable
   gps-location geo-fencing-config
    geo-fencing-range 1000
    sms
     sms-enable
     mobile-number +112312345676
     !
     mobile-number +112312345677
     !
     mobile-number +112312345678
```

```
!
mobile-number +112312345679
!
!
!
```

第 17 章

VRRP インターフェイス トラッキング

表 *190* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス の VRRP インターフェイス トラッキング	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、VRRP は、WAN インターフェイスまたはSIG トラッカーイベントに基づいてエッジをアクティブまたはスタンバイとして設定し、新しいアクティブな VRRP の TLOC プリファレンス値を増やして、Cisco IOS XE SD-WAN デバイス のトラフィックの対称性を確保できます。 このリリース以降、Cisco IOS XE SD-WAN デバイス での Cisco vManage の機能テンプレートおよび CLI テンプレートを使用して VRRP インターフェイス トラッキングを設定できます。

VRRP インターフェイス トラッキングに関する情報

Virtual Router Redundancy Protocol（VRRP）は、スイッチおよび他の IP エンドステーションに冗長ゲートウェイサービスを提供する LAN 側のプロトコルです。Cisco IOS XE SD-WAN デバイスでは、Cisco vManage テンプレートと CLI アドオンテンプレートを使用して、インターフェイスとサブインターフェイスに VRRP を設定できます。

詳細については、「VRRP の設定」を参照してください。

制約事項と制限

- VRRP は、サービス側 VPN でのみサポートされます。サブインターフェイスを使用している場合は、VPN 0 で VRRP 物理インターフェイスを設定します。
- VRRP トラッキングは、物理アップリンク インターフェイスまたは論理トンネルインターフェイス（IPSEC または GRE、またはその両方）でイネーブルになります。
- VRRP トラッキング機能は、オブジェクトとして IP プレフィックスをサポートしていません。
- 複数の VRRP グループまたは VPN で同じトラッカーを使用できます。
- 同じトラックオブジェクトを使用して複数のインターフェイスを追跡することはできません。
- リストトラックオブジェクトの下に最大 16 のトラックオブジェクトをグループ化できます。

VRRP トラッキングの使用例

VRRP の状態は、トンネルリンクのステータスに基づいて決定されます。トンネルまたはインターフェイスがプライマリ VRRP でダウンしている場合、トラフィックはセカンダリ VRRP に送信されます。LAN セグメントのセカンダリ VRRP ルータは、サービス側のトラフィックにゲートウェイを提供するプライマリ VRRP になります。

Zscaler トンネルの使用例 1：プライマリ VRRP、単一のインターネットプロバイダー

プライマリおよびセカンダリの Zscaler トンネルは、単一のインターネットプロバイダーを介してプライマリ VRRP に接続されます。プライマリおよびセカンダリ VRRP ルータは、TLOC 拡張を使用して接続されます。このシナリオでは、プライマリ VRRP でプライマリトンネルとセカンダリトンネルがダウンすると、VRRP 状態遷移が発生します。トラッキングオブジェクトがダウンし、VRRP 状態遷移がトリガーされると、既定のプライオリティ値がデクリメントされます。非対称ルーティングを回避するために、VRRP は OMP を介してこの変更をオーバーレイに通知します。

Zscaler トンネルの使用例 2：TLOC 拡張の VRRP ルータ、デュアル インターネット プロバイダー

プライマリおよびセカンダリ VRRP ルータは、TLOC 拡張高可用性モードで設定されます。プライマリおよびセカンダリの Zscaler トンネルは、デュアル インターネット プロバイダーを使用して、それぞれプライマリおよびセカンダリ VRRP ルータに直接接続されます。このシナリオでも、プライマリ トンネルおよびセカンダリ トンネルがプライマリ VRRP でダウンすると、VRRP 状態遷移が発生します。トラッキング オブジェクトがダウンし、VRRP 状態遷移がトリガーされると、既定のプライオリティ値がデクリメントされます。VRRP は OMP を介してこの変更をオーバーレイに通知します。

TLOC プリファレンス

トランスポート ロケータ（TLOC）により、OMP ルートは物理的な場所に接続されます。TLOC は、物理ネットワークのルーティング テーブル内のエントリを使用して直接到達可能であるか、NAT デバイス越えのプレフィックスによって表されます。

Cisco IOS XE SD-WAN デバイスでは、設定値に基づいて、TLOC 変更増加プリファレンス値が増加します。アクティブ ノードとバックアップ ノードの両方で、TLOC 変更増加プリファレンス値を設定できます。

VRRP トラッキングを設定するためのワークフロー

1. オブジェクト トラッカーを設定します。詳細については、オブジェクト トラッカーの設定（723 ページ）を参照してください。
2. VPN インターフェイス テンプレートの VRRP を設定し、オブジェクト トラッカーをテンプレートと関連付けます。詳細については、VPN インターフェイス テンプレートと関連するインターフェイス オブジェクト トラッカーの VRRP の設定（725 ページ）を参照してください。

オブジェクト トラッカーの設定

オブジェクト トラッカーを設定するには、[Cisco System] テンプレートを使用します。

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. デバイスの [Cisco System] テンプレートに移動します。

（注） [System]テンプレートを作成するには、「システムテンプレートの作成」を参照してください

4. [Tracker] をクリックし、[New Object Tracker] を選択して、トラッカーパラメータを設定します。

表 *191* : トラッカーパラメータ

フィールド	説明
[Tracker Type]	[Interface] または [SIG] を選択して、オブジェクトトラッカーを設定します。
オブジェクト ID	オブジェクト ID 番号を入力します。
インターフェイス（Interface）	グローバルまたはデバイス固有のトラッカーインターフェイス名を選択します。

5. [Add] をクリックします。
6. オプションで、トラッカーグループを作成するには、[Tracker] を選択し、**[Tracker Groups]** > **[New Object Tracker Groups]** をクリックして、トラッカーパラメータを設定します。

（注） トラックグループを作成するために 2 つのトラッカーを作成したことを確認してください。

表 *192* : オブジェクト トラッカー グループ パラメータ

フィールド	説明
[Group Tracker ID]	トラッカーグループの名前を入力します。
[Tracker ID]	グループ化するオブジェクトトラッカーの名前を入力します。
基準	[AND] または [OR] を明示的に選択します。 [OR] は、トラッカーグループの関連付けられたトラッカーのいずれかがルートがアクティブであると報告した場合に、トランスポート インターフェイスのステータスがアクティブとして報告されることを保証します。 [AND] 操作を選択した場合、トラッカーグループの関連付けられた両方のトラッカーがルートがアクティブであると報告した場合、トランスポート インターフェイスのステータスはアクティブであると報告されます。

（注） テンプレートを保存する前に、すべての必須フィールドに情報を入力してください。

7. [Add] をクリックします。
8. [Save] をクリックします。

VPN インターフェイス テンプレートと関連するインターフェイス オブジェクト トラッカーの VRRP の設定

Cisco VPN テンプレートの VRRP を設定するには、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. [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. デバイスの [Cisco VPN Interface Ethernet] テンプレートに移動します。

（注） 新しい **Cisco VPN インターフェイス イーサネット** テンプレートの作成については、「VPN イーサネット インターフェイスの設定」を参照してください。

4. [VRRP] をクリックし、[IPv4] を選択します。
5. [New VRRP] をクリックして新しい VRRP を作成するか、既存の VRRP を編集して次のパラメータを設定します。

パラメータ名	説明
TLOC Preference Change	（オプション）[On] または [Off] を選択して、TLOC プリファレンスを変更できるかどうかを設定します。
TLOC Preference Change Value	（オプション）TLOC プリファレンスの変更を入力します。範囲は 1 ～ 4294967295 です。

6. [Add Tracking Object] リンクをクリックし、表示される [Tracking Object] ダイアログボックスで [Add Tracking Object] をクリックします。

7. [Tracker ID] フィールドに、インターフェイス オブジェクト ID またはオブジェクト グループ トラッカー ID を入力します。
8. [Action] ドロップダウンリストから [Decrement] を選択し、[Decrement Value] として 1 を入力します。Cisco vEdge デバイスでは 1 のデクリメント値がサポートされています。

   または

   [Shutdown] を選択します。
9. [Add] をクリックします。
10. [Add] をクリックして、VRRP の詳細を保存します。
11. [Save] をクリックします。

CLI テンプレートを使用した VRRP トラッキングの設定

CLI アドオン機能テンプレートおよび CLI デバイステンプレートを使用して、VRRP トラッキングを設定できます。詳細については、「CLI Templates」を参照してください。

CLI を使用した VRRP オブジェクトトラッキング

CLI を使用したインターフェイス オブジェクト トラッキング

Cisco vManage デバイス CLI テンプレートを使用してインターフェイスをトラックリストに追加するには、次の設定を使用します。

```
Device(config)# track <object-id1> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track < object-id2> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit
Device(config)# interface GigabitEthernet2


Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ipv4 address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)# exit
```

SIG コンテナトラッキング

次の例は、Cisco vManage デバイス CLI テンプレートを使用して、SIG コンテナの追跡リストと追跡を設定する方法を示しています。

（注） Cisco IOS XE リリース 17.7.1a SIG オブジェクトトラッキングでは、サービス名の変数として *global* のみを設定できます。

CLI を使用した SIG オブジェクトトラッキング

```
Device(config)# track <object-id1> service global


Device(config-tracker)# exit
Device(config)# track <object-id2> service global
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit

Device(config)# interface GigabitEthernet2

Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ip address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)#exit
```

CLI を使用した VRRP オブジェクトトラッキングの設定例

CLI を使用したインターフェイス オブジェクト トラッキング

```
config-transaction
  track 100 interface Tunnel123 line-protocol
   exit
 track 200 interface GigabitEthernet5 line-protocol
  exit
track 400 list boolean and
  object 100
  object 200
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 400 decrement 10
```

```
  tloc-change increase-preference 333
  exit
```

SIG オブジェクトトラッキングの設定例

CLI を使用した SIG オブジェクトトラッキング

```
config-transaction
  track 1 service global
  exit
  exit
  track 2 service global
track 3 list boolean and
  object 1
  object 2
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 3 decrement 10
  tloc-change increase-preference 333
  exit
```

VRRP 設定のモニタリング

VRRP 設定に関する情報を表示するには、次の手順を実行します。

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、[VRRP Information] を選択します。

（注） VRRP 設定のステータスは [Track State] で表示できます。

VRRP トラッキングの確認

Device# **show vrrp**

次に、**show vrrp** コマンドの出力例を示します。

```
GigabitEthernet2 - Group 1 - Address-Family IPv4
  State is MASTER
  State duration 37 mins 52.978 secs
  Virtual IP address is 10.10.1.10
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 100
  State change reason is VRRP_TRACK_UP
  Tloc preference configured, value 333
    Track object 400 state UP decrement 10
  Master Router is 10.10.1.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 607 msec)
  Master Down interval is unknown
  FLAGS: 1/1
```

Device# **show track brief**

次に、**show track brief** コマンドの出力例を示します。

```
Track Type        Instance                  Parameter        State Last Change
100   interface   Tunnel123                 line-protocol    Up    00:12:48
200   interface   GigabitEthernet5          line-protocol    Up    00:49:57
400   list                                  boolean          Up    00:12:47
```

Device# **show track list**

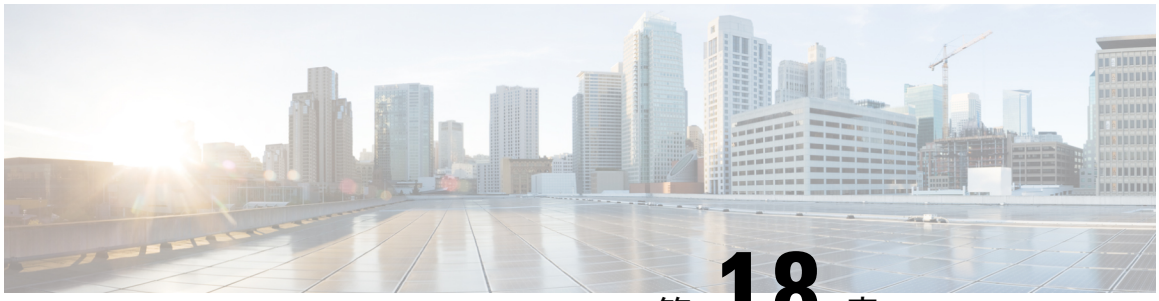
次に、**show track list** コマンドの出力例を示します。

```
Track 400
  List boolean and
  Boolean AND is Up
    6 changes, last change 00:12:58
    object 100 Up
    object 200 Up
  Tracked by:
    VRRPv3 GigabitEthernet2 IPv4 group 1
```

Device# **show track list brief**

次に、**show track brief** コマンドの出力例を示します。

```
Track Type        Instance                  Parameter        State Last Change
400   list                                  boolean          Up    00:13:02
```



第 18 章

VDSL および G.SHDSL の設定

この章では、SD-WAN モードでの超高データレート DSL（VDSL）および G. 対称高ビットレート DSL（G.SHDSL）の設定に関する使用情報とガイドラインを提供します。

VDSL の設定

次の表は、SD-WAN モードでサポートされているサービス統合型ルータ ネットワーク インターフェイス モジュール（ISR NIM）の非対称 DSL（ADSL2/2+）および VDSL を構成するための使用情報とガイドラインを示しています。VDSL2 および ADSL2/2+ は、リモートサイトに信頼性の高い WAN 接続を提供します。

関連情報については、「VDSL Commands」を参照してください。

機能	コマンド	ガイドライン
操作モードの設定	Device# **configure terminal** Device(config)# **controller VDSL** *slot/subslot/port* Device(config)# **operating mode auto**	動作モード auto adsl1（adsl2+/または vdsl2）から動作モード auto ads2+（adsl1 または vdsl2）に切り替えるには、最初に動作モード auto に切り替えます。 動作モードを変更する前に、line-mode が line-mode single-wire line 0 に変更されていることを確認してください。
回線で DSL を有効にする	Device(config)# **line-mode single-wire line***line-number*	このコマンドは、DSL NIM-VAB-A でのみサポートされます。

機能	コマンド	ガイドライン
ボンディングを有効にする	Device(config)# **line-mode bonding**	このコマンドは、DSL NIM-VAB-A でのみサポートされます。
デバイスにファームウェアをロードする	Device# **configure terminal** Device(config)# **controller VDSL** *slot/subslot/port* Device(config-controller)# **firmware phy filename** *filename*	Cisco SD-WAN CLI テンプレートは、ファイルの場所の指定をサポートしていません。場所に応じて、ファイル名の前に flash: または bootflash: を付けます。
SRA を有効または無効にする	Device(config-controller)# **sra**	Cisco SD-WAN CLI テンプレートは、sra *line number* コマンドをサポートしていません。ラインモードボンディングでは、sra は両方の回線で sra を有効にし、no sra は両方の回線で sra を無効にします。
ビットスワップを有効または無効にする	Device(config-controller)# **bitswap**	Cisco SD-WAN CLI テンプレートは、bitswap *line number* コマンドをサポートしていません。ラインモードボンディングでは、bitswap は両方の回線でビットスワップを有効にし、no bitswap は両方の回線でビットスワップを無効にします。
モデム機能を有効にする	Device(config-controller)# **modem***keyword*	–
コントローラの説明を表示する	Device(config-controller)# **description** *string*	–
デュアルエンド回線テストを有効にする	Device(config-controller)# **diagnostics DELT**	–
トレーニングログが保存されているファイルを変更する	Device(config-controller)# **training log filename flash:** *filename*	Cisco SD-WAN CLI テンプレートは、ファイルの場所の指定をサポートしていません。ファイルの保存場所に応じて、ファイル名の前に flash: または bootflash: を付加します。

機能	コマンド	ガイドライン
同期モードを有効にする	Device(config-controller)# **sync mode** *mode*	ある同期モードから別の同期モードに切り替えるには、既存の同期モードを削除してから、新しい同期モードを設定します。
同期間隔を有効にする	Device(config-controller)# **sync interval** *seconds*	–

コマンドの例

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config)# operating mode auto


Device# config-transaction
Device(config)# line-mode single-wire line 1


Device# config-transaction
Device(config)# line-mode bonding


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename flash:IDC_1.7.2.6_DFE_FW_BETA_120111A.pkg



Device# config-transaction
Device(config-controller)# sra


Device# config-transaction
Device(config-controller)# bitswap


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# modem customUKAnnexM


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# description to ISP 1


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# diagnostics DELT


Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# training log filename bootflash:VDSLLOG.log


Device# config-transaction
Device(config)# controller VDSL 0/0/0
```

```
Device(config-controller)# sync mode ansi previous


Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

設定例

```
Device(config)# show controllers vdSL 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xA39A
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:     FGL2149956Y C1117-4P 16.7.20180
Serial Number Far:
Modem Version Near:     16.7.20180709:09395
Modem Version Far:      0xa39a

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.993.2 (VDSL2) Profile 17a

TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039t.d26d

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     enabled                 enabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          1                       3
Line Attenuation:        18.4 dB                  0.0 dB
Signal Attenuation:       0.0 dB                  0.0 dB
Noise Margin:             5.2 dB                 6.0 dB
Attainable Rate:        46022 kbits/s           18866 kbits/s
Actual Power:           14.5 dBm                10.4 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   13.9    32.7    50.1    N/A     25.6    37.7    42.3
Signal Attenuation(dB): 13.5    32.4    N/A     N/A     25.0    36.9    41.9
Noise Margin(dB):       5.3     5.1     N/A     N/A     6.0     6.0     5.9
Total FECC:             446                      0
Total ES:               3                        0
Total SES:              0                        0
Total LOSS:             0                        0
```

```
Total UAS:              50                      50
Total LPRS:             0                       0
Total LOFS:             0                       0
Total LOLS:             0                       0

                   DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):             NA           47610            NA             18859
SRA Previous Speed:       NA               0            NA                 0
Previous Speed:           NA               0            NA                 0
Reed-Solomon EC:          NA             446            NA                 0
CRC Errors:               NA              51            NA                 0
Header Errors:            NA            3935            NA                 0
Interleave (ms):          NA            1.00            NA              1.00
Actual INP:               NA            0.00            NA              0.00

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

G.SHDSL の設定

概要

G.SHDSL は、デバイスが 1 組の銅線を介して高速対称データストリームを送受信できるようにする国際標準です。このセクションでは、Cisco G.SHDSL EFM/ATM NIM に関する情報を提供し、SD-WAN モードで G.SHDSL を設定するためのガイドラインを提供します。

関連情報については、『Configuring Cisco G.SHDSL HWICs in Cisco Access Routers』および「VDSL Commands」を参照してください。

Cisco G.SHDSL EFM/ATM NIM

Cisco G.SHDSL EFM/ATM NIM は、Cisco 4000 シリーズ サービス統合型ルータをセントラルオフィスのデジタル加入者線アクセスマルチプレクサ（DSLAM）に接続し、最大 4 つの DSL ペアをサポートします。この DSL ペアは、グループ分けされており、Cisco IOS CLI 上で dsl-group コマンドを使用して設定します。mode コマンドを使用して、モード（ATM または EFM）を選択します。

NIM は、次の設定をサポートします。

- 最大 4 つの DSL グループを設定できます。
- 自動モードは 1 つの DSL グループにのみ設定できます。たとえば、DSL group 0 です。
- ATM モードでは、2 線、4 線（標準または拡張）、または m ペアを使用するように回線を設定できます。
- EFM モードでは、2 線非結合モードのいずれかの回線、または結合モードの複数の回線を使用して DSL グループを設定できます。
- モード（ATM または EFM）に応じて、対応するインターフェイス（ATM または EFM）が自動的に作成されます。

Cisco G.SHDSL 設定ガイドライン

次の表に、CPE または CO モードで Cisco G.SHDSL EFM/ATM を設定するときに適用される使用情報とガイドラインを示します。

機能	コマンド	ガイドライン
dsl-group auto コマンドを使用してデバイスを設定する	Device(config-controller)# **dsl-group auto**	dsl-group auto コマンドでデバイスを設定するときは、顧客宅内機器（CPE）モードを使用します。このコマンドをセントラルオフィス（CO）モードで使用すると、設定は有効になりません。
リンクを追加または削除する	—	efm-grp コマンドはサポートされません。dsl-group へのリンクを追加または削除するには、dsl-group を削除してから、新しい dsl-group を作成します。
デバイスにファームウェアをロードする	Device(config-controller)# **firmware phy filename** *location*	firmware phy コマンドを使用する場合、ファイル名の場所のオプションはサポートされていません。場所に応じて、ファイル名の前に flash: または bootflash: を付けます。
付録を作成または削除する	Device(config-controller-dsl-group)# **no shdsl annex** Device(config-controller-dsl-group)# **no shdsl rate** *rate*	付録を作成または削除するときに Cisco IOS と Cisco SD-WAN の設定が同期しなくなるのを避けるには、同じトランザクションでレートを作成または削除します。
SHDSL で拡張モードを使用できるようにする	(config-controller-dsl-group)# **shdsl 4-wire mode enhanced**	2 ペアのデジタル加入者線（DSL）グループ内で拡張モードを使用する SHDSL を有効にするには、設定コントローラ DSL グループモードで shdsl 4-wire mode enhanced コマンドを使用します。

機能	コマンド	ガイドライン
CRC エラーを無視する	(config-controller-dsl-group)# **ignore***seconds*	CRC エラーを無視するようにデバイスを設定するには、ignore コマンドを使用します。*timeout* を 0 ～ 60 の値に置き換えます。これは、デバイスがアクションを終了する前に、解決されない CRC エラーをデバイスが無視する秒数を示します。
DSL グループをシャットダウンする	(config-controller-dsl-group)# **shutdown**	DSL グループをシャットダウンするには、shutdown コマンドを使用します。

例

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group auto
```

```
Device# config-transaction
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename
bootflash:IDC_1.1.1.0_DFE_1.1-1.8.1__001.pkg
```

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# dsl-group 0 pairs 0
Device(config-controller-dsl-group)# no shdsl annex
Device(config-controller-dsl-group)# no shdsl rate 5696
```

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
(config-controller-dsl-group)# shdsl 4-wire mode enhanced
```

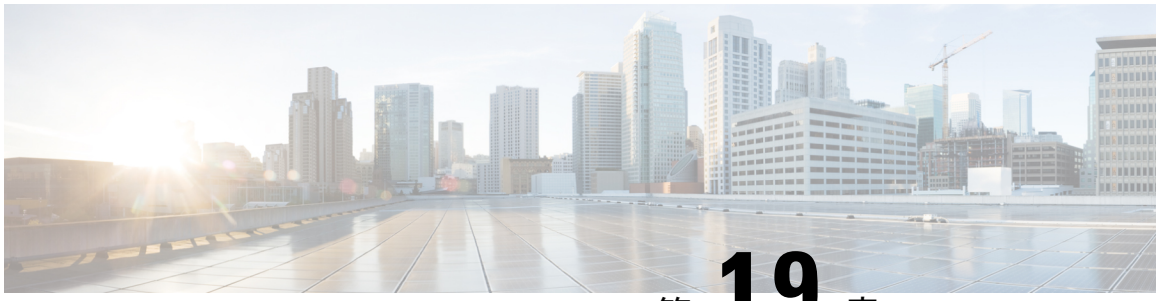
```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# ignore 30
```

```
Device# config-transaction
Device(config)# controller SHDSL 0/0/0
Device(config-controller)# termination cpe
Device(config-controller)# dsl-group 0 pairs 0
config-controller-dsl-group)# shutdown
```

設定例

```
Device# sh controllers shDSL 0/1/0
Controller SHDSL 0/1/0 is UP
  Hardware is NIM-SHDSL-EA, on slot 0,bay 0
  Capabilities: EFM: 2-wire, EFM-Bond, Annex A, B, F & G
                ATM: 2-wire, Mpair, Annex A, B, F & G
  CPE termination
  cdb=0x7F7EB723D8A8
  Vendor: Intel, Chipset: SOCRATES-4e
  PHY Source: System
  IDC Firmware version: 0.0.0.0
  DFE Firmware version:
  Group 0 info:
        Type: EFM Auto status: Down
         Ethernet Interface: Ethernet0/1/0, hwidb: 0x7F7EB723B648
         ATM Interface: ATM0/1/0, hwidb: 0x7F7EB724CE08
        Configured/active num links: 4/0, bit map: 0xF/0x0
        Line termination: CPE, Annex: auto
        PMMS disabled,Line coding: AUTO-TCPAM
        Configured/actual rate: AUTO/0 kbps
        Dying Gasp: Present
        SHDSL wire-pair (0) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
        SHDSL wire-pair (1) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
```

```
        SHDSL wire-pair (2) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
        SHDSL wire-pair (3) is in DSL DOWN state
                LOSWS Defect alarm: none
                SNR Margin alarm: none
                Loop Attenuation alarm: none
                Termination: CPE, Line mode: EFM Auto, Annex: auto
                Line coding: AUTO-TCPAM
                Configured/actual rate: AUTO/0 kbps
                Modem status: DOWN_NOT_READY,Condition: NO_COND_
        DSL Stats:
                Power Back Off: 0dB
                LoopAttn: 0dB, SnrMargin: 0dB
                Current 15 minute statistics (Time elapased 1 seconds)
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 15 minute statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Current 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
                Previous 24 hr statistics
                        ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
        EFM Stats:
                EFM-TC Tx: data frames: 0
                EFM-TC Rx: data frames: 0
Group 1 is not configured
Group 2 is not configured
Group 3 is not configured
```



第 19 章

ダイナミック オンデマンド トンネル

表 *193 :* 機能の履歴

機能名	リリース情報	説明
ダイナミック オンデマンド トンネル	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、エッジデバイス間のトンネルに非アクティブ状態を設定できるため、デバイスのパフォーマンスの要求を減らし、ネットワークトラフィックを削減できます。

Cisco SD-WAN は、任意の 2 つの Cisco SD-WAN スポークデバイス間の動的オンデマンドトンネルをサポートします。これらのトンネルは、2 つのデバイス間にトラフィックがある場合にのみ設定されるようにトリガーされます。デバイス間のトラフィックのフローが停止すると、ユーザーが設定可能な非アクティブタイマーが開始され、設定された時間が経過すると、デバイス間のトンネルが削除されます。その後、2 つのデバイス間のオンデマンドリンクは、非アクティブであると見なされます。この非アクティブ状態では、ネットワーク帯域幅を使用せず、デバイスのパフォーマンスに影響しません。

ルートのバックアップとトンネルの再アクティブ化

2 つのスポークデバイスピアがオンデマンドトンネルを使用できるようにするには、ハブを経由する代替ルート（バックアップルート）が必要です。バックアップルートを使用すると、どちらのスポークデバイスも2つのスポーク間のトラフィックフローを再開できます。これにより、トンネルが再アクティブ化され、ピアからピアへのトラフィックが直接処理されます。

利点

オンデマンドトンネルには、次の利点があります。

- 特に、フルメッシュネットワークで動作するあまり強力ではないプラットフォームのパフォーマンスが向上。

- スポーク間でオンデマンドトンネルが使用されている場合にハブアンドスポーク展開の遅延が改善。
- 非アクティブ状態のトンネルは Bidirectional Forwarding Detection（BFD）プローブを必要としないため、ネットワークで使用される帯域幅が削減され、ネットワークで生成される BFD トラフィックが少ない。
- CPU とメモリの使用量を最適化しながら、スポーク間の直接トンネル。

- オンデマンド トンネル メカニズムの詳細 （742 ページ）
- 注意事項と制限事項 （744 ページ）
- オンデマンドトンネルの設定 （745 ページ）

オンデマンド トンネル メカニズムの詳細

ダイナミックトンネルを使用するようにサイトを設定すると、オンデマンド機能が有効になります。この動作モードでは、Cisco SD-WAN エッジルータは、オンデマンド機能も有効になっている他のサイトへの直接トンネルを起動しません。

Cisco SD-WAN はバックアップ転送ノードとして機能する 1 つ以上のエッジルータ（通常は中央に配置されたルータ）を選択し、2 つのノード間のトラフィックにセカンダリパスを提供します。バックアップノードはオンデマンドで有効になっていません。すべてのオンデマンドサイトは、バックアップノードと静的トンネルを形成します。バックアップノードは、オンデマンドが有効になっている2つのノード間のトラフィックに静的バックアップルートを提供します。

2 つのノード間のトラフィックの最初のパケットは、静的バックアップパスを介してルーティングされ、サイト間でオンデマンドトンネルがアクティブになるようにトリガーします。バックアップパスは、直接パスがアクティブになるまでトラフィックを転送し続けます。

すべてのオンデマンドサイトは、他のすべてのオンデマンドリモートサイトの TLOC とプレフィックスを学習します。プレフィックスには、Cisco vSmart コントローラ制御ポリシーによって設定されたバックアップパスもあります。したがって、コントロールプレーンでは、オンデマンド トンネル ネットワークは、バックアップパスを含むフルメッシュ トンネル ネットワークと同じ状態になります。コントロールプレーンはデータプレーンにダウンロードし、バックアップパスと、2 つのサイト間の潜在的な直接パスを表すリモート TLOC を使用してルーティングしますが、リモート TLOC への直接パストンネルは設定しません。

オンデマンドトンネルのいずれかの端からのトラフィックは、トンネルの設定をトリガーします。これにより、オンデマンドトンネルがネットワークアドレス変換（NAT）トラバーサルに対応することができます。

オンデマンドトンネル機能により、オンデマンドブランチサイトには2つの状態が導入されます。

- **非アクティブ**：リモートサイトとのオンデマンドトンネルは設定されていません。リモートサイトとの間でアクティブなトラフィックはありません。リモートサイトの TLOC は非アクティブです。Bidirectional Forwarding Detection（BFD）は設定されず、プレフィックス

には非アクティブパスがインストールされ、バックアップパスがトラフィックを転送するパスとして設定されます。非アクティブパスはフローを検出し、直接のサイト間トンネルの設定をトリガーします。

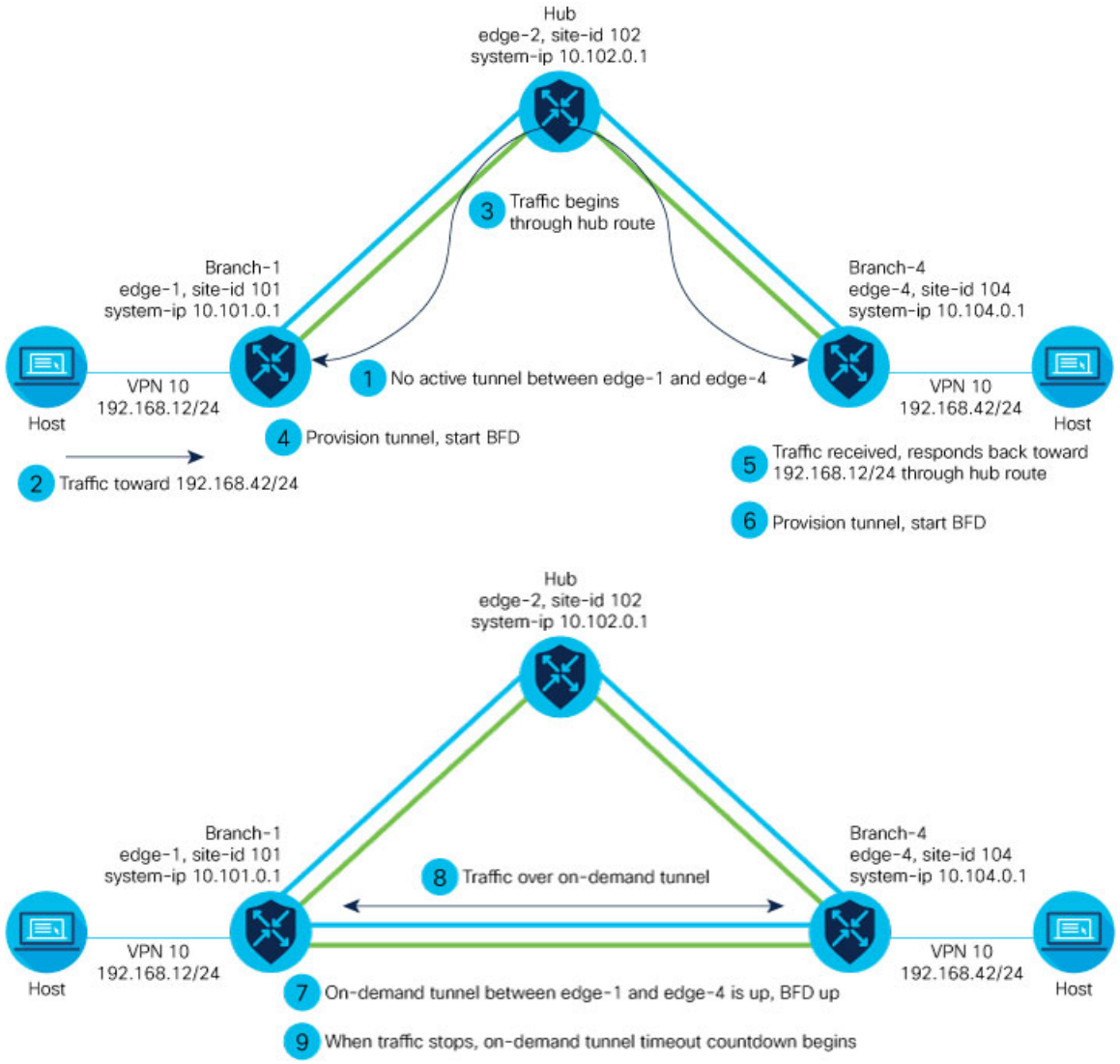
- **アクティブ**：オンデマンドの直接のサイト間トンネルがリモートサイトに設定されています。リモートサイトとの間にはアクティブなトラフィックがあります。この状態は一般的なトンネルの場合と同じであり、リモート TLOC に BFD が設定され、プレフィックスには直接パストンネルがインストールされます。この状態で、トンネルアクティビティが追跡されます。「アイドル時間」の期間（デフォルトは10分）にトラフィックがない場合、直接のサイト間トンネルは削除され、状態は非アクティブに変わります。

図の手順

次の図は、オンデマンドトンネルが設定された2つのエッジルータ間で行われる次の手順を示しています。

1. 2つのエッジルータ間にアクティブなトンネルはありません。edge-1 と edge-4 は非アクティブ状態です。
2. edge-1 の背後にあるホストは、edge-4 の背後にあるホストへのトラフィックを開始します。
3. edge-1 は、ハブまたはバックアップノードを使用してバックアップパス経由でトラフィックを edge-4 に転送します。
4. edge-1 はオンデマンドトンネルをプロビジョニングし、Bidirectional Forwarding Detection（BFD）を開始します。edge-4 は、edge-1 でアクティブ状態になります。
5. edge-4 は、edge-1 の背後にあるホストへのリターントラフィックを受信すると、ハブまたはバックアップノードを使用してバックアップパス経由でトラフィックを edge-1 に転送します。
6. edge-4 はオンデマンドトンネルをプロビジョニングし、BFD を開始します。edge-1 は、edge-4 でアクティブ状態になります。
7. この時点で、edge-1 と edge-4 の間のオンデマンドトンネルが稼働していて、BFD が稼働しています。
8. 2 つのエッジデバイス間のトラフィックは、オンデマンドトンネルを経由する直接ルートを使用します。
9. edge-1 と edge-4 の両方が、オンデマンドトンネルのトラフィックアクティビティを双方向に追跡します。

   アイドルタイムアウト期間中にトラフィックがない場合、オンデマンドトンネルは削除され、edge-1 および edge-4 デバイスは非アクティブ状態に戻ります。



注意事項と制限事項

- オンデマンドトンネルの Performance Routing（PfR）統計の収集は、オンデマンドトンネルがセットアップされるたびに新たに開始されます。アイドルタイムアウト後、削除されたオンデマンドトンネルの PFR 統計はキャッシュされません。
- トラフィックがバックアップパスから直接オンデマンドトンネルに移動すると、Out Of Order（OOO）パケットが発生することがあります。パケットは、受信時に Cisco SD-WAN ルータによって転送されます。
- 単方向のフローは、オンデマンドのトンネルセットアップをトリガーしません。バックアップパスを引き続き使用します。

- マルチキャストトラフィックは、オンデマンドのトンネルセットアップをトリガーしません。バックアップパスを引き続き使用します。
- オンデマンドサイト TLOC に **set tloc-list** アクションを適用するデータポリシーは設定しないでください。設定されている場合、トラフィックはドロップされます。
- ペアワイズキー（PWK）IPSEc機能が有効になっている場合、オンデマンドトンネルはサポートされません。
- **on-demand enable** または **no on-demand enable** が実行されると、システム内のすべての TLOC がリセット（無効化および有効化）されます。
- エッジデバイスがオンデマンドトンネルをプロビジョニングすると、リモートサイトのすべての TLOC にプロビジョニングされます。
- マルチホームサイトをオンデマンドモードにするには、サイトのすべてのシステムで on-demand enable を設定する必要があります。
- いずれかの方向のオンデマンドトンネルにサービスまたはユーザートラフィックがある場合、オンデマンドトンネルを使用するすべてのエッジデバイスはアクティブなままです。
- オンデマンドトンネルは、両方のサイトがオンデマンドモードで有効になっている場合にのみ、2 つのサイト間で有効にできます。
- リモートサイトの背後にあるホストへの最初のパケットは、そのリモートサイトへのオンデマンドトンネルセットアップをトリガーします。そのホストからのリターントラフィックは、反対方向のトンネルセットアップをトリガーします。
- オンデマンドリモートサイトからのすべてのプレフィックスにも、バックアップパスが設定されている必要があります。設定されていない場合、サイトはオンデマンドトンネルをセットアップできません。バックアップパスは静的トンネルであり、常に稼働している必要があります。
- オンデマンドトンネルのセットアップまたは削除は、Cisco vSmart コントローラによるオーバーレイルート（OMP）アップデート、またはサービス/LAN 側のルートアップデート（例：OSPF または BGP）には影響しません。
- ローカルサイトまたはリモートサイトのいずれかがオンデマンドモードでない場合、サイト間には静的トンネルがセットアップされます。

オンデマンドトンネルの設定

オンデマンドトンネルの前提条件

オンデマンドトンネルを使用するには、いくつかの前提条件があります。

- 前提条件：Cisco vSmart コントローラ 集中管理ポリシー （746 ページ）
- 前提条件：OMP 設定 （747 ページ）

- 前提条件：ハブデバイス （748 ページ）
- 前提条件：スポークデバイス （748 ページ）

前提条件：Cisco vSmart コントローラ 集中管理ポリシー

1. Cisco vSmart コントローラ 集中管理ポリシーには、**tloc-action backup** アクションを含める必要があります。

   説明：これにより、すべてのスポークデバイス間の通信のためにハブを介したバックアップパスが確保されます。

2. Cisco vSmart コントローラ 集中管理ポリシーは、すべてのスポーク プレフィックス ルートを受け入れる必要があります。

3. Cisco vSmart コントローラ 集中管理ポリシーは、すべてのスポークの TLOC を受け入れる必要があります。

   Cisco vSmart コントローラの**集中管理ポリシー**の設定については、『Cisco SD-WAN Configuration Guides』のポリシー設定ガイドを参照してください。

CLI の例（集中管理ポリシーアドレッシングの前提条件）

```
viptela-policy:policy
 control-policy Dynamic-Tunnel-Control-Policy
    sequence 100
     match route
      site-list Branches
     !
     action accept
      set
       tloc-action backup
       tloc-list Hub-TLOCs
      !
     !
     sequence 200
      match tloc
     !
     action accept
    !
  default-action accept
 !
 lists
  site-list Branches
   site-id 200
   site-id 300
  !
  tloc-list Hub-TLOCs
   tloc 10.0.0.1 color mpls encap ipsec
   tloc 10.0.0.1 color public-internet encap ipsec
!
!
apply-policy
 site-list Branches
  control-policy Dynamic-Tunnel-Control-Policy out
 !
!
```

Cisco vManage の手順

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Centralized Policy] を選択します。
3. [Add Topology] をクリックし、[Custom Control (Route & TLOC)] を選択します。
4. [Match Conditions] の [Site] で、1 つまたは複数のサイトリストを選択し、[Accept] をクリックします。
5. [Actions] の [TLOC Action] で、[Backup] アクションを選択します。
6. [TLOC List] から、既存の TLOC リストを選択するか、新しいリストを作成します。

前提条件：OMP 設定

1. Cisco vSmart コントローラ の send-path-limit は、デフォルトの 4 より大きい必要があります。推奨：16

   説明：オンデマンドトンネルが有効になっている場合、スポークはハブ経由のバックアップパスを使用するため、より高いパス制限が必要です。これに対応するには、使用可能なすべてのパスをアドバタイズするように Cisco vSmart コントローラ の send-path-limit を増やします。

   vSmart の **send-path-limit** の設定については、Cisco SD-WAN の『Configuration Guides』ページのルーティング設定ガイドを参照してください。

CLI の例

```
omp
 no shutdown
 send-path-limit 16
 graceful-restart
```

Cisco vManage の手順

1. Cisco vManage のメニューから、[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. デバイスを選択し、[Cisco OMP] をクリックします。
5. [Basic Configuration] で、[Number of Paths Advertised per Prefix] を 16（推奨）に設定します。

前提条件：ハブデバイス

1. ハブデバイスで、トラフィック エンジニアリング サービス（サービス TE）を有効にする必要があります。

   説明：これにより、スポークデバイスの Cisco SD-WAN オーバーレイ管理プロトコル（OMP）が、2 つのスポークデバイス間の中間パスとして追加されるハブを経由するバックアップパスを受け入れるようになります。これがないと、ハブを経由するバックアップパスは無効と見なされ、スポークデバイスによって解決されません。

CLI の例（Cisco vEdge デバイス）

```
vpn 0
 service TE
 exit
```

CLI の例（Cisco IOS XE SD-WAN デバイス）

```
sdwan
 service TE vrf global
exit
```

Cisco vManage の手順

1. Cisco vManage で、[Configuration] > [Templates] を開きます。
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. プラットフォームを選択します。
5. [VPN] から [VPN] を選択します。
6. [Basic Configuration] で、[VPN] フィールドが 0 に設定されていることを確認します。
7. [Service] から、[New Service] をクリックし、[TE] を選択します。
8. [Add] をクリックしてから、[Update] をクリックします。サービスのテーブルに TE サービスが表示されます。
9. VPN-0 テンプレートをハブに適用します。

前提条件：スポークデバイス

1. スポークデバイスでは、ecmp-limit をデフォルトの 4 より大きくする必要があります。推奨：16

説明：オンデマンドトンネルが有効になっている場合、スポークデバイスはダイレクトパスとバックアップパスの両方を作成します。より多いパスのニーズに対応するため、ecmp-limit を増やします。

CLI の例

```
omp
 no shutdown
 ecmp-limit       16
```

（注） **show running-config omp** コマンドを使用して、現在の ecmp-limit を表示できます。

Cisco vManage の手順

1. Cisco vManage のメニューから、[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. デバイスを選択し、[Cisco OMP] をクリックします。
5. [Basic Configuration] で、[ECMP Limit] フィールドを 16（推奨）に設定します。

Cisco vManage を使用したオンデマンドトンネルの設定

（注）
- 「オンデマンドトンネルの前提条件」を参照してください。
- ハブデバイスでオンデマンドを有効にしないでください。

スポークデバイスで、すべての VPN-0 トランスポート インターフェイスのシステムレベルでオンデマンドを有効にします。マルチホームサイトの場合は、サイト内のすべてのシステムでオンデマンドを有効にします。

1. Cisco vManage のメニューから、[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. デバイスを選択します。
5. [Basic Information] から、[Cisco System] を選択します。
6. [詳細設定（Advanced）] をクリックします。
7. [On-demand Tunnel] を有効にします。
8. （オプション）[On-demand Tunnel Idle Timeout] 時間を設定します。デフォルトのアイドルタイムアウト値は 10 分です。範囲：1 ー 65535 分
9. システム機能テンプレートをスポークデバイスのデバイステンプレートにアタッチします。

CLI を使用したオンデマンドトンネルの設定

（注）
- オンデマンドトンネルの前提条件 （745 ページ）を参照してください。
- ハブデバイスでオンデマンドを有効にしないでください

1. スポークデバイスで、システムレベルでのオンデマンドトンネルを有効にします。マルチホームサイトの場合は、サイト内のすべてのシステムでオンデマンドを有効にします。

   デフォルトのアイドルタイムアウト値は 10 分です。範囲：1 ー 65535 分

例

```
system
     on-demand enable
     on-demand idle-timeout 10
```

Cisco vManage でオンデマンドトンネルの現在のステータスを表示

1. Cisco vManage のメニューから [Monitor] > [Devices] を選択します。

   Cisco vManage リリース 20.6.x 以前のリリース：Cisco vManage のメニューから [Monitor] > [Network] を選択します。
2. デバイスを選択します。
3. **[リアルタイム (Real Time)]** を選択します。

4. [Device Options] で、次のいずれかを選択します。
   - **On Demand Local**：指定したデバイスのオンデマンドトンネルのステータスを表示します。
   - **On Demand Remote**：指定したデバイスおよび接続されているすべてのデバイスのオンデマンドトンネルのステータスを表示します。

出力は、**show** [**sdwan**] **system on-demand** [**remote-system**] [**system-ip** *ip-address*] CLI コマンドを実行した場合と同等です。オンデマンドトンネルのステータスを表示します。

CiscovManageでオンデマンドトンネルのステータスの経時的なチャートを表示

1. Cisco vManage のメニューから [Monitor] > [Devices] を選択します。

   Cisco vManage リリース 20.6.x 以前のリリース：Cisco vManage のメニューから [Monitor] > [Network] を選択します。
2. デバイスを選択します。
3. [WAN] から、[Tunnel] を選択します。
4. [Chart Options] ドロップダウンリストから、[On-Demand Tunnel Status] を選択します。チャートには、トンネルのステータスが [ACTIVE] または [INACTIVE] として表示されます。[INACTIVE] は、オンデマンドトンネルが非アクティブモードであることを示します。

詳細については、「Cisco SD-WAN Configuration Guides」ページのモニタリングおよびメンテナンスガイドを参照してください。

第 20 章

サービス VPN の静的ルートのトラッキング

表 *194* : 機能の履歴

機能名	リリース情報	説明
サービス VPN の静的ルートトラッカー	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、サービス VPN の IPv4 静的ルートのエンドポイントトラッキングを設定できます。 エンドポイントトラッキングにより、静的ルートの場合、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、設定されたエンドポイントが到達可能かどうかを判断します。
Cisco IOS XE SD-WAN デバイス 用の TCP/UDP エンドポイントトラッカーおよびデュアルエンドポイントの静的ルートトラッカー	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、TCP/UDP 静的ルートのエンドポイントトラッカーを設定できます。この機能を使用して、サービス VPN の IPv4、TCP/UDP デュアルエンドポイントの静的ルートトラッカーグループを構成して、プローブの信頼性を強化することもできます。

静的ルートトラッキングに関する情報

サービス VPN の静的ルートトラッキングを使用すると、設定されたエンドポイントアドレスの可用性を追跡して、静的ルートをデバイスのルーティングテーブルに含めることができるかどうかを判断できます。これは、サイトがサービス VPN の静的ルートを使用して、オーバーレイ管理プロトコル（OMP）経由でそのルートをアドバタイズする場合に適用されます。静的ルートトラッカーは、設定されたエンドポイントに ICMP ping プローブを定期的に送信します。トラッカーが応答を受信しない場合、静的ルートはルーティングテーブルに含まれず、OMP にアドバタイズされません。代替ネクストホップアドレスまたはより高いアドミニストレーティブディスタンスを持つ静的ルートを設定して、バックアップパスを提供できます。このパスは OMP を介してアドバタイズされます。

（注） Cisco IOS XE リリース 17.7.1a から、TCP/UDP の個々のエンドポイントトラッカーを設定し、（2つのトラッカーを使用して）デュアルエンドポイントを持つトラッカーグループを設定し、トラッカーとトラッカーグループを静的ルートに関連付けることができます。デュアルエンドポイントは、ルートが利用できないために取り込まれる可能性のある検出漏れを回避するのに役立ちます。

サポートされるプラットフォーム

• Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
• Cisco ISR 1000 シリーズ サービス統合型ルータ
• Cisco ISR 4000 シリーズ サービス統合型ルータ
• Cisco CSR 1000 シリーズ クラウド サービス ルータ

IPv4 静的ルートトラッキングの制約事項

• ネクストホップアドレスごとに、スタティックルートごとにサポートされるエンドポイントトラッカーは 1 つだけです。
• IPv6 スタティックルートはサポートされていません。
• トラッカーを使用するスタティックルートを設定するには、次の手順を実行します。

1. トラッカーなしですでに設定されている場合は、既存のスタティックルートを削除します。スタティック ルート アドバタイズメントのこのステップ中に発生する可能性のある接続のダウンタイムに備えて計画します。
2. 削除されたスタティックルートと同じプレフィックスとネクストホップを使用して、トラッカーを使用する新しいスタティックルートを設定します。

- ルータごとの最大トラッカー制限に達した後に新しいトラッカーを追加するには、次の手順を実行します。
  1. 古いトラッカーを削除し、テンプレートをデバイスにアタッチします。
  2. 新しいトラッカーを追加し、デバイスをテンプレートに再度アタッチします。
- IP SLA UDP パケットレスポンダが有効になっている UDP トラッカーエンドポイントは、Cisco IOS XE SD-WAN デバイスでのみサポートされています。
- 同じエンドポイントトラッカーを異なる VPN のスタティックルートにリンクすることはできません。エンドポイントトラッカーは名前で識別され、単一の VPN 内の複数のスタティックルートに使用できます。

IPv4 静的ルートトラッキングを設定するためのワークフロー

1. システムテンプレートを使用してエンドポイントトラッカーを設定します。
2. VPN テンプレートを使用して静的ルートを構成します。
3. ネクストホップアドレスにトラッカーを適用します。

静的ルートトラッカーの作成

[System Template] を使用して、静的ルートトラッカーを作成します。

（注） 静的ルートトラッカーを作成する前に、既存の静的ルートを削除します（存在する場合）。削除された静的ルートと同じプレフィックスとネクストホップを使用して、新しい静的ルートトラッカーを設定します。

1. Cisco vManage のメニューから、**[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. デバイスの [Cisco System] テンプレートに移動します。

（注） システムテンプレートの作成については、「システムテンプレートの作成」を参照してください

4. [Tracker] をクリックします。[New Endpoint Tracker] をクリックしてトラッカーパラメータを設定します。

表 *195*：トラッカーパラメータ

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。
しきい値	構成されたエンドポイントがダウンしていることを宣言する前に、プローブが応答を返すまでの待機時間。範囲は 100 ～ 1000 ミリ秒です。デフォルトは 300 ミリ秒です。
インターバル	構成されたエンドポイントのステータスを判断するためのプローブ間の時間間隔。デフォルトは 60 秒（1 分）です。 範囲は 20 ～ 600 秒です。
Multiplier（乗数）	エンドポイントがダウンしていることを宣言する前にプローブを送信できる回数。指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
[Tracker Type]	ドロップダウンリストから [Global] を選択します。[Tracker Type field] ドロップダウンから、[Static Route] を選択します。 Cisco IOS XE リリース 17.7.1a から、Cisco IOS XE SD-WAN デバイスでデュアルエンドポイントを持つトラッカーグループを設定し、このトラッカーグループを静的ルートに関連付けることができます。
エンドポイント タイプ	エンドポイントタイプの IP アドレスを選択します。
End-Point Type: IP Address	静的ルートエンドポイントの IP アドレス。これは、ルータがプローブを送信してルートのステータスを判断するインターネット上の宛先です。

5. [Add] をクリックします。
6. [Save] をクリックします。
7. トラッカーグループを作成するには、**[Tracker Groups]** > **[New Endpoint Tracker Group]** をクリックし、トラッカーパラメータを設定します。

（注） トラッカーグループを作成するために2つのトラッカーを作成したことを確認してください。

表 *196*: トラッカー グループ パラメータ

フィールド	説明
Name	トラッカーグループの名前。
[Tracker Type]	ドロップダウンから [Global] を選択します。[Tracker Type field] ドロップダウンから、[Static Route] を選択します。 Cisco IOS XE リリース 17.7.1a から、Cisco IOS XE SD-WAN デバイス でデュアルエンドポイントを持つトラッカーグループを設定し、このトラッカーグループを静的ルートに関連付けることができます。
Tracker Elements	このフィールドは、トラッカータイプとして [Tracker-group] を選択した場合にのみ表示されます。既存のインターフェイストラッカー名（スペースで区切る）を追加します。このトラッカーをテンプレートに追加すると、トラッカーグループがこれらの個々のトラッカーに関連付けられ、そのトラッカーグループを静的ルートに関連付けることができます。
Tracker Boolean	ドロップダウンリストから [Global] を選択します。このフィールドは、[Tracker Type] として [tracker-group] を選択した場合にのみ表示されます。デフォルトでは、[OR] オプションが選択されています。[AND] または [OR] を選択します。 [OR] は、トラッカーグループの関連付けられたトラッカーのいずれかがルートがアクティブであると報告した場合に、静的ルートのステータスがアクティブとして報告されることを保証します。 [AND] を選択した場合、トラッカーグループの関連付けられた両方のトラッカーがルートがアクティブであると報告した場合、静的ルートのステータスはアクティブであると報告されます。

8. [Add] をクリックします。
9. [Save] をクリックします。

（注） テンプレートを保存する前に、すべての必須アクションを完了してください。

トラッカーでネクスト ホップ スタティック ルートを構成する

[VPN]テンプレートを使用して、トラッカーを静的ルートのネクストホップに関連付けます。

（注） 静的ルートのネクストホップごとに 1 つのトラッカーのみを適用できます。

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. デバイスの [Cisco VPN Template] に移動します。

（注） VPN テンプレートの作成については、「VPN テンプレートの作成」を参照してください。

4. 必要に応じて、[Template Name] および [Description] を入力します。
5. 基本設定では、VPN はデフォルトで 0 に設定されています。Cisco IOS XE SD-WAN デバイス のサービス側のデータトラフィックに対して、サービス VPN の VPN 値を（1 ～ 511、513 ～ 65530）の範囲内に設定します。

（注） 静的ルートトラッカーは、サービス VPN でのみ設定できます。

6. [IPv4 Route] をクリックします。
7. [New IPv4 Route] をクリックします。
8. [IPv4 Prefix] フィールドに値を入力します。
9. [Next Hop] をクリックします。
10. [Add Next Hop with Tracker] をクリックし、テーブルにリストされているフィールドに値を入力します。

パラメータ名	説明
Address	ネクストホップ IPv4 アドレスを指定します。
距離	ルートのアドミニストレーティブディスタンスを指定します。
Tracker	ゲートウェイトラッカーの名前を入力して、ネクストホップが到達可能かどうかを判断してから、そのルートをデバイスのルートテーブルに追加します。
Add Next Hop with Tracker	ネクストホップアドレスを含むゲートウェイトラッカーの名前を入力して、ネクストホップが到達可能かどうかを判断してから、そのルートをデバイスのルートテーブルに追加します。

11. [Add]をクリックして、ネクストホップトラッカーを使用して静的ルートを作成します。
12. **[Save]** をクリックします。

（注） VPNテンプレートを保存するには、フォームのすべての必須フィールドに入力する必要があります。

静的ルートトラッカー設定のモニタリング

静的ルートトラッカーの表示

トランスポートインターフェイスで静的トラッカーに関する情報を表示するには、次を実行します。

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。

CLI を使用した静的ルートの設定

ここでは、CLI を使用した静的ルートの設定方法に関する情報について説明します。

静的ルートトラッカーの設定

（注） Cisco vManage CLI アドオン機能テンプレートおよび CLI デバイステンプレートを使用して、静的ルートトラッキングを設定できます。CLI テンプレートを使用した構成の詳細については、「CLI テンプレート」を参照してください。

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

エンドポイントとして TCP ポートを使用して静的ルートトラッカーを設定する

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

エンドポイントとして UDP ポートを使用して静的ルートトラッカーを設定する

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name> endpoint-tracker
```

トラッカーグループの設定

（注） Cisco IOS XE リリース 17.7.1a および Cisco vManage リリース 20.7.1 から静的ルートをプローブするトラッカーグループを作成できます。

```
Device# config-transaction
Device(config)# endpoint-tracker <tracker-name1>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> tcp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name1> endpoint-tracker

Device# config-transaction
Device(config)# endpoint-tracker <tracker-name2>
Device(config-endpoint-tracker)# tracker-type <tracker-type>
Device(config-endpoint-tracker)# endpoint-ip <ip-address> udp <port-number>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# interval <value>
Device(config-endpoint-tracker)# exit
Device(config)# track <tracker-name2> endpoint-tracker

Device(config)# endpoint-tracker <static-tracker-group>
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements <tracker-name1> <tracker-name2>
Device(config-endpoint-tracker)# boolean {and | or}
Device(config-endpoint-tracker)# exit
Device(config)# track <static-tracker-group> endpoint-tracker

Device(config)# ip route vrf <vrf-name> <prefix> <mask> <nexthop-ipaddress>
<administrative-distance> track name <static-tracker-group>
```

（注）

- **ip route** コマンドを使用して、トラッカーまたはトラッカーグループを静的ルートにバインドし、アドミニストレーティブディスタンスがデフォルト値の 1 より大きいバックアップルートを設定します。
- エンドポイントに適用できるトラッカーは 1 つだけです。
- トラッカーグループには、エンドポイントトラッカーを混在させることができます。たとえば、IP アドレストラッカーと UDP トラッカーを使用してトラッカーグループを作成できます。

CLI を使用した静的ルートトラッキングの設定例

トラッカーの設定

次に、静的ルートトラッカーの設定例を示します。

```
config-transaction
!
 endpoint-tracker tracker1
!
  tracker-type static-route
  endpoint-ip 10.1.1.1
  threshold 100
  multiplier 5
  interval 20
  exit
!
track tracker1 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tracker1
```

次に、TCP ポートをエンドポイントとしてトラッカーを設定する例を示します。

```
config-transaction
!
 endpoint-tracker tcp-10001
!
  tracker-type static-route
  endpoint-ip 10.0.0.1 tcp 10001
  threshold    100
  interval     10
  multiplier   1
  exit
!
track tcp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name tcp-10001
```

次に、UDP ポートをエンドポイントとしてトラッカーを設定する例を示します。

```
config-transaction
!
  endpoint-tracker udp-10001
!
    tracker-type static-route
    endpoint-ip 10.0.0.1 udp 10001
    threshold    100
    interval     10
    multiplier   1
    exit
!
track udp-10001 endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name udp-10001
```

トラッカーグループの設定

この例は、2 つのトラッカー（2 つのエンドポイント）を持つトラッカーグループを設定する方法を示しています。Cisco IOS XE リリース 17.7.1a からスタティックルートをプローブするトラッカーグループを作成できます。

```
config-transaction
!
 endpoint-tracker tcp-10001
!
    tracker-type static-route
    endpoint-ip 10.1.1.1 tcp 10001
    threshold 100
    multiplier 5
    interval 20
    track tcp-10001 endpoint-tracker
!
 endpoint-tracker udp-10002
!
   tracker-type static-route
   endpoint-ip 10.2.2.2 udp 10002
   threshold 100
   multiplier 5
   interval 20
   track udp-10002 endpoint-tracker
!
endpoint-tracker static-tracker-group
!
  tracker-type tracker-group
  tracker-elements tcp-10001 udp-10002
  boolean and
  track static-tracker-group endpoint-tracker
!
ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name static-tracker-group
```

（注）
- CLIテンプレートを使用して設定する場合は、アドミニストレーティブディスタンスを設定する必要があります。
- **ip route** コマンドを使用して、トラッカーまたはトラッカーグループをスタティックルートにバインドし、アドミニストレーティブディスタンスがデフォルト値の 1 より大きい場合のバックアップルートを設定します。
- エンドポイントに適用できるトラッカーは 1 つだけです。

CLI を使用した静的ルートトラッキング設定の確認

コマンドの確認

次のコマンドを使用して、設定がコミットされているかどうかを確認します。次の設定例は、静的ルートトラッカーのトラッカー定義と、IPv4 スタティックルートへの適用を示しています。

```
Device# show running-config | sec endpoint-tracker
endpoint-tracker tracker1
endpoint-ip 10.1.1.1
interval 60
multiplier 5
tracker-type static-route
endpoint-tracker tracker2
endpoint-ip 10.1.1.12
interval 40
multiplier 2
tracker-type static-route
track tracker2 endpoint-tracker
track tracker1 endpoint-tracker
```

次のコマンドを使用して、IPv4 ルートを確認します。

```
Device# show running-config | inc ip route
ip route vrf 1 10.1.1.11 255.255.0.0 10.20.2.17 track name tracker2
ip route vrf 1 10.1.1.12 255.255.0.0 10.20.24.17 track name tracker1
```

次に、個々の静的ルートトラッカーのステータスを表示する **show endpoint-tracker static-route** コマンドの出力例を示します。

```
Device#  show endpoint-tracker static-route
Tracker Name   Status     RTT (in msec) Probe ID
tcp-10001         UP          3             1
udp-10002         UP          1             6
```

次に、トラッカーグループのステータスを表示する **show endpoint-tracker tracker-group** コマンドの出力例を示します。

```
Device# show endpoint-tracker group
Tracker Name               Element trackers name    Status         RTT in msec  Probe
ID
group-tcp-10001-udp-10002  tcp-10001, udp-10002     UP(UP AND UP)  5, 1          9, 10
```

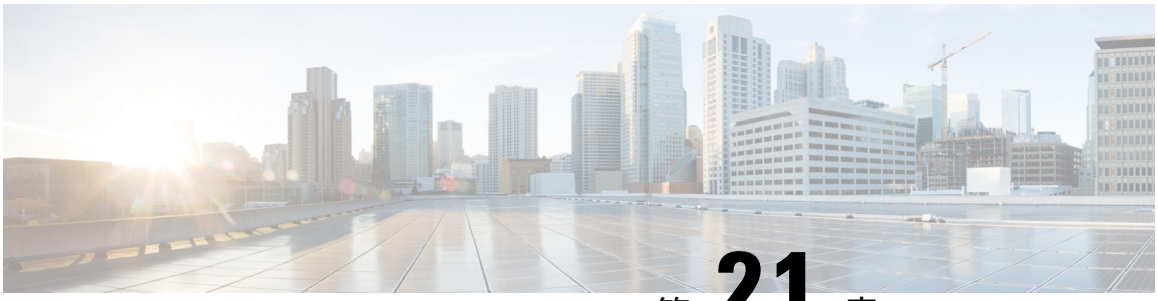
次に、トラッカーまたはトラッカーグループの設定を表示する **show endpoint-tracker records** コマンドの出力例を示します。

```
Device# show endpoint-tracker records
Record Name              Endpoint                EndPoint Type Threshold(ms) Multiplier
 Interval(s) Tracker-Type
group-tcp-10001-udp-10002  tcp-10001 AND udp-10002  N/A           N/A           N/A
    N/A         static-tracker-group
tcp-10001                  10.1.1.1                TCP           100           1
    20          static-route
udp-10002                  10.2.2.2                UDP           100           1
    20          static-route
```

次に、**show ip static route vrf** コマンドの出力例を示します。

```
Device# show ip static route vrf 1
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect, Vx - VXLAN static route
       LT - Cellular LTE, Ev - L2EVPN static route
```

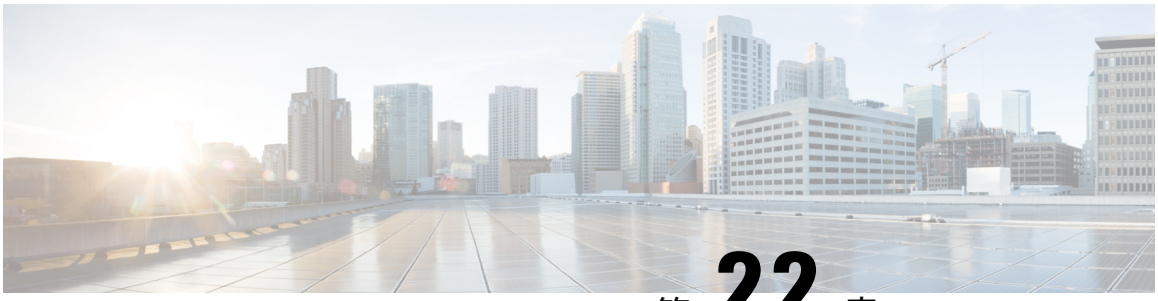
```
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent,
 -T Default Track
Codes in (): UP - up, DN - Down, AD-DN - Admin-Down, DL - Deleted
Static local RIB for 1
T  192.168.0.0 [1/0] via 10.1.19.16 [A]
```



第 21 章

Cisco IOS XE SD-WAN デバイス の NAT DIA トラッカー

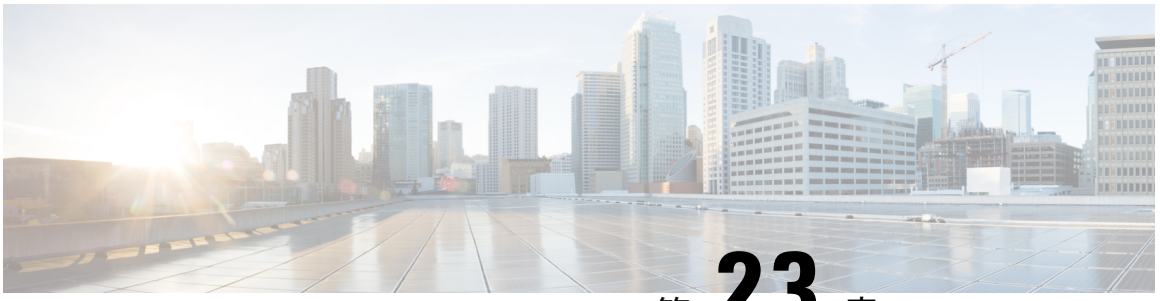
Cisco IOS XE SD-WAN デバイス の NAT DIA トラッカーについては、『*Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.x*』の「NAT DIA Tracker」セクションを参照してください。



第 22 章

Cisco IOS XE SD-WAN デバイス のサービス側 NAT

Cisco IOS XE SD-WAN デバイスのサービス側 NAT については、『*Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE* リリース *17.x*』の「Service-Side NAT」セクションを参照してください。



第 23 章

IPv6 機能

この章では、Cisco SD-WAN テンプレートとポリシーの IPv6 機能を有効にするオプションについて説明します。展開で IPv6 を使用する場合は、この章の情報を使用してください。

インターフェイスまたはサブインターフェイス テンプレートの IPv6 機能の設定

インターフェイスまたはサブインターフェイス テンプレートの IPv6 機能を設定するには、次の手順を実行します。

Cisco SD-WAN でのデュアルスタックのサポート：同じ展開で IPv4 と IPv6 を設定できます。インターフェイスごとに最大 3 つのグローバル IPv6 アドレスを設定できます。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [Basic Configuration] で、[IPv6] をクリックし、次の表に記載されているパラメータを設定します。

パラメータ名	説明
スタティック	IPv6 アドレスは固定であるため、このラジオボタンはデフォルトで選択されています。
IPv6 Address	インターフェイスまたはサブインターフェイスの IPv6 アドレスを入力します。

CLI の同等の設定：

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

OMP テンプレートの IPv6 機能の設定

オーバーレイ管理プロトコル（OMP）テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco OMP] を選択します。
4. [Advertise] をクリックし、[IPv6] を選択して、次の表に示すパラメータを設定します。

パラメータ名	説明
接続済み	OMP への接続ルートのアドバタイズを無効にするには、[Off] をクリックします。 デフォルトでは、接続ルートは OMP にアドバタイズされます。
スタティック	OMP へのスタティックルートのアドバタイズを無効にするには、[Off] をクリックします。 デフォルトでは、スタティックルートは OMP にアドバタイズされます。
BGP	BGP ルートを OMP にアドバタイズするには、[On] をクリックします。デフォルトでは、BGP ルートは OMP にアドバタイズされません。

CLI の同等の設定：

まず、IPv6 のサービス VRF を有効にします。

```
config-transaction
vrf definition 1
  rd 1:1
  address-family ipv6
```

次に OMP を有効にします。

OMP ではグローバル IPv6 設定がサポートされます。また、VRF レベルごとの設定が可能です。VRF レベルごとの設定により、グローバル設定はオーバーライドされます。

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    advertise static
```

グローバル設定がデフォルトの設定であるため、IPv6 は OMP に対してデフォルトで有効になっています。特定の VRF の IPv6 OMP ルート再配布を無効にするには、次のように再配布プロトコルを no に設定します。

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    no advertise connected
    no advertise static
    no advertise bgp
```

BGP テンプレートの IPv6 機能の設定

ボーダー ゲートウェイ プロトコル（BGP）テンプレートの IPv6 機能を設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco BGP] を選択します。
4. [Unicast Address Family] をクリックし、[IPv6] を選択して、次の表に示すパラメータを設定します。

タブ	パラメータ名	説明
	Maximum Paths	IBGP マルチパス ロード シェアリングを有効にするために、ルートテーブルにインストールできるパラレル IBGP パスの最大数を指定します。範囲：0 ー 32
	Address Family	BGP IPv6 ユニキャスト アドレス ファミリを入力します。

タブ	パラメータ名	説明
RE-DISTRIBUTE		[Redistribute] タブをクリックし、[Add New Redistribute] をクリックします。
	プロトコル	すべての BGP セッションでルートを BGP に再配布するプロトコルを選択します。オプションは、[Connected]、[NAT]、[OMP]、[OSPF]、および [Static] です。少なくとも、次のように選択します。 • サービス側 BGP ルーティングの場合は、[OMP] を選択します。デフォルトでは、OMP ルートは BGP に再配布されません。 • トランスポート側 BGP ルーティングの場合は、[Connected] を選択し、[Route Policy] で、BGP がループバック インターフェイス アドレスをネイバーにアドバタイズするルートポリシーを指定します。
	ルート ポリシー（ルート ポリシー）	再配布されるルートに適用するルートポリシーの名前を入力します。
		[Add] をクリックして再配布情報を保存します。
NETWORK		[Network] タブをクリックし、[Add New Network] をクリックします。
	[Network Prefix]	BGP によってアドバタイズされるネットワークプレフィックスを *prefix*/*length* の形式で入力します。
		[Add] をクリックして、ネットワークプレフィックスを保存します。
AGGREGATE ADDRESS		[Aggregate Address] タブをクリックして、[Add New Aggregate Address] をクリックします。
	[Aggregate Prefix]	すべての BGP セッションに対して集約するアドレスのプレフィックスをプレフィックス/長さの形式で入力します。
	[AS Set Path]	集約されたプレフィックスの設定パス情報を生成するには、[On] をクリックします。
	[Summary Only]	BGP 更新から詳細ルートを除外するには、[On] をクリックします。
		[Add] をクリックして、集約アドレスを保存します。

1. [Neighbor] 領域で、[IPv6] をクリックし、新しいネイバーを作成するか、既存のネイバーを編集して、次の表に記載されている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。

パラメータ名	説明
IPv6 Address*	BGP ネイバーの IPv6 アドレスを指定します。
説明	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Address Family	ドロップダウンリストから [Global] を選択し、[On] をクリックしてアドレスファミリを選択します。アドレスファミリ情報を入力します。
シャットダウン	テンプレートをプッシュするときにBGPネイバーをシャットダウンする場合は、ドロップダウンリストから [Global] を選択し、[Yes] をクリックします。デフォルト：[Off]

CLI の同等の設定：

```
config-transaction
router bgp 1
 bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

VRRP テンプレートの IPv6 機能の設定

Virtual Router Redundancy Protocol（VRRP）テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [VRRP] をクリックし、[IPv6] を選択します。
5. [New VRRP] をクリックします。

6. 次の表に示すパラメータを設定します。

パラメータ名	説明
グループ ID（Group ID）	ルータのグループを表す仮想ルータ ID を入力します。 範囲： 1 ～ 255
プライオリティ	VRRP グループ内のルータの優先度を入力します。 • 範囲：1 ～ 254 • デフォルト：100
Timer	未使用です。
Track OMP	プライマリ VRRP 仮想ルータを決定するときに、WAN 接続で実行されているオーバーレイ管理プロトコル（OMP）セッションをトラッキングする場合は、[On] を選択します。デフォルト：[Off]
Track Prefix List	IPv6 リモートプレフィックスのリストをトラッキングするための値を入力します。この値は、ポリシーで設定されている英数字の文字列です。
Link Local IPv6 Address	グループのリンクローカルアドレスを表す仮想リンクローカル IPv6 アドレスを入力します。アドレスは、標準のリンクローカルアドレス形式になっている必要があります。たとえば、FE80::AB8 です。
Global IPv6 Address	グループのグローバルアドレスを表す仮想グローバルユニキャスト IPv6 アドレスを入力します。このアドレスは、VRRP グループが設定されているインターフェイス転送アドレスと同じマスクを持つIPv6 グローバル プレフィックス アドレスである必要があります。たとえば、2001::2/124 です。 最大 3 つのグローバル IPv6 アドレスを設定できます。

CLI の同等の設定：

```
config-transaction
interface GigabitEthernet1

 vrrp 10 address-family ipv6
   priority 20
   track omp shutdown
   address FE80::10:100:1 primary
   address 2001:10:100::1/64

Prefix-list tracking
track 1 ipv6 route 1:1::1/128
 reachability
 ipv6 vrf 1
```

```
 track 2 ipv6 route 2:2::2/128
 reachability
 ipv6 vrf 2

 track 20 list boolean or
  object 1
  object 2

vrrp 10 address-family ipv6
  track 20 shutdown
```

SNMP テンプレートの IPv6 機能の設定

SNMP テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco SNMP] をクリックします。
4. [SNMP Version] > [TRAP TARGET SERVER] を選択し、SNMP トラップターゲットを作成または編集します。
5. 次の表に示すパラメータを設定します。

パラメータ名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ～ 65530。
IP アドレス	SNMP サーバーの IP アドレスを入力します。
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ～ 65535。
Trap Group Name	[Group] タブで設定したトラップグループの名前を選択します。
User Name	[Community] タブで設定されたコミュニティの名前を選択します。
Source Interface	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

（注） SNMP コミュニティとトラップターゲットグループがすでに設定されていることを確認してください。

CLI の同等の設定：

次に、コミュニティストリング public を使用して、SNMP が読み取り専用アクセス権ですべてのオブジェクトにアクセスすることを許可する例を示します。また、デバイスは SNMP v1 を使用して、ボーダーゲートウェイプロトコル（BGP）トラップ IPv6 ホスト 3ffe:b00:c18:1::3/127 を送信します。public という名前のコミュニティ文字列が、トラップとともに送信されます。

```
デバイス# config-transaction
デバイス(config)# snmp-server community public
デバイス(config)# snmp-server enable traps bgp
デバイス(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

次に、SNMP コンテキスト A を SNMPv2c グループ GROUP1 のビューと IPv6 の名前付きアクセス リスト public2 に関連付ける例を示します。

```
デバイス# config-transaction
デバイス(config)# snmp-server context A
デバイス(config)# snmp mib community-map commA context A target-list comm AVpn
デバイス(config)# snmp mib target list commAVpn vrf CustomerA
デバイス(config)# snmp-server view viewA ciscoPingMIB included
デバイス(config)# snmp-server view viewA ipForward included
デバイス(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify
access ipv6 public2
```

次に、IPv6 ホストを通知サーバとして設定する例を示します。

```
デバイス> enable
デバイス# config-transaction
デバイス(config)# snmp-server community mgr view restricted rw ipv6 mgr2
デバイス(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
デバイス(config)# snmp-server group publicv2c access ipv6 public2
デバイス(config)# snmp-server hosthost1.com2c vrf trap-vrf mgr
デバイス(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6
 public2
デバイス(config)# snmp-server enable traps bgp
デバイス(config)# exit
```

DHCP リレー エージェント テンプレートの IPv6 機能の設定

DHCP リレー エージェント テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [Basic Configuration] で、[IPv6] をクリックします。
5. [DHCP Helper] の横にある [Add] をクリックします。
6. 次の表に示すパラメータを設定します。

表 *197*:

パラメータ名	説明
DHCPv6 Helper #	DHCP ヘルパーの IP アドレス
DHCPv6 Helper VPN	DHCP ヘルパーの VPN 送信元インターフェイスの VPN ID。

CLI の同等の設定：

```
device-configuration
interface GigabitEthernet8
 vrf forwarding 2
 no ip address
 ipv6 address 2001:A14:99::F/64
 ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

ACL テンプレートまたは QoS テンプレートの IPv6 機能の設定

ACL および QoS テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [ACL/QoS] で、次の表に示すパラメータを設定します。

パラメータ名	説明
入力 ACL – IPv6	[On] をクリックして、IPv6 入力アクセスリストを有効にします。

パラメータ名	説明
IPv6 Ingress Access List	IPv6 入力アクセスリストの名前を入力します。
出力 ACL – IPv6	[On] をクリックして、IPv6 出力アクセスリストを有効にします。
IPv6 Egress Access List	IPv6 出力アクセスリストの名前を入力します。

ACL テンプレートの *IPv6* 機能の設定に相当する *CLI*：

```
デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv6_acl
デバイス(config-access-list-ipv6_acl)#    sequence 11
デバイス(config-sequence-11)#     match
デバイス(config-match)#       source-ip 2001:380:1::64/128
デバイス(config-match)#      destination-ip 2001:3c0:1::64/128
デバイス(config-match)#      source-port      4000
デバイス(config-match)#      destination-port 3000
デバイス(config-match)#      traffic-class    6
デバイス(config-match)#      next-header      6
デバイス(config-match)#      packet-length    1000
デバイス(config-match)#     action accept
デバイス(config-action)#

デバイス(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
デバイス(config-interface-GigabitEthernet6)#
デバイス(config-interface-GigabitEthernet6)#

デバイス(config)# policy lists data-ipv6-prefix-list source_ipv6_list
デバイス(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv_ipv6_prefix
デバイス(config-access-list-ipv_ipv6_prefix)# sequence 11
デバイス(config-sequence-11)#     match
デバイス(config-match)#       source-data-prefix-list data-ipv6-prefix-list
デバイス(config-match)#       destination-data-prefix-list source_ipv6_list
デバイス(config-match)#      destination-ip 2001:3c0:1::64/128
デバイス(config-match)#      source-port      4000
デバイス(config-match)#      destination-port 3000
デバイス(config-match)#      traffic-class    6
デバイス(config-match)#      next-header      6
デバイス(config-match)#      packet-length    1000
デバイス(config-match)#     !
デバイス(config-match)#     action accept
```

QoS テンプレートの *IPv6* 機能の設定に相当する *CLI*：

```
デバイス(config)# class-map match-any class0
デバイス(config-cmap)#  match qos-group 0
デバイス(config-cmap)# class-map match-any class1
```

```
デバイス(config-cmap)#  match qos-group 1
デバイス(config-cmap)# !
デバイス(config-cmap)# policy-map qos_map_for_data_policy
デバイス(config-pmap)#  class class0
デバイス(config-pmap-c)#   bandwidth percent 10
デバイス(config-pmap-c)#   random-detect
デバイス(config-pmap-c)#  class class1
デバイス(config-pmap-c)#   bandwidth percent 10
デバイス(config-pmap-c)#   random-detect
デバイス(config-pmap-c)#
デバイス(config-pmap-c)# policy
デバイス(config-policy)#  no app-visibility
デバイス(config-policy)#  class-map
デバイス(config-class-map)#   class class0 queue 0
デバイス(config-class-map)#   class class1 queue 1
デバイス(config-class-map)# !
デバイス(config-class-map)#  ipv6
デバイス(config-ipv6)#   access-list fwd_class_data_policy
デバイス(config-access-list-fwd_class_data_policy)#    sequence 5
デバイス(config-sequence-5)#     match
デバイス(config-match)#      traffic-class 0
デバイス(config-match)#     !
デバイス(config-match)#     action accept
デバイス(config-action)#      count fwd_class_data_policycnt_5
デバイス(config-action)#      class class0
デバイス(config-action)#     !
デバイス(config-action)#    !
デバイス(config-action)#    sequence 6
デバイス(config-sequence-6)#     match
デバイス(config-match)#      traffic-class 1
デバイス(config-match)#     !
デバイス(config-match)#     action accept
デバイス(config-action)#      count fwd_class_data_policycnt_6
デバイス(config-action)#      class class1
デバイス(config-action)#     !
デバイス(config-action)#    !
デバイス(config-action)#    !
デバイス(config-action)#    default-action drop

class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
  bandwidth percent 10
  random-detect
class class1
  bandwidth percent 10
  random-detect

policy
no app-visibility
class-map
  class class0 queue 0
```

```
  class class1 queue 1
!
ipv6
  access-list fwd_class_data_policy
   sequence 5
    match
     traffic-class 0
    !
    action accept
     count fwd_class_data_policycnt_5
     class class0
    !
   sequence 6
    match
     traffic-class 1
    !
    action accept
     count fwd_class_data_policycnt_6
     class class1
!
default-action drop
```

ロギングテンプレートの IPv6 機能の設定

ロギングテンプレートの IPv6 機能を設定するには、次の手順に従います。

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、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. テンプレートのリストから [Cisco Logging] を選択します。
4. [Server] で、[IPv6] をクリックします。
5. 次の表に示すパラメータを設定します。

パラメータ名	説明
IPv6 Hostname/IPv6 Address	ロギング情報を送信するサーバーのホスト名またはIPアドレス。
VPN ID	VPN 送信元インターフェイスの VPN ID。
Source Interface	送信元インターフェイスの名前。
プライオリティ	ログに記録されるメッセージの最大重大度を選択します。

CLI の同等の設定：

```
config-transaction
デバイス(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```

（注） 同じトランザクションでロギングホスト設定を作成および削除すると、予期しない動作が発生します。たとえば、同じトランザクションで **logging host** *ipv6-address* を削除し、**logging host** *ipv6-address* **vrf** *vrf-name* 設定を作成すると、両方の設定がデバイスから消えます。2 つのリクエストを別々のトランザクションで送信することをお勧めします。

新しいプレフィックスリストの IPv6 機能の設定

新しいプレフィックスリストの IPv6 アドレスを設定するには、次の手順に従います。

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Custom Options] ドロップダウンリストから、[Lists] を選択します。[Centralized Policy] または [Localized Policy] に対してこの選択を行うことができます
3. 左側のリストから [Prefix] を選択し、[New Prefix List] を選択します。
4. [IPv6] をクリックし、[Add Prefix] に IPv6 アドレスを入力します。

CLI の同等の設定：

```
config-transaction
デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv6_acl
デバイス(config-access-list-ipv6_acl)#  sequence 11
デバイス(config-sequence-11)#  match
デバイス(config-match)# source-ip 2001:380:1::64/128
デバイス(config-match)# destination-ip 2001:3c0:1::64/128
```

データプレフィックスの IPv6 機能の設定

新しいプレフィックスリストの IPv6 アドレスを設定するには、次の手順に従います。

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Custom Options] ドロップダウンリストから、[Lists] を選択します。[Centralized Policy] または [Localized Policy] に対してこの選択を行うことができます
3. 左側のリストから [Data Prefix] を選択し、[New Data Prefix List] を選択します。
4. [Internet Protocol] で [IPv6] をクリックし、[Add Prefix] に IPv6 アドレスを入力します。

CLI の同等の設定：

```
デバイス(config)# policy lists data-ipv6-prefix-list source_ipv6_list
デバイス(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64
```

一元化されたポリシーの IPv6 機能の設定

IPv6 アドレスファミリに適用する一元化されたポリシーを設定するには、次の手順に従います。

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Custom Options] ドロップダウンメニューの [Centralized Policy] で [Traffic Policy] を選択します。
3. [Traffic Data] を選択します。
4. [Add Policy] をクリックし、[Create New] をクリックします。
5. [Sequence Type] をクリックし、[Traffic Engineering] を選択します。
6. [Sequence Rule] をクリックします。
7. [Protocol] ドロップダウンリストから、[IPv6] を選択してポリシーを IPv6 アドレスファミリのみに適用するか、[Both] を選択してポリシーを IPv4 および IPv6 アドレスファミリを適用します。
8. [Sequence Type] をクリックし、[QoS] を選択します。
9. [Sequence Rule] をクリックします。
10. [Protocol] ドロップダウンリストから、[IPv6] をクリックしてポリシーを IPv6 アドレスファミリのみに適用するか、[Both] を選択してポリシーを IPv4 および IPv6 アドレスファミリを適用します。

CLI の同等の設定：

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                 ipv6-prefix-list ipv6-1
                 ipv6-prefix 1::1/128
```

ローカライズされたポリシーの IPv6 機能の設定

IPv6 アドレスファミリに適用するローカライズされたポリシーを設定するには、次の手順に従います。

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Custom Options] ドロップダウンリストの [Localized Policy] で [Access Control Lists] を選択します。
3. [Add Access Control List Policy] をクリックし、[Add IPv6 ACL Policy] を選択します。作成したポリシーは、IPv6 アドレスファミリにのみ適用されます。

CLI の同等の設定：

次の例では、marketing という名前のプレフィックスリストで指定されたアドレスを持つ IPv6 ルートが一致します。

```
config-transaction
デバイス(config)# route-map name
デバイス(config-route-map)# match ipv6 address prefix-list marketing
```

• DHCP for IPv6 （785 ページ）

DHCP for IPv6

表 *198 :* 機能の履歴

機能名	リリース情報	説明
DHCP for IPv6	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能を使用すると、Cisco IOS XE SD-WAN デバイス で DHCP for IPv6（DHCPv6）を構成して、IPv6 アドレスを IPv6 対応ネットワーク上のホストに割り当てることができます。 IPv6 アドレスの割り当ては、SLAAC、DHCPv6、DHCPv6 プレフィックス委任、または DHCPv6 リレーを使用して行われます。 Cisco IOS XE SD-WAN デバイス は、DHCPv6 用に DHCP サーバー、DHCP クライアント、または DHCP リレーエージェントとして設定できます。

DHCPv6 の前提条件

- Cisco IOS XE SD-WAN デバイスに接続されたホストに IPv6 アドレスを割り当てるための基本的な IPv6 接続。

DHCPv6 の制約事項

- この機能は、CLI 設定を使用する場合のみサポートされます。
- VRF ごとに一意の DHCPv6 プール名を指定する必要があります。

DHCPv6 に関する情報

IPv6 の Dynamic Host Configuration Protocol（DHCP）を設定して、IPv6 対応ネットワークにアドレスを割り当てることができます。または、Stateless Address Autoconfiguration（SLAAC）を設定して、IPv6 対応ネットワークにアドレスを割り当てることもできます。

SLAAC

IPv6 クライアントアドレス割り当て用の最も一般的な方法は、SLAAC です。SLAAC はホストが IPv6 プレフィックスに基づいてアドレスを自己割り当てするシンプルなプラグアンドプレイ接続を提供します。

SLAAC は次のように設定されます。

- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータアドバタイズメント（RA）メッセージを待機します。
- ホストは、RA メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルトゲートウェイとして、RA メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出（DAD）は、選択されるランダムアドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。
- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

SLAAC および DHCPv6

DHCPv6

IPv6 デバイスはマルチキャストを使用して IP アドレスを取得し、DHCPv6 サーバを見つけます。DHCPv6 クライアント/サーバの基本概念は、IPv4 の DHCP に似ています。クライアントが設定パラメータを受信する必要がある場合は、接続しているローカルネットワークで要求を送信し、利用可能な DHCPv6 サーバを検出します。サーバは要求された情報を応答メッセージで返します。

DHCPv6 クライアントは、リンクローカル ネットワーク上のルータからの指示に基づいて DHCPv6 を使用するかどうかを認識します。デフォルトゲートウェイの RA には、この目的で使用できる 2 つの設定可能なビットがあります。

- O ビット：このビットを設定すると、クライアントは自身の IP アドレスではなく、その他の設定パラメータ（たとえば、TFTP サーバーアドレスまたは DNS サーバーアドレス）を取得するために DHCPv6 を使用できます。
- M ビット：このビットを設定すると、クライアントは DHCPv6 サーバから管理対象 IPv6 アドレスとその他の設定パラメータを取得するために DHCPv6 を使用できます。

ステートレス DHCP

ステートレス DHCPv6 は、SLAAC と DHCPv6 の組み合わせです。このオプションでは、IP アドレスを取得するために SLAAC を使用し、TFTP サーバーアドレスまたは DNS サーバーアドレスなどの追加情報を取得するために DHCP を使用します。この場合、デバイスは O ビットが設定された RA を送信しますが、M ビットは設定しません。DHCPv6 サーバーがクライアント アドレス バインディングを追跡する必要がないため、これはステートレス DHCPv6 と呼ばれます。

ステートフル DHCP

ステートフル DCHPv6 は、ホストが IPv6 アドレスと追加パラメータの両方を DHCP サーバーから受信する DHCP IPv4 とまったく同じように機能します。M ビットが設定された RA をデバイスが送信する場合、クライアントは DHCP を使用して自身の IP アドレスを取得する必要があることを意味します。M ビットが設定されている場合、DHCP サーバはアドレスとともに他の設定情報も返すので、O ビットの設定は意味がありません。DHCPv6 サーバーがクライアント アドレス バインディングを追跡するため、これはステートフル DHCPv6 と呼ばれます。

DHCPv6 プレフィックス委任

DHCPv6 プレフィックス委任機能は、委任側エッジデバイス（DHCP サーバー）から要求側エッジデバイス（DHCP クライアント）にプレフィックスを単純に委任するためのステートフルな動作モードです。

DHCPv6 プレフィックス委任機能は、次のような状況に最適です。

- 要求側のエッジデバイスが接続されているネットワークのトポロジに関する情報を持たない委任側のエッジデバイス。
- 委任するプレフィックスを選択するために要求側のエッジデバイスの ID 以外の情報を必要としない委任側のエッジデバイス。このメカニズムは、ISP がプレフィックスをサブスクライバに委任するために使用するのに適しています。ISP がプレフィックスをサブスクライバに委任した後、サブスクライバはプレフィックスをさらにサブネット化してサブスクライバのネットワーク内のリンクに割り当てることができます。

DHCPv6リレー

DHCPv6 リレーエージェントは、クライアントのネットワーク上にあるエッジデバイスであり、DHCPv6 サーバーが DHCPv6 クライアントと同じネットワークにない場合に、クライアントとサーバーの間でメッセージをリレーするために使用されます。

DHCPv6 の利点

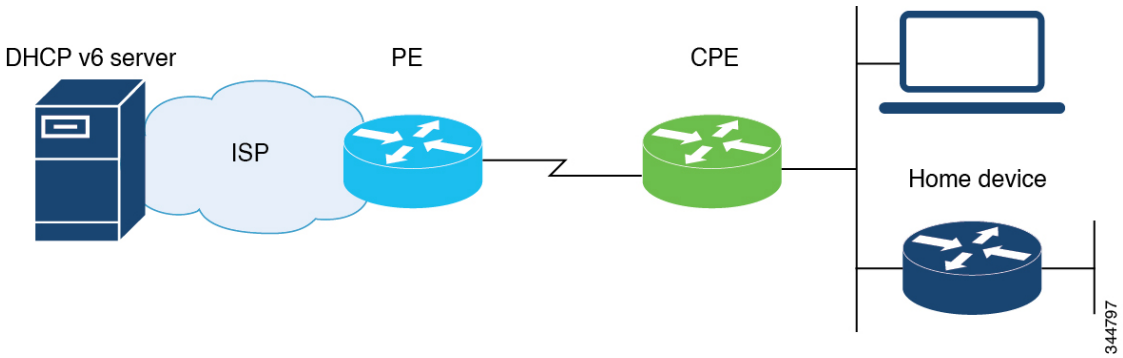
IPv6 用に DHCP を設定すると、IPv4 と比較してより多くの IP アドレスを持つことができます。IPv6 では、IP アドレスが枯渇することはありません。

DHCPv6 の使用例

Cisco IOS XE SD-WAN デバイス は、サーバー、クライアント、またはリレーエージェントとして DHCPv6 用に設定できます。サーバーとして、Cisco IOS XE SD-WAN デバイス は SLAAC、ステートレス DHCP、またはプレフィックス委任用に設定できます。

DHCP を使用した SLAAC

次の図に、一般的なブロードバンド展開を示します。



顧客宅内（CPE）に展開され、ISP エッジ（PE）デバイスに接続されている Cisco IOS XE SD-WAN デバイス は、ステートレスまたはステートフルな DHCPv6 クライアントにすることができます。どちらの場合も、ISP 側の DHCPv6 サーバは、ドメイン ネーム システム（DNS）サーバ アドレス、ドメイン名、Simple Network Time Protocol（SNTP）サーバなどの設定パラメータを CPE 上の DHCP クライアントに提供できます。このような情報は ISP に固有です。

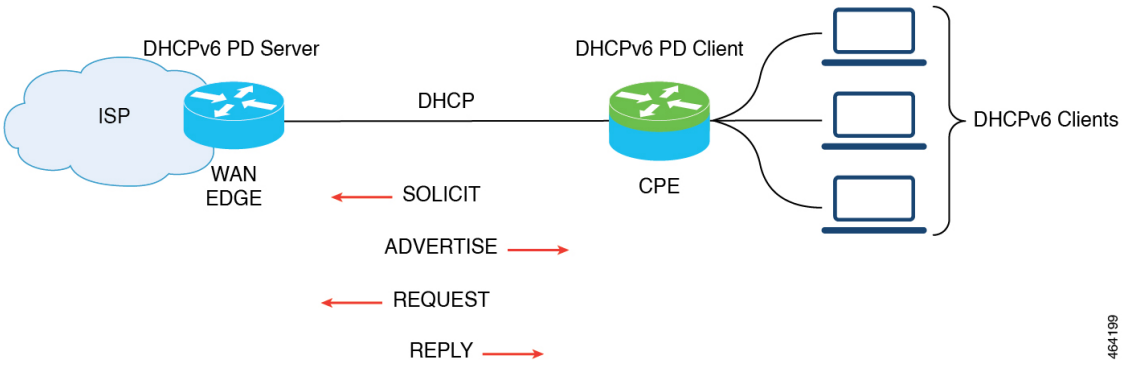
CPE は、DHCPv6 クライアント（ISP に対するクライアント）であるだけでなく、ホームネットワークに対する DHCPv6 サーバーとして機能する場合もあります。たとえば、ネイバー探索に続けて、ステートレスまたはステートフルの DHCPv6 クライアントが CPE とホーム デバイスの間のリンクに現れることがあります。また、ホーム ネットワークに提供される情報は、ISP 側の DHCPv6 サーバから取得されたものと同じでになることもあります。そのため、CPE 上の DHCPv6 コンポーネントでは、設定パラメータを DHCPv6 クライアントから DHCPv6 サーバ プールに自動的にインポートできます。

DHCPv6 プレフィックス委任

プレフィックス委任の運用モデルは次のとおりです。このサンプルトポロジでは、エッジデバイスは、DHCP クライアントに委任されるプレフィックスでプロビジョニングされた DHCP サーバーとして構成されています。Cisco IOS XE SD-WAN デバイス は DHCP クライアントとして構成され、サーバーからのプレフィックスを要求します。サーバーは、委任のプレフィッ

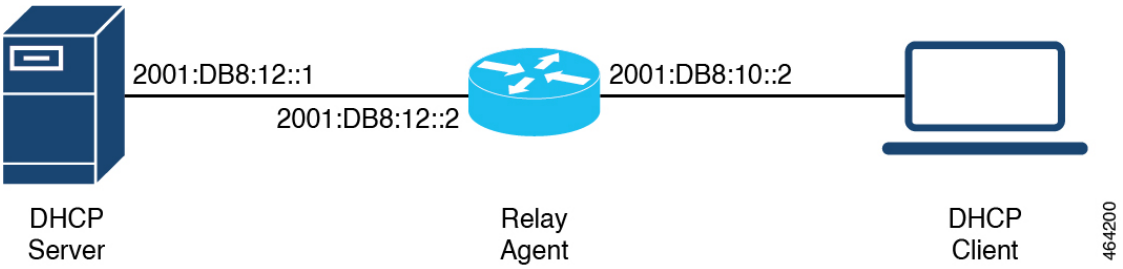
クスを選択し、DHCP クライアントにプレフィックスを付けて応答します。DHCP クライアントは、委任されたプレフィックスを担当します。

たとえば、クライアントは、委任されたプレフィックスからそのインターフェイスのいずれかにサブネットを割り当て、そのリンクのプレフィックスのルータアドバタイズメントの送信を開始できます。各プレフィックスには優先ライフタイムと有効なライフタイムが関連付けられており、クライアントがプレフィックスを使用できる時間の長さに関する合意が構成されます。クライアントは、委任されたプレフィックスのライフタイムの延長を要求でき、プレフィックスの有効なライフタイムが期限切れになった場合に委任されたプレフィックスの使用を終了する必要があります。



DHCPv6リレー

このサンプルトポロジでは、DHCP サーバーは DHCP クライアントと同じネットワークにありません。クライアントのネット上に常駐する Cisco IOS XE SD-WAN デバイス は、リレーエージェントとして動作し、クライアントとサーバー間のメッセージの中継に使用されます。



DHCPv6 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] ドロップダウンから、[CLI Template] を選択します。

（注） CLI アドオンテンプレートを使用して、クライアントとサーバーの IPv6 の DHCP を構成することもできます。詳細については、「Create a CLI Add-On Feature Template」を参照してください。

4. [Device Model] から、テンプレートを作成するデバイスモデルを選択します。
5. [Template Name] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
6. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
7. [CLI Configuration] フィールドで、クライアントとサーバーの IPv6 の DHCP 構成を手入力するか、カットアンドペーストするか、ファイルをアップロードして入力します。
8. [Save] をクリックします。

SLAAC の設定

この例は、クライアント側で SLAAC を設定する方法を示しています。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# end
```

この例は、サーバー側で SLAAC を設定する方法を示しています。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

オプションの SLAAC および DHCPv6 プールの設定

次に、クライアント側で SLAAC および DHCPv6 プールを設定する例を示します。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

次に、サーバー側で SLAAC および DHCPv6 プールを設定する例を示します。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd other-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

DHCPv6（ステートフル）アドレス割り当ての設定

この例は、クライアント側で DHCPv6 アドレス割り当てを設定する方法を示しています。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

この例は、サーバー側で DHCPv6 アドレス割り当てを設定する方法を示しています。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# address prefix 2010:AB8:0:1::1/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

プレフィックス委任を使用した DHCPv6 の設定（ステートフル）

次に、クライアント側でプレフィックス委任を使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client pd prefix_from_provider
```

```
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

次に、サーバー側でプレフィックス委任を使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 nd ra interval 20
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool1 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
device(config)# ipv6 local pool dhcpv6-pool1 2001:DB8:1200::/40 48
```

リレーを使用した DHCPv6 の設定

次に、クライアント側でリレーを使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet3
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp client pd pr-from-pd
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# no mop enabled
device(config-if)# no mop sysid
device(config-if)# end
```

次に、リレーエージェントとして機能するクライアント側 WAN エッジデバイスの設定を示します。

```
device(config)# interface TenGigabitEthernet0/0/5
device(config-if)# vrf forwarding 10
device(config-if)# load-interval 30
device(config-if)# ipv6 address 2001:BB:1000::10/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp relay destination 2001:BB8:1200::2
device(config-if)# ipv6 dhcp relay option vpn
device(config-if)# end
```

次に、サーバー側 WAN エッジデバイスの設定を示します。

```
device(config)# interface GigabitEthernet0/0/3
device(config-if)# vrf forwarding 10
device(config-if)# no ip address
device(config-if)# negotiation auto
device(config-if)# ipv6 address 2001:BB8:1200::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

次に、サーバー側でリレーを使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet2
device(config-if)# ipv6 address 2001:BB8:1200::2/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool10 lifetime infinite infinite
device(config-dhcpv6)# address prefix 2001:BB:1000::/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:BB:1200::42
device(config-dhcpv6)# domain-name relay.com
device(config)# ipv6 local pool dhcpv6-pool10 8001:ABCD::/40 48
```

DHCPv6 クライアントおよびサーバー設定の確認

DHCPv6 インターフェイス情報の確認

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x00080001, T1 100, T2 160
        Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
                 preferred lifetime 200, valid lifetime 200
                 expires at Oct 26 2021 07:28 AM (170 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00080001, T1 100, T2 160
        Prefix: 2001:DB8:1202::/48
                 preferred lifetime 200, valid lifetime 200
```

```
                expires at Oct 26 2021 07:30 AM (194 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
  Prefix name: prefix_from_server
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

次に、DHCP を使用した SLAAC に関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:59:49
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

DHCPv6 プール情報の表示

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp pool** コマンドの出力例を示します。

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in
use, 0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp pool** コマンドの出力例を示します。

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in
use, 0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
```

```
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

DHCPv6 バインディングの表示

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  IA NA: IA ID 0x00080001, T1 10000, T2 16000
    Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
             preferred lifetime 20000, valid lifetime 20000
             expires at Oct 26 2021 01:17 PM (19925 seconds)
```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  Interface : GigabitEthernet0/0/3
  IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:BB8:1602::/48
             preferred lifetime 200, valid lifetime 200
             expires at Oct 26 2021 08:01 AM (173 seconds)
```

DHCPv6 データベースの表示

次に、**show ipv6 dhcp database** コマンドの出力例を示します。

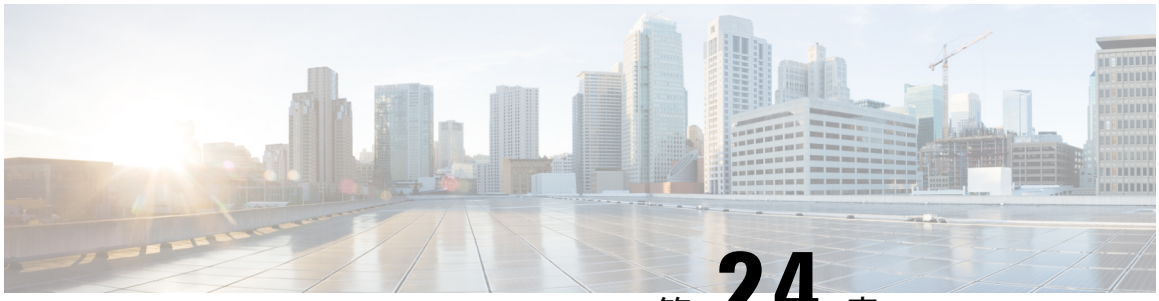
```
Device# show ipv6 dhcp database
Database agent bootflash:
  write delay: 300 seconds, transfer timeout: 300 seconds
  last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2
  failed write times 0
```

DHCPv6 リレーバインディングの表示

次に、DHCPv6 リレーに関する詳細を提供する **show ipv6 dhcp relay bindings** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding

Relay Bindings associated with default vrf:
```

```
Relay Bindings associated with vrf 10:
Prefix: 2001:AA8:1100::/48 (GigabitEthernet3)
  DUID: 00030001001E49674C00
  IAID: 851969
  lifetime: INFINITE
  expiration: INFINITE
Summary:
  Total number of Relay bindings = 1
  Total number of IAPD bindings = 1
  Total number of IANA bindings = 0
  Total number of Relay bindings added by Bulk lease = 0
```



第 24 章

IP Directed Broadcast

IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャストアドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。

あるインターフェイスでダイレクトブロードキャストがイネーブルになっている場合、着信したIPパケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。

（注） ダイレクトブロードキャストのアクセス制御リスト（ACL）オプションは、vManage ではサポートされていません。

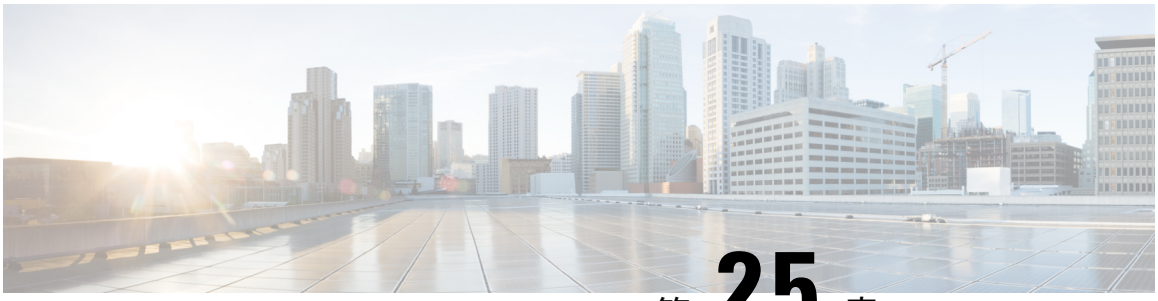
ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにするには、ip directed-broadcast コマンドを使用します。この機能をディセーブルにするには、このコマンドの no 形式を使用します。デフォルトでは、ip directed-broadcast は無効になっていて、すべての IP ダイレクトブロードキャストがドロップされます。

ip directed-broadcast および **no ip directed-broadcast**

例

次に、イーサネットインターフェイス 2/1 上で IP ダイレクトブロードキャストの転送をイネーブルにする例を示します。

```
device# configure-transaction
device(config)# interface ethernet 2/1
device(config-if)# ip address 10.114.114.1 255.255.255.0
device(config-if)# ip directed-broadcast
device(config-if)# end
```



第 25 章

共有テンプレートから Cisco IOS XE SD-WAN テンプレートへの移行

概要

Cisco vManage 20.1.1 では、Cisco IOS XE SD-WAN デバイス専用の追加機能テンプレートのサポートが追加されています。

Cisco vManage 20.1.1 より前のリリースでは、Cisco vEdge デバイスと Cisco IOS XE SD-WAN デバイスの両方にテンプレートを作成した場合、同じテンプレートが両方のデバイスタイプで共有されていました。これらのテンプレートの場合、設定は Cisco vEdge コマンドを使用して指定されます。その後、テンプレートが Cisco IOS XE デバイスで使用される場合、設定は Cisco IOS XE デバイス用に変換されました。Cisco vEdge コマンドのこの変換により、一部の機能は Cisco IOS XE SD-WAN デバイスでは使用できませんでした。たとえば、NAT DIA です。

これらのリリースには、次の 2 種類の共有テンプレートがあります。

- 共有機能テンプレート：機能テンプレートの作成時に Cisco IOS XE SD-WAN デバイスを指定すると、共有機能テンプレートが作成されます。
- 共有デバイステンプレート：共有機能テンプレートを含むデバイステンプレート。

Cisco vManage 20.1.1 以降、機能テンプレートは Cisco vEdge デバイス用と Cisco IOS XE SD-WAN デバイス用に分けられています。Cisco IOS XE SD-WAN デバイス専用に作成されたこれらの機能テンプレートにより、追加機能のサポートが可能になります。これらの機能テンプレートを使用するには、共有機能テンプレートを専用テンプレートに移行します。

移行されたテンプレートのリスト

次の表に、Cisco vManage 20.1.1 以降で使用できる Cisco IOS XE SD-WAN デバイスの共有テンプレートとそれに対応する専用テンプレートを示します。

（注） AAA 機能テンプレートは、専用の Cisco IOS XE SD-WAN デバイス機能テンプレートではサポートされていません。

既存のテンプレートに AAA 機能テンプレートが含まれている場合は、移行前または移行後に置き換えることができます。

- 移行前：19.1 で導入された AAA-Cisco テンプレートに置き換えます。

  または
- 移行後：移行完了後、Cisco AAA テンプレートを手動で作成し、デバイステンプレートにアタッチします。

共有機能テンプレート	共有テンプレートタイプ	専用 Cisco IOS XE SD-WAN デバイス機能テンプレート	専用 Cisco IOS XE SD-WAN デバイス機能テンプレートタイプ
バナー	banner	Cisco バナー	cisco_banner
BFD	bfd-vedge	Cisco BFD	cisco_bfd
BGP	bgp	Cisco BGP	cisco_bgp
DHCP サーバ	dhcp-server	Cisco DHCP サーバー	cisco_dhcp_server
ログ	logging	Cisco ロギング	cisco_logging
NTP	ntp	Cisco NTP	cisco_ntp
OMP	omp-vedge	Cisco OMP	cisco_omp
OSPF	ospf	Cisco OSPF	cisco_ospf
セキュリティ	security-vedge	シスコのセキュリティ	cisco_security
SNMP	snmp	Cisco SNMP	cisco_snmp
システム	system-vedge	Cisco System	cisco_system
VPNインターフェイス GRE	vpn-vedge-interface-gre	Cisco VPN インターフェイス GRE	cisco_vpn_interface_gre
VPNインターフェイス IPsec	vpn-vedge-interface-ipsec	Cisco VPN インターフェイス IPsec	cisco_vpn_interface_ipsec
VPNインターフェイスイーサネット	vpn-vedge-interface	Cisco VPN インターフェイスイーサネット	cisco_vpn_interface
VPN	vpn-vedge	Cisco VPN	cisco_vpn

共有テンプレートの移行

古い共有テンプレートを引き続き使用できますが、共有テンプレートでは最新の機能にアクセスできない場合があります。最新の機能にアクセスできるように、既存のテンプレートを移行

することをお勧めします。たとえば、VPN インターフェイス イーサネット共有テンプレートを使用している場合、テンプレートは引き続き機能します。ただし、NAT DIA などの新機能を使用するには、Cisco VPN インターフェイス イーサネットと呼ばれる専用の機能テンプレートに移行する必要があります。

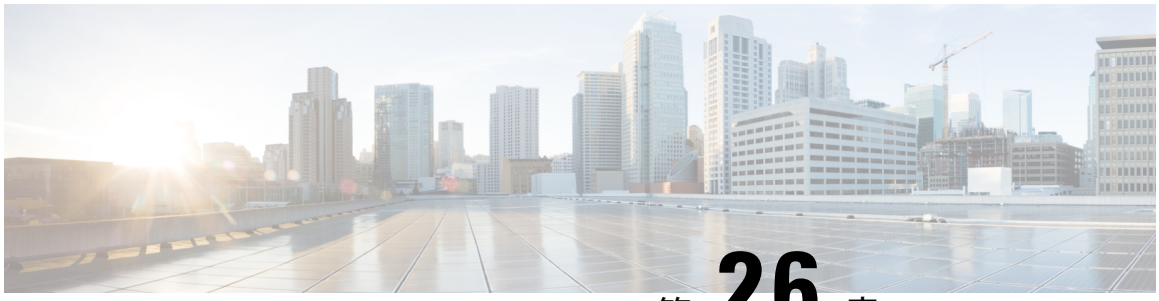
Cisco vManage 移行ツールを使用した共有テンプレートの移行

前提条件：

- Cisco vManage 20.1.1 またはそれ以上にアップグレードする前に、共有 Cisco IOS XE SD-WAN デバイス機能テンプレートがアタッチされた Cisco IOS XE SD-WAN デバイステンプレートが少なくとも 1 つ存在している必要があります。

Cisco vManage を使用して既存の共有テンプレートを移行するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Tools]** > **[Template Migration]** を選択します。
2. [Migrate All Templates] をクリックします。
3. 移行された新しいテンプレートのプレフィックスを入力します。たとえば、Migrated_ です。移行されたすべてのテンプレートには、この識別子がプレフィックスとして付けられます。
4. テンプレートを移行するには、[OK] をクリックします。
5. 移行が開始されたら、[Tasks] をクリックして移行のステータスを追跡します。
6. 移行が完了したら、移行したテンプレートをデバイスに手動でアタッチする必要があります。移行された各テンプレートについて、[...] をクリックし、[Attach Devices to Migrated Template] を選択します。



第 26 章

Cisco IOS XE SD-WAN ルータの CLI テンプレート

Cisco IOS XE SD-WAN デバイスの CLI テンプレートは、次の方法で設定できます。

（注） Cisco vManage の上位バージョンで CLI テンプレートを生成し、それを下位バージョンに適用しようとすると、構成によってはサポートされない場合があります。この場合、Cisco vManage はアクセスを拒否し、エラーメッセージを生成することもあります。Cisco vManage の以前のバージョンで生成された CLI テンプレートを使用することをお勧めします。たとえば、Cisco vManage リリース 20.7.x を使用している場合、Cisco vManage リリース 20.6.x 以前のリリースで生成された CLI テンプレートを使用できます。

- Cisco IOS XE SD-WAN デバイス のデバイス設定ベース CLI テンプレート （803 ページ）
- Cisco IOS XE SD-WAN ルータ用のインテントベースの CLI テンプレート （805 ページ）

Cisco IOS XE SD-WAN デバイス のデバイス設定ベース CLI テンプレート

Cisco vManage は、機能テンプレートとポリシー（ローカライズされたポリシー、セキュリティポリシー）の組み合わせを使用して Cisco IOS XE SD-WAN デバイス を設定します。Cisco vManage 20.1.1 以降では、Cisco vManage により、Cisco IOS XE SD-WAN デバイス でデバイス設定を使用する CLI テンプレートを指定できます。これらのテンプレートを使用して、デバイス設定（yang-cli）をデバイスに直接プッシュできます。

1 回の操作で、Cisco vManage は、デバイス設定とテンプレートでユーザーが指定した設定の相違部分を Cisco IOS XE SD-WAN デバイス に直接プッシュします。Cisco vManage は、他のテンプレートの場合と同様に、デバイスにプッシュする前に設定のプレビューも表示します。既述のワークフローは、テンプレートに対して追加、変更、または削除を行う場合にも適用されます。

（注） Cisco vManage を使用してアクセスできない機能を構成するには、次の手順を実行することをお勧めします。

1. CLI アドオン機能テンプレートに加えて、関連する機能テンプレートを使用します。詳細については、CLI アドオン機能テンプレートの認定 CLI （835 ページ）を参照してください。
2. 前のオプションでは不十分な場合は、このセクションで説明されているデバイス設定ベース CLI テンプレートを使用します。

Cisco XE SD-WAN ルータの CLI テンプレートに関する機能情報

表 *199* : 機能の履歴

機能名	リリース情報	説明
デバイス設定 CLI テンプレート	Cisco IOS XE リリース 17.2.1r Cisco vManage 20.1.1	CLI テンプレート機能は、デバイス設定ベースの CLI をサポートするように更新されました。これらのテンプレートを使用して、デバイス設定（yang-cli）をデバイスに直接プッシュできます。

制限事項

補助ポート：補助ポートを持つ Cisco サービス統合型ルータの CLI テンプレートを使用する場合は、補助ポート用のコマンド（**line aux 0** など）を含めないでください。そうした場合、エラーが発生します。これらのコマンドは、デバイス上で直接実行できます。

コマンド `show sdwan running-config` を使用して CLI テンプレート設定をインポートする場合は、Cisco vManage 上の CLI テンプレートの引用符を手動で追加する必要があります。

Cisco vManage での CLI テンプレートの設定

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、[CLI 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. [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。
6. [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。
7. [Device configuration] を選択します。このオプションを使用すると、`show sdwan running-config` コマンドの出力に表示される IOS-XE 設定コマンドを指定できます。
8. （オプション）接続されたデバイスの実行構成をロードするには、[Load Running config from reachable device] リストから選択し、[Search] をクリックします。
9. [CLI Configuration] で、手入力するか、カットアンドペーストするか、ファイルをアップロードして、設定を入力します。
10. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。{{*variable-name*}}; の形式で変数名を直接入力することもできます。たとえば、{{hostname}} です。

    これらの変数は、テンプレートをアタッチした後、デバイスごとにデバイス変数ページに入力できます。値は手入力するか、CSV ファイル使用してアップロードできます。
11. 機能テンプレートを保存するには、[Add] をクリックします。新しいデバイステンプレートが [Device Template] テーブルに表示されます。

Cisco IOS XE SD-WAN ルータ用のインテントベースの CLI テンプレート

Cisco IOS XE SD-WAN デバイス の CLI テンプレート機能により、Cisco vManage を使用して、Cisco IOS XE SD-WAN デバイス のインテントベースの CLI テンプレートを設定できます。インテントベースの CLI テンプレートは、Cisco vEdge デバイスの構文に基づくコマンド ライン インターフェイス設定を参照します。CLI テンプレートを使用して、Cisco vManage では Cisco vEdge 構文ベースのコマンドを Cisco IOS XE 構文の Cisco IOS XE SD-WAN デバイス にプッシュできるようになります。

（注） デバイス設定ベースの CLI テンプレートのサポートにより、インテントベースの CLI テンプレートは廃止されます。Cisco IOS XE SD-WAN デバイス のデバイス設定ベース CLI テンプレート （803 ページ）で説明されているように、デバイス設定ベースの CLI テンプレートを使用することをお勧めします。

Cisco vManage CLI テンプレートを使用すると、機能テンプレートを設定する手間が大幅に削減されます。

Cisco XE SD-WAN ルータの CLI テンプレートに関する機能情報

表 *200 :* 機能の履歴

機能名	リリース情報	説明
Cisco XE SD-WAN ルータの CLI テンプレート	Cisco IOS XE リリース 16.11.1a Cisco SD-WAN リリース 19.1	Cisco XE SD-WAN ルータの CLIテンプレート機能により、vManage を使用して Cisco XE SD-WAN ルータのインテントベースの CLI テンプレートを設定できます。
VRF 設定	Cisco IOS XE リリース 17.2.1r	VRF設定のサポートが合計100から合計 300 VRF に増加しました。サポート対象：Cisco ASR 1001-HX および Cisco ASR 1002-HX

CLI テンプレートの利点

- Cisco IOS XE ルータ用の Cisco vEdge 固有の vManage 機能テンプレートを再利用できます。Cisco XE SDWAN 機能テンプレートを使用してデバイステンプレートを作成すると、vManage はインテントベースの設定（vEdge CLI 構文）と対応するデバイスベース（Cisco XE SDWAN ルータ）の設定を表示します。インテントベースの設定を調べて、それを再利用して、XE SDWAN ルータ用の個別の CLI テンプレートを作成できます。
- 1 回の編集で CLI テンプレートに複数の変更を加えることができます。
- 同じデバイスモデルの複数のデバイスで 1 つの設定を使用できます。変数はデバイスごとに固有の設定を使用した一括設定の迅速な展開に使用することができます。システム IP、サイト ID、ホスト名、IP アドレスなどの一般的な設定は、テンプレートで編集可能な変数として定義でき、同じテンプレートを複数のデバイスにアタッチできます。
- CLI テンプレートで変数のカスタム長を定義できます。
- CLI テンプレートの入力として、既存の IOS-XE デバイスインテント設定を使用できます。
- CLI テンプレートのコンテンツは、複数の IOS-XE デバイスタイプ（VPN、VPN インターフェイス、BGP、OSPF などの一般的な CLI）で使用できます。

制限事項

補助ポート：補助ポートを持つ Cisco サービス統合型ルータの CLI テンプレートを使用する場合は、補助ポート用のコマンド（**line aux 0** など）を含めないでください。そうした場合、エラーが発生します。これらのコマンドは、デバイス上で直接実行できます。

Cisco vManage での CLI テンプレートの設定

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] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[CLI 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. [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。
6. [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。
7. CLI テンプレートの設定は、インテントベースまたはデバイス設定に基づくことができます。
   - [Intent]：[Intent] を指定する場合は、Cisco vEdge 形式でコマンドを指定します。選択したデバイスが Cisco IOS XE SD-WAN デバイス の場合、Cisco vManage はデバイスの設定を変換します。
   - [Device configuration]：このオプションは、Cisco IOS XE リリース 17.2.1r 以降で、Cisco IOS XE SD-WAN デバイス でのみ使用できます。このオプションでは、`show sd-wan running config` に表示されるデバイス設定全体を指定する必要があります。

（注） この機能は、CLI アドオン機能テンプレートの認定 CLI（835 ページ）で詳しく説明されている認定 CLI でのみ使用できます。

[Select a File] を使用して設定ファイルをアップロードするか、CLI 設定をコピーして貼り付けることができます。以下は、変数を使用したインテントベースの CLI の例です。

```
system

   host-name {{hostname}}
   system-ip {{system_ip}}
   domain-id 1

   site-id {{site_id}}
   port-offset           1
   admin-tech-on-failure
   organization-name "XYZ"
   logging
    disk
```

```
    enable
! !
```

これらの変数は、テンプレートをアタッチした後、デバイスごとにデバイス変数ページに入力できます。値は手入力するか、CSV ファイル使用してアップロードできます。

8. 機能テンプレートを保存するには、[Add] をクリックします。

（注） デバイスをテンプレートにアタッチし、同じデバイスモデルの複数のデバイスにテンプレートを再利用する方法の詳細については、このトピックの、デバイステンプレートへのデバイスの接続のセクションを参照してください。

CLI テンプレートのサンプル設定

システムレベルの設定

表 *201 :* システムレベルのパラメータ

CLI テンプレート設定	デバイスの設定
system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346	system host-name pm4 system-ip 172.16.255.14 overlay-id 1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name “XYZ Inc Regression” organization-name “XYZ Inc Regression” console-baud-rate 11520 vbond 10.0.12.26 port 12346

AAA 設定：RADIUS および TACACS+ を使用した認証、許可、およびアカウンティング（AAA）

表 *202 : AAA* 設定

CLI テンプレート設定	デバイスの設定

aaa
 auth- order local radius tacacs
 usergroup basic
 	
 task system read write
 task interface read write
!
 	
usergroup netadmin
!
 	
usergroup operator
task system read
task interface read
task policy read
task routing read
task security read
!
user admin password
 	
6nbbLkA==$ae/DO78l/wluPUohhBU2L6h/
Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F
MW57vuEHvo3zp3qdYVinLmMIu/p/
secret
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiLMOFQfD.QPAmMxDdxz.c
 	
! !
radius
 	
 server 10.99.144.200
  source-interface GigabitEthernet0/0/1
 exit
 server 10.99.144.201
 	
  source-interface GigabitEthernet0/1/0
 exit
!
tacacs
 	
 server 10.0.1.1
  auth-port 50
 	
  vpn 0
 	
  source-interface GigabitEthernet0/0/1
 	
  key 1
 	
  secret-key
8Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrpCg=
 	
 exit !
!
	aaa group server tacacs+ server-10.0.1.1
	  server-private 10.0.1.1 timeout 5 key
	8vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=
	
	 ip tacacs source-interface
	GigabitEthernet0/0/1
	!
	aaa group server radius server-10.99.144.200
	
	 server-private 10.99.144.200 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/0/1
	!
	
	aaa group server radius server-10.99.144.201
	
	 server-private 10.99.144.201 auth-port 1812
	 timeout 5 retransmit 3
	 ip radius source-interface
	GigabitEthernet0/1/0
	!
	aaa authentication login default local group
	 radius group tacacs+
	aaa authorization exec default local group
	radius group tacacs+ a
	aa session-id common --- added by default
	
	username admin privilege 15 secret 9
	$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiLMOFQfD.QPAmMxDdxz.c

ロギングの設定：ローカルハードドライブまたはリモートホストへのロギングを設定します

表 *203 :* ロギングの設定

CLI テンプレート設定	デバイスの設定
logging disk enable file size 12 file rotate 6 ! server 192.168.13.1 vpn 0 source-interface Loopback1 priority alert exit !	logging disk enable ! ! logging persistent size 75497472 filesize 12582912 logging buffered 512000 --- added by default logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent

スイッチポートと VLAN の設定

表 *204 :* スイッチ ポートの設定

CLI テンプレート設定	デバイスの設定
interface GigabitEthernet0/1/4 switchport mode trunk access vlan vlan 10 access vlan name "DHCP Vlan" trunk allowed vlan 10 ! no shutdown vpn 10 name "DHCP VPN" interface Vlan10 description "Vlan 10 Mgmt interface" ip address 10.29.35.1/24 no shutdown ! !	interface GigabitEthernet0/1/4 switchport ios-sw:mode trunk switchport ios-sw:trunk allowed vlan 10 no shutdown no ip address exit interface Vlan10 description Vlan 10 Mgmt interface no shutdown arp timeout 1200 vrf forwarding 10 ip address 10.29.35.1 255.255.255.0 ip mtu 1500 exit

セルラーの設定

表 *205 :* セルラーの設定：セルラーコントローラとセルラーインターフェイスを設定します

CLI テンプレート設定	デバイスの設定

vpn 0
  interface Cellular0/2/0
  description "Cellular interface"
  no shutdown
  !
 	
  controller cellular 0/2/0
  lte sim max-retry 1
  lte failovertimer 7
  profile id 1 apn Broadband
  !
	interface Cellular0/2/0
	  description Cellular interface
	  no shutdown
	  ip address negotiated
	  ip mtu 1428
	  mtu 1500
	  exit
	
	  controller Cellular 0/2/0
	  lte sim max-retry 1
	  lte failovertimer 7
	  profile id 1 apn Broadband authentication none pdn-type ipv4

BGP、**OSPF**、および **EIGRP**：トランスポートまたはサービス **VPN** で **BGP**、**OSPF**、および **EIGRP** ルーティングプロトコルを設定します

表 *206 : BGP*、*OSPF* および *EIGRP* の設定

CLI テンプレート設定	デバイスの設定

CLI テンプレート設定	デバイスの設定

vpn1
  bgp 2
     shutdown
     distance external 30
     distance internal 250
     distance local 10
     address-family ipv4-unicast
      network 10.0.100.0/24
      redistribute static route-policy
route_map
      redistribute connected route-policy
route_map
     !
     neighbor 10.0.100.1
      no shutdown
      remote-as   3
      timers
       keepalive   12
       holdtime   20
       connect-retry   300
       advertisement-interval 123
      !
      update-source GigabitEthernet0/0/1
      ebgp-multihop 1
      password
$8$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=
 	
      address-family ipv4-unicast
 	
vpn 1
   router
    ospf
     router-id 172.16.255.15
     compatible rfc1583
     timers spf 200 1000 10000
     redistribute connected route-policy
route_map
     max-metric router-lsa administrative
     area 23
      stub
      interface GigabitEthernet0/0/1
       cost 23
       authentication type message-digest
       authentication authentication-key
key1
      exit
     exit
    !
 	
vpn 1
 router
  eigrp 1
   af-interface GigabitEthernet0/0/2
   no split-horizon
   exit-af-interface
  !
 address-family ipv4 network 10.1.10.1/32
 address-family ipv4 topology base
 redistribute omp
 exit-af-topology	

CLI テンプレート設定	デバイスの設定
	router bgp 2 bgp log-neighbor-changes distance bgp 30 250 10 address-family ipv4 unicast vrf 1 neighbor 10.0.100.1 remote-as 3 neighbor 10.0.100.1 activate neighbor 10.0.100.1 ebgp-multihop 1 neighbor 10.0.100.1 maximum-prefix 2147483647 100 neighbor 10.0.100.1 password 0 password neighbor 10.0.100.1 send-community both neighbor 10.0.100.1 timers 12 20 neighbor 10.0.100.1 update-source GigabitEthernet0/0/1 network 10.0.100.0 mask 255.255.255.0 redistribute connected redistribute static route-map route_map exit-address-family ! timers bgp 60 180 router ospf 1 vrf 1 auto-cost reference-bandwidth 100 max-metric router-lsa timers throttle spf 200 1000 10000 router-id 172.16.255.15 default-information originate distance ospf external 110 distance ospf inter-area 110 distance ospf intra-area 110 redistribute connected subnets route-map route_map ! interface GigabitEthernet0/0/1 no shutdown arp timeout 1200 vrf forwarding 1 ip address 10.1.100.14 255.255.255.0 ip redirects ip mtu 1500 ip ospf 1 area 23 ip ospf network broadcast mtu 1500 negotiation auto exit ! router eigrp eigrp-name address-family ipv4 vrf 1 autonomous-system 1 af-interface GigabitEthernet0/0/2 hello-interval 5 hold-time 15 no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0 topology base redistribute omp

CLI テンプレート設定	デバイスの設定
	exit-af-topology ! exit-address-family ! !

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

表 *207 : VPN*、インターフェイス、およびトンネルの設定

CLI テンプレート設定	デバイスの設定

vpn 0
  interface GigabitEthernet0/2/0
  ip address 10.1.14.14/24
  tunnel-interface
  encapsulation ipsec
  color lte
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  !
  autonegotiate
  no shutdown
  !
  ip route 0.0.0.0/0 10.1.14.13
 	
vpn 512
interface GigabitEthernet0
  ip dhcp-client
ipv6 dhcp-client autonegotiate
no shutdown
! !
	ip route 0.0.0.0 0.0.0.0 10.1.14.13 1
	
	interface GigabitEthernet0/2/0
	  no shutdown
	  arp timeout 1200 - added by default
	  ip address 10.1.14.14 255.255.255.0
	  ip redirects --> added by default
	  ip mtu 1500
	  mtu 1500
	  negotiation auto --> added by default
	  exit
	
	interface Tunnel20 ---> based on the
	interface 0/2/0
	  no shutdown
	  ip unnumbered GigabitEthernet0/2/0
	  no ip redirects
	  ipv6 unnumbered GigabitEthernet0/2/0
	  no ipv6 redirects
	  tunnel source GigabitEthernet0/2/0
	  tunnel mode sdwan
	
	sdwan
	  interface GigabitEthernet0/2/0
	  tunnel-interface
	  encapsulation ipsec weight 1
	  color lte
	  no last-resort-circuit
	  vmanage-connection-preference 5
	  no allow-service all
	  no allow-service bgp
	  allow-service dhcp
	  allow-service dns
	  allow-service icmp
	  no allow-service sshd
	  no allow-service netconf
	  no allow-service ntp
	  no allow-service ospf
	  no allow-service stun
	
	interface GigabitEthernet0
	no shutdown
	arp timeout 1200
	vrf forwarding Mgmt-intf
	ip address dhcp client-id GigabitEthernet0
	ip redirects
	ip dhcp client default-router distance 1 ip
	  mtu 1500
	mtu 1500
	negotiation auto

ダイレクト インターネット アクセス（DIA）経由のネットワークアドレス変換（NAT）

表 *208 : DIA* 経由の *NAT*

CLI テンプレート設定	デバイスの設定
vpn 201 interface GigabitEthernet0/0/2.2901 description gigi21 ip address 10.201.201.1/24 mtu 1496 no shutdown vrrp 100 track-omp ipv4 10.201.201.3 ! ! ! dhcp-server address-pool 10.201.201.0/24 exclude 10.201.201.1-10.201.201.10 10.201.201.20-10.201.201.22 offer-time 600 lease-time 86400 admin-state up options default-gateway 10.201.201.1 dns-servers 10.99.139.201 tftp-servers 10.99.139.201 ! ! ! ip route 0.0.0.0/0 vpn 0 ! vpn 0 interface GigabitEthernet0/0/0 ip address 172.16.10.1/24 nat udp-timeout 3 tcp-timeout 40 respond-to-ping ! !	interface GigabitEthernet0/0/2.2901 no shutdown encapsulation dot1Q 2901 vrf forwarding 201 ip address 10.201.201.1 255.255.255.0 ip mtu 1496 vrrp 100 address-family ipv4 vrrpv2 address 10.201.201.3 priority 100 track omp shutdown exit exit ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901 option 150 ip 10.99.139.201 vrf 201 lease 1 0 0 default-router 10.201.201.1 dns-server 10.99.139.201 network 10.201.201.0 255.255.255.0 exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload ip nat translation tcp-timeout 40 ip nat translation udp-timeout 3 ip nat route vrf 201 0.0.0.0 0.0.0.0 global interface GigabitEthernet1/0/2 no shutdown arp timeout 1200 ip address 10.1.15.15 255.255.255.0 ip nat outside ip redirects ip mtu 1500 mtu 1500 negotiation auto

NAT64 の設定

表 *209 : NAT64* の設定

vpn 1
  nat64
  v4 pool pool1 start-address 10.1.1.10
  v4 pool pool1 end-address 10.1.1.100
  !
  interface GigabitEthernet3
  ip address 10.1.19.15/24
  nat64
  !
  autonegotiate
  no shutdown
  !
	interface GigabitEthernet3
	  no shutdown
	  arp timeout 1200
	  vrf forwarding 1
	  ip address 10.1.19.15 255.255.255.0
	  negotiation auto
	  nat64 enable
	  nat64 prefix stateful 2001::F/64 vrf 1
	
	  nat64 v4 pool pool1 10.1.1.10 10.1.1.100
	  nat64 v6v4 list global-list pool pool1 vrf
	  1
	  nat64 translation timeout tcp 60
	  nat64 translation timeout udp 1

マルチリンクおよび T1/E1：T1/E1 コントローラおよびシリアル、マルチリンク インターフェイスを設定します

表 *210 :* マルチリンクの設定

CLI テンプレート設定	デバイスの設定

card type t1 0 2
  controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  cablelength long 0db
  channel-group 1 timeslots 15
  channel-group 2 timeslots 12
  channel-group 3 timeslots 10
  channel-group 4 timeslots 10
!
interface Multilink1
  no shutdown
  encapsulation ppp
  ip address 10.1.10.30 255.255.255.0
  ppp pap sent-username admin password admin
  ppp authentication pap
  ppp multilink
  ppp multilink links minimum 1
  ppp multilink fragment disable
  ppp multilink group 1
exit
interface Serial0/2/0:1
  no shutdown
  encapsulation ppp
  bandwidth 1536
  no ip address
  load-interval 30
  ppp pap sent-username admin password admin
  ppp authentication pap
  ppp multilink
  ppp multilink group 1
exit
	interface Multilink1
	ip address 10.1.10.30/24 shutdown
	controller T1 0/2/0
	  linecode b8zs
	  channel-group 1
	  channel-group 3
	!
	ppp pap sent-username admin password admin
	ppp authentication pap
	ppp multilink
	ppp multilink group 1

ローカル QoS ポリシー

表 *211 :* ローカル *QoS* ポリシー

CLI テンプレート設定	デバイスの設定

CLI テンプレート設定	デバイスの設定
vpn 1 interface GigabitEthernet0/0/1 ip address 10.2.54.15/24 no shutdown access-list MyACL in ! policy class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 ! ! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! ! sequence 40 action accept class best-effort set dscp 0 ! ! ! default-action accept ! qos-scheduler be-scheduler class best-effort bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler bulk-scheduler	interface GigabitEthernet0/0/1 access-list MyACL in exit class-map match-any best-effort match qos-group 3 ! class-map match-any bulk-data match qos-group 2 ! class-map match-any critical-data match qos-group 1 ! class-map match-any voice match qos-group 0 ! policy-map MyQoSMap class best-effort random-detect bandwidth percent 20 ! class bulk-data random-detect bandwidth percent 20 ! class critical-data random-detect bandwidth percent 40 ! class voice priority percent 20 ! ! policy no app-visibility no flow-visibility no implicit-acl-logging log-frequency 1000 class-map class best-effort queue 3 class bulk-data queue 2 class critical-data queue 1 class voice queue 0 ! access-list MyACL sequence 10 match dscp 46 ! action accept class voice ! ! sequence 20 match source-ip 10.1.1.0/24 destination-ip 192.168.10.0/24 ! action accept class bulk-data set dscp 32 !

CLI テンプレート設定	デバイスの設定
class bulk-data bandwidth-percent 20 buffer-percent 20 drops red-drop ! qos-scheduler critical-scheduler class critical-data bandwidth-percent 40 buffer-percent 40 drops red-drop ! qos-scheduler voice-scheduler class voice bandwidth-percent 20 buffer-percent 20 scheduling llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! !	! ! sequence 30 match destination-ip 192.168.20.0/24 ! action accept class critical-data set dscp 22 ! ! sequence 40 action accept class best-effort set dscp 0 ! ! default-action accept ! ! ! !

セキュリティポリシー（ZBFW、IPS/IDS、URL フィルタリング）の設定

表 *212 :* セキュリティポリシー（*ZBFW*、*IPS/IDS*、*URL* フィルタリング）

CLI テンプレート設定	デバイスの設定
policy zone internet vpn 0 ! zone zone1 vpn 1 ! zone zone2 vpn 2 ! zone-pair ZP_zone1_internet_fw_policy source-zone zone1 destination-zone internet zone-policy fw_policy ! zone-pair ZP_zone1_zone2_fw_policy source-zone zone1 destination-zone zone2 zone-policy fw_policy ! zone-based-policy fw_policy sequence 1 match source-data-prefix-list subnet1 ! action inspect ! ! default-action pass ! zone-to-nozone-internet deny lists data-prefix-list subnet1 ip-prefix 10.0.10.0/24 ! ! url-filtering url_filter web-category-action block web-categories games block-threshold moderate-risk block text "<![CDATA[<h3>Access" to the requested page has been denied]]>" target-vpns 1 ! intrusion-prevention intrusion_policy security-level connectivity inspection-mode protection log-level err target-vpns 1 ! failure-mode open ! ! !	

CLI テンプレート設定	デバイスの設定
	ip access-list extended fw_policy-seq-1-acl_ 11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_ match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy class fw_policy-seq-1-cm_ inspect ! class class-default pass ! ! object-group service fw_policy-seq-1-service-og_ ip ! parameter-map type inspect-global alert on log dropped-packets multi-tenancy vpn zone security ! parameter-map type umbrella global token A5EA676087BF66A42DC4F722C2AFD10D00256274 dnscrypt vrf 1 dns-resolver umbrella match-local-domain-to-bypass ! ! zone security internet vpn 0 ! zone security zone1 vpn 1 ! zone security zone2 vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2 service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0

CLI テンプレート設定	デバイスの設定

	guest-interface 0
	  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
	 !
	 app-vnic gateway1 virtualportgroup 1 guest-interface 1
	  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
	 !
	 start
	 !
	 utd multi-tenancy
	 utd engine standard multi-tenancy
	  web-filter block page profile block-url_filter
	  text <\![CDATA[Access to the requested page has been denied Please contact your Network Administrator]]>
	 !
	 web-filter url profile url_filter
	  categories block
	  games
	  !
	  block page-profile block-url_filter
	  log level error
	  reputation
	  block-threshold moderate-risk
	  !
	 !
	 threat-inspection profile intrusion_policy
	
	  threat protection
	  policy connectivity
	  logging level err
	 !
	 utd global
	 !
	 policy utd-policy-vrf-1
	  all-interfaces
	  vrf 1
	  threat-inspection profile intrusion_policy
	  web-filter url profile url_filter
	 exit
	 !

NTP の設定

表 *213 : NTP* の設定

CLI テンプレート設定	デバイスの設定
ntp server 10.29.43.1 source-interface GigabitEthernet1 version 4 exit ! !	ntp server 198.51.241.229 source GigabitEthernet1 version 4

IPv6 設定

表 *214 : IPv6* 設定

CLI テンプレートの設定	デバイスの設定
vpn 1 interface GigabitEthernet3 ipv6 address 2671:123A::1/128 shutdown ! !	interface GigabitEthernet3 shutdown arp timeout 1200 vrf forwarding 1 no ip address ip redirects ip mtu 1500 ipv6 address 2671:123A::1/128 ipv6 redirects mtu 1500 negotiation auto exit vrf definition 1 rd 1:1 address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! !

サービス構成

Cisco IOS XE リリース 17.7.1a 以前は、CLI テンプレートを介して設定できるのは、**service** の下の次の設定のみです。

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

no service password-recovery コマンドは、Cisco vManage からデバイスにプッシュできません。

VRF 設定

各 VRF に対応するサブインターフェイスを使用して、最大 300 の VRF を設定します。この例では、2 つの VRF を設定します。

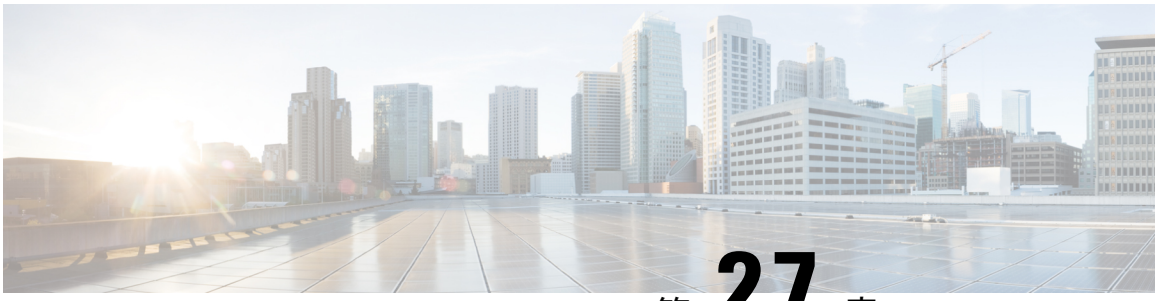
（注） VLAN 1 は設定しないでください。ネイティブ VLAN 用に予約されています。

CLI テンプレート設定	デバイスの設定
! vpn 2 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.2.2 no shutdown remote-as 2 ! ipv6-neighbor 2001:DB8:2::2 remote-as 2 ! ! interface GigabitEthernet0/0/0.2 ip address 192.0.2.1/24 ipv6 address 2001: DB8:2::1/64 mtu 1496 no shutdown ! ! vpn 3 router bgp 1000 address-family ipv4-unicast redistribute omp address-family ipv6-unicast redistribute omp ! neighbor 192.0.3.2 no shutdown remote-as 3 ! ipv6-neighbor 2001: DB8:3::2 remote-as 3 ! ! interface GigabitEthernet0/0/0.3 ip address 192.0.3.1/24 ipv6 address 2001: DB8:3::1/64 mtu 1496 no shutdown !	

CLI テンプレート設定	デバイスの設定

	vrf definition 2
	rd 1:2
	address-family ipv4
	  route-target export 1000:2
	  route-target import 1000:2
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 2
	  redistribute omp
	  neighbor 192.0.2.2 remote-as 2
	  neighbor 192.0.2.2 activate
	  neighbor 192.0.2.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 2
	  redistribute omp
	  neighbor 2001:DB8:2::2 remote-as 2
	  neighbor 2001: DB8:2::2 activate
	  neighbor 2001: DB8:2::2 send-community
	both
	exit-address-family
	!
	interface GigabitEthernet0/0/0.2
	encapsulation dot1Q 2
	vrf forwarding 2
	ip address 192.0.2.1 255.255.255.0
	ip mtu 1496
	ipv6 address 2001:DB8:2::1/64
	end
	
	vrf definition 3
	rd 1:3
	address-family ipv4
	  route-target export 1000:3
	  route-target import 1000:3
	  exit-address-family
	!
	address-family ipv6
	  exit-address-family
	!
	!
	router bgp 1000
	bgp log-neighbor-changes
	distance bgp 20 200 20
	!
	address-family ipv4 vrf 3
	  redistribute omp
	  neighbor 192.0.3.2 remote-as 3
	  neighbor 192.0.3.2 activate
	  neighbor 192.0.3.2 send-community both
	exit-address-family
	!
	address-family ipv6 vrf 3
	  redistribute omp

CLI テンプレート設定	デバイスの設定
	neighbor 2001:DB8:3::2 remote-as 3 neighbor 2001: DB8:3::2 activate neighbor 2001: DB8:3::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.3 encapsulation dot1Q 3 vrf forwarding 3 ip address 192.0.3.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:3::1/64 end



第 27 章

CLI アドオン機能テンプレート

表 *215 :* 機能の履歴（表）

機能名	リリース情報	説明
CLI アドオン機能テンプレート	Cisco IOS XE リリース 17.2.1r Cisco vManage 20.1.1	この機能により、CLI アドオン機能テンプレートと呼ばれる新しい機能テンプレートが追加されます。この機能テンプレートを使用して、特定の CLI 設定をデバイスにアタッチできます。Cisco vManage を使用して設定を指定できないが、デバイスの CLI を使用して設定できる場合は、この機能テンプレートを使用してそのような設定を指定できます。また、CLI アドオン機能テンプレートを使用して、実行コンフィギュレーション全体ではなく、CLI 設定の一部を追加することもできます。 この機能は、既存の機能テンプレートを置き換えるものではなく、その機能を強化することを目的としています。すべての CLI が認定されているわけではないことに注意してください。詳細については、『Qualified CLIs for Cisco IOS XE Release 17.2.1r』を参照してください。

機能名	リリース情報	説明
CLI アドオン機能テンプレートの認定されている追加コマンド	Cisco IOS XE リリース Amsterdam 17.2.1v Cisco SD-WAN リリース 20.1.12	リリースごとに、CLI アドオン機能テンプレート機能で使用するコマンドを認定しています。このリリースでは、追加のコマンドを認定しました。『Cisco IOS XE SD-WAN Qualified Command Reference』の「Appendix」を参照してください。

CLI アドオン機能テンプレートの概要

機能テンプレートと新しいCLIアドオン機能テンプレートの両方を含むデバイステンプレートをアタッチすると、設定がマージされます。マージでは、新しいCLIアドオン機能テンプレートが優先されます。Cisco vManageは最初に、機能テンプレートに基づいて構成を生成します。構成が生成されると、CLIアドオン機能テンプレートからの構成を使用して、以前に生成された機能テンプレートの構成出力にそれをマージします。したがって、この機能を使用すると、既存の機能テンプレートでは提供されない特定のデバイス構成を追加したり、既存の機能テンプレートの構成を上書きしたりできます。

テンプレートを使用してコマンドを指定する場合は、`show sdwan running-config`出力に表示される構文に従ってコマンドを使用します。テンプレートをデバイスにアタッチすると、Cisco vManage ではすべての機能テンプレートから情報が取得され、CLI アドオン機能テンプレートを使用して指定したデータも取得されて、デバイス構成が作成されます。CLIアドオン機能テンプレートで指定したコマンドは、対応する機能テンプレートの同等のコマンドを上書きします。

既存のコマンドの変更に加えて、CLI アドオン機能テンプレートを使用して、Cisco vManage では使用できないがデバイスに適したコマンドを指定することもできます。たとえば、Cisco AAA の場合、`attempts login`コマンドはCisco vManage で使用できません。CLI アドオン機能テンプレートを使用すると、デバイスに`aaa authentication sessions login` *`number`* コマンドを指定できます。機能テンプレートを作成したら、それをデバイステンプレートに追加してください。

（注） デバイステンプレートで使用する前に、CLI アドオン機能テンプレートを定義する必要があります。

認定されている CLI のリストについては、「Qualified CLIs for CLI Add-on Feature Templates」を参照してください。

CLI アドオン機能テンプレートの制約事項

CLI アドオン機能テンプレートを使用する場合、次の制限が適用されます。

- この機能は、Cisco IOS XE リリース 17.2.1r 以降を実行している Cisco IOS XE SD-WAN デバイス でのみサポートされています。
- デバイステンプレートごとに接続できる CLI アドオンテンプレートは 1 つだけです。
- `show sdwan running-config` コマンドの出力に表示される設定コマンドのみを使用するようにしてください。CLI アドオン機能テンプレートでコマンドを使用する前に、ログインして目的のデバイスでコマンドを実行し、コマンドを確認してください。
- 構成でサポートされていないコマンドを使用するとエラーが発生し、構成をデバイスにプッシュするときに失敗します。たとえば、「login local」はサポートされていないコマンドです。

  CLI アドオン機能テンプレートでの使用が認定されたコマンドのリリースごとのリストについては、「Qualified CLI Commands for CLI Add-on Feature templates」を参照してください。

CLI アドオン機能テンプレートの作成

CLI アドオン機能テンプレートを作成するには、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. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. [Select Devices] で、テンプレートを作成するデバイスを選択します。
4. [Select Template] で、[OTHER TEMPLATES] セクションまで下にスクロールします。

5. [CLI Add-On Template] をクリックします。
6. [Template Name] に、機能テンプレートの名前を入力します。

   このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
7. [Description] にデバイステンプレートの説明を入力します。

   このフィールドは必須であり、任意の文字とスペースを含めることができます。
8. [CLI Configuration] で、手入力するか、カットアンドペーストするか、ファイルをアップロードして、設定を入力します。
9. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。`{{variable-name}}` の形式で変数名を直接入力することもできます。例：`{{hostname}}`。
10. **[Save]** をクリックします。

    新しい機能テンプレートが [Feature Template] テーブルに表示されます。
11. CLI アドオン機能テンプレートを使用するには、デバイステンプレートを次のように編集します。
    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. CLI アドオン機能テンプレートを追加するデバイステンプレートを選択します。
    4. [...] をクリックし、[Edit] を選択します。
    5. [Additional Templates] までスクロールします。
    6. [CLI Add-On Template] から、以前に作成した CLI アドオン機能テンプレートを選択します。
    7. [更新（Update）] をクリックします。

（注） Cisco IOS XE リリース 17.7.x で、CLI テンプレートの作成中に次の CLI がテンプレートに表示されている場合は、テンプレートをデバイスにアタッチする前に、テンプレートから CLI を手動で削除してください。

licensing config enable false

licensing config privacy hostname false

licensing config privacy version false

licensing config utility utility-enable false

CLI アドオン機能テンプレートの認定 CLI

Cisco vManage CLI テンプレートでの使用が認定されている CLI コマンドのリリースごとのリストについては、『Cisco IOS XE SD-WAN Qualified Command Reference』の「Appendix」を参照してください。

第 28 章

Cisco SD-WAN EtherChannel

表 *216* : 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN EtherChannel	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、サービス側 VPN の Cisco IOS XE SD-WAN デバイス に EtherChannel を設定できます。 EtherChannel は、Cisco IOS XE SD-WAN デバイス と、ネットワークに接続されたルータ、スイッチ、サーバーなどの他のデバイスとの間のフォールトトレラントな高速リンク、冗長性、および帯域幅の増加を提供します。 CLI デバイステンプレートと CLI アドオン機能テンプレートを使用してのみ、EtherChannel を設定できます。

Cisco SD-WAN EtherChannel でサポートされるデバイス

次のプラットフォームは、サービス側 VPN で EtherChannel をサポートしています。

- **Cisco 4000 シリーズ サービス統合型ルータ**
  - Cisco 4451-X サービス統合型ルータ
  - Cisco 4461 サービス統合型ルータ
  - Cisco 4431 サービス統合型ルータ
  - Cisco 4331 サービス統合型ルータ
  - Cisco 4351 サービス統合型ルータ
- **Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ**
  - Cisco ASR 1001-X ルータ
  - Cisco ASR 1006-X ルータ
  - Cisco ASR 1001-HX ルータ
  - Cisco ASR 1002-HX ルータ
  - Cisco ASR 1002-X ルータ
- Cisco Catalyst 8000V Edge ソフトウェア
- Cisco Catalyst 8200 ルータ
- Cisco Catalyst 8300 ルータ
- Cisco Catalyst 8500 シリーズ エッジルータ

サポートされる NIM

サービス統合型ルータプラットフォームでは、次の NIM がサポートされています。

- NIM-1GE-CU-SFP
- NIM-2GE-CU-SFP
- SM-X-4x1G-1x10G
- SM-X-6X1G

（注） L2 ポートを備えたネットワーク インターフェイス モジュール（NIM）は、サービス側 VPN の EtherChannel をサポートしていません。

Cisco SD-WAN EtherChannel の前提条件

- 各 EtherChannel のすべての LAN ポートは同じ速度でなければなりません。
- すべての LAN ポートは、レイヤ 3 サービス側ポートで設定する必要があります。

Cisco SD-WAN EtherChannel の制約事項

- EtherChannel 機能は、サービス側 VPN でのみサポートされます。
- CLI を使用するか、CLI テンプレートまたは Cisco vManage の CLI アドオン機能テンプレートのみを使用して、デバイスに EtherChannel を設定できます。
- L2 ポートを備えたネットワーク インターフェイス モジュール（NIM）は、サービス側 VPN の EtherChannel をサポートしていません。
- ポートチャネルの EtherChannel Quality of Service（QoS）機能は、サービス側 VPN ではサポートされていません。
- ポートチャネルの集約 EtherChannel QoS EtherChannel Quality of Service 機能は、サービス側 VPN ではサポートされていません。
- EtherChannel は、デジタルシグナルプロセッサ（DSP）ファームサービスと音声サービスをサポートしていません。

Cisco SD-WAN EtherChannel の利点

- 耐障害性を提供します。EtherChannel のいずれかのリンクに障害が発生した場合、EtherChannel は残りのリンクにトラフィックを自動的に再配布します。
- Cisco IOS XE SD-WAN デバイス と、ネットワークに接続されているスイッチやサーバーなどの他のデバイスとの間の帯域幅を増やすのに役立ちます。

Cisco SD-WAN EtherChannel について

EtherChannel は、スイッチ、ルータ、およびサーバー間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリングクローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上の任意の場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。ポートチャネル インターフェイスに適用した設定変更は、チャネル グループにまとめてバインドされるすべての物理ポートに適用されます。

サービス側 VPN の EtherChannel

EtherChannel を作成するには、ポートチャネルを設定することから始めます。ポートチャネルは、Cisco IOS XE SD-WAN デバイス 上の論理インターフェイスです。EtherChannel の作成後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートにも適用されます。ポートチャネルインターフェイスでサポートされる最大範囲は 1 ～ 64 です。

次のいずれかの方法を使用して、EtherChannel を設定できます。

- リンク集約制御プロトコル（LACP）モード
- スタティック モード

  デバイスの両端でサポートされている場合は、LACP モードを使用して EtherChannel を設定します。いずれかのデバイスがLACPモードをサポートしていない場合は、固定モードを使用して EtherChannel を設定します。

LACP Mode

LACP を使用すると、イーサネットポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

次の表に、ユーザー側で設定可能な EtherChannel LACP モードを示します。

表 *217 : EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信するパケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

[active] モードと [passive] モードの両方で、ポートはポート速度に基づいてパートナーポートとネゴシエートできます。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive**モードの別のポートとともに EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、[passive] モードのポートは、[passive] モードの別のポートと EtherChannel を形成することはできません。

固定モード

グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用して、EtherChannel を手動で作成できます。その後、グローバル コンフィギュレーション モードで **channel-group interface** コマンドを使用して、EtherChannel にインターフェイスを割り当てます。EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネルインターフェイスに割り当てられたすべての物理ポートに適用されます。LACP モードとは異なり、固定モードでは、他のポートとのネゴシエーションのためにパケットが送信されません。代わりに、ポートを EtherChannel の一部として手動で設定する必要があります。

EtherChannel ロード バランシング

EtherChannel は、チャネルのリンク全体でトラフィックの負荷を分散させます。いくつかの異なるロードバランシングモードのいずれかを指定できます。EtherChannel は、動的なフローベースのロードバランシングか手動仮想 LAN（VLAN）ロードバランシングが使用されます。

すべてのポートチャネルに対してグローバルにロードバランシング方式を設定するか、特定のポートチャネルに直接設定できます。グローバル コンフィギュレーションは、ロード バランシングが明示的には設定されていないポート チャネルだけに適用されます。ポートチャネルの設定はグローバル コンフィギュレーションを上書きします。

Cisco IOS XE SD-WAN デバイス では、次のロードバランシング方式がサポートされています。

- フローベース

  VLAN ベース

フローベースのロード バランシング

フローベースのロードバランシングはデフォルトのロードバランシング方式で、グローバルレベルでデフォルトで有効になっています。フローベースのロード バランシングは、データ パケットのキーフィールドに基づいてトラフィックのさまざまなフローを識別します。フローを識別するために、たとえば、IPv4 送信元および宛先 IP アドレスを使用できます。次に、さまざまなデータ トラフィックがポート チャネルの異なるメンバー リンクにマッピングされます。マッピングが完了したら、フローのデータ トラフィックは、割り当てられたメンバー リンクを通じて送信されます。フロー マッピングは動的で、フローが割り当てられたメンバー リンクの状態が変わったときに変更されます。メンバーリンクが追加または削除されると、フローマッピングは動的になります。

VLAN ベースのロードバランシング

VLAN ベースのロードバランシングを使用すると、EtherChannel の特定のメンバーリンクに VLAN ID で識別されるユーザートラフィックのスタティックな割り当てを設定することができます。プライマリおよびセカンダリ リンクに手動で VLAN サブインターフェイスを割り当

てることができます。この機能は、ベンダー機器の能力に関係なく、ダウンストリーム機器へのロード バランシングを可能にし、プライマリ リンクに障害が発生すると、トラフィックをセカンダリ メンバー リンクにリダイレクトすることでフェールオーバー保護を提供します。シャーシあたり最大 16 バンドルでメンバー リンクがサポートされます。

Cisco SD-WAN EtherChannel の使用例

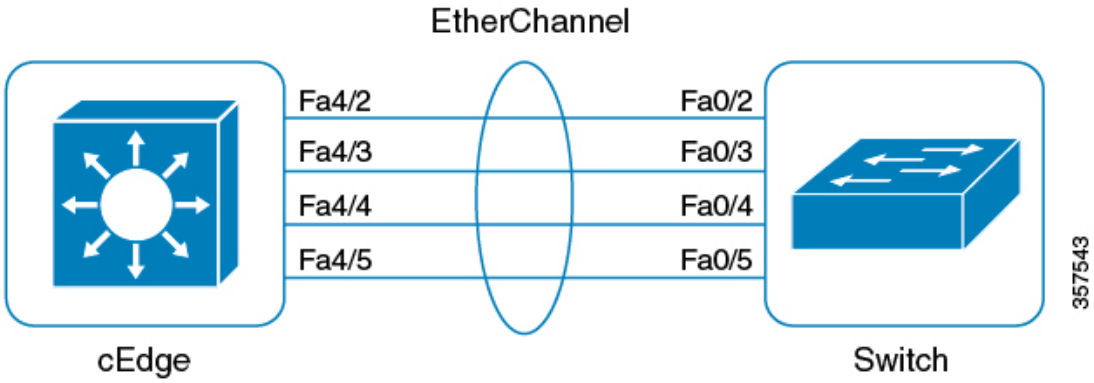
Etherchannel は、ネットワークの帯域幅と耐障害性を向上させるため、サービス側の VPN 構成に使用できます。

帯域幅の増加

EtherChannel を使用すると、複数のリンクを 1 つの論理リンクに統合できます。EtherChannel はリンクの冗長性を提供するため、EtherChannel を設定してネットワークの速度を上げることができます。

耐障害性の向上

EtherChannel は、ネットワークの耐障害性も提供します。EtherChannel 内のリンクで障害が発生した場合でも、障害リンク上でそれまで伝送されていたトラフィックが EtherChannel 内の他のリンクに切り替えられます。このため、EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。



Cisco SD-WAN EtherChannel の設定

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. [Create Template] ドロップダウンから、[CLI Template] を選択します。

（注） CLI アドオンテンプレートを使用して、EtherChannel を設定することもできます。詳細については、「Create a CLI Add-On Feature Template」を参照してください。

4. [Device Model] から、テンプレートを作成するデバイスモデルを選択します。
5. [Template Name] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
6. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
7. [CLI Configuration] フィールドで、手入力するか、カットアンドペーストするか、ファイルをアップロードして、EtherChannel 設定を入力します。
8. [Save] をクリックします。

CLI を使用した Cisco SD-WAN EtherChannel の設定

このセクションでは、CLI を使用して Cisco SD-WAN EtherChannel を設定するためのサンプル CLI 設定について説明します。

1. レイヤ 3 ポートチャネルを設定します。

```
Device# config-transaction
Device(config)# interface Port-channel channel-number
Device(config-if)# ip address ip-address mask
```

2. インターフェイスをレイヤ 3 ポートチャネルに割り当てます。

LACP EtherChannel の設定

```
Device# config-transaction
Device(config)# interface GigabitEthernet slot/subslot/port
Device(config-if)# no ip address
Device(config-if)# channel-group channel-group-number mode {active passive}
Device(config-if)# exit

Device# config-transaction
Device(config)# lacp system-priority priority
Device(config)# interface GigabitEthernet slot/subslot/port
Device(config-if)# lacp port-priority priority
```

静的 EtherChannel の設定

```
Device# config-transaction
Device(config)# interface GigabitEthernet slot/subslot/port
Device(config-if)# no ip address
Device(config-if)# channel-group channel-group-number
```

ロード バランシングの設定

ポートチャネルごとにフローベースのロードバランシングを有効にする

```
Device(config)# interface Port-channel channel-number
Device(config-if)#load-balancing flow
```

フローベースのロードバランシングのハッシュアルゴリズム

```
Device(config)# port-channel load-balance-hash-algo {dst-ip dst-mac
src-dst-ip src-dst-mac  src-dst-mixed-ip-port src-ip src-mac}
```

（注） フローベース ロード バランシングのデフォルトのハッシュアルゴリズムは **src-dst-ip** です。

（注） **フローベースのロードバランシングのハッシュアルゴリズム**機能は、Etherchannel のハードウェア ロード バランシングがサポートされている Cisco アグリゲーション サービス ルータ プラットフォームでのみサポートされます。このコマンドは、Cisco サービス統合型ルータおよび Cisco Catalyst ルータプラットフォームではサポートされていません。

VLAN ID に基づく手動トラフィック分散

```
Device(config)# port-channel load-balancing vlan-manual
```

（注） このコマンドは、グローバル コンフィギュレーション モードでの設定に使用でき、デバイスに設定されているすべてのポートチャネルに適用されます。

ポートチャネルごとの VLAN ロードバランシングの有効化

```
Device(config)# interface Port-channel channel-number
Device(config-if)#load-balancing vlan
```

VLAN ロードバランシングの設定例

```
Device# config-transaction
Device(config)# interface Port-channel channel-number
Device(config)# interface GigabitEthernet slot/subslot/port
Device(config-if)# channel-group channel-group-number
Device(config)# interface GigabitEthernet slot/subslot/port
Device(config-if)# channel-group channel-group-number
```

```
Device(config)# interface Port-channelchannel-number
Device(config-if)# load-balancing vlan
Device(config)# interface Port-channel channel-number.channel-number
Device(config-subif)# encapsulation dot1Q vlan_id primary interface1
secondaryinterface2
```

（注） **encapsulation dot1q** が設定されている場合、インターフェイス 1 およびインターフェイス 2 はポートチャネルのメンバーポートである必要があります。

次に、固定モードで EtherChannel を作成するための完全な設定例を示します。

```
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

Cisco SD-WAN EtherChannel の設定例

例

次に、EtherChannel 1 を設定し、スタティックモードで物理インターフェイスを EtherChannel に追加する例を示します。

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# channel-group 1
Device(config-if)# end
```

LACP を使用した EtherChannnel の設定例

例

次に、レイヤ 3 EtherChannel を設定し、LACP モードを active として 2 つのポートをチャネル 5 に割り当てる例を示します。

```
Device# config-transaction
Device(config)# interface Gigabitethernet 0/1/2
Device(config-if-range)# no ip address
```

```
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

フローベースのポートチャネル ロード バランシングの設定例

例

次に、フローベースのロードバランシングがポートチャネル2で設定され、VLAN手動方式がグローバルに設定されている設定の例を示します。

```
!
no aaa new-model
port-channel load-balancing vlan-manual
ip source-route
.
.
.
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
 load-balancing flow
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

VLAN 手動ロードバランシングの設定例

例

次に、**port-channel load-balancing** コマンドを使用して、トラフィックを処理するポリシーを定義するために、ロードバランシングの設定をグローバルに適用する例を示します。

```
port-channel load-balancing vlan-manual

!
interface Port-channel1
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0
```

```
 !
interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

CLI を使用した設定済み EtherChannel のモニタリング

例 1

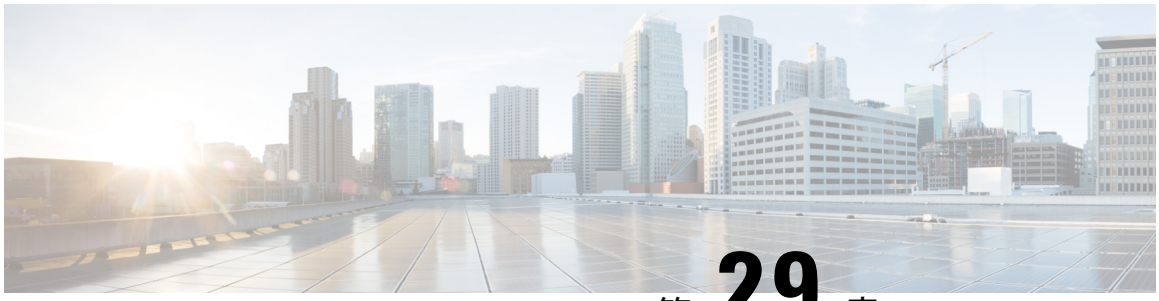
次に、**show etherchannel summary** コマンドの出力例を示します。この例は、各チャネルグループの概要を示しています。

```
Device# show etherchannel summary

Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

例 2

次に、**show etherchannel load-balancing** コマンドの出力例を示します。この例は、各ポートチャネルに適用されるロードバランシング方式を表示します。

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual
  Port-Channel:                       LB Method
    Port-channel1                   :  flow-based
```



第 29 章

Cisco SD-WAN マルチテナント機能

Cisco SD-WAN マルチテナント機能の概要

Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。テナントは、基盤となる Cisco SD-WAN コントローラの同じセット（Cisco vManage、Cisco vBond オーケストレーション、および Cisco

vSmart コントローラ）を共有します。テナントデータは、これらの共有コントローラ上で論理的に分離されます。

サービスプロバイダーは、Cisco vManage クラスタの IP アドレスにマッピングされたドメイン名を使用して Cisco vManage にアクセスし、マルチテナント展開を管理します。各テナントには、テナント固有の Cisco vManage ビューにアクセスしてテナントの展開を管理するためのサブドメインが提供されます。たとえば、ドメイン名 `managed-sp.com` を使用するサービスプロバイダーは、テナント Customer1 と Customer2 にサブドメイン `customer1.managed-sp.com` と `customer2.managed-sp.com` を割り当て、各顧客に専用の Cisco SD-WAN コントローラセットを備えたシングルテナントのセットアップを提供する代わりに、それらを同じ Cisco SD-WAN コントローラセットで管理することができます。

Cisco SD-WAN マルチテナント機能の主な機能は次のとおりです。

- 完全なエンタープライズ マルチテナント機能：Cisco SD-WAN はマルチテナント機能をサポートし、企業はサービスプロバイダーやテナントなどの役割を柔軟に分離することができます。サービスプロバイダーは、マルチテナント機能を使用して顧客に Cisco SD-WAN サービスを提供できます。
- マルチテナント Cisco vManage
- マルチテナント Cisco vBond オーケストレーション
- マルチテナント Cisco vSmart コントローラ
- テナント固有の WAN エッジデバイス
- VPN 番号の重複：特定の VPN または共通の VPN のセットは、独自の設定および監視ダッシュボード環境を使用して、特定のテナントに割り当てられます。これらの VPN 番号は、他のテナントが使用する場所で重複する可能性があります。
- オンプレミスおよびクラウド展開モデル：Cisco SD-WAN コントローラは、VMware ESXi 6.7 以降またはカーネルベースの仮想マシン（KVM）ハイパーバイザを実行しているサーバー上の組織のデータセンターに展開できます。Cisco SD-WAN コントローラは、Cisco CloudOps によって Amazon Web Services（AWS）サーバー上でホストすることもできます。
- テナント固有の Cisco vAnalytics：Cisco vAnalytics は、アプリケーションのパフォーマンスと基盤となる SD-WAN ネットワーク インフラストラクチャに関するインサイトを提供するクラウドベースのサービスです。各テナントは、テナント固有の Cisco vAnalytics インスタンスを要求し、Cisco vManage でのデータ収集を有効にすることで、オーバーレイネットワークに関する Cisco vAnalytics のインサイトを取得できます。サービスプロバイダーは、テナント オーバーレイ ネットワークの Cisco vAnalytics インスタンスのオンボーディングを促進するために、プロバイダービューで Cisco vManage のクラウドサービスを有効にする必要があります。

マルチテナント Cisco vManage

Cisco vManage はサービスプロバイダーによって展開および設定されます。プロバイダーは、マルチテナント機能を有効にし、テナントにサービスを提供する Cisco vManage クラスタを作

成します。SSH 端末を介して Cisco vManage インスタンスにアクセスできるのはプロバイダーのみです。

Cisco vManage は、サービスプロバイダーに SD-WAN マルチテナント展開の全体像を提供し、プロバイダーが共有 Cisco vBond オーケストレーション デバイスと Cisco vSmart コントローラ デバイスを管理できるようにします。また、Cisco vManage により、サービスプロバイダーは各テナントの展開を監視および管理できます。

Cisco vManage により、テナントは展開を監視および管理できます。Cisco vManage により、テナントは WAN エッジデバイスを展開および設定できます。テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定することもできます。

マルチテナント Cisco vBond オーケストレーション

Cisco vBond オーケストレーション は、サービスプロバイダーによって展開および設定されます。SSH 端末を介して Cisco vBond オーケストレーション にアクセスできるのはプロバイダーのみです。

Cisco vBond オーケストレーションは、デバイスがオーバーレイネットワークに追加されると、複数のテナントの WAN エッジデバイスにサービスを提供します。

マルチテナント Cisco vSmart コントローラ

Cisco vSmart コントローラは、サービスプロバイダーによって展開されます。デバイスおよび機能テンプレートを作成して Cisco vSmart コントローラに接続できるのはプロバイダーのみで、SSH 端末を介して Cisco vSmart コントローラにアクセスできます。

- テナントが作成されると、Cisco vManage はテナントに 2 つの Cisco vSmart コントローラを割り当てます。Cisco vSmart コントローラは、アクティブ/アクティブクラスタを形成します。

  各テナントには 2 つの Cisco vSmart コントローラのみが割り当てられます。テナントを作成する前に、テナントにサービスを提供するために 2 つの Cisco vSmart コントローラを使用できる必要があります。

- テナントにサービスを提供するために複数の Cisco vSmart コントローラのペアを使用できる場合、Cisco vManage は、最も少ない数の予測デバイスに接続されている Cisco vSmart コントローラのペアをテナントに割り当てます。Cisco vSmart コントローラの 2 つのペアが同じ数のデバイスに接続されている場合、Cisco vManage は、テナントの数が最も少ない Cisco vSmart コントローラのペアをテナントに割り当てます。

- Cisco vManage リリース 20.9.1 以降では、テナントをマルチテナント展開にオンボーディングするときに、テナントにサービスを提供するマルチテナント Cisco vSmart コントローラのペアを選択できます。テナントのオンボーディング後、必要に応じて、テナントをマルチテナント Cisco vSmart コントローラの別のペアに移行できます。詳細については、「マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置」を参照してください。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントに対応できます。

- テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定できます。Cisco vManage はポリシーテンプレートをプルするように Cisco vSmart コントローラに通知します。Cisco vSmart コントローラはテンプレートをプルし、特定のテナントのポリシー設定を展開します。
- Cisco vManage で Cisco vSmart コントローラのイベント、監査ログ、および OMP アラームを表示できるのは、プロバイダーのみです。

テナント固有の WAN エッジデバイス

テナントまたはテナントに代わって機能するプロバイダーは、WAN エッジデバイスをテナントネットワークに追加したり、デバイスを設定したり、テナントネットワークからデバイスを削除したり、SSH 端末を介してデバイスにアクセスしたりできます。

プロバイダーは、テナントとしてのプロバイダービューからのみ WAN エッジデバイスを管理できます。プロバイダービューでは、Cisco vManage は WAN エッジデバイスの情報を表示しません。

Cisco vManage は、WAN エッジデバイスのイベント、ログ、およびアラームを、テナントロールビューおよびテナントとしてのプロバイダービューでのみレポートします。

マルチテナント環境でのユーザーロール

マルチテナント環境には、サービスプロバイダーとテナントのロールが含まれます。各ロールには、個別の権限、ビュー、および機能があります。

プロバイダーロール

プロバイダーロールは、システム全体の管理者権限を付与します。プロバイダーロールを持つユーザーは、デフォルトのユーザー名 **admin** を持っています。プロバイダーユーザーは、サービスプロバイダーのドメイン名または Cisco vManage IP アドレスを使用して Cisco vManage にアクセスできます。ドメイン名を使用する場合、ドメイン名の形式は `https://managed-sp.com` です。

admin ユーザーは、ユーザーグループ **netadmin** の一部です。このグループのユーザーは、テナントのコントローラと WAN エッジデバイスに対するすべての操作を実行することが許可されます。**netadmin** グループにユーザーを追加できます。

netadmin グループの権限は変更できません。Cisco vManage では、**[Administration]** > **[Manage Users]** > **[User Groups]**ページからユーザーグループの権限を表示できます。

（注） **netadmin** ユーザーを含む新しいプロバイダーユーザーを Cisco vManage で作成すると、デフォルトでは、ユーザーは Cisco vManage VM への SSH アクセスを許可されません。SSH アクセスを有効にするには、AAA テンプレートを使用して SSH 認証を設定し、Cisco vManage へテンプレートをプッシュします。SSH 認証の有効化の詳細については、「SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices」を参照してください。

ユーザーとユーザーグループの構成の詳細については、「Configure User Access and Authentication」を参照してください。

Cisco vManage は、プロバイダーに次の 2 つのビューを提供します。

- **プロバイダービュー**

  プロバイダーユーザーが **admin** または別の **netadmin** ユーザーとしてマルチテナント Cisco vManage にログインすると、Cisco vManage にプロバイダービューが表示され、プロバイダーダッシュボードが表示されます。

  プロバイダービューから次の機能を実行できます。

  - Cisco vManage、Cisco vBond Orchestrator、および Cisco vSmart Controller をプロビジョニングおよび管理します。
  - テナントを追加、変更、または削除します。
  - オーバーレイネットワークのモニタリング。

- **テナントとしてのプロバイダービュー**

  プロバイダーユーザーがプロバイダーダッシュボードの上部にある [Select Tenant] ドロップダウンリストから特定のテナントを選択すると、Cisco vManage にテナントとしてのプロバイダービューが表示され、選択したテナントのテナントダッシュボードが表示されます。プロバイダーユーザーは、**tenantadmin** としてログインしたときのテナントユーザーと同じ Cisco vManage のビューを持ちます。プロバイダーは、このビューから、テナントに代わってテナントの展開を管理できます。

  プロバイダーダッシュボードでは、テナントのテーブルに各テナントのステータスの概要が表示されます。プロバイダーユーザーは、このテーブルのテナント名をクリックして、テナントとしてのプロバイダービューを起動することもできます。

テナントロール

テナントロールは、テナント管理権限を付与します。テナントロールを持つユーザーは、デフォルトのユーザー名 **tenantadmin** を持っています。デフォルトのパスワードは **Cisco#123@Viptela** です。最初のログイン時にデフォルトのパスワードを変更することをお勧めします。デフォルトのパスワードの変更については、「Hardware and Software Installation」を参照してください。

tenantadmin ユーザーは、ユーザーグループ **tenantadmin** の一部です。このグループのユーザーは、テナントの WAN エッジデバイスですべての操作を実行できます。**tenantadmin** グループにユーザーを追加できます。

tenantadmin グループの権限は変更できません。Cisco vManage では、**[Administration]** > **[Manage Users]** > **[User Groups]**ページからユーザーグループの権限を表示できます。

ユーザーとユーザーグループの構成の詳細については、「Configure User Access and Authentication」を参照してください。

テナントユーザーは、専用の URL とデフォルトのユーザー名 **tenantadmin** を使用して Cisco vManage にログインできます。たとえば、ドメイン名 `https://managed-sp.com` を使用するプロバイダーの場合、テナントの専用 URL は `https://customer1.managed-sp.com` になる可能性があります。ユーザーがログインすると、Cisco vManage にテナントビューが表示され、テナントダッシュボードが表示されます。

ヒント　専用テナント URL にアクセスできない場合は、ローカルマシンの `/etc/hosts` ファイルでサブドメインの詳細を更新します。または、外部 DNS サーバーを使用する場合は、テナントサブドメインの DNS エントリを追加します。

管理者権限を持つテナントユーザーは、次の機能を実行できます。

- テナントルータのプロビジョニングと管理
- テナントのオーバーレイネットワークのモニタリング
- 割り当てられた Cisco vSmart コントローラにカスタムポリシーを作成
- テナントルータのソフトウェアをアップグレード。

サポートされているデバイスとコントローラの仕様

次の Cisco SD-WAN エッジデバイスはマルチテナント機能をサポートしています。

表 *218* : サポートされるデバイス

Platform	デバイス モデル
Cisco IOS XE SD-WAN デバイス	• Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco ISR 1000 シリーズ サービス統合型ルータ • Cisco ISR 4000 シリーズ サービス統合型ルータ • Cisco Catalyst 8200 シリーズエッジプラットフォーム • Cisco Catalyst 8300 シリーズエッジプラットフォーム • Cisco Catalyst 8500 シリーズエッジプラットフォーム • Cisco Catalyst 8000V Edge ソフトウェア • Cisco ENCS プラットフォーム

マルチテナント機能では、次のハイパーバイザがサポートされています。

- VMware ESXi 6.7 以降
- KVM
- AWS（クラウドホスト型、Cisco CloudOps による管理）

Cisco vManage リリース 20.6.1 以降、マルチテナント Cisco vManage インスタンスは、次の 3 つのいずれかのペルソナを使用できます。ペルソナにより、Cisco vManage インスタンスで事前定義された一連のサービスが有効になります。

表 *219* : *Cisco vManage* のペルソナ

ペルソナ	サービス
コンピューティング + データ	クラスタ Oracle、サービスプロキシ、メッセージングサービス、調整サービス、設定データベース、Data Collection Agent、統計データベース、およびアプリケーションサーバー
データ	クラスタ Oracle、サービスプロキシ、アプリケーションサーバー、Data Collection Agent、および統計データベース

ペルソナ	サービス
コンピューティング	クラスタ Oracle、サービスプロキシ、メッセージングサービス、調整サービス、設定データベース、およびアプリケーションサーバー

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart Controller でサポートされるハードウェア仕様は次のとおりです。

50 テナントと 1000 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart コントローラでサポートされるハードウェア仕様の詳細については、『Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources』を参照してください。

75 テナントと 2500 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart コントローラでサポートされるハードウェア仕様の詳細については、『Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources』を参照してください。

100 テナントと 5000 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart コントローラでサポートされるハードウェア仕様の詳細については、『Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources』を参照してください。

150 テナントと 7500 デバイスをサポートするハードウェア仕様

Cisco vBond Orchestrator、Cisco vManage、および Cisco vSmart コントローラでサポートされるハードウェア仕様の詳細については、『Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources』を参照してください。

機能制限

- ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。代わりに、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。

  `vmanage_system` インターフェイスの IP アドレスを見つけるには、次のいずれかの方法を使用します。

  - Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から `vmanage_system` の IP アドレスを見つけることもできます。
  - **show interface description** コマンドを実行し、コマンド出力から `vmanage_system` IP アドレスを見つけます。

- テナントを追加した直後に 2 番目のテナントを追加すると、Cisco vManage はそれらを並行してではなく順番に追加します。
- 以前に無効にしてオーバーレイネットワークから削除した WAN エッジデバイスを追加する場合は、デバイスの追加後にデバイスソフトウェアをリセットする必要があります。Cisco IOS XE SD-WAN デバイスのソフトウェアをリセットするには、**request platform software sdwan software reset** コマンドを使用します。

マルチテナント機能の初期設定

前提条件

- 次の表で推奨されているソフトウェアバージョンをダウンロードしてインストールします。

表 *220 : Cisco SD-WAN* マルチテナント機能の最小ソフトウェア前提条件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

1 つまたは複数のコントローラまたは WAN エッジデバイスが、上記の表に示すものより前のソフトウェアバージョンを実行している構成はサポートされていません。

- 既存の Cisco vManage インスタンスにおいてデバイスをすべて無効化または削除した場合でも、既存のシングルテナント Cisco vManage インスタンスをマルチテナントモードに移行しないでください。代わりに、新しい Cisco vManage ソフトウェアイメージをダウンロードしてインストールします。

（注） マルチテナント機能用に Cisco vManage を有効にした後は、シングルテナントモードに戻すことはできません。

- このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションにある推奨ハードウェア仕様に従ってください。
- プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。

1. Cisco vManage クラスタを作成します。

1. すべてのテナントで 50 のテナントと 1000 のデバイスをサポートするには、3 ノードの Cisco vManage クラスタの作成。
2. すべてのテナントで 100 のテナントと 5000 のデバイスをサポートするには、6 ノードの Cisco vManage クラスタの作成。
3. Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 のテナントと 7500 のデバイスをサポートするには、6 ノードの Cisco vManage クラスタの作成。

2. Cisco vBond Orchestrator インスタンスを作成して設定します。「Deploy Cisco vBond Orchestrator」を参照してください。

   Cisco vBond Orchestrator インスタンスを設定するときに、サービスプロバイダーの組織名（`sp-organization-name`）と組織名（`organization-name`）を設定します。「Configure Organization Name in Cisco vBond Orchestrator」を参照してください。

   ```
   sp-organization-name multitenancy
   organization-name multitenancy
   ```

3. Cisco vSmart コントローラインスタンスを作成します。「Deploy the Cisco vSmart Controller」を参照してください。
   - すべてのテナントで 50 のテナントと 1000 のデバイスをサポートするには、6 つの Cisco vSmart Controller インスタンスを展開します。
   - すべてのテナントで 100 のテナントと 5000 のデバイスをサポートするには、10 の Cisco vSmart コントローラを展開します。
   - Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 のテナントと 7500 のデバイスをサポートするには、16 の Cisco vSmart コントローラを展開します。

   1. オーバーレイネットワークに Cisco vSmart コントローラの追加 します。

4. 新しいテナントを導入準備します。新規テナントの追加 （871 ページ）を参照してください。

3 ノードの Cisco vManage クラスタの作成

1. Cisco Software Download から、Cisco vManage リリース 20.6.1 以降のソフトウェアイメージをダウンロードします。
2. ダウンロードしたソフトウェアイメージファイルをインストールして、3 つの Cisco vManage インスタンス（vManage1、vManage2、および vManage3 など）を作成します。「Deploy Cisco vManage」を参照してください。

重要
- このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 50 Tenants and 1000 Devices*」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。
- Cisco vManage インスタンスごとに [Compute+Data] ペルソナを選択します。

3. vManage1 で次の操作を実行します。
   1. CLI を使用して以下を設定します。
      - システム IP アドレス
      - サイト ID
      - サービスプロバイダーの組織名（`sp-organization-name`）
      - 組織名
      - vBond IP アドレス
      - VPN 0 トランスポート/トンネルインターフェイス
      - VPN 0 アウトオブバンド（OOB）インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
      - VPN 512 管理インターフェイス

（注） VPN 0 にデフォルトルートを 1 つだけ設定します。

   2. Cisco vManage でのマルチテナント機能の有効化 （864 ページ）。
   3. （オプション）CLI を使用して、vManage1 のルート CA 証明書をインストールします。

（注） Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

   4. Cisco vManage GUI を使用して以下を実行します。
      1. 証明書署名要求を生成します
      2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
   5. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

次のステップに進む前に、**[Administration]** > **[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

4. vManage2 および vManage 3 で次の操作を実行します。

重要 vManage2 および vManage3 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。
   - システム IP アドレス
   - サイト ID
   - サービスプロバイダーの組織名（`sp-organization-name`）
   - 組織名
   - vBond IP アドレス
   - VPN 0 トランスポート/トンネルインターフェイス
   - VPN 0 アウトオブバンド（OOB）インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
   - VPN 512 管理インターフェイス
2. （オプション）CLI を使用して、vManage1 のルート CA 証明書をインストールします。

（注） Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
   1. 証明書署名要求を生成します
   2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名付き証明書をインストールします。
4. Cisco vManage Web アプリケーションサーバーにログインします。
5. 他の 2 つの Cisco vManage インスタンスの OOB インターフェイスに ping を送信し、到達可能であることを確認します。
6. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

次のステップに進む前に、**[Administration]** > **[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

5. vManage1 GUI にログインし、vManage2 をクラスタに追加します。

   vManage2 は、クラスタに追加される前に再起動します。

   vManage2 がクラスタに追加されている間、**[Administration]** > **[Cluster Management]** ページで、vManage2 の [Configure Status] には [Pending] と表示されます。[System Generated Cluster Sync] トランザクションを監視すると、クラスタへの vManage2 の追加の進行状況を確認できます。

   操作が完了すると、**[Administration]** > **[Cluster Management]** ページで、vManage1 と vManage2 の両方、およびそれらのノードペルソナを表示できます。

6. **ステップ 5** を繰り返し、vManage3 をクラスタに追加します。

（注） 再起動後、CLI からペルソナ（非クラウドセットアップ）を選択する必要があり、サービスは選択したペルソナに従ってノードで実行を開始します。

6 ノードの Cisco vManage クラスタの作成

1. Cisco Software Download から、Cisco vManage リリース 20.6.1 以降のソフトウェアイメージをダウンロードします。
2. ダウンロードしたソフトウェアイメージファイルをインストールして、6 つの Cisco vManage インスタンスを作成します。「Deploy Cisco vManage」を参照してください。

重要

- すべてのテナントで 100 テナントと 5000 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「100 テナントと 5000 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

  Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、すべてのテナントで 150 テナントと 7500 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「150 テナントと 7500 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

- 3 つの Cisco vManage インスタンス（vManage1、vManange2、および vManage 3 など）には、[Compute+Data] ペルソナを選択します。他の 3 つの Cisco vManage インスタンス（vManage4、vManage5、および vManage6 など）には、[Data] ペルソナを選択します。

3. vManage1 で次の操作を実行します。
   1. CLI を使用して以下を設定します。
      - システム IP アドレス
      - サイト ID
      - サービスプロバイダーの組織名（`sp-organization-name`）
      - 組織名
      - vBond IP アドレス
      - VPN 0 トランスポート/トンネルインターフェイス
      - VPN 0 アウトオブバンド（OOB）インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
      - VPN 512 管理インターフェイス

（注） VPN 0 にデフォルトルートを 1 つだけ設定します。

   2. Cisco vManage でのマルチテナント機能の有効化 （864 ページ）。
   3. （オプション）CLI を使用して、vManage1 のルート CA 証明書をインストールします。

（注） Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

   4. Cisco vManage GUI を使用して以下を実行します。
      1. 証明書署名要求を生成します。
      2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
   5. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

      次のステップに進む前に、**[Administration]** > **[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

4. vManage2 から vManage6 で次の操作を実行します。

重要　vManage2 から vManage6 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。
   - システム IP アドレス
   - サイト ID
   - サービスプロバイダーの組織名（`sp-organization-name`）
   - 組織名
   - vBond IP アドレス
   - VPN 0 トランスポート/トンネルインターフェイス
   - VPN 0 アウトオブバンド（OOB）インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
   - VPN 512 管理インターフェイス
2. （オプション）CLI を使用して、vManage1 のルート CA 証明書をインストールします。

（注）　Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
   1. 証明書署名要求を生成します。
   2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
4. Cisco vManage Web アプリケーションサーバーにログインします。
5. 他の Cisco vManage インスタンスの OOB インターフェイスに ping して、到達可能であることを確認します。
6. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

   次のステップに進む前に、**[Administration]** > **[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

5. vManage1 GUI にログインし、vManage2 をクラスタに追加します。

   vManage2 は、クラスタに追加される前に再起動します。

vManage2 がクラスタに追加されている間、**[Administration]** > **[Cluster Management]** ページで、vManage2 の [Configure Status] には [Pending] と表示されます。[System Generated Cluster Sync] トランザクションを監視すると、クラスタへの vManage2 の追加の進行状況を確認できます。

操作が完了すると、**[Administration]** > **[Cluster Management]** ページで、vManage1 と vManage2 の両方、およびそれらのノードペルソナを表示できます。

6. **ステップ 5** を繰り返し、vManage3 から vManage6 をクラスタに追加します。

Cisco vManage でのマルチテナント機能の有効化

前提条件

既存の Cisco vManage からすべてのデバイスを無効にするか削除した場合でも、既存のシングルテナント Cisco vManage をマルチテナントモードに移行しないでください。代わりに、Cisco vManage リリース 20.6.1 またはそれ以降のリリースの新しいソフトウェアイメージをダウンロードしてインストールします。

（注） Cisco vManage でマルチテナンシーを有効にした後、シングルテナントモードに戻すことはできません。

1. URL `https://vmanage-ip-address:port` を使用して Cisco vManage を起動します。プロバイダーの **admin** ユーザーとしてログインします。
2. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
3. テナンシーモードバーで、[Edit] をクリックします。
4. [Tenancy] フィールドで、[Multitenant] をクリックします。
5. [Domain] フィールドに、サービスプロバイダーのドメイン名（たとえば、managed-sp.com）を入力します。
6. クラスタ ID（たとえば、cluster-1 または 123456）を入力します。
7. **[Save]** をクリックします。
8. [Proceed] をクリックして、テナンシーモードを変更することを確認します。

   Cisco vManage はマルチテナントモードで再起動し、プロバイダーユーザーが Cisco vManage にログインすると、プロバイダーダッシュボードが表示されます。

（注） ステップ 5 および 6 で作成された [Domain] と [Cluster Id] の値は、プロバイダー FQDN として機能します。これらの値が現在の DNS 命名規則に準拠していることを確認してください。設定の保存後にこれらの値を変更することはできません。これらの値を変更するには、新しい Cisco vManage クラスタを展開する必要があります。プロバイダーとテナントの DNS 要件の詳細については、「新規テナントの追加」のステップ 3.d を参照してください。

Cisco vSmart コントローラの追加

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
3. [Controllers] をクリックします。
4. [Add Controller] をクリックし、[vSmart] をクリックします。
5. [Add vSmart] ダイアログボックスで、次を実行します。
   1. [vSmart Management IP Address] フィールドに、Cisco vSmart コントローラのシステム IP アドレスを入力します。
   2. Cisco vSmart コントローラへのアクセスに必要な [Username] と [Password] を入力します。
   3. コントロールプレーン接続に使用するプロトコルを選択します。デフォルトは[DTLS] です。

      [TLS] を選択した場合は、TLS 接続に使用するポート番号を入力します。デフォルトは 23456 です。
   4. 証明書署名要求を作成するには、Cisco vManage の [Generate CSR] チェックボックスをオンにします。
   5. [Add] をクリックします。
6. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。

   Cisco vSmart コントローラを新規に追加した場合、[Operation Status] には「CSR Generated」と表示されます。
   1. Cisco vSmart コントローラを新規に追加した場合、[More Options] アイコンをクリックし、[View CSR] をクリックします。
   2. CSR を認証局（CA）に提出して、署名付き証明書を取得します。
7. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
8. [Install Certificate] をクリックします。

9. [Install Certificate] ダイアログボックスで証明書を [Certificate Text] に貼り付けるか、[Select a File] をクリックして証明書ファイルをアップロードします。[Install] をクリックします。

   Cisco vManage により、証明書が Cisco vSmart コントローラにインストールされます。Cisco vManage により、証明書のシリアル番号が他のコントローラにも送信されます。

   [Configuration] > **[Certificates]** ページで、新しく追加された Cisco vSmart コントローラの [Operation Status] には、「vBond Updated」と表示されます。

   [Configuration] > **[Devices]** ページで、新しいコントローラがコントローラテーブルに表示されます。このテーブルにはコントローラタイプ、コントローラのホスト名、IP アドレス、サイト ID、およびその他の詳細も表示されます。[Mode] は [CLI] に設定されています。

10. テンプレートをデバイスにアタッチして、新しく追加された Cisco vSmart コントローラのモードを [vManage] に変更します。

    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. Cisco vSmart コントローラにアタッチするテンプレートを見つけます。
    4. [...] をクリックして、[Attach Devices] をクリックします。
    5. [Attach Devices] ダイアログボックスで、新しいコントローラを [Selected Device] リストに移動し、[Attach] をクリックします。
    6. [Config Preview] を確認し、[Configure Devices] をクリックします。

Cisco vManage は、テンプレートの設定を新しいコントローラにプッシュします。

[Configuration] > **[Devices]** ページでは、Cisco vSmart コントローラの [Mode] に [vManage] と表示されます。新しい Cisco vSmart コントローラをマルチテナント展開で使用する準備ができました。

マルチテナント展開を拡張してテナントとテナントデバイスのサポート数を追加

サービスプロバイダーは、50 のテナントと 1000 のデバイスをサポートする Cisco SD-WAN マルチテナント オーバーレイを展開したとします。より多くのテナントまたはデバイスをサポートする必要がある場合は、Cisco vManage クラスタを拡張し、Cisco vSmart コントローラをオー

バーレイに追加して、最大 100 のテナントと 5000 のデバイスをサポートできます。Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、Cisco vManage クラスタを拡張し、Cisco vSmart コントローラをオーバーレイに追加して、最大 150 のテナントと 7500 のデバイスをサポートできます。

前提条件

最大 50 のテナントと 1000 のデバイスをサポートするマルチテナント Cisco SD-WAN オーバーレイ（このドキュメントの「マルチテナント機能の初期設定」セクションの手順に従って展開します）。

1. 3 ノードクラスタから 6 ノードクラスタへの拡張
2. 最大 100 のテナントと 5000 のデバイスをサポートするには、オーバーレイに 10 の Cisco vSmart コントローラが必要です。したがって、オーバーレイ内の 6 つの既存の Cisco vSmart コントローラに加えて、4 つの Cisco vSmart コントローラを展開します。

   最大 150 のテナントと 7500 のデバイスをサポートするには、オーバーレイに 16 の Cisco vSmart コントローラが必要です。したがって、オーバーレイ内の 6 つの既存の Cisco vSmart コントローラに加えて、10 の Cisco vSmart コントローラを展開します。

   1. Cisco vSmart コントローラインスタンスを作成します。「Deploy the Cisco vSmart Controller」を参照してください。
   2. オーバーレイネットワークに Cisco vSmart コントローラの追加 します。

テナントを追加するか、既存のテナントで関連する制限に従ってデバイスを追加できるようになりました。

3 ノードクラスタから 6 ノードクラスタへの拡張

（注） 3 ノードの Cisco vManage クラスタは、6 ノードの Cisco vManage クラスタにのみ拡張できます。3 ノードクラスタを他のクラスタサイズに拡張することはサポートされていません。

1. 100 のテナントと 5000 のデバイスをサポートするには、既存の 3 ノードクラスタ内の 3 つの Cisco vManage サーバーを、このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 100 Tenants and 5000 Devices*」の表のハードウェア仕様にアップグレードします。

   Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降で、150 のテナントと 7500 のデバイスをサポートするには、既存の 3 ノードクラスタ内の 3 つの Cisco vManage サーバーを、このドキュメントの「*Supported Devices and Controller Specifications*」セクションにある表「*Hardware Specifications to Support 150 Tenants and 7500 Devices*」のハードウェア仕様にアップグレードします。

2. Cisco Software Download から、Cisco vManage リリース 20.6.1 以降のリリースのソフトウェアイメージをダウンロードします。
3. ダウンロードしたソフトウェアイメージファイルをインストールして、3 つの Cisco vManage インスタンス（vManage1、vManage2、および vManage3 など）を作成します。「Deploy Cisco vManage」を参照してください。

重要
- このドキュメントの「*Supported Devices and Controller Specifications*」セクションの「*Hardware Specifications to Support 100 Tenants and 5000 Devices*」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。

  Cisco IOS XE リリース 17.6.3a、Cisco vManage リリース 20.6.3 以降、150 テナントと 7500 デバイスをサポートするには、このドキュメントの「サポートされているデバイスとコントローラの仕様」セクションの「150 テナントと 7500 デバイスをサポートするハードウェア仕様」の表にあるハードウェア仕様の Cisco vManage サーバーを展開します。
- Cisco vManage インスタンスごとに [Data] ペルソナを選択します。

4. vManage1 から vManage3 で次の操作を実行します。

重要 vManage1 から vManage3 でマルチテナント機能を有効にしないでください。

1. CLI を使用して以下を設定します。
   - システム IP アドレス
   - サイト ID
   - サービスプロバイダーの組織名（`sp-organization-name`）
   - 組織名
   - vBond IP アドレス
   - VPN 0 トランスポート/トンネルインターフェイス
   - VPN 0 アウトオブバンド（OOB）インターフェイス：このインターフェイスに静的 IP アドレスを割り当てていることを確認します。DHCP は有効にしないでください。
   - VPN 512 管理インターフェイス

（注） VPN 0 にデフォルトルートを 1 つだけ設定します。

2. （オプション）CLI を使用して、vManage1 のルート CA 証明書をインストールします。

（注） Symantec または Cisco PKI 証明書を使用している場合は、このステップをスキップします。

3. Cisco vManage GUI を使用して以下を実行します。
   1. 証明書署名要求を生成します
   2. Symantec またはエンタープライズルート CA が証明書に署名した後、署名された証明書をインストールします。
4. Cisco vManage Web アプリケーションサーバーにログインします。
5. 他の Cisco vManage インスタンスの OOB インターフェイスに ping して、到達可能であることを確認します。
6. Cisco vManage サーバーのクラスタ IP アドレスを設定します。

   次のステップに進む前に、**[Administration]** > **[Cluster Management]** ページの [vManage IP Address] フィールドに OOB インターフェイスアドレスが表示されていることを確認してください。

5. 既存の 3 ノード Cisco vManage クラスタの GUI にログインし、vManage1 をクラスタに追加します。

   vManage1 は、クラスタに追加される前に再起動します。

   vManage1 がクラスタに追加されている間、**[Administration]** > **[Cluster Management]** ページで、vManage1 の [Configure Status] には [Pending] と表示されます。[System Generated Cluster Sync] トランザクションを監視すると、クラスタへの vManage1 の追加の進行状況を確認できます。

   操作が完了すると、**[Administration]** > **[Cluster Management]**ページで、元の 3 ノードクラスタの一部であった 3 つの Cisco vManage インスタンスとともにリストされた vManage1 とそのノードペルソナを表示できます。

6. **ステップ 4** を繰り返し、vManage2 と vManage3 をクラスタに追加します。

テナントの管理

表 *221 :* 機能の履歴

機能名	リリース情報	説明
テナントデバイスの予測	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、サービスプロバイダーは、テナントがオーバーレイネットワークに追加できる WAN エッジデバイスの数を制御できます。これを行うと、プロバイダーは Cisco SD-WAN コントローラリソースを効率的に利用できます。

テナントデバイスの予測

マルチテナント Cisco SD-WAN 展開に新しいテナントを追加する際、サービスプロバイダーは、テナントがオーバーレイネットワークに展開できる WAN エッジデバイスの数を予測できます。Cisco vManage は、この予測制限を適用します。テナントがこの制限を超えてデバイスを追加しようとすると、Cisco vManage は該当するエラーメッセージで応答し、デバイスの追加は失敗します。

マルチテナント展開では、テナントは最大で 1000 台のデバイスをオーバーレイネットワークに追加できます。

（注） Cisco IOS XE リリース 17.6.2、Cisco vManage リリース 20.6.2 以降では、テナントの追加後にテナントのデバイス予測を変更できます。この変更は、Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1 ではサポートされていません。

利点：

- サービスプロバイダーは、Cisco SD-WAN コントローラリソースがより効率的に使用されるようにすることができます。
- 設定によっては、マルチテナント展開では、すべてのテナントで固定数の WAN エッジデバイスをサポートできます。テナントが追加できるデバイスの数を予測することにより、サービスプロバイダーは、展開でサポートできるエッジデバイスのプール全体から各テナントにクォータを割り当てることができます。

新規テナントの追加

前提条件

- 新しいテナントを追加する前に、少なくとも 2 つの Cisco vSmart コントローラが動作し、vManage モードになっている必要があります。

  テンプレートを Cisco vManage からコントローラにプッシュすると、Cisco vSmart コントローラは vManage モードに入ります。CLI モードの Cisco vSmart コントローラは、複数のテナントに対応できません。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントと最大 1000 のテナントデバイスに対応できます。新しいテナントに対応できる Cisco vSmart コントローラが少なくとも 2 つあることを確認します。展開内の Cisco vSmart コントローラのペアが新しいテナントに対応できない場合は、2 つの Cisco vSmart コントローラを追加して、それらのモードを vManage に変更します。

- テナントを追加した直後に 2 番目のテナントを追加すると、Cisco vManage はそれらを並行してではなく順番に追加します。

- 各テナントには、Cisco Software Central の**プラグアンドプレイコネクト**に一意のバーチャルアカウント（VA）が必要です。テナント VA は、プロバイダー VA と同じスマートアカウント（SA）に属している必要があります。

- オンプレミス展開の場合、**プラグアンドプレイコネクト**でテナント用の Cisco vBond Orchestrator コントローラプロファイルを作成します。次の表のフィールドは必須です。

表 *222*：コントローラ プロファイル フィールド

フィールド	説明/値
プロファイル名	コントローラプロファイル名を入力します
マルチテナント機能	ドロップダウンリストから、[Yes] を選択します。
SP Organization Name	プロバイダー組織名を入力します。
組織名	テナント組織名を <SP Org Name>-<Tenant Org Name> の形式で入力します。 （注） 組織名には最大 64 文字を使用できます。
プライマリ コントローラ（Primary Controller）	プライマリ Cisco vBond Orchestrator のホストの詳細を入力します。

クラウド展開の場合、テナント作成プロセスの一部として Cisco vBond Orchestrator コントローラプロファイルが自動的に作成されます。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。

2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. [Add Tenant] をクリックします。[Add Tenant] ダイアログボックスで、次の手順を実行します。
   1. テナントの名前を入力します。

      クラウド展開の場合、テナント名は**プラグアンドプレイコネクト**のテナント VA 名と同じである必要があります。
   2. テナントの説明を入力します。

      説明の最大長は 256 文字で、英数字のみを使用できます。
   3. 組織の名前を入力します。

      組織名では、大文字と小文字が区別されます。各テナントまたは顧客には、一意の組織名が必要です。

      組織名を次の形式で入力します。

      ```
      <SP Org Name>-<Tenant Org Name>
      ```

      たとえば、プロバイダーの組織名が「multitenancy」でテナントの組織名が「Customer1」の場合、テナントを追加するときに、組織名を **multitenancy-Customer1** として入力します。

（注） 組織名には最大 64 文字を使用できます。

   4. [URL Subdomain Name] フィールドに、テナントの完全修飾サブドメイン名を入力します。
      - サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、`managed-sp.com`サービスプロバイダーの場合、有効なドメイン名は `customer1.managed-sp.com` です。

（注） サービスプロバイダー名はすべてのテナントで共有されます。したがって、URL 命名規則が、**[Administration]** > **[Settings]** > **[Tenancy Mode]**からマルチテナンシーを有効にするときに提供されたものと同じドメイン名規則に従っていることを確認してください。

      - オンプレミス展開の場合、テナントの完全修飾サブドメイン名を DNS に追加します。完全修飾サブドメイン名を、Cisco vManage クラスタ内の 3 つの Cisco vManage インスタンスの IP アドレスにマッピングします。
        - **プロバイダーレベル**：DNS A レコードを作成し、Cisco vManage クラスタで実行されている Cisco vManage インスタンスの IP アドレスにマップします。A レコードは、「Enable Multitenancy on Cisco vManage」の手順 5 と 6 で作成

されたドメインとクラスタ ID から派生しています。たとえば、ドメインが **sdwan.cisco.com** でクラスタ ID が **vmanage123** の場合、A レコードは **vmanage123.sdwan.cisco.com** として設定する必要があります。

（注） DNS エントリの更新に失敗すると、Cisco vManage へのログイン時に認証エラーが発生します。**nslookup vmanage123.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

- **テナントレベル**：作成された各テナントの DNS CNAME レコードを作成し、プロバイダーレベルで作成された FQDN にマップします。たとえば、ドメインが **sdwan.cisco.com** でテナント名が **customer1** の場合、CNAME レコードは **customer1.sdwan.cisco.com** として設定する必要があります。

（注） CNAME レコードにはクラスタ ID は必要ありません。**nslookup customer1.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

クラウド展開の場合、テナントの完全修飾サブドメイン名は、テナント作成プロセスの一部として DNS に自動的に追加されます。テナントを追加した後、テナントの完全修飾サブドメイン名が DNS によって解決されるまでに最大 1 時間かかる場合があります。

5. [Number of Devices] フィールドに、テナントが展開できる WAN エッジデバイスの数を入力します。

   テナントがこの数を超える WAN エッジデバイスを追加しようとすると、Cisco vManage はエラーを報告し、デバイスの追加は失敗します。

6. **[Save]** をクリックします。

   [Create Tenant] 画面が表示され、テナント作成の [Status] が [In progress] と表示されます。テナントの作成に関連するステータスメッセージを表示するには、ステータスの左側にある [>] ボタンをクリックします。

   Cisco vManage は次のことを行います。

   - テナントを作成します
   - テナントにサービスを提供する 2 つの Cisco vSmart コントローラを割り当て、CLI テンプレートをこれらのコントローラにプッシュしてテナント情報を設定します
   - テナントと Cisco vSmart コントローラの情報を Cisco vBond Orchestrator に送信します。

次に行う作業：

[Status] 列が [Success] に変わったら、**[Administration]** > **[Tenant Management]**ページでテナント情報を表示できます。

テナント情報の変更

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. 左ペインで、テナントの名前をクリックします。

   右ペインにテナント情報が表示されます。
4. テナントデータを変更するには、次のようにします。
   1. 右側のペインで、鉛筆アイコンをクリックします。
   2. [Edit Tenant] ダイアログボックスでは、以下を変更できます。
      - [Description]：説明の最大長は 256 文字で、英数字のみを使用できます。
      - [Forecasted Device]：テナントが展開できる WAN エッジデバイスの数。

        テナントは、最大 1000 台のデバイスを追加できます。

（注） このオプションは、Cisco IOS XE リリース 17.6.2、Cisco vManage リリース 20.6.2 から利用できます。

テナントが展開できるデバイスの数を増やす場合は、必要な数のデバイスライセンスを Cisco Software Central の **Plug and Play Connect** のテナントバーチャルアカウントに追加する必要があります。

テナントが展開できるデバイスの数を増やす前に、テナントに割り当てられた Cisco vSmart コントローラペアがこの増加した数をサポートできることを確認してください。Cisco vSmart コントローラのペアは、これらのすべてのテナントで最大 24 のテナントと 1000 のデバイスをサポートできます。

      - [URL Subdomain Name]：テナントの完全修飾サブドメイン名を変更します。
   3. [Save（保存）] をクリックします。

テナントの削除

テナントを削除する前に、すべてのテナント WAN エッジデバイスを削除します。テナントネットワークからの WAN エッジデバイスの削除 （881 ページ）を参照してください。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. 左ペインで、テナントの名前をクリックします。

   右ペインにテナント情報が表示されます。
4. テナントを削除するには、次のようにします。
   1. 右側のペインで、ごみ箱アイコンをクリックします。
   2. [Delete Tenant] ダイアログボックスで、プロバイダーの [admin] のパスワードを入力し、[Save] をクリックします。

マルチテナント機能の Cisco vManage ダッシュボード

マルチテナント機能について Cisco vManage を有効にした場合、Cisco vManage にログインすると、マルチテナント ダッシュボードを表示できます。Cisco vManage マルチテナント ダッシュボードは、プロバイダーまたはテナントが基盤となるシステムを表示およびプロビジョニングできるポータルです。

すべての Cisco vManage マルチテナント画面の上部にあるバーには、スムーズなナビゲーションを可能にするアイコンがあります。

テナントアクティビティ、デバイス、およびネットワーク情報の表示

マルチテナント Cisco vManage に管理者としてログインすると、プロバイダーダッシュボードに次のコンポーネントが表示されます。他の Cisco vManage 画面からプロバイダーダッシュボードに戻るには、[Dashboard] をクリックします。

- デバイスペイン：マルチテナント ダッシュボード画面の上部に表示されます。デバイスペインには、アクティブな Cisco vSmart コントローラ、Cisco vBond Orchestrator、および Cisco vManage インスタンスの数、デバイスの接続ステータス、および期限切れまたは期限切れ間近の証明書に関する情報が表示されます。
- テナントペイン：テナントの総数と、すべてのテナントの制御ステータス、サイトの正常性、ルータの正常性、および Cisco vSmart Controller ステータスの概要が表示されます。
- オーバーレイネットワーク内のテナントのテーブル：各テナントの制御ステータス、サイトの正常性、WAN エッジデバイスの正常性、および Cisco vSmart コントローラステータスに関する個別の情報を含む、個々のテナントのリストです。

  テナント固有のステータスの概要情報を表示するには、次の手順を実行します。

1. テナントリストからテナント名をクリックします。

   画面の右側にダイアログボックスが開き、テナントのステータスに関する追加情報が提供されます。

2. 選択したテナントのテナントダッシュボードにアクセスするには、[<Tenant name> Dashboard] をクリックします。

   Cisco vManage に、テナントとしてのプロバイダービューが表示され、テナントダッシュボードが表示されます。プロバイダービューに戻るには、ページの上部にある [Provider] をクリックします。

3. ダイアログボックスを閉じるには、テナントリストからテナント名をクリックします。

テナント設定の詳細情報の表示

Cisco vManage は、次の場合にテナント展開に関する情報を提供するテナントダッシュボードを表示します。

- プロバイダーの **admin** ユーザーがプロバイダーダッシュボードの [Select Tenant] ドロップダウンリストから特定のテナントを選択する。このビューは、テナントとしてのプロバイダービューと呼ばれます。
- **tenantadmin** ユーザーが Cisco vManage にログインする。このビューはテナントビューと呼ばれます。

テナント オーバーレイ ネットワークのすべてのネットワーク接続を表示する

[Device] ペインは、テナントダッシュボードの上部に表示され、テナントのオーバーレイネットワーク内の Cisco vManage から Cisco vSmart コントローラおよびルータへの制御接続の数を表示します。WAN エッジデバイスごとに、[Device] ペインに次の情報が表示されます。

- Cisco vSmart コントローラと WAN エッジデバイス間の制御接続の総数
- Cisco vSmart コントローラと WAN エッジデバイス間の有効な制御接続の数
- Cisco vSmart コントローラと WAN エッジデバイス間の無効な制御接続の数

接続番号をクリックするか、上矢印または下矢印をクリックして、各接続に関する詳細情報を示す表を表示します。各テーブル行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Network]**画面から [Device Dashboard] または [Real Time] ビューにアクセスするか、または**[Tools]** > **[SSH Terminal]**画面にアクセスします。

デバイスの再起動に関する情報の表示

[Reboot] ペインには、ネットワーク内のすべてのデバイスについて、過去 24 時間の再起動の合計数が表示されます。これには、ソフト再起動とコールド再起動、およびデバイスの電源再投入の結果として発生した再起動が含まれます。再起動ごとに、次の情報が表示されます。

- 再起動したデバイスのシステム IP およびホスト名。
- デバイスが再起動された時刻。
- デバイスの再起動の理由

同じデバイスが 2 回以上再起動すると、各再起動オプションが個別に報告されます。

[Reboot] ペインをクリックして、[Reboot] ダイアログボックスを開きます。[Reboot] ダイアログボックスで、[Crashes] タブをクリックします。すべてのデバイスクラッシュについて、次の情報が表示されます。

- クラッシュが発生したデバイスのシステム IP およびホスト名。
- デバイスのクラッシュインデックス
- デバイスがクラッシュしたコアタイム。
- デバイスクラッシュログのファイル名

ネットワーク接続の表示

[Control Status] ペインには、Cisco vSmart コントローラと WAN エッジデバイスが接続されているかどうかが表示されます。各 Cisco vSmart コントローラは、ネットワーク内の他のすべての Cisco vSmart コントローラに接続する必要があります。各 WAN エッジデバイスは、設定された最大数の Cisco vSmart コントローラに接続する必要があります。[Control Status] ペインには、3 つのネットワーク接続数が表示されます。

- [Control Up]：必要な数の動作可能なコントロールプレーンが Cisco vSmart コントローラに接続されているデバイスの総数
- [Partial]：動作可能なコントロールプレーンの一部（すべてではない）が Cisco vSmart コントローラに接続されているデバイスの総数。
- [Control Down]：Cisco vSmart コントローラにコントロールプレーンが接続されていないデバイスの総数

デバイスの詳細を含むテーブルを表示するには、[Control Status] ダイアログボックスの行をクリックします。各テーブル行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Network]**画面から [Device Dashboard] または [Real Time] ビューにアクセスします。

サイトのデータ接続の状態の表示

[Site Health] ペインには、サイトのデータ接続の状態が表示されます。サイトに複数の WAN エッジデバイスがある場合、このペインには、個々のデバイスではなくサイト全体の状態が表示されます。[Site Health] ペインには、次の 3 つの接続状態が表示されます。

- [Full WAN Connectivity]：すべてのルータ上のすべての BFD セッションが稼働状態にあるサイトの総数。

- [Partial WAN Connectivity]：トンネルおよびすべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトでは、データプレーン接続が制限されています。
- [No WAN Connectivity]：すべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトにはデータプレーン接続がありません。

各サイト、ノード、またはトンネルに関する詳細情報を含むテーブルを表示するには、[Site Health]ダイアログボックスの行をクリックします。テーブルの各行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Network]**画面から [Device Dashboard] または [Real Time] ビューにアクセスするか、または**[Tools]** > **[SSH Terminal]**画面にアクセスします。

WAN エッジインターフェイスのインターフェイス使用状況の表示

[Transport Interface Distribution] ペインには、VPN 0 のすべての WAN エッジインターフェイスにおける過去 24 時間のインターフェイスの使用状況が表示されます。これには、すべての TLOC インターフェイスが含まれます。ペインをクリックして、[Transport Interface Distribution] ダイアログボックスにインターフェイスの使用状況の詳細を表示します。

WAN エッジデバイス数の表示

[WAN Edge Inventory] ペインには、次の 4 つの WAN エッジデバイスのカウントが表示されます。

- [Total]：Cisco vManage にアップロードされた WAN エッジデバイスの認証済みシリアル番号の総数。シリアル番号は**[Configuration]** > **[Devices]**画面でアップロードします。
- [Authorized]：オーバーレイネットワーク内の認証済み WAN エッジデバイスの総数。これらの WAN エッジデバイスは、**[Configuration]** > **[Certificates]** > **[WAN Edge List]**画面で [Valid] としてマークされています。
- [Deployed]：導入されている WAN エッジデバイスの総数。これらは、[Valid] とマークされ、現在ネットワークで動作している WAN エッジデバイスです。
- [Staging]：オーバーレイネットワークの一部になる前に、ステージングサイトで構成する WAN エッジデバイスの総数。これらのルータは、ルーティングの決定には関与せず、Cisco vManage によるネットワークモニタリングに影響を与えることもありません。

  ペインをクリックして、[WAN Edge Inventory] ダイアログボックスから各ルータのホスト名、システム IP、サイト ID、およびその他の詳細を表示します。

WAN エッジデバイスの集約状態の表示

[WAN Edge Health] ペインは、各状態のデバイス数のカウントを表示することで、WAN エッジデバイスの状態を集約したビューを提供し、ハードウェアノードの正常性を示します。3 つの WAN エッジデバイスの状態は次のとおりです。

- Normal：メモリ、ハードウェア、CPU が正常な状態の WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% 未満の場合は、正常な状態に分類されます。

- Warning：メモリ、ハードウェア、または CPU が注意状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% ～ 90% の場合は、注意状態に分類されます
- Error：メモリ、ハードウェア、または CPU がエラー状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 90% を超える場合は、エラー状態に分類されます。

  数値または WAN エッジデバイスの状態をクリックすると、過去 12 時間または 24 時間のメモリ使用量、CPU 使用率、およびハードウェア関連のアラーム（温度、電源、PIM モジュールなど）のテーブルが表示されます。テーブルの各行の右側にある [More Actions] アイコンをクリックして、以下にアクセスします。

  - **ハードウェア環境**
  - **[Monitor]** > **[Network]**画面から [Real Time] ビュー
  - **[Tools]** > **[SSH Terminal]**画面。

WAN エッジデバイスの損失、遅延、ジッターの表示

[Transport Health] ペインには、すべてのリンクとすべてのカラーの組み合わせ（すべての LTE-to-LTE リンク、すべての LTE-to-3G リンクなど）の集約された平均損失、遅延、およびジッターが表示されます。

[Type] ドロップダウン矢印から、損失、遅延、またはジッターを選択します。

アイコンをクリックして、トランスポートの正常性を表示する期間を選択します。

アイコンをクリックして、[Transport Health] ダイアログボックスを開きます。このダイアログボックスには、より詳細なビューが表示されます。情報を表形式で表示するには、[Details] タブをクリックします。表示される正常性のタイプと期間を変更することを選択できます。

DPI を表示 WAN エッジデバイスのフロー情報

[Top Applications] ペインには、オーバーレイネットワーク内のルータを通過するトラフィックの DPI フロー情報が表示されます。

（注） DPI フロー情報は、過去 24 時間のみ表示されます。過去 24 時間より前の DPI フロー情報を表示するには、特定のデバイスの情報を確認する必要があります。

アイコンをクリックして、データを表示する期間を選択します。[VPN] ドロップダウンリストから VPN を選択して、その VPN 内のすべてのフローの DPI 情報を表示します。

アイコンをクリックして、[Top Applications] ダイアログボックスを開きます。このダイアログボックスには、同じ情報のより詳細なビューが表示されます。VPN と期間を変更できます。

トンネルデータの表示

[Application-Aware Routing] ペインでは、[Type] ドロップダウン矢印から次のトンネル基準を選択できます。

- 損失
- 遅延
- Jitter

トンネル基準に基づいて、ペインに下位 10 件のトンネルが表示されます。たとえば、損失を選択した場合、ペインには、過去 24 時間の平均損失が最も大きい 10 のトンネルが表示されます。

行に対して アイコンをクリックすると、データがグラフィック形式で表示されます。データを表示する期間を選択するか、[Custom] をクリックして、カスタム期間を指定するためのドロップダウン矢印を表示します。

アイコンをクリックして、[Application-Aware Routing] ダイアログボックスを開きます。このダイアログボックスには、[Type] ドロップダウン矢印から選択した基準（損失、遅延、およびジッター）に基づいて下位 25 件のトンネルが表示されます。

テナント WAN エッジデバイスの管理

テナントネットワークへの WAN エッジデバイスの追加

（注） 以前に無効にしてオーバーレイネットワークから削除した WAN エッジデバイスを追加する場合は、デバイスの追加後にデバイスソフトウェアをリセットする必要があります。Cisco IOS XE SD-WAN デバイスのソフトウェアをリセットするには、**request platform software sdwan software reset** コマンドを使用します。

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、**admin** としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択し、テナントとしてのプロバイダービューを表示します。

   テナントユーザーの場合は、**tenantadmin** としてログインします。

2. デバイスのシリアル番号ファイルを Cisco vManage にアップロードします。
3. デバイスを検証し、詳細をコントローラに送信します。
4. デバイスの設定テンプレートを作成し、デバイスをテンプレートにアタッチします。

デバイスの設定中に、次の例のようにサービスプロバイダーの組織名とテナントの組織名を設定します。

```
sp-organization-name multitenancy
organization-name multitenancy-Customer1
```

（注） organization-name は <SP Org Name>-<Tenant Org Name> の形式で入力します。

5. Cisco vManage によって生成されたブートストラップ設定を使用してデバイスをブートストラップするか、デバイスで初期設定を手動で作成します。
6. エンタープライズ証明書を使用してデバイスを認証する場合は、CSR を Cisco vManage からダウンロードし、エンタープライズ CA によって署名された CSR を取得します。Cisco vManage に証明書をインストールします。

テナントネットワークからの WAN エッジデバイスの削除

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。
2. 構成テンプレートからデバイスを切り離します。
3. WAN エッジルータを削除します。

Cisco vSmart コントローラのテナント固有のポリシー

プロバイダーの **admin** ユーザー（Cisco vManage のテナントとしてのプロバイダービューから）または **tenantadmin** ユーザー（Cisco vManage のテナントビューから）は、テナントにサービスを提供する Cisco vSmart コントローラでテナント固有のポリシーを作成および展開できます。ユーザーは、CLI ポリシーを設定するか、UI ポリシー構成ウィザードを使用してポリシーを作成できます。

ポリシーをアクティブ化または非アクティブ化すると、次のようになります。

1. Cisco vManage は、テナントにサービスを提供する Cisco vSmart コントローラを識別します。
2. Cisco vManage は、ポリシー設定をプルするように Cisco vSmart コントローラに通知します。
3. Cisco vSmart コントローラは、ポリシー設定をプルして展開します。

4. Cisco vManage は、Cisco vSmart コントローラによるポリシープルのステータスを報告します。

テナントデータの管理

テナントデータのバックアップ

Cisco vManage マルチテナント機能のテナント データ バックアップ ソリューションは、次の機能を提供します。

- 構成データのバックアップファイルの作成、抽出、および表示。
- 後で復元するオプションを使用して、特定のテナントの設定データベースをバックアップします。「テナントデータのバックアップファイルの復元と削除」を参照してください。
- Cisco vManage に保存されているテナントのバックアップファイルを削除します。テナントデータ バックアップ ファイルの削除については、「テナントデータのバックアップファイルの復元と削除」をご覧ください。

データ バックアップ ソリューションを使用する場合、次の要因が適用されます。

- テナントデータ バックアップ ソリューションの操作は、テナント管理者がテナントビューで、またはプロバイダー管理者がテナントとしてのプロバイダービューで実行できます。さまざまなビューからテナントダッシュボードにアクセスする方法については、マルチテナント環境でのユーザーロール （852 ページ）を参照してください。
- テナントは、特定の時間に次のバックアップ操作を実行でき、1 つの操作を完了してから新しい操作を開始する必要があります。
  - 単一の設定データベースのバックアップ
  - バックアップファイルのダウンロード。
  - バックアップファイルの復元またはインポート
  - バックアップファイルの削除。
  - バックアップファイルの一覧表示
- テナントのバックアップファイルの形式は次のとおりです。

  ```
  Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz
  ```
- テナントデータのバックアップ操作は、設定データベースに対する読み取り専用操作です。ただし、データの整合性を確保し、データの損失を防ぐために、操作の進行中にネットワーク上で大きな変更を行わないでください。
- 複数のテナントが並行してバックアップと復元の操作を実行できます。

- テナントデータベースの復元操作が進行中の場合、テナントは他のバックアップ操作を実行できません。したがって、テナントは単一のバックアップ操作を実行でき、この操作が進行中の場合、すべての新しいバックアップ操作要求は拒否されます。

  残りのテナントは、バックアップ操作を続行できます。

- テナントは、同一の Cisco vManage ソフトウェアバージョンを実行している Cisco vManage インスタンスでバックアップおよび復元操作を実行する必要があります。
- テナントは、最大 3 つのバックアップファイルを Cisco vManage に保存でき、ダウンロードして Cisco vManage リポジトリの外部に保存できます。テナントにすでに 3 つのバックアップファイルがある場合、後続のバックアップ操作により、最も古いバックアップファイルが削除され、新しいバックアップファイルが生成されます。
- バックアップファイルと、テナントが復元操作を要求したセットアップの両方で、次のパラメータ値が一致していることを確認します。
  - テナントID（Tenant Id）
  - 組織名
  - SP Organization Name
- テナントデータのバックアップソリューションは、Cisco vManage のテナントビューにタスクを作成します。そのため、テナントはテナントダッシュボードのタスクビューから操作の進行状況を監視できます。
- プロバイダーは、このソリューションを使用してプロバイダーデータをバックアップすることはできません。したがって、プロバイダーは、CLI を使用してすべてのテナント設定データベースをバックアップすることにより、すべてのテナント情報を一度にバックアップできます。

構成データのバックアップファイルの作成、抽出、および表示

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。

2. アドレスバーで、REST API 接続の `dataservice` を使用して URL パスを変更します。

   例：`https://<tenant_URL>/dataservice`

3. 次の API を使用して構成バックアップファイルを作成します。
   `https://<tenant_URL>/dataservice/tenantbackup/export`。

4. 構成バックアップファイルが正常に作成されると、Cisco vManage タスクビューにバックアップファイルが生成されたことが示されます。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

   例：

   ```
   {
      "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
   "status": "in-progress"
   }
   ```

5. 取得したプロセス識別子でタスクの状態を確認します。

   例：
   `https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061`

   検証により、タスクの詳細が JSON ファイル形式で生成されます。

6. タスクが完了したら、JSON タスクファイルの [data] セクションにあるバックアップファイルを抽出またはダウンロードします。

   例：バックアップファイルを抽出またはダウンロードするには、次の API を使用します。
   `https://<tenannt_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

7. 次の API を使用して、Cisco vManage に保存されているバックアップファイルを一覧表示します。

   例：`https://<tenant_URL>//dataservice/tenantbackup/list`

テナントデータのバックアップファイルの復元と削除

始める前に

テナント データ バックアップ ファイルの復元および削除 API を実行するには、Postman ツールまたはhttpアプリケーションとサービスをテストするための他の代替ツールをダウンロードしてインストールします。このドキュメントでは、Postman ツールを使用してテナントデータのバックアップファイルを復元および削除する手順を説明しました。Postman は、API 開発環境として使用されるソフトウェアツールです。このツールは、Postman の Web サイトからダウンロードできます。

1. Google Chrome または別のブラウザを開き、開発者モードを有効にします。
2. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。

3. 復元 API のヘッダー情報を取得するには、次のようにします。
   1. 画面の右側で、[Network] タブをクリックして、ネットワーク キャプチャ ビューを表示します。

2. ネットワーク キャプチャ ビューで、[Name] 列をクリックして、リストされている項目を並べ替えます。
3. index.html を検索してクリックします。
4. [Headers] タブをクリックし、[Request Headers] を展開します。
5. Request Headers の下のすべてのテキストを選択し、クリップボードにコピーします。

4. Postman UI を使用してバックアップファイルをインポートします。
   1. Postman UI を開きます。
   2. SSL 証明書の検証を無効にするには、**[Postman]** > **[Preferences]** > **[General]** > **[Request]** をクリックします。[SSL Certificate Verification] をオフにします。
   3. Postman UI で、新しいタブを作成します。
   4. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
   5. [Request Headers] ブロックからステップ 3 でコピーしたテキストを、編集可能なフォームに貼り付けます。
   6. [GET] メソッド ドロップダウン リストから、[POST] を選択します。
   7. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、`dataservice/tenantbackup/import` を含めます。

      例：`https://customer1.managed-sp.com/dataservice/tenantbackup/import`
   8. [Body] タブをクリックし、[form-data] を選択します。
   9. [KEY] 列に *bakup.tar.gz* と入力します。
   10. [VALUE] 列で、[Select Files] をクリックし、インポートするバックアップファイルを選択します。
   11. API を実行するには、[Send] をクリックします。

       Postman UI の [Response] セクションで、復元されたファイルを示す JSON 情報を表示できます。

5. 次のいずれかの方法で、バックアップファイルの復元を監視します。
   1. バックアップファイルが正常にインポートされたかどうかを示す Cisco vManage タスク ビューを使用します。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

      例：

      ```
      {"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
          "status": "Import Successfully Submitted for tenant 1579026919487"
      }
      ```
   2. 次の URL を使用してステータスを取得します。`https://<tenant_URL>/dataservice/device/action/status/<processId>`

例：
`https://customer1.managed-sp.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d`

6. Postman UI を使用してテナントデータのバックアップファイルを削除します。
   1. Postman UI で、新しいタブを作成します。
   2. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
   3. [Request Headers] ブロックからステップ 3 でコピーしたテキストを、編集可能なフォームに貼り付けます。
   4. [GET] メソッド ドロップダウン リストから [DELETE] を選択します。
   5. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、`dataservice/tenantbackup/delete?fileName='filename'` を含めます。ファイル名には、バックアップファイルの名前または all を指定できます。

      例：
      `https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz`

      例：`https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=all`
   6. API を実行するには、[Send] をクリックします。

   Postman UI の [Response] セクションで、削除されたファイルを示す JSON 情報を表示できます。

   例：

```
{
    "Deleted": [
        "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
    ]
}
```

Cisco vSmart コントローラでのテナントごとの OMP 統計表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. 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。
3. デバイスのテーブルで、Cisco vSmart コントローラのホスト名をクリックします。
4. 左側のペインで、[Real Time] をクリックします。
5. [Device Options] フィールドに [OMP] と入力し、表示する OMP 統計を選択します。

6. [Select Filters] ダイアログボックスで [Show Filters] をクリックします。
7. [Tenant Name] を入力し、[Search] をクリックします。

Cisco vManage は、特定のテナントの選択された OMP 統計を表示します。

Cisco vSmart コントローラに関連付けられたテナントの表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. **vSmart** 接続番号をクリックし、各接続に関する詳細情報を示す表を表示します。

   Cisco vManage は、Cisco vSmart コントローラとその接続の概要を示す表を表示します。
3. Cisco vSmart コントローラの場合は、[...] をクリックし、[Tenant List] をクリックします。

   Cisco vManage は、Cisco vSmart コントローラに関連付けられたテナントの概要を表示します。

シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行

はじめる前に

- 移行を開始する前に、次の手順を実行します。
  - シングルテナントオーバーレイからマルチテナント展開への移行は、オンプレミスに展開された Cisco SD-WAN コントローラでのみサポートされます。クラウドホスト型の Cisco SD-WAN コントローラでは、移行はまだサポートされていません。
  - シングルテナント展開のエッジデバイスがマルチテナント展開の Cisco vBond Orchestrator に到達できることを確認します
  - エッジデバイスのテンプレート、ルーティング、およびポリシー構成が Cisco vManage の現在の構成と同期していることを確認します
  - この手順を実行する前に、シングル テナント オーバーレイのメンテナンスウィンドウを構成します。「Configure or Cancel vManage Server Maintenance Window」を参照してください。
- 移行するシングルテナント オーバーレイの最小ソフトウェア要件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

- シングルテナントオーバーレイの移行先となるマルチテナント展開の最小ソフトウェア要件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.6.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.6.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.6.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.6.1a

- Cisco SD-WAN コントローラと WAN エッジデバイスのソフトウェアバージョンは、シングルテナント展開とマルチテナント展開の両方で同一である必要があります。
- API 呼び出しを実行するには、カスタムスクリプトまたは Postman などのサードパーティアプリケーションを使用することをお勧めします。

移行手順

1. オーバーレイを制御する Cisco vManage インスタンスからシングルテナントの展開および構成データをエクスポートします。

メソッド	`POST`
URL	`https://ST-vManage-IP-address`
エンドポイント	`/dataservice/tenantmigration/export`
許可	管理者ユーザーログイン情報。

本文	必須 フォーマット：Raw JSON `{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }` Field Description: • desc：テナントの説明。説明の最大長は 256 文字で、英数字のみを使用できます。 • name：マルチテナント展開のテナントの一意の名前。 • subdomain：テナントの完全修飾サブドメイン名。サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、managed-sp.com がサービスプロバイダーのドメイン名であり、テナント名が Customer1 である場合、テナントのサブドメイン名は customer1.managed-sp.com になります。 • orgName：テナント組織の名前。組織名では、大文字と小文字が区別されます。
応答	フォーマット：JSON `{ "processId": <vManage_process_ID>, }`

データのエクスポート中に、Cisco vManage は、マルチテナント展開への移行に備えて、エッジデバイスから CLI テンプレートを切り離そうとします。Cisco vManage によってプロンプトが表示された場合は、CLI テンプレートをエッジデバイスから切り離し、エクスポート API 呼び出しを再度実行します。

2. Cisco vManage でデータエクスポートタスクのステータスを確認します。タスクが成功したら、URL `https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz` を使用してデータをダウンロードします

3. マルチテナント Cisco vManage インスタンスで、シングルテナント オーバーレイからエクスポートされたデータをインポートします。

メソッド	POST
URL	https://*MT-vManage-IP-address*
エンドポイント	/dataservice/tenantmigration/import
許可	プロバイダー管理者ユーザーログイン情報。

本文	必須 フォーマット：フォームデータ キータイプ：ファイル 値：`default.tar.gz`

応答	フォーマット：JSON
	`{`
	`"processId": <vManage_process_ID>,`
	`"migrationTokenURL": <token_URL>,`
	`}`

タスクが成功すると、マルチテナント Cisco vManage で、シングルテナント オーバーレイからインポートされたデバイス、テンプレート、およびポリシーを表示できます。

4. **手順 3** の API 呼び出しに応答して取得したトークン URL を使用して、移行トークンを取得します。

方法	`GET`
URL	`https://MT-vManage-IP-address`
エンドポイント	**手順 3** で取得した `migrationTokenURL`。
許可	プロバイダー管理者ユーザーログイン情報。
応答	エンコードされたテキストの大きな BLOB としての移行トークン。

5. シングルテナント Cisco vManage インスタンスで、マルチテナント展開へのオーバーレイの移行を開始します。

メソッド	`POST`
URL	`https://ST-vManage-IP-address`
エンドポイント	`dataservice/tenantmigration/networkMigration`
許可	管理者ユーザーログイン情報。
本文	必須 フォーマット：生のテキスト 内容：**手順 4** で取得した移行トークン。

応答	フォーマット：JSON
	`{`
	`"processId": <vManage_process_ID>,`
	`}`

Cisco vManage で、移行タスクのステータスを確認します。移行タスクの一部として、マルチテナント vBond Orchestrator のアドレス、サービスプロバイダーおよびテナントの組織名が、シングルテナント オーバーレイの WAN エッジデバイスにプッシュされます。タス

クが成功すると、WAN エッジデバイスはマルチテナント展開のコントローラへの制御接続を形成します。WAN エッジデバイスは、シングル テナント オーバーレイのコントローラに接続されなくなります。

マルチテナント展開への移行後に、（手順 1 で）エッジデバイスから切り離された CLI テンプレートを接続します。テンプレートを接続する前に、マルチテナント展開の構成と一致するように Cisco vBond Orchestrator の IP アドレスと組織名を更新します。

（注） シングルテナント展開では、Cisco vManage 署名付き証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、デバイスがマルチテナント展開に移行されるときに証明書がクリアされます。マルチテナント Cisco vManage でデバイスを再認証する必要があります。エンタープライズ証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、証明書は移行の影響を受けません。詳細については、「Enterprise Certificates」を参照してください。

マルチテナント Cisco SD-WAN オーバーレイの移行

表 *223 :* 機能の履歴

機能名	リリース情報	説明
マルチテナント Cisco SD-WAN オーバーレイの移行	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、共有 Cisco vManage インスタンスと Cisco vBond Orchestrator で構成されるマルチテナント Cisco SD-WAN オーバーレイ、およびテナント固有の Cisco vSmart コントローラを、共有 Cisco vManage インスタンス、Cisco vBond Orchestrator、および Cisco vSmart コントローラで構成されるマルチテナントオーバーレイに移行できます。

前提条件

移行するマルチテナントオーバーレイ内の Cisco SD-WAN コントローラおよび WAN エッジデバイスの最小ソフトウェア要件：

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.3.3
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.3.3

デバイス	ソフトウェア バージョン
Cisco vSmart Controller	Cisco SD-WAN リリース 20.3.3
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.3.3

制約事項

- この移行手順は、オンプレミスに展開された Cisco SD-WAN コントローラにのみ適用されます。
- マルチテナントオーバーレイは、Cisco vManage インスタンスが Cisco vManage リリース 20.6.1 ソフトウェアを実行し、Cisco SD-WAN コントローラが Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行するセットアップにのみ移行できます。
- この移行手順を使用して、複数のマルチテナントオーバーレイをマージすることはできません。新しいセットアップに一度に移行できるマルチテナントオーバーレイは1つだけです。

移行手順

1. クラスタ内の 3 つの Cisco vManage インスタンスのソフトウェアを Cisco vManage リリース 20.6.1 にアップグレードします。詳細については、「Upgrade Cisco vManage Cluster」を参照してください。

（注） いずれかの Cisco vManage インスタンスのみで、**request nms configuration-db upgrade** コマンドを実行します。

2. Cisco vManage ソフトウェアが Cisco vManage リリース 20.6.1 にアップグレードされたら、Cisco vManage GUI にログインします。

   新しいパスワードの設定を求めるメッセージが表示されます。

   1. パスワードガイドラインに準拠した新しいパスワードを入力します。

3. Cisco SD-WAN リリース 20.6.1 ソフトウェアを Cisco vManage にアップロードします。詳細については、「Add an Image to the Software Repository」を参照してください。
4. Cisco vBond Orchestrator ソフトウェアを Cisco SD-WAN リリース 20.6.1 にアップグレードします。詳細については、「Upgrade the Software Image on a Device」を参照してください。
5. Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行する 2 つの Cisco vSmart コントローラ インスタンスを作成します。「Deploy the Cisco vSmart Controller」を参照してください。

（注） 2 つの Cisco vSmart コントローラインスタンスで、最大 24 のテナントをサポートできます。最大 50 のテナントをサポートする場合は、6 つの Cisco vSmart コントローラインスタンスを作成します。

1. オーバーレイネットワークに Cisco vSmart コントローラの追加 します。

[Provider Dashboard] には、Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行している新しい Cisco vSmart コントローラが表示されます。[Tenant Dashboard] には、Cisco SD-WAN リリース 20.3.3 ソフトウェアを実行している古い Cisco vSmart コントローラが表示されます。

6. Cisco vManage でメンテナンスウィンドウを有効にします。詳細については、「Configure or Cancel vManage Server Maintenance Window」を参照してください。

3 ～ 4 時間のメンテナンスウィンドウをお勧めします。

7. Cisco SD-WAN リリース 20.3.3 ソフトウェアを実行している古いテナント固有の Cisco vSmart コントローラから、Cisco SD-WAN リリース 20.6.1 ソフトウェアを実行している新しい共有 Cisco vSmart コントローラにテナント設定を移行します。

メソッド	`POST`
URL	`https://<vmanageip>:<port>`
エンドポイント	`dataservice/tenant/vsmart-mt/migrate`
許可	プロバイダーの **admin** ユーザーログイン情報。
本文	必須 フォーマット：Raw JSON `{}`
応答	フォーマット：JSON `{ "processId": <vManage_process_ID>, }`

Cisco vManage で、API 応答の `processId` を使用して、移行タスクのステータスを確認します。移行タスク中に、次の変更が反映されます。

1. 古い Cisco vSmart コントローラは無効化され、オーバーレイネットワークから削除されます。
2. テナントビューでは、古い Cisco vSmart コントローラが [Tenant Dashboard] および、[Devices] と [Certificates] のページから削除されます。
3. テナント WAN エッジデバイスは、新しい Cisco vSmart コントローラに接続されます。

8. （オプション）Cisco IOS XE SD-WAN デバイスソフトウェアを Cisco IOS XE リリース 17.6.1a にアップグレードします。詳細については、「Upgrade the Software Image on a Device」および「Activate a New Software Image」を参照してください。

ヒント　マルチテナントオーバーレイを移行するのと同じメンテナンスウィンドウで、テナント WAN エッジデバイスソフトウェアをアップグレードする必要はありません。ただし、移行から数週間以内にテナント WAN エッジデバイスソフトウェアをアップグレードすることをお勧めします。

移行の確認

1. プロバイダービューで、次のチェックを実行します。
   1. [Main Dashboard] ページで、テナント WAN エッジデバイスが新しいマルチテナント Cisco vSmart コントローラに接続されているかどうかを確認します。
   2. Cisco vSmart コントローラに関連付けられたテナントの表示 （887 ページ）。
   3. Cisco vSmart コントローラ CLI で、**show control connections** コマンドを実行します。コマンド出力で、Cisco vSmart コントローラとテナント WAN エッジデバイスの間に制御接続が確立されていることを確認します。
2. テナントとしてのプロバイダービューで、マルチテナント Cisco vSmart コントローラが [Tenant Dashboard] に表示されるかどうかを確認します。

Cisco SD-WAN コントローラおよびエッジデバイスソフトウェアのアップグレード

前提条件

Cisco SD-WAN コントローラおよび WAN エッジデバイスの最小ソフトウェア要件：

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.4.1 以降
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.4.1 以降
Cisco vSmart Controller	Cisco SD-WAN リリース 20.4.1 以降
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1 以降

アップグレード手順

1. クラスタ内の 3 つの Cisco vManage インスタンスのソフトウェアを Cisco vManage リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「Upgrade Cisco vManage Cluster」を参照してください。

（注） **request nms configuration-db upgrade** コマンドを使用して configuration-db サービスをアップグレードする手順をスキップします。

2. Cisco vManage ソフトウェアを Cisco vManage リリース 20.6.1 またはそれ以降のリリースにアップグレードしたら、Cisco vManage GUI にログインします。
3. Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースおよび Cisco IOS XE リリース 17.6.1a またはそれ以降のリリースのソフトウェアを Cisco vManage にアップロードします。詳細については、「Add an Image to the Software Repository」を参照してください。
4. Cisco vBond Orchestrator ソフトウェアを Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「Upgrade the Software Image on a Device」および「Activate a New Software Image」を参照してください。
5. Cisco vManage でメンテナンスウィンドウを有効にします。詳細については、「Configure or Cancel vManage Server Maintenance Window」を参照してください。
6. Cisco vSmart コントローラソフトウェアを Cisco SD-WAN リリース 20.6.1 またはそれ以降のリリースにアップグレードします。詳細については、「Upgrade the Software Image on a Device」および「Activate a New Software Image」を参照してください。
7. Cisco IOS XE SD-WAN デバイスソフトウェアを Cisco IOS XE リリース 17.6.1a またはそれ以降のリリースにアップグレードします。詳細については、「Upgrade the Software Image on a Device」および「Activate a New Software Image」を参照してください。

ヒント 同じメンテナンスウィンドウ内で WAN エッジデバイスソフトウェアをアップグレードすることをお勧めします。OMP グレースフル リスタート ウィンドウ内で WAN エッジデバイスソフトウェアがアップグレードされない場合、トラフィックが失われる可能性があります。

マルチテナント Cisco vManage：ディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。

スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。

2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。

3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

ディザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする 1 つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

前提条件

- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードの数は同じである必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、同じ Cisco vManage ソフトウェアリリースを実行する必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、オーバーレイネットワーク内の Cisco vBond Orchestrator の WAN トランスポート IP アドレスに接続できる必要があります。
- 最初に、スタンバイクラスタの Cisco vManage ノードのトンネルインターフェイスを無効にする必要があります。
- スタンバイクラスタの Cisco vManage ノードは認定されている必要があります。
- スタンバイクラスタのすべての Cisco vManage ノードのクロックは、オーバーレイネットワーク内の Cisco SD-WAN コントローラおよび WAN エッジデバイスのクロックと同期されている必要があります。オーバーレイで NTP が設定されている場合は、スタンバイ Cisco vManage ノードでも同様に設定します。
- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードは、同一の neo4j ログイン情報を使用する必要があります。

制約事項

- 設定データベースのバックアップ中は、アクティブなプロセスを中断しないでください。

- SD-AVC を有効にする場合は、スタンバイ Cisco vManage ノードで設定データベースを復元する前に行う必要があります。

スタンバイ Cisco vManage クラスタの設定

1. アクティブな Cisco vManage ノードと同様の実行中の設定でスタンバイ Cisco vManage ノードを設定します。スタンバイ Cisco vManage ノードにローカル証明書をインストールします。

（注） スタンバイ Cisco vManage の実行コンフィギュレーションは、通常、アクティブな Cisco vManage ノードの実行コンフィギュレーションと同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。

3. スタンバイ Cisco vManage ノードを使用してスタンバイクラスタを作成します。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db backup path** *file-path*

   このコマンドは、設定データベースを `.tar.gz` ファイルにバックアップし、そのファイルを指定された *file-path* に保存します。

   次の例では、データベースは、`/home/admin/` ディレクトリの `db_backup.tar.gz` という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

   次の例では、`db_backup.tar.gz` がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの `/home/admin/` ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
```

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                                  100%  399KB   4.4MB/s   00:00
```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。

（注）
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
- 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

1. スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db restore path** *file-path*

   次の例では、バックアップファイル db_backup.tar.gz を使用して設定データベースを復元します。

   ```
   Standby-vManage# request nms configuration-db restore path
   /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。

3. すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。

   1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** > **[Controllers]** を選択します。
   2. ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。

4. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

   次の 2 つの方法のいずれかを使用します。

   1. VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

5. 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。
   1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
   2. [Controllers] をクリックします。
   3. Cisco vBond Orchestrator で、[...] をクリックし、[Edit] をクリックします。
   4. [Edit] ダイアログボックスで、Cisco vBond Orchestrator の詳細（WAN トランスポート IP アドレス、ユーザー名、およびパスワード）を入力します。
   5. すべての Cisco vBond Orchestrator について、**ステップ 5c** と**ステップ 5d** を繰り返します。

6. アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。

（注） 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

コントローラのリストの送信：

1. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
2. [Controllers] をクリックします。
3. [Send to vBond] をクリックします。

   設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

   - スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
   - 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
   - アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
   - すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。

4. [WAN Edge List] をクリックします。
5. [Send to Controllers] をクリックします。

8. 以下が失われていないことを確認します。
   - ポリシー
   - テンプレート （Templates）
   - コントローラと WAN エッジデバイスのリスト
9. 有効な Cisco vManage ノードを確認します。
   1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

      コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。
   2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

      コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。
10. 以前にアクティブだった Cisco vManage ノードを無効にします。

（注） Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
2. [Controllers] をクリックします。
3. 以前にアクティブだった Cisco vManage ノードごとに、[...] をクリックし、[Invalidate] をクリックします。

11. 有効な Cisco vManage ノードを確認します。

1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

   コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。

2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

   コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

マルチテナント Cisco vManage：仮想ルータを使用したオーバーレイネットワークでのディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。

   スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。

2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。

3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

ディザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする 1 つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

次のディザスタリカバリ手順は、Cisco vEdge Cloud ルータがブランチロケーションに導入されているオーバーレイネットワークに適用されます。

前提条件

- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードの数は同じである必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、同じ Cisco vManage ソフトウェアリリースを実行する必要があります。
- アクティブクラスタとスタンバイクラスタの各 Cisco vManage ノードは、オーバーレイネットワーク内の Cisco vBond Orchestrator の WAN トランスポート IP アドレスに接続できる必要があります。
- 最初に、スタンバイクラスタの Cisco vManage ノードのトンネルインターフェイスを無効にする必要があります。
- スタンバイクラスタの Cisco vManage ノードは認定されている必要があります。
- スタンバイクラスタのすべての Cisco vManage ノードのクロックは、オーバーレイネットワーク内の Cisco SD-WAN コントローラおよび WAN エッジデバイスのクロックと同期されている必要があります。オーバーレイで NTP が設定されている場合は、スタンバイ Cisco vManage ノードでも同様に設定します。
- アクティブクラスタとスタンバイクラスタの Cisco vManage ノードは、同一の neo4j ログイン情報を使用する必要があります。

制約事項

- 設定データベースのバックアップ中は、アクティブなプロセスを中断しないでください。
- SD-AVC を有効にする場合は、スタンバイ Cisco vManage ノードで設定データベースを復元する前に行う必要があります。

スタンバイ Cisco vManage クラスタの設定

1. アクティブな Cisco vManage ノードと同様の実行中の設定でスタンバイ Cisco vManage ノードを設定します。スタンバイ Cisco vManage ノードにローカル証明書をインストールします。

（注） スタンバイ Cisco vManage の実行中の設定は、通常、アクティブな Cisco vManage ノードの実行中の設定と同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。

3. スタンバイ Cisco vManage ノードを使用してスタンバイクラスタを作成します。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db backup path** *file-path*

   このコマンドは、設定データベースを `.tar.gz` ファイルにバックアップし、そのファイルを指定された *file-path* に保存します。

   次の例では、データベースは、`/home/admin/` ディレクトリの `db_backup.tar.gz` という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

   次の例では、`db_backup.tar.gz` がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの `/home/admin/` ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5
```

```
admin@10.126.93.92's password:
db_backup.tar.gz                              100%  399KB   4.4MB/s   00:00
```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。

（注）
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
- 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

1. スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db restore path** *file-path*

   次の例では、バックアップファイル db_backup.tar.gz を使用して設定データベースを復元します。

   ```
   Standby-vManage# request nms configuration-db restore path
   /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。

3. すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。

   1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** > **[Controllers]** を選択します。
   2. ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。

4. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

   コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。

5. Cisco vEdge Cloud ルータの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。

6. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。

2. [Controllers] をクリックします。

3. Cisco vBond Orchestrator で、[...] をクリックし、[Edit] をクリックします。

4. [Edit] ダイアログボックスで、Cisco vBond Orchestrator の詳細（WAN トランスポート IP アドレス、ユーザー名、およびパスワード）を入力します。

5. すべての Cisco vBond Orchestrator について、**ステップ 7c** と**ステップ 7d** を繰り返します。

8. アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。

（注） 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

9. スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

   コントローラのリストの送信：

   1. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
   2. [Controllers] をクリックします。
   3. [Send to vBond] をクリックします。

      設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

      - スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
      - 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
      - アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
      - すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。

   4. [WAN Edge List] をクリックします。
   5. [Send to Controllers] をクリックします。

10. 以下が失われていないことを確認します。

    - ポリシー
    - テンプレート （Templates）
    - コントローラと WAN エッジデバイスのリスト

11. 有効な Cisco vManage ノードを確認します。

    1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

       コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。

    2. Cisco vEdge Cloud ルータの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

12. 以前にアクティブだった Cisco vManage ノードを無効にします。

以前にアクティブだった Cisco vManage は、クラウド WAN エッジデバイスの証明書発行者です。アクティブな Cisco vManage は、以前にアクティブだった Cisco vManage ノードが無効化された後にのみ、クラウド WAN エッジデバイスに証明書を発行します。

（注）
- Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。
- 以前にアクティブだった Cisco vManage ノードを無効にすると、Cisco vManage はノードを無効としてマークし、すべてのコントローラに更新を送信します。ただし、以前にアクティブだった Cisco vManage はクラウド WAN エッジデバイスの CA であるため、Cisco vManage は有効な Cisco vManage UUID の更新されたリストを Cisco vBond Orchestrator にすぐには送信しません。したがって、Cisco vBond Orchestrator での **show orchestrator valid-vmanage-id** コマンドの出力には、無効化された Cisco vManage ノードの UUID が含まれます。

  Cisco vManage には、24 時間ごとに実行されるスケジュールされたタスクがあり、すべてのクラウド WAN エッジがアクティブな Cisco vManage に移動されたかどうかを確認します。Cisco vManage は、クラウド WAN エッジデバイスがアクティブな Cisco vManage に移動された後にのみ、有効な Cisco vManage UUID の更新されたリストを Cisco vBond Orchestrator に送信します。このリストを受信した後、Cisco vBond Orchestrator での **show orchestrator valid-vmanage-id** コマンドの出力には、無効化された Cisco vManage ノードの UUID は含まれません。

1. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
2. [Controllers] をクリックします。
3. 以前にアクティブだった Cisco vManage ノードごとに、[...] をクリックし、[Invalidate] をクリックします。

13. 24 時間後に有効な Cisco vManage ノードを確認します。

1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

   コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。

2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

マルチテナント Cisco vManage：障害が発生したデータセンターが稼働状態になった後のディザスタリカバリ

マルチテナント Cisco vManage クラスタ、またはクラスタ内の Cisco vManage ノードをホストするデータセンターに障害が発生した場合、スタンバイ Cisco vManage クラスタをアクティブ化することで障害から回復できます。ディザスタリカバリは次のように実行できます。

1. スタンバイ Cisco vManage クラスタを展開して設定します。

   スタンバイ Cisco vManage クラスタはオーバーレイネットワークの一部ではなく、アクティブではありません。

2. アクティブな Cisco vManage クラスタの設定データベースを定期的にバックアップします。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、設定データベースをバックアップします。

3. アクティブな Cisco vManage クラスタに障害が発生した場合は、スタンバイ Cisco vManage クラスタで最新の設定データベースを復元し、スタンバイ Cisco vManage クラスタをアクティブにして、以前にアクティブだった Cisco vManage クラスタをオーバーレイネットワークから削除します。

   設定データベースサービスをホストするクラスタ内の Cisco vManage ノードを選択し、以前にアクティブだった Cisco vManage クラスタからバックアップした設定データベースを復元します。

ディザスタリカバリをテストするには、アクティブな Cisco vManage クラスタに障害が発生するシナリオをシミュレートします。このような障害をシミュレートする 1 つの方法は、このドキュメントで説明されているようにトンネルインターフェイスを無効にすることです。

次の手順は、最初にアクティブだった Cisco vManage クラスタ、またはクラスタをホストするデータセンターに障害が発生し、スタンバイ Cisco vManage クラスタがアクティブな Cisco vManage クラスタになるように設定されているシナリオに適用されます。最初にアクティブだったクラスタが再び動作可能になると、スタンバイクラスタとして機能します。以下の手順を完了することで、このスタンバイクラスタをアクティブクラスタに変えることができます。

スタンバイ vManage NMS の設定の確認

1. スタンバイ Cisco vManage ノードの実行中の設定がアクティブな Cisco vManage ノードの実行中の設定と同様かどうかを確認します。ローカル証明書は、スタンバイ Cisco vManage ノードにインストールされている必要があります。

（注） スタンバイ Cisco vManage の実行中の設定は、通常、アクティブな Cisco vManage ノードの実行中の設定と同じです。ただし、システム IP アドレスやトンネルインターフェイス IP アドレスなどの設定が一意であることは確認する必要があります。

2. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスをシャットダウンします。CLI で、トランスポート インターフェイス設定に **shutdown** コマンドを含めます。

この方法で設定されたスタンバイ Cisco vManage ノードでは、オーバーレイネットワークはスタンバイ Cisco vManage クラスタを認識しません。

アクティブな Cisco vManage クラスタ設定のバックアップ

アクティブな Cisco vManage クラスタの完全な設定データベースを定期的にバックアップします。また、アクティブな Cisco vManage 仮想マシンのスナップショットを作成します。

1. 設定データベースサービスをホストするアクティブな Cisco vManage ノードを選択し、設定データベースのバックアップをエクスポートします。Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db backup path** *file-path*

   このコマンドは、設定データベースを .tar.gz ファイルにバックアップし、そのファイルを指定された *file-path* に保存します。

   次の例では、データベースは、/home/admin/ ディレクトリの db_backup.tar.gz という名前のファイルにバックアップされます。

```
Active-vManage# request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

2. 設定データベースサービスをホストするスタンバイ Cisco vManage ノードを選択し、設定データベースのバックアップをこのノードにコピーします。

   次の例では、db_backup.tar.gz がアクティブな Cisco vManage ノードからスタンバイ Cisco vManage ノードの /home/admin/ ディレクトリにコピーされます。

```
Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                              100%  399KB   4.4MB/s   00:00
```

設定データベースのバックアップを使用した Cisco vManage クラスタの復元

このバックアップをコピーしたスタンバイ Cisco vManage ノードで、アクティブな Cisco vManage クラスタからの設定データベースの最新バックアップを復元します。

（注）
- 復元操作では、設定データベースに含まれるすべての情報が復元されるわけではありません。ユーザーやリポジトリなどの Cisco vManage 設定は、バックアップを使用して設定データベースを復元した後、スタンバイ Cisco vManage ノードで設定する必要があります。
- 次の手順を完了すると、以前にアクティブだった Cisco vManage ノードは再利用できなくなります。ノードを再利用するには、このドキュメントの範囲を超える追加手順を実行する必要があります。

1. スタンバイ Cisco vManage ノードの CLI で、次のコマンドを実行します。**request nms configuration-db restore path** *file-path*

   次の例では、バックアップファイル db_backup.tar.gz を使用して設定データベースを復元します。

   ```
   Standby-vManage# request nms configuration-db restore path
   /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. 適切なサービスがスタンバイ Cisco vManage ノードで実行されていることを確認します。各スタンバイ Cisco vManage ノードの CLI で、**request nms all status** コマンドを実行します。コマンド出力から、ノードで実行されているサービスを確認します。

3. すべてのスタンバイ Cisco vManage ノードに、アクティブおよびスタンバイ Cisco vManage ノードの全リストがあることを確認します。

   1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** > **[Controllers]** を選択します。
   2. ページにすべてのアクティブおよびスタンバイ Cisco vManage ノードが表示されていることを確認します。

4. スタンバイ Cisco vManage ノードで、VPN 0 のトランスポート インターフェイスを有効にします。

   次の 2 つの方法のいずれかを使用します。

   1. VPN 0 のトランスポート インターフェイスを有効にします。各スタンバイ Cisco vManage ノードの CLI で、**no shutdown** コマンドを実行します。

      ```
      Active-vManage# config
      Active-vManage(config)# vpn 0 interface interface-name
      Active-vManage(config-interface)# no shutdown
      Active-vManage(config-interface)# commit and-quit
      ```

   2. VPN 0 のトンネルインターフェイスをアクティブにします。各スタンバイ Cisco vManage ノードの CLI で、**tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

5. 各スタンバイ Cisco vManage ノードをオーバーレイネットワークに追加します。
   1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
   2. [Controllers] をクリックします。
   3. Cisco vBond Orchestrator で、[...] をクリックし、[Edit] をクリックします。
   4. [Edit] ダイアログボックスで、Cisco vBond Orchestrator の詳細（WAN トランスポート IP アドレス、ユーザー名、およびパスワード）を入力します。
   5. すべての Cisco vBond Orchestrator について、**ステップ 5c** と**ステップ 5d** を繰り返します。

6. アクティブな Cisco vManage ノードをオーバーレイネットワークから接続解除します。

（注） 災害シナリオをシミュレートするラボ環境では、このステップを実行できます。しかし、実際の災害シナリオで Cisco vManage インスタンスに到達できない場合、このステップは実行できない可能性があり、省略できます。

次の 2 つの方法のいずれかを使用します。

1. VPN 0 のトランスポート インターフェイスをシャットダウンします。アクティブな各 Cisco vManage ノードの CLI で、**shutdown** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

2. VPN 0 のトンネルインターフェイスを非アクティブにします。アクティブな各 Cisco vManage ノードの CLI で、**no tunnel-interface** コマンドを実行します。

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. スタンバイ Cisco vManage から、更新されたコントローラとデバイスのリストを Cisco vBond Orchestrator に送信します。

   コントローラのリストの送信：

   1. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
   2. [Controllers] をクリックします。
   3. [Send to vBond] をクリックします。

設定タスクが完了するまで待ちます。タスクが完了すると、次のようになります。

- スタンバイ Cisco vManage ノードがアクティブな Cisco vManage ノードになります。
- 以前にアクティブだった Cisco vManage ノードはオーバーレイネットワークの一部ではなくなります。
- アクティブな Cisco vManage ノードの設定は、最新の設定データベースバックアップからの設定になります。
- すべてのコントローラがネットワーク内の他のコントローラとの接続を確立します。

4. [WAN Edge List] をクリックします。
5. [Send to Controllers] をクリックします。

8. 以下が失われていないことを確認します。
   - ポリシー
   - テンプレート （Templates）
   - コントローラと WAN エッジデバイスのリスト

9. 有効な Cisco vManage ノードを確認します。
   1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

      コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。
   2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

      コマンド出力で、アクティブな Cisco vManage ノードと以前にアクティブだった Cisco vManage ノードのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

10. 以前にアクティブだった Cisco vManage ノードを無効にします。

（注） Cisco vManage ノードを無効にした後は、このドキュメントの範囲を超える追加手順を実行しない限り、ノードを再利用することはできません。

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

3. 以前にアクティブだった Cisco vManage ノードごとに、[...] をクリックし、[Invalidate] をクリックします。

11. 有効な Cisco vManage ノードを確認します。

    1. 各 Cisco vBond Orchestrator の CLI にログインし、**show orchestrator valid-vmanage-id** コマンドを実行します。

       コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。

    2. WAN エッジデバイスの CLI にログインし、**show control valid-vmanage-id** コマンドを実行します。

       コマンド出力で、アクティブな Cisco vManage ノードのみのシャーシ番号がリストされていることを確認します。また、デバイスがアクティブな Cisco vManage ノードおよび Cisco vSmart コントローラに接続されているかどうかを確認します。

当初はスタンバイクラスタであった Cisco vManage クラスタが、アクティブな Cisco vManage クラスタになりました。

障害が発生した Cisco vSmart コントローラの交換

障害のある Cisco vSmart コントローラを新しいインスタンスで置き換えるには、次の手順に従います。

1. Cisco vSmart コントローラインスタンスを作成します。「Deploy the Cisco vSmart Controller」を参照してください。
2. オーバーレイネットワークに Cisco vSmart コントローラの追加 。
3. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
4. [Controllers] をクリックします。
5. 障害のある Cisco vSmart コントローラに対して、[...] をクリックし、[Invalidate] をクリックします。

   [Invalidate] ダイアログボックスが表示されます。

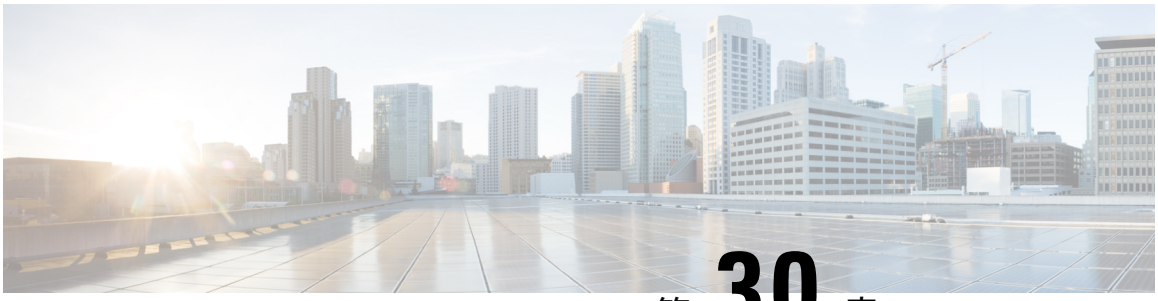
（注） 障害のある Cisco vSmart コントローラを置き換えることができる新しい Cisco vSmart コントローラを追加していない場合、Cisco vManage はエラーメッセージを通じてこのことを示します。[Invalidate] ダイアログボックスで [Cancel] をクリックし、新しい Cisco vSmart コントローラを追加してから、障害のあるインスタンスを無効化します。

6. [Invalidate] ダイアログボックスで、次の操作を行います。

   1. [Replace vSmart] チェックボックスをオンにします。

2. [Select vSmart] ドロップダウンリストから、障害のあるインスタンスを置き換える新しい Cisco vSmart コントローラを選択します。
3. [Invalidate] をクリックします。

Cisco vManage で、[Invalidate Device] および [Push CLI Template Configuration] タスクが起動します。これらのタスクが完了すると、障害のある Cisco vSmart コントローラが無効化され、オーバーレイネットワークから削除されます。障害のある Cisco vSmart コントローラがサービスを提供していたテナントは、置き換えとして選択した新しい Cisco vSmart コントローラが対応するようになりました。



第 30 章

マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置

表 *224 :* 機能の履歴

機能名	リリース情報	説明
マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置	Cisco vManage リリース 20.9.1	この機能を使用すると、テナントをマルチテナント展開にオンボーディングするときに、テナントにサービスを提供するマルチテナント Cisco vSmart コントローラのペアを選択できます。テナントのオンボーディング後、テナントをマルチテナント Cisco vSmart コントローラの別のペアに移行して、オンボーディング中に予測されたよりも多くのテナント WAN エッジデバイスを許可できます。

マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置に関する情報

Cisco vManage による自動テナント配置

Cisco vManage リリース 20.8.x 以前のリリースでは、テナントをオンボードすると、Cisco vManage は、次のような要因を考慮する内部アルゴリズムに基づいて、マルチテナント Cisco vSmart コントローラのペアをテナントに割り当てます。

- テナントに対して予測するテナント WAN エッジデバイスの数
- マルチテナント Cisco vSmart コントローラのペアによってサービスされるテナントの数
- マルチテナント Cisco vSmart コントローラのペアに接続された WAN エッジデバイスの数

テナントがオンボーディングされた後、最初に予測したよりも多くのデバイスをテナントに追加する必要がある場合、テナントにサービスを提供するマルチテナント Cisco vSmart コントローラのペアがこれらの追加の WAN エッジデバイスに対応できる場合は、予測を変更できます。Cisco vSmart コントローラが追加の WAN エッジデバイスに対応できない場合は、テナントを削除し、変更したデバイス予測を使用してテナントを再度オンボーディングして、Cisco vManage が Cisco vSmart コントローラの適切なペアを割り当てるようにする必要があります。マルチテナント Cisco vSmart コントローラのペアのいずれも、変更したデバイス予測に対応できない場合は、Cisco vSmart コントローラの新しいペアを追加してから、テナントをオンボーディングします。

プロバイダー管理者ユーザーによる柔軟なテナント配置

Cisco vManage リリース 20.9.1 以降、テナントのオンボーディング中に、テナントに割り当てられているマルチテナント Cisco vSmart コントローラのペアを柔軟に選択できます。Cisco vManage による自動テナント配置は引き続きデフォルトの動作であり、オプションの構成として柔軟なテナント配置が可能です。

柔軟なテナント配置を支援するために、Cisco vManage は使用可能なマルチテナント Cisco vSmart コントローラをリストし、各コントローラについて次の詳細をパーセンテージで指定します。

- 割り当てられているテナントの数
- 接続されているテナント WAN エッジデバイスの数
- メモリの使用率
- CPU 使用率

マルチテナント Cisco vSmart コントローラは、すべてのテナントで最大 24 のテナントと 1000 のテナント WAN エッジデバイスにサービスを提供できます。1 つ以上のテナントを割り当てることができ、テナントについて予測される数の WAN エッジデバイスにも接続できるコントローラのペアを選択する必要があります。

テナントがオンボーディングされた後、最初に予測したよりも多くのデバイスをテナントに追加する必要があり、マルチテナント Cisco vSmart コントローラの割り当てられたペアがこれらの追加の WAN エッジデバイスに接続できない場合、テナントを Cisco vSmart コントローラの別のペアに移行できます。これによってより多くのテナントにサービスを提供し、テナントに対する WAN エッジデバイスの変更された予測に対応します。マルチテナント Cisco vSmart コントローラのペアのいずれも変更されたデバイス予測に対応できない場合は、他のテナントを代替 Cisco vSmart コントローラに移行して、コントローラの容量をより効率的に使用し、テナントへの割り当てを最適化することができます。最適化によって、テナントに対する変更されたデバイス予測に対応するために必要な容量が作成されない場合は、Cisco vSmart コントローラの新しいペアを追加してから、テナントを移行します。

マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置の利点

- 異なる障害ゾーンに展開された Cisco vSmart コントローラを選択して、両方のコントローラが同時に障害を起こす可能性を減らします。クラウド環境では、異なるリージョンに展開されたコントローラを選択します。
- テナント WAN エッジデバイスと同じ地理的リージョンに展開された Cisco vSmart コントローラを選択して、遅延を減らします。
- 割り当てられた CPU、DRAM、ハードディスクリソース、およびこれらのリソースの使用率に基づいて、Cisco vSmart コントローラを選択します。
- テナントデバイスの予測の変更に対応するために、テナントを別の Cisco vSmart コントローラに移行します。

マルチテナント Cisco vSmart コントローラでの柔軟なテナント配置の制約事項

テナントを Cisco vSmart コントローラの別のペアに移行する場合は、テナントに割り当てられている Cisco vSmart コントローラを一度に 1 つずつ変更する必要があります。これにより、移行中に Cisco vSmart コントローラの 1 つをテナント WAN エッジデバイスで使用できるようになり、トラフィックの中断が防止されます。

オンボーディング中に Cisco vSmart コントローラをテナントに割り当て

前提条件

- 新しいテナントを追加する前に、少なくとも 2 つの Cisco vSmart コントローラが動作し、vManage モードになっている必要があります。

  テンプレートを Cisco vManage からコントローラにプッシュすると、Cisco vSmart コントローラは vManage モードに入ります。CLI モードの Cisco vSmart コントローラは、複数のテナントに対応できません。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントと最大 1000 のテナントデバイスに対応できます。新しいテナントに対応できる Cisco vSmart コントローラが少なくとも 2 つあることを確認します。展開内の Cisco vSmart コントローラのペアが新しいテナントに対応できない場合は、2 つの Cisco vSmart コントローラを追加して、それらのモードを vManage に変更します。

- 1 回の操作で最大 16 のテナントを追加します。複数のテナントを追加する場合、[Add Tenant] タスク中、Cisco vManage はテナントを同時に追加するのではなく、1 つずつ追加します。

  [Add Tenant] タスクの進行中は、2 つ目のテナント追加操作を実行しないでください。これを行うと、2 つ目の [Add Tenant] タスクが失敗します。

- 各テナントには、Cisco Software Central のプラグアンドプレイコネクトに一意のバーチャルアカウント（VA）が必要です。テナント VA は、プロバイダー VA と同じスマートアカウント（SA）に属している必要があります。

- オンプレミス展開の場合、プラグアンドプレイコネクトでテナント用の Cisco vBond Orchestrator コントローラプロファイルを作成します。次の表のフィールドは必須です。

フィールド	説明
プロファイル名	コントローラプロファイル名を入力します
マルチテナント機能	ドロップダウンリストから、[Yes] を選択します。
SP Organization Name	プロバイダー組織名を入力します。
組織名	テナント組織名を <SP Org Name>-<Tenant Org Name> の形式で入力します。組織名には最大 64 文字を使用できます。
プライマリ コントローラ（Primary Controller）	プライマリ Cisco vBond Orchestrator のホストの詳細を入力します。

クラウド展開の場合、テナント作成プロセスの一部として Cisco vBond Orchestrator コントローラプロファイルが自動的に作成されます。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. [Add Tenant] をクリックします。
4. [Add Tenant] スライドインペインで、[New Tenant] をクリックします。
5. 次のテナントの詳細を設定します。

フィールド	説明
Name	テナントの名前を入力します。 クラウド展開の場合、テナント名はプラグアンドプレイコネクトのテナント VA 名と同じである必要があります。
Description	テナントの説明を入力します。 説明の最大長は 256 文字で、英数字のみを使用できます。
組織名	テナント組織の名前を入力します。組織名には最大 64 文字を使用できます。 組織名では、大文字と小文字が区別されます。各テナントまたは顧客には、一意の組織名が必要です。 組織名を次の形式で入力します。 `<SP Org Name>-<Tenant Org Name>` たとえば、プロバイダーの組織名が「managed-sp」でテナントの組織名が「customer1」の場合、テナントを追加するときに、組織名を「managed-sp-customer1」と入力します。

フィールド	説明
URL Subdomain	

フィールド	説明
	テナントの完全修飾サブドメイン名を入力します。 • サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、managed-sp.com サービスプロバイダーの場合、customer1 の有効なドメイン名は customer1.managed-sp.com です。 （注） サービスプロバイダー名はすべてのテナントで共有されます。URL命名規則が、**[Administration]** > **[Settings]** > **[Tenancy Mode]** を使用してマルチテナント機能を有効にするときに従ったものと同じドメイン名規則に従っていることを確認してください。 • オンプレミス展開の場合、テナントの完全修飾サブドメイン名を DNS に追加します。完全修飾サブドメイン名を、Cisco vManage クラスタ内の 3 つの Cisco vManage インスタンスの IP アドレスにマッピングします。 • プロバイダー DNS：DNS A レコードを作成し、Cisco vManage クラスタで実行されている Cisco vManage インスタンスの IP アドレスにマップします。A レコードは、プロバイダーのドメイン名と、Cisco vManage でマルチテナント機能を有効にするときに作成されたクラスタ ID から導出されます。たとえば、プロバイダーのドメイン名が `sdwan.cisco.com` で、クラスタ ID が `vmanage123` である場合、A レコードは `vmanage123.sdwan.cisco.com` として設定します。 DNS A レコードの追加に失敗すると、Cisco vManage へのログイン時に認証エラーが発生します。 **nslookup** コマンドを使用して、DNS が正しく設定されていることを検証します。例：`nslookup vmanage123.sdwan.cisco.com` • テナント DNS：作成された各テナントの DNS CNAME レコードを作成し、プロバイダーの FQDN にマップします。たとえば、プロバイダーのドメイン名が `sdwan.cisco.com` でテナント名が `customer1` の場合、CNAME レコードは `customer1.sdwan.cisco.com` として設定します。

フィールド	説明
	CNAME レコードにはクラスタ ID は必要ありません。 **nslookup** コマンドを使用して、DNS が正しく設定されていることを検証します。例：`nslookup customer1.sdwan.cisco.com` • クラウド展開の場合、テナントの完全修飾サブドメイン名は、テナント作成プロセスの一部として DNS に自動的に追加されます。テナントを追加した後、テナントの完全修飾サブドメイン名が DNS によって解決されるまでに最大 1 時間かかる場合があります。
Forecasted Devices	テナントがオーバーレイに追加できる WAN エッジデバイスの数を入力します。 テナントがこの数を超える WAN エッジデバイスを追加しようとすると、Cisco vManage はエラーを報告し、デバイスの追加は失敗します。

<table>
<tr><th>フィールド</th><th>説明</th></tr>
<tr><td>Select two vSmarts</td><td>

自動テナント配置：[Select two vSmarts] の値が [Autoplacement] であることを確認します。これはデフォルトの設定です。
柔軟なテナント配置：

[Select two vSmarts] ドロップダウンリストをクリックします。

Cisco vManage に、使用可能な Cisco vSmart コントローラのホスト名が一覧表示されます。Cisco vManage は、Cisco vSmart コントローラごとに、コントローラが到達可能かどうかを示し、次の使用状況の詳細を報告します。
<table>
<tr><td>テナントのホスティング容量</td><td>各 Cisco vSmart コントローラは、最大
ナントに対応できます。テナントのホ
ング容量は、Cisco vSmart コントローラ
当てられているテナントの数をパーセ
ジの形式で表します。この値は、この
ローラに別のテナントを割り当てるこ
きるかどうかを示します。</td></tr>
<tr><td>使用デバイス容量</td><td>各 Cisco vSmart コントローラは、最大
テナント WAN エッジデバイスをサポー
ます。使用デバイス容量は、Cisco vSm
トローラに接続されているテナント WA
ジデバイスの数をパーセンテージの形
します。この値は、オンボーディング
るテナントについて予測されるデバイ
Cisco vSmart コントローラがサポートで
どうかを示します。</td></tr>
<tr><td>メモリ使用率</td><td>この値は、メモリ消費量をパーセンテ
表します。</td></tr>
<tr><td>CPU 使用率</td><td>この値は、CPU 使用率をパーセンテー
します。</td></tr>
</table>

使用率の詳細に基づいてテナントに割り当てる 2 つの Cisco vSmart コントローラを選択します。

Cisco vSmart コントローラを選択するには、そのホスト名の隣にあるチェックボックスをオンにします。

</td></tr>
</table>

6. テナント設定を保存するには、[Save] をクリックします。

7. 別のテナントを追加するには、ステップ 4 ～ 6 を繰り返します。
8. テナントを展開にオンボーディングするには、[Add] をクリックします。

Cisco vManage は、[Create Tenant Bulk] タスクを開始して、テナントをオンボーディングします。

このタスクの一環として、Cisco vManage は次のアクティビティを実行します。

- テナントを作成します
- テナントにサービスを提供する 2 つの Cisco vSmart コントローラを割り当て、CLI テンプレートをこれらのコントローラにプッシュしてテナント情報を設定します

  テナントと Cisco vSmart コントローラの情報を Cisco vBond Orchestrator に送信します。

タスクが正常に完了すると、**[Administration]** > **[Tenant Management]**ページで、テナントに割り当てられた Cisco vSmart コントローラを含むテナント情報を表示できます。

テナントの Cisco vSmart コントローラ配置の更新

現在テナントに割り当てられているコントローラから、別の Cisco vSmart コントローラペアにテナントを移行できます。たとえば、テナント WAN エッジデバイスの予測を増やす必要があり、テナントに割り当てられたコントローラがこれらの変更された数のテナント WAN エッジデバイスに接続できない場合、テナントを、変更された予測に対応できるコントローラのペアに移行できます。

テナントを Cisco vSmart コントローラの別のペアに移行する場合は、テナントに割り当てられている Cisco vSmart コントローラを一度に 1 つずつ変更する必要があります。これにより、移行中に Cisco vSmart コントローラの 1 つをテナント WAN エッジデバイスで使用できるようになり、トラフィックの中断が防止されます。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. 別のコントローラに移行するテナントについては、テナント組織名の横にある [...] をクリックします。
4. [Update vSmart Placement] をクリックします。
5. [Update vSmart Placement] スライドインペインで、次のように設定します。

<table>
<tr><th>フィールド</th><th>説明</th></tr>
<tr><td>Source vSmart (currently applied)</td><td>
1. [Source vSmart (currently applied)] ドロップダウンリストをクリックします。

Cisco vManage に、テナントに割り当てられた Cisco vSmart コントローラのホスト名が一覧表示されます。Cisco vManage は、Cisco vSmart コントローラごとに、コントローラが到達可能かどうかを示し、次の使用状況の詳細を報告します。
<table>
<tr><td>テナントのホスティング容量</td><td>各 Cisco vSmart コントローラは、最大 24 のナントに対応できます。テナントのホステング容量は、Cisco vSmart コントローラが割当てられているテナントの数をパーセンテージの形式で表します。この値は、このコントローラに別のテナントを割り当てることができるかどうかを示します。</td></tr>
<tr><td>使用デバイス容量</td><td>各 Cisco vSmart コントローラは、最大 1000 テナント WAN エッジデバイスをサポートでます。使用デバイス容量は、Cisco vSmart コトローラに接続されているテナント WAN エジデバイスの数をパーセンテージの形式で表します。この値は、オンボーディングしているテナントについて予測されるデバイス数をCisco vSmart コントローラがサポートできるどうかを示します。</td></tr>
<tr><td>メモリ使用率</td><td>この値は、メモリ消費量をパーセンテージで表します。</td></tr>
<tr><td>CPU 使用率</td><td>この値は、CPU 使用率をパーセンテージでします。</td></tr>
</table>
2. テナントに割り当てられたいずれかの Cisco vSmart コントローラのホスト名の隣にあるチェックボックスをオンにします。
</td></tr>
</table>

<table>
<tr><th>フィールド</th><th>説明</th></tr>
<tr><td>Destination vSmart</td><td>
1. [Destination vSmart] ドロップダウンリストをクリックします。

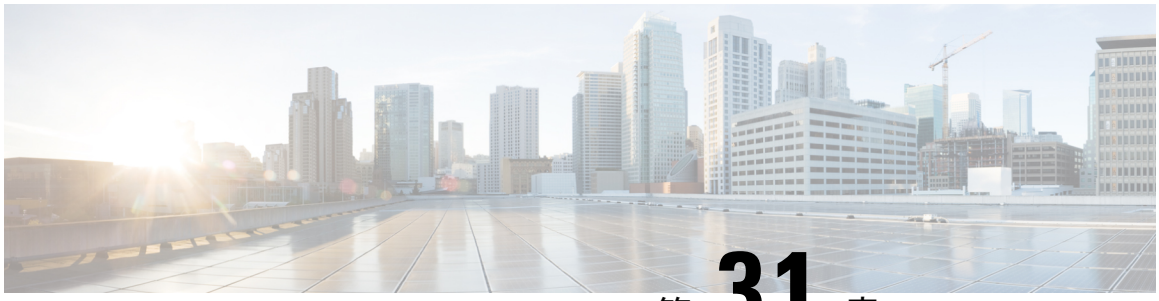
Cisco vManage に、テナントに割り当てられていない使用可能な Cisco vSmart コントローラのホスト名が一覧表示されます。Cisco vManage は、Cisco vSmart コントローラごとに、コントローラが到達可能かどうかを示し、次の使用状況の詳細を報告します。
<table>
<tr><td>テナントのホスティング容量</td><td>各 Cisco vSmart コントローラは、最大 24 のテナントに対応できます。テナントのホスティング容量は、Cisco vSmart コントローラが割り当てられているテナントの数をパーセンテージの形式で表します。この値は、このコントローラに別のテナントを割り当てることができるかどうかを示します。</td></tr>
<tr><td>使用デバイス容量</td><td>各 Cisco vSmart コントローラは、最大 1000 のテナント WAN エッジデバイスをサポートできます。使用デバイス容量は、Cisco vSmart コントローラに接続されているテナント WAN エッジデバイスの数をパーセンテージの形式で表します。この値は、オンボーディングしているテナントについて予測されるデバイス数を Cisco vSmart コントローラがサポートできるかどうかを示します。</td></tr>
<tr><td>メモリ使用率</td><td>この値は、メモリ消費量をパーセンテージで表します。</td></tr>
<tr><td>CPU 使用率</td><td>この値は、CPU 使用率をパーセンテージで表します。</td></tr>
</table>
2. テナントに割り当てる Cisco vSmart コントローラのホスト名の隣にあるチェックボックスをオンにします。

テナントデバイスに対応するために必要な容量がない Cisco vSmart コントローラを選択すると、更新操作は失敗します。
</td></tr>
</table>

6. [更新（Update）] をクリックします。

7. テナントに割り当てられている他の Cisco vSmart コントローラを変更するには、手順 3 から手順 6 を繰り返します。

Cisco vManage は、テナント vSmart 更新タスクを開始して、選択した Cisco vSmart コントローラをテナントに割り当て、以前に割り当てられた Cisco vSmart コントローラからテナントの詳細を移行します。タスクが正常に完了すると、**[Administration]** > **[Tenant Management]**ページで、テナントに割り当てられた Cisco vSmart コントローラを含むテナント情報を表示できます。



第 31 章

Cisco SD-WAN マルチテナント機能（Cisco IOS XE リリース 17.4.x および 17.5.x）

表 *225 :* 機能の履歴

機能名	リリース情報	機能説明
Cisco SD-WAN マルチテナント機能	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。マルチテナント Cisco SD-WAN 展開では、テナントは Cisco vManage インスタンス、Cisco vBond オーケストレーション、および Cisco vSmart コントローラを共有します。テナントデータは、これらの共有リソース上で論理的に分離されます。

Cisco SD-WAN マルチテナント機能の概要

Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。テナントは、Cisco vManage インスタンス、Cisco vBond オーケストレーション、および Cisco vSmart コントローラを共有します。サービスプロバイダーのドメイン名には、テナントごとにサブドメインがあります。たとえば、`multitenancy.com` サービスプロバイダーは、テナント Customer1（`Customer1.multitenancy.com`）と Customer2（`Customer2.multitenancy.com`）を管理できます。

Cisco SD-WAN マルチテナント機能の主な機能は次のとおりです。

- 完全なエンタープライズ マルチテナント機能：Cisco SD-WAN はマルチテナント機能をサポートし、企業はサービスプロバイダーやテナントなどの役割を柔軟に分離することができます。サービスプロバイダーは、マルチテナント機能を使用して顧客に Cisco SD-WAN サービスを提供できます。
- マルチテナント Cisco vManage：
  - Cisco vManage はサービスプロバイダーによって展開および設定されます。プロバイダーは、マルチテナント機能を有効にし、テナントにサービスを提供する Cisco vManage クラスタを作成します。SSH 端末を介して Cisco vManage インスタンスにアクセスできるのはプロバイダーのみです。

（注） SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から vmanage_system の IP アドレスを見つけることもできます。

  - Cisco vManage は、サービスプロバイダーに SD-WAN マルチテナント展開の全体像を提供し、プロバイダーが共有 Cisco vBond オーケストレーション デバイスと Cisco vSmart コントローラデバイスを管理できるようにします。また、Cisco vManage により、サービスプロバイダーは各テナントの展開を監視および管理できます。
  - Cisco vManage により、テナントは展開を監視および管理できます。Cisco vManage により、テナントは WAN エッジデバイスを展開および設定できます。テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定することもできます。

- マルチテナント Cisco vBond オーケストレーション：
  - Cisco vBond オーケストレーション は、サービスプロバイダーによって展開および設定されます。SSH 端末を介して Cisco vBond オーケストレーション にアクセスできるのはプロバイダーのみです。

（注） SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から vmanage_system の IP アドレスを見つけることもできます。

  - Cisco vBond オーケストレーション は、デバイスがオーバーレイネットワークに追加されると、複数のテナントの WAN エッジデバイスにサービスを提供します。

- マルチテナント Cisco vSmart コントローラ：
  - Cisco vSmart コントローラは、サービスプロバイダーによって展開されます。デバイスおよび機能テンプレートを作成して Cisco vSmart コントローラに接続できるのはプロバイダーのみで、SSH 端末を介して Cisco vSmart コントローラにアクセスできます。

（注） SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から vmanage_system の IP アドレスを見つけることもできます。

  - テナントが作成されると、Cisco vManage はテナントに 2 つの Cisco vSmart コントローラを割り当てます。Cisco vSmart コントローラは、アクティブ/アクティブクラスタを形成します。

各テナントには 2 つの Cisco vSmart コントローラのみが割り当てられます。テナントを作成する前に、テナントにサービスを提供するために 2 つの Cisco vSmart コントローラを使用できる必要があります。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントに対応できます。
- テナントは、割り当てられた Cisco vSmart コントローラでカスタムポリシーを設定できます。Cisco vManage はポリシーテンプレートをプルするように Cisco vSmart コントローラに通知します。Cisco vSmart コントローラはテンプレートをプルし、特定のテナントのポリシー設定を展開します。
- Cisco vManage で Cisco vSmart コントローラのイベント、監査ログ、および OMP アラームを表示できるのは、プロバイダーのみです。

- WAN エッジデバイス：
  - テナントまたはテナントに代わって機能するプロバイダーは、WAN エッジデバイスをテナントネットワークに追加したり、デバイスを設定したり、テナントネットワークからデバイスを削除したり、SSH 端末を介してデバイスにアクセスしたりできます。

（注） SSH 経由でデバイスに接続するには、`vmanage_system` インターフェイスの IP アドレスを使用します。この IP アドレスは、Cisco vManage によって割り当てられます。ユーザー設定のシステム IP アドレスを使用して SSH 経由でデバイスに接続することはしないでください。

`vmanage_system` インターフェイスの IP アドレスは、**show interface description** コマンドの出力から見つけることができます。または、Cisco vManage からデバイスの SSH 端末を起動し、ログインプロンプトの最初の行から vmanage_system の IP アドレスを見つけることもできます。

  - プロバイダーは、テナントとしてのプロバイダービューからのみ WAN エッジデバイスを管理できます。プロバイダービューでは、Cisco vManage は WAN エッジデバイスの情報を表示しません。
  - Cisco vManage は、WAN エッジデバイスのイベント、ログ、およびアラームを、テナントロールビューおよびテナントとしてのプロバイダービューでのみレポートします。

- VPN 番号の重複：特定の VPN または共通の VPN のセットは、独自の設定および監視ダッシュボード環境を使用して、特定のテナントに割り当てられます。これらの VPN 番号は、他のテナントが使用する場所で重複する可能性があります。
- オンプレミスおよびクラウド展開モデル：Cisco SD-WAN コントローラは、VMware vSphere ESXi またはカーネルベースの仮想マシン（KVM）ハイパーバイザを実行しているサーバー

上の組織のデータセンターに展開できます。Cisco SD-WAN コントローラは、Amazon Web Services（AWS）サーバー上のクラウドに展開することもできます。

マルチテナント環境でのユーザーロール

マルチテナント環境には、サービスプロバイダーとテナントのロールが含まれます。各ロールには、個別の権限、ビュー、および機能があります。

プロバイダーロール

プロバイダーロールは、システム全体の管理者権限を付与します。プロバイダーロールを持つユーザーは、デフォルトのユーザー名 **admin** を持っています。プロバイダーユーザーは、サービスプロバイダーのドメイン名または Cisco vManage IP アドレスを使用して Cisco vManage にアクセスできます。ドメイン名を使用する場合、ドメイン名の形式は `https://multitenancy.com` です。

admin ユーザーは、ユーザーグループ **netadmin** の一部です。このグループのユーザーは、テナントのコントローラと Cisco SD-WAN デバイスに対するすべての操作を実行することが許可されます。**netadmin** グループにユーザーを追加できます。

netadmin グループの権限は変更できません。Cisco vManage では、**[Administration]** > **[Manage Users]** > **[User Groups]**ページからユーザーグループの権限を表示できます。

（注） **netadmin** ユーザーを含む新しいプロバイダーユーザーを Cisco vManage で作成すると、デフォルトでは、ユーザーは Cisco vManage VM への SSH アクセスを許可されません。SSH アクセスを有効にするには、AAA テンプレートを使用して SSH 認証を設定し、Cisco vManage へテンプレートをプッシュします。SSH 認証の有効化の詳細については、「SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices」を参照してください。

ユーザーとユーザーグループの構成の詳細については、「Configure User Access and Authentication」を参照してください。

Cisco vManage は、プロバイダーに 2 つのビューを提供します。

- **プロバイダービュー**

  プロバイダーユーザーが **admin** または別の **netadmin** ユーザーとしてマルチテナント Cisco vManage にログインすると、Cisco vManage にプロバイダービューが表示され、プロバイダーダッシュボードが表示されます。

  プロバイダービューから次の機能を実行できます。

  - Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ のプロビジョニングと管理。
  - テナントの追加、変更、または削除。

- オーバーレイネットワークのモニタリング。

- **テナントとしてのプロバイダービュー**

  プロバイダーユーザーがプロバイダーダッシュボードの上部にある [Select Tenant] ドロップダウンリストから特定のテナントを選択すると、Cisco vManage にテナントとしてのプロバイダービューが表示され、選択したテナントのテナントダッシュボードが表示されます。プロバイダーユーザーは、**tenantadmin** としてログインしたときのテナントユーザーと同じ Cisco vManage のビューを持ちます。プロバイダーは、このビューから、テナントに代わってテナントの展開を管理できます。

  プロバイダーダッシュボードでは、テナントのテーブルに各テナントのステータスの概要が表示されます。プロバイダーユーザーは、このテーブルのテナント名をクリックして、テナントとしてのプロバイダービューを起動することもできます。

テナントロール

テナントロールは、テナント管理権限を付与します。テナントロールを持つユーザーは、デフォルトのユーザー名 **tenantadmin** を持っています。デフォルトのパスワードは **Cisco#123@Viptela** です。最初のログイン時にデフォルトのパスワードを変更することをお勧めします。デフォルトのパスワードの変更については、「Hardware and Software Installation」を参照してください。

tenantadmin ユーザーは、ユーザーグループ **tenantadmin** の一部です。このグループのユーザーは、テナントの WAN エッジデバイスですべての操作を実行できます。**tenantadmin** グループにユーザーを追加できます。

tenantadmin グループの権限は変更できません。Cisco vManage では、**[Administration]** > **[Manage Users]** > **[User Groups]**ページからユーザーグループの権限を表示できます。

ユーザーとユーザーグループの構成の詳細については、「Configure User Access and Authentication」を参照してください。

テナントユーザーは、専用の URL とデフォルトのユーザー名 **tenantadmin** を使用して Cisco vManage にログインできます。たとえば、ドメイン名 `https://multitenancy.com` を使用するプロバイダーの場合、テナントの専用 URL は `https://Customer1.multitenancy.com` になる可能性があります。ユーザーがログインすると、Cisco vManage にテナントビューが表示され、テナントダッシュボードが表示されます。

管理者権限を持つテナントユーザーは、次の機能を実行できます。

- テナントルータのプロビジョニングと管理
- テナントのオーバーレイネットワークのモニタリング
- 割り当てられた Cisco vSmart コントローラ にカスタムポリシーを作成
- テナントルータのソフトウェアをアップグレード。

ハードウェアのサポートと仕様

次のプラットフォームはマルチテナント機能をサポートしています。

表 *226 :* ルータモデル

Platform	ルータモデル
Cisco IOS XE SD-WAN デバイス	• Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco ISR 1000 シリーズ サービス統合型ルータ • Cisco ISR 4000 シリーズ サービス統合型ルータ • Cisco Catalyst 8300 シリーズ エッジ プラットフォーム • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco Catalyst 8000V Edge ソフトウェア

マルチテナント機能では、次のハイパーバイザと展開モデルがサポートされています。

表 *227 :* 展開モデル

仕様	Description
サポートされるハイパーバイザ	VMware、KVM、AWS（シスコがクラウドホスト）
Cisco vManage 展開モデル	クラスタ、各インスタンスがすべての NMS サービスを実行する 3 つの vManage インスタンス。

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 でサポートされるハードウェア仕様は次のとおりです。

表 *228 :* オンプレミス展開

サーバー	Cisco vManage	Cisco vBond オーケストレーション	Cisco vSmart コントローラ
デプロイメントモデル	クラスタ	該当なし	非コンテナ化
インスタンス数	3	2	24 テナントあたり 2

CPU **DRAM** ハード ディスク	32 vCPU 72 GB 1 TB	4 vCPU 4 GB 10 GB	8 vCPU 16 GB 16 GB
NMS サービスの分散	一部のサービスは、クラスタ内の 3 つの Cisco vManage インスタンスすべてで実行されますが、一部のサービスは、クラスタ内の 3 つのインスタンスのうち 1 つでのみ実行されます。したがって、CPU負荷はインスタンス間で異なる場合があります。	該当なし	該当なし

（注） DPI が有効になっている場合、すべての Cisco vManage インスタンス全体で集約された DPI データが 1 日あたり 350 GB を超えないようにすることをお勧めします。

マルチテナント機能の初期設定

前提条件

- 次の表で推奨されているソフトウェアバージョンをダウンロードしてインストールします。

表 *229 : Cisco SD-WAN* マルチテナント機能のソフトウェア前提条件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.4.1
Cisco vBond オーケストレーション	Cisco SD-WAN リリース 20.4.1
Cisco vSmart コントローラ	Cisco SD-WAN リリース 20.4.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1a

1 つまたは複数のコントローラまたは WAN エッジデバイスが、上記の表に示すものより前のソフトウェアバージョンを実行している構成はサポートされていません。

- 既存の Cisco vManage インスタンスにおいてデバイスをすべて無効化または削除した場合でも、既存のシングルテナント Cisco vManage インスタンスをマルチテナントモードに移行しないでください。代わりに、新しい Cisco vManage ソフトウェアイメージをダウンロードしてインストールします。

（注） マルチテナント機能用に Cisco vManage を有効にした後は、シングルテナントモードに戻すことはできません。

- プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。

1. 3 つの Cisco vManage インスタンスと関連する設定テンプレートを作成します。「Deploy Cisco vManage」を参照してください。
   1. Cisco vManage インスタンスを設定するときに、サービスプロバイダーの組織名（`sp-organization-name`）と組織名（`organization-name`）を設定します。

      例：

      ```
      sp-organization-name multitenancy
      organization-name multitenancy
      ```

2. マルチテナント機能をサポートするように Cisco vManage インスタンスの 1 つを設定します。Cisco vManage でのマルチテナント機能の有効化 （938 ページ）を参照してください。
3. 3 つの Cisco vManage インスタンスで構成される Cisco vManage クラスタを作成します。「Cluster Management」を参照してください。
   - Cisco vManage クラスタには 3 つの Cisco vManage インスタンスが必要です。インスタンスが 4 つ以上または 3 つ未満のクラスタは、Cisco SD-WAN マルチテナント機能でサポートされる構成ではありません。
   - Cisco vManage クラスタの作成時は、マルチテナント機能をサポートするように設定した Cisco vManage インスタンスを追加してから、他の 2 つの Cisco vManage インスタンスを追加します。
4. Cisco vManage のすべてのインスタンスを認可します。「Generate vManage NMS Certificate」を参照してください。
5. Cisco vBond Orchestrator インスタンスを作成して設定します。「Deploy Cisco vBond Orchestrator」を参照してください。

   Cisco vBond Orchestrator インスタンスを設定するときに、サービスプロバイダーの組織名（`sp-organization-name`）と組織名（`organization-name`）を設定します。「Configure Organization Name in Cisco vBond Orchestrator」を参照してください。

   ```
   sp-organization-name multitenancy
   organization-name multitenancy
   ```

6. Cisco vSmart コントローラインスタンスを作成します。「Deploy the Cisco vSmart Controller」を参照してください。

すべてのテナントで 50 のテナントと 1000 のデバイスをサポートするには、6 つの Cisco vSmart Controller インスタンスを展開します。すべてのテナントで 100 のテナントと 5000 のデバイスをサポートするには、12 の Cisco vSmart コントローラを展開します。

1. オーバーレイネットワークに Cisco vSmart コントローラの追加 します。

7. 新しいテナントを導入準備します。「新規テナントの追加」を参照してください。

Cisco vManage でのマルチテナント機能の有効化

1. URL `https://vmanage-ip-address:port` を使用して Cisco vManage を起動します。プロバイダーの **admin** ユーザーとしてログインします。
2. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
3. テナンシーモードバーで、[Edit] をクリックします。
4. [Tenancy] フィールドで、[Multitenant] をクリックします。
5. [Domain] フィールドに、サービスプロバイダーのドメイン名（たとえば、multitenancy.com）を入力します。
6. クラスタ ID（たとえば、cluster-1 または 123456）を入力します。
7. **[Save]** をクリックします。
8. [Proceed] をクリックして、テナンシーモードを変更することを確認します。

   Cisco vManage はマルチテナントモードで再起動し、プロバイダーユーザーが Cisco vManage にログインすると、プロバイダーダッシュボードが表示されます。

Cisco vSmart コントローラの追加

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
3. [Controllers] をクリックします。
4. [Add Controller] をクリックし、[vSmart] をクリックします。
5. [Add vSmart] ダイアログボックスで、次を実行します。
   1. [vSmart Management IP Address] フィールドに、Cisco vSmart コントローラのシステム IP アドレスを入力します。
   2. Cisco vSmart コントローラへのアクセスに必要な [Username] と [Password] を入力します。
   3. コントロールプレーン接続に使用するプロトコルを選択します。デフォルトは[DTLS] です。

[TLS] を選択した場合は、TLS 接続に使用するポート番号を入力します。デフォルトは 23456 です。

4. 証明書署名要求を作成するには、Cisco vManage の [Generate CSR] チェックボックスをオンにします。
5. [Add] をクリックします。

6. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。

   Cisco vSmart コントローラを新規に追加した場合、[Operation Status] には「CSR Generated」と表示されます。

   1. Cisco vSmart コントローラを新規に追加した場合、[More Options] アイコンをクリックし、[View CSR] をクリックします。
   2. CSR を認証局（CA）に提出して、署名付き証明書を取得します。

7. [Cisco vManage] メニューから、**[Configuration]** > **[Certificates]** を選択します。
8. [Install Certificate] をクリックします。
9. [Install Certificate] ダイアログボックスで証明書を [Certificate Text] に貼り付けるか、[Select a File] をクリックして証明書ファイルをアップロードします。[Install] をクリックします。

   Cisco vManage により、証明書が Cisco vSmart コントローラにインストールされます。Cisco vManage により、証明書のシリアル番号が他のコントローラにも送信されます。

   [Configuration] > **[Certificates]** ページで、新しく追加された Cisco vSmart コントローラの [Operation Status] には、「vBond Updated」と表示されます。

   [Configuration] > **[Devices]** ページで、新しいコントローラがコントローラテーブルに表示されます。このテーブルにはコントローラタイプ、コントローラのホスト名、IP アドレス、サイト ID、およびその他の詳細も表示されます。[Mode] は [CLI] に設定されています。

10. テンプレートをデバイスにアタッチして、新しく追加された Cisco vSmart コントローラのモードを [vManage] に変更します。

    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. Cisco vSmart コントローラにアタッチするテンプレートを見つけます。
    4. [...] をクリックして、[Attach Devices] をクリックします。

5. [Attach Devices] ダイアログボックスで、新しいコントローラを [Selected Device] リストに移動し、[Attach] をクリックします。
6. [Config Preview] を確認し、[Configure Devices] をクリックします。

Cisco vManage は、テンプレートの設定を新しいコントローラにプッシュします。

[Configuration] > **[Devices]** ページでは、Cisco vSmart コントローラの [Mode] に [vManage] と表示されます。新しい Cisco vSmart コントローラをマルチテナント展開で使用する準備ができました。

テナントの管理

新規テナントの追加

前提条件

- 新しいテナントを追加する前に、少なくとも 2 つの Cisco vSmart コントローラが動作し、`vManage` モードになっている必要があります。

  テンプレートを Cisco vManage からコントローラにプッシュすると、Cisco vSmart コントローラは `vManage` モードに入ります。`CLI` モードの Cisco vSmart コントローラは、複数のテナントに対応できません。

- Cisco vSmart コントローラの各ペアは、最大 24 のテナントに対応できます。新しいテナントに対応できる Cisco vSmart コントローラが少なくとも 2 つあることを確認します。展開内の Cisco vSmart コントローラのペアが新しいテナントに対応できない場合は、2 つの Cisco vSmart コントローラを追加して、それらのモードを `vManage` に変更します。
- テナントを追加した直後に 2 番目のテナントを追加すると、Cisco vManage はそれらを並行してではなく順番に追加します。
- 各テナントには、Cisco Software Central の**プラグアンドプレイコネクト**に一意のバーチャルアカウント（VA）が必要です。テナント VA は、プロバイダー VA と同じスマートアカウント（SA）に属している必要があります。
- オンプレミス展開の場合、**プラグアンドプレイコネクト**でテナント用の Cisco vBond Orchestrator コントローラプロファイルを作成します。次の表のフィールドは必須です。

表 *230* : コントローラ プロファイル フィールド

フィールド	説明/値
プロファイル名	コントローラプロファイル名を入力します
マルチテナント機能	ドロップダウンリストから、[Yes] を選択します。

フィールド	説明/値
SP Organization Name	プロバイダー組織名を入力します。
組織名	テナント組織名を `<SP Org Name>-<Tenant Org Name>` の形式で入力します。 （注） 組織名には最大 64 文字を使用できます。
プライマリ コントローラ（Primary Controller）	プライマリ Cisco vBond Orchestrator のホストの詳細を入力します。

クラウド展開の場合、テナント作成プロセスの一部として Cisco vBond Orchestrator コントローラプロファイルが自動的に作成されます。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. [Add Tenant] をクリックします。[Add Tenant] ダイアログボックスで、次の手順を実行します。
   1. テナントの名前を入力します。

      クラウド展開の場合、テナント名は**プラグアンドプレイコネクト**のテナント VA 名と同じである必要があります。
   2. テナントの説明を入力します。

      説明の最大長は 256 文字で、英数字のみを使用できます。
   3. 組織の名前を入力します。

      組織名では、大文字と小文字が区別されます。各テナントまたは顧客には、一意の組織名が必要です。

      組織名を次の形式で入力します。

      ```
      <SP Org Name>-<Tenant Org Name>
      ```

      たとえば、プロバイダーの組織名が「multitenancy」でテナントの組織名が「Customer1」の場合、テナントを追加するときに、組織名を **`multitenancy-Customer1`** として入力します。

（注） 組織名には最大 64 文字を使用できます。

   4. [URL Subdomain Name] フィールドに、テナントの完全修飾サブドメイン名を入力します。

- サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、`multitenancy.com` サービスプロバイダーの場合、有効なドメイン名は `Customer1.multitenancy.com` です。

（注） サービスプロバイダー名はすべてのテナントで共有されます。したがって、URL 命名規則が、Cisco vManage の**[Administration]** > **[Settings]** > **[Tenancy Mode]**の GUI ナビゲーションパスからマルチテナンシーを有効にするときに提供されたものと同じドメイン名規則に従っていることを確認してください。

- オンプレミス展開の場合、テナントの完全修飾サブドメイン名を DNS に追加します。完全修飾サブドメイン名を、Cisco vManage クラスタ内の 3 つの Cisco vManage インスタンスの IP アドレスにマッピングします。

  完全修飾ドメイン名（FQDN）を作成する場合、次の DNS エントリが必要です。

  - **プロバイダーレベル**：DNS A レコードを作成し、Cisco vManage クラスタで実行されている Cisco vManage インスタンスの IP アドレスにマップします。A レコードは、「Enable Multitenancy on Cisco vManage」の手順 5 と 6 で作成されたドメインとクラスタ ID から派生しています。たとえば、ドメインが **sdwan.cisco.com** でクラスタ ID が **vmanage123** の場合、A レコードは **vmanage123.sdwan.cisco.com** として設定する必要があります。

（注） DNS エントリの更新に失敗すると、vManage へのログイン時に認証エラーが発生します。**nslookup vmanage123.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

  - **テナントレベル**：作成された各テナントの DNS CNAME レコードを作成し、プロバイダーレベルで作成された FQDN にマップします。たとえば、ドメインが **sdwan.cisco.com** でテナント名が **customer1** の場合、CNAME レコードは **customer1.sdwan.cisco.com** として設定する必要があります。

（注） CNAME レコードにはクラスタ ID は必要ありません。**nslookup customer1.sdwan.cisco.com** を実行して、DNS が正しく設定されていることを確認します。

クラウド展開の場合、テナントの完全修飾サブドメイン名は、テナント作成プロセスの一部として DNS に自動的に追加されます。テナントを追加した後、テナントの完全修飾サブドメイン名が DNS によって解決されるまでに最大 1 時間かかる場合があります。

5. **[Save]** をクリックします。

   [Create Tenant] 画面が表示され、テナント作成の [Status] が [In progress] と表示されます。テナントの作成に関連するステータスメッセージを表示するには、ステータスの左側にある [>] ボタンをクリックします。

   Cisco vManage は次のことを行います。

   - テナントを作成します
   - テナントにサービスを提供する 2 つの Cisco vSmart コントローラを割り当て、CLI テンプレートをこれらのコントローラにプッシュしてテナント情報を設定します
   - テナントと Cisco vSmart コントローラの情報を Cisco vBond Orchestrator に送信します。

次に行う作業：

[Status] 列が [Success] に変わったら、**[Administration]** > **[Tenant Management]**ページでテナント情報を表示できます。

テナント情報の変更

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. 左ペインで、テナントの名前をクリックします。

   右側のペインにテナント情報が表示されます。
4. テナントデータを変更するには、次のようにします。
   1. 右側のペインで、鉛筆アイコンをクリックします。
   2. [Edit Tenant] ダイアログボックスで、テナント名、説明、またはドメイン名を変更します。
   3. [Save（保存）] をクリックします。

テナントの削除

テナントを削除する前に、すべてのテナント WAN エッジデバイスを削除します。テナントネットワークからの WAN エッジデバイスの削除 （950 ページ）を参照してください。

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. Cisco vManage のメニューから**[Administration]** > **[Tenant Management]**の順に選択します。
3. 左ペインで、テナントの名前をクリックします。

右ペインにテナント情報が表示されます。

4. テナントを削除するには、次のようにします。
   1. 右側のペインで、ごみ箱アイコンをクリックします。
   2. [Delete Tenant] ダイアログボックスで、プロバイダーの [admin] のパスワードを入力し、[Save] をクリックします。

マルチテナント機能の Cisco vManage ダッシュボード

マルチテナント機能について Cisco vManage を有効にした場合、Cisco vManage にログインすると、マルチテナント ダッシュボードを表示できます。Cisco vManage マルチテナント ダッシュボードは、プロバイダーまたはテナントが基盤となるシステムを表示およびプロビジョニングできるポータルです。

すべての Cisco vManage マルチテナント画面の上部にあるバーには、スムーズなナビゲーションを可能にするアイコンがあります。

テナントアクティビティ、デバイス、およびネットワーク情報の表示

マルチテナント Cisco vManage に管理者としてログインすると、プロバイダーダッシュボードに次のコンポーネントが表示されます。他の Cisco vManage 画面からプロバイダーダッシュボードに戻るには、左側のバーにある [Dashboard] をクリックします。

- デバイスペイン：マルチテナント ダッシュボード画面の上部に表示されます。デバイスペインには、アクティブな Cisco vSmart コントローラ、Cisco vBond オーケストレーション、および Cisco vManage インスタンスの数、デバイスの接続ステータス、および期限切れまたは期限切れ間近の証明書に関する情報が表示されます。
- テナントペイン：テナントの総数と、すべてのテナントの制御ステータス、サイトの正常性、ルータの正常性、および Cisco vSmart コントローラステータスの概要が表示されます。
- オーバーレイネットワーク内のテナントのテーブル：各テナントの制御ステータス、サイトの正常性、WAN エッジデバイスの正常性、および Cisco vSmart コントローラステータスに関する個別の情報を含む、個々のテナントのリストです。

  テナント固有のステータスの概要情報を表示するには、次の手順を実行します。

  1. テナントリストからテナント名をクリックします。

     画面の右側にダイアログボックスが開き、テナントのステータスに関する追加情報が提供されます。

  2. 選択したテナントのテナントダッシュボードにアクセスするには、[<Tenant name> Dashboard] をクリックします。

Cisco vManage に、テナントとしてのプロバイダービューが表示され、テナントダッシュボードが表示されます。プロバイダービューに戻るには、ページの上部にある [Provider] をクリックします。

3. ダイアログボックスを閉じるには、テナントリストからテナント名をクリックします。

テナント設定の詳細情報の表示

Cisco vManage は、次の場合にテナント展開に関する情報を提供するテナントダッシュボードを表示します。

- プロバイダーの **admin** ユーザーがプロバイダーダッシュボードの [Select Tenant] ドロップダウンリストから特定のテナントを選択する。このビューは、テナントとしてのプロバイダービューと呼ばれます。
- **tenantadmin** ユーザーが Cisco vManage にログインする。このビューはテナントビューと呼ばれます。

テナント オーバーレイ ネットワークのすべてのネットワーク接続を表示する

[Device] ペインは、テナントダッシュボードの上部に表示され、テナントのオーバーレイネットワーク内の Cisco vManage から Cisco vSmart コントローラおよびルータへの制御接続の数を表示します。WAN エッジデバイスごとに、[Device] ペインに次の情報が表示されます。

- Cisco vSmart コントローラと WAN エッジデバイス間の制御接続の総数
- Cisco vSmart コントローラと WAN エッジデバイス間の有効な制御接続の数
- Cisco vSmart コントローラと WAN エッジデバイス間の無効な制御接続の数

接続番号をクリックするか、上矢印または下矢印をクリックして、各接続に関する詳細情報を示す表を表示します。各テーブル行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Devices]**画面から [Device Dashboard] または [Real Time] ビューにアクセスするか、または**[Tools]** > **[SSH Terminal]**画面にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前のリリースでは、[Real Time] ビューは **[Monitor]** > **[Network]** 画面の一部です。

デバイスの再起動に関する情報の表示

[Reboot] ペインには、ネットワーク内のすべてのデバイスについて、過去 24 時間の再起動の合計数が表示されます。これには、ソフト再起動とコールド再起動、およびデバイスの電源再投入の結果として発生した再起動が含まれます。再起動ごとに、次の情報が表示されます。

- 再起動したデバイスのシステム IP およびホスト名。

- デバイスが再起動された時刻。
- デバイスの再起動の理由

同じデバイスが 2 回以上再起動すると、各再起動オプションが個別に報告されます。

[Reboot] ペインをクリックして、[Reboot] ダイアログボックスを開きます。[Reboot] ダイアログボックスで、[Crashes] をクリックします。すべてのデバイスクラッシュについて、次の情報が表示されます。

- クラッシュが発生したデバイスのシステム IP およびホスト名。
- デバイスのクラッシュインデックス
- デバイスがクラッシュしたコアタイム。
- デバイスクラッシュログのファイル名

ネットワーク接続の表示

[Control Status] ペインには、Cisco vSmart コントローラと WAN エッジデバイスが接続されているかどうかが表示されます。各 Cisco vSmart コントローラは、ネットワーク内の他のすべての Cisco vSmart コントローラに接続する必要があります。各 WAN エッジデバイスは、設定された最大数の Cisco vSmart コントローラに接続する必要があります。[Control Status] ペインには、3 つのネットワーク接続数が表示されます。

- [Control Up]：必要な数の動作可能なコントロールプレーンが Cisco vSmart Controller に接続されているデバイスの総数。
- [Partial]：動作可能なコントロールプレーンの一部（すべてではない）が Cisco vSmart コントローラに接続されているデバイスの総数。
- [Control Down]：Cisco vSmart コントローラにコントロールプレーンが接続されていないデバイスの総数

デバイスの詳細を含むテーブルを表示するには、[Control Status] ダイアログボックスの行をクリックします。各テーブル行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Devices]** 画面から [Device Dashboard] または [Real Time] ビューにアクセスします。

（注） Cisco vManage リリース 20.6.x 以前のリリースでは、[Real Time] ビューは **[Monitor]** > **[Network]** 画面の一部です。

サイトのデータ接続の状態の表示

[Site Health] ペインには、サイトのデータ接続の状態が表示されます。サイトに複数の WAN エッジデバイスがある場合、このペインには、個々のデバイスではなくサイト全体の状態が表示されます。[Site Health] ペインには、次の 3 つの接続状態が表示されます。

- [Full WAN Connectivity]：すべてのルータ上のすべての BFD セッションが稼働状態にあるサイトの総数。
- [Partial WAN Connectivity]：トンネルおよびすべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトでは、データプレーン接続が制限されています。
- [No WAN Connectivity]：すべてのルータ上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトにはデータプレーン接続がありません。

各サイト、ノード、またはトンネルに関する詳細情報を含むテーブルを表示するには、[Site Health] ダイアログボックスの行をクリックします。テーブルの各行の右側にある [More Actions] アイコンをクリックして、**[Monitor]** > **[Devices]**画面から [Device Dashboard] または [Real Time] ビューにアクセスするか、または**[Tools]** > **[SSH Terminal]**画面にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前のリリースでは、[Real Time] ビューは **[Monitor]** > **[Network]** 画面の一部です。

WAN エッジインターフェイスのインターフェイス使用状況の表示

[Transport Interface Distribution] ペインには、VPN 0 のすべての WAN エッジインターフェイスにおける過去 24 時間のインターフェイスの使用状況が表示されます。これには、すべての TLOC インターフェイスが含まれます。ペインをクリックして、[Transport Interface Distribution] ダイアログボックスにインターフェイスの使用状況の詳細を表示します。

WAN エッジデバイス数の表示

[WAN Edge Inventory] ペインには、次の 4 つのカウントが表示されます。

- [Total]：Cisco vManage にアップロードされた WAN エッジデバイスの認証済みシリアル番号の総数。シリアル番号は**[Configuration]** > **[Devices]**画面でアップロードします。
- [Authorized]：オーバーレイネットワーク内の認証済み WAN エッジデバイスの総数。これらの WAN エッジデバイスは、**[Configuration]** > **[Certificates]** > **[WAN Edge List]**画面で [Valid] としてマークされています。
- [Deployed]：導入されている WAN エッジデバイスの総数。これらは、[Valid] とマークされ、現在ネットワークで動作している WAN エッジデバイスです。
- [Staging]：オーバーレイネットワークの一部になる前に、ステージングサイトで構成する WAN エッジデバイスの総数。これらのルータは、ルーティングの決定には関与せず、Cisco vManage によるネットワークモニタリングに影響を与えることもありません。

  ペインをクリックして、[WAN Edge Inventory] ダイアログボックスから各ルータのホスト名、システム IP、サイト ID、およびその他の詳細を表示します。

WAN エッジデバイスの集約状態の表示

[WAN Edge Health] ペインは、各状態のデバイス数のカウントを表示することで、WAN エッジデバイスの状態を集約したビューを提供し、ハードウェアノードの正常性を示します。3 つの WAN エッジデバイスの状態は次のとおりです。

- Normal：メモリ、ハードウェア、CPU が正常な状態の WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% 未満の場合は、normal 状態に分類されます。
- Warning：メモリ、ハードウェア、または CPU が注意状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 70% ～ 90% の場合は、注意状態に分類されます
- Error：メモリ、ハードウェア、または CPU がエラー状態にある WAN エッジデバイスの数。合計メモリまたは合計 CPU の使用率が 90% を超える場合は、エラー状態に分類されます。

  数値または WAN エッジデバイスの状態をクリックすると、過去 12 時間または 24 時間のメモリ使用量、CPU 使用率、およびハードウェア関連のアラーム（温度、電源、PIM モジュールなど）のテーブルが表示されます。テーブルの各行の右側にある [More Actions] アイコンをクリックして、以下にアクセスします。

  - **ハードウェア環境**
  - **[Monitor]** > **[Devices]**画面の [Real Time] ビュー

    Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Network]** 画面の [Real Time] ビュー
  - **[Tools]** > **[SSH Terminal]**画面。

WAN エッジデバイスの損失、遅延、ジッターの表示

[Transport Health] ペインには、すべてのリンクとすべてのカラーの組み合わせ（すべての LTE-to-LTE リンク、すべての LTE-to-3G リンクなど）の集約された平均損失、遅延、およびジッターが表示されます。

[Type] ドロップダウン矢印から、損失、遅延、またはジッターを選択します。

アイコンをクリックして、トランスポートの正常性を表示する期間を選択します。

アイコンをクリックして、[Transport Health] ダイアログボックスを開きます。このダイアログボックスには、より詳細なビューが表示されます。情報を表形式で表示するには、[Details] をクリックします。表示される正常性のタイプと期間を変更することを選択できます。

WAN エッジデバイスの DPI フロー情報の表示

[Top Applications] ペインには、オーバーレイネットワーク内のルータを通過するトラフィックの DPI フロー情報が表示されます。

（注） DPI フロー情報は、過去 24 時間のみ表示されます。過去 24 時間より前の DPI フロー情報を表示するには、特定のデバイスの情報を確認する必要があります。

アイコンをクリックして、データを表示する期間を選択します。[VPN] ドロップダウンリストから VPN を選択して、その VPN 内のすべてのフローの DPI 情報を表示します。

アイコンをクリックして、[Top Applications] ダイアログボックスを開きます。このダイアログボックスには、同じ情報のより詳細なビューが表示されます。VPN と期間を変更できます。

トンネルデータの表示

[Application-Aware Routing] ペインでは、[Type] ドロップダウン矢印から次のトンネル基準を選択できます。

- 損失
- 遅延
- Jitter

トンネル基準に基づいて、ペインに下位 10 件のトンネルが表示されます。たとえば、損失を選択した場合、ペインには、過去 24 時間の平均損失が最も大きい 10 のトンネルが表示されます。

行に対して アイコンをクリックすると、データがグラフィック形式で表示されます。データを表示する期間を選択するか、[Custom] をクリックして、カスタム期間を指定するためのドロップダウン矢印を表示します。

アイコンをクリックして、[Application-Aware Routing] ダイアログボックスを開きます。このダイアログボックスには、[Type] ドロップダウン矢印から選択した基準（損失、遅延、およびジッター）に基づいて下位 25 件のトンネルが表示されます。

テナント WAN エッジデバイスの管理

テナントネットワークへの WAN エッジデバイスの追加

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。

2. デバイスのシリアル番号ファイルを Cisco vManage にアップロードします。
3. デバイスを検証し、詳細をコントローラに送信します。

4. デバイスの設定テンプレートを作成し、デバイスをテンプレートにアタッチします。

   デバイスの設定中に、次の例のようにサービスプロバイダーの組織名とテナントの組織名を設定します。

   ```
   sp-organization-name multitenancy
   organization-name multitenancy-Customer1
   ```

（注） organization-name は <SP Org Name>-<Tenant Org Name> の形式で入力します。

5. Cisco vManage によって生成されたブートストラップ設定を使用してデバイスをブートストラップするか、デバイスで初期設定を手動で作成します。
6. エンタープライズ証明書を使用してデバイスを認証する場合は、CSR を Cisco vManage からダウンロードし、エンタープライズ CA によって署名された CSR を取得します。Cisco vManage に証明書をインストールします。

テナントネットワークからの WAN エッジデバイスの削除

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。
2. 構成テンプレートからデバイスを切り離します。
3. WAN エッジルータを削除します。

Cisco vSmart コントローラ でのテナント固有のポリシー

プロバイダーの admin ユーザー（Cisco vManage のテナントとしてのプロバイダービューから）または tenantadmin ユーザー（Cisco vManage のテナントビューから）は、テナントにサービスを提供する Cisco vSmart コントローラ でテナント固有のポリシーを作成および展開できます。ユーザーは、CLI ポリシーを設定するか、UI ポリシー構成ウィザードを使用してポリシーを作成できます。

ポリシーをアクティブ化または非アクティブ化すると、次のようになります。

1. Cisco vManage は、テナントにサービスを提供する Cisco vSmart コントローラ を識別します。
2. Cisco vManage は、ポリシー構成をプルするように Cisco vSmart コントローラ に通知します。

3. Cisco vSmart コントローラ は、ポリシー構成をプルして展開します。
4. Cisco vManage は、Cisco vSmart コントローラ によるポリシープルのステータスを報告します。

テナントデータの管理

テナントデータのバックアップ

Cisco vManage マルチテナント機能のテナント データ バックアップ ソリューションは、次の機能を提供します。

- 設定データのバックアップファイルの作成、抽出、および表示。
- 後で復元するオプションを使用して、特定のテナントの設定データベースをバックアップします。「テナントデータのバックアップファイルの復元と削除」を参照してください。
- Cisco vManage に格納されているテナントのバックアップファイルを削除します。テナントデータ バックアップ ファイルの削除については、「テナントデータのバックアップファイルの復元と削除」をご覧ください。

データ バックアップ ソリューションを使用する場合、次の要因が適用されます。

- テナントデータのバックアップソリューションの操作は、テナント管理者がテナントビューを介し、プロバイダーとして実行できます。さまざまなビューからテナントダッシュボードにアクセスする方法については、マルチテナント環境でのユーザーロール（933ページ）を参照してください。
- テナントは、特定の時間に次のバックアップ操作を実行でき、1 つの操作を完了してから新しい操作を開始する必要があります。
  - 単一の設定データベースのバックアップ
  - バックアップファイルのダウンロード
  - バックアップファイルの復元またはインポート
  - バックアップファイルの削除
  - バックアップファイルの一覧表示
- テナントのバックアップファイルの形式は次のとおりです。

  ```
  Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz
  ```
- テナントデータのバックアップ操作は、設定データベースに対する読み取り専用操作です。ただし、データの整合性を確保し、データの損失を防ぐため、ネットワーク上で大きな変更は実行しないでください。

- 特定のテナントのバックアップまたは復元操作が進行中のとき、他のテナントはバックアップおよび復元操作をスムーズに実行できます。
- テナントデータベースの復元操作が進行中の場合、テナントは他のバックアップ操作を実行できません。したがって、テナントは単一のバックアップ操作を実行でき、この操作が進行中の場合、すべての新しいバックアップ操作要求は拒否されます。

  残りのテナントは、バックアップ操作を続行できます。
- テナントは、バックアップの生成および復元操作に対して、同じ Cisco vManage バージョンを使用する必要があります。
- テナントは最大 3 つのバックアップファイルを Cisco vManage に保存でき、ダウンロードして Cisco vManage リポジトリの外部に保存できます。テナントにすでに 3 つのバックアップファイルがある場合、後続のバックアップ操作により、最も古いバックアップファイルが削除され、新しいバックアップファイルが生成されます。
- バックアップファイルと、テナントが復元操作を要求したセットアップの両方で、次のパラメータ値が一致していることを確認します。
  - テナントID（Tenant Id）
  - 組織名
  - SP Organization Name
- テナントデータのバックアップソリューションは、Cisco vManage のテナントビューにタスクを作成します。そのため、テナントはテナントダッシュボードのタスクビューから操作の進行状況を監視できます。
- プロバイダーは、このソリューションを使用してプロバイダーデータをバックアップすることはできません。したがって、プロバイダーは、CLI を使用してすべてのテナント設定データベースをバックアップすることにより、すべてのテナント情報を一度にバックアップできます。

設定データのバックアップファイルの作成、抽出、および表示

1. Cisco vManage にログインします。

   プロバイダーユーザーの場合は、管理者としてログインします。プロバイダーダッシュボードで、ドロップダウンリストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナントユーザーの場合は、tenantadmin としてログインします。
2. アドレスバーで、REST API 接続の `dataservice` を使用して URL パスを変更します。

   例：`https://<tenant_URL>/dataservice`
3. 次の API を使用して構成バックアップファイルを作成します。
   `https://<tenant_URL>/dataservice/tenantbackup/export`。

4. 構成バックアップファイルが正常に作成されると、Cisco vManage タスクビューにバックアップファイルが生成されたことが示されます。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

   例：

   ```
   {
      "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
   "status": "in-progress"
   }
   ```

5. 取得したプロセス識別子でタスクの状態を確認します。

   例：
   `https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061`

   検証により、タスクの詳細が JSON ファイル形式で生成されます。

6. タスクが完了したら、JSON タスクファイルの [data] セクションにあるバックアップファイルを抽出またはダウンロードします。

   例：バックアップファイルを抽出またはダウンロードするには、次の API を使用します。
   `https://<tenannt_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

7. 次の API を使用して、Cisco vManage に保存されているバックアップファイルを一覧表示します。

   例：`https://<tenant_URL>//dataservice/tenantbackup/list`

テナントデータのバックアップファイルの復元と削除

始める前に

テナント データ バックアップ ファイルの復元および削除 API を実行するには、Postman ツールまたはhttpアプリケーションとサービスをテストするための他の代替ツールをダウンロードしてインストールします。このドキュメントでは、Postman ツールを使用してテナントデータのバックアップファイルを復元および削除する手順を説明しました。Postman は、API 開発環境として使用されるソフトウェアツールです。このツールは、Postman の Web サイトからダウンロードできます。

1. Google Chrome または別のブラウザを開き、開発者モードを有効にします。
2. Cisco vManage にログインします。

   プロバイダー ユーザーの場合は、管理者としてログインします。プロバイダー ダッシュボードで、ドロップダウン リストからテナントを選択して、テナントとしてのプロバイダービューに入ります。

   テナント ユーザーの場合は、tenantadmin としてログインします。

3. 復元 API のヘッダー情報を取得するには、次のようにします。
   1. 画面の右側で、[Network] タブをクリックして、ネットワーク キャプチャ ビューを表示します。

2. ネットワーク キャプチャ ビューで、[Name] 列をクリックして、リストされている項目を並べ替えます。
3. index.html を検索してクリックします。
4. [Headers] タブをクリックし、[Request Headers] を展開します。
5. Request Headers の下のすべてのテキストを選択し、クリップボードにコピーします。

4. Postman UI を使用してバックアップファイルをインポートします。
   1. Postman UI を開きます。
   2. SSL 証明書の検証を無効にするには、**[Postman]** > **[Preferences]** > **[General]** > **[Request]** をクリックします。[SSL Certificate Verification] をオフにします。
   3. Postman UI で、新しいタブを作成します。
   4. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
   5. [Request Headers] ブロックからステップ 3 でコピーしたテキストを、編集可能なフォームに貼り付けます。
   6. [GET] メソッド ドロップダウン リストから、[POST] を選択します。
   7. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、`dataservice/tenantbackup/import` を含めます。

      例：`https://Customer1.multitenancy.com/dataservice/tenantbackup/import`
   8. [Body] タブをクリックし、[form-data] を選択します。
   9. [KEY] 列に *bakup.tar.gz* と入力します。
   10. [VALUE] 列で、[Select Files] をクリックし、インポートするバックアップファイルを選択します。
   11. API を実行するには、[Send] をクリックします。

       Postman UI の [Response] セクションで、復元されたファイルを示す JSON 情報を表示できます。

5. 次のいずれかの方法で、バックアップファイルの復元を監視します。
   1. バックアップファイルが正常にインポートされたかどうかを示す Cisco vManage タスクビューを使用します。作成されたプロセスまたはタスクのプロセス識別子を表示できます。

      例：

      ```
      {"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
          "status": "Import Successfully Submitted for tenant 1579026919487"
      }
      ```
   2. 次の URL を使用してステータスを取得します。`https://<tenant_URL>/dataservice/device/action/status/<processId>`

例：
https://Customer1.multitenancy.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d

6. Postman UI を使用してテナントデータのバックアップファイルを削除します。
   1. Postman UI で、新しいタブを作成します。
   2. [Request Headers] をクリックし、[Bulk Edit] をクリックします。
   3. [Request Headers] ブロックからステップ 3 でコピーしたテキストを、編集可能なフォームに貼り付けます。
   4. [GET] メソッド ドロップダウン リストから [DELETE] を選択します。
   5. [Paste request URL] フィールドに、テナントの専用 URL を貼り付け、`dataservice/tenantbackup/delete?fileName='filename'` を含めます。ファイル名には、バックアップファイルの名前または all を指定できます。

      例：
      https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz

      例：`https://Customer1.multitenancy.com/dataservice/tenantbackup/delete?fileName=all`
   6. API を実行するには、[Send] をクリックします。

   Postman UI の [Response] セクションで、削除されたファイルを示す JSON 情報を表示できます。

   例：

```
{
    "Deleted": [
        "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
    ]
}
```

Cisco vSmart コントローラでのテナントごとの OMP 統計表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. 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 のメニューから **[Monitor]** > **[Network]** の順に選択します。
3. デバイスのテーブルで、Cisco vSmart コントローラのホスト名をクリックします。
4. 左側のペインで、[Real Time] をクリックします。
5. [Device Options] フィールドに [OMP] と入力し、表示する OMP 統計を選択します。

6. [Select Filters] ダイアログボックスで [Show Filters] をクリックします。
7. [Tenant Name] を入力し、[Search] をクリックします。

Cisco vManage は、特定のテナントの選択された OMP 統計を表示します。

Cisco vSmart コントローラに関連付けられたテナントの表示

1. プロバイダーの **admin** ユーザーとして Cisco vManage にログインします。
2. **vSmart** 接続番号をクリックし、各接続に関する詳細情報を示す表を表示します。

   Cisco vManage は、Cisco vSmart コントローラとその接続の概要を示す表を表示します。
3. Cisco vSmart コントローラの場合は、[...] をクリックし、[Tenant List] をクリックします。

   Cisco vManage は、Cisco vSmart コントローラに関連付けられたテナントの概要を表示します。

シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行

表 *231 :* 機能の履歴

機能名	リリース情報	説明
シングルテナント Cisco SD-WAN オーバーレイからマルチテナント Cisco SD-WAN 展開への移行	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、一連の Cisco vManage API 呼び出しを使用して、シングルテナントの Cisco SD-WAN オーバーレイをマルチテナント展開に移行できます。

はじめる前に

- 移行を開始する前に、次の手順を実行します。
  - シングルテナント展開のエッジデバイスがマルチテナント展開の Cisco vBond Orchestrator に到達できることを確認します
  - エッジデバイスのテンプレート、ルーティング、およびポリシー構成が Cisco vManage の現在の構成と同期していることを確認します

- この手順を実行する前に、シングル テナント オーバーレイのメンテナンスウィンドウを構成します。「Configure or Cancel vManage Server Maintenance Window」を参照してください。

- 移行するシングルテナント オーバーレイの最小ソフトウェア要件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.5.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.5.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.5.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.4.1a

- シングルテナント オーバーレイの移行先となるマルチテナント展開の最小ソフトウェア要件

デバイス	ソフトウェア バージョン
Cisco vManage	Cisco vManage リリース 20.5.1
Cisco vBond Orchestrator	Cisco SD-WAN リリース 20.5.1
Cisco vSmart Controller	Cisco SD-WAN リリース 20.5.1
Cisco IOS XE SD-WAN デバイス	Cisco IOS XE リリース 17.5.1a

- API 呼び出しを実行するには、カスタムスクリプトまたは Postman などのサードパーティアプリケーションを使用することをお勧めします。

移行手順

1. オーバーレイを制御する Cisco vManage インスタンスからシングルテナントの展開および構成データをエクスポートします。

メソッド	`POST`
URL	`https://ST-vManage-IP-address`
エンドポイント	`/dataservice/tenantmigration/export`
許可	管理者ユーザーログイン情報。

本文	必須 フォーマット：Raw JSON `{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }` Field Description: • `desc`：テナントの説明。説明の最大長は 256 文字で、英数字のみを使用できます。 • `name`：マルチテナント展開のテナントの一意の名前。 • `subdomain`：テナントの完全修飾サブドメイン名。サブドメイン名には、サービスプロバイダーのドメイン名が含まれている必要があります。たとえば、`multitenancy.com` がサービスプロバイダーのドメイン名であり、テナント名が `Customer1` である場合、テナントのサブドメイン名は `Customer1.multitenancy.com` になります。 • `orgName`：テナント組織の名前。組織名では、大文字と小文字が区別されます。
応答	フォーマット：JSON `{ "processId": <vManage_process_ID>, }`

データのエクスポート中に、Cisco vManage は、マルチテナント展開への移行に備えて、エッジデバイスから CLI テンプレートを切り離そうとします。Cisco vManage によってプロンプトが表示された場合は、CLI テンプレートをエッジデバイスから切り離し、エクスポート API 呼び出しを再度実行します。

2. Cisco vManage でデータエクスポートタスクのステータスを確認します。タスクが成功したら、URL
`https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz` を使用してデータをダウンロードします

3. マルチテナント Cisco vManage インスタンスで、シングルテナント オーバーレイからエクスポートされたデータをインポートします。

メソッド	`POST`
URL	`https://MT-vManage-IP-address`
エンドポイント	`/dataservice/tenantmigration/import`
許可	プロバイダー管理者ユーザーログイン情報。

本文	必須 フォーマット：フォームデータ キータイプ：ファイル 値：`default.tar.gz`

応答	フォーマット：JSON
	`{`
	`"processId": <vManage_process_ID>,`
	`"migrationTokenURL": <token_URL>,`
	`}`

タスクが成功すると、マルチテナント Cisco vManage で、シングルテナント オーバーレイからインポートされたデバイス、テンプレート、およびポリシーを表示できます。

4. **手順 3** の API 呼び出しに応答して取得したトークン URL を使用して、移行トークンを取得します。

方法	`GET`
URL	`https://MT-vManage-IP-address`
エンドポイント	**手順 3** で取得した `migrationTokenURL`。
許可	プロバイダー管理者ユーザーログイン情報。
応答	エンコードされたテキストの大きな BLOB としての移行トークン。

5. シングルテナント Cisco vManage インスタンスで、マルチテナント展開へのオーバーレイの移行を開始します。

メソッド	`POST`
URL	`https://ST-vManage-IP-address`
エンドポイント	`dataservice/tenantmigration/networkMigration`
許可	管理者ユーザーログイン情報。
本文	必須 フォーマット：生のテキスト 内容：**手順 4** で取得した移行トークン。

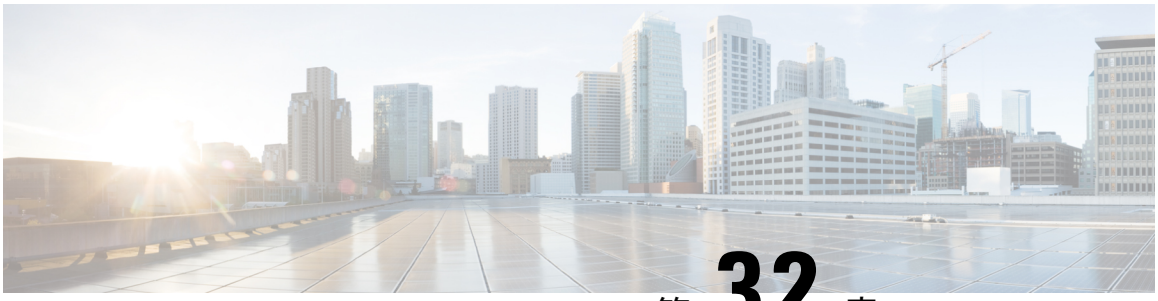
応答	フォーマット：JSON
	`{`
	`"processId": <vManage_process_ID>,`
	`}`

Cisco vManage で、移行タスクのステータスを確認します。移行タスクの一部として、マルチテナント vBond Orchestrator のアドレス、サービスプロバイダーおよびテナントの組織名が、シングルテナント オーバーレイの WAN エッジデバイスにプッシュされます。タス

クが成功すると、WAN エッジデバイスはマルチテナント展開のコントローラへの制御接続を形成します。WAN エッジデバイスは、シングル テナント オーバーレイのコントローラに接続されなくなります。

マルチテナント展開への移行後に、（手順 1 で）エッジデバイスから切り離された CLI テンプレートを接続します。テンプレートを接続する前に、マルチテナント展開の構成と一致するように Cisco vBond Orchestrator の IP アドレスと組織名を更新します。

（注） シングルテナント展開では、Cisco vManage 署名付き証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、デバイスがマルチテナント展開に移行されるときに証明書がクリアされます。マルチテナント Cisco vManage でデバイスを再認証する必要があります。エンタープライズ証明書がクラウドベースの WAN エッジデバイスにインストールされている場合、証明書は移行の影響を受けません。詳細については、「Enterprise Certificates」を参照してください。



第 32 章

Cisco SD-WAN Carrier Supporting Carrier

表 *232 :* 機能の履歴

機能名	リリース情報	説明
Carrier Supporting Carrier接続のための Cisco SD-WAN サポート	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Cisco IOS XE SD-WAN デバイスで Carrier Supporting Carrier（CSC）接続のサポートが追加されます。 CSC を使用すると、マルチプロトコル ラベル スイッチング（MPLS）バックボーンネットワークを介してさまざまなサイトで動作する IP または MPLS ネットワークをインターコネクトできます。CSC を使用するには、キャリアエッジ（CE）デバイスと呼ばれる CSC 機能をサポートするエッジルータが各サイトに必要です。この機能により、Cisco IOS XE SD-WAN デバイスは CE デバイスとして機能できるため、Cisco SD-WAN が管理する各サイトで個別の専用 CE デバイスを用意する必要がなくなります。

Cisco SD-WAN Carrier Supporting Carrier の前提条件

CSC カスタマーエッジ（CSC-CE）デバイスとして機能する Cisco IOS XE SD-WAN デバイスには、CSC プロバイダーエッジ（CSC-PE）ルータとの外部ボーダー ゲートウェイ プロトコル（eBGP）ピア接続が必要です。

Cisco SD-WAN Carrier Supporting Carrier の制約事項

- IPv6 アドレス指定はサポートされていません。
- MPLS リンクのネットワークアドレス変換（NAT）はサポートされていません。
- MPLS リンク上のファイアウォールサービスはサポートされていません。
- Software as a Service（SaaS）の Cloud OnRamp はサポートされていません。
- VPN ルートリークはサポートされていません。

Cisco SD-WAN Carrier Supporting Carrier に関する情報

Carrier Supporting Carrier

Carrier Supporting Carrier（CSC）は、組織が MPLS バックボーンネットワークを介してさまざまなサイトにある IP または MPLS ネットワークを相互接続できるようにする階層型 VPN モデルです。これにより、組織は独自の MPLS バックボーンを構築および維持する必要がなくなります。

CSC のコンポーネントは次のとおりです。

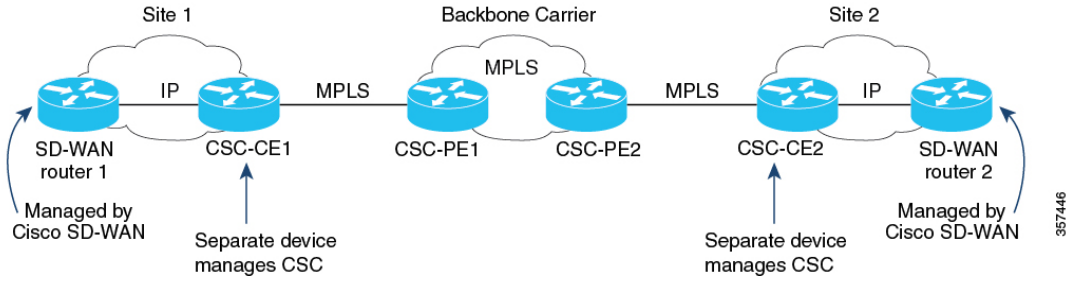
- バックボーンキャリア：バックボーンネットワークを提供するサービスプロバイダー。通常、バックボーン キャリア ネットワークは複数のセグメントを使用して、バックボーン キャリア ネットワークを共有するさまざまなカスタマーキャリアのトラフィックを分離します。バックボーンキャリアは、カスタマーキャリアと同じ組織によって管理される場合もあれば、異なる組織によって管理される場合もあります。
- カスタマーキャリア：バックボーンネットワークを使用して、あるサイトから別のサイトにトラフィックをルーティングする組織。カスタマーキャリアは、バックボーンネットワークを運用する組織の一部である場合もあれば、独立している場合もあります。
- CSC-CE：カスタマーエッジ（CE）デバイス。このデバイスはローカルサイトネットワーク内で動作し、MPLS 接続を使用してサイトをバックボーンキャリアに接続します。バックボーンキャリアを利用して他のサイトに接続します。
- CSC-PE：プロバイダーエッジ（PE）デバイス。このデバイスはバックボーン キャリア ネットワーク内で動作し、MPLS 接続を使用してカスタマーサイトの CSC-CE デバイスに接続します。

Cisco SD-WAN Carrier Supporting Carrier

次の図は、Cisco IOS XE リリース 17.6.1a より前のリリースを使用する Cisco IOS XE SD-WAN デバイス を各サイトに配置した CSC ネットワークトポロジを示しています。これらのリリースを使用する場合、Cisco IOS XE SD-WAN デバイス は CSC-CE として機能できないため、こ

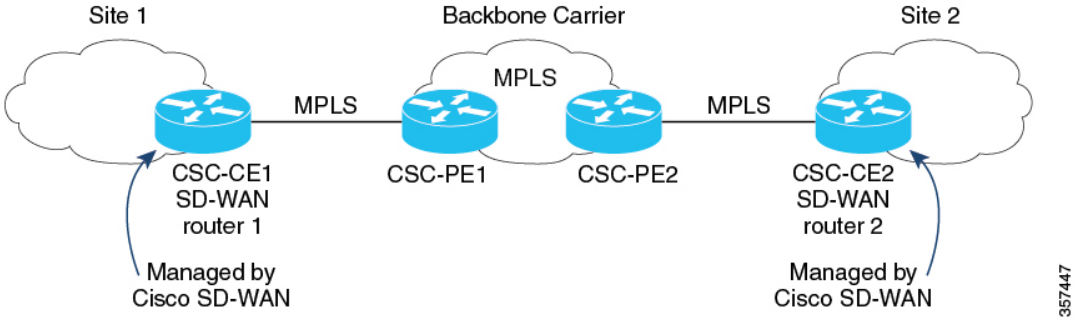
のトポロジでは各サイトに 2 つの個別のデバイスが必要です。つまり、Cisco SD-WAN で管理するエッジデバイスと別の CSC-CE デバイスです。

図 *4 : Cisco SD-WAN* を使用した *Carrier Supporting Carrier*（*Cisco IOS XE* リリース *17.6.1a* よりも前のリリース）



Cisco IOS XE リリース 17.6.1a 以降、Cisco IOS XE SD-WAN デバイス は CSC-CE デバイスとして機能できるため、個別の専用 CSC-CE デバイスを用意する必要はありません。次の図は、CSC-CE 機能を提供する Cisco IOS XE SD-WAN デバイス を使用する、前の図よりも単純な CSC ネットワークトポロジを示しています。

図 *5 : Cisco SD-WAN* を使用した *Carrier Supporting Carrier*（*Cisco IOS XE* リリース *17.6.1a* 以降のリリース）



トラフィック フロー

CSC-CE デバイスにネイバー CSC-PE デバイスへの MPLS 接続のみがある場合、CSC-CE デバイスからのすべてのトラフィックは、次のトラフィックタイプを含む MPLS 接続を使用します。

- サービス VPN トラフィック
- 制御トラフィック
- Cisco SD-WAN Bidirectional Forwarding Detection（BFD）プローブトラフィック

CSC-CE デバイスにネイバー CSC-PE デバイスへの MPLS 接続があり、インターネットへの別の接続もある場合、CSC-CE デバイスからのトラフィックは、次のように異なる接続を使用できます。

- 設定されたトラフィックポリシーに基づいて、制御トラフィックと BFD プローブトラフィックは、インターネットと MPLS 接続を使用できます。

- サービス VPN トラフィックは、MPLS 接続のみを使用します。

ラベルスイッチング

CSCデバイスとバックボーンキャリア間でMPLS接続を使用するトラフィックの場合、バックボーンキャリアはラベルスイッチドパスを使用してトラフィックを管理するため、カスタマーキャリアルートに関する情報はありません。

Cisco SD-WAN Carrier Supporting Carrier の利点

Cisco SD-WAN が CSC をサポートすることで、Cisco IOS XE SD-WAN デバイスは、CSC が必要なサイトでエッジデバイスとして機能できます。Cisco IOS XE SD-WAN デバイスが CSC-CE 機能を提供することで、CE の役割を提供する別個のルータを用意する必要がありません。

Cisco SD-WAN Carrier Supporting Carrier の使用例

Cisco SD-WAN の CSC のサポートは、バックボーンキャリアで CSC を使用して組織の複数の独立した部門をサポートするグローバル組織に役立ちます。各部門のトラフィックはプライベートですが、共通のバックボーンキャリアを共有します。

CSC トポロジを使用するサービスプロバイダーは、Cisco SD-WAN による CSC のサポートから恩恵を受ける可能性があります。Cisco SD-WAN によって管理されるキャリアエッジデバイスは CSC をサポートできるため、CSC 機能を管理するために別のデバイスを用意する必要はありません。

Carrier Supporting Carrier の設定

次の方法で、CSC の CE デバイスを設定できます。

- （推奨）Cisco vManage では、BGP 機能テンプレートを使用します。
- Cisco vManage では、CLI テンプレートを使用して、CLI で CSC を設定します。

Carrier Supporting Carrier の設定

新しい機能テンプレートを使用してCSCのCEデバイスを設定するには、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. [Device Templates] をクリックし、[Create Template] をクリックします。ドロップダウンから、[From Feature Template] を選択します。

（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. [Device Model] フィールドで、正しいデバイスモデルを選択します。
4. [Device Role] フィールドで、[SDWAN Edge] を選択します。
5. [Template Name] フィールドに、テンプレートの名前を入力します。
6. [Transport & Management VPN] セクションの [Cisco VPN 0] フィールドで、ネットワークアーキテクチャに従って VPN 0 を設定するためのテンプレートを選択します。

   VPN 0 の設定については、『Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「Configure Interfaces in the WAN Transport VPN (VPN 0)」を参照してください。
7. [Cisco VPN Interface Ethernet] フィールドで、インターフェイスを設定するためのテンプレートを選択します。

   このフィールドの設定については、『Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「Configure VPN Ethernet Interface」を参照してください。
8. [Transport & Management VPN] セクションで、[Cisco BGP] をクリックして [Cisco BGP] フィールドを追加します。

   BGP テンプレートの設定の詳細については、『Cisco SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x』の「Configure BGP Using vManage Templates」を参照してください。
9. [MPLS Interface] セクションの [Interface Name 1] フィールドに、デバイスをバックボーンキャリアに接続するために使用するインターフェイスを入力します。
10. [Neighbor] セクションで、[Advanced Options] をクリックして、CSC オプションを表示します。
11. CSC サポートに固有の次のフィールドを設定します。

フィールド	説明
Send Label	[On] を選択して、CSC サポートを有効にします。
Explicit Null	デバイスがループバック WAN インターフェイスを使用している場合は、[On] を選択します。
As Override	バックボーンキャリアを介して接続する 2 つの CE デバイス（CE1 および CE2）が同じ自律システム（AS）番号を使用する場合は、[On] を選択します。

フィールド	説明
Allowas In	[As Override] と同様に、2 つの CE サイトが同じ AS 番号を使用する場合は、[On] を選択します。

12. [Save] をクリックして BGP 設定を保存します。
13. [Create] をクリックして機能テンプレートを作成します。

    [Configuration] > **[Templates]** ページが表示され、使用可能なテンプレートが表示されます。
14. テンプレートをデバイスにアタッチします。
    1. **[Configuration]** > **[Templates]** ページを参照してください。
    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. 新しいテンプレートについて、[...] をクリックし、[Attach Devices] を選択します。
    4. デバイスを [Selected Devices] 列に移動し、[Attach] をクリックします。

CLI を使用した Carrier Supporting Carrier の設定

Cisco vManage の BGP 機能テンプレートを使用して、Cisco IOS XE SD-WAN デバイス を CSC で使用するように設定することをお勧めします。CLI でデバイスを設定する必要がある場合は、Cisco vManage で CLI テンプレートを使用します。

はじめる前に

CSC-CE 機能を提供するように Cisco IOS XE SD-WAN デバイス を設定する前に、デバイスに BGP 設定を適用します。次の手順では、CSC 機能を追加します。

CLI を使用した Carrier Supporting Carrier の設定

1. CSC-CE1 で次を設定します。
    1. MPLS ラベルを VRF にマッピングするようにデバイスを設定します。着信トラフィックの場合、ルータはトラフィックの MPLS ラベルをチェックし、そのラベルにマッピングされた VRF の IP ルックアップテーブルを使用します。たとえば、MPLS ラベル 10 が VRF 1 にマッピングされている場合、MPLS ラベル 10 の着信トラフィックに対して、ルータは VRF 1 の IP ルックアップテーブルを使用します。MPLS ラベルを VRF にマッピングする方法については、MPLS 転送コマンドに関するシスコのドキュメントを参照してください。

```
Device# config-transaction
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
Device(config)# mpls label range min-label max-label static min-static-label
max-static-label
```

2. インターフェイスでマルチプロトコルラベルスイッチング（MPLS）を有効にします。

```
Device(config)# interfaceinterface
Device(config-if)# mpls bgp forwarding
```

3. ルータコンフィギュレーションモードを開始し、BGPプロセスを実行するようにルータを設定します。

```
Device(config-if)# router bgp bgp-number
```

4. CSC-PEデバイスをネイバーとして設定します。ここで、*neighbor-ip* はネイバーCSC-PEデバイスのアドレスです。

```
Device(config-router)# neighbor neighbor-ip allowas-in
```

5. デバイスでループバック WAN インターフェイスを使用する場合は、BGP ルートとともに MPLS ラベルを送信するルータの機能をアドバタイズします。**explicit-null** キーワードにより、CSC-CE ルータは値 0 のラベルをネイバーに送信できます。

（注） ループバック WAN インターフェイスを使用しないデバイスで **neighbor** *neighbor-ip* **send-label explicit-null** コマンドを使用しても、パフォーマンスに悪影響を与えることはありません。

```
Device(config-router)# neighbor neighbor-ip send-label explicit-null
```

2. CSC-CE2 で次を設定します。

1. MPLS ラベルを VRF にマッピングするようにデバイスを設定します。着信トラフィックの場合、ルータはトラフィックの MPLS ラベルをチェックし、そのラベルにマッピングされた VRF の IP ルックアップテーブルを使用します。たとえば、MPLS ラベル 10 が VRF 1 にマッピングされている場合、MPLS ラベル 10 の着信トラフィックに対して、ルータは VRF 1 の IP ルックアップテーブルを使用します。MPLS ラベルを VRF にマッピングする方法については、MPLS 転送コマンドに関するシスコのドキュメントを参照してください。

```
Device# config-transaction
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
Device(config)# mpls label range min-label max-label static min-static-label
max-static-label
```

2. インターフェイスでマルチプロトコルラベルスイッチング（MPLS）を有効にします。

```
Device(config)# interfaceinterface
Device(config-if)# mpls bgp forwarding
```

3. ルータコンフィギュレーションモードを開始し、BGPプロセスを実行するようにルータを設定します。

```
Device(config-if)# router bgp bgp-number
```

4. CSC-PEデバイスをネイバーとして設定します。ここで、*neighbor-ip* はネイバーCSC-PEデバイスのアドレスです。

   ```
   Device(config-router)# neighbor neighbor-ip as-override
   ```

5. デバイスでループバック WAN インターフェイスを使用する場合は、BGP ルートとともに MPLS ラベルを送信するルータの機能をアドバタイズします。

   ```
   Device(config-router)# neighbor neighbor-ip send-label explicit-null
   ```

例

次の例は、CSC-CE1 と CSC-CE2 の 2 つのデバイスの、CSC 機能を含む完全な BGP 設定を示しています。

- CSC-CE1 のアドレスは 10.1.1.10 です。
- CSC-CE2 のアドレスは 10.1.1.20 です。
- CSC-PE1（CSC-CE1 のネイバー）のアドレスは 10.2.2.10 です。
- CSC-PE2（CSC-CE2 のネイバー）のアドレスは 10.2.2.20 です。

CSC-CE1 の設定は次のとおりです。

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet2
 no shutdown
 mpls bgp forwarding
 ip address 10.1.1.15 255.255.255.0

router bgp 10
 bgp log-neighbor-changes
 bgp router-id 172.16.255.15
 neighbor 10.1.1.20 remote-as 100
 neighbor 10.1.1.20 fall-over bfd
address-family ipv4 unicast
  maximum-paths 4
  neighbor 10.1.1.20 activate
  neighbor 10.1.1.20 advertisement-interval 30
  neighbor 10.2.2.10 allowas-in
  neighbor 10.2.2.10 send-label explicit-null
  neighbor 10.1.1.20 send-community both
  exit-address-family
 !
 timers bgp 60 180
```

CSC-CE2 の設定は次のとおりです。

```
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
mpls label range 100000 1048575 static 16 99
interface GigabitEthernet5
 ip address 10.0.6.11 255.255.255.0
 negotiation auto
 mpls bgp forwarding

router bgp 10
```

```
bgp log-neighbor-changes
bgp router-id 172.16.255.11
neighbor 10.1.1.10 remote-as 200
address-family ipv4 unicast
 neighbor 10.1.1.10 activate
 neighbor 10.1.1.10 advertisement-interval 30
   neighbor 10.2.2.20 as-override
   neighbor 10.2.2.20 send-label explicit-null
 network 10.0.7.0 mask 255.255.255.0
 redistribute connected
 redistribute static
 exit-address-family
```

デバイスが Carrier Supporting Carrier 用に設定されていることの確認

デバイスがリモートCSC-CEデバイスに到達するように正しく設定されていることを確認するには、デバイスで **show ip route** *remote-csc-ce-device-address* コマンドを実行します。コマンド出力に次のように表示されることを確認します。

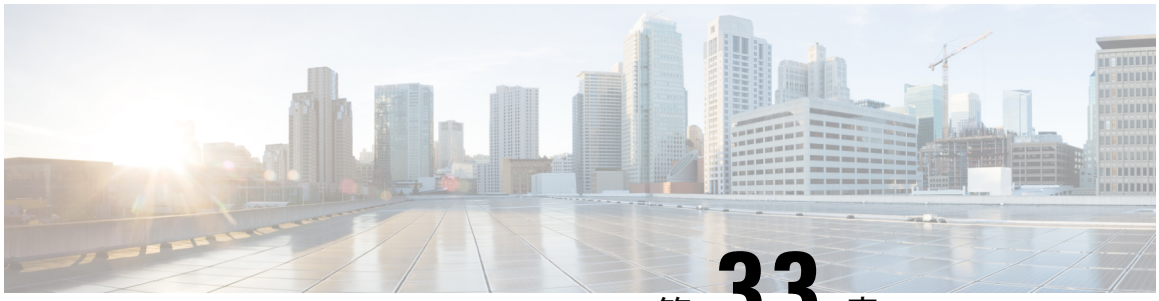
- リモートサイトの IP アドレスのルーティングエントリ。
- リモート CSC-CE デバイスへのパスのネクストホップアドレスを記述する 1 つ以上のルーティング記述子ブロック。各記述子ブロックにMPLS ラベルが含まれていることを確認します。

例

```
Device# show ip route 10.0.1.100
Routing entry for 10.0.1.0/24
...
Routing Descriptor Blocks:
* 10.1.1.100, from 10.1.1.100, 00:00:50 ago
...
MPLS label: 26
…
```

デバイスが正しく構成されていない場合、出力には次のように表示されます。

```
% Subnet not in table
```



第 33 章

Cisco 1000 シリーズ統合型サービスルータでのワイヤレス管理

表 *233 :* 機能の履歴

機能名	リリース情報	説明
Cisco ISR 1000 シリーズ ルータでのワイヤレス管理（Wi-Fi 5 WLAN モジュールをサポート）	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco vManage を使用する Wi-Fi 5 対応 Cisco 1000 シリーズ サービス統合型ルータでワイヤレス LAN 設定を構成できます。 Cisco vManage を使用すると、ワイヤレス LAN コントローラの設定を自動化してワイヤレス接続を提供することができます。別の外部コントローラでルータのワイヤレス設定を構成および管理する必要がありません。

機能名	リリース情報	説明
Cisco ISR 1000 シリーズ ルータでのワイヤレス管理（Wi-Fi 6 WLAN モジュールをサポート）	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、Cisco vManage を使用する Wi-Fi 6 対応 Cisco 1000 シリーズ サービス統合型ルータでワイヤレス LAN 設定を構成できます。 Cisco 1000 シリーズ サービス統合型ルータの組み込みワイヤレスコントローラを使用すると、ワイヤレス接続を提供でき、別の外部コントローラでルータのワイヤレス設定を構成および管理する必要がありません。

Cisco ISR 1000 シリーズ ルータのワイヤレス管理でサポートされるデバイス

次の表に、WLAN モジュールを搭載し、WiFi 5 をサポートする Cisco ISR 1000 シリーズ ルータのリストを示します。

表 *234 : Cisco ISR 1000* シリーズ ルータ

デバイス ファミリ	Device Name	リリースバージョン
WiFi 5 をサポートする WLAN モジュールを備えた Cisco ISR 1000 シリーズ ルータ	• C1101-4PLTEPW • C1109-4PLTE2PW • C1111-4PW • C1111-8PLTEEAW • C1111-8PW • C1112-8PLTEEAW • C1112-8PW • C1113-8PLTEEAW • C1113-8PMW • C1113-8PW • C1116-4PLTEEAW • C1116-4PW • C1117-4PLTEEAW • C1117-4PLTELAW • C1117-4PMLTEEAW • C1117-4PMW • C1117-4PW • C1121-8PLTEPW • C1121X-8PLTEPW	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1
WiFi 6 をサポートする WLAN モジュールを備えた Cisco ISR 1000 シリーズ ルータ	• C1131X-8PLTEPW • C1131-8PLTEPW • C1131X-8PW • C1131-8PW	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1

Cisco ISR 1000 シリーズ ルータでのワイヤレス管理の前提条件

- DHCP や RADIUS などのサーバーにアクセスするには、ワイヤレス LAN（WLAN）モジュールの管理インターフェイスを特定の VLAN に追加します。

- アクセスポイントに IP アドレスを割り当てるように DHCP サーバーを設定します。
- 仮想 WLAN コントローラ管理のために、Cisco ISR 1000 サービスルータでスイッチ仮想インターフェイス（SVI）を設定します。

Cisco ISR 1000 シリーズ ルータでのワイヤレス管理の制約事項

- Cisco Mobility Express が設定されているルータの LAN 側に設定できるアクセスポイントは 1 つだけです。ただし、Cisco Mobility Express が設定されていないルータに他の外部アクセスポイントを接続することはできます。
- LAN 側に他のアクセス可能なワイヤレスコントローラがないことを確認します。

Cisco ISR 1000 シリーズ ルータでのワイヤレス管理に関する情報

WiFi 5 をサポートする WLAN モジュールは、ワイヤレス接続用に Cisco ISR 1000 シリーズ ルータにプロビジョニングされています。仮想ワイヤレス LAN コントローラである Cisco Mobility Express は、ワイヤレス LAN アクセスを提供するために WLAN モジュールにインストールされます。ワイヤレス LAN アクセスのワイヤレス設定は Cisco Mobility Express で利用できます。これらの設定は、Cisco vManage を使用して設定および管理できます

C1131 Cisco IOS XE SD-WAN デバイス には、WiFi 6 をサポートする組み込みワイヤレスコントローラ（EWC）が含まれています。EWC は、WLAN モジュールにインストールされる仮想ワイヤレスコントローラとしても機能します。ワイヤレス LAN アクセスのワイヤレス設定は EWC で使用できます。これらの設定は、Cisco vManage を使用して設定および管理できます。

Cisco ISR 1000 シリーズ ルータでのワイヤレス管理の設定

Cisco ISR 1000 シリーズ ルータでワイヤレス設定を設定および管理するには、次の手順を実行します。

1. Cisco vManage のメニューから、 [Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックします。
3. [Add Template] をクリックして、該当するデバイスモデルを選択します。

（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。

4. 左ペインの [Select Devices] から、テンプレートを作成する Cisco ISR 1000 シリーズ ルータを選択します。
5. [OTHER TEMPLATES] で、[ISR1K Wireless] をクリックして機能テンプレートとして選択します。
6. [Template Name] フィールドに、機能テンプレートの名前を入力します。

   このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
7. [Description] フィールドに機能テンプレートの説明を入力します。

   このフィールドは必須であり、すべての文字とスペースを含めることができます。
8. ワイヤレス LAN を設定するための Wi-Fi SSID の詳細を入力します。

パラメータ名	説明
ワイヤレス ネットワーク名（SSID）	ワイヤレス SSID の名前を入力します。 4 ～ 32 文字の文字列を指定できます。SSID は一意である必要があります。
VLAN (Range 1-4094)	ワイヤレス LAN トラフィックの VLAN ID を入力します。
Security Type	セキュリティタイプを選択します。 • [WPA2 Enterprise]：リモート RADIUS サーバーでネットワークユーザーを認証および承認する企業では、このオプションを選択します。 • [WPA2 Personal]：パスフレーズを使用してワイヤレスネットワークにアクセスするユーザーを認証するには、このオプションを選択します。 • [Open]：認証なしでワイヤレスネットワークへのアクセスを許可するには、このオプションを選択します。

パラメータ名	説明
RADIUS Server IP	（オプション）このフィールドは、セキュリティタイプとして [WPA2 Enterprise] オプションを選択する場合に使用できます。RADIUS サーバの IP アドレスを入力します。
Authentication Port	（オプション）このフィールドは、セキュリティタイプとして [WPA2 Enterprise] オプションを選択する場合に使用できます。RADIUS サーバーの認証ポート番号を入力します。
Shared Secret	（オプション）このフィールドは、セキュリティタイプとして [WPA2 Enterprise] オプションを選択する場合に使用できます。RADIUS サーバーの共有秘密キーを入力します。
[Passphrase]	（オプション）このフィールドは、セキュリティタイプとして [WPA2 Personal] オプションを選択する場合に使用できます。パスフレーズを設定します。このパスフレーズを使用して、ユーザーがワイヤレスネットワークにアクセスできます。
Admin State	管理状態を選択します。
Radio Type	次のいずれかの無線タイプを選択します。 • 2.4GHz • **5GHz** • **両方**
ブロードキャスト SSID	SSID をブロードキャストする場合は、[On] を選択します。すべてのワイヤレスクライアントに SSID が表示されないようにする場合は、[Off] を選択します。
QoS プロファイル	QoS プロファイルを選択します。

9. ワイヤレス LAN の [General] の詳細を入力します。

パラメータ名	説明
国	ISR がインストールされている国を選択します。
Username	Cisco Mobility Express のユーザー名を指定します。 C1131 Cisco IOS XE SD-WAN デバイスを使用している場合は、EWC のユーザー名を指定します。
Password	Cisco Mobility Express または EWC のパスワードを指定します。

10. ワイヤレス LAN の [Advanced] の詳細を入力します。

パラメータ名	説明
コントローラ IP アドレス	（注） Cisco IOS XE リリース 17.6.1a、および Cisco vManage リリース 20.6.1 以前のリリースでは、このフィールドは [ME IP Address] として表示されます。 Cisco Mobility Express または EWC の管理 IP アドレスを指定します。
[Subnet Mask]	管理 IP アドレスのサブネットマスクを指定します。
デフォルト ゲートウェイ	Cisco Mobility Express または EWC のデフォルト ゲートウェイ アドレスを指定します。
2.4GHz Shutdown	2.4 GHz の無線タイプをシャットダウンするには、[Yes] をクリックします。この無線タイプをシャットダウンしない場合は、[No] をクリックします。
5GHz Shutdown	5 GHz の無線タイプをシャットダウンするには、[Yes] をクリックします。この無線タイプをシャットダウンしない場合は、[No] をクリックします。

11. [Save] をクリックしてワイヤレス設定を保存します。

CLI テンプレートを使用した Cisco ISR 1000 シリーズ ルータでのワイヤレス管理の設定

このセクションでは、CLI テンプレートを使用して Cisco ISR 1000 シリーズ ルータでワイヤレス設定を構成および管理するためのサンプル CLI 設定を提供します。

CLI テンプレートを使用した無線プロファイルの設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

```
radio-profile 24ghz
shutdown
exit
radio-profile 5ghz
no shutdown
```

CLI テンプレートを使用した WLAN プロファイルの設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

```
wlan-profile wlan-profile-sample-1
vlan-id 100
ssid sample-ssid-1
data-security personal
passphrase 0 Pass-Phrase-Sample123#
qos-type silver
wlan-profile wlan-profile-sample-2
vlan-id 200
ssid sample-ssid-2
data-security enterprise
aaa radius-server 10.2.3.4 auth-port 1812 shared-secret 0 EsrdT_23sss

qos-type gold
nobroadcast-ssid
```

CLI テンプレートを使用した一般的な WLAN 設定の構成

CLI テンプレートの使用の詳細については、「CLI Add-On Feature Templates」および「CLI Templates」を参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

```
wireless-lan country US
wireless-lan mgmt ip address10.16.1.100 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 0 sRe32dfst#asd
```

Cisco ISR 1000 シリーズ ルータでワイヤレス設定を構成および管理する方法を示す完全な構成例を次に示します。

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Cisco ISR 1000 シリーズ ルータでのワイヤレス設定のモニタリング

Cisco vManage を使用して Cisco ISR 1000 シリーズ ルータで構成されているワイヤレス設定を監視するには、次の手順を実行します。

1. Cisco vManage のメニューから、[Monitor] > [Network] に移動します。
2. ルータのリストからルータを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストから、次のオプションのいずれかを選択します。

デバイスオプション	説明
ワイヤレス無線	ワイヤレス LAN の無線パラメータを表示します。
Wireless SSID	ワイヤレス SSID に関する情報を表示します。
Wireless Clients	ワイヤレス LAN のワイヤレスクライアントに関する情報を表示します。

Cisco ISR 1000 シリーズ ルータでのワイヤレス設定の設定例

次に、Cisco ISR 1000 シリーズ ルータのワイヤレス設定の例を示します。

```
wlan-profile TEST-Enterprise
radio-band all
vlan-id 300
ssid TEST-Enterprise
data-security enterprise
aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6 EsrdT_23sss
qos-type silver


wlan-profile TEST-Personal
radio-band all
ssid TEST-Personal
data-security personal
passphrase 0 IdSvs23452#
qos-type silver


radio-profile 24ghz
channel auto
channel-bandwidth auto


radio-profile 5ghz
channel auto
channel-bandwidth auto


wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
```

```
wireless-lan mgmt credential username admin password 6 sRe32dfst#asd
wireless-lan country US
```

Cisco ISR 1000 シリーズ ルータでのワイヤレス設定のトラブルシューティング

アクセスポイントが Cisco Mobility Express または EWC に接続できない

問題

アクセスポイントが Cisco Mobility Express または EWC に接続できません。

Possible Causes

この問題は、管理 VLAN（インターフェイス Wlan-GigabitEthernet のネイティブ VLAN）に DCHP サーバーがない場合に発生する可能性が最も高くなります。

ソリューション

DHCP や RADIUS などのサーバーにアクセスするには、WLAN モジュールの管理インターフェイスを特定の VLAN に追加します。Cisco ISR 1000 シリーズ ルータでのワイヤレス管理の前提条件 （973 ページ）を参照してください。

アクセスポイントに IP アドレスを割り当てるには、WiFi モジュールのネイティブ VLAN に DHCP サーバーが必要です。IP アドレスがないと、アクセスポイントは Cisco Mobility Express または EWC に接続できません。

第 34 章

Cisco SD-WAN および Cisco ThousandEyes による可視性の強化

表 *235 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN および Cisco ThousandEyes による可視性の強化	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	Cisco ThousandEyes Enterprise エージェントを、サポートされている Cisco IOS XE SD-WAN デバイスにコンテナアプリケーションとしてネイティブに導入して、Cisco SD-WAN を Cisco ThousandEyes と統合できます。Cisco ThousandEyes Enterprise エージェントは、Cisco vManage を介してインストールおよびアクティブ化できます。 Cisco SD-WAN を Cisco ThousandEyes と統合することにより、インターネット全体の完全なホップバイホップパス分析によってネットワークとアプリケーションのパフォーマンスに関する詳細なインサイトを得ることができ、迅速なトラブルシューティングと解決のために障害ドメインを分離できます。
Cisco 1000 シリーズサービス統合型ルータの Cisco ThousandEyes サポート	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	Cisco ThousandEyes Enterprise エージェントは、Cisco ISR 1100X-6G デバイスのコンテナアプリケーションとしてネイティブに導入できます。Cisco ThousandEyes Enterprise エージェントは、Cisco vManage を介してインストールおよびアクティブ化できます。

機能名	リリース情報	説明
Cisco Catalyst 8500 シリーズエッジプラットフォームおよび Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの Cisco ThousandEyes サポート	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	Cisco ThousandEyes Enterprise エージェントは、Cisco Catalyst 8500 シリーズ エッジ プラットフォームおよび Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上のコンテナアプリケーションとしてネイティブに導入できます。Cisco ThousandEyes Enterprise エージェントは、Cisco vManage を介してインストールおよびアクティブ化できます。

- Cisco SD-WAN および Cisco ThousandEyes による可視性の強化でサポートされるデバイス（985 ページ）
- Cisco SD-WAN および Cisco ThousandEyes による可視性の強化の前提条件 （987 ページ）
- Cisco SD-WAN および Cisco ThousandEyes による可視性の強化の制約事項 （987 ページ）
- Cisco SD-WAN および Cisco ThousandEyes による可視性の強化に関する情報 （987 ページ）
- Cisco IOS XE SD-WAN デバイスでの Cisco ThousandEyes Enterprise Agent の設定 （988 ページ）
- Cisco IOS XE SD-WAN デバイスでの Cisco ThousandEyes Enterprise Agent のトラブルシューティング （996 ページ）

Cisco SD-WAN および Cisco ThousandEyes による可視性の強化でサポートされるデバイス

リリース	プラットフォーム	デバイス モデル	サポートされる ThousandEyes Enterprise Agent の最小バージョン
Cisco IOS XE リリース 17.6.1a 以降	Cisco Catalyst 8300 シリーズ エッジ プラットフォーム	C8300-1N1S-6T	4.0.2
		C8300-1N1S-4T2X	
		C8300-2N2S-6T	
		C8300-2N2S-4T2X	
	Cisco Catalyst 8200 シリーズ エッジ プラットフォーム	C8200-1N-4T	4.0.2
		C8200L-1N-4T	
	Cisco 4000 シリーズ サービス統合型ルータ	ISR4461	4.0.2
		ISR4451	
		ISR4431	
		ISR4351	
		ISR4331	
		ISR4321	
		ISR4221X	
Cisco IOS XE リリース 17.7.1a 以降	Cisco 1000 シリーズ サービス統合型ルータ	ISR1100X-6G	4.1.0
Cisco IOS XE リリース 17.8.1a 以降	Cisco Catalyst 8500 シリーズ エッジ プラットフォーム	C8500-12X	4.2.0
		C8500-12X4QC	
		C8500L-8S4X	
	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	ASR 1001-HX	4.2.0
		ASR 1001-X	
		ASR 1002-HX	
		ASR 1002-X	
		ASR 1006-X（RP3）	

ストレージと DRAM の要件

- **外部ストレージ**：外部ストレージ（SSD M.2 NVMe）が装備されているデバイスでは、Cisco ThousandEyes Enterprise Agent が外部ストレージにインストールされます。Cisco ThousandEyes Enterprise Agent のインストールに必要な最小外部ストレージ容量は 8 GB です。デバイスに十分な外部ストレージ容量がない場合は、最小要件を満たすようにストレージ容量をアップグレードします。

  必要な最小外部ストレージ容量は 8 GB ですが、16 GB 以上の外部ストレージ容量でデバイスをプロビジョニングすることをお勧めします。最小の外部ストレージ容量では、デバイスでソフトウェアイメージをアップグレードするときに、ファイルを手動でクリーンアップする必要がある場合があります。

- **ブートフラッシュ**：外部ストレージが装備されていないデバイスでは、Cisco ThousandEyes Enterprise Agent がブートフラッシュにインストールされます。Cisco ThousandEyes Enterprise Agent のインストールに必要な最小ブートフラッシュ容量は 8 GB です。デバイスに十分なブートフラッシュ容量がない場合は、最小要件を満たすようにストレージ容量をアップグレードします。

重要 ISR1100X-6G では、Cisco ThousandEyes Enterprise Agent がブートフラッシュにインストールされます。この特定のデバイスモデルの場合、エージェントのインストールに必要な最小ブートフラッシュ容量は 16 GB です。

  必要な最小ブートフラッシュ容量は 8 GB ですが、16 GB 以上のブートフラッシュ容量でデバイスをプロビジョニングすることをお勧めします。最小のブートフラッシュ容量では、デバイスのソフトウェアイメージをアップグレードするときに、ファイルを手動でクリーンアップする必要がある場合があります。

- **DRAM**：Cisco ThousandEyes Enterprise Agent のインストールに必要な最小 DRAM 容量は 8 GB です。Cisco ThousandEyes Enterprise Agent のインストールに必要な最小 DRAM 容量がデバイスにない場合は、最小要件を満たすように DRAM をアップグレードします。

- Cisco ThousandEyes Enterprise Agent は、デバイスに他のアプリケーションを実行するためのリソース（CPU、メモリ、およびストレージ）がある場合、他のアプリケーションとともに展開できます。使用可能なリソースが他のアプリケーションを実行するのに十分でない場合、IOX はエラーメッセージを生成し、他のアプリケーションを実行しません。

  Cisco ThousandEyes Enterprise Agent をホストするには、Cisco IOS XE SD-WAN デバイスに最低 8 GB の DRAM が必要です。同じデバイスで UTD や DRE などの追加のアプリケーションをホストする場合は、デバイスに少なくとも 16 GB の DRAM をプロビジョニングすることをお勧めします。

Cisco SD-WAN および Cisco ThousandEyes による可視性の強化の前提条件

- Cisco ThousandEyes Enterprise エージェントを展開する前に、Cisco ThousandEyes ポータルでアカウントを作成し、アカウントグループトークンを取得する必要があります。エージェントは、トークンを使用して Cisco ThousandEyes で自身を認証し、正しい Cisco ThousandEyes アカウントにチェックインします。

  アカウントグループトークンの取得については、Cisco ThousandEyes Documentation ポータルで「*Where Can I Get the Account Group Token?*」を参照してください。

- Cisco ThousandEyes Enterprise エージェントでは、Cisco ThousandEyes ポータルを検出して登録するために、DNS 名前解決と HTTP/HTTPS 接続が必要です。適切なファイアウォールルール、NAT 設定、アップストリーム ルーティング、およびその他の関連設定を構成して、エージェントを展開する前に、この接続が存在することを確認してください。

  必要なファイアウォール設定の詳細については、Cisco ThousandEyes Documentation ポータルの「*Firewall Configuration for Enterprise Agents*」を参照してください。

Cisco SD-WAN および Cisco ThousandEyes による可視性の強化の制約事項

- Cisco ThousandEyes Enterprise エージェントプローブは、仮想ポート グループ インターフェイスから発信され、AppRoute データポリシーの影響を受けません。
- Cisco ThousandEyes Enterprise エージェントは、Cisco IOS XE SD-WAN デバイス上のコンテナアプリケーションとしてネイティブにホストされており、ページロードテストやトランザクションテストなどのブラウザベースのアプリケーションテストをサポートしていません。

Cisco SD-WAN および Cisco ThousandEyes による可視性の強化に関する情報

Cisco ThousandEyes は、ビジネスに影響を与えるネットワークとサービス全体のエンドツーエンドのビューを提供する SaaS アプリケーションです。内部、外部、キャリアネットワーク、およびインターネット全体のネットワーク トラフィック パスをリアルタイムでモニターして、ネットワーク パフォーマンス データを提供します。Cisco ThousandEyes は、WAN とクラウドに関するインテリジェントな洞察を提供し、アプリケーション配信とエンドユーザーエクスペリエンスを最適化するのに役立ちます。

Cisco IOS XE リリース 17.6.1 以降、Cisco ThousandEyes Enterprise エージェントを Cisco IOS XE SD-WAN デバイスに展開および設定して、WAN トラフィックの広範なモニタリングを有効にして、Cisco SD-WAN ファブリック内外での可視性を向上させることができます。Cisco ThousandEyes Enterprise エージェントは、IOX Docker アプリケーション ホスティング機能を使用して、Docker タイプのコンテナアプリケーションとして Cisco IOS XE SD-WAN デバイス上で実行される組み込みの Docker ベースのアプリケーションです。

Cisco ThousandEyes の詳細、および Cisco ThousandEyes ポータルでのテストの設定と結果の表示については、Cisco ThousandEyes のスタートアップガイドのドキュメントを参照してください。

Cisco IOS XE SD-WAN デバイスでの Cisco ThousandEyes Enterprise Agent の設定

Cisco ThousandEyes Enterprise Agent ソフトウェアの Cisco vManage へのアップロード

1. 「Cisco ThousandEyes Agent Settings」ページから Cisco ThousandEyes Enterprise エージェントソフトウェアの最新バージョンをダウンロードします。
2. [Cisco vManage] メニューから、**[Maintenance]** > **[Software Repository]**を選択します。
3. [Virtual Images] をクリックします。
4. [Upload Virtual Image] をクリックし、[vManage] をクリックします。
5. [Upload VNF's Package to vManage] ダイアログボックスで、ダウンロードした Cisco ThousandEyes Enterprise エージェント ソフトウェア ファイルの場所を参照し、ファイルを選択します。

   または、Cisco ThousandEyes Enterprise エージェント ソフトウェア ファイルをドラッグアンドドロップします。
6. ファイルの説明を入力します。
7. （オプション）必要なタグを追加します。
8. [Upload] をクリックします。

トランスポート VPN（VPN 0）での Cisco ThousandEyes Enterprise Agent のプロビジョニング

VPN 0 に Cisco ThousandEyes Enterprise エージェントをプロビジョニングして、Cisco SD-WAN ファブリックを超えたアンダーレイネットワークのパフォーマンスをより詳細に把握できま

す。VPN 0 にプロビジョニングされている場合、Cisco ThousandEyes Enterprise エージェントは Cisco SD-WAN ファブリックをプローブしません。

前提条件

- Cisco ThousandEyes Enterprise エージェントが Cisco ThousandEyes アプリケーションを検出して接続できるように、適切な DNS および NAT 設定が存在することを確認します。
- Cisco ThousandEyes Enterprise エージェントソフトウェアを Cisco vManage にアップロードします。

（注） Cisco ThousandEyes Enterprise エージェントソフトウェアの複数のバージョンを Cisco vManage ソフトウェアリポジトリにアップロードした場合、エージェントのプロビジョニング中に、Cisco vManage は最新バージョンのエージェントソフトウェアをインストールしてアクティブ化します。

手順

1. Cisco ThousandEyes Enterprise エージェントの機能テンプレートを作成します。
    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、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. このテンプレートを適用するサポートされているデバイスを選択します。
    4. [Other Templates] セクションで、[ThousandEyes Agent] をクリックします。
    5. [Template Name]：テンプレートの名前を入力します。テンプレートの名前が一意であることを確認してください。
    6. [Description]：テンプレートの説明を入力します。
    7. [BASIC CONFIGURATION] セクションで、Cisco ThousandEyes の [Account Group Token] を入力します。
    8. [ADVANCED] セクションで、希望する [Name Server] の IP アドレスを入力します。

（注） Cisco vManage リリース 20.7.1 および Cisco IOS XE リリース 17.7.1a 以降、この手順はオプションです。

9. **[Save]** をクリックします。

2. ThousandEyes Agent 機能テンプレートをデバイステンプレートに添付します。
   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. ターゲットデバイスのデバイステンプレートを見つけます。
   4. このテンプレートで、[…] をクリックし、[Edit] をクリックします。
   5. [Additional Templates] をクリックします。
   6. [Additional Templates] セクションで、前に作成した [ThousandEyes Agent] 機能テンプレートを選択します。
   7. [更新（Update）] をクリックします。
   8. 必要な変数があれば更新し、[Next] をクリックします。
   9. 構成を確認し、[Configure Devices] をクリックします。

3. Cisco ThousandEyes Enterprise エージェントを展開するデバイスごとに、ステップ 2 を繰り返します。

Cisco ThousandEyes Enterprise エージェントは、選択したデバイスに展開されます。エージェントは、クラウドベースの Cisco ThousandEyes アプリケーションに登録して安全な通信を確立し、必要な更新と設定を受け取ります。Cisco ThousandEyes ポータルでさまざまなテストを設定し、結果のネットワークおよびアプリケーション テレメトリ データを確認できます。

サービス VPN での Cisco ThousandEyes Enterprise Agent のプロビジョニング

サービス VPN に Cisco ThousandEyes Enterprise エージェントをプロビジョニングして、Cisco SD-WAN オーバーレイおよびアンダーレイネットワークのパフォーマンスをより詳細に把握できます。

前提条件

- Cisco ThousandEyes Enterprise エージェントが Cisco ThousandEyes アプリケーションを検出して接続できるように、適切な DNS および NAT 設定が存在することを確認します。
- Cisco ThousandEyes Enterprise エージェント ソフトウェアを Cisco vManage にアップロードします。

（注） Cisco ThousandEyes Enterprise エージェントソフトウェアの複数のバージョンを Cisco vManage ソフトウェアリポジトリにアップロードした場合、エージェントのプロビジョニング中に、Cisco vManage は最新バージョンのエージェントソフトウェアをインストールしてアクティブ化します。

手順

1. Cisco ThousandEyes Enterprise エージェントの機能テンプレートを作成します。
   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、[Add Template] をクリックして適切なデバイスモデルを選択します。

（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. このテンプレートを適用するサポートされているデバイスを選択します。
   4. [Other Templates] セクションで、[ThousandEyes Agent] をクリックします。
   5. [Template Name]：テンプレートの名前を入力します。テンプレートの名前が一意であることを確認してください。
   6. [Description]：テンプレートの説明を入力します。
   7. [BASIC CONFIGURATION] セクションで、次のフィールドを設定します。

Account Group Token	Cisco ThousandEyes アカウントグループトークンを入力します。
VPN	1. VPN 設定を [Global] または [Device Specific] 設定として設定します。 2. Cisco ThousandEyes Enterprise エージェントをプロビジョニングするサービス VPN の ID を入力します。

Agent IP Address	Cisco ThousandEyes Enterprise エージェントの IP アドレスを入力します。 このIPアドレスは、ファブリック内で一意である必要があり、他のブランチエージェントの IP アドレスと重複してはなりません。
Agent Default Gateway	デフォルトゲートウェイのアドレスを入力します。この IP アドレスは、ルータの仮想ポートグループに割り当てられます。

ヒント　エージェントネットワークのサービスサブネットを作成して割り当てることができます。各 Cisco IOS XE SD-WAN デバイスで Cisco ThousandEyes Enterprise エージェントをプロビジョニングするには、2 つの使用可能な IP アドレスが必要です。IP アドレスの 1 つをエージェントに割り当て、もう 1 つの IP アドレスをルータ仮想ポートグループに割り当てる必要があります。

8. [ADVANCED] セクションで、次の手順を実行します。

ネーム サーバー	（Cisco vManage リリース 20.7.1 および Cisco IOS XE リリース 17.7.1a のオプションパラメータ） 優先 DNS サーバーの IP アドレスを入力します。 このサーバーは、Cisco SD-WAN ファブリックの内部または外部に存在できますが、サービス VPN から到達可能である必要があります。
ホストネーム	（オプション）Cisco ThousandEyes ポータルに登録するときにエージェントが使用する必要があるホスト名を入力します。デフォルトでは、エージェントは Cisco IOS XE SD-WAN デバイスのホスト名を使用します。

Web Proxy Type	（オプション）Cisco ThousandEyes Enterprise エージェントが外部アクセスにプロキシサーバーを使用する必要がある場合は、プロキシタイプとして次のいずれかを選択します。 • **[Static]** • **PAC** スタティックプロキシの設定： • [Proxy Host]：設定を [Global] 設定として設定し、プロキシサーバーのホスト名を入力します。 • [Proxy Port]：設定を [Global] 設定として設定し、プロキシサーバーのポート番号を入力します。 PAC の設定： • [PAC URL]：設定を [Global] 設定として設定し、プロキシ自動構成（PAC）ファイルの URL を入力します。

9. **[Save]** をクリックします。

2. ThousandEyes Agent 機能テンプレートをデバイステンプレートに添付します。
   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. ターゲットデバイスのデバイステンプレートを見つけます。
   4. このテンプレートの場合は、[…] をクリックし、[Edit] をクリックします。
   5. [Additional Templates] をクリックします。
   6. [Additional Templates] セクションで、前に作成した [ThousandEyes Agent] 機能テンプレートを選択します。
   7. [更新（Update）] をクリックします。
   8. 必要な変数があれば更新し、[Next] をクリックします。
   9. 構成を確認し、[Configure Devices] をクリックします。

3. Cisco ThousandEyes Enterprise エージェントを展開するデバイスごとに、ステップ 2 を繰り返します。

Cisco ThousandEyes Enterprise エージェントは、選択したデバイスに展開されます。エージェントは、クラウドベースの Cisco ThousandEyes アプリケーションに登録して安全な通信を確立し、必要な更新と設定を受け取ります。Cisco ThousandEyes ポータルでさまざまなテストを設定し、結果のネットワークおよびアプリケーション テレメトリ データを確認できます。
https://app.thousandeyes.com/

CLI を使用したサービス VPN での Cisco ThousandEyes Enterprise Agent のプロビジョニング

このセクションでは、デバイス CLI テンプレートまたはアドオン CLI テンプレートを使用して Cisco IOS XE SD-WAN デバイスに Cisco ThousandEyes Enterprise Agent をプロビジョニングするコマンドシーケンスの例を示します。

前提条件

- Cisco ThousandEyes Enterprise エージェントが Cisco ThousandEyes アプリケーションを検出して接続できるように、適切な DNS および NAT 設定が存在することを確認します。
- Cisco ThousandEyes Enterprise エージェント ソフトウェアを Cisco vManage にアップロードします。

（注） Cisco ThousandEyes Enterprise エージェントソフトウェアの複数のバージョンを Cisco vManage ソフトウェアリポジトリにアップロードした場合、エージェントのプロビジョニング中に、Cisco vManage は最新バージョンのエージェントソフトウェアをインストールしてアクティブ化します。

このセクションでは、サービス VPN で Cisco ThousandEyes Enterprise Agent をプロビジョニングする CLI 設定の例を示します。

1. デバイスで IOX を有効にします。

```
iox
```

2. 仮想ポートグループを設定します。仮想ポートグループは、Cisco ThousandEyes Enterprise Agent のゲートウェイとして機能します。

```
interface VirtualPortGroup4
 vrf forwarding 100
  ip address 192.168.61.1 255.255.255.252
```

3. ThousandEyes Enterprise Agent のアプリケーションホスティング パラメータを設定します。

```
app-hosting appid te
app-vnic gateway0 virtualportgroup 4 guest-interface 0
 guest-ipaddress 192.168.61.2 netmask 255.255.255.252
app-default-gateway 192.168.61.1 guest-interface 0
app-resource docker
 prepend-pkg-opts
 run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=z0kemf"
```

```
 run-opts 2 "--hostname ISR4461TE"
 run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e
TEAGENT_PROXY_LOCATION=proxy-exmaple.com:80"
name-server0  192.168.168.183
start
```

（注）
- プロキシ設定は、Cisco ThousandEyes エージェントがプロキシなしでインターネットにアクセスできない場合にのみ使用できます。また、ホスト名はオプションです。インストール時にホスト名を指定しない場合、デバイスのホスト名が Cisco ThousandEyes エージェントのホスト名として使用されます。デバイスのホスト名が Cisco ThousandEyes ポータルに表示されます。Cisco IOS XE リリース 17.7.1a 以降では、DNS ネームサーバー情報はオプションです。
- Cisco ThousandEyes Agent がプライベート IP アドレスを使用する場合は、NAT 経由でデバイスへの接続を確立します。

Cisco ThousandEyes Enterprise Agent ソフトウェアのアップグレード

（注） 外部ストレージを持たない Cisco IOS XE SD-WAN デバイスでは、Cisco ThousandEyes Enterprise Agent ソフトウェアをアップグレードできません。このようなデバイスでは、エージェントのインストールと起動にブートフラッシュが使用されています。ブートフラッシュには、エージェントソフトウェアのアップグレードをサポートするストレージ容量がありません。エージェントソフトウェアをアップグレードする代わりに、既存のソフトウェアをアンインストールして、新しいバージョンのソフトウェアをプロビジョニングできます。

1. 新しいバージョンの Cisco ThousandEyes Enterprise Agent ソフトウェアをダウンロードし、ソフトウェアを Cisco vManage にアップロードします。「Cisco ThousandEyes Enterprise Agent ソフトウェアの Cisco vManage へのアップロード」を参照してください。
2. Cisco vManage のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
3. Cisco ThousandEyes Enterprise Agent ソフトウェアをアップグレードする Cisco IOS XE SD-WAN デバイスを選択します。
4. [Upgrade Virtual Image] をクリックします。
5. [Virtual Image Upgrade] ダイアログボックスで、ドロップダウンリストから新しいバージョンの Cisco ThousandEyes Enterprise Agent ソフトウェアを選択します。**[Upgrade]** をクリックします。
6. **[Maintenance]** > **[Software Upgrade]** ページで、Cisco ThousandEyes Enterprise Agent ソフトウェアをアップグレードした Cisco IOS XE SD-WAN デバイスを選択します。
7. [Activate Virtual Image] をクリックします。

Cisco ThousandEyes Enterprise Agent ソフトウェアのアンインストール

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。

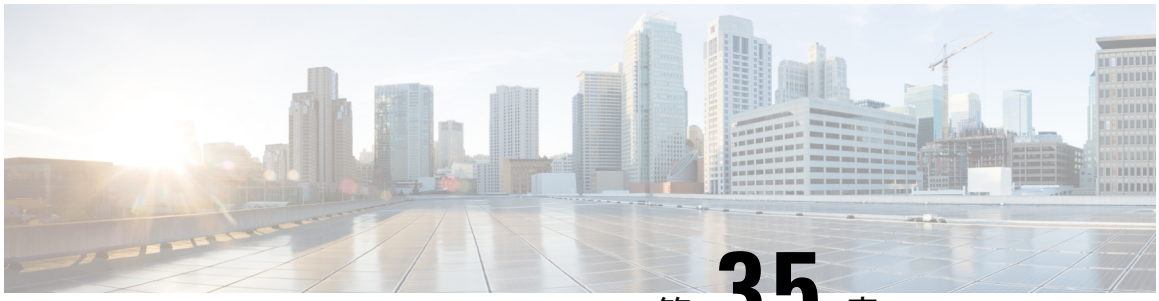
3. Cisco ThousandEyes エージェントソフトウェアを削除する必要があるデバイスのデバイステンプレートを見つけます。
4. このテンプレートで、[…] をクリックし、[Edit] をクリックします。
5. [Additional Templates] をクリックします。
6. [Additional Templates] セクションの [ThousandEyes Agent] で、ドロップダウンリストから [None] を選択します。
7. [更新（Update）] をクリックします。
8. 必要な変数があれば更新し、[Next] をクリックします。
9. 構成を確認し、[Configure Devices] をクリックします。

Cisco IOS XE SD-WAN デバイスでの Cisco ThousandEyes Enterprise Agent のトラブルシューティング

1. Cisco ThousandEyes Enterprise エージェントに接続します。

```
Device#app-hosting connect appid Appid session /bin/bash
```

2. エージェント設定を確認するには、次のCFGファイルを確認します。`/etc/te-agent.cfg`
3. エージェントログを表示するには、次のファイルを確認します。
`var/log/agent/te-agent.log`



第 35 章

付録：vManage How-To マニュアル

カスタムvManageアプリケーションサーバーロゴをロードする方法

Cisco vManage Web アプリケーションサーバーのロゴを変更し、新しいカスタムロゴをロードするには、**request nms application-server update-logo** コマンドを使用します。

ロゴ画像は、すべての Cisco vManage Web アプリケーションサーバー画面の左上隅にあります。広いブラウザ画面に表示される大きいバージョンと、画面サイズが狭いときに表示される小さいバージョンの2つのファイルを読み込むことができます。どちらのファイルもローカルデバイス上の PNG ファイルで、サイズが 1 MB 以下である必要があります。最適な解像度を得るには、大きいロゴの画像を 180 x 33 ピクセル、小さいロゴの画像を 30 x 33 ピクセルにすることをお勧めします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。