設定グループと機能プロファイル

表 *1*: 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 （3 ページ）
- 設定グループでサポートされるデバイス （5 ページ）
- 設定グループの前提条件 （5 ページ）
- 設定グループの制約事項 （6 ページ）
- 設定グループの使用例 （6 ページ）
- 設定グループワークフローの使用 （7 ページ）
- 設定グループへのデバイスの追加 （9 ページ）
- デバイスの展開 （13 ページ）
- 設定グループからのデバイスの削除 （14 ページ）
- 機能の管理 （14 ページ）

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

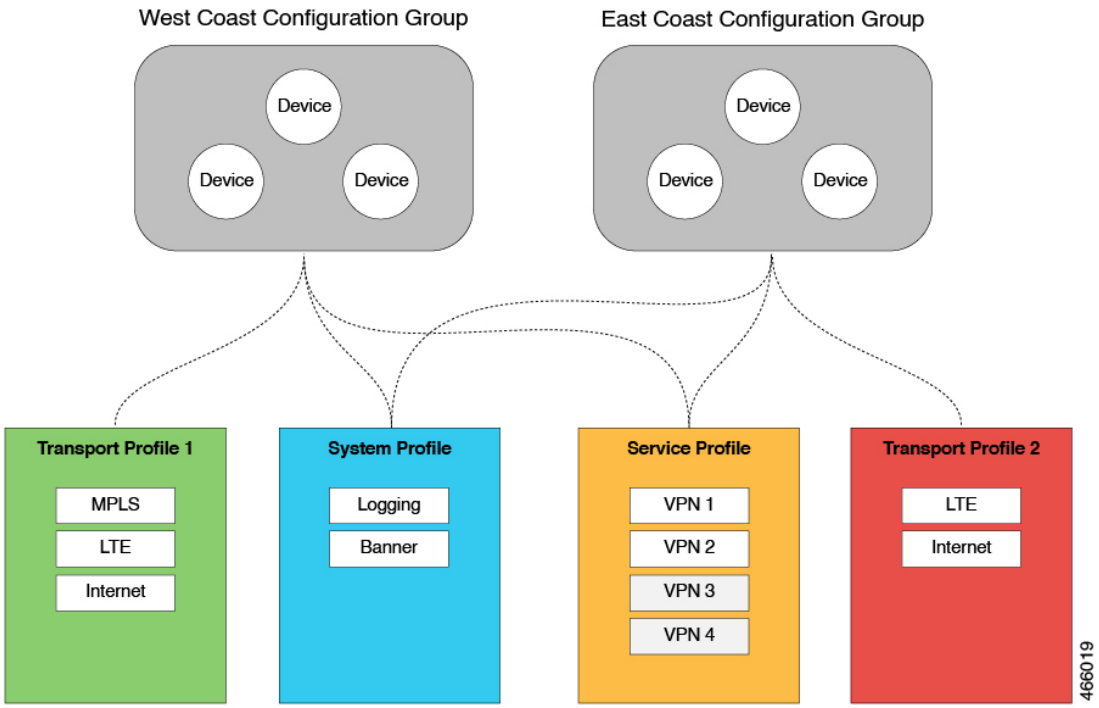
- デバイスは、設定グループまたはデバイステンプレートのいずれかに関連付けることができますが、両方に関連付けることはできません。
- デバイスは 1 つの設定グループにのみ追加できます。
- 設定グループに追加できるタグルールは 1 つだけです。

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 *2:* 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 *3:* 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 *4:* 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 *5:* 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 *6 :* 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 *7:* 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 *8 : 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 *9 :* 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 10 : 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。

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。