SD ルーティングデバイスの設定グループの使用

最終更新：2024 年 8 月 30 日

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

目 次

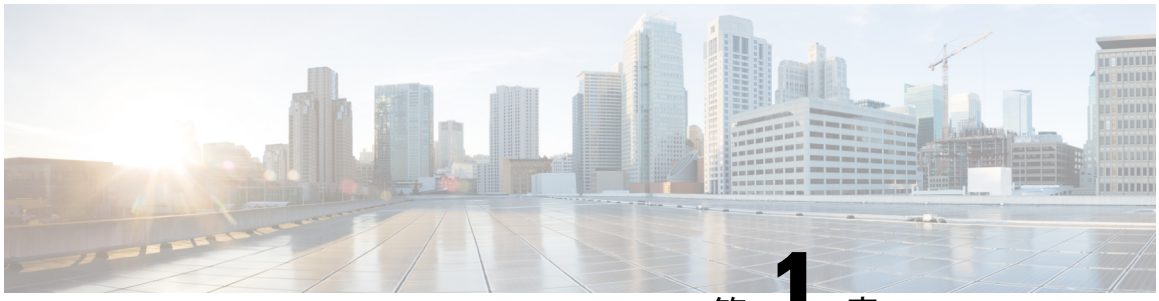
はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

ここに参照前文マップ

はじめに



第 1 章

はじめに

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する（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する）
- [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

設定グループの概要

設定グループ機能は、Cisco SD ルーティング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ルーティング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。

設定グループのワークフローの概要

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VRF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VRF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。

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。

Cisco SD ルーティングの [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 SD-WAN ルーティング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 SD ルーティングデバイスに対して、サイトレベルのトポロジが生成されます。
- 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。

設定グループの制約事項

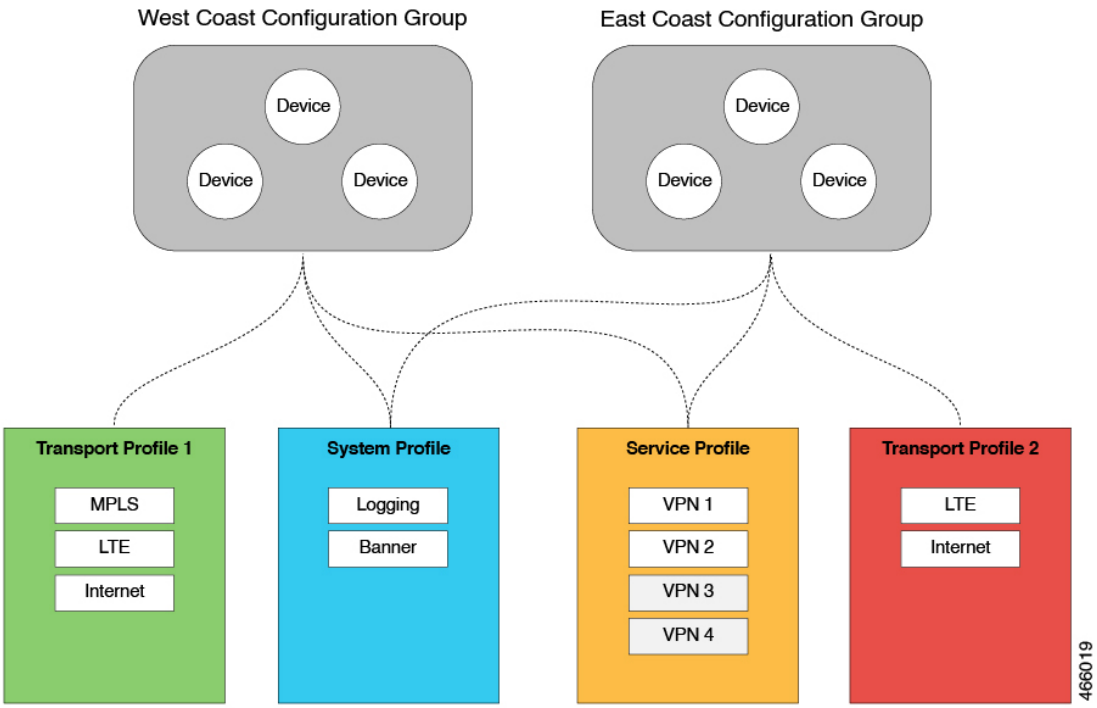
- デバイスは 1 つの設定グループにのみ追加できます。
- 設定グループに追加できるタグルールは 1 つだけです。

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

各機能プロファイルの詳細なRBACが展開されて指定されていることを確認します。ユーザーグループに設定された権限を使用して、Cisco SD-WAN Manager から必要な機能プロファイルにアクセスできることを確認し、Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Configuration Groups]**の順に選択します。

1. Cisco Catalyst SD-WAN Manager のメニューから、**[Administration]** > **[Manage Users]** > **[User Groups]**の順に選択します。

2. [Add a User Group] をクリックします。
3. [User Group Name] を入力します。
4. ユーザーグループに割り当てる機能に対して、[Read] または [Write] チェックボックスをオンにします。
5. [Save] をクリックします。

（注） 設定グループを使用してサービス、システム、およびトランザクション機能プロファイルを作成するには、各設定グループにアクセスするために必要な次の機能に対する読み取りおよび書き込み権限を指定する必要があります。

- **[Feature Profile]** > **[System]**
- **[Feature Profile]** > **[System]** > **[AAA]**
- **[Feature Profile]** > **[System]** > **[Banner]**
- **[Feature Profile]** > **[System]** > **[Logging]**
- **[Feature Profile]** > **[System]** > **[NTP]**
- **[Feature Profile]** > **[System]** > **[SNMP]**
- **[Feature Profile]** > **[Service]** > **[VRF]**
- **[Feature Profile]** > **[Service]** > **[DHCP]**
- **[Feature Profile]** > **[Transport]** > **[VRF]**

設定グループワークフローの作成の実行

Cisco SD-WAN Manager のメニューから、**[Workflows]** > **[Create Configuration Group]**を選択します。または、次の手順を実行します。

1. **[Workflows]** > **[Workflow Library]** を選択します。
2. [Workflow Library] ページの [Library] セクションで、[Create Configuration Group] をクリックします。

   または、Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a の Cisco SD-WAN Manager メニューから**[Configuration]** > **[Configuration Groups]**を選択し、[Add Configuration Group] をクリックします。
3. 進行中のワークフローを再開する：[In-progress] セクションで、[Create SD-Routing Configuration] をクリックします。

ワークフローにより、次のコンポーネントが作成されます。

- 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、ポリシー オブジェクト 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 SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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 SD-WAN のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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。
   - Rule Conditions：[Match All] または [Match Any] の条件のいずれかを選択します。

- **Device Attribute**：[Tags] を選択します。
- Condition：[Equal]、[Contains]、[Not contain]、[Not equal]、[Starts with]、[Ends with] 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。

   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 Cisco SD ルーティングに表示されます。

2. Cisco SD ルーティングのツールバーから [Task-list] アイコンをクリックします。

   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 Cisco SD ルーティングに表示されます。

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。次の例では、5 つの Cisco Catalyst 8000V デバイスにタグが追加されています。

   表 *1*: 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. 次のルール条件のいずれかを選択します。
   - Match All
   - Match Any

3. 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。
   - （サポートされている最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1）

     Starts with：この演算子は、指定された値で始まるデータをフィルタリングします。
   - （サポートされている最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1）

     Ends with：この演算子は、指定された値で終わるデータをフィルタリングします。

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

条件：Match Any

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

条件：Match Any

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

条件：Match Any

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

条件：Match Any

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。

ルールの例 5

条件：Match Any

演算子：STARTS with

指定タグ：CA

効果：指定した値で始まるタグを持つデバイスを照合します。

設定グループ：E

結果：デバイス C8K-0001、C8K-0002、C8K-0003、C8K-0004、および C8K-0005 が設定グループ E に追加されます。

ルールの例 6

条件：Match All

演算子：ENDS WITH

指定されたタグ：1

効果：指定した値で終わるタグを持つデバイスを照合します。

設定グループ：F

結果：デバイス C8K-0001、C8K-0002、および C8K-0003 が設定グループ F に追加されます。

デバイスの展開

機能のフィールドはデバイス固有としてマークできます。これはデバイス変数と呼ばれます。デバイスを追加して任意の機能に展開する際に、デバイス変数値を指定できます。

手動でのデバイスの展開

1. Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a の Cisco SD-Routing メニューから **[Configuration]** > **[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。

デバイスの展開

1. Cisco SD-WAN Manager のメニューから**[Workflows]** > **[Workflow Library]**の順に選択します。
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。

デバイス値の設定

[Change Device Values] ワークフローを使用すると、設定グループをデバイスに展開せずにデバイス変数値を指定できます。展開するための RBAC 権限がない場合は、[Change Device Values] ワークフローを使用してデバイス変数値を変更できます。

異なるモデルのデバイスを同じ設定グループに関連付けることができます。関連付けられているすべてのデバイスが、設定グループに設定されている各機能をサポートしているとは限りません。たとえば、Cisco Catalyst 8000v デバイスは ThousandEyes 機能をサポートしていません。設定グループをデバイスに展開すると、Cisco SD-WAN Manager はデバイスごとに、そのデバイスがサポートする機能のみを適用します。

はじめる前に

ロールベース アクセス コントロール（**[Administration]** > **[Manage Users]** > **[User Group]**）の権限によって、表示および更新できる変数が決まります。

デバイス値の設定

1. Cisco SD-WAN のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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、[Change Device Values] をクリックします。

   [Change Device Values] ワークフローが開始されます。
5. ワークフローの指示に従ってください。

   選択したデバイスが [Devices] テーブルにリストされます。
6. [Next] をクリックします。

   [Select Devices to Change Values] ページが表示されます。
7. デバイスを選択します。
8. [Next] をクリックします。

   [Add and Review Device Configuration] ページが表示されます。

9. 指示に従って、 [Device Configuration] の詳細を更新します。

   必要に応じて設定を変更するか、テーブルを編集してシステム IP やサイト ID を追加します。

10. [Save] をクリックします。

設定グループからのデバイスの削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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。

機能とサブ機能

次の手順は、設定グループ内にある機能プロファイルの機能とサブ機能の追加、編集、および削除に関連しています。

機能プロファイルへの機能の追加

はじめる前に

機能プロファイルに機能を追加するには、設定グループが必要です。

機能プロファイルへの機能の追加

1. Cisco SD-WAN メニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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. 機能プロファイルをクリックして開きます。
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。

（注） すでに追加されている機能はグレー表示されます。

6. [Name] フィールドに、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。

7. [Description] フィールドに機能の説明を入力します。

   説明は英数字とスペースのみを使用して、2048 文字以内で指定します。

8. 必要に応じてオプションを設定します。

   一部のパラメータには範囲のドロップダウンリストがあり、パラメータ値として [Global]、[Device Specific]、または [Default] を選択できます。以下に示す表の説明に従って、次のオプションのいずれかを選択します。

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すると、その値はすべてのデバイスに適用されます。 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。
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。 [Device Specific] を選択すると、フィールドにキーの値を入力できます。キーは、パラメータの識別に役立つ一意の文字列です。デフォルトのキー値を変更するには、フィールドに新しい文字列を入力します。 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。
デフォルト（チェックマークで示されます）	デフォルト設定を持つパラメータには、デフォルト値が表示されます。

9. [Save] をクリックします。

サブ機能の追加

はじめる前に

一部の機能には、サブ機能オプションが用意されています。

サブ機能の追加

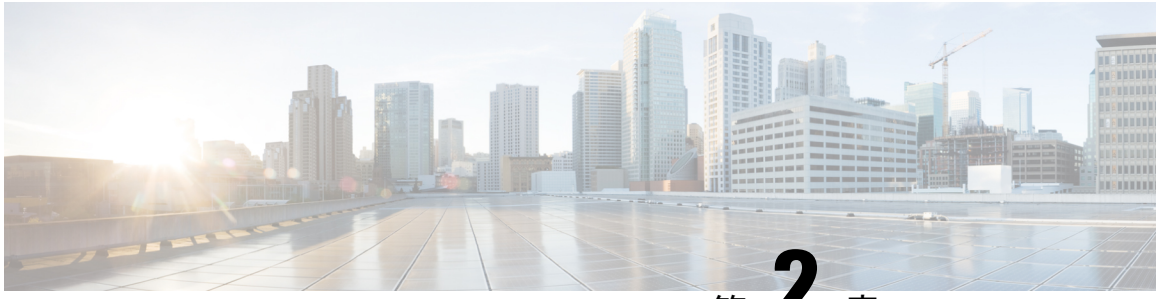
1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. 機能プロファイルをクリックして開きます。
4. 機能の横にある […] をクリックし、[Add Sub-Feature] を選択します。
5. ドロップダウンリストからサブ機能を選択します。
6. [Name] フィールドに、機能の名前を入力します。
7. [Description] フィールドに機能の説明を入力します。
8. 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 SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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. 機能プロファイルをクリックして開きます。
4. 機能の隣にある […] 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 SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]**の順に選択します。
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。



第 2 章

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、Cisco SD ルーティングデバイスにログインしているユーザーの認証、ユーザーに与える権限の決定、およびアクションのアカウンティングの実行をサポートします。

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。

Local

フィールド	説明
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。

フィールド	説明
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。
Privilege	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。
公開キーチェーンの追加	
SSH RSA Key	[ssh-rsa] を選択します。

RADIUS

フィールド	説明
Add Radius Server	
IP Address (v4 or v6)	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

フィールド	説明
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：3 秒
Timeout	要求を再送信する前に、デバイスが RADIUS 要求への応答を待機する秒数を入力します。 デフォルト：5 秒 範囲：1 ～ 1000
Key*	認証と暗号化のために、Cisco SD ルーティングデバイスから RADIUS サーバーに渡されるキーを入力します。
Key Type	[Protected Access Credential (PAC)] またはキータイプを選択します。

TACACS サーバー

フィールド	説明
Add TACACS Server	
IP Address (v4 or v6)	TACACS+ サーバーホストの IP アドレスを入力します。
Authentication 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 [second]	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 SD ルーティングデバイスから TACACS+ サーバーに渡されるキーを入力します。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
アカウンティングルールの追加	
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。
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。
Groups	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
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。
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。
認証ルールの追加	
Rule Id	認証ルール ID を入力します。
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。
Level	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。

フィールド	説明
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。
Group(s)	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。

802.1X

フィールド	説明
Authentication Param	認証パラメータを有効にします。
Accounting Param	アカウンティングパラメータを有効にします。

認証と承認の順序

フィールド	説明
Server Auth Order	[local] を選択します。

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。

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
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。
Login	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
Message of the Day	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。

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。

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。

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 Server	セキュア HTTPS サーバーを有効または無効にします。
FTP Passive	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 Proxy	プロキシ ARP を有効または無効にします。
RSH/RCP	デバイスでリモートシェル（RSH）とリモートコピー（rcp）を有効または無効にします。
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。
Link Layer Discovery Protocol (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。
HTTP Client Source Interface	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

フィールド	説明
NAT 64 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）
NAT 64 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）
NAT 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：3600 秒（1 時間）
NAT 64 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：300 秒（5 分）

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。
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。

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
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

フィールド	説明
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	
TLS Profile Name	TLS プロファイル名を入力します。
TLS Version	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。

フィールド	説明
Cipher Suite List	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	
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。
VRF	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

フィールド	説明
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、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
Severity	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。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。
IPv6 サーバーの追加	
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。

フィールド	説明
VRF	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、設定は無視されます。複数の syslog サーバーを設定する場合、送信元インターフェイスは syslog サーバーすべてで同じにする必要があります。
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 ネットワークで NTP 設定を行うのに役立ちます。

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。

サーバ

フィールド	説明
サーバの追加	
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。
VRF to reach NTP Server*	NTP サーバーに到達するために使用する VRF 名を入力します。32 文字以内の英数字で指定します
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 ルーティング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
認証キーの追加	
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。

Advanced

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。
Source	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。

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 SD ルーティングデバイスで SNMP 機能を設定するのに役立ちます。

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。

SNMP

表 2 : Advanced

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。
Contact Person	Cisco SD ルーティングデバイスの管理を担当するネットワーク管理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 Version

表 *3 :* 基本 *(Basic)*

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：ビューの追加	
Name	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 ルーティングデバイス 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。

フレキシブルポート速度

フレキシブルポート速度機能は、Cisco Catalyst 8500-12X4QC ルータにのみ適用されます。この機能を使用して、要件に基づいて 100GE、40GE、10GE、または 1GE として動作するようにインターフェイスを設定します。ポートタイプに対して行った変更は、設定グループをデバイスに適用した後にのみ有効になります。

フレキシブルポート速度機能を使用してポート設定を更新すると、一部のポートが有効になり、他のポートが無効になる場合があります。たとえば、デフォルトでは C8500-12X4QC はベイ 1 を 10GE モードで、ベイ 2 を 40GE モードで動作させます。ベイ 1 のモードは、10GE、40GE、または 100GE にできます。ベイ 1 を 100GE に設定すると、ベイ 0 のすべてのポートが無効になります。詳細については、Cisco Catalyst 8500-12X4QC デバイスガイドの「Bay Configuration」[英語] を参照してください。

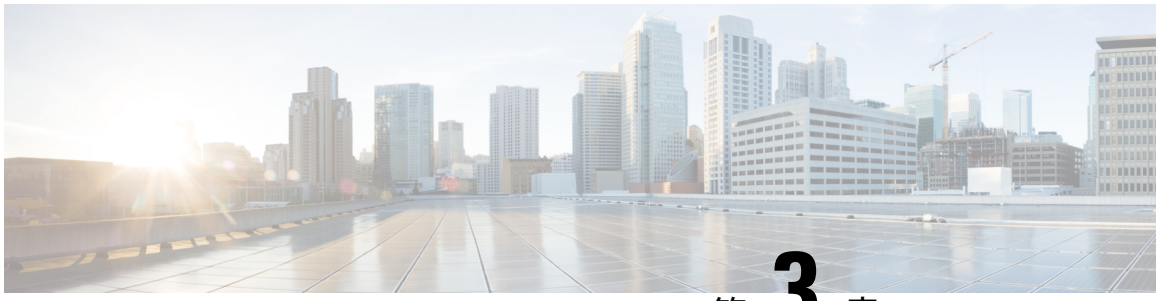
Cisco Catalyst 8500-12X4QC プラットフォームの各ベイのポートオプションの詳細については、『*Cisco Catalyst 8500 Series Edge Platforms Data Sheet*』の C8500-12X4QC 製品概要を参照してください。

一部のパラメータには範囲のドロップダウンリストがあり、パラメータ値として [Global]、[Device Specific]、または [Default] を選択できます。以下に示す表の説明に従って、次のオプションのいずれかを選択します。

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）	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。
デバイス固有（ホストのアイコン）	デバイス固有の値がパラメータに使用されます。 [Device Specific] を選択すると、フィールドにキーの値を入力できます。キーは、パラメータの識別に役立つ一意の文字列です。デフォルトのキー値を変更するには、フィールドに新しい文字列を入力します。 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。
デフォルト（チェックマークで示されます）	デフォルト設定を持つパラメータには、デフォルト値が表示されます。

基本設定

パラメータ名	説明
Port Type	次のポートの組み合わせのいずれかを選択します。 • 12 ports of 1/10GE + 3 ports of 40GE • 8 ports of 1/10GE + 4 ports of 40GE • 2 ports of 100GE • 12 ports of 1/10GE + 1 port of 100GE • 8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE • 3 ports of 40GE + 1 port of 100GE デフォルトは、[12 ports of 1/10GE + 3 ports of 40GE] です。



第 3 章

トランスポートおよび管理

トランスポートおよび管理プロファイルは、WAN レベルで VRF 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。

トランスポート VRF

トランスポート VPN 機能は、WAN で VRF 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。

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。

基本設定

フィールド	説明
VRF	VRF の ID 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 VRF 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 VRF 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 を追加	
Primary DNS Address (IPv6)	この VRF 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 VRF 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 14 個まで入力します。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、VRF 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、VRF 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。
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]：ネクストホップを null インターフェイスに設定するには、このオプションを有効にします。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。

ACL IPv4

次の表では、ACL IPv4 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
ACL Sequence Name	ACL シーケンスの名前を指定します。
Standard	標準 ACL は、IP パケットの送信元アドレスと ACL に設定されているアドレスを比較して、トラフィックを制御します。
Extended	拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
Add ACL Sequence	IP パケットに適用される許可および拒否条件を集めたものです。
Import ACL Sequence	デバイスへの ACL シーケンスのインポート。
Drop or Accept	一致が存在するかどうかに応じて実行するアクション。
ACL シーケンスの編集	
ACL Sequence Name	ACL シーケンスの名前を入力します。
Source Address	IP パケットの送信元アドレス
Source Address Host	単一の送信元アドレスホスト
Action Type	デフォルト値は accept です
Accept Actions	標準 IP アクセスリストによって許可または拒否されたパケットに関するメッセージを記録するログをドロップダウンリストから選択します。

[ACL Policy] ウィンドウで特定の ACL シーケンスを選択して、編集、削除、または追加できます。

（注） 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の設定グループから **ACL ポリシー** 機能を設定することもできます。

管理 VRF

次の表では、管理 VRF 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。

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。

ホストマッピング

フィールド	説明
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	
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、VRF 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、VRF 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。
Next Hop/Null 0	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。

オブジェクトトラッカー

トラッカー機能を使用すると、トラッカーエンドポイントのステータスを追跡できます。

次の表では、オブジェクト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。

基本設定

パラメータ名	説明
Name	トラッカーの名前。名前には128文字以内の英数字を使用できます。最大 8 つのトラッカーを設定できます。
Description	オブジェクトトラッカーの説明を入力します
Object Tracker ID	オブジェクトトラッカーの名前
Interface Name	グローバルまたはデバイス固有のトラッカーインターフェイス名を入力します（例：Gigabitethernet1、Gigabitethernet2）。
Interface Track Type	トランスポート インターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲：100 ～ 1000 ミリ秒。デフォルト：300 ミリ秒。次のオプションがあります。 • Line-protocol • Ip-routing • Ipv6-routing
Route IP	ネットワークのルート IP プレフィックス
Route IP Mask	ネットワークのサブネットマスク
VRF Name	ルート到達可能性を追跡するためのベースとして使用される VRF 名
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのUPステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのDownステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

オブジェクト トラッカー グループ

この機能を使用して、オブジェクト トラッカー グループを設定します。正確なトラッキングのため、オブジェクト トラッカー グループを作成する前に、少なくとも 2 つのオブジェクト トラッカーを追加してください。

基本設定

パラメータ名	説明
Object tracker ID	オブジェクト トラッカー グループの ID を入力します。 範囲：1 ～ 1000
Object tracker	ドロップダウンリストから、以前に作成したオブジェクトトラッカーを 2 つ以上選択します。
Reachable	次の値のいずれかを選択します。 • Either：トラッカーグループの関連付けられたトラッカーのいずれかでルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。 • Both：トラッカーグループの関連付けられたトラッカーの両方でルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの UP ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの Down ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

ルート ポリシー

特定のパケットを明らかに最短のパス以外の特定のパス経由でルーティングする必要がある場合は、この機能を使用してポリシーベースルーティングを設定します。

次の表では、ルートポリシ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
Routing Sequence Name	ルーティングシーケンスの名前を指定します。
Protocol	インターネットプロトコルを指定します。オプションは、[IPv4]、[IPv6]、またはその両方です。

フィールド	説明
Condition	ルーティング条件を指定します。次のオプションがあります。 • アドレス • AS パスリスト • コミュニティ リスト • 拡張コミュニティリスト • BGP ローカル プリファレンス • Metric • Next Hop • インターフェイス • OSPF タグ
Action Type	アクションタイプを指定します。オプションは、[Accept] または [Reject] です。
Accept Condition	受け入れ条件タイプを指定します。次のオプションがあります。 • AS パス • コミュニティ • ローカルプリファレンス • Metric • Metric Type • Next Hop • 発信元 • OSPF タグ • 重量

VRF サービスプロファイル

DNS

次の表では、管理 VRF 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
VRF Name	VRF の名前を入力します。
RD	VRF のルート識別子を指定します。
DNS	
IP Address	この VRF のプライマリ DNS サーバーの IPv4 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 14 個まで入力します。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、VRF 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、VRF 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。
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。
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。

イーサネット インターフェイス

この機能は、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。

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 VRF を選択します。
Associated VRF	VRF を選択します。

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。
Control Connection	トンネルで制御接続を有効にするには、[on] を選択します。
Bind Interface	ループバックインターフェイスにバインドする物理インターフェイスの名前を入力します。
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 Settings	IPv4 VRF 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
IPv4 Settings	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。 の「Configuring RAID Levels」の章を参照してください。
Subnet Mask	サブネットマスクを入力します。

フィールド	説明
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 Settings	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。

BFD

フィールド	説明
Enable BFD	リンク障害を検出するには、このオプションを有効にします

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。

ACL

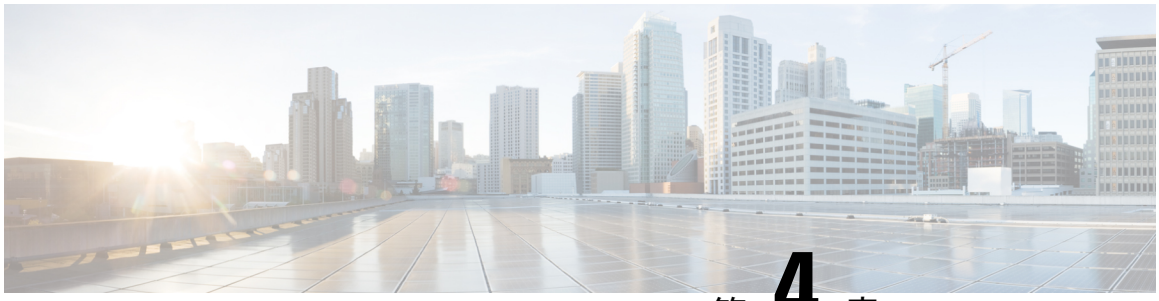
フィールド	説明
ACL IPv4 Ingress	インターフェイスで受信されるパケットに対して使用する IPv4 アクセスリストの名前を指定します。
ACL IPv4 Egress	インターフェイスから送信されるパケットに対して使用する IPv4 アクセスリストの名前を指定します。
ACL IPv6 Ingress	インターフェイスで受信されるパケットに対して使用する IPv6 アクセスリストの名前を指定します。
ACL IPv6 Egress	インターフェイスから送信されるパケットに対して使用する IPv6 アクセスリストの名前を指定します。

Advanced

フィールド	説明
Duplex	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
Interface 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

フィールド	説明
Speed	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
Autonegotiate	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。
Media Type	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。
Load Interval	インターフェイス負荷計算の間隔値を入力します。

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。
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。



第 4 章

ACL IPv4

次の表では、ACL IPv4 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
ACL Sequence Name	ACL シーケンスの名前を指定します。
Standard	標準 ACL は、IP パケットの送信元アドレスと ACL に設定されているアドレスを比較して、トラフィックを制御します。
Extended	拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
Add ACL Sequence	IP パケットに適用される許可および拒否条件を集めたものです。
Import ACL Sequence	デバイスへの ACL シーケンスのインポート。
Drop or Accept	一致が存在するかどうかに応じて実行するアクション。
ACL シーケンスの編集	
ACL Sequence Name	ACL シーケンスの名前を入力します。
Source Address	IP パケットの送信元アドレス
Source Address Host	単一の送信元アドレスホスト
Action Type	デフォルト値は accept です
Accept Actions	標準 IP アクセスリストによって許可または拒否されたパケットに関するメッセージを記録するログをドロップダウンリストから選択します。

[ACL Policy] ウィンドウで特定の ACL シーケンスを選択して、編集、削除、または追加できます。

（注） 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の設定グループから **ACL ポリシー** 機能を設定することもできます。

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。

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。
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	

フィールド	説明
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
Interface 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
Domain Name	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。
Default Gateway	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 Servers	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

オブジェクトトラッカー

トラッカー機能を使用すると、トラッカーエンドポイントのステータスを追跡できます。

次の表では、オブジェクト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。

基本設定

パラメータ名	説明
Name	トラッカーの名前。名前には128文字以内の英数字を使用できます。最大8つのトラッカーを設定できます。
Description	オブジェクトトラッカーの説明を入力します
Object Tracker ID	オブジェクトトラッカーの名前
Interface Name	グローバルまたはデバイス固有のトラッカーインターフェイス名を入力します（例：Gigabitethernet1、Gigabitethernet2）。
Interface Track Type	トランスポート インターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲：100 ～ 1000 ミリ秒。デフォルト：300 ミリ秒。次のオプションがあります。 • Line-protocol • Ip-routing • Ipv6-routing
Route IP	ネットワークのルート IP プレフィックス
Route IP Mask	ネットワークのサブネットマスク
VRF Name	ルート到達可能性を追跡するためのベースとして使用される VRF 名
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのUPステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストのDownステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

オブジェクト トラッカー グループ

この機能を使用して、オブジェクト トラッカー グループを設定します。正確なトラッキングのため、オブジェクト トラッカー グループを作成する前に、少なくとも 2 つのオブジェクト トラッカーを追加してください。

基本設定

パラメータ名	説明
Object tracker ID	オブジェクト トラッカー グループの ID を入力します。 範囲：1 ～ 1000
Object tracker	ドロップダウンリストから、以前に作成したオブジェクトトラッカーを 2 つ以上選択します。
Reachable	次の値のいずれかを選択します。 • Either：トラッカーグループの関連付けられたトラッカーのいずれかでルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。 • Both：トラッカーグループの関連付けられたトラッカーの両方でルートがアクティブであると報告された場合に、トランスポート インターフェイスのステータスがアクティブと報告されるようにします。
Delay Up (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの UP ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。
Delay Down (Seconds)	追跡対象オブジェクトまたはオブジェクトのリストの Down ステータスが通信されるまでの遅延を 0 ～ 180 秒の範囲で設定します。

ルート ポリシー

特定のパケットを明らかに最短のパス以外の特定のパス経由でルーティングする必要がある場合は、この機能を使用してポリシーベースルーティングを設定します。

次の表では、ルートポリシ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
Routing Sequence Name	ルーティングシーケンスの名前を指定します。
Protocol	インターネットプロトコルを指定します。オプションは、[IPv4]、[IPv6]、またはその両方です。

フィールド	説明
Condition	ルーティング条件を指定します。次のオプションがあります。 • アドレス • AS パスリスト • コミュニティ リスト • 拡張コミュニティリスト • BGP ローカル プリファレンス • Metric • Next Hop • インターフェイス • OSPF タグ
Action Type	アクションタイプを指定します。オプションは、[Accept] または [Reject] です。
Accept Condition	受け入れ条件タイプを指定します。次のオプションがあります。 • AS パス • コミュニティ • ローカルプリファレンス • Metric • Metric Type • Next Hop • 発信元 • OSPF タグ • 重量

VRF サービスプロファイル

DNS

次の表では、管理 VRF 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
VRF Name	VRF の名前を入力します。
RD	VRF のルート識別子を指定します。
DNS	
IP Address	この VRF のプライマリ DNS サーバーの IPv4 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 14 個まで入力します。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、VRF 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。

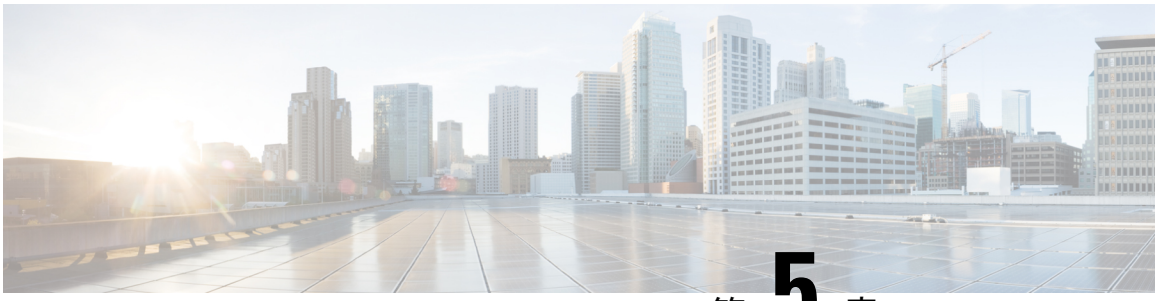
フィールド	説明
Gateway*	次のいずれかのオプションを選択して、ネクストホップがスタティックルートに到達するように設定します。 • [nextHop]：このオプションを選択して [Add Next Hop] をクリックすると、次のフィールドが表示されます。 • [Address]：ネクストホップ IPv4 アドレスを入力します。 • [Administrative distance]：ルートのアドミニストレーティブ ディスタンスを入力します。 • **[dhcp]** • [null0]：このオプションを選択すると、次のフィールドが表示されます。 • [Administrative distance]：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、VRF 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。
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。
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。

IPv4/IPv6スタティックルートサービス

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。
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
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。 • [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。



第 5 章

ポリシー オブジェクト プロファイル

ポリシーオブジェクト機能プロファイルを使用すると、ポリシー構成をデバイスにアタッチできます。

次の表に、ポリシープロファイルを構成するためのオプションを示します。

表 *4:*

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。説明では、 文字とスペースを使用できます。

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。