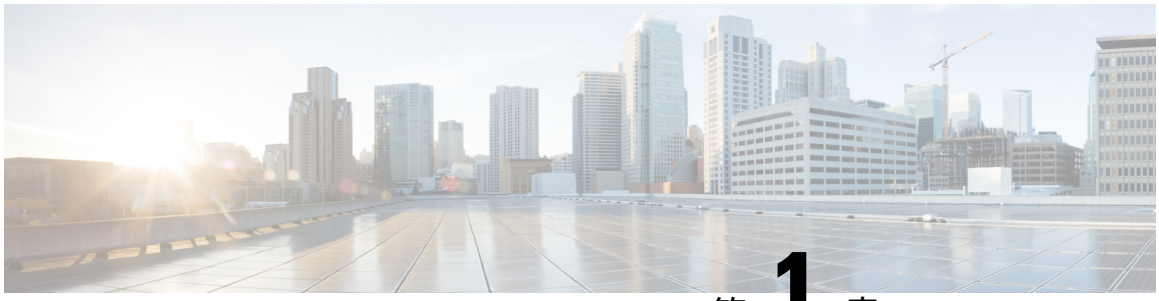
Cisco Catalyst SD-WAN ポータル コンフィギュレーション ガイド

最終更新：2025 年 6 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

最初にお読みください

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

参考資料

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations [英語]
- Cisco Catalyst SD-WAN Device Compatibility [英語]

ユーザーマニュアル

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17 [英語]

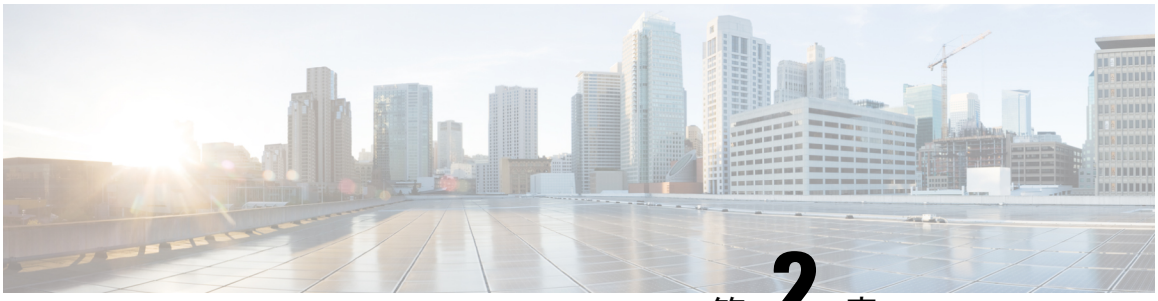
通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリケーション、製品、ソリューション、サービスをお求めの場合は、Cisco DevNet にアクセスしてください。

- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Tool にアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルマニュアルに関するフィードバックを提供するには、それぞれのオンラインマニュアルの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco Catalyst SD-WAN ポータル 機能の履歴

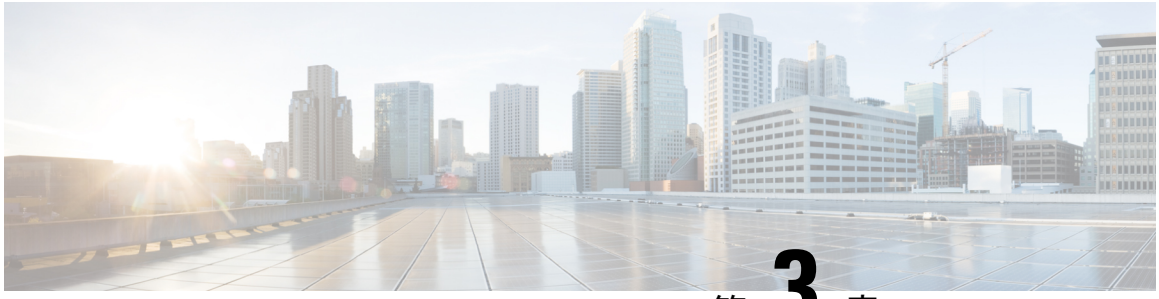
Cisco Catalyst SD-WAN ポータル 機能の履歴

表 *1*：機能の履歴

リリース日	機能名	説明
2025 年 4 月	Cisco Catalyst SD-WAN ポータルのロード時間の改善	Cisco Catalyst SD-WAN ポータル のロード時間が大幅に改善されました。
2025 年 4 月	スナップショットの保持の変更	ゴールデンスナップショットの保持期間が 180 日から 90 日に変更されました。オンデマンドスナップショットの保持期間が 90 日から 10 日に変更されました。 自動的に作成される定期的なスナップショットの保持数が 10 から 7 に変更されました。 スナップショットは、プライマリリージョンでのみ保持されます。

Cisco Catalyst SD-WAN ポータル 機能の履歴

リリース日	機能名	説明
2025 年 3 月	設定変換ツール	Cisco Catalyst SD-WAN ポータル から入手できる設定変換ツールを使用すると、デバイステンプレートを設定グループに変換したり、従来から設定されていたポリシーをポリシーグループに変換したりできます。ポリシー変換は、このリリースではベータレベルで機能すると見なされ、ベストエフォート変換を実行します。 設定を設定グループに変換すると、デバイスに依存しない新たな設定モデルの利点をすべて活かすことができます。
2025 年 2 月	追加のネットワーク コンプライアンス認定のサポート	Cisco Catalyst SD-WAN ソリューションは、SOC2 Type2、ISO 27001、ISO 27701、ISO 27017、ISO 27018、C5、ENS のネットワークコンプライアンス認定をサポートしています。 これらのコンプライアンス認定は、すべての長期リリースでサポートされます。
2024 年 10 月	ウェブフック通知サポート	Cisco SD-WAN ファブリックのネットワークイベントに基づく通知の送信をサポート。
2024 年 8 月	サポートチケットでの任意の電子メールアカウントの使用	**[Dashboard]** > **[Oerlays]** > **[Details]**ページで、Cisco SD-WAN ファブリックのサポートチケットを開くことができます。サポートチケットを開く際、連絡先情報に任意の電子メールアドレスを指定できます。
2024 年 8 月	ファブリックの詳細ページには、シスコのサポートケースの情報が表示されます	Cisco SD-WAN ポータルでは、**[Fabric Details]** ページの **[Service Requests]** セクションに、ファブリックに関連するシスコのサポートケースが表示されます。



第 3 章

Cisco Catalyst SD-WAN ポータル

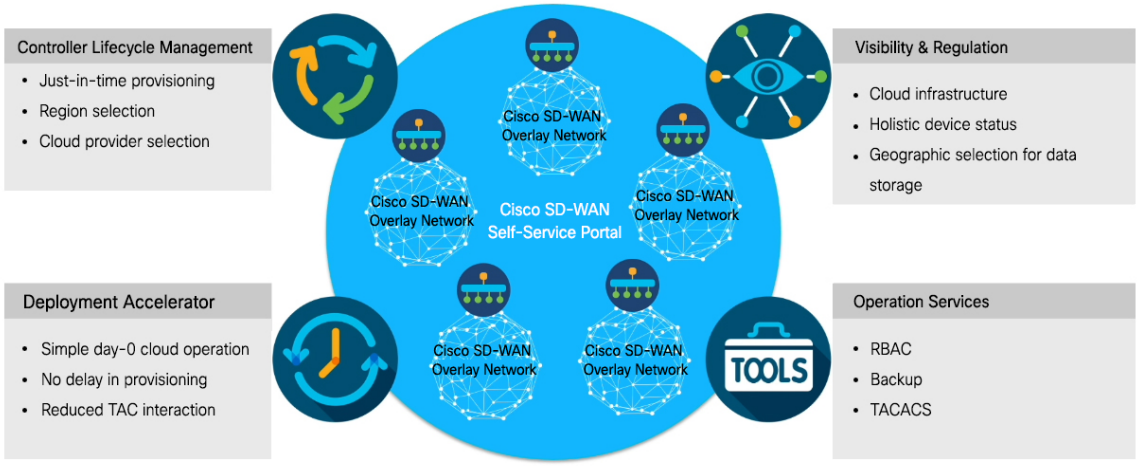
Cisco Catalyst SD-WAN ポータル の概要

Cisco Catalyst SD-WAN ポータル は、Cisco Catalyst SD-WAN に適したクラウド インフラストラクチャ自動化ツールであり、パブリック クラウド プロバイダーで Cisco Catalyst SD-WAN コントローラをプロビジョニング、モニター、および保守するための迅速な方法を提供します。

Cisco Catalyst SD-WAN ポータル を使用して、次のコントローラをプロビジョニングできます：

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN コントローラ

図 *1 : Cisco Catalyst SD-WAN* ポータル の利点と運用



Cisco Catalyst SD-WAN ポータル は、ポータルアクセスにデフォルトで多要素認証（MFA）を適用します。シングルサインオン（SSO）を使用して、任意のユーザーを任意のデバイスの任意のアプリケーションに接続できるアイデンティティ プロバイダー（IdP）を使用するように Cisco Catalyst SD-WAN ポータル を設定できます。

対象読者

このドキュメントは、サービスプロバイダー、パートナー、その他のエンドユーザーなどのシスコのお客様を対象としています。

Cisco Catalyst SD-WAN ポータルの前提条件

- Cisco Commerce Workspace で Cisco DNA サブスクリプションを購入します。 https://apps.cisco.com/Commerce/home
- **スマートアカウント**を作成するか、既存のものを開きます。
- そのスマートアカウントに関連付けられた**バーチャルアカウント**を作成します。
- Cisco プラグアンドプレイ（PnP）Connect ポータルで**デバイスのシリアル番号**を追加します。

  詳細に関しては、「Cisco Network Plug and Play Connect Capability Overview」[英語] を参照してください。

Cisco Catalyst SD-WAN ポータル の利点

- インスタンスの CPU 使用率などの重要な統計情報を可視化します。

- Cisco Catalyst SD-WAN オーバーレイネットワークをリアルタイムで監視する上で集中型ダッシュボードを提供します。
- ワークフロー内の適切なタスクに簡単に移動するためのウィザード駆動のインターフェイスが含まれています。
- プライマリおよびセカンダリデータストレージの地理的位置を指定するためのオプションをクラウドプロバイダーに提供します。
- 多要素認証（MFA）でのシングルサインオン（SSO）に IdP を使用した、セキュアなログインをサポートします。
- ロールベース アクセス コントロール（RBAC）をサポートします。
- オーバーレイへのオンプレミス TACACS サーバー接続用のカスタムサブネットを使用した新しいオーバーレイネットワークのプロビジョニングをサポートします。

スマート アカウントとバーチャル アカウント

スマートアカウントには、組織が購入したライセンスが含まれます。スマートアカウントは、購入したソフトウェア資産、登録、ソフトウェア使用の報告を表示、および組織全体のライセンス管理を行うことができる中央リポジトリです。

Cisco Catalyst SD-WAN ポータル について、シスコは Cisco Catalyst SD-WAN ポータル スマートアカウント管理者にアクセス権限を付与しました。スマートアカウント管理者は、コントローラの IP アドレスの表示やコントローラの IP アクセスリストの変更など、コントローラ インフラストラクチャに関連する運用タスクを表示および実行できます。このアクセスを特定のユーザに付与しない場合は、Cisco Software Central の [Manage Smart Account] セクションに移動し、それらのユーザをスマートアカウント管理者から削除するか、IDP（ID プロバイダー）オンボーディング機能を使用して、Cisco Catalyst SD-WAN ポータル へのアクセスを IDP の信頼できるユーザに基づいて付与してください。

詳細については、「コントローラをプロビジョニングするためのスマートアカウントとバーチャルアカウントのワークフロー」を参照してください。

バーチャルアカウントは、スマートアカウント内のサブアカウントです。バーチャルアカウントを使用すると、ビジネスにとって論理的な方法でシスコの資産を整理できます。部門、製品、地域、またはその他の指定別に会社のビジネスモデルに最適なバーチャルアカウントを設定できます。

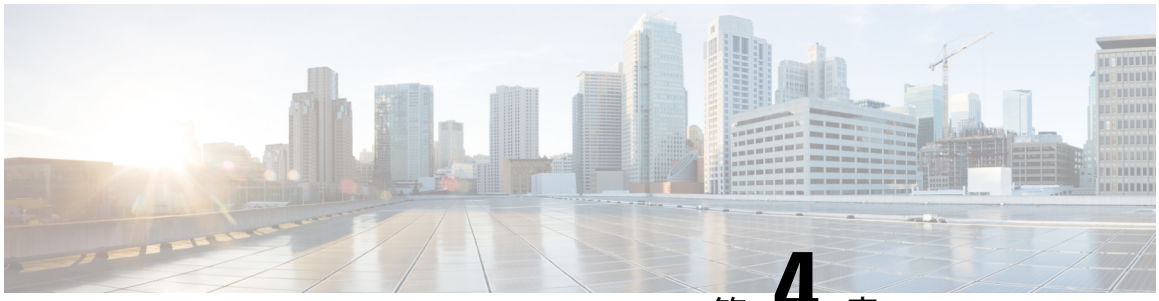
デフォルトのバーチャルアカウントが作成されます。Cisco Catalyst SD-WAN オーバーレイを作成するための専用のバーチャルアカウントを作成することをお勧めします。

詳細については、「スマートアカウントに関連付けられたバーチャルアカウントの作成」を参照してください。

Cisco Catalyst SD-WAN コントローラをプロビジョニングするには、Cisco Catalyst SD-WAN 対応の製品属性にバーチャルアカウントを関連付ける必要があります。Cisco Catalyst SD-WAN

対応属性は、Cisco DNA クラウドライセンスの注文時にバーチャルアカウントに関連付けられます。

（注） エンタープライズアグリーメントを使用してCisco DNA ライセンスを注文する場合、SD-WAN 対応属性へのバーチャルアカウントの自動関連付けは使用できません。Cisco CloudOps チームがコントローラをプロビジョニングするには、エンタープライズアグリーメントワークスペースを介してクラウドコントローラのプロビジョニング要求フォームを送信する必要があります。Cisco Catalyst SD-WAN テクニカルサポートに連絡して、目的のバーチャルアカウントを Cisco Catalyst SD-WAN ポータル で使用できるように依頼してください。目的のバーチャルアカウントが Cisco Catalyst SD-WAN ポータル で使用可能になったら、必要なエンタープライズアグリーメント契約情報を提供した後で、コントローラをプロビジョニングできます。



第 4 章

Cisco Catalyst SD-WAN ポータルへのアクセス

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

コントローラをプロビジョニングするためのスマートアカウントとバーチャルアカウントのワークフロー

以下は、スマートアカウント、バーチャルアカウントを作成し、Cisco DNA サブスクリプションをバーチャルアカウントに関連付けるためのワークフローです。

1. Cisco Software Central で組織のスマートアカウントを作成します。https://software.cisco.com/software/csws/ws/platform/home?locale=en_US

2. スマートアカウントに関連付けられたバーチャルアカウントを作成します。

   バーチャルアカウントの作成方法については、「スマートアカウントに関連付けられたバーチャルアカウントの作成」を参照してください。

3. Cisco Commerce Workspace で Cisco DNA サブスクリプションを購入します。
   https://apps.cisco.com/Commerce/home

（注） Cisco DNA サブスクリプションは、それぞれのスマートアカウントのいずれかのバーチャルアカウントに関連付ける必要があります。

通常、お客様に代わってアカウントマネージャまたはシスコの営業担当者が注文を行います。

4. ライセンスとして DNA クラウドサブスクリプション製品 ID（PID）を選択します。

   DNA クラウドサブスクリプション PID を選択すると、コントローラをプロビジョニングするために、SD-WAN 対応属性が自動的にバーチャルアカウントに関連付けられます。

5. 注文が完了すると、バーチャルアカウントはコントローラをプロビジョニングするために、Cisco Catalyst SD-WAN ポータル で使用できるようになります。

（注） バーチャルアカウントには、シスコプラグアンドプレイ（PnP）ポータルで追加されたデバイスのシリアル番号が含まれている必要があります。Cisco Catalyst SD-WAN ポータル でオーバーレイが作成されたら、Cisco PnP ポータルの [Controller Profile] タブを参照して、デバイスのシリアル番号とそれぞれのコントローラのマッピングを表示します。コントローラへのデバイスシリアル番号のマッピングは、デバイスを Cisco SD-WAN Manager に追加する、またはゼロタッチプロビジョニング（ZTP）を実行するために必要な情報を提供します。Cisco PnP ポータル の [Controller Profile] タブを表示し、Cisco Catalyst SD-WAN ポータル を使用した Cisco Catalyst SD-WAN オーバーレイ作成プロセスの一部としてコントローラがプロビジョニングされたことを確認します。

詳細に関しては、「Cisco Network Plug and Play Connect Capability Overview」[英語] を参照してください。

スマートアカウントに関連付けられたバーチャルアカウントの作成

はじめる前に

- スマートアカウントを作成します。

スマートアカウントの作成については、「コントローラをプロビジョニングするためのスマートアカウントとバーチャルアカウントのワークフロー」を参照してください。

バーチャルアカウントを作成します。

1. Cisco Software Central で、**[Manage Smart Account]** の下にある **[Manage Account]** を選択します。
2. [Virtual Accounts] をクリックします。
3. [Create Virtual Account] をクリックします。
4. [Review Notice] をクリックし、通知を確認した後、[I have Review the Notice] をクリックします。
5. 必要なフィールドに必要な情報を入力します。

（注） [Parent Account] フィールドに [At Top Level] が自動入力されます。この選択を保持できます。

6. [Next] をクリックします。
7. （任意）バーチャルアカウントにユーザーを割り当てます
8. [Next] をクリックします。
9. [Create Virtual Account] をクリックします。

   新しく作成したバーチャルアカウントがバーチャルアカウントのリストに表示されます。

認定オーバーレイのワークフロー

新規のお客様向けの認定オーバーレイのワークフロー

1. 新規の Cisco Catalyst SD-WAN お客様またはパートナーである場合は、Cisco Commerce Workspace でご注文してください。
2. [Certified Hosting Infra for vManage PID] サブスクリプション オプションを選択します。
3. 他の注文と同じ手順に従います。

（注） 認定オーバーレイに対応する正しい PID を選択していることを確認してください。

既存のお客様向けの認定オーバーレイのワークフロー

1. 既存の Cisco Catalyst SD-WAN のお客様またはパートナーである場合は、既存のバーチャルアカウントをご利用のうえ、Cisco Commerce Workspace でご注文ください。
2. [Certified Hosting Infra for vManage PID] サブスクリプション オプションを選択します。
3. Cisco ONE でチケットを作成します。

   チケットには次の情報を含めてください。

   - Virtual Account
   - 組織名
   - Order Number
   - 地域

4. Cisco CloudOps チームは注文番号を確認し、既存のオーバーレイを認定オーバーレイとしてアップグレードします。

初めての Cisco Catalyst SD-WAN ポータル へのアクセス

Cisco Catalyst SD-WAN ポータル に初めてログインすると、ガイド付きワークフローが表示されます。このワークフローでは、一部の機能を設定し、最初の Cisco Catalyst SD-WAN オーバーレイネットワークを作成するオプションが提供されます。

ID プロバイダー（IdP）を使用していない場合、Cisco Catalyst SD-WAN ポータル に初めてログインし、その後もログインを行うには、スマートアカウント管理者である必要があります。

IdP を使用している場合、Cisco Catalyst SD-WAN ポータル へのアクセスは IdP によって提供されるユーザアクセスに基づきます。

（注） software.cisco.com などの他の Cisco ポータルとは異なり、バーチャルアカウント管理者レベルのアクセスを使用して Cisco Catalyst SD-WAN ポータル にログインすることはできません。Cisco Catalyst SD-WAN ポータル は、バーチャルアカウント管理者レベルのアクセスを受付けません。

Cisco Catalyst SD-WAN ポータルへのログイン

Cisco Catalyst SD-WAN ポータル にログインするときは、シスコのクレデンシャルを使用する必要があります。

1. Cisco Catalyst SD-WAN ポータル URLhttps://ssp.sdwan.cisco.com/ に移動します。
2. シスコのログイン情報を入力します。

3. プロンプトが表示されたら、MFA ログイン情報をセットアップまたは入力します。

追加のMFAオプションの設定または既存のMFAオプションの更新

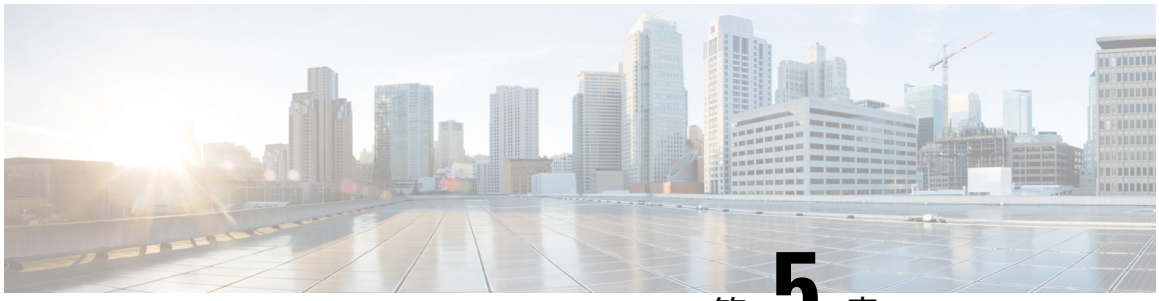
Cisco SD-WAN ポータルを使用して、追加の MFA オプションを追加したり、既存の MFA オプションを更新したりできます。

はじめる前に

Cisco Catalyst SD-WAN ポータル にログインできることを確認します。

MFA オプションの追加または更新

1. Cisco SD-WAN セルフサービスポータルにログインできたら、Cisco SD-WAN SSO に移動します。
2. SSO ページで、[Work] タブの下に Cisco Catalyst SD-WAN ポータル が表示されます。
3. ページの右隅にある自分の名前のドロップダウンリストから、[Settings] をクリックします。
4. [Extra Verification] セクションで、MFA オプションを追加するか、既存の MFA オプションを更新します。



第 5 章

ID プロバイダーの設定

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

Cisco Catalyst SD-WAN ポータル の IdP の設定

Cisco Catalyst SD-WAN ポータル に初めてログインするときに、Okta ID 管理など、組織の ID プロバイダー（IdP）を使用するように Cisco Catalyst SD-WAN ポータル を設定するオプションがあります。

（注） Cisco Catalyst SD-WAN ポータル の IdP の設定はオプションです。

IdPとロールを設定した後（「IdP ユーザーの Cisco SD-WAN セルフサービス ポータル ロールの設定」）、Cisco.com アカウントのクレデンシャルの代わりに独自の IdP を使用してログインできます。

（注） Cisco Catalyst SD-WAN ポータル で IdP をセットアップする場合、発行者、ログイン URL、およびプライバシー強化メール（PEM）キーを組織の IdP から使用できません。この情報は、Assertion Consumer Service（ACS）URL とオーディエンスを組織の IdP に設定した後に使用できます。組織の IdP を設定する場合は、ACS URL とオーディエンスのプレースホルダ値を追加することをお勧めします。後で、Cisco Catalyst SD-WAN ポータル で IdP を設定し、Cisco Catalyst SD-WAN ポータル で編集可能な ACS URL およびオーディエンスの Uniform Resource Identifier（URI）の正しい値で組織の IdP を更新できます。

はじめる前に

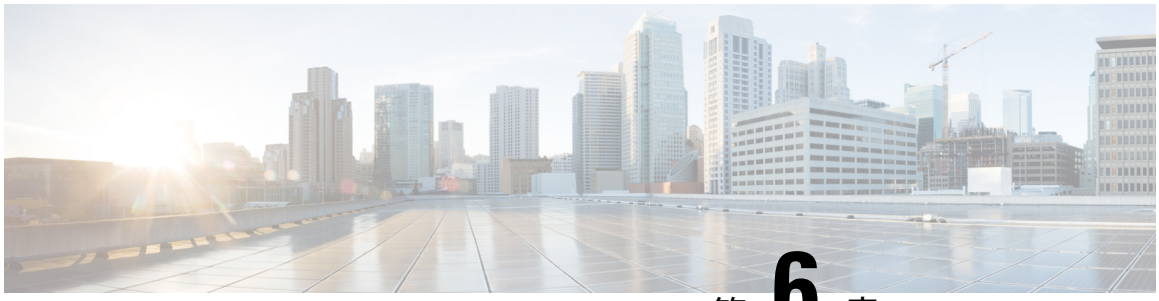
Cisco Catalyst SD-WAN ポータル で IdP を設定する前に、組織の IdP に次の変数を作成する必要があります。Cisco Catalyst SD-WAN ポータル では、ログインするユーザーごとにこれらの変数が必要です。

- firstName
- lastName
- email
- SSP_User_Role

  ロールの詳細については、「IdP ユーザーの Cisco SD-WAN セルフサービス ポータル ロールの設定」を参照してください。

Cisco Catalyst SD-WAN ポータル の IdP の設定

1. IdP の次の情報を指定します。この情報は IdP で確認できます。
   - ドメイン名
   - IdP の発行元 URL
   - IdP SSO URL
   - IdP 署名証明書（.pem 形式）
2. [Submit Request] をクリックします。
3. IdP サイトで、IdP の作成を確認します。



第 6 章

ロールベースのアクセスの管理

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

IdP ユーザーの Cisco Catalyst SD-WAN ポータル ロールの設定

はじめる前に

（注） ID プロバイダー（IdP）の Cisco Catalyst SD-WAN ポータル ロールの設定はオプションです。

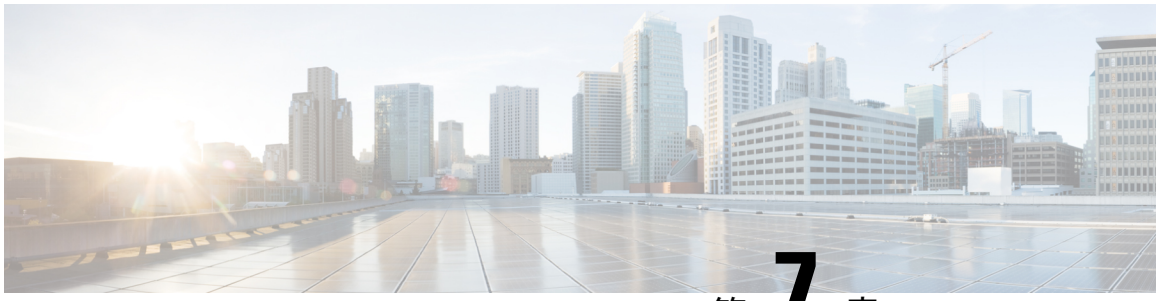
IdP ユーザーのロールの設定

1. Cisco Catalyst SD-WAN ポータル メニューから、[Manage Roles] を選択します。
2. 権限の名前を入力します。

3. バーチャルアカウントごとに、次のリストからロールを割り当てます。
   - [Monitor]：Cisco Catalyst SD-WAN ポータル のすべてのオーバーレイオプションを表示およびモニタできます。
   - [Overlay Management]：オーバーレイネットワークを作成、変更、およびモニタできます。
   - [Administration]：モニタおよびオーバーレイ ネットワーク ロールによって定義されたすべてのタスクを実行し、セカンダリ IdP をオンボードできます。
4. [Add Role] をクリックします。
5. すべてのロールを追加したら、[Done] をクリックします。
6. IdP クレデンシャルを使用して Cisco Catalyst SD-WAN ポータル に再度ログインします。

追加ロールの作成

追加ロールを作成するには、スマートアカウント管理者が「IdP ユーザーの Cisco SD-WAN セルフサービス ポータル ロールの設定」の項で説明されている手順を実行する必要があります。



第 7 章

オーバーレイネットワークの管理

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

Cisco Catalyst SD-WAN クラウドホスト型ファブリックの作成

Cisco Catalyst SD-WAN ポータル は、次の手順の中で提供する情報に従って Cisco Catalyst SD-WAN ファブリックをプロビジョニングします。

はじめる前に

次の点を確認してください。

- アクティブな Cisco スマートアカウント。
- アクティブな Cisco バーチャルアカウント。
- Cisco スマートアカウントの SA 管理者ロール。（Cisco Catalyst SD-WAN ポータル に初めてアクセスしてファブリックを作成するために必要です。以降は不要です。）
- Cisco Commerce（旧 CCW）でのコントローラの有効な注文。

手順

1. シスコからの電子メールで受け取った URL に移動して Cisco Catalyst SD-WAN ポータルにアクセスし、ログインします。
2. Cisco Catalyst SD-WAN ポータル メニューから **[Create Overlay]** を選択します。

   [Create Cisco Hosted Fabric] ページが表示されます。
3. **[Smart Account]** ドロップダウンリストから、ファブリックを関連付ける Cisco スマートアカウントの名前を選択します。
4. **[Virtual Account]** ドロップダウンリストから、ファブリックを関連付ける Cisco バーチャルアカウントの名前を選択します。
5. **[Assign Controllers]** をクリックし、**[Assign Controllers]** エリアで次の操作を実行します。
   1. 次の表で説明されているように、専用ファブリックのコントローラタイプの数のオプションを設定します。

オプション	説明
Assign (for the **vManage** controller type)	展開内の Cisco SD-WAN Manager コントローラの数を入力します。 有効値は **1**、**3**、または **6** です。
Assign (for the **vBond** controller type)	展開内の Cisco SD-WAN Validator の数を入力します。 最小値は **2** です。
Assign (for the **vSmart** controller type)	展開内の Cisco SD-WAN コントローラ の数を入力します。 最小値は **2** です。
Enable Cluster	Cisco SD-WAN Manager コントローラの数に **3** または **6** を選択した場合にのみ適用されます。 Cisco SD-WAN Manager クラスタを作成するには、このオプションをオンにします。

オプション	説明
Cluster Type	**[Enable Cluster]** オプションをオンにした場合にのみ適用されます。 **[Single Tenant Cluster]** を選択して、単一テナントクラスタを有効にします。

2. [**Assign**] をクリックします。

6. **[Fabric]** フィールドにファブリックの名前を入力します。
7. **[Cloud Provider]** で、シスコがファブリックのコントローラをホストするクラウドプロバイダーとして **[AWS]** を選択します。
8. **[SD-WAN Version]** ドロップダウンリストから、コントローラで使用する Cisco Catalyst SD-WAN のバージョンを選択します。

   必要な特定の機能があり、その機能が別のバージョンでのみ利用可能な場合を除き、推奨バージョンを選択します。推奨バージョンについては、Cisco Software Central でご確認ください。Cisco Catalyst SD-WAN リリースの詳細については、『User Documentation for Cisco IOS XE (SD-WAN) Release 17』の「**Release Information**」エリアにある Cisco Catalyst SD-WAN リリースノートを参照してください。
9. **[Locations]**で、次のアクションを実行します。
   1. **[Primary Location]** ドロップダウンリストから、Cisco SD-WAN Manager コントローラがプロビジョニングされている地理的な場所を選択します。

      ネットワークに比較的近い場所を選択することをお勧めします。
   2. **[Secondary Location]** ドロップダウンリストから、バックアップのデータストレージとロードバランシングの地理的な場所を選択します。プライマリとセカンダリの両方に同じリージョンを選択すると、SSP は自動的に同じリージョン内の 2 つの異なるゾーンにインスタンスを配置します。

（注） プライマリロケーションに最も近い場所を選択することをお勧めします。

   3. **[Data Location]** ドロップダウンリストから、Cisco Catalyst SD-WAN Analytics データストレージの地理的な場所を選択します。

      プライマリロケーションに最も近い場所を選択することをお勧めします。
10. **[Contacts]** で次の情報を入力します。
    - **[Fabric Admins]** フィールドに、Cisco Catalyst SD-WAN ポータル がファブリックに関する通知を送信する 1 つ以上のカンマ区切りの電子メールアドレスまたはメーリストリスト名を入力します。

- **[Cisco Contact Email]** フィールドに、緊急の問題が発生し、ファブリックの管理者と連絡が取れない場合に連絡可能なシスコの連絡先の電子メールアドレスを入力します。
- **[Enter Contract number of service]** フィールドに、Cisco Catalyst SD-WAN ポータルサービス契約の番号を入力します。
- **[Enter CCO ID of Service Requester]** フィールドに、Cisco Catalyst SD-WAN ポータルのチケットを作成した人の Cisco ID を入力します。

アラート通知：SSP は、サブスクリプションの期限切れ、メンテナンス期間、機能の変更などさまざまな理由でお客様にアラート通知を送信します。SSP 通知は、オーバーレイの詳細で設定された、登録済みの「オーバーレイ管理者」の連絡先である電子メールアドレスに送信されます。この電子メールアドレスを最新の状態に保つのはお客様の責任となります。複数の電子メールアドレスを登録できます。電子メールアドレスを更新するには、次の手順を実行します。

1. https://ssp.sdwan.cisco.com で SSP にログインします。 ログインするには、Cisco PNP スマートアカウント管理者ロールが必要です。

   または、スマートアカウント管理者が SSP 上で IDP をすでにセットアップしている場合は、管理者から提供されたロールでログインできます。
2. **[Overlay Details]** > **[Description]** > **[Overlay Admin]**に移動します。
3. 編集するには、鉛筆アイコンをクリックします。
4. 電子メールアドレスを入力し、**Tab キー**を押します。
5. チェックマークアイコンをクリックして保存します。

11. 必要に応じて次の**詳細オプション**を設定します。

    これらのオプションの詳細については、「Cisco Catalyst SD-WAN クラウドホスト型ファブリックの詳細オプションの設定」を参照してください。

    - **[Custom Subnets]**：コントローラ インターフェイスの IP アドレスに使用するプライベート IP アドレスを設定します。
    - **[Custom Domain Settings]**：Cisco SD-WAN Validator および Cisco SD-WAN Manager コントローラにアクセスするためのカスタムドメインを設定します。
    - **[Snapshot Settings]**：展開で Cisco SD-WAN Manager インスタンスのスナップショットを作成する頻度を設定します。
    - **[Custom Organization Name]**：ネットワークを識別する一意の組織名を設定します。
    - **[Compliance]**：ファブリックの認定コンプライアンスを選択します。
    - **[Dual Stack]**：IPv6 デュアルスタックを有効にします。

12. **[Click here to review and agree to Terms & Conditions before proceeding]** をクリックし、**[Terms and Conditions]** ダイアログボックスに表示される情報を確認して、**[I Agree]** をクリックします。

13. **[Create Fabric]** をクリックします。

    システムによってファブリックが作成されます。このプロセスには最大60分かかる場合があります。このプロセスの進行状況に関する情報は、**[Create Fabric Progress]** 領域に表示されます。

    また、Cisco Catalyst SD-WAN ポータル の **[Notification]** ページにはパスワードが表示されます。ファブリックに初めてアクセスする場合は、このパスワードを使用します。

    環境を保護するために、ログイン後すぐにパスワードを変更することをお勧めします。

（注） システムによって提供されるコントローラのパスワードは、7 日後から Cisco Catalyst SD-WAN ポータルに表示されなくなります。パスワードを保持する場合は、パスワードのコピーを取っておくことをお勧めします。

14. ファブリックの準備ができたという通知を受け取ったら、次の手順を実行します。
    - デバイスにコントローラ証明書をインストールします。コントローラ証明書のインストールについては、「Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above」を参照してください。
    - Web サーバー証明書をインストールします。Web サーバー証明書のインストールについては、「Web Server Certificates」を参照してください。

Cisco Catalyst SD-WAN クラウドホスト型ファブリックの詳細オプションの設定

詳細オプションを使用すると、デフォルト設定が望むものではない場合に、ファブリックのさまざまな設定を指定できます。

ファブリックの詳細オプションを設定するには、Cisco Catalyst SD-WAN ポータル で **[Advanced Options]** をクリックし、以降のセクションで説明するオプションを設定します。

- [カスタムサブネット][カスタムサブネット] （24 ページ）
- [Custom Domain Settings][Custom Domain Settings] （26 ページ）
- [Snapshot Settings][Snapshot Settings] （26 ページ）
- [Custom Organization Name][Custom Organization Name] （27 ページ）
- コンプライアンス

- デュアル スタック

[カスタムサブネット]

[Custom Subnets] エリアには、コントローラ インターフェイスの IP アドレスに使用するプライベート IP アドレスを設定するためのオプションがあります。

エンタープライズ TACACS への接続、認証、許可、およびアカウンティング（AAA）サーバーへの接続、syslog サーバーへのメッセージの送信、またはファブリックを介したインスタンスへの管理アクセスなどの使用例では、特定のプレフィックスのプライベート IP アドレスでコントローラを展開することをお勧めします。これらのプレフィックスは一意であり、ファブリック内の他の場所では使用されていません。

オプション	説明
プライマリサブネット	
VPC サブネット	プライマリリージョンの VPC のプライベート IP アドレスブロックを入力します（例：192.168.0.0/24）。 この IP アドレスブロックは、プライベートネットワークから到達可能である必要があります。
プライマリロケーション	ファブリックのプライマリリージョンを表示します。
管理サブネット	プライマリリージョンの管理サブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力する IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。
制御サブネット	プライマリリージョンの制御サブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力した IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。

オプション	説明
クラスタサブネット	プライマリリージョンのクラスタサブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力した IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。
セカンダリサブネット	
VPC サブネット	セカンダリリージョンの VPC のプライベート IP アドレスブロックを入力します（例：192.168.1.0/24）。 この IP アドレスブロックは、プライベートネットワークから到達可能である必要があります。
プライマリロケーション	ファブリックのセカンダリリージョンを表示します。
管理サブネット	セカンダリリージョンの管理サブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力した IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。
制御サブネット	セカンダリリージョンの制御サブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力した IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。
クラスタサブネット	セカンダリリージョンのクラスタサブネットのプライベート IP アドレスブロックを入力します。 このアドレスは、VPC について入力した IP アドレスブロック内である必要があります。 IP アドレスブロックの最小サイズは 16 です。

[Custom Domain Settings]

[Custom Domain Settings] エリアには、Cisco SD-WAN Validator および Cisco SD-WAN Manager コントローラにアクセスするためのカスタムドメインを設定するオプションがあります。

デフォルトでは、ドメイン名は cisco.com です。必要な場合は、展開する別のドメインを指定できます。

カスタムドメインを指定する場合、シスコはユーザーのドメインにアクセスできないため、Cisco SD-WAN Validator と Cisco SD-WAN Manager について独自のドメインネームシステムを作成する必要があります。

カスタムドメインを設定したら、次のマッピングを作成し、コントローラ証明書が起動できるようにします。

- Cisco SD-WAN Validator DNS をすべての VPN 0 IP アドレスにマッピングします。
- Cisco SD-WAN Manager DNS をすべての VPN 512 IP アドレスにマッピングします。

オプション	説明
vBond	Cisco SD-WAN Validator の DNS 名を入力します。
vManage	Cisco SD-WAN Manager の DNS 名を入力します。

[Snapshot Settings]

[Snapshot Settings] エリアには、展開で Cisco SD-WAN Manager インスタンスのスナップショットを作成する頻度を設定するオプションがあります。

デフォルトでは、ネットワークオーバーレイ設定は 1 日に 1 回バックアップされ、10 個のスナップショットが保存されます。

スナップショットの詳細については、『スナップショットについて』を参照してください。

オプション	説明
Frequency	システムが Cisco SD-WAN Manager インスタンスのスナップショットを作成する頻度を選択します。次のオプションがあります。 • **1 日に 1 回** • **2 日に 1 回** • **3 日に 1 回** • **4 日に 1 回**

[Custom Organization Name]

[Custom Organization Name] エリアには、ネットワークを識別する一意の組織名を設定するオプションがあります。

オプション	説明
[Custom Organization Name]	組織の一意の名前を入力します。 最大 56 文字の名前を入力できます。 組織名が確実に一意のものとなるように、Cisco Catalyst SD-WAN ポータル では入力した名前の末尾にハイフン（-）とバーチャルアカウント ID が自動的に付加されます。

認定コンプライアンスモード

[Compliance Configuration] エリアには、ファブリックの認定コンプライアンスオプションがあります。次のコンプライアンスモードを使用できます。

表 *2:* サポートされる認定

オプション	Description
PCI-DSS	PCI DSS（クレジットカードデータ保護基準）、サービスプロバイダー、レベル 1
SOC2	System and Organization Controls
ISO27001、ISO27017、ISO27018、ISO27701	国際標準化機構（ISO）
C5	クラウド コンピューティング コンプライアンス コントロール カタログ（ドイツ）
ENS	Esquema Nacional de Seguridad（スペイン）
Tx-RAMP	Texas Risk and Authorization Management Program レベル 2

デュアル スタック

[Dual Stack] エリアには、コントローラの IPv6 を有効にするオプションがあります。

企業ネットワークが IPv6 で設定されている場合は、このオプションを有効にする必要があります。このオプションを有効にすると、ファブリックサブネットは IPv4 と IPv6 の両方で設定されます。IPv6 アドレスは、クラウド サービス プロバイダーによって割り当てられます。

（注） ファブリックに対してこのオプションを有効にすると、後で無効にすることはできません。

オプション	説明
IPv6 デュアルスタック	コントローラの IPv6 デュアルスタックを有効にするには、このチェックボックスをオンにします。

オーバーレイネットワークの削除

オーバーレイネットワークを削除するには、Cisco Catalyst SD-WAN のテクニカルサポートにお問い合わせください。オーバーレイネットワークは削除できません。

コントローラアクセスを管理するための IP アドレス許可リストの指定

シスコがホストするオーバーレイネットワークの場合、プレフィックスを含む信頼できる IP アドレスを指定して、そこからコントローラアクセスを管理できます。管理アクセスを有効化するには、アクセスが必要なルールタイプ、プロトコル、ポート範囲、および送信元 IP（IP アドレスとプレフィックス）を指定します。

（注） オーバーレイに参加するために WAN エッジデバイスの IP アドレスを追加する必要はありません。Cisco SD-WAN Manager がデバイスのシリアル番号を許可している限り、任意の IP アドレスを持つデバイスは、Datagram Transport Layer Security（DTLS）または Transport Layer Security（TLS）トンネルを使用してオーバーレイに参加できます。

- オーバーレイごとに最大 200 のルールを追加できます。
- 各ルールは、オーバーレイ内のすべてのクラウドホストコントローラに一律に適用されます。
- 新しいクラウドホスト型インスタンスが追加されるか、既存のインスタンスが置き換えられた場合は、同じルールが自動的に適用されます。ルールは、単一の IP アドレスまたはより大きな IP プレフィックスのいずれかです。

1. Cisco Catalyst SD-WAN ポータル ダッシュボードから、オーバーレイネットワークに移動します。
2. **[List View]** タブでオーバーレイネットワークの名前をクリックします。
3. [Inbound Rules] をクリックします。
4. **[Add Inbound Rule]** をクリックします。
5. IP アドレスまたはプレフィックスの次のパラメータを指定します。

- [Rule type]：[All]、[SSH]、[HTTPS]、[Custom TCP rule]、または [Custom UDP rule] のいずれかを選択します。
- [Port range]：カスタム TCP および UDP ルールの場合、ポート範囲を指定します。
- [Source]：IP アドレスまたは IP アドレスプレフィックスを指定します。
- **[Description]**：インバウンドルールの説明を入力します。

6. [Add Rule] をクリックします。
7. （オプション）**[Add New Inbound Rule]** をクリックして、他の許可する IP アドレスまたは IP アドレスプレフィックスを追加します。

事前定義されたインバウンドルールの作成

表 *3*：機能の履歴

機能名	リリース情報	説明
事前定義されたインバウンドルール	2023 年 3 月リリース	この機能を使用すると、信頼できる IP アドレスを指定できます。これらの IP アドレスは、この機能を設定するスマートアカウントで作成する新しいオーバーレイに適用されます。これらの IP アドレスは、この機能を設定するスマートアカウントの既存のオーバーレイに適用することもできます。

事前定義されたインバウンドルールについて

この機能を使用すると、それぞれが信頼できる IP アドレスを指定するインバウンドルールを作成できます。これらの IP アドレスは、この機能を設定するスマートアカウントで作成する新しいオーバーレイに適用されます。これらの IP アドレスは、この機能を設定するスマートアカウントの既存のオーバーレイに適用することもできます。

インバウンドルールには、ルール名、ルールが適用されるプロトコルとポート範囲、および送信元 IP アドレスまたはプレフィックスの情報が含まれます。最大で 200 のインバウンドルールを作成できます。

事前定義されたインバウンドルールの使用例

事前定義されたインバウンドルールにより、同じ信頼できる IP アドレスのグループを既存のオーバーレイと新しいオーバーレイに追加するための便利な方法が提供されます。事前定義さ

れたインバウンドルールを作成することで、各オーバーレイの信頼できる IP アドレスを手動で設定する必要がなくなります。

事前定義されたインバウンドルールの設定

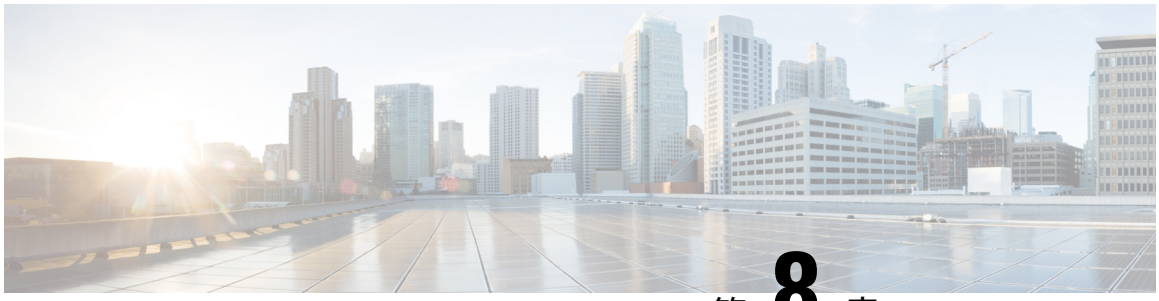
1. Cisco Catalyst SD-WAN ポータル メニューから **[Admin Settings]** を選択します。
2. 定義済みのインバウンドルールを設定するスマートアカウントの横にある **[...]** をクリックし、**[Manage Predefined Inbound Rules]** をクリックします。

   設定されているインバウンドルールのリストが表示されます。
3. **[Add Predefined Inbound Rules]** をクリックします。
4. **[Add Inbound Rule]** エリアで次のアクションを実行します。
   1. **[Name]** フィールドに、ルールの一意の名前を入力します。
   2. **[Rule Type]** ドロップダウンリストから、ルールを適用するプロトコルのタイプ（**[All]**、**[SSH]**、**[HTTPS]**、**[Custom TCP rule]**、または **[Custom UDP rule]**）を選択します。
   3. **[Custom TCP rule]** または **[Custom UDP rule]** のルールタイプを選択した場合は、**[Port Range]** フィールドにルールを適用するポート範囲を入力します。
   4. **[Source]** フィールドに、IP アドレスまたは IP アドレスプレフィックスを入力します。
   5. **[Description]** フィールドに、事前定義されたインバウンドルールの説明を入力します。
   6. （オプション） **[Automatically add this rule to ALL overlays]** をクリックすると、このスマートアカウントで今後作成されるオーバーレイに加え、このスマートアカウントの既存のオーバーレイにもこの新しいルールが追加されます。

      このオプションをクリックしない場合、このルールは今後作成されるオーバーレイにのみ追加されます。
   7. [Add] をクリックします。

追加のオーバーレイネットワークの作成

追加の Cisco Catalyst SD-WAN クラウドホスト型オーバーレイネットワークを作成するには、「Cisco SD-WAN クラウドホスト型オーバーレイネットワークの作成」に記載されている手順に従います。



第 8 章

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V について

表 *4:* 機能の履歴

機能名	リリース情報	説明
ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V	2023 年 5 月	この機能を使用すると、仮想プライベートクラウドをプライベートデータセンターに接続するためのクラウドゲートウェイとして Cisco Catalyst 8000V デバイスを設定できます。

Cisco Catalyst 8000V は、仮想プライベートクラウド（VPC）をプライベートデータセンターに接続するためのクラウドゲートウェイとして機能します。

要件に応じて、次の方法で Cisco Catalyst 8000V デバイスをクラウドゲートウェイとして設定できます。

- 新しいファブリックを作成し、ファブリック内の各リージョンのクラウドゲートウェイとして Cisco Catalyst 8000V デバイスを追加します。
- 既存のファブリックの各リージョンに Cisco Catalyst 8000V デバイスを追加します。
- 既存のファブリックの Cisco vEdge Cloud を Cisco Catalyst 8000V デバイスに置き換えます。

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V の使用例

- VPN経由でアクセスするプライベートデータセンターにサーバーが存在する場合の認証、許可、およびアカウンティング（AAA）のための、ファブリックとTACACSまたはRADIUSサーバーとの統合。
- VPN 経由でアクセスするプライベートデータセンターへの syslog 情報の送信。

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V の前提条件

- Cisco SD-WAN Manager 管理者のユーザー名とパスワードが必要です。
- Cisco スマートアカウント管理者のユーザー名とパスワードが必要です。
- ファブリックに追加する Cisco Catalyst 8000V のシリアル番号を知っている必要があります。

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V の制約事項

- バージョン 20.6 以降のファブリックバージョンを使用している必要があります。

ファブリックのクラウドゲートウェイとしての Cisco Catalyst 8000V の設定

はじめる前に

設定する各 Cisco Catalyst 8000V デバイスのシリアル番号を取得します。これを行うには、Cisco Software Central に移動し、**[Smart Licensing]** エリアの **[Network Plug and Play]** の下にある **[Manage Devices]** をクリックします。

設定手順

次の表では、さまざまなシナリオで Cisco Catalyst 8000V デバイスをクラウドゲートウェイとして設定する手順について説明します。各シナリオについて、一般的な手順と詳細情報の参照先を表に示します。要件に該当するシナリオを参照してください。

シナリオ	一般的な手順	参照先
新しいファブリックを作成し、ファブリック内の各リージョンのクラウドゲートウェイとして Cisco Catalyst 8000V デバイスを追加します。	**ステップ 1**：Cisco Catalyst SD-WAN ポータル で新しいファブリックを作成します。	「Cisco Catalyst SD-WAN クラウドホスト型ファブリックの作成」を参照してください。
	ステップ 2：Cisco Catalyst SD-WAN ポータル でクラウドゲートウェイを設定します。	Cisco Catalyst SD-WAN ポータル でのクラウドゲートウェイの設定 （34 ページ）を参照してください。
既存のファブリックの各リージョンに Cisco Catalyst 8000V デバイスを追加します。	Cisco Catalyst SD-WAN ポータル でクラウドゲートウェイを設定します。	Cisco Catalyst SD-WAN ポータル でのクラウドゲートウェイの設定 （34 ページ）を参照してください。
既存のファブリックで Cisco vEdge Cloud を Cisco Catalyst 8000V デバイスに置き換えます。	**ステップ 1**：Cisco Catalyst SD-WAN ポータル でクラウドゲートウェイを設定します。	Cisco Catalyst SD-WAN ポータル でのクラウドゲートウェイの設定 （34 ページ）を参照してください。
	ステップ2：（オプション）シスコにサポートケースをオープンし、既存の Cisco vEdge Cloud の削除を要求します。	ファブリック更新のサポートケースのオープン （37 ページ）を参照してください。

Cisco Catalyst SD-WAN ポータル でのクラウドゲートウェイの設定

1. 管理者のログイン情報で Cisco Catalyst SD-WAN ポータル にログインします。
2. クラウドゲートウェイを設定するファブリックをクリックします。
3. **[Actions]** ドロップダウンメニューから **[Add Cloud Gateways]** を選択します。
4. 次の表で説明するフィールドを設定します。

（注） Cisco Catalyst SD-WAN ポータル は、これらのフィールドに入力したユーザー名とパスワードを保存しません。

フィールド	説明
vManage 管理者のログイン情報	
[Username]	Cisco SD-WAN Manager 管理者のユーザー名を入力します。

フィールド	説明
[Password]	Cisco SD-WAN Manager 管理者のパスワードを入力します。
スマートアカウント管理者のログイン情報	
[Username]	Cisco スマートアカウントの管理者のユーザー名を入力します。
[Password]	Cisco スマートアカウントの管理者パスワードを入力します。
クラウドゲートウェイのシリアル	
シリアル（**Serial**）	表示される **[Serial]** フィールドの数は、ファブリック内のリージョンの数と一致します。 各フィールドに、クラウドゲートウェイとして機能する Cisco 8000V のシリアル番号を入力します。 各シリアル番号は一意である必要があります。
カスタム **IP**	

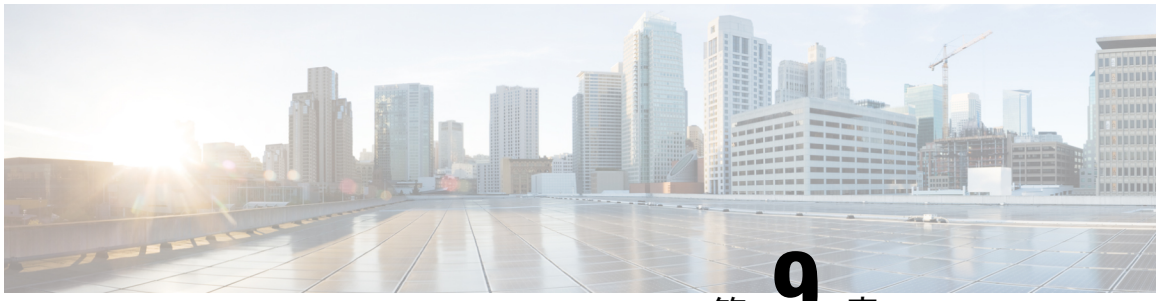
フィールド	説明
[System IPs]	表示される **[System IPs]** フィールドの数は、ファブリック内のリージョンの数と一致します。 （オプション）各フィールドに、追加するクラウドゲートウェイのシステムインターフェイスを設定する IP アドレスを入力します。 システムインターフェイスの IP アドレスは、デバイスを識別する永続的なアドレスです。これは通常のルータのルータ ID に似ていて、パケットの発信元のルータを識別するために使用されるアドレスです。 システムの IP アドレスを 10 進 4 部ドット表記の IPv4 アドレスとして指定します。アドレスだけを指定してください。プレフィックス長（/32）は暗黙的です。 システム IP アドレスには、0.0.0.0/8、127.0.0.0/8、224.0.0.0/4、および 240.0.0.0/4 以降を除く任意の IPv4 アドレスを使用できます。 システム IP アドレスを指定しない場合、Cisco Catalyst SD-WAN ポータル はシステムのランダム IP アドレスを割り当てます。このアドレスは別のデバイスの IP アドレスと重複する可能性があります。 ファブリックで競合が発生することなくクラウドゲートウェイがプロビジョニングされるようにするために、入力する IP アドレスが既存のファブリックで使用されていないことを確認してください。

フィールド	説明
[Enable Webhook via Cloud Gateway]	このオプションは、AWS がクラウドプロバイダーである専用ファブリックにのみ適用されます。 Cisco SD-WAN Manager がクラウドゲートウェイを介して Cisco SD-WAN Manager からウェブフックメッセージをルーティングできるようにするには、このチェックボックスをオンにします このオプションを有効にすると、ウェブフックサーバーがプライベートネットワークでホストされており、インターネットトラフィックがこのサーバーに転送されない場合に役立ちます。このオプションが有効になっている場合、SD-WAN ファブリックとプライベートネットワーク間の接続がプロビジョニングされます。 このオプションを有効にした後、Cisco SD-WAN Manager サーバーのルーティングテーブルにエントリを追加し、ネットワークトラフィックがクラウドゲートウェイを介してウェブフックサーバーに転送されるようにします。手順については、クラウドゲートウェイのプロビジョニング後に受信する電子メールを参照してください。

5. [Submit] をクリックします。

ファブリック更新のサポートケースのオープン

ファブリック更新のサポートケースをオープンするには、シスコの Support Case Manager に移動し、シスコのログイン情報でログインして、**[Open New Case]** をクリックします。



第 9 章

オーバーレイネットワークのモニタリング

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

オーバーレイネットワークの Cisco Catalyst SD-WAN コントローラとデバイスのモニタリング

1. Cisco Catalyst SD-WAN ポータル ダッシュボードで **[List View]** タブをクリックします。

   オーバーレイのリストが表示されます。

2. オーバーレイの名前をクリックします。

3. **[Controller View]** エリアで、モニターするコントローラ（**vManage**、**vBond**、**vSmart**、**Cloud Gateways**、または **vEdge**）をクリックします。

4. [Controllers] ウィンドウで、ネットワーク使用率、CPU 使用率、または期間でフィルタリングできます。このウィンドウでは、状態、タイプ、バージョン、またはリージョンでフィルタ処理することもできます。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、**[Controllers]** タブの名前が **[Control Components]** タブに変更されました。

オーバーレイとコントローラの詳細の表示

1. Cisco Catalyst SD-WAN ポータルのダッシュボードで、**[List View]** タブをクリックします。

   オーバーレイのリストが表示されます。

2. オーバーレイの名前をクリックします。

   [Dashboard] > **[Overlays]** > **[Details]** ページに、オーバーレイの詳細情報が表示されます。

変更ウィンドウの通知の表示

表 *5:* 機能の履歴

機能名	リリース情報	説明
変更ウィンドウ通知	2021 年 2 月リリース	この機能を使用すると、Cisco Catalyst SD-WAN のオーバーレイメンテナンスの開始時または終了時を確認できます。これには、変更ウィンドウ通知がスケジュールされたときの詳細情報、およびメンテナンスにおいて予定されている操作が含まれます。 Cisco Catalyst SD-WAN ポータル カスタマーは変更ウィンドウ通知のみを表示できます。CloudOps ユーザーは、変更ウィンドウ通知をスケジュールまたは開始する必要があります。

変更ウィンドウ通知により、Cisco Catalyst SD-WAN のオーバーレイメンテナンスの開始時または終了時を確認できます。これには、変更通知がスケジュールされたときの詳細情報、およびメンテナンスにおいて予定されている操作が含まれます。

変更ウィンドウ通知アラートは、10 日以内に開始またはスケジュールされた通知に対して表示されます。通知が完了状態であるか、または 10 日後以降に開始するようにスケジュールされ

ている場合、バナーアラートは Cisco Catalyst SD-WAN ポータル のダッシュボードに表示されません。

変更通知が開始されると、バナーアラートに進行中として表示されます。

変更通知がスケジュールされている場合、バナーアラートに開始として表示されます。

はじめる前に

Cisco Catalyst SD-WAN ポータル カスタマーは変更ウィンドウ通知のみを表示できます。

CloudOps ユーザーは、変更ウィンドウ通知をスケジュールまたは開始する必要があります。

すべてのオーバーレイの変更ウィンドウ通知の表示

1. Cisco Catalyst SD-WAN ポータル のダッシュボードの [Change Window Notifications] で、スケジュール済みまたは開始済みのオーバーレイをクリックします。

   [Dashboard] > **[Change Window Notifications]** ページが表示され、オーバーレイのリストが示されます。

   すべての変更ウィンドウ通知にバナーアラートが表示されます。

   これは、すべてのオーバーレイの変更ウィンドウ通知すべてを表示するためのグローバルビューです。

2. （任意）ステータスでオーバーレイをフィルタリングして、オーバーレイのリストを制限または展開できます。

3. [Change Window Notifications] をクリックすると、変更ウィンドウ通知のリストが表示されます。これには、変更通知の説明の詳細カラムが含まれます。

   [Dashboard] > **[Overlays]** > **[Details]** > **[Change Window Notifications]** ページが表示されます。

特定オーバーレイの変更ウィンドウ通知の表示

1. 特定のオーバーレイの変更通知を表示するには、Cisco Catalyst SD-WAN ポータル ダッシュボードで、スケジュール済みまたは開始済みの変更通知があるオーバーレイをクリックします。

   [Dashboard] > **[Overlays]** > **[Details]** ページが表示されます。

2. スケジュール済みまたは開始済みの変更ウィンドウ通知があるオーバーレイをクリックします。

   オーバーレイ固有の変更ウィンドウ通知のバナーアラートが表示されます。すでにオーバーレイ内にいるため、バナーアラートにはオーバーレイの名前は含まれません。

   これは、特定のオーバーレイの変更ウィンドウ通知を表示する個別のビューです。

変更ウィンドウ通知のリストの表示

1. Cisco Catalyst SD-WAN ポータル ダッシュボードで、スケジュール済みまたは開始済みの変更ウィンドウ通知があるオーバーレイをクリックします。

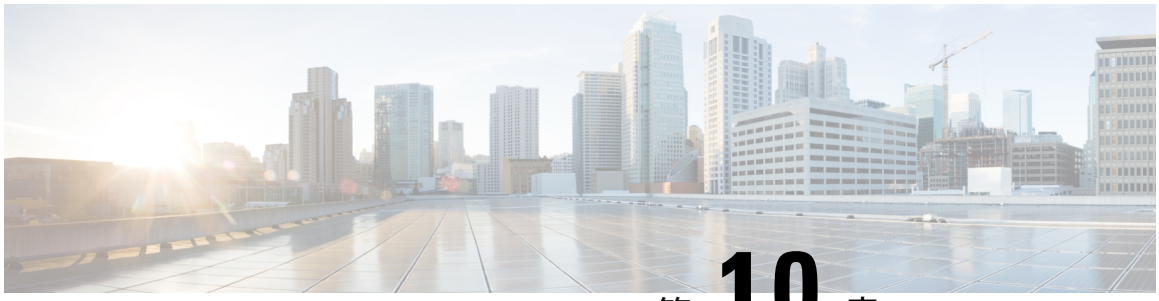
   [Dashboard] > **[Overlays]** ページが表示されます。

2. オーバーレイ名をクリックします。

   [Dashboard] > **[Overlays]** > **[Details]** ページが表示されます。

3. [Change Window Notifications] で、スケジュール済みまたは開始済みの変更ウィンドウ通知を選択します。

   [Dashboard] > **[Overlays]** > **[Details]** > **[Change Window Notifications]** ページが表示され、変更通知イベントに関する詳細情報を表示できます。



第 10 章

コンプライアンス

Cisco Catalyst SD-WAN のコンプライアンスと認定

民間の認定やコンプライアンスは多くの業界で不可欠な要素であり、それぞれ独自のお客様の要件があります。主な問題とクラウドサービスプロバイダー（CSP）の民間認定を必要とする理由の一部を次に示します。

- 適合規格の遵守
- データセキュリティとプライバシー
- 監査とアセスメントに基づくリスクの軽減
- 信頼性
- ディザスタリカバリと事業継続
- サービス品質の向上
- 競争優位
- 相互運用性
- 監査の簡素化

Cisco Catalyst SD-WAN は、規制を受けるさまざまな業界に適用される、国際的に認められた認定を提供できます。

- PCI-DSS
- SOC 2 Type 2/SOC 3

- ISO 27001、ISO 27701、ISO 27017、ISO27018
- C5
- ENS
- Tx-RAMP

Cisco Catalyst SD-WAN 認定のレポートについては、チャネルパートナーにお問い合わせください。

認定環境の利点

- セキュアな Center for Internet Security（CIS）または Security Technical Implementation Guide（STIG）設定基準規格を使用した集中型構成管理によるセキュアなネットワーク。
- 送信中および保管中にネットワーク全体のデータを暗号化することによるデータ保護。
- 一意のログイン情報と厳密なロールベースアクセス制御による一元化されたユーザーアカウント管理を通じた識別、アクセス、および認証の設定。
- Cisco Catalyst SD-WAN 制御コンポーネントでの、継続的なペネトレーションテストと脆弱性スキャン。

新しいファブリックの業界認定へのコンプライアンスの有効化

DNA サブスクリプションを購入済みで、認定リリースバージョンを使用しており、ファブリックを作成する前に Cisco Catalyst SD-WAN ポータル で認定オプションを選択している場合、認定環境の利点を活用できます。

（注） 民間認定はすべて、共有の クラウド提供型 Cisco Catalyst SD-WAN を通じて管理されます。

手順

ステップ 1 https://ssp.sdwan.cisco.com を開いて Cisco Catalyst SD-WAN ポータル にアクセスします。
ステップ 2 ログイン情報を使用して Cisco Catalyst SD-WAN ポータル にログインします。
ステップ 3 **[Create Cisco Hosted Fabric]** ページから、**[Smart Account]** と **[Virtual Account]** を選択します。
ステップ 4 **[Fabric Name]** フィールドに**ファブリック名**を入力します。
ステップ 5 **[Assign Controllers]** を選択します。

ステップ 6 **[Advanced Options]** で **[Compliance Configuration]** オプションを選択し、必要な業界認定コンプライアンスを選択します。

ステップ 7 **[Create Fabric]** をクリックします。

既存のファブリックの業界認定へのコンプライアンスの有効化

始める前に

業界認定へのコンプライアンスは、専用ファブリックでのみ可能です。

手順

ステップ 1 Cisco Catalyst SD-WAN ポータル にログインします。

ステップ 2 **[Fabric]** をクリックして、ファブリックオーバーレイを見つけます。

ステップ 3 **[Actions]** ドロップダウンリストで **[Compliance Mode]** を選択します。

ステップ 4 **[Compliance]** パネルで、必要な業界認定を選択します。

ステップ 5 [Apply] をクリックします。

認定コンプライアンスの表示

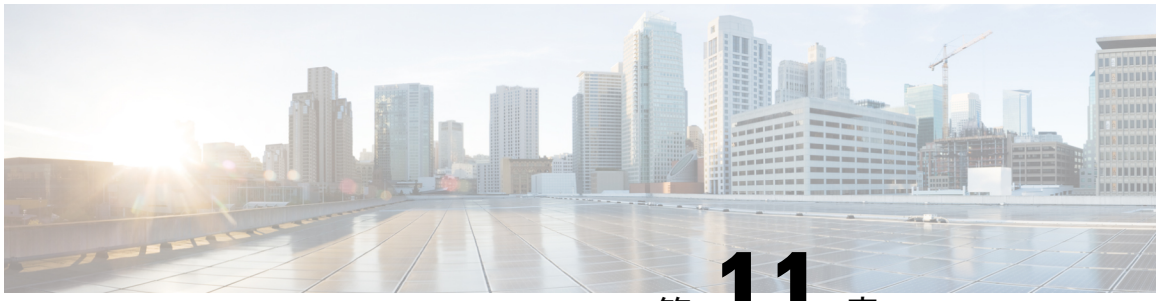
手順

ステップ 1 https://ssp.sdwan.cisco.com を開いて Cisco Catalyst SD-WAN ポータル にアクセスします。

ステップ 2 ログイン情報を使用して Cisco Catalyst SD-WAN ポータル にログインします。

ステップ 3 目的のファブリックを選択し、**[View Details]** をクリックします。

ファブリックのアクティブなコンプライアンスは、[Description] ペインに一覧表示されます。



第 11 章

スナップショット

スナップショットについて

Cisco Catalyst SD-WAN クラウドホスト型サービスには、Cisco SD-WAN Manager インスタンスの定期的なスナップショットの取得が含まれます。

- オンデマンド スナップショット

  Cisco SD-WAN Manager ソフトウェアについて予定されている主要な変更期間について、Cisco SD-WAN Manager のオンデマンド スナップショットを作成できます。Cisco Catalyst SD-WAN ポータルは、作成日から 10 日間、単一のオンデマンド スナップショットを保持します。10 日以内に新しいオンデマンド スナップショットを作成すると、以前のオンデマンド スナップショットが削除されます。

  オンデマンドスナップショットを作成して完了させるには、変更期間の 8 時間前までに設定変更を凍結して割り当てる必要があります。

  2023 年 4 月以降は、Cisco Catalyst SD-WAN ポータル からオンデマンド スナップショットをトリガーします。「オンデマンド スナップショットの作成」 を参照してください。

- 日別のスナップショット

  日次スナップショットは、指定された Cisco SD-WAN Manager の地域の場所に基づき、毎晩午前 0 時前後に自動的に取得されます。オーバーレイネットワークの作成時に選択した頻度に従って日次スナップショットが取得されます。スナップショットの頻度はデフォルトで毎日 1 回（通常は展開された地域の午前 0 時）に設定され、最後の 7 個のスナップショットが保持されます。保持できるのは、最大で最後の 7 個の定期スナップショットのみです。設定された頻度を超えた古いスナップショットは、毎日自動的に破棄されます。これらのスナップショットは、プライマリリージョンにのみ保存されます。

[Advanced Options] > **[Edit]** をクリックし、次に [Snapshot Settings] をクリックして、Cisco Catalyst SD-WAN ポータル オーバーレイ作成手順の一部としてスナップショットの頻度を設定します。

詳細については、「Cisco SD-WAN クラウドホスト型オーバーレイネットワークの作成」を参照してください。

設定できるのは Cisco Catalyst SD-WAN ポータル スナップショットの頻度のみです。

スナップショットが作成されたオーバーレイの名前をクリックすると、オーバーレイのスナップショットの詳細を表示できます。

詳細については、「スナップショットの表示」を参照してください。

（注） Cisco SD-WAN コントローラ と Cisco SD-WAN Validator はステートレスであるため、スナップショットは取得されません。Cisco SD-WAN Manager テンプレートを使用して Cisco SD-WAN コントローラ および Cisco SD-WAN Validator を設定し、保存します。

（注） スナップショットは Cisco Catalyst SD-WAN ポータル のクラウドアカウント内に保存されるため、Cisco Catalyst SD-WAN ポータル スナップショットのダウンロードはできません。Cisco Catalyst SD-WAN ポータル スナップショットの詳細は、読み取り専用で確認できます。Cisco CloudOps チームが、ディザスタリカバリのためにスナップショットを使用します。

- ゴールデンスナップショット

  既存の日別のスナップショットまたはオンデマンドスナップショットをゴールデンスナップショットとしてマークすると、作成日から 3 ヵ月間保存されます。Cisco Catalyst SD-WAN ポータル は単一のゴールデンスナップショットを保存できます。新しい日別のスナップショットまたはオンデマンドスナップショットがゴールデンスナップショットとしてマークされると、以前にマークされたゴールデンスナップショットからゴールデンタグが自動的に削除されます。古いスナップショットはその後、有効期限スケジュールに従って削除されます。

  Cisco SD-WAN Manager の状態がスナップショットの時点で理想的な状態であり、後で適切なリカバリポイントとして機能すると考えられる場合は、スナップショットをゴールデンとしてマークする必要があります。

オンデマンド スナップショットの作成

必要に応じて、Cisco SD-WAN Manager の設定のオンデマンド スナップショットを作成できます。一般に、主要な変更期間の前にスナップショットを作成します。

オンデマンドスナップショットを作成する場合、スナップショットを完了させるには、変更期間の 8 時間前までに設定変更を凍結して割り当てる必要があります。

オンデマンドスナップショットは作成日から 15 日間保存され、その後自動的に削除されます。新しいオンデマンドスナップショットは保存されている既存のスナップショットを置き換えるため、一度に保存されるオンデマンド スナップショットは 1 つだけです。

（注） オンデマンド スナップショットは、共有テナントでは使用できません。

1. Cisco Catalyst SD-WAN ポータル から、使用可能なオーバーレイのリストに移動します。

   [Dashboard] > **[Overlays]**ページが表示されます。

2. スナップショットを作成するオーバーレイの名前をクリックします。

3. **[Dashboard]** > **[Cisco Hosted Overlays]** > **[Details]**ページで、**[Snapshot]** タイルをクリックします。

4. **[Actions]** ドロップダウンメニューから **[On-Demand Snapshot]** を選択します。

5. **[On-Demand Snapshot]** エリアで、スナップショットを作成する Cisco SD-WAN Manager インスタンスのスイッチをオンにします。

   Cisco SD-WAN Manager クラスタの場合は、クラスタ内の各 Cisco SD-WAN Manager インスタンスのスイッチをオンにします。

6. [Submit] をクリックします。

   スナップショットが作成されます。Cisco SD-WAN Manager のデータ量に応じて、作成プロセスは完了するまでに最大で 8 時間かかることがあります。

スナップショットの表示

はじめる前に

スナップショットの詳細を表示するには、オーバーレイ用にシスコがプロビジョニングしたクラウド ホスト コントローラ セットが必要です。

詳細については、「Cisco SD-WAN クラウドホスト型オーバーレイネットワークの作成」を参照してください。

スナップショットの詳細については、『スナップショットについて』を参照してください。

スナップショットの表示

1. Cisco Catalyst SD-WAN ポータル ダッシュボードから、使用可能なオーバーレイのリストに移動します。

   [Dashboard] > **[Overlays]** ページが表示されます。

2. スナップショットを表示するオーバーレイの名前をクリックします。

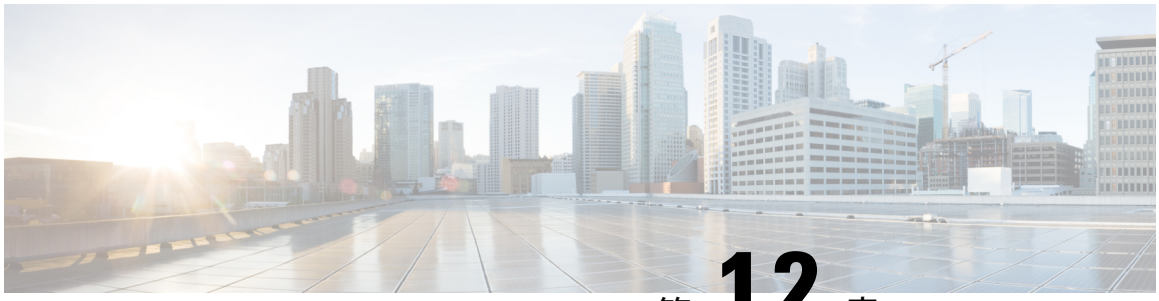
3. **[Dashboard]** > **[Cisco Hosted Overlays]** > **[Details]** ページで、[Snapshot] のタイルをクリックします。

   [Dashboard] > **[Cisco Hosted Overlays]** > **[Details]** > **[Snapshots]** ページが表示されます。

表 *6:* スナップショットフィールド

フィールド	説明
[Snapshot ID (*denotes golden snapshot)]	スナップショット ID を指定します。 スナップショットがゴールデンスナップショットの場合は、アスタリスクで示されます。
[Name]	スナップショットの名前を指定します。
[Version]	Cisco SD-WAN Manager ソフトウェアのバージョン番号を指定します。
[Progress]	スナップショット作成プロセスの進行状況を指定します。
[Duration]	スナップショット作成プロセスの期間を指定します。
[State]	スナップショット作成プロセスの状態を指定します。
[Device]	Cisco SD-WAN Manager でスナップショットが取得されたディスクを指定します。デバイスが最初にプロビジョニングされたバージョンに応じて、Cisco SD-WAN Manager インスタンスには 2 つまたは 3 つのディスクがあります。 ディザスタリカバリを成功させるには、同時に取得したすべてのディスクのスナップショットを使用して、Cisco SD-WAN Manager インスタンスのリカバリと構築を行います。

フィールド	説明
[Golden]	スナップショットがゴールデンスナップショットかどうかを指定します。 使用可能な値は次のとおりです。 • **false** • **true**
[Region]	このスナップショットが保存されるリージョンを指定します。
[Type]	スナップショットのタイプを指定します。 使用可能な値は次のとおりです。 • [REGULAR] • [ON-DEMAND] • [Golden]
[Overlay ID]	オーバーレイ ID を指定します。
[Overlay]	オーバーレイの名前と ID を指定します。
[Instance ID]	Cisco SD-WAN Manager インスタンス ID を指定します。
[Instance]	Cisco SD-WAN Manager インスタンスの名前と ID を指定します。
[Actions]	[Make Golden Snapshot] をクリックして、特定の日付のスナップショットをゴールデンとしてマークします。



第 12 章

ウェブフック

ウェブフックについて

ウェブフックは、2 つのシステム間で HTTP を介して通信する方法であり、指定したイベントによって開始できます。Cisco Catalyst SD-WAN ポータルは、ファブリックに関するイベント通知を送信するためのウェブフックの使用をサポートしています。Cisco SD-WAN ポータルの **[Administration Settings]** エリアのタブでウェブフックを設定および管理できます。

ウェブフックの設定

手順

ステップ 1 Cisco SD-WAN ポータルメニューで **[Administration]** をクリックし、**[Admin Settings]** を選択します。

ステップ 2 **[Webhooks]** タブを選択します。

ステップ 3 **[Configure Webhook]** をクリックします。

ステップ 4 次の情報を入力または選択します。

- スマートアカウント名
- バーチャルアカウント名
- ウェブフックエンドポイントの URL（https:// で始まる）
- 承認タイプ：基本（ユーザー名/パスワード）またはなし

ステップ 5 [Add] をクリックします。

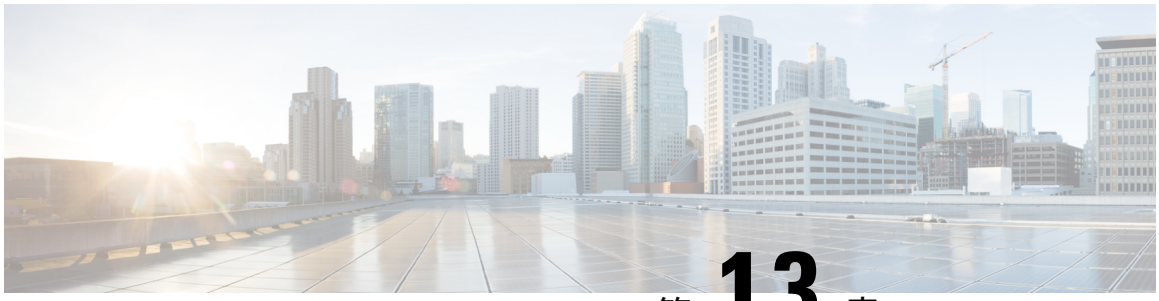
定義済みのウェブフックのテーブルが表示されます。

ウェブフック通知の送信

手順

ステップ 1 定義済みのウェブフックのテーブルで、編集するウェブフックを右クリックして **[Send]** を選択します。

ステップ 2 ウェブフックサーバーに送信するウェブフックのプレーンテキスト通知を入力し、**[Send]** をクリックします。
通知がウェブフックサーバーに送信されます。



第 13 章

トラブルシューティング

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

期限切れ IdP 証明書の更新

期限切れのアイデンティティプロバイダー（IdP）証明書を更新するには、[Sign In] ウィンドウの Cisco Catalyst SD-WAN ポータル の下にある [Need help signing in] リンクを使用します。

1. Cisco Catalyst SD-WAN ポータル URL に移動します。
2. [Need help signing in] リンクをクリックします。
3. [Need to reset IDP] リンクをクリックします。

   シスコアカウントにリダイレクトされます。
4. シスコのログイン情報を入力します。

5. プロンプトが表示されたら、MFA ログイン情報をセットアップまたは入力します。

誤って設定された IdP のリセット

IdP の設定に誤りがあり、ログインできない場合は、新しい IdP を設定できます。

1. Cisco Catalyst SD-WAN ポータル URL に移動します。
2. [Need help signing in] リンクをクリックします。
3. [Need to reset IDP] リンクをクリックします。

   シスコアカウントにリダイレクトされます。
4. シスコのログイン情報を入力します。
5. プロンプトが表示されたら、MFA ログイン情報をセットアップまたは入力します。

IdP の削除

1. Cisco Catalyst SD-WAN ポータル URL に移動します。
2. [Need help signing in] リンクをクリックします。
3. [Need to reset IDP] リンクをクリックします。
4. シスコアカウントにリダイレクトされます。
5. シスコのログイン情報を入力します。
6. プロンプトが表示されたら、MFA ログイン情報をセットアップまたは入力します。
7. [IdP details, actions] に移動し、IDP を削除します。

IdP を Cisco Catalyst SD-WAN ポータル から削除できるのは IdP 管理者のみです。IdP 管理者がアクティブでなくなった場合は、TAC ケースをオープンします。

スマートアカウントに関する問題のトラブルシューティング

問題

Cisco Catalyst SD-WAN ポータル へのログイン後、スマートアカウントは [Smart Account] ドロップダウンリストに表示されません。

これは通常、スマートアカウントに関連付けられた SD-WAN 対応属性がない場合に発生します。

ソリューション

Cisco DNA サブスクリプションをスマートアカウントとバーチャルアカウントに関連付けます。

詳細については、「コントローラをプロビジョニングするためのスマートアカウントとバーチャルアカウントのワークフロー」を参照してください。

Cisco Catalyst SD-WAN テクニカルサポートに連絡して、スマートアカウントを Cisco DNA クラウドサブスクリプションに関連付けます。

バーチャルアカウントに関する問題のトラブルシューティング

問題

Cisco Catalyst SD-WAN ポータル でバーチャルアカウントが SD-WAN に対応していないというエラーが表示されます。

このエラーは、Cisco DNA サブスクリプションがバーチャルアカウントに関連付けられていないことを示します。

ソリューション

エンタープライズ アグリーメントをお持ちのお客様の場合、SD-WAN 対応属性へのバーチャルアカウントの自動関連付けは使用できません。

企業のお客様としてバーチャルアカウントを Cisco DNA サブスクリプションに関連付けるには、次の手順を実行します。

1. CloudOps チームがコントローラをプロビジョニングするには、エンタープライズアグリーメント ワークスペースを介してクラウドコントローラのプロビジョニング要求フォームを送信します。
2. Cisco Catalyst SD-WAN テクニカルサポートに連絡して、目的のバーチャルアカウントを Cisco Catalyst SD-WAN ポータル で使用できるように依頼してください。
3. 目的のバーチャルアカウントが Cisco Catalyst SD-WAN ポータル で使用可能になったら、必要なエンタープライズアグリーメント契約情報を提供した後で、コントローラをプロビジョニングできます。

詳細については、「スマートアカウントとバーチャルアカウント」を参照してください。

詳細については、「コントローラをプロビジョニングするためのスマートアカウントとバーチャルアカウントのワークフロー」を参照してください。

バーチャルアカウントをCisco DNAサブスクリプションに関連付けることができない場合は、Cisco Catalyst SD-WAN テクニカルサポートに連絡して、バーチャルアカウントを Cisco DNA クラウドサブスクリプションに関連付けてください。

ブラウザのセキュリティ問題のトラブルシューティング

問題

次のエラーが表示されます：

```
CSRF Failed: CSRF token missing or incorrect
```

クロスサイト リクエスト フォージェリ（CSRF）トークンの不一致は、ブラウザでセキュア Cookie が作成できないか、ブラウザがログイン用の Cookie にアクセスできないというエラーです。

ソリューション

このエラーは、Web ブラウザの特定のセキュリティ設定が原因で発生します。

ブラウザのキャッシュをクリアするか、別のブラウザを試してください。

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。