Cisco SD-WAN セルフサービス ポータル コンフィギュレーション ガイド

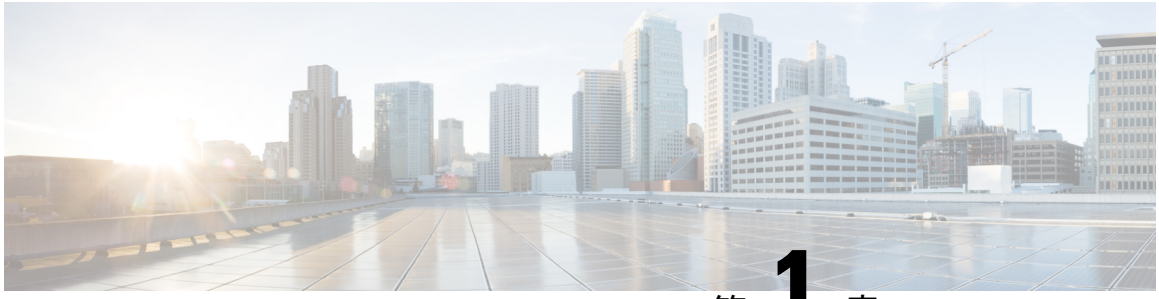
初版：2022 年 12 月 26 日

最終更新：2022 年 10 月 20 日

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

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

目 次



第 1 章

最初にお読みください

参考資料

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

ユーザマニュアル

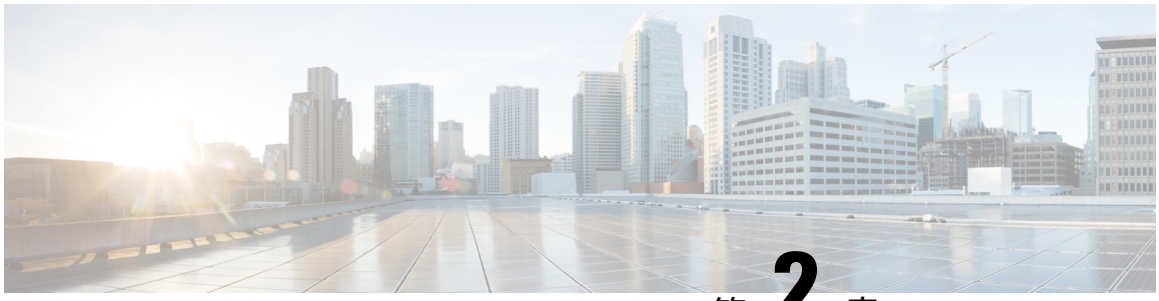
- Cisco IOS XE (Cisco IOS XE SD-WAN Devices)[英語]
- Cisco IOS XE (SD-WAN) Qualified Command Reference[英語]
- Cisco IOS XE（SD-WAN）リリース 17 のユーザーマニュアル

通信、サービス、およびその他の情報

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

マニュアルに関するフィードバック

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



第 2 章

Cisco SD-WAN セルフサービスポータル

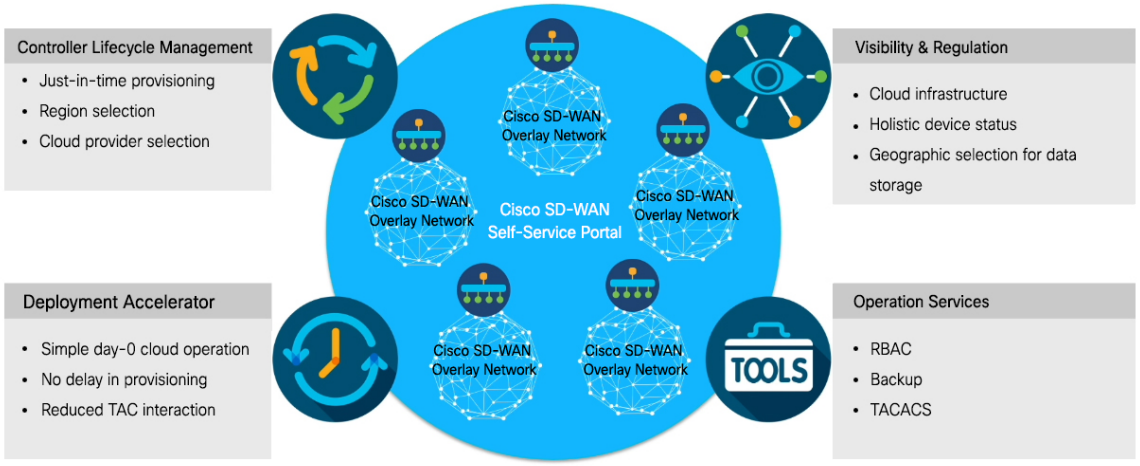
Cisco SD-WAN セルフサービスポータル の概要

Cisco SD-WAN セルフサービスポータル は、Cisco 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 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 SD-WAN セルフサービスポータル 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 vManage
- Cisco vBond オーケストレーション
- Cisco vSmart コントローラ

図 *1 : Cisco SD-WAN* セルフサービスポータル の利点と運用



アイデンティティプロバイダー（IdP）を使用してポータルアクセスの多要素認証（MFA）を有効にするように Cisco SD-WAN セルフサービスポータル を設定できます。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 IdP を使用するように Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービス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
- 既存のスマートアカウントを作成または使用します。
- 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 SD-WAN セルフサービスポータルの利点

- 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 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ユーザー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 SSO に IdP を使用したセキュア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 SD-WAN セルフサービスポータル について、シスコは Cisco SD-WAN セルフサービスポータルにスマートアカウント管理者へアクセスする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、顧客のホスト型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 SD-WAN セルフサービスポータル 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 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 SD-WAN コントローラをプロビジョニングするには、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。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 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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。

PCI DSS 認定

表 *1:* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN オーバーレイネットワークにおける PCI DSS レベル 1 認定のサポート	2022 年 2 月リリース	この機能により、Cisco SD-WAN オーバーレイネットワークに対してクレジットカードデータ保護基準（PCI DSS）レベル 1 認定が提供されます。決済カード業界（PCI）コンプライアンスは、カード所有者データのデータ漏洩から Cisco SD-WAN オーバーレイネットワークを保護します。

PCI DSS 認定に関する情報

PCI DSSとは、クレジット カード情報を受信、処理、保存、転送するすべての企業が安全性の高い環境を維持できるように設計された業界の情報セキュリティ規格です。詳細については、PCI セキュリティ規格審議会の Web サイトを参照してください。

クレジットカード情報を扱う企業は、機密性の高い金融データが盗まれる可能性を減らす安全性の高い方法でデータを維持する必要があります。加盟店がクレジットカード情報を安全に処理できないと、そのデータが侵害され、不正な購入に使用される可能性があります。さらに、カード所有者に関する機密情報は、ID 詐欺で使用される可能性があります。

Cisco SD-WAN は、カード所有者データを直接保存または処理しませんが、Cisco SD-WAN はクラウド サービス プロバイダー（CSP）と見なされます。

Cisco SD-WAN ソフトウェア コントローラ バージョン 20.6.1 では、Cisco SD-WAN ソリューションは PCI DSS レベル 1 のサービスプロバイダーとして認定されています。

（注） Cisco SD-WAN ソフトウェア コントローラ バージョン 20.6.1にアップグレードしても、PCI 認定を受けているということにはなりません。Cisco SD-WAN 認定ソフトウェア コントローラ バージョン 20.6.1 を購入する必要があります。Cisco vManage リリース 20.6.1 とともにリリースされた認定 Cisco SD-WAN ソフトウェアコントローラのみが PCI 認定を受けています。

Cisco SD-WAN コントローラ ソフトウェア バージョン 20.6.1 の PCI DDS 認定は、ネットワークに Cisco SD-WAN ソリューションを持ち、以前に PCI DDS に準拠していると認定されていた既存のお客様には影響しません。ネットワークの PCI DDS 認定を取得を希望する新規のお客様は、Cisco SD-WAN 認定ソフトウェア コントローラ バージョン 20.6.1 を購入することをお勧めします。

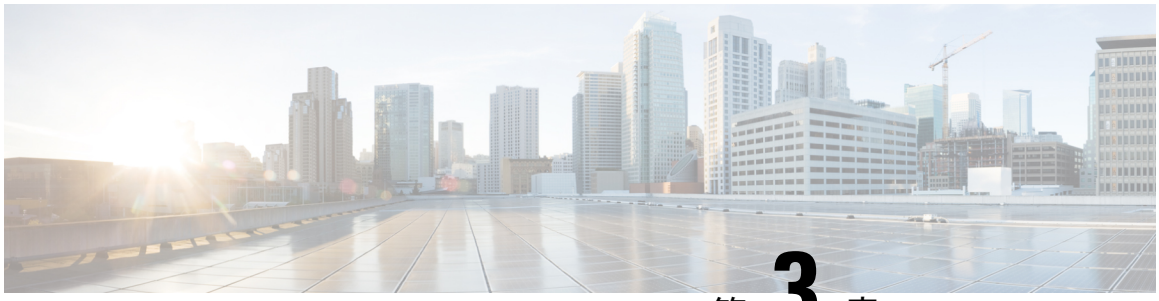
Cisco SD-WAN ソリューションには、PCI DSS 要件に沿ったセキュリティ制御が含まれています。シスコのお客様の多くは、Cisco SD-WAN をネットワークにおける不可欠な部分として使用することで、PCI DSS 認定バージョン 3.2.1 を取得しています。

クラウドコントローラの PCI DSS 認定に関してご質問がある場合は、Cisco SD-WAN テクニカルサポートにお問い合わせください。

PCI DSS 認定の前提条件

- PCI 認定オーバーレイは、クラウドの導入にのみ適用されます。
- クラウドプロバイダーとして Amazon Web Services（AWS）を使用していることを確認します。
- Cisco vManage リリース 20.6.1 または他の後続の延長サポートリリースを使用していることを確認します。標準サポートリリースを含む他のリリースバージョンは、PCI DSS 認定を受けていません。

  延長サポートリリースの詳細については、「16.x.x 以降の Cisco IOS ソフトウェアリリースの Cisco IOS XE ソフトウェア サポート タイムライン」を参照してください。



第 3 章

Cisco SD-WAN セルフサービスポータルにアクセス

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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 vManage 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 SD-WAN セルフサービスポータル を使用した Cisco 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] を選択し、[Manage Account] をクリックします。
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. [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。

PCI 認定オーバーレイのワークフロー

新規お客様向けの PCI 認定オーバーレイのワークフロー

1. 新規の Cisco 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） PCI 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 PCI 認定オーバーレイのワークフロー

1. 既存の Cisco 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 PCI 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 SD-WAN セルフサービスポータル へのアクセス

Cisco SD-WAN セルフサービスポータル 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 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル にログインすることはできません。Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータルへのログイン

Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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

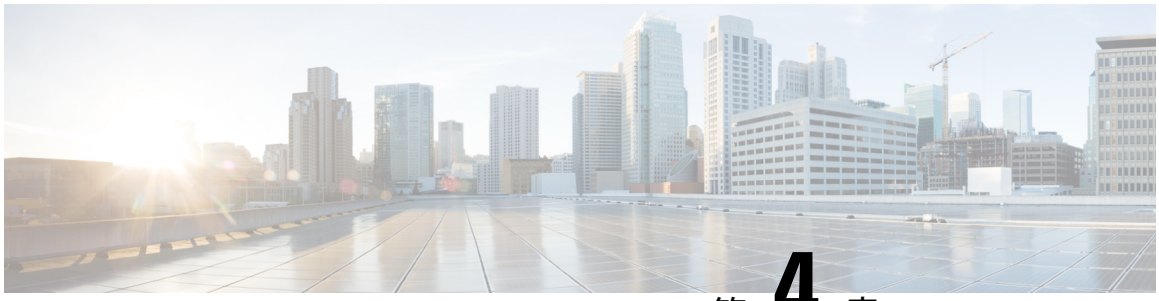
Cisco SD-WAN ポータルを使用して、追加の MFA オプションを追加したり、既存の MFA オプションを更新したりできます。

はじめる前に

Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 4 章

ID プロバイダーの設定

Cisco SD-WAN セルフサービスポータル の IdP の設定

Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル を設定するオプションがあります。

（注） Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル で IdP を設定し、Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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。

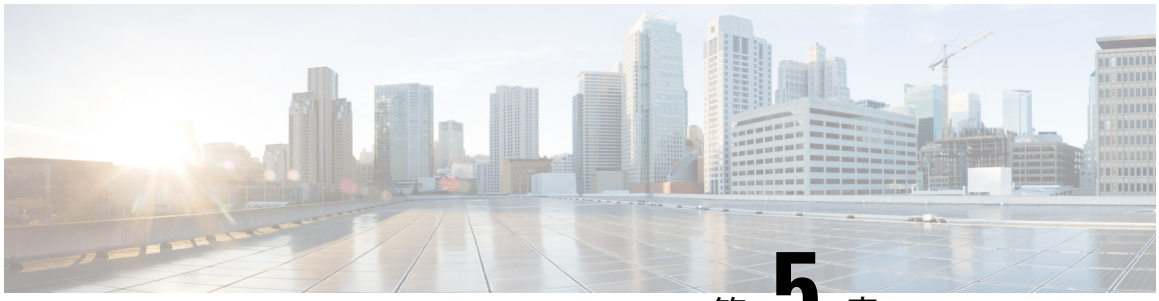
• firstName

- 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 SD-WAN セルフサービスポータル 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 5 章

ロールベースのアクセスの管理

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

はじめる前に

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

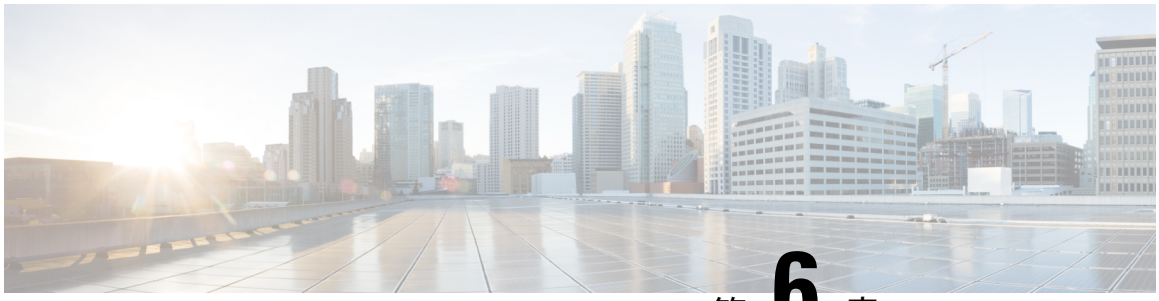
IdP ユーザーのロールの設定

1. Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 6 章

オーバーレイネットワークの管理

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

1. Cisco SD-WAN セルフサービスポータル メニューから [Create Overlay] を選択します。
2. [Select Smart Account] ドロップダウンリストから、オーバーレイネットワークを関連付けるスマートアカウントの名前を選択します。

   [Account Name] または [Domain ID] でスマートアカウントを検索できます。
3. [Overlay] ドロップダウンリストから、オーバーレイネットワークを関連付けるバーチャルアカウントの名前を選択します。
4. [Next] をクリックします。
5. [Select the Cloud Type and Version below] で、クラウドプロバイダーとして [Amazon Web Services AWS] または [Azure] を選択します。
6. [Select the appropriate version you would like to use] で、ドロップダウンリストから Cisco vManage バージョンを選択します。
7. [Next] をクリックします。
8. [Primary] で、クラウドホスト型コントローラのプライマリの場所を選択します。
9. [Secondary] で、クラウドホスト型コントローラのセカンダリの場所を選択します。

（注） 地理的な冗長性を実現するために、プライマリとセカンダリの異なる場所を選択することを推奨します。

10. [Location] で、モニタリングデータを保存する場所を選択します。
11. [Next] をクリックします。
12. [Overlay Admin(s)] で、オーバーレイ管理者の電子メールアドレスを入力します。
13. [Cisco Contact(s)] で、シスコの営業担当者またはアカウント担当者の電子メールアドレスを入力します。
14. [Overlay Status] で、ドロップダウンリストから [PROD] を選択します。
15. [Summary] をクリックします。
16. リクエストの概要を確認し、必要に応じて変更します。
17. （オプション）サブネット、ドメインネームシステム（DNS）名、組織名、またはスナップショット設定をカスタマイズするには、[Advanced Options] で [Edit] をクリックします。

    詳細オプションを指定すると、特定の使用例に必要なカスタムパラメータ入力を指定できます。詳細オプションは必須ではありませんが、使用例で必要な場合は、オーバーレイネットワークをプロビジョニングする前に詳細オプションを設定します。

（注） オーバーレイネットワークがプロビジョニングされると、詳細オプションは変更できません。

- [カスタムサブネット]
  - [Primary Subnet] および [Secondary Subnet] 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カスタム IP プレフィックスを指定します。最大 3 つのサブネットを指定できます。

    エンタープライズ TACACS、認証、許可、アカウンティング（AAA）、syslog サーバーへの接続、またはオーバーレイネットワー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（オーバーレイ内で一意で未使用のプレフィックス）にプライベートIPアドレスを指定してコントローラを展開することをお勧めします。

    オーバーレイの作成プロセス中に、リージョンごとに 1 つずつ、合計 2 つの /24 IP プレフィックスを指定します。

（注） 指定された IP プレフィックス（/24）がネットワーク内で一意であることを確認してください。

プライマリ サブネット フィールドとセカンダリ サブネット フィールドのそれぞれに /24 プレフィックスを入力し、次に**サブネット 1**、**サブネット 2**、および**サブネット 3** の下に 3 つの包括的 /26 サブネットを入力します。

たとえば、IP プレフィックス 10.6.117.0/24 は、次の 4 つの /26 サブネットに分割できます。

- 10.6.117.0/26
- 10.6.117.64/26
- 10.6.117.128/26
- 10.6.117.192/26

3 つのサブネットのいずれかを指定できます。両方のリージョンで同じ操作を実行します。

サブネットは次の順序で使用されます。

- サブネット 1：VPN 512
- サブネット 2：VPN 0
- サブネット 3：VPN 0（Cisco vManage インターフェイスのクラスタ専用）

- [vEdge Cloud router] フィールドで、[Enable] をクリックして、TACACS ベースのユーザー認証および認可用に vEdge クラウドルータ をプロビジョニングします。

- [Custom Domain Settings]

  DNS 名オプションを使用すると、DNS のホスト部分のカスタム名を設定できます。

  - Cisco vBond オーケストレーション のカスタム DNS 名を入力します。
  - Cisco vManage のカスタム DNS 名を入力します。

- [Snapshot Settings]
  - 次のいずれかからスナップショットを取得する頻度を選択します。
    - **1 日に 1 回**
    - **2 日に 1 回**
    - **3 日に 1 回**
    - **4 日に 1 回**

最大 10 個のスナップショットを選択できます。

（注） 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。

- [Custom Organization Name]

  オーバーレイネットワークのカスタム組織名を入力します。

  [Organization Name] オプションを使用すると、オーバーレイのすべての単一ノードで設定される組織の特定の名前を選択できます。組織名は、オーバーレイの一意の ID を提供します。

18. 入力した詳細を確認します。
19. [Submit Request] をクリックします。
20. 一意のコントローラパスワードが表示されます。作成後にオーバーレイネットワークにアクセスするには、このパスワードを使用します。

（注） 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。

コントローラのパスワードは 7 日後に Cisco SD-WAN セルフサービスポータル から削除されるため、パスワードを変更しない場合は、コントローラのパスワードのコピーを保存することを推奨します。

21. Cisco vManage にログインした後、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の詳細については、「Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above」[英語]を参照してください。

22. 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」[英語]を参照してください。

スナップショットについて

Cisco SD-WAN クラウドホスト型サービスには、Cisco vManage 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 セルフサービスポータル 用に計画されている主要な変更時間帯については、Cisco SD-WAN CloudOps チームへの Cisco TAC サポートリクエストを使用して、ネットワークオーバーレイ設定のオンデマンドスナップショットをリクエストできます。オンデマンドスナップショットを取得して完了するには、変更時間帯の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。このオンデマンドスナップショット1つは、スナップショットの作成日から3か月間保存されます。新しいスナップショットは、それぞれ古いオンデマンド スナップショットに置き換わります。

- 日次スナップショット

  日次スナップショットは、指定された Cisco vManage 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 10 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 10 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。

  [Advanced Options] > **[Edit]** をクリックし、次に [Snapshot Settings] をクリックして、Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 vSmart コントローラ と Cisco vBond オーケストレーション 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 vManage テンプレートを使用して Cisco vBond オーケストレーション および Cisco vSmart コントローラ を設定し、保存します。

（注） スナップショットはCisco SD-WANセルフサービスポータルのクラウドアカウント内に保存されるため、Cisco SD-WANセルフサービスポータル スナップショットのダウンロードはできません。Cisco SD-WAN セルフサービスポータル 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

  既存の日次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、自動的に削除されることがなくなります。ゴールデンスナップショットは最大1つ保存できます。新しい日次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ている場合、ゴールデンタグは以前のスナップショットから自動的に削除されます。その古いスナップショットは、スナップショットタイプの失効プロセスに従って削除される可能性があります。

  Cisco vManage 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 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 vManage 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。

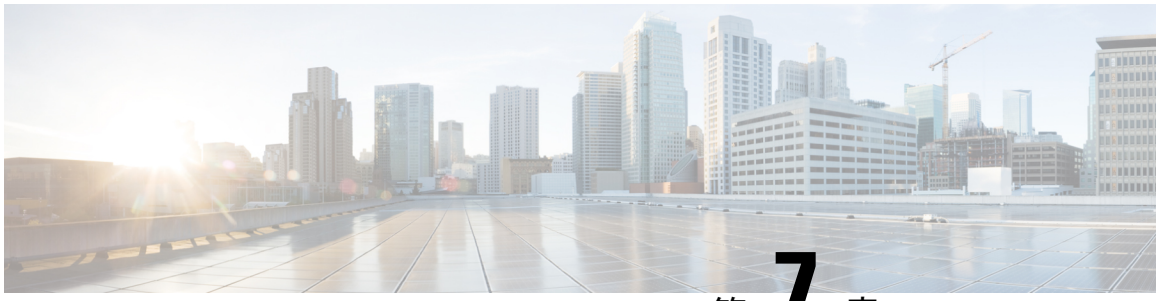
- オーバーレイごとに最大 200 のルールを追加できます。
- 各ルールは、オーバーレイ内のすべてのクラウドホストコントローラに一律に適用されます。
- 新しいクラウドホスト型インスタンスが追加されるか、既存のインスタンスが置き換えられた場合は、同じルールが自動的に適用されます。ルールは、単一の IP アドレスまたはより大きな IP プレフィックスのいずれかです。

1. Cisco SD-WAN セルフサービスポータル 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. ドロップダウンリストから、[Cisco Hosted Overlays] をクリックします。

   オーバーレイネットワークのリストが表示されます。
3. オーバーレイネットワークの名前をクリックします。
4. [Inbound Rules] 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。
6. [Enter] を押して、送信元 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。
7. [Add] をクリックします。
8. （任意）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。
9. [Save] 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 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 7 章

オーバーレイネットワークのモニタリング

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

1. Cisco SD-WAN セルフサービスポータル ダッシュボードで、オーバーレイをクリックします。

   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] タブで、[Cisco vManage]、[Cisco vBond Orchestrator]、[Cisco vSmart Controller]、[Cisco vEdge Cloud] などモニタリングするコントローラをクリックします。
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、コントローラの状態、タイプ、またはIPアドレスでフィルタリングすることもできます。

オーバーレイとコントローラの詳細の表示

1. Cisco SD-WAN セルフサービスポータル ダッシュボードで、詳細を表示す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 *2:* 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 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 SD-WAN セルフサービスポータル 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 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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。

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 SD-WAN セルフサービスポータル 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。

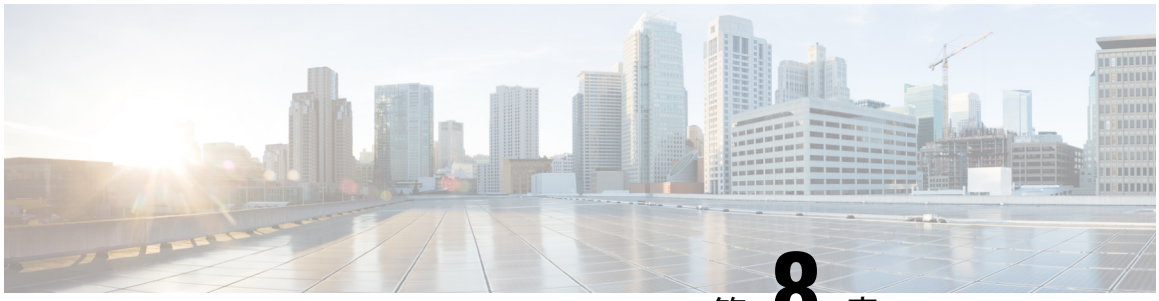
3. **[Dashboard]** > **[Cisco Hosted Overlays]** > **[Details]** ページで、[Snapshot] のタイルをクリックします。

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

表 *3*: 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 vManage 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。

フィールド	説明
[Device]	Cisco vManage 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 vManage 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 vManage インスタンスのリカバリと構築を行います。
[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 vManage インスタンス ID を指定します。
[Instance]	Cisco vManage 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 8 章

トラブルシューティング

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 SD-WAN セルフサービスポータル の下にある [Need help signing in] リンクを使用します。

1. Cisco SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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。

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 SD-WAN セルフサービス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 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 SD-WAN セルフサービスポータル 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 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 SD-WAN セルフサービスポータル 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 SD-WAN セルフサービスポータル 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 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。