



Cisco SD-WAN Cloud ガイド

最終更新：2025年10月15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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2025 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	最初にお読みください	1
-------	------------	---

第 2 章	使用する前に	3
	Cisco SD-WAN Cloud プラットフォーム	3
	Cisco SD-WAN Cloud の前提条件	4
	Cisco Catalyst SD-WAN ポータルでのファブリックの作成	4
	Cisco SD-WAN Cloud ファブリックの作成	4
	ユーザーロールの追加	5
	Cisco Catalyst SD-WAN Manager へのアクセス	6
	スマートアカウントから Cisco SD- WAN Manager へのデバイスの追加	7
	ファブリックの Cisco Catalyst SD-WAN Analytics へのアクセス	7

第 3 章	デバイスのアップグレードと更新	9
	新しいデバイスソフトウェアのインストール	9

第 4 章	Cisco SD- WAN Cloud-Pro から Cisco SD- WAN Cloud への移行	11
	Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行	11
	移行に関する FAQ	13

第 5 章	Cisco SD- WAN Cloud での Cisco API の使用	19
	Cisco SD- WAN Cloud 用 Cisco API に関する情報	19
	Cisco API キーの取得	19
	Cisco API キーの使用に関する制限事項	21
	Cisco API 要求の例	22



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]
- [User Documentation for Cisco SD-WAN Release 20](#) [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

使用する前に

- [Cisco SD-WAN Cloud プラットフォーム](#) (3 ページ)
- [Cisco SD-WAN Cloud の前提条件](#) (4 ページ)
- [Cisco Catalyst SD-WAN ポータルでのファブリックの作成](#) (4 ページ)
- [ユーザーロールの追加](#) (5 ページ)
- [Cisco Catalyst SD-WAN Manager へのアクセス](#) (6 ページ)
- [スマートアカウントから Cisco SD-WAN Manager へのデバイスの追加](#) (7 ページ)
- [ファブリックの Cisco Catalyst SD-WAN Analytics へのアクセス](#) (7 ページ)

Cisco SD-WAN Cloud プラットフォーム

Cisco SD-WAN Cloud ネットワーキング ソリューション（以前の「クラウド提供型 Catalyst SD-WAN」）は、Cisco Catalyst SD-WAN サービス向けのプラットフォームであり、次の特徴を備えています。

- Cisco Catalyst SD-WAN ファブリックの運用タスクを削減および簡素化します。
- 柔軟にクラウドを利用でき、運用が簡素化され、Cisco Catalyst SD-WAN に含まれる包括的な分析機能を利用できます。
- ファブリックの運用上のほとんどすべての責任はシスコが管理し、お客様が管理するのはエッジデバイスとエッジネットワークのみです。
- ネットワークリソースが限られているために Cisco Catalyst SD-WAN ファブリックを稼働させる際の運用上の負担を抑える必要がある小規模または中規模のビジネスに最適です。

Cisco SD-WAN Cloud の制限事項

Cisco SD-WAN Cloud プラットフォームは、次の機能のいずれかを必要とする場合、お客様のビジネスニーズを満たさない可能性があります。

- BYO-IDP（Bring Your Own Identity Provider、お客様独自のアイデンティティプロバイダーの持ち込み）
- SDA、Trustsec、ACI などの、Identity Services Engine（ISE）との統合

- マルチリージョン ファブリック (MRF)
- AAA /TACACS/SYSLOG のクラウドゲートウェイ
- 制御コンポーネントの正確な配置場所に対する要件 (データ主権などのため)

これらに該当する場合は、『[Cisco Catalyst SD-WAN Portal Configuration Guide](#)』で Cisco SD-WAN Cloud-Pro 専用ファブリックの作成手順を参照してください。

このガイドでは、Cisco SD-WAN Cloud の初期セットアップと設定の手順について説明します。Cisco Catalyst SD-WAN ポータルから次の手順を実行します。このポータルには、Cisco SD-WAN Cloud でファブリックの管理ツールを作成してアクセスするためのオプションが用意されています。

Cisco SD-WAN Cloud の前提条件

- 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。

これは、Catalyst SD-WAN Manager 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。その後は必要ありません。

- Cisco Commerce サイト (旧称 Cisco Commerce Workspace) での DNA Cloud サブスクリプションまたは有料 SD-WAN 制御コンポーネント SKU の有効な注文。

Cisco Catalyst SD-WAN ポータルでのファブリックの作成

Cisco Catalyst SD-WAN ポータルにログインすると、次を実行できます。

- Cisco SD-WAN Cloud ファブリックをデフォルトで作成する。
- Cisco SD-WAN Cloud-Pro 専用ファブリックの要求に関する情報を検索する。

Cisco SD-WAN Cloud ファブリックの作成

Cisco SD-WAN Cloud は、米国、EU、およびアジア太平洋地域の限られた場所でのみ利用できます。Cisco SD-WAN Cloud ファブリックで利用可能な場所とは別の特定の場所で Cisco Catalyst SD-WAN ファブリックをホストするには、Cisco SD-WAN Cloud-Pro 専用ファブリックをプロビジョニングします。

始める前に

Cisco SD-WAN Cloud ファブリックを追加するには、有効なスマートアカウントとバーチャルアカウントが必要です。

手順

ステップ 1 CCO ユーザー名とパスワードを使用して、Cisco Catalyst SD-WAN ポータル (<https://ssp.sdwan.cisco.com>) にログインします。

ステップ 2 [SD-WAN Customer] ロールを選択します。

ステップ 3 [Cisco Catalyst SD-WAN Portal Dashboard] で、[Create Fabric] をクリックします。

ステップ 4 ファブリックタイプとして [SD-WAN Cloud] を選択します。

これらの手順は、Cisco SD-WAN Cloud ファブリックにのみ適用されます。

ステップ 5 [Create Fabric] ページで、次の手順を実行します。

a) 自身のスマートアカウントとバーチャルアカウントを選択します。

b) [Fabric Name]、[Fabric Location]、[Fabric Admin(s)]、[Release Category] を入力または選択します。

- [Recommended] リリースカテゴリでは、バグ修正に加えて、新機能と新しいハードウェアプラットフォームのサポートが提供されます。このカテゴリでは、最大の安定性と信頼性が提供されません。
- [Early Adopter] リリースカテゴリ（使用場所で利用可能な場合）では、新機能と拡張プラットフォームサポートが提供されますが、バグ修正のために、より頻繁なメンテナンスと更新が必要になる場合があります。

(注)

選択して入力したすべての情報は、ページの右側のパネルにある [Preview] セクションに表示されます。

ステップ 6 [Preview] セクションで利用規約に同意します。

ステップ 7 ダッシュボードで [Create Fabric] をクリックします。

ファブリックが作成されたことが電子メールで通知されます。

次のタスク

Cisco Catalyst SD-WAN ポータル にログインし直すことで、ファブリックへのアクセスを開始できます。

ユーザーロールの追加

ロールは、ユーザーが読み取り専用モードでアクセスできる Cisco Catalyst SD-WAN Manager 機能と、読み取りおよび書き込み権限でアクセスできる機能を決定します。

ファブリックを作成すると、そのファブリックの管理者ロールが自動的に付与され、他のユーザーのロールを設定できます。



(注) ユーザーに対してロールを追加するには、そのユーザーが Cisco Connection Online のアカウントを持っている必要があります。

1. ファブリックの管理者ロールで Cisco Catalyst SD-WAN ポータルにログインします。
2. [Show Details] をクリックします。
3. [Fabric Details] ページで [User Role] をクリックします。
4. [ユーザーの追加 (Add User)] をクリックします。
5. [User Email ID] フィールドに、ロールを追加するユーザーの CCO E メールアドレスを入力します。
6. [Role] ドロップダウンリストから、このユーザーが属するユーザーグループを選択します。
ユーザーグループは Cisco Catalyst SD-WAN Manager で設定されています。ユーザーグループによって、そのグループ内のユーザーが読み取り専用アクセス権を持つ機能と、読み取りおよび書き込みアクセス権を持つ機能が指定されます。
7. [Add] をクリックします。

Cisco Catalyst SD-WAN Manager へのアクセス

Cisco SD-WAN Manager には、ファブリックを設定、管理、およびモニタリングするためのオプションがあります。ユーザーロールを持つユーザーは、Cisco Catalyst SD-WAN ポータルに追加されると Cisco SD-WAN Manager にアクセスできます。

1. Cisco Catalyst SD-WAN ポータル (<https://ssp.sdwan.cisco.com>) にログインします。
Cisco Catalyst SD-WAN ポータルおよび Cisco SD-WAN Manager では、このログインでシングルサインオン認証を利用できます。
2. アクセスするファブリックの [Manage Fabric] をクリックします。



(注) SD-WAN Manager の URL をブックマークして、CCO の電子メールアドレスとパスワードを使用して SD-WAN Manager に直接アクセスすることもできます。

3. Cisco SD-WAN Manager を終了して Cisco Catalyst SD-WAN ポータルに戻るには、Cisco SD-WAN Manager のメニューから [SD-WAN Portal] を選択します。

スマートアカウントから Cisco SD- WAN Manager へのデバイスの追加

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 使用可能なファブリックのリストから、デバイスを追加するファブリックを選択して [Manage Fabric] をクリックします。
 - ステップ 3 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]**の順に選択します。
 - ステップ 4 **[Sync Smart Account]** をクリックします。
 - ステップ 5 **[Sync Smart Account]** ペインで、**[Sync]** をクリックします。
-

同期後、スマートアカウント内のデバイスが、選択したファブリックの Cisco SD-WAN Manager インスタンス内のエッジデバイスのリストに表示されます。

ファブリックの Cisco Catalyst SD-WAN Analytics へのアクセス

Cisco SD-WAN Analytics では、ファブリック内のデバイスの動作、トラフィック、および関連アクティビティに関する情報を確認できます。

1. ファブリックの管理者ロールを持つユーザーとして Cisco Catalyst SD-WAN ポータル にログインします。
2. ファブリックの Cisco Catalyst SD-WAN ページに移動します。
3. Cisco Catalyst SD-WAN のメニューから**[Analytics]** > **[Overview]**の順に選択します。

詳細については、[Cisco Catalyst SD-WAN Analytics](#)を参照してください。



第 3 章

デバイスのアップグレードと更新

- [新しいデバイスソフトウェアのインストール \(9 ページ\)](#)

新しいデバイスソフトウェアのインストール

リモートリポジトリサーバーを使用したソフトウェアの更新

シスコが管理しているリモートリポジトリサーバー (cloudopsremoterepo.sdwan.cisco.com) に保存されているソフトウェアイメージを使用して、ネットワーク内のデバイスのソフトウェアを更新できます。

ネットワーク内のデバイスがリモートサーバーからソフトウェア更新を受信できるようにするには、「[Enable Software Updates by a Remote Repository Server](#)」を参照してください。

エッジデバイスでサポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

イメージの要求

必要なソフトウェアイメージがリモートリポジトリに存在しない場合は、TAC ケースをオープンして要求してください。また、ネットワーク内のエッジデバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a より前のリリースを使用している場合は、TAC ケースをオープンしてソフトウェアイメージを要求してください。

必要なイメージについて、次の詳細情報を提供してください。

- 必要なイメージバージョン
- [ソフトウェアダウンロードポータル](#)上のイメージへのリンク
- Cisco SD-WAN Manager への接続に使用するリンク
- 組織名



第 4 章

Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行

- [Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行 \(11 ページ\)](#)
- [移行に関する FAQ \(13 ページ\)](#)

Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行

概要

Cisco SD-WAN Cloud-Pro を専用ファブリックと 800 台未満のデバイスで使用している場合は、Cisco SD-WAN Cloud に移行して、運用を簡素化し、日常のネットワーキング管理タスクを削減し、ファブリックを Cisco Catalyst SD-WAN コントローラポリシーに準拠させることを推奨します。

移行しない場合は、専用 Cisco SD-WAN Cloud-Pro ファブリック向けの制御コンポーネント SKU または管理アドオンを購入する必要があります。

移行プロセス

お客様が Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行の資格をお持ちの場合は、シスコからご連絡いたします。シスコは、お客様の資格を確認し、移行を完了するために必要な情報をお客様に要求します。

または、Technical Assistance Center (TAC) でケースをオープンして、クラウドオペレーションチームによる移行の実施をリクエストすることもできます。

移行に必要な情報を入力すると、移行を実施するメンテナンス期間のスケジュールを設定するため、48時間以内にシスコからご連絡いたします。ファブリック内にあるデバイスの数に応じて、移行には最大 6 時間かかる場合があります。

クラウドオペレーションチームがリモートで移行を実施します。何らかの問題によって移行が正常に行われない場合は、必要に応じてシスコが問題を解決してお客様にご連絡いたします。

移行が完了すると制御接続が自動的に再確立されるため、移行によるデータプレーンへの影響は最小限に抑えられます。

予想される移行の影響

- エンタープライズ証明書は Cisco SD-WAN Cloud ではサポートされません。
- カスタムサブネットは Cisco SD-WAN Cloud ではサポートされません。Cisco SD-WAN Cloud-Pro 専用ファブリック向けに設定されたカスタムサブネットは、移行中に削除されます。
- Cisco Catalyst SD-WAN Manager にアクセスするための新しい URL が生成されます。
 - この URL には、[Cisco Catalyst SD-WAN Portal](#) からアクセスできます。
 - Cisco Catalyst SD-WAN Manager にアクセスするための古い URL は使用できなくなります。
- Cisco SD-WAN Cloud-Pro 専用ファブリックのプロキシ設定は無効になります。
- Cisco SD-WAN Cloud-Pro 専用ファブリックの統計データは保持されません。
- Cisco SD-WAN Cloud-Pro 専用ファブリックの分析データは保持されません。
- Cisco SD-WAN Cloud-Pro 専用ファブリックのアイデンティティプロバイダー情報は保持されません。
- Cisco SD-WAN Cloud は、お客様独自のアイデンティティプロバイダー情報の設定には対応していません。
- Cisco SD-WAN Cloud では、インバウンドルールの設定は必要ありません。

移行の前提条件

Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud への移行を実行する前に、次の手順を実行します。

- 現在の専用ファブリックの Cisco スマートアカウントとバーチャルアカウントに、有効な Cisco SD-WAN Cloud ライセンスがあることを確認します。

これらのライセンスを取得する方法の詳細については、シスコ代理店にお問い合わせください。
- Cisco SD-WAN Cloud-Pro ファブリックを、Cisco SD-WAN Cloud の現在のバージョンと一致するようにアップグレードします。このバージョンについてはシスコからお知らせします。

アップグレード手順については、『[Upgrade SD-WAN Controllers with the Use of vManage GUI or CLI](#)』を参照してください。

- 要求された場合は、既存の Cisco SD-WAN Cloud-Pro のファブリックの netadmin ログイン情報をシスコにお知らせください。
- 必要に応じて、TACACS のクラウドゲートウェイとして使用しているすべての Cisco Catalyst 8000 エッジプラットフォームを削除します。Cisco SD-WAN Cloud は現在、TACACS のクラウドゲートウェイをサポートしていません。これらのプラットフォームを削除しない場合、移行後も存在しますが機能しません。

移行後

移行が完了すると、それまで使用していた Cisco SD-WAN Cloud-Pro のファブリックは動作しなくなります。新しい Cisco SD-WAN Cloud のファブリックには、[Cisco Catalyst SD-WAN ポータル](#)を使用してアクセスできます。詳細については、『[Cisco Catalyst SD-WAN Portal Configuration Guide](#)』を参照してください。

移行に関する FAQ

Cisco SD-WAN Cloud ファブリックの移行では、既存の Cisco SD-WAN Cloud-Pro 環境を Cisco SD-WAN Cloud 環境に移行します。これにより、拡張性が強化され、最新の機能が提供され、管理と分析が簡素化されます。

Cisco SD-WAN Cloud では、ネットワーク管理者がネットワーク エッジデバイスを管理することで運用が簡素化される一方で、シスコが SD-WAN 制御コンポーネントの運用上の責任を負います。また、柔軟なクラウドの利用、運用の簡素化、包括的な分析が可能になります。

Q. 移行を開始する前に完了する必要がある準備手順を教えてください。

A. 移行の前に、次の手順を行う必要があります。

- Cisco SD-WAN Cloud-Pro 制御コンポーネントに必要なソフトウェアのバージョンをシスコの担当者に問い合わせて、指定のバージョンにアップグレードします。
- エッジデバイスに必要なソフトウェアバージョンをシスコの担当者に問い合わせて、指定のバージョンにアップグレードします。

[Cisco SD-WAN 制御コンポーネントの互換性マトリックス](#)を使用して、SD-WAN 制御コンポーネントとデバイスの互換性を確認します。

- 到達不能または未使用のエッジデバイスのシリアル番号を、現在の SD-WAN Manager から削除します。
- すべてのエッジデバイスで、稼働している NTP サーバーおよび DNS サーバーが構成されていることを確認します。
- どのエッジデバイスにも SD-WAN Validator (旧 vBond) の完全修飾ドメイン名 (FQDN) の IP マッピングへの静的ホスト名が設定されておらず、エッジデバイスのシステ

ム設定で（SD- WAN Validator の正確な IP ではなく）SD- WAN Validator の FQDN 値が設定されていることを確認します。

- エッジデバイス、特にソフトウェアベースのデバイスにアウトオブバンド（OOB）のダイレクトアクセスが可能であることを確認します。これは、Cisco SD-WAN Cloud-Pro から Cisco SD-WAN Cloud ファブリックへの移行中の接続の問題に対処するために必要となる場合があります。

Q. 移行は一度に行う必要がありますか。または段階的に移行を実行できますか。

A. Cisco SD-WAN Cloud-Pro ファブリックから Cisco SD-WAN Cloud ファブリックへの実際の移行は、1回のメンテナンス期間で実行されます。これには、移行時および移行後のチェック、および移行が失敗した場合のリカバリが含まれます。

Q. 移行プロセスの所要時間はどのくらいですか。

A. 通常、移行には8時間の変更期間が必要ですが、これはファブリックのサイズによって異なります。

Q. 移行中の当事者間のコミュニケーションチャンネルにはどのようなものがありますか。

A. 移行中のコミュニケーションは、主にテクニカルアシスタンスセンター（TAC）のサポートケースを通じて行います。これにより、移行プロセス全体でスムーズな調整とサポートが確保されます。

Q. Cisco SD-WAN Cloud-Pro 制御コンポーネントとエッジデバイスのアップグレードを担当するのは誰ですか。

A. 移行準備の一環として、お客様が Cisco SD-WAN Cloud-Pro 制御コンポーネントとエッジデバイスの両方をアップグレードする必要があります。アップグレードに関してサポートが必要な場合は、CloudOps にお問い合わせください。Cisco SD-WAN Cloud に移行すると、SD- WAN 制御コンポーネントの今後のソフトウェアバージョンアップグレードはシスコが実施します。

Q. 移行リクエスト中に提供する必要がある情報は何か。

A. 以下を指定する必要があります。

- SD- WAN サブスクリプションの販売/Web 注文の詳細
- SD- WAN 制御コンポーネントのファブリック名と展開リージョン
- 連絡先電子メールアドレス
- 既存の Cisco SD-WAN Cloud-Pro 制御コンポーネントファブリックの SD- WAN Manager 管理者ログイン情報

Q. 移行中にはどのような注意事項がありますか。

A. トラブルシューティング用に、エッジデバイスへのアウトオブバンド（OOB）アクセスが可能であることを確認します。エッジサイトにファイアウォールがある場合は、エッジデ

デバイスが Cisco SD-WAN Cloud 制御コンポーネントの新しいパブリック IP アドレスと通信できるように、移行中にこのファイアウォールを更新する必要がある場合があります。

- Q.** 現在 Cisco SD-WAN Cloud-Pro 制御コンポーネントでエンタープライズ証明書を使用している場合、どのような手順が必要ですか。
- A.** 以下の手順を実行します。
1. 証明書を更新して、すべての SD-WAN 制御コンポーネントで PKI ベースの証明書に移行します。
 2. ルート CA バンドルがすべてのエッジデバイスにインストールされていることを確認します。
- Q.** 現在 Cisco SD-WAN Cloud-Pro 制御コンポーネントでエンタープライズ証明書を使用している場合、どのような手順が必要ですか。
- A.** 以下の手順を実行します。
1. 証明書を更新して、すべての SD-WAN 制御コンポーネントで PKI ベースの証明書に移行します。
 2. ルート CA バンドルがすべてのエッジデバイスにインストールされていることを確認します。
- Q.** 設定データは Cisco SD-WAN Cloud ファブリックへどのように転送されますか。
- A.** ポリシー、テンプレート、エッジデバイスのシリアル番号を含むすべての設定データが現在の SD-WAN Manager から抽出され、移行スクリプトを使用して新しい SD-WAN Manager に復元されます。
- Q.** 移行後、エッジデバイスは Cisco SD-WAN Cloud ファブリックに自動的に接続されますか。
- A.** 移行スクリプトが新しい設定をプッシュすると、エッジデバイスは以前に設定されたポリシーを使用して認証を行い、Cisco SD-WAN Cloud ファブリックに接続します。
- Q.** 移行中に SD-WAN Analytics はオンボードされますか。
- A.** SD-WAN Analytics は、移行プロセス中に自動的に Cisco SD-WAN Cloud ファブリックに対して有効になります。
- Q.** プラグアンドプレイ (PnP) ポータルで設定されるコントローラプロファイルは、Cisco SD-WAN Cloud 環境で作成されますか。
- A.** コントローラプロファイルが、Cisco SD-WAN Cloud スマートアカウントとバーチャルアカウント (SA/VA) で、組織とサービスプロバイダーの組織名を使用して作成されます。

さらに、エンタープライズ SA/VA は、PnP の外部管理機能を使用して Cisco SD-WAN Cloud SA/VA にリンクされます。

- Q.** 変更期間中にデータプレーンは影響を受けますか。
- A.** 中断が最小限に抑えられるよう、変更期間中のダウンタイムを計画的に設定してください。予期しないイベントが発生する可能性があります、データプレーンは通常、この変更中は影響を受けません。
- Q.** 移行後の新しい環境にアクセスするにはどこでログインすればよいですか。
- A.** ユーザーは引き続き Cisco Catalyst SD- WAN ポータルを使用し、シングルサインオン (SSO) を使用して Cisco SD-WAN Cloud ファブリックと SD- WAN Manager ダッシュボードにアクセスします。
- Q.** 移行が成功したことを確認する方法を教えてください。
- A.** サポートチームから移行が完了したことが通知されます。次に、Cisco Catalyst SD- WAN ポータルにログインして Cisco SD- WAN Manager を開き、デバイスと設定を確認して、すべてが存在し、想定どおりに動作していることを確認します。
- Q.** 移行後にエッジデバイスに問題がある場合はどうすればよいですか。
- A.** サポートが制御接続の再確立を支援できるように、エッジデバイスへのアウトオブバンド (OOB) アクセスを提供してください。
- Q.** 移行後に自分の権限とロールが正しく設定されていることを確認する方法を教えてください。
- A.** Cisco Catalyst SD- WAN ポータルで **[Overlay Details] > [User]** を選択して、ユーザーロールの割り当てを確認し、必要に応じて更新します。問題が発生した場合は、サポートが支援します。
- Q.** ロールバックの場合、どのような準備が必要ですか。
- A.** エッジデバイスへのアウトオブバンド (OOB) アクセスを可能にして、SD- WAN Validator の DNS およびソース Cisco SD- WAN Manager にフォールバックするデバイスの組織 (sp-org-name) の値を更新します。
- Q.** この移行に関連するリスクを教えてください。
- A.** リスクには、一時的な接続喪失の可能性、デバイスの制御に関する問題、または不完全な移行などが含まれます。シスコは、これらのリスクを最小限に抑えるために、非常に厳格な手順に従います。
- Q.** 新しい Cisco SD-WAN Cloud ファブリックでデフォルトで有効になっている機能は何ですか。
- A.** SD- WAN Analytics と Cloud OnRamp for SaaS は、既存の Cisco SD-WAN Cloud-Pro 制御コンポーネントで以前に有効になっていなかった場合でも、デフォルトで有効になります。

また、Software-Defined Application Visibility and Control (SD AVC)、SSO、およびリモートソフトウェアアップグレードイメージリポジトリもシステムで有効になります。

- Q. 既存の SD-WAN Analytics とレポート機能は移行後も継続されますか。
- A. SD-WAN Analytics は引き続き機能し、レポート機能は変わらず維持されます。

- Q. Cisco SD-WAN Cloud-Pro 制御コンポーネントは移行後にどうなりますか。
- A. すべてのデバイスとデータが新しい Cisco SD-WAN Cloud ファブリックに移行された後に、現在の Cisco SD-WAN Cloud-Pro 制御コンポーネントが削除されます。

- Q. 移行後、SD-WAN 制御コンポーネントへの CLI アクセスは使用できますか。
- A. 移行後、SD-WAN 制御コンポーネントへの CLI アクセスは使用できません。

- Q. SD-WAN 制御コンポーネントのパブリック IP アドレスは変更されますか。
- A. SD-WAN 制御コンポーネントのパブリック IP アドレスが変更されたら、ファイアウォールルールを更新して新しい IP アドレスを許可します。Cisco SD-WAN Cloud のお客様は、TAC サポートケースを使用して、SD-WAN 制御コンポーネントのパブリック IP アドレスをいつでも SD-WAN Cloud インフラストラクチャ チームに要求できます。



第 5 章

Cisco SD- WAN Cloud での Cisco API の使用

- [Cisco SD- WAN Cloud 用 Cisco API に関する情報](#) (19 ページ)
- [Cisco API キーの取得](#) (19 ページ)
- [Cisco API キーの使用に関する制限事項](#) (21 ページ)
- [Cisco API 要求の例](#) (22 ページ)

Cisco SD- WAN Cloud 用 Cisco API に関する情報

この章では、Cisco SD- WAN Cloud リリース 20.15 以降で、Cisco SD- WAN Cloudファブリック上の Cisco API にアクセスし、これらを使用する方法について説明します。

Cisco SD- WAN Cloud のお客様が Cisco API にアクセスするには、API キーまたは JSON Web トークン (JWT) が必要です。

キーは、指定されたファブリックユーザーによる Cisco API の呼び出しに使用され、このユーザーが削除されるか、ユーザーロールが変更されるまで有効です。

Cisco API キーの取得

Cisco SD-WAN Cloud リリース 20.15 は、API キーを直接生成するメカニズムを提供します。次の手順に従って API キーを生成し、ゲートウェイ URL とクロスサイトリクエストフォージェリ保護 (CSRF) トークンの値を見つけます。

手順

ステップ 1 ファブリックにログインします。

ステップ 2 ユーザー ID の下にあるドロップダウンメニューから [My Profile] を選択します。

ステップ 3 [Profile] ページで、[API token] の下にある [Generate] をクリックします。API キーが生成され、表示されます。

ステップ 4 キーの内容をコピーまたはダウンロードします。

生成された API キーの例：

```
{
  "token": "eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkyW
  ...
  a_fcNoeAlVYvrXzDXA",
  "sub": "example@example.com",
  "iss": "b8edab9d-aaaa-4019-9999-f980cd5df3af",
  "aud": "vmanage",
  "userGroup": "[tenantadmin]",
  "tenant": "kdk-va2 - 999999-va-7aaaaaa5 - 640565",
  "duration": 315360000,
  "exp": 2058818495,
  "csrf": "AB0E71CAE...",
  "isAPIKey": true
}
```

ステップ 5 ここで提供されるエンドポイント情報を使用して、API ゲートウェイ URL を見つけます。ペイロード "org" フィールドに、API キーからの "tenant" 値を入力し、"apikey" フィールドに "token" 値を入力します。

例：

投稿

<https://ssp.sdwan.cisco.com/ssp/api/v6/apigw/info/>

ペイロード

```
{
  "org": "kdk-va2 - 999999-va-7aaaaaa5 - 640565",
  "apikey": "eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkyW
  ...
  a_fcNoeAlVYvrXzDXA",
  "is_redirect": false
}
```

応答

```
{
  "gateway_url": "apigw1clouduswest2-1024.viptela.info",
  "org": "kdk-va2 - 999999-va-7aaaaaa5 - 640565"
}
```

(注)

新しい API ゲートウェイがお客様の地理的な場所から近い場所にプロビジョニングされている場合は、このプロセスを繰り返して、オーバーレイを提供している新しいゲートウェイに接続します。

ステップ 6 受信した API キーとゲートウェイ URL ホスト名の値を使用して、エンドポイント "/dataservice/client/token" に GET 要求を送信して、受信した応答に含まれている CSRF トークンを取得します。この例で返されたゲートウェイ URL に基づくと、完全なパス名は <https://apigw1clouduswest2-1024.viptela.info/dataservice/client/token> となります。

Cisco API キーの使用に関する制限事項

Cisco API キーを使用すると、SSO ログインを介して Cisco SD- WAN Cloud からすべての Cisco API にアクセスできますが、いくつかの制限事項があります。Cisco API の詳細については、[Cisco DevNet](#) を参照してください。

- 認証方法

ヘッダーフィールドでベアラートークン認証方式を指定する必要があります。GET 要求から受け取った値を使用します。

- クロスサイトリクエストフォージェリ (CSRF/XSRF) に対する保護

クロスサイトリクエストフォージェリから保護するため、API リクエストヘッダーに X-XSRF-Token ヘッダーフィールドを含める必要があります。GET 要求から受け取った値を使用します。

- API 本文の使用

実行する API 呼び出しに基づいて、必要に応じて API 本文を含めることができます。

- Rate limit

リアルタイム API と一括 API は使用できません。他のすべての API を使用できますが、毎秒 10 件のレート制限の対象となります。Cisco SD- WAN Manager では、1 秒あたり 5 件の API レート制限が課されます。

- 継続的な監視

継続的な監視にはこの機能を使用しないでください。API レート制限の詳細については、『Cisco Catalyst SD- WAN スタートアップガイド』を参照してください。

- サポートされているカテゴリ

API 呼び出しは、次のカテゴリの操作に対してのみ提供されます。

- 証明書管理
- 設定
- デバイスおよびデバイスインベントリ
- モニタリング
- トラブルシューティング ツール

- NAT 構成非対応

REST API を使用した NAT 構成はサポートされていません。

Cisco API 要求の例

このセクションの例は、API キー、ゲートウェイ URL、および CSRF/XSRF トークンを使用して API コールを実行する方法を示しています。

Curl を使用した GET API 要求の例

この GET 要求は、location パラメータで指定された URL のページを取得します。

```
curl --location
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE...'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkyW
...
a_fcNoeAlVYvrXzDXA'
```

Curl を使用した PUT/POST API 要求の例

この PUT 要求は、data パラメータのデータを location パラメータで指定されたページ URL に送信します。

```
curl --location --request PUT
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE72C6D...'
--header 'Content-Type: application/json'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkyW
...
a_fcNoeAlVYvrXzDXA'
--data '{"mode":"on","bannerDetail":"check"}'
```

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。