

# Cisco IOS XE Catalyst SD-WAN デバイス、 Cisco IOS XE Catalyst SD-WAN リリース 17.15.x リリースノート

最終更新：2025 年 7 月 8 日

## 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、アドバンスドサービス、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。

## Cisco IOS XE Catalyst SD-WAN デバイス、Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a リリースノート

これらのリリースノートでは、Cisco Catalyst SD-WAN 機能を提供する Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a についても言及しています。これには、Cisco Catalyst SD-WAN コントローラ、Cisco Catalyst SD-WAN Validator、Cisco Catalyst SD-WAN Manager のリリース固有の情報が含まれており、Cisco IOS XE Catalyst SD-WAN デバイス に適用可能です。

#### 関連リリース

Cisco Catalyst SD-WAN 制御コンポーネントのリリース情報については、『[Release Notes for Cisco SD-WAN 制御コンポーネント, Cisco Catalyst SD-WAN 制御コンポーネント Release 20.15.x](#)』[英語]を参照してください。

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a の新機能

ここで説明する内容は、Cisco IOS XE Catalyst SD-WAN デバイス にのみ適用されます。

シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

表 1: Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a

機能	説明
<b>Cisco SD-WAN のシステムとインターフェイス</b>	
レイヤ 2 (L2) VPN マルチホーミングおよびハブアンドスポークのサポート	この機能を使用すると、アクティブ/スタンバイ設定されている同じサイト上の複数のデバイスでレイヤ 2 VPN を設定できます。  また、Cisco Catalyst SD-WAN ファブリック内のポイントツーマルチポイント接続で、ハブをはじめとした間接パスを使用した L2 接続が可能になります。
設定グループを使用した EtherChannel の設定	この機能により、設定グループを使用してサービス側とトランスポート側で EtherChannel を設定できます。
個々のポートチャネルでの EtherChannel のロードバランシング	この機能により、CLI テンプレートをを使用して、サービス側とトランスポート側で個々のポートチャネルの EtherChannel をロードバランシングできます。
<b>Cisco Catalyst SD-WAN Routing</b>	
放射性トレースを使用した Cisco Catalyst SD-WAN の BFD 障害対応	この機能は、放射性 (RA) トレースを使用して BFD プロトコルをトラブルシューティングする機能を提供します。  RA トレースは、特定の BFD セッションに参加し、セッションを処理するさまざまなプロセス全体のデバッグログを有効にします。
ハブアンドスポークトポロジのマルチキャストサポート	この機能により、ハブアンドスポークデバイスで 1 対多のトラフィックを効率的に分散できます。IPv4 マルチキャスト、IGMPv3、PIM SSM、PIM ASM、Auto-RP、スタティック RP などのマルチキャストルーティングプロトコルは、複数の受信者にデータを配信します。  ハブアンドスポークトポロジでマルチキャスト オーバーレイ プロトコルを使用すると、送信元は単一のデータパケットを単一のマルチキャストアドレスに送信し、受信者のグループ全体に配信できます。
<b>Cisco Catalyst SD-WAN ポリシー</b>	
アンダーレイ フラグメンテーションを使用したパケット複製	この機能では、隣接関係 MTU をを使用してアンダーレイ フラグメンテーションと組み合わせることにより、MTU の制限を超えるパケットを管理可能なフラグメントに分割し、信頼性の高い配信を確保することでパケットを正常に送信できます。

機能	説明
データポリシーの優先リモートカラー	データポリシーで優先リモートカラーを設定して、SLA 基準に基づいてトラフィック回送を制御できます。 「 <a href="#">Configure Traffic Rules</a> 」 [英語] の情報を参照してください。
Equinix でのサービス挿入	この機能を使用すると、Equinix に Palo Alto Networks ファイアウォールを展開し、Cisco SD-WAN Manager のワークフローライブラリから Equinix インターコネクト ゲートウェイにサービスチェーンを接続できます。
<b>Cisco Catalyst SD-WAN セキュリティ</b>	
Cisco Umbrella スコープログイン情報	この機能により、Cisco Umbrella SIG と Cisco Umbrella DNS の両方に新しい単一の Cisco Umbrella ログイン情報を定義および設定できます。
拡張 SGACL のロギング	この機能は、Cisco IOS XE Catalyst SD-WAN デバイスの高速ロギング (HSL) を使用して、セキュリティグループアクセスコントロールリスト (SGACL) のロギング機能を強化します。HSL を介した SGACL ロギングは、セキュリティイベントの効率性と拡張性の高いロギング方法を提供します。これは大量のトラフィックが発生するネットワーク環境で役立ちます。
Zscaler のサブロケーション	この機能により、特定のロケーションで1つ以上のZscalerサブロケーションを設定できます。
Cisco Catalyst SD-WAN ファイアウォールの高可用性	Cisco Catalyst SD-WAN に高可用性 (HA) を導入することで、2つの Cisco IOS XE Catalyst SD-WAN デバイスをアクティブ/アクティブまたはアクティブ/スタンバイ構成のいずれかに設定できます。HA が有効になっている場合、ゾーン ベース ファイアウォール (ZBF) やネットワークアドレス変換 (NAT) などの機能はこの HA 機能を使用して、アクティブ - スタンバイモードやアクティブ - アクティブモードでデバイス間の状態を同期します。アクティブデバイスに障害が発生した場合、スタンバイデバイスがセッションフローを中断することなくシームレスに動作を引き継ぐため、再接続の必要性がなくなります。
Cisco Security Service Edge とのトラフィック情報の共有	Cisco SD-WAN Manager は、VPN およびセキュリティグループタグ (SGT) 情報を Cisco Security Service Edge (SSE) と共有します。これはコンテキスト情報と呼ばれます。SSE はトラフィックのコンテキスト情報に基づいて、トラフィックにさまざまなポリシーを適用します。
<b>Cisco Catalyst SD-WAN Cloud OnRamp</b>	
Cloud onRamp for SaaS のワークフロー	Cisco SD-WAN Manager では、完全ガイド付きワークフローを使用して、特定の SaaS アプリケーションを選択し、各 SaaS アプリケーションのベストパフォーマンスパスを特定できます。
<b>Cisco Catalyst SD-WAN のモニタリングとメンテナンス</b>	

機能	説明
ウェブフックを使用したアラーム通知	Webex や Slack でアラーム通知を受信するように、Cisco SD-WAN Manager でウェブフックの URL を設定します。
Cisco RADKit を使用した Cisco Catalyst SD-WAN ソリューションの接続と障害対応	Cisco Remote Automation Development Kit (RADKit) のツールと Python モジュールを使用して、リモート端末、WebUI、デスクトップに安全に接続できます。TAC エンジニアは障害対応プロセス中に RADKit を使用して、安全かつ制御された方法でさまざまなデバイスやサービスの必要な情報を要求できます。
カスタムコマンドを使用した admin-tech ファイルの生成	この機能は追加のコマンド出力情報が加えて、admin-tech ファイルの出力内容を充実させます。この機能を使用すると、必要な show コマンドの出力結果を含むようにカスタマイズした admin-tech ファイルを生成して、障害対応に役立てることができます。カスタム admin-tech は、tech、core、logs のフラグから独立しています。
トンネルの packets 重複情報の表示	この機能は、Cisco SD-WAN Manager でトンネルの packets 重複情報を表示するための 1 つのチャートオプションを提供します。
<b>Cisco Catalyst SD-WAN NAT</b>	
サービス側 NAT でのアプリケーションレベルゲートウェイ	アプリケーションレベルゲートウェイ (ALG) を使用してアプリケーション層プロトコルを解釈し、FTP プロトコルのサービス側 NAT 変換を実行します。
<b>Cisco Catalyst SD-WAN マルチリージョン ファブリック (階層型 SD-WAN)</b>	
リージョンの作成とコントローラ ワークフローの割り当て	Cisco SD-WAN Manager には、Cisco Catalyst SD-WAN ファブリック内に複数のリージョンを作成し、それらに Cisco SD-WAN コントローラを割り当てることができる完全ガイド付きワークフローが導入されています。
<b>ポリシー グループ</b>	
AAR ポリシーの優先リモートカラー	AAR ポリシーで優先リモートカラーを設定して、SLA 基準に基づいてトラフィック回送を制御できます。
トポロジでのリージョンサポート	[Level] のトポロジ属性がカスタムトポロジでサポートされており、[Sites] と [Regions] のいずれかを選択できます。トポロジにルールを追加する場合は、[Region] の条件を使用して条件を照合します。
ポリシーグループでのリージョンサポート	ポリシーグループを展開する際に、特定のリージョンまたはサブリージョンからデバイスを関連付けます。

機能	説明
<b>Cisco Catalyst SD-WAN 設定グループ</b>	
設定カタログ	この機能により、事前定義された一連のインテントベースの設定やポリシーを提供するカタログ機能が導入されます。  Cisco Catalyst SD-WAN ポータルは、シスコが管理するカタログサービスをホストします。Cisco SD-WAN Manager を使用すると、すぐに利用可能なクラウドホスト型カタログエントリを Cisco Catalyst SD-WAN ポータルからダウンロードして、必要に応じてカスタマイズした後にカタログエントリからネットワーク内のデバイスに設定オブジェクトを展開できます。
ワークフローを使用しない設定グループの作成	この機能により、ワークフローを起動せずに Cisco SD-WAN Manager の [Configuration Groups] ページで設定グループを直接作成する方法が導入されました。製品ソリューションを選択すると、そのソリューションで利用可能なプロファイルに基づいて設定グループを作成できます。Cisco SD-WAN Manager では、必要なプロファイルを含む設定グループが作成されます。このプロファイルは要件に基づいて設定できます。この機能により、以前に作成したプロファイルを再利用できます。1つのページで設定グループを作成、管理、展開できます。
機能のデバイス固有の変数のデフォルト値を指定するためのサポート	[Device Specific] の範囲を選択するときに、デフォルト値と説明を機能パラメータに指定できます。Cisco SD-WAN Manager では、設定グループの展開時にパラメータのデフォルト値がデバイスに適用されます。
<b>Cisco Catalyst SD-WAN Network-Wide Path Insight ユーザー</b>	
IPSec のパケットドロップの可視性	この機能により、Network-Wide Path Insight 機能が強化され、IPSec のパケットドロップを高精度で可視化できます。
<b>シスコ マネージド セルラー アクティベーション</b>	
IoT プラットフォームおよびモジュールのマネージドセルラーアクティベーションのサポート	マネージドセルラーアクティベーションソリューションは、IoT プラットフォームとモジュールでサポートされています。
<b>Cisco Catalyst SD-WAN 高耐久性シリーズ ルータ設定ガイド</b>	
Cisco SD-WAN Manager を使用した PIM での GPS の設定	この機能により、Cisco SD-WAN Manager を使用して、Cisco IOS XE Catalyst SD-WAN デバイスの GNSS（全地球航法衛星システム）の PIM モジュールを設定および管理できます。
<b>Cisco Catalyst SD-WAN への Smart Licensing Using Policy の展開</b>	

機能	説明
デバイスにライセンスを割り当てるためのワークフロー	ライセンスをデバイスに割り当てるためのライセンス割り当てワークフローが導入されました。
<b>Cisco Catalyst SD-WAN との統合</b>	
Cisco Cyber Vision との統合	Cisco SD-WAN Manager は、Cisco Cyber Vision ネットワーク セキュリティ ソリューションとの統合をサポートします。1 つまたは複数のインターフェイスのトラフィックをモニターして、セキュリティ上の懸念事項を分析するためにトラフィックを Cisco Cyber Vision Center に送信するようにネットワーク内のデバイスを設定できます。

表 2: クラウド提供型 Cisco Catalyst SD-WAN

フィールド	説明
Cisco Catalyst SD-WAN と Cisco Meraki SD-WAN 間のインターコネクト	<p>Cisco SD-WAN インターコネクトは、管理者が Cisco Meraki ダッシュボードを使用して、Cisco Catalyst SD-WAN トポロジと Cisco Meraki SD-WAN トポロジ間のインターコネクトを簡単に設定、展開、およびモニターできるようにする自動化されたワークフローです。</p> <p>Cisco Meraki ダッシュボードの [Interconnects] ページから、IPSec トンネルのステータス、eBGP セッションのステータス、および VPN トンネルの統計情報をモニターできます。</p>

## ハードウェアの新機能および拡張機能

### 新機能

- シスコ マネージド セルラー アクティベーション (eSIM) に対応: マネージド セルラー アクティベーション ソリューションは、eSIM と呼ばれるプログラム可能な Subscriber Identity Module (SIM) を提供します。これは、お好みのセルラーサービスプランを設定できる物理 SIM カードです。マネージド セルラー アクティベーションは、5G Sub-6 GHz Pluggable Interface Module (PIM) P-5GS6-GL モデル、および Cisco Catalyst Wireless Gateway 113-4GW6 で利用できます。

このソリューションではデータ制限が設けられた「ブートストラップ」セルラープランも用意されており、Day-0 にデバイスをインターネットに接続するために利用できます。デバイスの電源をオンにしてオンボードする前に、Cisco SD-WAN Manager でセルラープランの詳細を設定する必要があります。こうすることで、オンボードが完了する前にブートストラップデータを使い果たすことを回避できます。

デバイスのオンボードの準備段階で、セルラープランの詳細に基づいて Cisco SD-WAN Manager を設定する方法については、『Cisco Managed Cellular Activation Configuration Guide』を参照してください。



- (注) このドキュメント内では、eSIMはシスコによって事前に取り付けられた、取り外しが可能な SIM を指します。eSIM がセルラー対応デバイスに埋め込まれた取り外し不可能な SIM を指す場合もあります。

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a でのソフトウェアとハードウェアの動作の変更

動作の変更	説明
<b>show platform software ipsec fp active flow</b> コマンド出力を更新しました。	<b>show platform software ipsec fp active flow</b> の出力を変更しました。フロー ID は 0 ~ 4294967295 の範囲をサポートするようになりました。 <a href="#">show platform software ipsec fp active flow</a> コマンドを参照してください。
SLA クラスのしきい値を更新しました。	新しい SLA クラスのしきい値については、「 <a href="#">SLA Classes</a> 」のセクション [英語] を参照してください。
<b>request platform software sdwanadmin-tech</b> コマンドとサポートされるオプションを更新しました。	<a href="#">request platform software sdwan admin-tech</a> コマンドを参照してください。
[Policy Object Profile] セクションを更新して、50 を超えるプロファイルがある場合のページネーションの新しい動作を追加しました。	「 <a href="#">Policy Object Profile</a> 」のセクション [英語] を参照してください。
<b>organization-name</b> コマンドの組織名のサイズ制限を 1 ~ 128 の範囲に更新し、 <b>interface</b> コマンドのインターフェイス名のサイズ制限を 1 ~ 31 の範囲に更新しました。	<a href="#">sp-organization-name (system)</a> および <a href="#">interface</a> のセクションを参照してください。
[Configure Device Values] セクションを更新して、ロールバックタイマーの設定グループを変更しました。設定グループ内の [Cellular Gateway] ソリューションのみがロールバックタイマーをサポートします。	「 <a href="#">Configure Device Values</a> 」のセクション [英語] を参照してください。

動作の変更	説明
show sdwan app-fwd cflowd コマンドの [View Cflowd Information] のセクションを更新して、cflowd データベースでモニター (IPv4 および IPv6) ごとに最大 4000 のフローレコードをサポートするようになりました。	「 <a href="#">View Cflowd Information</a> 」のセクション [英語] を参照してください。
[Configure BFD for Routing Protocols] のセクションを更新して、トンネルインターフェイスに SD-WAN モードが設定されていない場合、トンネルインターフェイスの BFD が非アクティブになるようになりました。	「 <a href="#">Configure BFD for Routing Protocols</a> 」のセクション [英語] を参照してください。
Cisco SD-WAN Manager のプロバイダーおよびテナントのリモートサーバーとイメージに関する情報。	「 <a href="#">Provider and Tenant Remote Servers and Images</a> 」のセクション [英語] を参照してください。
設定グループを使用して SDCI クラウドゲートウェイ拡張機能でデバイスを設定できなくなりました。	「 <a href="#">Information About Configuring Devices for AWS Integration Using Configuration Groups</a> 」のセクション [英語] を参照してください。
ユーザー設定の値が計算値を下回る場合、ポリサーはバースト値を上げて輻輳を防ぎ、パフォーマンスを最適化するようになりました。	「 <a href="#">Policer Burst Tolerance</a> 」のセクション [英語] を参照してください。
設定グループワークフローを使用してサイトを設定するときに、WAN インターフェイスにプライベートカラーを割り当てると、デフォルトで静的 IP アドレスが割り当てられます。	「 <a href="#">Overview of Configuration Group Workflows</a> 」のセクション [英語] を参照してください。
一貫性を保つために、[ Hunt Stop Rules ] テーブルの [ Response Code End ] フィールドを更新しました。	「 <a href="#">Server Group</a> 」のセクション [英語] を参照してください。
Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a 以前では、[ Send to Validator ] ボタンをクリックすると、コントローラのシリアル番号のみが Cisco Catalyst SD-WAN Validator に 1 回送信されます。	「 <a href="#">Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator</a> 」のセクション [英語] を参照してください。

## 特記事項、既知の動作、回避策

### マルチリージョン ファブリック

Cisco IOS XE Catalyst SD-WAN リリース 17.15.x および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.x は、次の機能をサポートする最後のリリースです。

- セカンダリリージョン
- サブリージョン
- 管理リージョン

Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.1 以降では、これらの機能は API によってのみ設定できます。

以降のリリースではこれらの機能がサポートされないため、ネットワーク設計と設定を更新して、可能な場合は代替のソリューションを使用することを推奨します。

詳細については、「[End of support for three types of regions](#)」[英語]を参照してください。

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.x で解決済みのバグと未解決のバグ

ここでは、このリリースで修正されたバグと未解決のバグのすべてについて詳しく説明します。これらのバグは、[Cisco バグ検索ツール](#)を使用して表示できます

### Cisco IOS XE Catalyst SD-WAN リリース 17.15.2a のバグ

#### Cisco IOS XE Catalyst SD-WAN リリース 17.15.2a で解決済みのバグ

ID	見出し
<a href="#">CSCwk28794</a>	スイッチポートを使用すると、SNMPがインターフェイスに誤った値を返す。
<a href="#">CSCwk39391</a>	IPSec出力のドロップ（OUT_IPV4_SA_NOT_FOUND）が原因でマルチキャストドロップが発生する。
<a href="#">CSCwk75733</a>	カスタムアプリケーションが正しくプログラムされていない可能性がある。
<a href="#">CSCwk69490</a>	不完全なコマンド show sdwan app-route stats local-color を誤って実行するとクラッシュする。
<a href="#">CSCwk70415</a>	NAT BPA が設定されている場合、IOS-XE でスタックしたスレッドにより予期しないリロードが発生する。
<a href="#">CSCwk31804</a>	リモート Cisco IOS XE Catalyst SD-WAN デバイスのアップリンクがダウンしている場合、Cisco SD-WAN Manager の制御接続がローカルダイヤラで確立されない。
<a href="#">CSCwm05718</a>	「probe-path trigger」が設定されている場合、17.12 から 17.15 にアップグレードすると CXPDP がクラッシュする。
<a href="#">CSCwm07994</a>	暗号化された IPSec パケットバッファが復号キューに入ると、IOS-XE で予期しないリロードが発生する。

ID	見出し
CSCwm07564	Cisco IOS XE Catalyst SD-WAN デバイス : data-policy local-tloc-list によって RTP メディアストリームが中断される。
CSCwm02632	「aggregate-only」を指定せずに Cisco SD-WAN Manager で route-aggregate を設定すると、誤解を招く。
CSCwk87944	TLOC プリファレンスの変更による VRRP スイッチオーバーにより、キー再生成および暗号追加/削除イベントが生成される。
CSCwm27495	OMP ルートが利用できないにもかかわらず、アドバタイズされている (ネットワークステートメント + NAT DIA VPN)。
CSCwm28775	17.6/9/12 でトークン方式が採用されている場合、Cisco Umbrella DNS で必証明書 (ios_core.p7b パンドル) の更新が必要。
CSCwf62943	Cisco IOS XE Catalyst SD-WAN デバイス : ディスク容量が原因でイメージの拡張が失敗した場合、システムイメージファイルが packages.conf に設定されない。

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.2a で未解決のバグ

ID	見出し
CSCwn53881	キーの再生成が PWK および非 PWK インターワーキングのユースケースで機能しない。
CSCwf51721	Viptela から IOS-XE へのロールバック後、エンタープライズ証明書のステータスが「該当なし」と表示されます。
CSCwn93052	track-default-gateway の問題により、スタティック デフォルトルートがルーティングテーブルにインストールされない。
CSCwn34457	電源の再投入後、認証エラーによりルータにログインできない。
CSCwn52348	NAT を削除して再追加すると、BFD がダウンする (断続的に)。
CSCwn49931	トリガーにより長時間のトラフィックを実行している FMAN_FP がクラッシュする。
CSCvu18068	Cisco IOS XE Catalyst SD-WAN デバイス と Cisco Umbrella の統合。
CSCwm13277	SIT : テレメトリ設定を使用して C8000v デバイスを再起動すると、crb_linux_iosd_vxe がクラッシュする。
CSCwm48459	重要プロセス vip_confid_startup_sh の rp_0_0 (rc=6) で障害が発生し、ソフトウェアがクラッシュする。

ID	見出し
<a href="#">CSCwm50619</a>	Cflowd 設定で export-spread が有効になっていると、データポリシーのコミットに失敗する。
<a href="#">CSCwn51404</a>	重要プロセス ftmd が原因でクラッシュし、子の TLOC が追加される前に親の TLOC が削除される。
<a href="#">CSCwm72748</a>	OMPd プロセスで pthread の制限に達すると、SIGABORT エラーでクラッシュする。
<a href="#">CSCwn12847</a>	Cisco Umbrella 側でキーの再生成が実行されるたびに、IPSec の Cisco Umbrella トンネルがダウンする。
<a href="#">CSCwn45328</a>	他のルールに TLS アクション復号を使用した AIP がある場合、IPv6 ルールを使用して統合ポリシーを作成できない。
<a href="#">CSCwm72414</a>	CoR SaaS DIA パスを使用したデータポリシーの SIG アクションが DNS トラフィックをブラックホール化する。
<a href="#">CSCwn82653</a>	OMPD が原因でメモリ使用率が高くなり、デバイスがクラッシュした。
<a href="#">CSCwn65833</a>	NWPI トレースのエレファントフローが原因で、Cisco IOS XE Catalyst SD-WAN デバイス で予期しないリロードが発生する。

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a のバグ

## Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a で解決済みのバグ

ID	見出し
<a href="#">CSCwj83844</a>	Cisco Catalyst IR1101 高耐久性シリーズルータ：デフォルトのキューサイズが小さすぎるため、QoS 帯域幅を設定できない。
<a href="#">CSCwj51700</a>	QFP の使用率が高い状態で「ip nat settings pap limit ... bpa」機能を再設定すると、CPP がクラッシュする。
<a href="#">CSCwk03686</a>	負の値によるセグメンテーション違反が原因でクラッシュする。
<a href="#">CSCwk42634</a>	%PMAN-0-PROCFAILCRIT: R0/0: pvp : クリティカルプロセス vip_confid_startup_sh has に失敗した (rc 6)。
<a href="#">CSCwj53456</a>	「crypto ikev2 cluster detail」 コマンドによってクラッシュがトリガーされた。
<a href="#">CSCwk26247</a>	自律モードで NetFlow 機能进行处理しているときに、Catalyst 8500L Edge プラットフォームの QFP スタックスレッドがクラッシュする。

ID	見出し
CSCwk33173	EzPM アプリケーションパフォーマンスプロファイルにより TCP フローが長時間アイドル状態になり、メモリークとクラッシュが発生する。
CSCwk16333	FNF フローの追加が原因で、FTMd で Cisco IOS XE Catalyst SD-WAN デバイスが繰り返しクラッシュする。
CSCwj95633	SDWAN : SAIE アプリケーション - Cisco SD-WAN Manager を介して IOS XE ルータに表示するデータがない。
CSCwk42190	設定と dp show コマンドが dp oper の出力と一致しない。
CSCwj06950	Cisco 1000 シリーズ サービス統合型ルータ : DSL モジュールが起動状態でスタックする。
CSCwj96852	1 つの TLOC で受信した外部の NAT トラフィックの内部へのリターントラフィックが、他の TLOC から転送される。
CSCwk39131	「show sdwan ftm next-hop chain all」を発行すると、Cisco IOS XE Catalyst SD-WAN デバイスがクラッシュする。
CSCwi28967	Encore-C9606R- Fo0/2/0 が複数の電源サイクルで断続的にダウンしたままになる。
CSCwk37351	IOS XE ルータ : PVDM OIR 中に予期しないリポートが発生する。
CSCwk22225	ログイン情報の機能テンプレートの更新を Cisco SD-WAN Manager から受信すると、FTMd がクラッシュする。
CSCwj48909	exp_sig_auto_tunnel スイートの実行中にトラッカーモジュールで 17.14 のコアダンプが確認された。
CSCwk23723	Cisco 1000 シリーズ サービス統合型ルータ/Cisco Catalyst シリーズ 8200/8300/8500L : WRED 階層型 QoS で平均キューの計算が正しくない。
CSCwj31476	Cisco IOS XE Catalyst SD-WAN リリース 17.14.x/ 20.14 : DSL デバイスの機能テンプレートスイートで CONFD ERROR no switchport access vlan 4 の障害が発生する。
CSCwk45165	Catalyst 8500L エッジプラットフォームでの fman_fp メモリーク。
CSCwj16153	C8300-2N2S-4T2X : Rx 側がダウンしても、シングルモードファイバの 10G 前面パネルポートがダウンしない。
CSCwj76501	Catalyst 8500L エッジプラットフォーム : ERSPAN 処理でデータプレーンがクラッシュする。
CSCwj84949	FLEXVPN ハブアンドスポークのセットアップで IPsec トンネルが機能していないため、トラフィックが暗号化されない。

ID	見出し
<a href="#">CSCwi56641</a>	100G/40G : QSFP ファイバ : ピア C8500-20X6C がリロードすると、C9500X-28C8D がリンクフラップエラーを報告する。
<a href="#">CSCwk20583</a>	C8500-12x4QC : ブレークアウト設定の 40G インターフェイスがリロード後にフラップする。
<a href="#">CSCwj90614</a>	confd_cli の CPU 使用率が高い。
<a href="#">CSCwi81026</a>	拡張環境での IPSec キーの再生成中に SDWAN BFD セッションがフラッピングする。
<a href="#">CSCwk39268</a>	[2.3.7.x] sdn-network-infra-iwan の「hash sha256」が 17.11 より大きいため更新できない。
<a href="#">CSCwj76662</a>	Cisco IOS XE Catalyst SD-WAN デバイス : ftmd プロセスが原因でメモリ使用率が高くなる。
<a href="#">CSCwj92560</a>	STCAPP コマンドがリロード後に VG410 から削除された。
<a href="#">CSCwk31715</a>	NAT 設定を削除した後も、IP アドレスがルーティングテーブルに表示されたままになる。
<a href="#">CSCwk42253</a>	コントローラモードのルータで HTTP 接続が 404 エラーにより失敗すると、予期しないリポートが発生する。
<a href="#">CSCwj42448</a>	セルラーコントローラプロファイルが設定されている場合、APN パスワードがプレーンテキストで表示される。
<a href="#">CSCwk12524</a>	ezManage モバイルアプリサービスが原因でデバイスがリロードされた。
<a href="#">CSCwk53680</a>	[vg400] VG400 経由の着信コールがファントムコールになる (64.3.0, 60.1.4, 62.3.3)。
<a href="#">CSCwk44078</a>	GETVPN/新しい KEK RSA キーへの移行しても、GM の再登録がトリガーされない。
<a href="#">CSCwj23674</a>	PPPOA に対応するダイヤラインターフェイスの最大 MTU が 1492 になる。
<a href="#">CSCwk22942</a>	一方のピアがもう一方のピアを介して PAT される場合、同じ送信元/宛先を持つ 2 つの IPSec SA を構築できない。
<a href="#">CSCwj96092</a>	20/17.14 : ICMP トラッカータイプのエコーからタイムスタンプへの変更が原因で、トラッカーで障害が発生する。
<a href="#">CSCwj99827</a>	「vdaemon」プロセスのクラッシュにより、Cisco IOS XE Catalyst SD-WAN デバイスが予期せずリロードする。

ID	見出し
<a href="#">CSCwi99454</a>	cEdgeFNF の test_tunnel_name_change_CSCvt57024 ケースが、pm5 のセッションが動作していないために失敗した。
<a href="#">CSCwj02401</a>	Cisco IOS XE Catalyst SD-WAN デバイス：フローの大量処理中に admin tech を生成すると、ルータがリロードされる。
<a href="#">CSCwj40223</a>	CISCO-SDWAN-APP-ROUTE-MIB で appRouteStatisticsTable シーケンスの順序が誤っているか、OS が誤った順序を返す。
<a href="#">CSCwk19725</a>	CSCwj02401 の show sdwan app-fwd フローに FNF キャッシュ制限が追加される。
<a href="#">CSCwk22312</a>	C8500-12X および C8500-12X4QC：ポートチャネルインターフェイスと物理インターフェイスで入力エラーとオーバーランが発生する。
<a href="#">CSCwk56504</a>	NAT64 のシナリオでは、変換が必要な IPv4 パケットが Cisco ASR 1000 シリーズルータによってドロップされる可能性がある。
<a href="#">CSCwj86794</a>	Cisco ASR 1000 シリーズルータが NWPI トレースの処理中にクラッシュする。
<a href="#">CSCwe52258</a>	VG420 は、WxC から設定をプルした後にスタートアップ vty 回線の設定を保持する必要がある。
<a href="#">CSCwj67591</a>	20.14:SD：SD-Routing ブラウンフィールド - シャーシのアクティブ化が、新しい UUID を使用して 2 回目に再試行した後にのみ有効になる。
<a href="#">CSCwj54638</a>	ASR1001-HX：EVC Q-in-Q 設定により、特定の VLAN が除外される場合がある。
<a href="#">CSCwj32347</a>	DIA エンドポイントトラッカーが ECMP ルートで機能しない。

#### Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a で未解決のバグ

ID	見出し
<a href="#">CSCwi76516</a>	マネージドセルラーアクティベーションソリューションの設定テンプレートの展開に失敗する。
<a href="#">CSCwk95308</a>	Catalyst 8500-12X のダウンインターフェイスで CRC エラーが増加する。
<a href="#">CSCwk75733</a>	カスタムアプリケーションが正しくプログラムされていない可能性がある。
<a href="#">CSCwk89256</a>	ISR に対するデバイステンプレートのプッシュ後に IOS-XE 設定で、Cisco SD-WAN Manager/IOS-XE 17.9.3 速度の不一致が発生する。

ID	見出し
CSCwm07994	スレッドのスタックによりルータがクラッシュする。
CSCwk85704	Cisco SD-WAN Manager を介した SD ルーチングの「:match traffic-category」アドオン CLI をプッシュできない。
CSCwm07396	ASR1K/C8500-12X* および C8500-20X6C : クライアントで mka セッションをクリアしても、ほとんどの BFD セッションがダウンしない。
CSCwm07651	DBGD プロセスが原因で ISR4K がクラッシュする。
CSCwm11819	SIGSEGV が原因で Cisco ASR 1000 シリーズ ルータがクラッシュする。 fp_0_0 (rc=139) での fman_fp_image 障害
CSCwj01917	17.9.4a へのアップグレード後にセルラーインターフェイスでネゴシエートされた IP アドレスが一致しない。
CSCwk87944	TLOC プリファレンスの変更による VRRP スイッチオーバーにより、キー再生成および暗号追加/削除イベントが生成される。
CSCwk98006	ZBFW が有効になっていると NAT 変換を確立できない。
CSCwk28794	スイッチポートを使用すると、SNMP がインターフェイスに誤った値を返す。
CSCwj76689	17.12.1 から 17.14.1 への .bin のアップグレード後、Cisco Catalyst 8000V Edge ソフトウェアの設定が失われる。
CSCwk86355	Cisco SD-WAN Manager 20.9.5 /home/admin から Cisco IOS XE Catalyst SD-WAN デバイス 17.6.5 ブートフラッシュへのファイル転送が失敗し、接続が失われた。
CSCwk49806	プロセス NHRP のクラッシュにより、IOS 17.06.05 を実行中の ASR1002-HX ルータが予期せずリブートした。
CSCwk81360	NAT スタティック変換の設定中に Cisco IOS-XE ルータが予期せずリブートすることがある。
CSCwk62954	複数の「match address local interface <int>」が Cisco SD-WAN Manager の暗号プロファイルでプッシュされない。
CSCwk63722	PKI サーバーを有効化するとスタートアップ設定に失敗する。
CSCwk97092	17.15 : EVC で shut/no shut を実行すると MKA セッションが起動しない。
CSCwm07564	Cisco IOS XE Catalyst SD-WAN デバイス : data-policy local-tloc-list によって RTP メディアストリームが中断される。

ID	見出し
CSCwk25731	[HCA] N7706 に接続された SRBD 光ファイバでインターフェイスがバウンズされると、C8500-20X6C が複数回フラッシングする。
CSCwk54544	Cisco Catalyst 8300 シリーズ エッジプラットフォームでルール順序が変更されると、SD-WAN ZBFW TCAM が誤ってプログラミングされる。
CSCwk89523	Cisco Catalyst 8500 シリーズ エッジプラットフォームにおいて、MAC アカウンティングテーブルで MAC アドレスを追加または削除する関数を実行中に IOSd がクラッシュする。
CSCwk74298	アプリケーションの通信エラーによりテンプレートのプッシュと一部の show コマンドで Cisco IOS XE Catalyst SD-WAN デバイスが拒否された。
CSCwk86062	LTE NIM-EM7455 では、ルータの再起動後、モデムのリセット後、またはセルラープロファイルの変更後にモデムがロックアップする。
CSCwk98578	Cisco Catalyst 8500 シリーズ エッジプラットフォーム/XE 17/GETVPN IPv6 暗号マップがインターフェイス設定に表示されない。
CSCwj42448	セルラーコントローラプロファイルが設定されている場合、APN パスワードがプレーンテキストで表示される。
CSCwj05500	Cisco Catalyst 8000V Edge ソフトウェア：ドライバの問題により、Accelerated Networking が動作を停止する。
CSCwk70630	9800-L 17.12.02 でデバイス証明書をインポートできない。
CSCwk69597	Cisco Catalyst 8000V Edge ソフトウェアで実行コンフィギュレーションのメモリ書き込みが、リロード後に保持されなかった。
CSCwk97930	リンクローカルの送信元の IPv6 パケットが SDWAN トンネルに転送されると、クラッシュが発生する。
CSCwm13223	不正な形式の DMVPN-5-NHRP_RES_REPLY_IGNORE syslog により、IOS-XE 17 が IOSd でクラッシュする。
CSCwk79454	デフォルトルートが削除されても、エンドポイントトラッカーが失敗しない。
CSCwi40697	LM960A18 および FN980 モデムでは、モデムが FW アップグレードから復旧しない場合がある。
CSCwk52677	%PLATFORM-3-ELEMENT_CRITICAL memory level/iomd プロセスが原因で C1118-8P/DSL ルータがクラッシュする。
CSCwk90014	ポート割り当ての失敗により、NAT/DIA トラフィックがドロップされる。

ID	見出し
<a href="#">CSCwi87546</a>	QFP CPP が rw_lock の待機中にスタックしたために Cisco 4000 ファミリー サービス統合型ルータが予期せずリブートし、ロック ID 0 が解放された。
<a href="#">CSCwk61238</a>	ステートフル IPSec が設定されている場合、リロード後に RRI スタティックでルートが入力されない。
<a href="#">CSCwk72795</a>	Cisco ASR 1000 シリーズ ルータに Sbfd プロトコルの統計情報がない。
<a href="#">CSCwk95044</a>	パケット複製リンクがフェールオーバーすると、17.12.03.CSCwj42249.SPA.smu.bin がドロップされる。
<a href="#">CSCwj87028</a>	DRE Opt の使用時に Cflowd でカスタムアプリの出力トラフィックが「unknown」と表示される。
<a href="#">CSCwm11348</a>	「DNS Query Error」が原因で、エンドポイントトラッカーがエラーを報告する。
<a href="#">CSCwk20995</a>	サブインターフェイスを使用する PPPoE セッションがリブート後にスタックする。
<a href="#">CSCwk89330</a>	BFD セッションの稼働中、Cisco IOS XE Catalyst SD-WAN デバイスでデータプレーンのパケットがドロップされる。
<a href="#">CSCwm08545</a>	集中型ポリシーポリサーが、サイトや vpn のリスト単位ではなく同じサイト上の PC 単位で機能する。
<a href="#">CSCwk34187</a>	cEdge_Nbar : ミドルウェアファミリの下での DICOM アプリケーションが DPI フローと Cisco SD-WAN Manager に表示されない。
<a href="#">CSCwm01269</a>	Cisco Catalyst 8300 シリーズ エッジプラットフォームの Cisco SD-WAN Manager 速度テストで、セカンダリルータの TLOC 拡張の方が良い結果が出る。
<a href="#">CSCwf62943</a>	Cisco IOS XE Catalyst SD-WAN デバイス : ディスク容量が原因でイメージの拡張が失敗した場合、システムイメージファイルが packages.conf に設定されない。
<a href="#">CSCwm00309</a>	一連の操作を変更後、パケットが正しいデータポリシーに到達しない。

## Cisco Catalyst SD-WAN 制御コンポーネント 互換性マトリックスおよびサーバー推奨事項

互換性情報とサーバー推奨事項については、『[Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#)』 [英語] を参照してください。

## サポートされるデバイス

デバイスの互換性については、「[Cisco Catalyst SD-WAN Device Compatibility](#)」 [英語] を参照してください。

## Cisco SD-WAN Manager の人工知能アシスタント

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.15.1

Cisco SD-WAN Manager で [Cisco AI Assistant] をクリックします。この人工知能アシスタントは、クラウドカスタマーのみが利用できます。この機能は、次のユースケースで使用できます。

- 製品と機能：Cisco Catalyst SD-WAN およびこのリリースで導入された機能に関する情報を提供します。
- ネットワークのモニター：ネットワークとアプリケーションの正常性に関する情報を提供します。

人工知能アシスタント機能を有効にするには、次の手順を実行します。

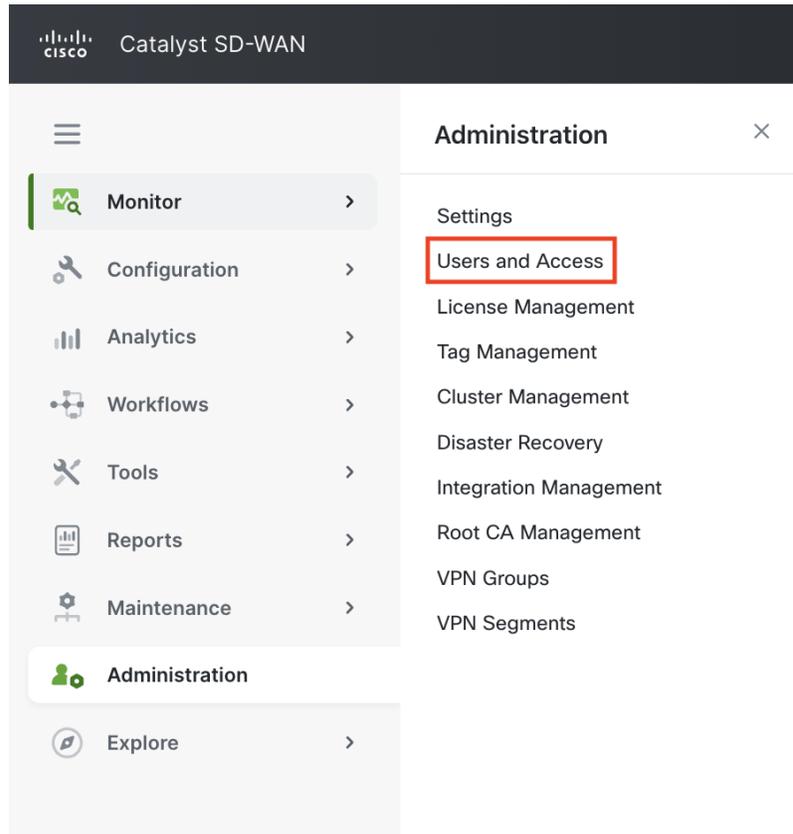
1. [Administration] > [Settings] でクラウドサービスを有効にします。
2. [Smart Account Credentials] に入力し、[Save] をクリックします。

## Cisco Catalyst SD-WAN Manager GUI の変更

このセクションでは、Cisco Catalyst SD-WAN Manager リリース 20.14.1 と Cisco Catalyst SD-WAN Manager リリース 20.15.1 間の GUI の重要な切り替えの概要を示します。

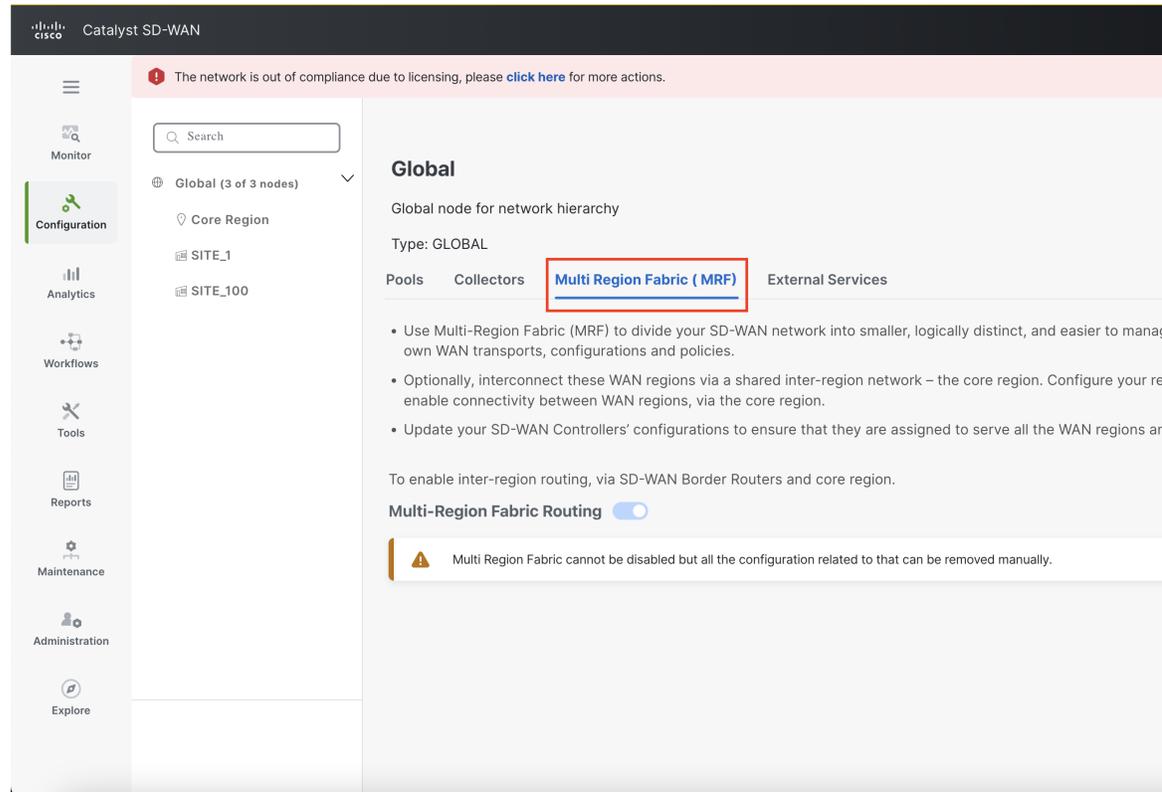
- [Administration] メニュー、[Users and Access]  
[Administration] メニュー内にある [Manage Users] メニューの名称が [Users and Access] に変更されました。

図 1: [Administration] メニュー



- [Network Hierarchy] ページの [Multi Region Fabric (MRF)] タブ  
[Configuration] > [Network Hierarchy] ページの [Network Settings] タブの名称が [Multi Region Fabric (MRF)] に変更されました。

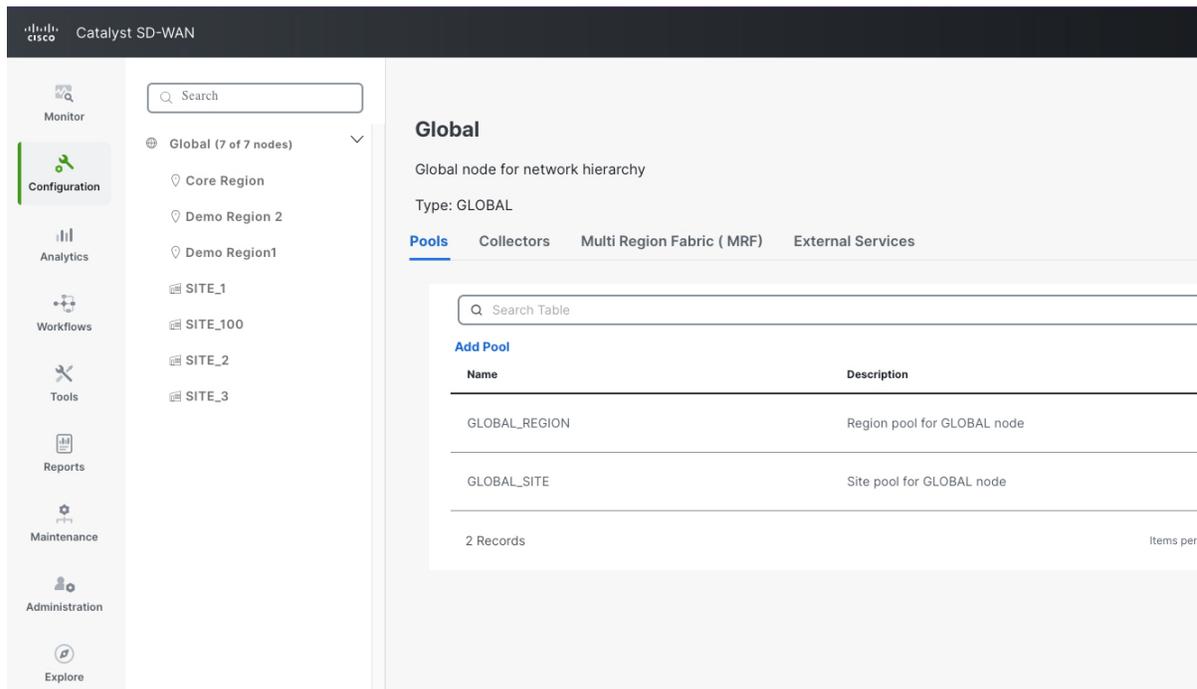
図 2: [Network Hierarchy] ページ、[Multi Region Fabric (MRF)] タブ



- セカンダリリージョンとサブリージョン

[Configuration] > [Network Hierarchy] ページで、セカンダリリージョンやサブリージョンを作成できなくなりました。このリリース以降、これらは API を介してのみ作成できます。

図 3 : [Network Hierarchy] ページ



## 関連資料

- [以前のリリースのリリースノート](#)
- [Cisco IOS XE ルータのソフトウェアのインストールとアップグレード](#)
- [vEdge ルータのソフトウェアのインストールとアップグレード](#)
- [フィールド通知](#)
- [推奨リリース](#)
- [セキュリティアドバイザリ](#)
- [シスコの情報](#)

## Full Cisco Trademarks with Software License

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 NONINFRINGEMENT 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](http://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)

---

【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/](http://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 NONINFRINGEMENT 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](http://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)

© 2024–2025 Cisco Systems, Inc. All rights reserved.

## 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。