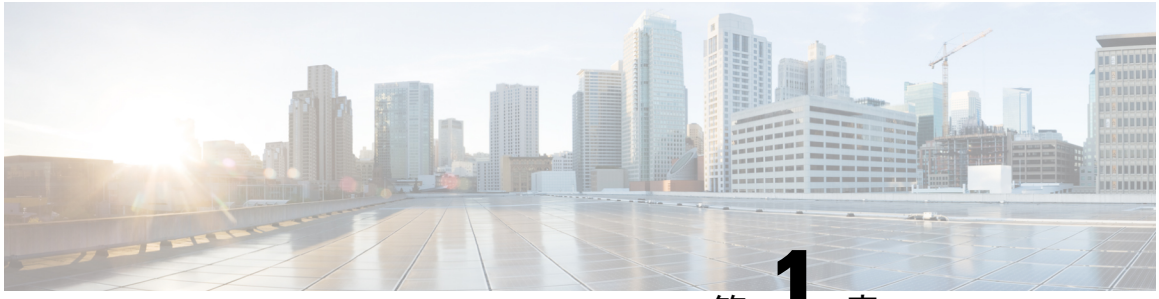
Cisco Catalyst SD-WAN SNMP コンフィギュレーションガイド

最終更新：2025 年 9 月 1 日

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

目 次



第 1 章

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

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

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。

Cisco Catalyst SD-WAN デバイスでの SNMP トラップのサポート

表 *1* : 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN トラップのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1 Cisco SD-WAN リリース 20.6.1	この機能では、次の SNMP トラップ通知の受信がサポートされています。 • Cisco IOS XE Catalyst SD-WAN デバイス、Cisco vEdge デバイス、Cisco Catalyst SD-WAN Validator、Cisco Catalyst SD-WAN コントローラ、および Cisco SD-WAN Manager でのエンタープライズ証明書の有効期限通知。 • Cisco vEdge デバイス、コントローラ、Cisco Catalyst SD-WAN Validator、Cisco Catalyst SD-WAN コントローラ、および Cisco SD-WAN Manager でのヘルスモニタリング通知。
アプリケーションルート SNMP トラップ	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	SLA クラスが変更されると、Cisco IOS XE Catalyst SD-WAN デバイスの **AppRouteSlaChange** SNMP トラップがトリガーされます。

デバイス上の SNMP エージェントでは、SNMP トラップを生成して SNMP マネージャに送信するための Cisco Catalyst SD-WAN がサポートされています。

（注） SNMP クエリの実行中は CPU 使用率が急増します。

SNMP マネージャに警告する通知は、次の問題に関するものです。

- Cisco IOS XE Catalyst SD-WAN デバイス、Cisco vEdge デバイス、およびコントローラでのエンタープライズ証明書の有効期限通知：認証局（CA）サーバーを使用すると、証明書が失効する前に証明書の登録が可能になり、認証中に証明書が利用できるようになります。ただし、ネットワークの停止、クロック更新の問題、および CA の過負荷は、証明書の更新を妨げる可能性があります。証明書の有効期限が近づいている場合、SNMP エージェントは SNMP トラップを使用してアラート通知を送信します。

  Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、SNMP エージェントは証明書の有効期限に関するアラート通知を次のように送信します。

  - 最初の通知間隔：現在の日付から 6 ヵ月～ 1 年の間に証明書の有効期限が切れます。

    間隔：毎月

  - 2 番目の通知間隔：現在の日付から 60 ～ 180 日後に証明書の有効期限が切れます。

    間隔：毎週

    タイプ：メジャー

  - 3 番目の通知間隔：現在の日付から 30 ～ 60 日後に証明書の有効期限が切れます。

    間隔：毎週

    タイプ：クリティカル

  - 4 番目の通知：現在の日付から 7 ～ 30 日後に証明書の有効期限が切れます。

    間隔：毎日

    タイプ：クリティカル

  - 5 番目の通知：1 週間以内に 証明書の有効期限が切れます。

    間隔：12 時間ごと

    タイプ：クリティカル

  - 期限切れの通知：証明書の有効期限が切れています。

    間隔：即時

    タイプ：クリティカル

  Cisco IOS XE Catalyst SD-WAN リリース 17.13.1aより前のリリースでは、SNMP エージェントが次の間隔で証明書の有効期限に関するトラップまたは通知を送信します。

  - 最初の通知：この通知は証明書が失効する 60 日前に送信されます。

- 通知の繰り返し：最初の通知の後、証明書が失効する 1 週間前まで後続の通知が毎週送信されます。最後の週には、証明書の失効日まで通知が毎日送信されます。

証明書の有効期限が 1 週間以上ある場合、通知は warning モードで送信されます。証明書の有効期限が 1 週間未満の場合、通知は alert モードで送信されます。通知には次の情報が含まれます。

- 証明書タイプ
- 証明書のシリアル番号
- 証明書の発行元名
- 証明書が失効するまでの残り日数

- Cisco vEdge デバイスおよびコントローラのヘルスモニタリング通知：これらの通知では、Cisco Catalyst SD-WAN コントローラと Cisco vEdge デバイスのファイルシステムまたはディスク使用率、CPU 使用率、メモリ使用率などの一連のオブジェクトに関するモニタリング情報が提供されます。

  リリース 20.6.1 以降、トラップは次のレベルの CPU 使用率で送信されます。

  - 90% 超：クリティカル
  - 75% 超：メジャー
  - 75% 未満：マイナー

設定グループを使用した SNMP の設定

始める前に

[Configuration] > **[Configuration Groups]** ページで、ソリューションタイプとして **[SD-WAN]** を選択します。

手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

ステップ 2 システムプロファイルで SNMP 機能を作成し設定します。

1. 基本設定を行います。

表 *2 : SNMP* バージョン（*SNMP Version*）

フィールド	説明
SNMP バージョン（SNMP Version）	次の SNMP バージョンのいずれかを選択します。 • SNMP v2 • **SNMP v3**
SNMP v2：ビューの追加	
名前*	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id*]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco Catalyst SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にして OID をビューから除外します。
SNMP v2：コミュニティの追加	
名前*	コミュニティ名を入力します。名前は 1 ～ 32 文字で、山括弧（< および >）を含めることができます。
User Label*	（最小リリース：Cisco vManage リリース 20.9.2）コミュニティ名のラベルまたは識別子を入力します。SNMP ターゲットに複数のコミュニティ名がある場合に、コミュニティ名を区別または更新するのに役立ちます。
View*	コミュニティに適用するビューを選択します。ビューは、コミュニティがアクセスできる MIB ツリーの部分を指定します。
Authorization*	ドロップダウンリストから、[read-only] を選択します。Cisco Catalyst SD-WAN でサポートされる MIB では書き込み操作が許可されないため、読み取り専用の許可のみを設定できます。
SNMP v2：ターゲットの追加	
VPN ID*	トラップサーバーに到達するために使用する VPN の番号を入力します。 範囲：0 ～ 65530

フィールド	説明
IPv4/IPv6 address of SNMP server*	SNMP サーバーの IP アドレスを入力します。
UDP port number to connect to SNMP server*	SNMP サーバーに接続するための UDP ポート番号を入力します。 範囲：1 ～ 65535
Community Name*	[Add Community] で構成されたコミュニティの名前を選択します。 このフィールドは、Cisco vManage リリース 20.9.1 以前のリリースにのみ適用されます。
User Label*	（最小リリース：Cisco vManage リリース 20.9.2）[Add Community] で構成されたユーザーラベルを選択します。
Source interface for outgoing SNMP trap*	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。
SNMP v3：ビューの追加	
名前*	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。
Add OID	このオプションをクリックして、オブジェクト識別子（OID）を追加し、次のパラメータを構成します。 • [Id*]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を入力します。Cisco Catalyst SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude]：このオプションを有効にして OID をビューに含めるか、このオプションを無効にして OID をビューから除外します。
SNMP v3：グループの追加	
名前*	トラップグループの名前を入力します。1 ～ 32 文字を使用できます。

フィールド	説明
Security Level*	グループに使用する認証を選択します。 • [no-auth-no-priv]：ユーザー名に基づいて認証します。この認証を構成する場合、認証またはプライバシー資格情報を構成する必要はありません。 [auth-no-priv]：選択した認証アルゴリズムを使用して認証します。この認証を構成する場合、このグループのユーザーに認証と認証パスワードを構成する必要があります。 [auth-priv]：選択した認証アルゴリズムを使用して認証します。この認証を構成する場合、このグループのユーザーに、認証と認証パスワード、およびプライバシーとプライバシーのパスワードを構成する必要があります。
View*	トラップグループがアクセスできる SNMP ビューを選択します。
SNMP v3：**ユーザーの追加**	
名前*	SNMP ユーザーの名前を入力します。1 ～ 32 文字の英数字を使用できます。
Authentication Protocol	ユーザーの認証メカニズムを選択します。 • **md5** • **sha**
Authentication Password	認証パスワードをクリアテキストまたは AES 暗号化キーとして入力します。
Privacy Protocol	ユーザーのプライバシータイプを選択します。 • [aes-cfb-128]：128 ビットキーで、暗号フィードバックモードで使用される Advanced Encryption Standard 暗号アルゴリズムを使用します。これは SHA-1 認証プロトコルです。 • [aes-256-cfb-128]：256 ビットキーで、暗号フィードバックモードで使用される Advanced Encryption Standard 暗号アルゴリズムを使用します。これは SHA-256 認証プロトコルです。
Privacy Password	プライバシーパスワードをクリアテキストまたは AES 暗号化キーのいずれかで入力します。
Group*	SNMPv3 グループの名前を選択します。
SNMP v3：**ターゲットの追加**	

フィールド	説明
VPN ID*	トラップサーバーに到達するために使用する VPN の番号を入力します。 範囲：0 ～ 65530
IPv4/IPv6 address of SNMP server*	SNMP サーバーの IP アドレスを入力します。
UDP port number to connect to SNMP server*	SNMP サーバーに接続するための UDP ポート番号を入力します。 範囲：1 ～ 65535
User*	[Add User] で構成されたユーザーの名前を選択します。
Source interface for outgoing SNMP trap*	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

2. 詳細設定を行います。

表 *3*：詳細設定（*Advanced Settings*）

フィールド	説明
Shutdown	デフォルトでは、SNMP は有効になっています。
Contact Person	Cisco IOS XE Catalyst SD-WAN デバイス を管理するネットワーク管理連絡先担当者の名前を入力します。これには、最大 255 文字を使用できます。
Location of Device	デバイスのロケーションの説明を入力します。これには、最大 255 文字を使用できます。

次のタスク

「Deploy a configuration group」[英語] も参照してください。

Cisco SD-WAN Manager を使用した SNMP の設定

SNMP テンプレートを使用して、Cisco Catalyst SD-WAN ソフトウェアを実行しているすべての Cisco vEdge デバイスおよび Cisco IOS XE Catalyst SD-WAN デバイスに対応する SNMP パラメータを設定します。

（注） 1 つのデバイステンプレートには、1 つの SNMP 機能テンプレートのみを含めることができます。したがって、1 つのデバイステンプレートに SNMPv2 または SNMPv3 のいずれかを設定できますが、両方を設定することはできません。

（注） すべての SNMP バージョンが Cisco IOS XE Catalyst SD-WAN デバイスでサポートされていますが、安全性が確保された SNMPv3 バージョンが推奨されます。

（注） Cisco IOS XE Catalyst SD-WAN デバイスでは Viptela Management Information Base（MIB）はサポートされません。

（注） Cisco IOS XE Catalyst SD-WAN デバイスを使用してネットワーク管理ステーション（NMS）に到達できる場合（.biz インターネットや MPLS など）、**allow-service snmp** コマンドがトランスポート VPN トンネルインターフェイスで有効になっていることを確認します。これにより、SNMP パケットがドロップされなくなります。

allow-service snmp コマンドは Cisco IOS XE Catalyst SD-WAN デバイスに固有です。次の例に示すように、**sdwan > interface > tunnel-interface** 設定セクションで **allow-service snmp** コマンドが有効になっていることを確認します。

```
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec
   color mpls
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
   allow-service snmp
  exit
 exit
```

[Template] 画面に移動し、テンプレートに命名する

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

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です

3. [Create Template] ドロップダウンから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンから、テンプレートを作成するデバイスのタイプを選択します。
5. [Additional Templates] をクリックし、[Additional Templates] セクションまでページをスクロールします。
6. [Additional Templates] の下にある [Cisco SNMP] ドロップダウンから、[Create Template] をクリックします。

   SNMP テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部にはSNMPパラメータを定義するためのフィールドがあります。
7. [Template Name] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
9. SNMP 機能テンプレートを保存するには、[Save] をクリックします。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンをクリックして次のいずれかを選択します。

表 *4:* パラメータ値の範囲を変更する

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco IOS XE Catalyst SD-WAN デバイスまたは Cisco vEdge デバイスをデバイステンプレートにアタッチするときに、値を入力します。 [Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに1つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Cisco IOS XE Catalyst SD-WAN デバイスまたは Cisco vEdge デバイスをデバイステンプレートにアタッチするときに、この CSV ファイルをアップロードします。 デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。 デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。
グローバル（地球のアイコンで示される）	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。

SNMP 機能テンプレートをデバイステンプレートにアタッチする

SNMP 機能テンプレートを作成したら、その機能テンプレートをデバイステンプレートにアタッチする必要があります。

（注） Cisco vManage リリース 20.5 より前に作成されたテンプレートはデバイスにアタッチされると失敗するため、SNMP 機能テンプレートを再作成する必要があります。

SNMP 機能テンプレートをアタッチするには、次の手順を実行します。

1. [Device Templates] で、作成した SNMP テンプレートを選択します。
2. [...] をクリックして、[Attach Devices] を選択します。[Select Devices] が選択された状態で [Attach Devices] ダイアログボックスが開きます。
3. [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。
4. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。

5. [Attach] をクリックします。

基本的な SNMP の設定

基本的な SNMP を設定するには、[SNMP] を選択して次のパラメータを設定します。すべてのパラメータが必須です。

表 *5 :* 基本的な *SNMP* のパラメータ

パラメータ名	説明
シャットダウン	[No] をクリックして、SNMP を有効にします。デフォルトでは、SNMP は無効です。
連絡先担当者	Cisco IOS XE Catalyst SD-WAN デバイスまたは Cisco vEdge デバイスの管理を担当するネットワーク管理担当者の名前を入力します。これには、最大 255 文字を使用できます。
デバイスの場所	デバイスのロケーションの説明を入力します。これには、最大 255 文字を使用できます。

機能テンプレートを保存するには、[Save] をクリックします。

Cisco SD-WAN Managerを使用した Cisco vEdge デバイスでの SNMPv2 の設定

SNMPv2 を設定するには、[SNMP Version] を選択して [V2] をクリックします。SNMPv2 では、コミュニティとトラップ情報を設定できます。

SNMP ビューを設定するには、[View & Community] セクションで [View] を選択します。次に、[Add New View] をクリックして、次のパラメータを設定します。

表 *6 : SNMPv2* ビューのパラメータ

パラメータ名	説明
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。

パラメータ名	説明
Object Identifiers	[Add Object Identifiers] をクリックして、次のパラメータを設定します。 • Exclude OID：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 と入力します。Viptela MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 と入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • On/Odd：[Off] をクリックして OID をビューに含めるか、[On] をクリックして OID をビューから除外します。 オブジェクト識別子を保存するには、[Save] をクリックします。 リストから OID を削除するには、エントリの横にあるマイナス記号をクリックします。

SNMP ビューを追加するには、[Add] をクリックします。

SNMP コミュニティを設定するには、[Community] を選択します。次に、[Add New Community] をクリックして、次のパラメータを設定します。

表 *7: SNMPv2* コミュニティのパラメータ

パラメータ名	説明
Name	コミュニティの名前を入力します。名前は 1 ～ 32 文字で、山括弧（< および >）を含めることができます。
Authorization	ドロップダウンリストから [read-only] を選択します。Cisco Catalyst SD-WAN ソフトウェアでサポートされている MIB では書き込み操作が許可されていないため、読み取り専用の許可のみを設定できます。
View	コミュニティに適用するビューを選択します。このビューにより、コミュニティがアクセスできる MIB ツリーの一部が指定されます。

SNMP コミュニティを追加するには、[Add] をクリックします。

トラップを設定するには、[Trap] セクションで [Trap Group] を選択します。次に、[Add New Trap Group] をクリックし、以下のパラメータを設定します。

表 *8:* トラップグループのパラメータ

パラメータ名	説明
Group Name	トラップグループの名前を入力します。1 ～ 32 文字を使用できます。

パラメータ名	説明
Trap Type Modules	[Add Trap Type Modules] をクリックして、次のパラメータを設定します。 [Severity Levels] で、トラップの重大度（クリティカル、メジャー、またはマイナー）を 1 つ以上選択します。 [Module Name] で、トラップグループに含めるトラップのタイプを選択します。 • [all]：すべてのトラップタイプ。 • [app-route]：アプリケーション認識型ルーティングによって生成されるトラップ。 • [bfd]：BFD および BFD セッションによって生成されるトラップ。 • [control]：DTLS および TLS セッションによって生成されるトラップ。 • [dhcp]：DHCP によって生成されるトラップ。 • [hardware]：Viptela ハードウェアによって生成されるトラップ。 • [omp]：OMP によって生成されるトラップ。 • [routing]：BGP、OSPF、および PIM によって生成されるトラップ。 • [security]：証明書、Cisco Catalyst SD-WAN コントローラ および vEdge シリアル番号ファイル、および IPsec によって生成されるトラップ。 • [system]：システム全体の機能によって生成されるトラップ。 • [vpn]：インターフェイスや VRRP など、VPN 固有の機能によって生成されるトラップ。

トラップタイプモジュールを保存するには、[Save] をクリックします。

トラップターゲットサーバーを設定するには、[Trap] セクションで [Trap Target Server] を選択します。次に、[Add New Trap Group] をクリックし、以下のパラメータを設定します。

（注） Cisco vEdge デバイスでは、異なる送信元インターフェイスを各トラップターゲットサーバーにバインドできます。

表 *9:* トラップターゲットサーバーのパラメータ

パラメータ名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ～ 65530
IP Address	SNMP サーバーの IP アドレスを入力します。

パラメータ名	説明
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ～ 65535
Group Name	[Group] で設定したトラップグループの名前を選択します。
Community Name	[Community] で設定したコミュニティの名前を選択します。
Source Interface	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

トラップターゲットを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

Cisco SD-WAN Manager を使用した Cisco vEdge デバイスでの SNMPv3 の設定

表 *10 :* 機能の履歴

機能名	リリース情報	説明
SNMPv3 AES-256 ビット認証プロトコルのサポート	Cisco vManage リリース 20.5.1 Cisco SD-WAN リリース 20.5.1	この機能を使用すると、Cisco vEdge デバイスで SHA-256 認証プロトコルおよび AES-256 ビット暗号化をサポートする SNMPv3 ユーザーを設定できます。

SNMPv3 を設定するには、[SNMP Version] で [Template] ページに移動し、グループとトラップ情報を設定します。

- Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Templates]** の順に選択します。
- [Device Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です

- [Create Template] ドロップダウンから、[From Feature Template] を選択します。
- [Device Model] ドロップダウンから、テンプレートを作成するデバイスのタイプを選択します。

- [Additional Templates] をクリックし、[Additional Templates] セクションまでページをスクロールします。
- [Additional Templates] の [SNMP] ドロップダウンから、[Create Template] をクリックします。

  SNMP テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には SNMP パラメータを定義するためのフィールドがあります。
- [Template Name] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
- [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
- [SNMP Version] セクションで、[V3] をクリックします。SNMPv3 の場合は、グループ、ユーザー、およびトラップ情報を設定できます。
- [Trap] セクションで、[Trap Group] を選択してトラップを設定します。次に、[Add New Trap Group] をクリックして以下に表示されたパラメータを設定します。

表 *11 : Cisco vEdge* デバイスに対応するトラップグループのパラメータ

パラメータ名	説明
Group Name	トラップグループの名前を入力します。長さは 1 ～ 32 文字で指定できます。

パラメータ名	説明
Trap Type Modules	[Add Trap Type Modules] をクリックして、次のパラメータを設定します。 [Severity Levels] で、トラップの重大度を 1 つ以上選択します。トラップでサポートされるセキュリティレベルは、クリティカル、メジャー、およびマイナーです。 [Module Name] で、トラップグループに含めるトラップのタイプを選択します。 • [all]：すべてのトラップタイプ。 • [app-route]：アプリケーション認識型ルーティングによって生成されるトラップ。 • [bfd]：BFD および BFD セッションによって生成されるトラップ。 • [control]：DTLS および TLS セッションによって生成されるトラップ。 • [dhcp]：DHCP によって生成されるトラップ。 • [hardware]：Viptela ハードウェアによって生成されるトラップ。 • [omp]：OMP によって生成されるトラップ。 • [routing]：BGP、OSPF、および PIM によって生成されるトラップ。 • [security]：証明書、Cisco Catalyst SD-WAN コントローラ および vEdge シリアル番号ファイル、および IPsec によって生成されるトラップ。 • [system]：システム全体の機能によって生成されるトラップ。 • [vpn]：インターフェイスや VRRP など、VPN 固有の機能によって生成されるトラップ。

トラップタイプモジュールを保存するには、[Save] をクリックします。

SNMP ビューを設定するには、[View & Groups] セクションで [View] を選択します。次に、[New View] をクリックして次のパラメータを設定します。

表 *12 :* パラメータの表示とグループ化

パラメータ名	説明
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。グループを追加する前に、すべてのビューにビュー名を追加する必要があります。

パラメータ名	説明
Object Identifiers (OID)	[Add Object Identifiers] をクリックして、次のパラメータを設定します。 • [Object Identifier]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 と入力します。Cisco Catalyst SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 （注） Cisco vManage リリース 20.6.1 以降、auth "sha-256" および priv "aes-256-cfb-128" を持つユーザーの SNMPv3 設定では、ワイルドカード（*）を使用した oid がサポートされません。 • [Exclude OID]：[Off] をクリックして OID をビューに含めるか、[On] をクリックして OID をビューから除外します。 リストから OID を削除するには、エントリの [Delete] アイコンをクリックします。 ビューリストに OID を追加するには、[Add] をクリックします。

SNMP グループを設定するには、[New Group] をクリックして次のパラメータを設定します。

（注） SNMP グループの構成に進む前に、SNMP ビューを作成する必要があります。

表 *13 : Cisco vEdge* デバイスに対応する *SNMP* グループのパラメータ

パラメータ名	説明
Name	グループの名前を入力します。名前は 1 ～ 32 文字で、山括弧（< および >）を含めることができます。

パラメータ名	説明
Security Level	SNMPv3 セキュリティモデルのドロップダウンから [Security Level] を選択します。 SNMPv3 は、ユーザーとユーザーが属するグループの認証戦略が設定されているセキュリティモデルです。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。 • [NoAuthNoPriv]：認証にユーザー名の一致を使用します。 • [authNoPriv]：Message Digest 5（MD5）またはセキュア ハッシュ アルゴリズム（SHA）のアルゴリズムに基づく認証を行います。 • [authPriv]：HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を行います。DES 56 ビット暗号化を提供し、CBC-DES（DES-56）標準に基づいて認証します。
View	グループに適用するビューをドロップダウンから選択します。このビューで、グループがアクセスできる MIB ツリーの部分を指定します。

SNMP グループを追加するには、[Add] をクリックします。

[User] セクションで [Add New User] をクリックし、次のパラメータを入力して SNMPv3 ユーザーを設定します。

表 *14 : SNMPv3* ユーザーパラメータ

パラメータ名	説明
User	SNMP ユーザーの名前を入力します。1 ～ 32 文字の英数字を使用できます。

パラメータ名	説明
Authentication Protocol	ユーザーの認証メカニズムを選択します。 • MD5 ダイジェスト。 • SHA-1 メッセージダイジェスト。 • SHA-256 メッセージダイジェスト。 （注） Cisco SD-WAN リリース 20.5.1 以降、SHA-256 認証プロトコルが導入されました。認証プロトコルとして SHA-256 を選択した場合は、セキュリティレベルを `authPriv` に設定する必要があります。 （注） MD5 認証プロトコルは、Cisco Catalyst SD-WAN リリース 20.3.2 以降のリリースでは廃止されています。 （注） Cisco Catalyst SD-WAN リリース 20.11.1 以降では、MD5 認証を選択すると、コンソールログに MD5 が廃止されたことを示す警告が含まれます。
Authentication Password	ローカライズされた MD5 または SHA ダイジェストがある場合は、それぞれの文字列をパスワードとして指定できます。ダイジェストの形式は aa:bb:cc:dd です。ここでの aa、bb、cc、および dd は 16 進数値です。また、ダイジェストの長さは正確に 16 オクテットにする必要があります。
Privacy Protocol	ユーザーのプライバシータイプを選択します。 • SHA-1 認証プロトコルで AES-CFB-128 を選択：高度暗号化規格の暗号アルゴリズムは 128 ビットキーを用いて、暗号フィードバックモードで使用されます。 • Cisco SD-WAN リリース 20.5.1 の SHA-256 認証プロトコルで AES-256-CFB-128 を選択：高度暗号化規格の暗号アルゴリズムは 256 ビットキーを用いて、暗号フィードバックモードで使用されます。 （注） 認証プロトコル SHA-1 はサポートされなくなりました。SNMPv3 ユーザーのトラップターゲットが SHA-1 で設定されている場合、SNMP トラップは生成されません。SHA-256 認証プロトコルを使用して SNMPv3 ユーザーを設定する必要があります。
Privacy Password	認証パスワードをクリアテキストまたは AES 暗号化キーとして入力します。
Group	ドロップダウンからグループ名を選択します。設定済みの SNMPv3 グループ名がすべてドロップダウンに表示されます。

（注） Cisco vManage リリース 20.6.x では、SNMP ユーザーが Auth-SHA-256 および Priv-AES-256 で設定されている場合、SNMP クエリに特別なポート 1161 を使用します。

（注） Cisco SD-WAN リリース 20.9.x 以降、SHA 認証プロトコルおよび AES-CFB-128 プライバシープロトコルを使用して SNMPv3 ユーザーを設定することはできません。ただし、アップグレードする既存のユーザーの場合、SNMP クエリはサポートされますが、SNMP トラップはサポートされません。

トラップターゲットサーバーを設定するには、[Trap] セクションで [Trap Target Server] を選択します。次に、[Add New Trap Group] をクリックして以下に表示されたパラメータを設定します。

（注） トラップターゲットサーバーを作成する前にユーザーを作成する必要があります。

表 *15:* トラップターゲットサーバーのパラメータ

パラメータ名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ～ 65530。
IP Address	SNMP サーバーの IP アドレスを入力します。
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ～ 65535。
User Name	ドロップダウンからユーザーの名前を選択します。
Source Interface	リモート SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

トラップターゲットサーバーを追加するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

（注） デバイステンプレートで SNMPv3 設定を SNMPv2 設定に切り替え、テンプレートのプッシュによってこの変更を適用すると、SNMP walk アプリケーションがブロックされます。これは、設定変更時に SNMPv3 の **snmp mib community-map** コマンドが削除されないためです。したがって、SNMPv3 設定テンプレートがアクティブな場合、SNMPv3 から SNMPv2 に直接切り替えることはできません。SNMPv2 に切り替えるには、最初にデバイスで SNMPv3 設定を削除してから、別のコミットによって SNMPv2 テンプレートをプッシュする必要があります。

Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイスでの SNMPv2 の設定

SNMPv2 を設定するには、[SNMP Version] を選択して [V2] をクリックします。SNMPv2 では、コミュニティとトラップ情報を設定できます。

SNMP ビューを設定するには、[View & Community] セクションで [View] を選択します。次に、[Add New View] をクリックして、次のパラメータを設定します。

表 *16 : SNMPv2* ビューのパラメータ

パラメータ名	説明
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。コミュニティを追加する前にすべてのビューにビュー名を追加する必要があります。
Object Identifiers	[Add Object Identifiers] をクリックして、次のパラメータを設定します。 • Exclude OID：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 と入力します。Viptela MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 と入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • On/Odd：[Off] をクリックして OID をビューに含めるか、[On] をクリックして OID をビューから除外します。 オブジェクト識別子を保存するには、[Save] をクリックします。 リストから OID を削除するには、エントリの横にあるマイナス記号をクリックします。

SNMP ビューを追加するには、[Add] をクリックします。

SNMP コミュニティを設定するには、[Community] を選択します。次に、[Add New Community] をクリックして、次のパラメータを設定します。

表 *17 : SNMPv2* コミュニティのパラメータ

パラメータ名	説明
Name	コミュニティの名前を入力します。名前は 1 ～ 32 文字で、山括弧（< および >）を含めることができます。
Authorization	ドロップダウンリストから [read-only] を選択します。Cisco Catalyst SD-WAN ソフトウェアでサポートされている MIB では書き込み操作が許可されていないため、読み取り専用の許可のみを設定できます。
View	コミュニティに適用するビューを選択します。このビューにより、コミュニティがアクセスできる MIB ツリーの一部が指定されます。

SNMP コミュニティを追加するには、[Add] をクリックします。

トラップターゲットサーバーを設定するには、[Trap] セクションで [Trap Target Server] を選択します。次に、[New Trap Target] をクリックして、以下のパラメータを設定します。

（注） ただし、Cisco IOS XE Catalyst SD-WAN デバイスでは、送信元インターフェイスの最後のオカレンスがグローバル送信元インターフェイスとして選択されます。

表 *18 :* トラップターゲットサーバーのパラメータ

パラメータ名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ～ 65530
IP Address	SNMP サーバーの IP アドレスを入力します。
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ～ 65535
Community Name	[Community] で設定したコミュニティの名前を選択します。
Source Interface	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

トラップターゲットを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

Cisco SD-WAN Manager を使用した Cisco IOS XE Catalyst SD-WAN デバイスでの SNMPv3 の設定

表 *19* : 機能の履歴

機能名	リリース情報	説明
SNMPv3 AES-128 および AES-256 ビット暗号化プロトコルのサポート	Cisco vManage リリース 20.7.1 Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a	この機能では、Cisco IOS XE Catalyst SD-WAN デバイスで SHA-1 認証プロトコルと AES-128 および AES-256 暗号化を使用する SNMPv3 ユーザーを設定できます。

SNMPv3 を設定するには、[SNMP Version] で [Template] ページに移動し、グループとトラップ情報を設定します。

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

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Additional Templates] をクリックします。この操作で [Additional Templates] セクションまで移動します。
6. [Cisco SNMP] ドロップダウンリストから、[Create Template] を選択します。

   テンプレートに名前を付け、SNMP パラメータを定義するためのフィールドが含まれた SNMP テンプレートフォームが表示されます。
7. [Template Name] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
9. [SNMP Version] セクションで、[V3] をクリックします。SNMPv3 の場合は、グループとトラップ情報を設定できます。

10. [View & Groups] セクションで [View] をクリックし、[New View] を選択して次のフィールドを設定します。

表 *20 : Cisco IOS XE Catalyst SD-WAN* デバイスに対するパラメータの表示とグループ化

フィールド名	説明
Name	ビューの名前を入力します。ビューは、SNMP マネージャがアクセスできる MIB オブジェクトを指定します。ビュー名は、最大 255 文字まで指定できます。グループを追加する前に、すべてのビューにビュー名を追加する必要があります。
Object Identifiers (OID)	[Add Object Identifiers] をクリックして、次のパラメータを設定します。 • [Object Identifier]：オブジェクトの OID を入力します。たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 と入力します。Cisco Catalyst SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.9 と入力します。OID サブツリーの任意の位置でアスタリスクワイルドカード（*）を使用して、特定のタイプまたは名前との一致ではなく、その位置の任意の値と一致させます。 • [Exclude OID]：[Off] をクリックして OID をビューに含めるか、[On] をクリックして OID をビューから除外します。 リストから OID を削除するには、対応するエントリの横にある [Delete] アイコンをクリックします。 OID をビューリストに追加するには、[Add] をクリックします。

11. [Add] をクリックします。

[Group] をクリックし、[New Group] を選択して、次のパラメータを設定します。

（注） SNMP グループの構成に進む前に、SNMP ビューを作成する必要があります。

表 *21 :* パラメータのグループ化

フィールド名	説明
Name	グループの名前を入力します。名前は 1 ～ 32 文字で、山括弧（<>）を含めることができます。

フィールド名	説明
Security Level	SNMPv3 セキュリティモデルのドロップダウンからセキュリティレベルを選択します。 SNMPv3 は、ユーザーとユーザーが属するグループの認証戦略が設定されているセキュリティモデルです。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。 • [NoAuthNoPriv]：認証にユーザー名の一致を使用します。 • [authNoPriv]：Message Digest 5（MD5）またはセキュア ハッシュ アルゴリズム（SHA）のアルゴリズムに基づく認証を行います。 • [authPriv]：HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を行います。DES 56 ビット暗号化を提供し、CBC-DES（DES-56）標準に基づいて認証します。
View	グループに適用するビューをドロップダウンリストから選択します。このビューで、グループがアクセスできる MIB ツリーの部分を指定します。

SNMP グループを追加するには、[Add] をクリックします。

SNMPv3 ユーザーを設定するには、[User] セクションで [New User] をクリックし、次のフィールドに情報を入力します。SNMP ユーザーの設定を続行する前に、SNMP グループを作成する必要があります。

表 *22 : SNMPv3* ユーザーのパラメータ

フィールド名	説明
User	ユーザの一意の名前を入力します。1～32 文字の英数字を使用できます。
Authentication Protocol	ユーザーの認証メカニズムを選択します。 • SHA-1 メッセージダイジェスト。 • MD5 ダイジェスト。 （注） MD5 認証プロトコルのサポートは間もなく廃止されます。 （注） Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a から MD5 認証を選択した場合、コンソールログには MD5 が廃止されたことを示す警告が含まれます。

フィールド名	説明
Authentication Password	ローカライズされた MD5 または SHA ダイジェストがある場合は、それぞれの文字列をパスワードとして指定できます。ダイジェストの形式は *aa:bb:cc:dd* です。ここでの *aa*、*bb*、*cc*、および *dd* は 16 進数値です。また、ダイジェストの長さは正確に 16 オクテットにする必要があります。
Privacy Protocol	SHA-1 認証プロトコルユーザーのプライバシータイプを選択します。 [AES-CFB-128]：高度暗号化規格の暗号アルゴリズムを使用します。このアルゴリズムは 128 ビットキーを用いて、暗号フィードバックモードで使用されます。 [AES-256-CFB-128]：高度暗号化規格の暗号アルゴリズムを使用します。このアルゴリズムは 256 ビットキーを用いて、暗号フィードバックモードで使用されます。
Privacy Password	プライバシーパスワードをクリアテキストまたは AES 暗号化キーのいずれかで入力します。
Group	ドロップダウンリストからグループ名を選択します。設定済みの SNMPv3 グループ名がドロップダウンリストに表示されます。

（注） SNMP 認証パスワードには、感嘆符（!）を除くすべての特殊文字を使用できます。パスワードに感嘆符（!）を使用する場合は、そのパスワードを二重引用符で囲む必要があります。たとえば、「"password!"」と入力します。

SNMP ユーザーを追加するには、[Add] をクリックします。

（オプション）トラップターゲットサーバーを設定するには、[Trap] セクションで [New Trap Target] をクリックし、次のフィールドに情報を入力します。トラップターゲットサーバーの設定を続行する前に、SNMP ユーザーを作成する必要があります。

表 *23*：トラップターゲットサーバーのパラメータ

フィールド名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ～ 65530。
IP Address	SNMP サーバーの IP アドレスを入力します。
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ～ 65535。
User Name	ドロップダウンリストから、設定されたユーザーの名前を選択します。

フィールド名	説明
Source Interface	リモート SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。

トラップターゲットサーバーを追加するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

（注） デバイステンプレートで SNMPv3 設定を SNMPv2 設定に切り替え、テンプレートのプッシュによってこの変更を適用すると、SNMP walk アプリケーションがブロックされます。これは、設定変更時に SNMPv3 の **snmp mib community-map** コマンドが削除されないためです。したがって、SNMPv3 設定テンプレートがアクティブなときは、SNMPv3 から SNMPv2 に直接切り替えることができません。SNMPv2 に切り替えるには、最初にデバイスで SNMPv3 設定を削除してから、別のコミットによって SNMPv2 テンプレートをプッシュする必要があります。

CLI テンプレートを使用した暗号化された文字列による SNMP の設定

表 *24* : 機能の履歴

機能名	リリース情報	説明
CLI テンプレートを使用した暗号化された文字列による SNMP の設定	Cisco vManage リリース 20.5.1	この機能により、CLI テンプレートまたは CLI アドオン機能テンプレートを使用して SNMP を設定できます。CLI 設定でサポートされている変数を暗号化することもできます。

CLI テンプレート機能または CLI アドオン機能テンプレートを使用して SNMP を設定し、Cisco IOS XE Catalyst SD-WAN デバイスでサポートされている変数も暗号化します。暗号化の詳細については、「Type 6 Passwords on Cisco IOS XE SD-WAN Routers」を参照してください。

（注） CLI アドオン機能テンプレートを使用してプレーンテキスト文字列を暗号化する場合、文字列は MIB で暗号化されません。

既存の SNMP コミュニティを変更して、暗号化された文字列に変換することはできません。文字列を暗号化するには、SNMP コミュニティを削除してから再作成する必要があります。

1. **[Configuration]** > **[Templates]** に移動します
2. CLI を追加するには、次のいずれかのテンプレートを使用します。
   - CLI アドオン機能テンプレート
     1. [Feature Templates] をクリックしてから、[Add Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

     2. [Select Devices] ペインで、テンプレートを作成する Cisco IOS XE Catalyst SD-WAN デバイスを選択します。
     3. [Select Template] ペインで、[Other Templates] セクションまで下にスクロールします。
     4. [CLI Add-On Template] をクリックします。
   - CLI テンプレート
     1. [Device Templates] で、[Add Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

     2. [Create Template] ドロップダウンから、[CLI Template] を選択します。
     3. [Select Devices] ペインで、テンプレートを作成する Cisco IOS XE Catalyst SD-WAN デバイスを選択します。
3. [Template Name] フィールドに、機能テンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（-）、下線（_）のみです。スペースやその他の文字を含めることはできません。
4. [Description] フィールドに、デバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
5. [CLI Configuration] ボックスで、手入力するか、カットアンドペーストするか、ファイルをアップロードして、構成を入力します。
6. パスワードや SNMP コミュニティストリングなどのプレーンテキスト値を暗号化するには、テキストを選択して [Encrypt Type6] をクリックします。
7. 実際の設定値を変数に変換するには、値を選択して [Create Variable] をクリックします。変数名を入力し、[Create Variable] をクリックします。`{{variable-name}}` の形式で変数名を直接入力することもできます。例：`{{hostname}}`。

8. **[Save]** をクリックします。新しい機能テンプレートが [Feature Template] テーブルに表示されます。
9. CLI アドオン機能テンプレートを使用するには、デバイステンプレートを次のように編集します。
   1. [Templates] ページで、[Device] をクリックします。
   2. CLI アドオン機能テンプレートを追加するデバイステンプレートを選択します。
   3. [...] をクリックし、[Edit] を選択します。
   4. 画面をスクロールして、[Additional Templates] セクションまで移動します。
   5. [CLI Add-On Template] フィールドで、以前に作成した CLI アドオン機能テンプレートを選択します。
   6. [Update] をクリックします。

CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイスでの SNMP の設定

次のセクションでは、Cisco IOS XE Catalyst SD-WAN デバイスで SNMP の設定を構成するさまざまな作業について説明します。

SNMP エージェントのシステム情報の割り当て

SNMP エージェントのシステムコンタクトとロケーションを設定します。

1. システムコンタクトを表す文字列（SNMP の担当者名）を設定します。

```
Device# config-transaction
Device(config)# snmp-server contact text
```

2. システムロケーションを表す文字列（SNMP の場所）を設定します。

```
Device(config)# snmp-server location text
```

コンテキストとネットワーク エンティティ間のマッピング設定

SNMP コンテキストと論理ネットワークエンティティ（仮想ルーティングおよび転送（VRF）など）間のマッピングを設定します。

1. SNMP コンテキストを論理ネットワークにマッピングするには、次のコマンドを使用します。

```
Device# config-transaction
Device(config)# snmp-server context context-name
```

2. 不明な SNMP コンテキストエラー時の SNMP 認証失敗（authFail）トラップを有効にします。

```
Device(config)# snmp-server trap authentication unknown-context
```

SNMPv1 および SNMPv2c の設定

（オプション）SNMPv1 および SNMPv2c を設定する際には、必要に応じて次の手順を使用し、コミュニティストリングのビューを作成または修正して SNMP マネージャがアクセスできる MIB オブジェクトを制限することができます。

1. オブジェクト識別子（OID）と SNMP ビューを作成または変更します。

```
Device# config-transaction
Device(config)# snmp-server view view-name oid-tree included
```

2. SNMP コミュニティのアクセスコントロールを作成または変更します。

```
Device(config)# snmp-server community string [view view-name][ro |rw
][access-list-number/name]
```

SNMPv3 の設定

SNMPv3 を設定していて、SNMP パケットの処理に SNMPv3 セキュリティメカニズムを使用するには、SNMP グループとパスワード付きのユーザーが設定されていることを確認します。

1. 新しい SNMPv3 サーバーグループ、または SNMP ユーザーを SNMP ビューにマッピングするテーブルを指定します。

```
Device# config-transaction
Device(config)# snmp-server group group-name v3 {auth |noauth |priv}[read
readview][write writeview
][notify notifyview][access [access-list-number | access-name][ipv6 named-access-list]
```

2. 新しいユーザーを SNMPv3 グループに設定します。

```
Device(config)# snmp-server user username group-name [remote ip-address[udp-port
port][vrf vrf-name]]
v3 [encrypted][auth {md5|sha} auth-password][access [ipv6 nacl][priv {des|3des|aes|aes
 {128|256}}privpassword]{acl-number|acl-name}]
```

（注） セキュリティ上の理由から、コマンドラインヘルプの補完候補には user コマンドは表示されません。ただし、SNMPv3 グループに新しいユーザーを設定する場合は、引き続き user コマンドを使用できます。

SNMP エージェントパケットの最大サイズの定義

SNMP エージェントが要求の受信または応答の生成を行うときに許容される最大パケットサイズを定義します。

```
Device# config-transaction
Device(config)# snmp-server packetsize byte-count
```

SNMP 通知の設定

デバイスを設定して SNMP トラップを送信します。

1. SNMP 通知操作の受信者を指定します。

```
Device# config-transaction
Device(config)# snmp-server host {host-name|ip-address}[vrf
vrf-name|traps|version{1|2c|3[auth|noauth|priv]}]community-string
[udp-port port [notification-type]|notification-type]
```

2. SNMP 通知操作値を変更します。

```
Device(config)# snmp-server  trap-source interface
```

SNMP 通知の有効化

SNMP 通知を有効または無効にできます。

指定した通知を有効にするには、コンフィギュレーション モードで次のコマンドを使用します。

1. Cisco Catalyst SD-WAN 通知に対して考えられるすべてのトラップ（omp、policy、security、system）を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps sdwan
```

2. 上昇アラームの変更に対して SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps alarms priority
```

3. 設定の変更に対して SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps config
```

4. エンティティ MIB 通知をホストに送信します。

```
Device# config-transaction
Device(config)# snmp-server enable traps entity
```

5. ディスク、メモリ、CPU 使用率などの物理コンポーネントの状態に関する情報を送信します。

```
Device# config-transaction
Device(config)# snmp-server enable traps entity-state
```

6. 仮想または非仮想 OSPF インターフェイスでの OSPF 遷移状態の変更に関する SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps ospf state-change
```

7. OSPF エラー（認証の失敗、不良パケットの問題、および設定エラー）に関する SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps ospf errors
```

8. OSFP リンクステートアドバタイズメント（LSA）に関する SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps ospf lsa
```

9. 仮想または非仮想インターフェイスでの OSPF 設定の不一致によるエラーに関する SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps ospf cisco-specific errors
```

10. 認証エラー、linkup、linkdown、warmstart、および coldstart 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps snmp
[authentication][linkup][linkdown][coldstart][warmstart]
```

11. SNMP 設定コピー通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps config-copy
```

12. SNMP 設定 CTID 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps config-ctid
```

13. SNMP Embedded Event Manager 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps event-manager
```

14. CPU しきい値違反通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps cpu threshold
```

15. フラッシュデバイスの挿入と取り外しに関する SNMP 通知を有効にします。

```
Device# config-transaction
Device(config)# snmp-server enable traps flash [insertion][removal]
```

16. メモリプールバッファの使用率が新しいピークに達したときに、デバイスが SNMP 通知を送信できるようにします。

```
Device# config-transaction
Device(config)# snmp-server enable traps memory [bufferpeak]
```

17. デバイスがシステムロギングメッセージ通知を送信できるようにします。

```
Device# config-transaction
Device(config)# snmp-server enable traps syslog
```

インターフェイス インデックス パーシステンスの設定

IF-MIB の ifIndex 値をグローバルに有効にして、リブート後も保持されるようにすることができます。この設定により、SNMP を使用する特定のインターフェイスを一貫して識別できるようになります。

```
Device# config-transaction
Device(config)# snmp ifmib ifindex persist
```

Cisco SD-WAN Manager を使用して SNMP トラップを設定するには、CLI アドオン機能テンプレートで指定された情報を使用して、お使いの環境に適した設定を入力します。次に、SNMPv2c を使用して 172.16.1.111 と 172.16.1.27 にトラップを送信し、SNMPv3 を使用してホスト 172.16.1.33 にトラップを送信するように SNMP を設定する方法の例を示します。SNMP トラップは、VRF ルーティングテーブルおよびアドレスファミリサブモードを設定することによって送信されます。

```
config-transaction
!
        vrf definition 172
        address-family ipv4
        exit-address-family

        snmp-server contact Admin
        snmp-server location Lab-7

        snmp-server context CISCOCONTEXT
        no snmp-server trap authentication unknown-context
!
        snmp-server view v2 1.3.6.1.6.3.15 included
        snmp-server community public view v2 ro
        snmp-server view v3 1.3.6.1.6.3.18 included
!
        snmp-server community private view v3 ro 5
        snmp-server community public view v3 ro
        snmp-server group groupNoAuthNoPriv v3 noauth read v3

!
        snmp-server packetsize 1300
        snmp-server host 172.16.1.27 vrf 172 version 2c public udp-port 162
        snmp-server host 172.16.1.111 vrf 172 version 2c public udp-port 161
       snmp-server host 172.16.1.33 vrf 172 version 3 auth v3userAuthPriv udp-port 16664


        snmp-server trap-source Loopback0
!
        snmp-server enable traps sdwan
        snmp-server enable traps alarms informational
        snmp-server enable traps config
        snmp-server enable traps entity
        snmp-server enable traps entity-state
        snmp-server enable traps snmp authentication coldstart linkdown linkup warmstart
        snmp-server enable traps ospf state-change
        snmp-server enable traps ospf errors
        snmp-server enable traps ospf lsa
        snmp-server enable traps ospf cisco-specific errors!
        snmp-server enable traps ospf state-change
        snmp-server enable traps ospf errors
!
        snmp ifmib ifindex persist
!
```

Cisco IOS XE Catalyst SD-WAN デバイス での SNMP トラップの検証

次に、SNMPv3 で設定されたユーザー情報を表示する **show snmp user** コマンドの出力例を示します。

```
Device# show snmp user

User name: v3userAuthPriv
Engine ID: 80000009030000C88B487400
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: groupAuthPriv

User name: v3userNoAuthNoPriv
Engine ID: 80000009030000C88B487400
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None
Group-name: groupNoAuthNoPriv
```

次に、**request platform software sdwan root-cert-chain uninstall** コマンドを使用して Cisco Catalyst 8000V のルート証明書をアンインストールした後に表示されるトラップ通知の例を示します。

```
2021-06-15 15:26:38 UDP: [198.51.100.1]:61114->[172.16.53.199]:162 [UDP:
[198.51.100.1]:61114->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (5155837) 14:19:18.37
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityRootCertChainUninstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

次に、**request platform software sdwan root-cert-chain install** コマンドを使用して Cisco Catalyst 8000V のルート証明書をインストールした後に表示されるトラップ通知の例を示します。

```
2021-06-15 01:16:55 UDP: [10.6.40.204]:50433->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50433->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2143576) 5:57:15.76
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityRootCertChainInstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

次に、**clear sdwan installed-certificates** コマンドを使用して Cisco Catalyst 8000V のインストール済み証明書を削除した後に表示されるトラップ通知の例を示します。

```
2021-06-15 14:18:26 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (103213) 0:17:12.13
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityClearInstalledCertificate
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

次に、**request platform software sdwan csr upload flash** コマンドを使用して Cisco Catalyst 8000V の証明書署名要求証明書を作成した後に表示されるトラップ通知の例を示します。

```
Uploading CSR via VPN 0
Enter organization-unit name : CISCO
Re-enter organization-unit name : CISCO
Generating private/public pair and CSR for this "vedge" device
Generated CSR for vedge device
Copying /usr/share/viptela/server.csr to /bootflash/c8kv1.csr via VPN 0
CSR upload successful
c8kv1#

2021-06-15 14:20:14 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (114062) 0:19:00.62
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityNewCsrGenerated
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

次に、**request platform software sdwan certificate install** コマンドを使用して Cisco Catalyst 8000V の署名付き証明書をインストールした後に表示されるトラップ通知の例を示します。

```
Installing certificate via VPN 0
Changing ownership of vedge_certs to binos...
Copying /bootflash/c8kv1.crt to /tmp/vconfd/server.crt.tmp via VPN 0
Got certificate_id 0123CF for /tmp/vconfd/server.crt.tmp vmanage_signed false
cp -f "/usr/share/viptela/tmp_csr/server.key" "/usr/share/viptela/server.key"
moving temp Cert "/tmp/vconfd/server.crt.tmp" to Cert
"/usr/share/viptela/vedge_certs/client_0123CF.crt"

Successfully installed the certificate 0

2021-06-15 14:24:02 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (136870) 0:22:48.70
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateInstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

次に、**show control local-properties** コマンドを使用して期限切れになる証明書のトラップ通知の例を示します。Cisco Catalyst 8000V の証明書は本日期限切れになりますが、まだ失効していません。

```
2021-07-06 21:04:17 UDP: [1.6.40.204]:53342->[172.27.53.199]:162 [UDP:
[1.6.40.204]:53342->[172.27.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (41478) 0:06:54.78
```

```
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateExpiring
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityCertificateType.0 = INTEGER: enterprise(2)
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityCertificateSerialNumber.0 = STRING: "01240F"

CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityIssuer.0 = STRING: "XCA"
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityDaysToExpiry.0 = INTEGER: 1
```

次に、**show control local-properties** コマンドを使用して Cisco Catalyst 8000V デバイスで期限切れになった証明書のトラップ通知を表示する例を示します。

```
2021-06-15 15:59:16 UDP: [209.165.202.129]:49387->[172.16.0.199]:162 [UDP:
[209.165.202.129]:49387->[172.16.0.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (44510) 0:07:25.10
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateExpired
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

CLI を使用した Cisco vEdge デバイスでの SNMP の設定

SNMP の有効化

デフォルトでは、SNMP は Cisco vEdge デバイスで無効になっています。これを有効にして SNMP バージョン 1、2、および 3 のサポートを提供するには、次の手順を実行します。

```
vEdge(config)# snmp
vEdge(config-snmp)# no shutdown
```

SNMP を有効にすると、デバイスで MIB の使用、トラップの生成、SNMP walk アプリケーションからの要求に対する応答を実行できるようになります。

SNMP ビューの設定

OID とともに SNMP ビューを作成し、SNMP サーバーで SNMP 情報を使用できるようにするには、SNMP ビューと対応する OID サブツリーを設定します。

```
vEdge(config-snmp)#  view string
vEdge(config-snmp)#  oid oid-subtree
```

OID サブツリーでは、任意の位置でワイルドカード *（アスタリスク）を使用して、その位置の任意の値と一致させることができます。

次に、SNMP MIB のインターネット部分のビューを作成する例を示します。

```
vEdge(config)# snmp view v2 oid 1.3.6.1
```

次に、Cisco Catalyst SD-WAN MIB のプライベート部分のビューを作成する例を示します。

```
vEdge(config)# snmp view vEdge-private oid 1.3.6.1.4.1.41916
```

SNMP ビューへのアクセスの設定

SNMP ビューにアクセスするために認証権限を要求するには、SNMPv3 を設定します。これを行うには、SNMPv3 ユーザーの認証情報と、SNMP ビューのグループおよびビューへのアクセスに必要な認証情報を設定します。

SNMPv3 ユーザーの認証情報を設定するには、ユーザーを作成し、SNMP グループに設定する認証タイプに応じて、認証レベルとプライバシーレベルを割り当てます（以下のように **snmp group** コマンドを使用します）。

```
vEdge(config)# snmp user username
vEdge(config-user)# auth authentication
vEdge(config-user)# auth-password password
vEdge(config-user)# priv privacy
vEdge(config-user)# priv-password password
```

ユーザー名は 1 ～ 32 文字の文字列で指定できます。

authentication コマンドで、ユーザーの認証権限を有効にします。パスワードはクリアテキスト文字列または AES 暗号化キーとして入力できます。

privacy コマンドで、ユーザーのプライバシーメカニズムを有効にします。パスワードはクリアテキスト文字列または AES 暗号化キーとして入力できます。

次に、SNMPv3 ユーザーを SNMP グループに関連付けます。

```
vEdge(config-user)# group group-name
```

group-name は、**snmp group** コマンドで設定するビューのグループ名です。

ビューのグループを設定するには、次の手順を実行します。

```
Device(config)# snmp group group-name authentication
Device(config-group)# view view-name
```

グループ名には、1 ～ 32 文字の文字列を指定できます。

グループに使用する認証は、次のいずれかになります。

- **auth-no-priv**：選択した認証アルゴリズムを使用して認証します。この認証方式を設定する場合は、このグループのユーザーに認証と認証パスワードを設定する必要があります（**snmp user auth** および **auth-password** コマンドを使用）。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、**auth-no-priv** 認証方式はサポートされていません。

- **auth-priv**：選択した認証アルゴリズムを使用して認証します。この認証方式を設定する場合は、このグループのユーザーに認証と認証パスワード（**snmp user auth** および **auth-password** コマンドを使用）、およびプライバシーとプライバシーのパスワード（**snmp user priv** および **priv-password** コマンドを使用）を設定する必要があります。

- **no-auth-no-priv**：ユーザー名に基づいて認証します。この認証を構成する場合、認証またはプライバシー資格情報を構成する必要はありません。

（注） SNMP ユーザーを新しいグループに移動し、古いグループを削除するには、2 つの個別のトランザクションを使用します。SNMP ユーザーの新しいグループへの移動と、同じトランザクションでの古いグループの削除はサポートされていません。

ビュー名は、**snmp view** コマンドを使用して設定する SNMP ビューの名前です。

連絡先パラメータの設定

Cisco vEdge デバイスごとに、SNMP ノード名、物理的な場所、およびデバイスの担当者または担当エンティティの連絡先情報を設定できます。

```
vEdge(config)#  snmp
vEdge(config-snmp)#  name string
vEdge(config-snmp)#  location string
vEdge(config-snmp)#  contact string
```

いずれかの文字列にスペースが含まれている場合は、文字列全体を引用符（""）で囲みます。

SNMP コミュニティの設定

SNMP コミュニティストリングでは、SNMP サーバーシステムとクライアントシステムとの関係を定義します。この文字列は、サーバーへのクライアントのアクセスを制御するためのパスワードのように機能します。コミュニティストリングを設定するには、**community** コマンドを使用します。

```
vEdge(config-snmp)#  community name
vEdge(config-community-name)# authorization read-only
vEdge(config-community-name)# view string
```

コミュニティ名の長さは 1 ～ 32 文字で指定できます。山括弧（<および>）を含めることができます。名前にスペースを含める場合は、名前全体を引用符（" "）で囲みます。

view コマンドを使用して、表示する MIB ツリーの部分を指定します。*string* は、以下で説明するように **snmp view** コマンドを使用して設定されたビューレコードの名前です。

Cisco Catalyst SD-WAN ソフトウェアは、標準インターフェイス、MIB、IF-MIB、およびシステム MIB（SNMPv2-MIB）をサポートします。これらは、Cisco Catalyst SD-WAN ソフトウェアをインストールすると Cisco vEdge デバイスに自動的にロードされます。エンタープライズ MIB のリストについては、「Supported SNMP MIBs」を参照してください。Cisco Catalyst SD-WAN ソフトウェアでサポートされている MIB では書き込み操作が許可されていないため、読み取り専用の許可（デフォルトの許可）のみを設定できます。

ビューレコードの設定

SNMP MIB の一部を表示するように設定するには、**view** コマンドを使用します。

```
vEdge(config-snmp)#  view string
vEdge(config-view)# oid oid-subtree [exclude]
```

たとえば、SNMP MIB のインターネット部分を表示するには、OID 1.3.6.1 を設定します。

```
vEdge(config-snmp)# view v2 oid 1.3.6.1
```

Cisco Catalyst SD-WAN MIB のプライベート部分を表示するには、OID 1.3.6.1.4.1.41916 を設定します。

SNMP コンフィギュレーション コマンド

SNMP を設定するには、次のコマンドを使用します。

```
snmp
  community name
    authorization (read-only | read-write)
    view string
  contact string
  group group-name authentication
    view string
  location string
  name string
  [no] shutdown
  trap
    group group-name
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name group-name
      source-interface interface-name
  user username
    auth authentication
    auth-password password
    group group-name
    priv privacy
    priv-password password
```

SNMP モニタリングコマンド

SNMP をモニターするには、次のコマンドを使用します。

SNMP をモニターするには、**show running-config snmp** コマンドを使用します。コマンドの出力には、Cisco vEdge デバイスで実行しているアクティブな設定が表示されます。

Cisco vEdge デバイスでの SNMP トラップの検証

次に、**show full-configuration** コマンドの出力例を示します。

```
vEdge(config-snmp)# show full-configuration
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 group groupAuthPriv auth-priv
  view v2
 !
 user noc-staff
  auth          sha
  auth-password $8$UZwdx9eu49iMElcJJINm0f202N8/+RGJvxO+e9h0Uzo=
  priv          aes-cfb-128
```

```
  priv-password $8$eB/I+VXrAWDw/yWmEqLMsgTcs0omxcHldkVN2ndU9QI=
  group         groupAuthPriv
 !
!
```

次に、Cisco SD-WAN リリース 20.5.1 で導入された **show running-config snmp** コマンドの出力例を示します。

```
vEdge(config-snmp)# show running-config snmp
snmp
 no shutdown
 view v3
  oid 1.3.6.1
!
 group groupAuthPriv auth-priv
  view v3
!
 user v3userAuthPriv-sha-aes
  auth          sha-256
  auth-password $8$QiM+RsTn8WBaufWNAPleqzhYtNSSQxtDPciQayxz73s=
  priv          aes-256-cfb-128
  priv-password $8$rsgqMKrWt4JwvBIrWW0gG/VH9tiMl7oAHjFbzrd818k=
  group         groupAuthPriv
 !
!
```

次に、ディスク使用率が 75% を超え、ネットワーク管理サーバー（NMS）に送信されるトラップ通知の例を示します。

```
2021-06-21 22:35:05 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53772780) 6 days, 5:22:07.80
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:7:3.0,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER:major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is above 75%." Please clean
 up unnecessary files. If disk usage grows beyond 90%, system will attempt to recover
disk space by deleting files"
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 1174
```

ディスク使用率が正常になると、トラップ通知が NMS に送信されます。

```
2021-06-21 22:40:29 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53805175) 6 days, 5:27:31.75
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:12:27.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is below 60%."
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 7362
```

次に、ディスク使用率が 75% を超えた場合のトラップ通知の例を示します。

```
2021-06-21 22:35:05 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.27.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53772780) 6 days, 5:22:07.80
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:7:3.0,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is above 75%." Please clean
 up unnecessary files. If disk usage grows beyond 90%, system will attempt to recover
disk space by deleting files
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 1174
```

ディスク使用率が 60% 未満に低下すると、トラップ通知が NMS に送信されます。

```
2021-06-21 22:40:29 UDP: [172.27.58.143]:54392->[172.27.53.199]:162 [UDP:
[172.27.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53805175) 6 days, 5:27:31.75
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:12:27.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is below 60%."
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 7362
```

次に、CPU 使用率が高レベルに上昇し、その後通常のレベルに戻った場合のトラップ通知の例を示します。

```
2021-06-21 22:53:49 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53885189) 6 days, 5:40:51.89
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:47.2,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage is above 75%"
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.01"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "80.40"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "18.59"

2021-06-21 22:53:53 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53885589) 6 days, 5:40:55.89
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:51.2,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: critical(1)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage is above 90% (critically
 high)"
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.51"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "98.49"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "0.00"

2021-06-21 22:54:01 UDP: [172.16.58.143]:54392->[172.16.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.16.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53886390) 6 days, 5:41:03.90
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:59.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage back to normal level"
```

```
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.52"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "1.52"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "96.97"
```

次に、システムメモリの使用率が 75% を超えた場合のトラップ通知を示します。

```
2021-06-21 23:15:22 UDP: [172.16.58.143]:54392->[172.16.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.16.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (54014426) 6 days, 6:02:24.26
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemMemoryUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:47:19.5,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System memory usage is above 75%"
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 3902
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 965
```

次に、間もなく期限切れになる証明書に対するトラップ通知を示します。ここでは、Cisco vEdgeデバイスの証明書が本日期限切れになりますが、まだ失効していません。

```
2021-06-15 16:53:29 UDP: [172.16.58.43]:56734->[172.16.53.199]:162 [UDP:
[172.16.58.43]:56734->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (92594) 0:15:25.94
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSecuritySecurityCertificateExpiring
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-15,23:53:3.5,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSecurityCertificateType.0 = INTEGER: enterprise(2)
VIPTELA-TRAPS::viptelaSecurityCertificateSerialNumber.0 = STRING: "0123D1"
VIPTELA-TRAPS::viptelaSecurityIssuer.0 = STRING: "XCA"
VIPTELA-TRAPS::viptelaSecurityDaysToExpiry.0 = INTEGER: 0
```

Cisco vEdge デバイスでの SNMP トラップの設定

SNMP トラップは、シスコのデバイスが SNMP 管理サーバーに送信する非同期通知です。トラップにより、デバイスで発生するイベント（正常なものであっても重大なものであっても）が管理サーバーに通知されます。デフォルトでは、SNMP トラップは SNMP サーバーに送信されません。SNMPv3 の場合は、通知の PDU タイプが SNMPv2c inform（InformRequest-PDU）または trap（Trapv2-PDU）のいずれかであることに注意してください。

SNMP トラップを設定するには、トラップを定義してトラップを受信する SNMP サーバーを設定します。

（注） **trap group** UI オプションは、Cisco SD-WAN リリース 20.1.1 以降ではサポートされていません。

Cisco vEdge デバイスで収集するトラップのグループを設定するには、**trap group** コマンドを使用します。

（注） Cisco IOS XE Catalyst SD-WAN デバイスでトラップのグループを設定する必要はありません。

```
vEdge(config-snmp)#  trap group group-name
vEdge(config-group)# trap-type level severity
```

1 つのトラップグループに複数のトラップタイプを含めることができます。設定では、行ごとに 1 つのトラップタイプを指定し、各トラップタイプに 1 ～ 3 つの重大度を追加できます。設定プロセスの図については、次の設定例を参照してください。

トラップを受信する SNMP サーバーを設定するには、Cisco vEdge デバイスで **trap target** コマンドを使用します。

（注） Cisco IOS XE Catalyst SD-WAN デバイスでトラップを受信するように SNMP サーバーを設定する必要はありません。

```
vedge(config-snmp)#  trap target vpn  vpn-id ipv4-address udp-port
vedge(config-target)# group-name name
vedge(config-target)# community-name community-name
vedge(config-target)# source-interface interface-name
```

SNMP サーバーごとに、サーバーが配置されている VPN の識別子、サーバーの IPv4 アドレス、および接続するサーバーの UDP ポートを指定します。トラップサーバーのアドレスを設定する場合は、IPv4 アドレスを使用する必要があります。IPv6 アドレスは使用できません。

group-name コマンドで、設定済みのトラップグループをサーバーに関連付けます。そのグループのトラップが SNMP サーバーに送信されます。

community-name コマンドで、設定済みの SNMP コミュニティを SNMP サーバーに関連付けます。

source-interface コマンドで、トラップ情報を受信している SNMP サーバーへトラップを送信するために使用するインターフェイスを設定します。このインターフェイスをサブインターフェイスにすることはできません。

次の設定例では、すべてのトラップが 1 つの SNMP サーバーに送信され、重要なトラップのみが別の SNMP サーバーに送信されます。2 つの SNMP トラップグループと 2 つのターゲット SNMP サーバーが設定されています。

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# snmp
vEdge(config-snmp)# view community-view
vEdge(config-view-community-view)# exit
vEdge(config-snmp)# community public
vEdge(config-community-public)# authorization read-only
vEdge(config-community-public)# view community-view
vEdge(config-community-public)# exit
vEdge(config-snmp)# trap group all-traps
```

```
vEdge(config-group-all-traps)# all level critical major minor
vEdge(config-group-all)# exit
vEdge(config-group-all-traps)# exit
vEdge(config-snmp)# trap group critical-traps
vEdge(config-group-critical-traps)# control level critical
vEdge(config-group-control)# exit
vEdge(config-group-critical-traps)# exit
vEdge(config-snmp)# trap target vpn 0 10.0.0.1 162
vEdge(config-target-0/10.0.0.1/162)# group-name all-traps
vEdge(config-target-0/10.0.0.1/162)# community-name public
vEdge(config-target-0/10.0.0.1/162)# exit
vEdge(config-snmp)# trap target vpn 0 10.0.0.2 162
vEdge(config-target-0/10.0.0.2/162)# group-name critical-traps
vEdge(config-target-0/10.0.0.2/162)# community-name public
vEdge(config-target-0/10.0.0.2/162)# exit
vEdge(config-snmp)# show full-configuration
snmp
 view community-view
 !
 community public
  view          community-view
  authorization read-only
 !
 group groupAuthPriv auth-priv
  view v2
 !
 user u1
  auth          sha
  auth-password $8$UZwdx9eu49iMElcJJINm0f202N8/+RGJvxO+e9h0Uzo=
  priv          aes-cfb-128
  priv-password $8$eB/I+VXrAWDw/yWmEqLMsgTcs0omxcHldkVN2ndU9QI=
  group         groupAuthPriv
 !
 trap target vpn 0 10.0.0.1 162
  group-name     all-traps
  community-name public
 !
 trap target vpn 0 10.0.0.2 162
  group-name     critical-traps
  community-name public
 !
 trap group all-traps
  all
   level critical major minor
  !
 !
 trap group critical-traps
  bfd
   level critical
  !
  control
   level critical
  !
  hardware
   level critical
  !
  omp
   level critical
  !
 !
!
vEdge(config-snmp)#
```

SNMP トラップと通知に関する情報

SNMPトラップでは、複数の重大度（クリティカル、メジャー、およびマイナー）がサポートされています。

次の表では、*trap-type* が変数の 1 つとなります。

表 *25 : Cisco IOS XE Catalyst SD-WAN* デバイスの *SNMP* トラップ

トラップ タイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
app-route	メジャー	AppRouteSlaChange	トンネルに対してSLAクラスが変更されると、この SNMP トラップが生成されます。
control	メジャー	ciscoSdwanSecurityControlConnectionStateChange	Cisco IOS XE Catalyst SD-WAN デバイス制御接続の状態が変更されると、SNMP トラップが生成されます。たとえば、Cisco Catalyst SD-WAN ルータ接続が確立された場合が挙げられます。
BFD	メジャー	ciscoSdwanBfdStateChange	Cisco IOS XE Catalyst SD-WAN デバイスBFDセッション状態が変更されると、SNMP トラップが生成されます。 BFD トラップは、Cisco IOS XE リリース17.8.1a以降でサポートされています。

トラップ タイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
omp	メジャー	ciscoSdwanOmpOmpNumberOfVsmartsChange	Cisco SD-WAN コントローラの数が変更されると、SNMP トラップが生成されます。
		ciscoSdwanOmpOmpPeerStateChange	ピアの状態が変更されると、SNMP トラップが生成されます。
		ciscoSdwanOmpOmpStateChange	OMP システムの動作状態が変更されると、SNMP トラップが生成されます。
		ciscoSdwanOmpOmpPolicy	Cisco SD-WAN コントローラから転送ポリシーが受信されると、SNMP トラップが生成されます（Cisco IOS XE SD-WAN デバイスでのみ）。
policy	メジャー	ciscoSdwanPolicyAccessListAssociationStatus	Cisco IOS XE Catalyst SD-WAN デバイスのアクセスポリシーが Cisco SD-WAN Manager から設定されると、SNMP トラップが生成されます。
		ciscoSdwanPolicyDataPolicyAssociationStatus	Cisco IOS XE Catalyst SD-WAN デバイスのデータポリシーが Cisco SD-WAN Manager から設定されると、SNMP トラップが生成されます。
		ciscoSdwanPolicySlaViolationPktDrop	パケットのドロップが原因で Cisco IOS XE Catalyst SD-WAN デバイスの SLA ポリシーに違反すると、SNMP トラップが生成されます。
	マイナー	ciscoSdwanPolicySlaViolation	Cisco IOS XE Catalyst SD-WAN デバイスの SLA ポリシーに違反すると、SNMP トラップが生成されます。

トラップ タイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
security	メジャー	ciscoSdwanSecuritySecurityCertificateExpired	Cisco IOS XE Catalyst SD-WAN デバイスの証明書が失効すると、SNMP トラップが生成されます。
		ciscoSdwanSecuritySecurityCertificateExpiring	証明書の有効期限から 60 日前を起点に、Cisco IOS XE Catalyst SD-WAN デバイスの証明書の有効期限が近づくと、SNMP トラップが生成されます。
		ciscoSdwanSecuritySecurityRootCertChainUninstalled	ルート証明書が正常にアンインストールされると、SNMP トラップが生成されます。
		ciscoSdwanSecuritySecurityClearInstalledCertificate	Cisco IOS XE Catalyst SD-WAN デバイスで Cisco Catalyst SD-WAN ルート証明書がアンインストールされると、SNMP トラップが生成されます。 証明書の失効に関する詳細については、「Support for SNMP Traps on Cisco Catalyst SD-WAN Devices」を参照してください。
		ciscoSdwanSecuritySecurityVsmartEntryAdded	Cisco IOS XE Catalyst SD-WAN デバイスが Cisco SD-WAN コントローラ に追加されると、SNMP トラップが生成されます。
	マイナー	ciscoSdwanSecuritySecurityRootCertChainInstalled	ルート証明書がインストールされると、SNMP トラップが生成されます。
		ciscoSdwanSecuritySecurityCertificateInstalled	セキュリティ証明書がインストールされると、SNMP トラップが生成されます。
		ciscoSdwanSecuritySecurityNewCsrGenerated	新しい証明書署名要求が生成されると、SNMP トラップが生成されます。

トラップ タイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
		ciscoSdwanSecurityTunnelIpsecRekey	トンネル IPSec のキーが再生成されると、SNMP トラップが生成されます。
system	メジャー	ciscoSdwanSystemPseudoCommitStatus	Cisco SD-WAN Manager が仮設定（疑似コミット）を Cisco IOS XE Catalyst SD-WAN デバイスにプッシュすると、SNMP トラップが生成されます。
	マイナー	ciscoSdwanSystemDomainIdChange	Cisco Catalyst SD-WAN ドメイン ID が Cisco IOS XE Catalyst SD-WAN デバイスで変更されると、SNMP トラップが生成されます。
		ciscoSdwanSystemOrgNameChange	Cisco IOS XE Catalyst SD-WAN デバイスで Cisco Catalyst SD-WAN の組織名が変更されると、SNMP トラップが生成されます。
		ciscoSdwanSystemSiteIdChange	Cisco IOS XE Catalyst SD-WAN デバイスで Cisco Catalyst SD-WAN のサイト ID が 変更されると、SNMP トラップが生成されます。
		ciscoSdwanSystemSystemCommit	Cisco IOS XE Catalyst SD-WAN デバイスの設定が変更され、コミットされると、SNMP トラップが生成されます。
		ciscoSdwanSystemSystemIpChange	Cisco IOS XE Catalyst SD-WAN デバイスのシステム IP が変更されると、SNMP トラップが生成されます。

表 *26 : Cisco vEdge* デバイスの *SNMP* トラップ

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
all	—	すべてのクリティカルトラップが、この表の次のセルに表示されます。	—
app-route	メジャー	viptelaAppRouteSlaChange	トンネルの SLA クラスが変更されると、SNMP トラップが生成されます。
BFD (bfd)	メジャー	viptelaBfdBfdStateChange	BFD セッション状態が変更されると、SNMP トラップが生成されます。
bridge	マイナー	viptelaBridgeCreation	CLI を介してブリッジが作成されると、SNMP トラップが生成されます。
		viptelaBridgeDeletion	CLI を介してブリッジが削除されると、SNMP トラップが生成されます。
		viptelaBridgeMaxMacReached	DOT1X STA MAC のしきい値を超えると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
control	クリティカル	viptelaSecurityControlNoActiveVbond	Cisco SD-WAN Validator との DTLS ピアリングが削除されると、SNMP トラップが生成されます。
	メジャー	viptelaSecurityControlConnectionAuthFail	制御接続の認証が失敗すると、SNMP トラップが生成されます。
		viptelaSecurityControlConnectionStateChange	ピアがアップまたはダウンとマークされ、制御接続の状態が変更されると、SNMP トラップが生成されます。
		viptelaSecurityControlConnectionTlocIpChange	制御接続 TLOC IP が変更されると、SNMP トラップが生成されます。
		viptelaSecurityControlVbondStateChange	Cisco SD-WAN Validator が SNMP トラップを送信して管理ステータスを表示すると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
dhcp	メジャー	viptelaVpnDhcpServerStateChange	DHCP サーバーの状態が変更されると、SNMP トラップが生成されます。
	マイナー	viptelaVpnDhcpAddressAssigned	DHCP アドレスが割り当てられると、SNMP トラップが生成されます。
		viptelaVpnDhcpAddressReleased	DHCP アドレスが解放されると、SNMP トラップが生成されます。
		viptelaVpnDhcpAddressRenewed	DHCP アドレスが更新されると、SNMP トラップが生成されます。
		viptelaVpnDhcpRequestRejected	DHCP サーバーに対するクライアントの要求が拒否されると、SNMP トラップが生成されます。
		viptelaVpnDhcpServerStateChange	DHCP サーバーの状態が変更されると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
hardware	メジャー	viptelaHardwareEmmcFault	eMMC障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwareFanFault	ファンの障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwareFantrayFault	ファントレイの障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwareFlashFault	フラッシュの障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwarePemFault	PEMの障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwarePemStateChange	PEMの状態が変更されると、SNMPトラップが生成されます。
		viptelaHardwarePimFault	PIMの電源障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwarePimStateChange	PIMモジュールの状態が変更されると、SNMPトラップが生成されます。
		viptelaHardwareSdcardFault	SDカードの障害が検出またはクリアされると、SNMPトラップが生成されます。
		viptelaHardwareSfpStateChange	SFPの状態が変更されると、SNMPトラップが生成されます。
		viptelaHardwareSfpSupportState	SFPのサポート状態が変更されると、SNMPトラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
		viptelaHardwareTempsensorFault	温度センサーの障害が検出またはクリアされると、SNMP トラップが生成されます。
		viptelaHardwareTempsensorState	温度センサーの状態が変更されると、SNMP トラップが生成されます。
		viptelaHardwareUsbStateChange	USB の状態が変更されると、SNMP トラップが生成されます。
omp	メジャー	viptelaOmpOmpNumberOfVsmartsChange	Cisco SD-WAN コントローラの数が変更されると、SNMP トラップが生成されます。
		viptelaOmpOmpPeerStateChange	ピアの状態が変更されると、SNMP トラップが生成されます。
		viptelaOmpOmpStateChange	OMP システムの動作状態が変更されると、SNMP トラップが生成されます。
		viptelaOmpOmpPolicy	Cisco SD-WAN コントローラから転送ポリシーを受信すると、SNMP トラップが生成されます（Cisco vEdge ルータのみ）。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
policy	メジャー	viptelaPolicyAccessListAssociationStatus	SNMP トラップは、アクセスリストの関連付けステータスに対して生成されます。
		viptelaPolicyDataPolicyAssociationStatus	SNMP トラップは、データポリシーの関連付けステータスに対して生成されます。
		viptelaPolicySlaViolationPktDrop	パケットの SLA クラス違反がドロップされると、SNMP トラップが生成されます。
		viptelaPolicySlaConfig	SLA クラスが追加、変更、または削除されると、SNMP トラップが生成されます。
		viptelaPolicyZbfFlowTableFull	フローテーブルがいっぱいになると、SNMP トラップが生成されます。
		viptelaPolicyZbfClearFlowTableFull	フローテーブルのしきい値が下がると、SNMP トラップが生成されます。
		viptelaPolicyZbfHalfOpenHit	ハーフオープン TCP 接続（SYN フラッド）が最大数に達すると、SNMP トラップが生成されます。
		viptelaPolicyZbfClearHalfOpenHit	ハーフオープン TCP 接続数（SYN フラッド）が減少すると、SNMP トラップが生成されます。
		viptelaPolicyAppListAppAliasesNotify	アプリケーションエイリアス（対応する NBAR アプリケーション）のリストが追加または変更されると、SNMP トラップが生成されます。
		viptelaPolicyAppListUnsupportedAppNotify	

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
			サポート対象外のアプリケーション（対応する NBAR アプリケーションがない）のリストが追加または変更されると、SNMP トラップが生成されます。
	マイナー	viptelaPolicySlaViolation	SLA クラスに違反すると、SNMP トラップが生成されます。
		viptelaPolicyZbfFlowCreation	ゾーンペアに一致するフローが作成されると、SNMP トラップが生成されます。
		viptelaPolicyZbfFlowDeletion	ゾーンペアに関連するフローがタイムアウトにより削除されるか、ゾーンペアが削除されると、SNMP トラップが生成されます。
		viptelaPolicyZbfPktLog	ZBFW パケットログが受信されると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
routing	メジャー	viptelaVpnBgpPeerStateChange	BGP ピアの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnOspfInterfaceStateChange	OSPF インターフェイスの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnOspfNeighborStateChange	OSPF ネイバーの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnPimInterfaceStateChange	PIM インターフェイスの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnPimNeighborStateChange	PIM ネイバーの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnPimTunnelStateChange	PIM ネイバーのトンネル状態が変更されると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
security	メジャー	viptelaSecuritySecurityCertificateExpired	証明書の有効期限が切れると、SNMP トラップが生成されます。
		viptelaSecuritySecurityCertificateExpiring	SNMP トラップは、証明書が失効する 60 日前から繰り返し生成されます。
		viptelaSecuritySecurityClearInstalledCertificate	公開キー、秘密キー、ルート証明書を含む、デバイス上のすべての証明書が消去され、デバイスが工場出荷時のデフォルト状態に戻ると、SNMP トラップが生成されます。
		viptelaSecuritySecurityRootCertChainUninstalled	ルート証明書キーチェーンを含むファイルがコントローラまたはルータから削除されると、SNMP トラップが生成されます。
		viptelaSecuritySecurityVedgeEntryAdded	csv または json ファイルを介して新しい Cisco vEdge デバイスのエントリが追加されると、コントローラで SNMP トラップが生成されます。
		viptelaSecuritySecurityVedgeEntryRemoved	Cisco vEdge デバイスのエントリが削除されるか、csv または json ファイルを介して削除されると、コントローラで SNMP トラップが生成されます。
		viptelaSecuritySecurityUnclaimedVedgeEntryAdded	要求されていない Cisco vEdge デバイスのエントリが追加されると、SNMP トラップが生成されます。
		viptelaSecuritySecurityVedgeSerialFileUploaded	

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
			WAN エッジのシリアル番号ファイルが Cisco SD-WAN Manager サーバーにアップロードされると、SNMP トラップが生成されます。
		viptelaSecurityVbondRejectVedgeConnection	チャレンジ ACK がコントローラで受信されたが検証できないと、SNMP トラップが生成されます。
		viptelaSecuritySecurityVsmartEntryAdded	新しい Cisco SD-WAN コントローラ シリアル番号のファイルが追加されると、すべてのデバイスで SNMP トラップが生成されます。
		viptelaSecuritySecurityVsmartEntryRemoved	新しい Cisco SD-WAN コントローラ シリアル番号のファイルが削除されると、すべてのデバイスで SNMP トラップが生成されます。
		viptelaSecuritySecurityVsmartSerialFileUploaded	Cisco SD-WAN Manager がオーバーレイネットワークにある Cisco SD-WAN コントローラ の証明書のシリアル番号を含むファイルをアップロードすると、SNMP トラップが生成されます。
		viptelaSecurityDeviceTemplateAttachedDuringZtp	ZTP プロセス中にエッジデバイスが ZTP に登録され、基本テンプレートが Cisco SD-WAN Manager で事前設定されている場合、Cisco SD-WAN Manager で SNMP トラップが生成されます。
		viptelaSecurityDeviceTemplateMissing	

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
			ZTP プロセス中にエッジデバイスが ZTP に登録され、基本テンプレートが Cisco SD-WAN Manager で事前設定されていない場合、Cisco SD-WAN Manager で SNMP トラップが生成されます。
	マイナー	viptelaSecuritySecurityCertificateInstalled	証明書がデバイスでインストールされると、SNMP トラップが生成されます。
		viptelaSecuritySecurityNewCsrGenerated	コントローラまたはルータで証明書署名要求（CSR）が生成されると、SNMP トラップが生成されます。
		viptelaSecuritySecurityRootCertChainInstalled	ルート証明書キーチェーンを含むファイルがエッジデバイスにインストールされると、SNMP トラップが生成されます。
		viptelaSecurityTunnelIpsecManualRekey	Cisco vEdge デバイスで request security ipsec-rekey が実行されると、SNMP トラップが生成されます。
		viptelaSecurityTunnelIpsecRekey	トンネル IPSec のキーがタイマーによって再生成されると、SNMP トラップが生成されます。
		viptelaSecurityVmanageConnectionPreferenceChanged	TLOC の Cisco SD-WAN Manager-conn-preference が変更されると、デバイスで SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
system	クリティカル	viptelaSystemCpuUsage	システムの CPU 使用率が 90% を超えると、SNMP トラップが生成されます。
		viptelaSystemDiskUsage	システムのディスク使用率が 90% を超えると、SNMP トラップが生成されます。
		viptelaSystemMemoryUsage	システムのメモリ使用率が 90% を超えると、SNMP トラップが生成されます。
	メジャー	viptelaSystemAaaAdminPwdChange	ルータまたはコントローラで AAA ユーザー admin のパスワードが変更されると、SNMP トラップが生成されます。
		viptelaSystemCpuUsage	システムの CPU 使用率が 75% を超えると、SNMP トラップが生成されます。
		viptelaSystemDiskUsage	システムのディスク使用率が 75% を超えると、SNMP トラップが生成されます。
		viptelaSystemMemoryUsage	システムのメモリ使用率が 75% を超えると、SNMP トラップが生成されます。
		viptelaSystemProcessRestart	コントローラまたはルータのプロセス（デーモン）が再起動すると、SNMP トラップが生成されます。
		viptelaSystemProcessDown	デバイス上のプロセス（デーモン）が終了すると、SNMP トラップが生成されます。
		viptelaSystemSystemAaaLoginFail	AAA ユーザーによる SSH ベースのログインが失敗すると、SNMP トラップが生成されます。
		viptelaSystemPseudoCommitStatus	

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
			Cisco SD-WAN Manager が仮設定（疑似コミットと呼ばれる）をデバイスにプッシュし、ロールバックタイマーを開始すると、SNMP トラップが生成されます。
		viptelaActionsSystemRebootComplete	デバイスのリブート手順が完了すると、SNMP トラップが生成されます。
		viptelaActionsSystemRebootAborted	デバイスのリブートが中止されると、SNMP トラップが生成されます。
	マイナー	viptelaSystemCpuUsage	システムの CPU 使用率が次の場合に、SNMP トラップが生成されます。 • 60 ～ 75% になる。 • 60% を下回る。
		viptelaSystemDiskUsage	システムのディスク使用率が次の場合に、SNMP トラップが生成されます。 • 60 ～ 75% になる。 • 60% を下回る。
		viptelaSystemDomainIdChange	オーバーレイネットワークのドメイン識別子が変更されると、SNMP トラップが生成されます。
		viptelaSystemMemoryUsage	システムのメモリ使用率が次の場合に、SNMP トラップが生成されます。 • 60 ～ 75% になる。 • 60% を下回る。
		viptelaSystemOrgNameChange	

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
			すべてのオーバーレイ ネットワークデバイスの証明書で使用されている組織名が変更されると、SNMP トラップが生成されます。
		viptelaActionsSystemRebootIssued	デバイスがリブートされると、SNMP トラップが生成されます。
		viptelaSystemSiteIdChange	オーバーレイネットワークのサイト識別子が変更されると、SNMP トラップが生成されます。
		viptelaActionsSystemSoftwareInstallStatus	システムソフトウェアのインストールステータスを通知するために、SNMP トラップが生成されます。
		viptelaSystemSystemCommit	ユーザー設定がコミットされると、SNMP トラップが生成されます。
		viptelaSystemSystemIpChange	ルータまたはコントローラでシステムの IP アドレスが変更されると、SNMP トラップが生成されます。
		viptelaSystemSystemLoginChange	ユーザーのシステムログインが変更されると、SNMP トラップが生成されます。
		viptelaSystemSystemLogoutChange	ユーザーがシステムからログアウトすると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
vpn	メジャー	viptelaVpnInterfaceStateChange	インターフェイスの管理ステータスまたは操作ステータスが変更されると、SNMP トラップが生成されます。
		viptelaVpnVrrpGroupStateChange	VRRP グループの状態が変更されると、SNMP トラップが生成されます。
		viptelaVpnCloudExpressApplicationChange	Cloud Express アプリケーションのベストパスが変更されると、SNMP トラップが生成されます。
		viptelaVpnCloudExpressMaxLocalExitExceeded	Cloud Express の最大ローカル出口（上限は 56）を超えると、SNMP トラップが生成されます。
		viptelaVpnCloudExpressScoreChange	Cloud Express アプリケーションのベストパススコアが変更されたが、ベストパスに変更がない場合に、SNMP トラップが生成されます（スコアは遅延または損失から計算されます）。
		viptelaVpnInterfaceBw	インターフェイスのダウンストリーム帯域幅が更新されると、SNMP トラップが生成されます。
		viptelaVpnInterfacePcsFaultDetected	インターフェイス PCS の障害が検出またはクリアされると、SNMP トラップが生成されます。
		viptelaVpnLastResortStateChange	ラストリゾートの状態が変更されると、SNMP トラップが生成されます。
	マイナー	viptelaVpnRouteInstallFail	ルートのインストールが失敗すると、SNMP トラップが生成されます。

トラップタイプ	重大度：クリティカル/メジャー/マイナー	トラップ名	説明
		viptelaVpnTunnelInstallFail	TLOC へのトンネルの追加が失敗すると、SNMP トラップが生成されます。
		viptelaVpnFibStateChange	FIB が更新されると、SNMP トラップが生成されます。
wwan	メジャー	viptelaWwanBearerChange	データベアラーが変更されると、SNMP トラップが生成されます。
		viptelaWwanDomainStateChange	ドメインの状態が変更されると、SNMP トラップが生成されます。
		viptelaWwanRegStateChange	ネットワーク登録が変更されると、SNMP トラップが生成されます。
		viptelaWwanSimStateChange	SIM の状態が変更されると、SNMP トラップが生成されます。
		viptelaWwanQosStateChange	QoS フローの状態が変更されると、SNMP トラップが生成されます。

Cisco vEdge デバイスの通知メッセージ

表 *27 : Cisco vEdge* デバイスの通知

通知	対応する SNMP トラップ
aaa-admin-pwd-change	viptelaSystemAaaAdminPwdChange
access-list-association-status	viptelaPolicyAccessListAssociationStatus
app-list-app-aliases-notify	viptelaPolicyAppListAppAliasesNotify
app-list-unsupported-app-notify	viptelaPolicyAppListUnsupportedAppNotify
bearer-change	viptelaWwanBearerChange
bfd-state-change	viptelaBfdBfdStateChange

通知	対応する SNMP トラップ
bgp-peer-state-change	viptelaVpnBgpPeerStateChange
bridge-creation	viptelaBridgeCreation
bridge-deletion	viptelaBridgeDeletion
bridge-max-mac-reached	viptelaBridgeMaxMacReached
cloudexpress-application-change	viptelaVpnCloudExpressApplicationChange
cloudexpress-max-local-exit-exceeded	viptelaVpnCloudExpressMaxLocalExitExceeded
cloudexpress-score-change	viptelaVpnCloudExpressScoreChange
control-connection-auth-fail	viptelaSecurityControlConnectionAuthFail
control-connection-state-change	viptelaSecurityControlConnectionStateChange
control-connection-tloc-ip-change	viptelaSecurityControlConnectionTlocIpChange
control-no-active-vbond	viptelaSecurityControlNoActiveVbond
control-no-active-vsmart	viptelaSecurityControlNoActiveVsmart
control-vbond-state-change	viptelaSecurityControlVbondStateChange
control-vedge-list-request	viptelaSecurityControlVedgeListRequest
cpu-usage	viptelaSystemCpuUsage
data-policy-association-status	viptelaPolicyDataPolicyAssociationStatus
device-template-attached-during-ztp	viptelaSecurityDeviceTemplateAttachedDuringZtp
device-template-missing	viptelaSecurityDeviceTemplateMissing
dhcp-address-assigned	viptelaVpnDhcpAddressAssigned
dhcp-address-released	viptelaVpnDhcpAddressReleased
dhcp-address-renewed	viptelaVpnDhcpAddressRenewed
dhcp-request-rejected	viptelaVpnDhcpRequestRejected
dhcp-server-state-change	viptelaVpnDhcpServerStateChange
disk-usage	viptelaSystemDiskUsage
domain-id-change	viptelaSystemDomainIdChange
domain-state-change	viptelaWwanDomainStateChange
emmc-fault	viptelaHardwareEmmcFault
fan-fault	viptelaHardwareFanFault

通知	対応する SNMP トラップ
fantray-fault	viptelaHardwareFantrayFault
fib-update	viptelaVpnFibStateChange
flash-fault	viptelaHardwareFlashFault
interface-admin-state-change	viptelaVpnInterfaceAdminStateChange
interface-bw	viptelaVpnInterfaceBw
interface-pcs-fault-detected	viptelaVpnInterfacePcsFaultDetected
interface-state-change	viptelaVpnInterfaceStateChange
last-resort-state-change	viptelaVpnLastResortStateChange
memory-usage	viptelaSystemMemoryUsage
omp-number-of-vsmarts-change	viptelaOmpOmpNumberOfVsmartsChange
omp-peer-state-change	viptelaOmpOmpPeerStateChange
omp-policy	viptelaOmpOmpPolicy
omp-state-change	viptelaOmpOmpStateChange
org-name-change	viptelaSystemOrgNameChange
ospf-interface-state-change	viptelaVpnOspfInterfaceStateChange
ospf-neighbor-state-change	viptelaVpnOspfNeighborStateChange
pem-fault	viptelaHardwarePemFault
pem-state-change	viptelaHardwarePemStateChange
pim-fault	viptelaHardwarePimFault
pim-interface-state-change	viptelaVpnPimInterfaceStateChange
pim-neighbor-state-change	viptelaVpnPimNeighborStateChange
pim-state-change	viptelaHardwarePimStateChange
pim-tunnel-state-change	viptelaVpnPimTunnelStateChange
process-down	viptelaSystemProcessDown
process-restart	viptelaSystemProcessRestart
pseudo-commit-status	viptelaSystemPseudoCommitStatus
qos-state-change	viptelaWwanQosStateChange
reg-state-change	viptelaWwanRegStateChange

通知	対応する SNMP トラップ
route-install-fail	viptelaVpnRouteInstallFail
sd-card-fault	viptelaHardwareSdcardFault
security-certificate-expired	viptelaSecuritySecurityCertificateExpired
security-certificate-expiring	viptelaSecuritySecurityCertificateExpiring
security-certificate-installed	viptelaSecuritySecurityCertificateInstalled
security-clear-installed-certificate	viptelaSecuritySecurityClearInstalledCertificate
security-new-csr-generated	viptelaSecuritySecurityNewCsrGenerated
security-root-cert-chain-installed	viptelaSecuritySecurityRootCertChainInstalled
security-root-cert-chain-uninstalled	viptelaSecuritySecurityRootCertChainUninstalled
security-unclaimed-vedge-entry-added	viptelaSecuritySecurityUnclaimedVedgeEntryAdded
security-vedge-entry-added	viptelaSecuritySecurityVedgeEntryAdded
security-vedge-entry-removed	viptelaSecuritySecurityVedgeEntryRemoved
security-vedge-serial-file-uploaded	viptelaSecuritySecurityVedgeSerialFileUploaded
security-vsmart-serial-file-uploaded	viptelaSecuritySecurityVsmartSerialFileUploaded
service-gre-state-update	viptelaSecurityGreStateUpdate
sfp-state-change	viptelaHardwareSfpStateChange
sfp-support-state	viptelaHardwareSfpSupportState
sim-state-change	viptelaWwanSimStateChange
site-id-change	viptelaSystemSiteIdChange
sla-change	viptelaAppRouteSlaChange
sla-config	viptelaPolicySlaConfig
sla-violation	viptelaPolicySlaViolation
sla-violation-pkt-drop	viptelaPolicySlaViolationPktDrop
system-aaa-login-fail	viptelaSystemSystemAaaLoginFail
system-commit	viptelaSystemSystemCommit
system-ip-change	viptelaSystemSystemIpChange
system-login-change	viptelaSystemSystemLoginChange
system-logout-change	viptelaSystemSystemLogoutChange

通知	対応する SNMP トラップ
system-reboot-aborted	viptelaActionsSystemRebootAborted
system-reboot-complete	viptelaActionsSystemRebootComplete
system-reboot-issued	viptelaActionsSystemRebootIssued
system-software-install-status	viptelaActionsSystemSoftwareInstallStatus
tempsensor-fault	viptelaHardwareTempsensorFault
tempsensor-state	viptelaHardwareTempsensorState
tunnel-install-fail	viptelaVpnTunnelInstallFail
tunnel-ipsec-manual-rekey	viptelaSecurityTunnelIpsecManualRekey
tunnel-ipsec-rekey	viptelaSecurityTunnelIpsecRekey
usb-state-change	viptelaHardwareUsbStateChange
vbond-reject-vedge-connection	viptelaSecurityVbondRejectVedgeConnection
vmanage-connection-preference-changed	viptelaSecurityVmanageConnectionPreferenceChanged
vrrp-group-state-change	viptelaVpnVrrpGroupStateChange
zbfw-clear-flow-table-full	viptelaPolicyZbfClearFlowTableFull
zbfw-clear-half-open-hit	viptelaPolicyZbfClearHalfOpenHit
zbfw-flow-creation	viptelaPolicyZbfFlowCreation
zbfw-flow-deletion	viptelaPolicyZbfFlowDeletion
zbfw-flow-table-full	viptelaPolicyZbfFlowTableFull
zbfw-half-open-limit-hit	viptelaPolicyZbfHalfOpenHit
zbfw-pkt-log	viptelaPolicyZbfPktLog

サポートされる SNMP MIB

表 *28 :* 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN MIB	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	次の Cisco Catalyst SD-WAN MIB が Cisco IOS XE Catalyst SD-WAN デバイスに導入されています。 CISCO-SDWAN-APP-ROUTE-MIB.my CISCO-SDWAN-BFD-MIB.my CISCO-SDWAN-OMP-MIB.my CISCO-SDWAN-OPER-SYSTEM-MIB.my CISCO-SDWAN-POLICY-MIB.my CISCO-SDWAN-SECURITY-MIB.my
Cisco Catalyst SD-WAN MIB	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	次の Cisco Catalyst SD-WAN MIB が Cisco IOS XE Catalyst SD-WAN デバイスに導入されています。 CISCO-SDWAN-PROBE-MIB.my CISCO-SDWAN-OMP-MIB.my（テーブル追加済み） CISCO-SDWAN-SECURITY-MIB.my（テーブル追加済み）

Cisco IOS XE Catalyst SD-WAN デバイスについて

Cisco IOS XE Catalyst SD-WAN デバイスでサポートされている MIB は、https://github.com/cisco/cisco-mibs からダウンロードできます。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a 以降、CISCO-SDWAN-OMP-MIB.my では OMP MIB テーブルとスカラーオブジェクトがサポートされています。

Cisco IOS XE リリース 17.6.1a では、ciscoSdwanOmpOmpNumberOfVsmartsChange、ciscoSdwanOmpOmpStateChange、ciscoSdwanOmpOmpPeerStateChange、および ciscoSdwanOmpOmpPolicy OMP トラップのみがサポートされ、OMP MIB テーブルとスカラーオブジェクトは CISCO-SDWAN-OMP-MIB.my でサポートされません。

（注） CISCO-SDWAN-POLICY-MIB.my MIB の場合、RFC 2578 で定義されているように、オブジェクト識別子（OID）値が 128 のサブ識別子を超えることはできません。OID の制限が 128 のサブ識別子を超える場合は、モニタリングとトラブルシューティング用の代替 API として、**リアルタイムモニタリング - ポリシー** Netconf または REST API を Cisco IOS XE Catalyst SD-WAN デバイスで使用することが推奨されます。

（注） Cisco IOS XE リリース 17.6.3 以降、CISCO-SDWAN-APP-ROUTE-MIB には、SNMP からの平均ジッター、遅延、およびパケットドロップのデータ要求をサポートする appRouteStatisticsAppProbeClassTable および appRouteStatisticsAppProbeClassIntervalTable OID が含まれています。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.2a 以降、SNMP MIB テーブルに多数のテーブルエントリが含まれている場合は、**snmp-server subagent fetch count***100* コマンドを使用することが推奨されます。デフォルトでは、カウント値は 50 です。

Cisco vEdge デバイスについて

サポートされている Cisco vEdge MIB については、https://github.com/cisco/cisco-mibs/tree/main/viptela-mibs を参照してください。

これらの MIB ファイルのダウンロードについては、ご使用のソフトウェアリリースに対応するリリースノートを参照してください。

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。