ハードウェアとソフトウェアの設置

（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。

表 *1*：機能の履歴

機能名	リリース情報	説明
CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイス のブートストラップファイルの生成	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a	この機能により、最小限のブートストラップ設定ファイルをデバイス上で直接生成できます。このファイルを使用すると、完全な設定が失われたり削除されたりした場合に、デバイスがコントローラに再接続することができます。

サーバー推奨事項

このトピックは、Cisco SD-WAN Validator サーバー、vEdge Cloud ルータサーバー、Cisco SD-WAN Manager サーバー、および Cisco SD-WAN コントローラ サーバーのハードウェア推奨事項（『Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources』）に結び付いています。

vEdge Cloud ルータサーバーの推奨事項

vEdge Cloud のデータシートを参照してください。

モジュールの追加または削除後の Cisco IOS XE Catalyst SD-WAN デバイス のデバイス設定のリセット

前提条件

ルータモジュールのハードウェアの設置に関する基礎知識が必要です。モジュールをプラットフォームに挿入する方法、またはプラットフォームから削除する方法については、それぞれのプラットフォームまたはモジュールのドキュメントを参照してください。

OIR サポート

（注） OIR は Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

活性挿抜（OIR）を行うと、システム運用に影響を与えずにシスコデバイスの部品を交換できます。モジュールが挿入されると、モジュールが通電し、モジュール自身が初期化され、動作を開始します。

ホットスワップ機能により、システムは、装置の物理構成に発生した変更の状況を判断し、すべてのインターフェイスが適切に機能するように装置のリソースを再度割り当てることができます。この機能を使用すると、モジュールのインターフェイスを再構成しても、ルータの他のインターフェイスを変更せずに済みます。

ソフトウェアは、モジュールの取り外しと挿入の処理に必要なタスクを実行します。ハードウェア割り込みは、ハードウェアの変更が検出されるとソフトウェアサブシステムに送られ、ソフトウェアがシステムを次のように再構成します。

- モジュールが挿入されると、エンドユーザーが適切に構成できるように分析および初期化されます。OIR 中に使用される初期化ルーチンは、ルータの電源投入時のルーチンと同じです。ソフトウェアによっても処理されるシステム リソースは、新しいインターフェイスに割り当てられます。
- モジュールを取り外すと、空きスロットに関連付けられたリソースは、解放されるか、ステータスの変更を示すために変更される必要があります。

デバイス設定のリセット

モジュールを Cisco IOS XE Catalyst SD-WAN デバイス に挿入または取り外した場合は、CLI を使用してデバイス設定のリセットを実行して、Cisco IOS XE Catalyst SD-WAN デバイス と物理的な変更との同期を保つ必要があります。コントローラモード構成のリセットの詳細については、「Controller Mode Configuration Reset」を参照してください。

Cisco Catalyst SD-WAN デバイスのオンサイト ブートストラップ プロセス

オンサイト ブートストラップ プロセスには、ブート可能な USB ドライブまたは内部ブートフラッシュから Cisco Catalyst SD-WAN をサポートするデバイスにロードするブートストラップ構成ファイルの生成が含まれます。デバイスは起動すると、構成ファイルの情報を使用してネットワークに接続します。

オンサイト ブートストラップ プロセスは、次の一般的なワークフローで構成されます。

- Cisco SD-WAN Manager を使用して構成ファイルを生成する
- 構成ファイルをブート可能な USB ドライブにコピーしてドライブをデバイスに接続するか、構成をデバイスのブートフラッシュにコピーします。
- デバイスを起動します。

挿入された USB ドライブとブートフラッシュの両方に構成ファイルがある場合、ブートフラッシュの構成ファイルが優先されます。

デバイスの要件

オンサイト ブートストラップ プロセスを使用して構成するデバイスは、次の要件を満たしている必要があります。

- サポートされている Cisco Catalyst SD-WAN イメージがデバイスにインストールされている
- デバイスは、構成が追加されていない工場出荷時のデフォルト状態である

オンサイト ブートストラップ プロセスの実行

デバイスのオンサイト ブートストラップ プロセスを実行するには、次の手順に従います。

1. デバイスのシャーシ ID とのシリアル番号を Cisco SD-WAN Manager にアップロードします。

   手順については、「vEdgeシリアル番号ファイルのアップロード」を参照してください。

2. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Settings]**の順に選択し、組織名と Cisco Catalyst SD-WAN Validator の IP アドレスが正しく設定されていることを確認します。

3. ネットワーク内のデバイス認証に独自のエンタープライズルート認証局（CA）を使用している場合は、Cisco SD-WAN Manager で次の操作を実行します。

   1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
   2. [WAN Edge Cloud Certificate Authorization] をクリックします。

      （Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前を使用している場合は、[Edit] をクリックします。）
   3. [Manual] をクリックします。
   4. [Save] をクリックします。

4. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
5. [Feature Templates] をクリックして、デバイスのテンプレートを作成します。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

6. 次の操作を行ってください。

   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]**の順に選択します。
   2. 目的のデバイスで [...] をクリックし、[Generate Bootstrap Configuration] を選択します。

3. ダイアログボックスで、[Cloud-init] を選択し、[OK] をクリックします。

   Multipurpose Internet Mail Extensions（MIME）ファイルが生成され、内容がポップアップウィンドウに表示されます。このファイルには、デバイスのシステムプロパティ、ルート CA（エンタープライズルート CA を使用している場合）、および作成したテンプレートの構成設定が含まれています。

7. [MIME file] ポップアップウィンドウで、[Download] をクリックします。

   ファイルがローカルシステムにダウンロードされ、ダウンロード用のディレクトリに保存されます。ファイル名は chassis.cfg で、chassis はステップ 1 でアップロードしたデバイスのシャーシ ID です。

（注） この手順の代わりに、MIME ファイルの内容をポップアップウィンドウからテキストファイルにコピーし、`ciscosdwan.cfg`（大文字と小文字を区別）という名前で保存してから、ステップ 8 にスキップできます。

（注） ハードウェアデバイスの場合は、ブートストラップファイル名を `ciscosdwan.cfg` として使用します。このファイルは Cisco SD-WAN Manager によって生成され、UUID が含まれていますが、OTP は含まれていません。ソフトウェアデバイス（CSR および ISRv）、および ASR1002-X などの OTP 認証デバイスの場合、ブートストラップファイル名を `ciscosdwan_cloud_init.cfg` として使用します。このファイルには OTP が含まれていますが、`ciscosdwan_cloud_init.cfg` の UUID 検証は含まれていません。

8. MIME ファイルをダウンロードした場合は、名前を `ciscosdwan.cfg`（大文字と小文字を区別）に変更します。

（注） これは、オンサイト ブートストラップ プロセスの構成ファイルです。

9. `ciscosdwan.cfg` ファイルをブート可能な USB ドライブまたはデバイスのブートフラッシュにコピーします。

（注） ファイルには、表示されているとおりに名前を付ける必要があります。そうしないと、デバイスがファイルを読み取れません。

10. USB ドライブを使用している場合は、USB ドライブをデバイスに接続します。

11. デバイスを起動します。

デバイスは、USB ドライブまたはブートフラッシュから構成ファイルを読み取り、構成情報を使用してネットワークに接続します。デバイスでは、ブートフラッシュにある構成ファイルが優先されます。

SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラップ プロセス

表 *2:* 機能の履歴

機能名	リリース情報	説明
SHA2 エンタープライズ証明書を使用した Cisco vEdge 5000 のオンサイト ブートストラップ プロセス	Cisco SD-WAN リリース 20.3.1 Cisco vManage リリース 20.3.1	デフォルトでは、Cisco vEdge 5000 デバイスは、オーバーレイネットワーク内のコントローラによる認証に SHA1 証明書を使用します。この機能を使用すると、OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をデバイスにインストールすることができます。OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をインストールすることにより、SHA1 証明書認証をバイパスし、SHA1 の脆弱性からデバイスを保護することができます。

Cisco vEdge 5000 デバイスは、トラステッド プラットフォームモジュール（TPM 1.2）を装備しており、オーバーレイネットワークへの接続時に認証に SHA1 証明書を使用します。SHA1 証明書を使用したブートストラッププロセスについては、「*Cisco Catalyst SD-WAN* デバイスのオンサイト ブートストラップ プロセス」を参照してください。

Cisco Catalyst SD-WAN リリース 20.3.1 以降では、Cisco vEdge 5000 デバイスのブートストラップおよびそのデバイスのオーバーレイネットワークへの接続時に、ワンタイムパスワード（OTP）と公開キーを使用してデバイスを認証し、そのデバイスに SHA2 エンタープライズ証明書をインストールすることができます。OTP と公開キーを使用してデバイスを認証し、SHA2 エンタープライズ証明書をインストールすることにより、SHA1 証明書認証をバイパスし、SHA1 の脆弱性からデバイスを保護することができます。

OTP と公開キーを使用して Cisco vEdge 5000 を認証する方法

1. **Plug and Play Connect** でデバイスの公開キーを入力し、`serial.viptela` ファイルを生成します。
2. `serial.viptela` ファイルを Cisco SD-WAN Manager にアップロードします。
3. Cisco SD-WAN Manager が、デバイスのランダム認証トークンを生成します。Cisco SD-WAN Manager が、デバイスの公開キーを使用して認証トークンを暗号化し、それを OTP として `<chassis>.config` ファイルに入力します。
4. `<chassis>.config` ファイルをブート可能 USB ドライブにダウンロードし、工場出荷時設定へのリセットを実行した後に、USB ドライブをデバイスに挿入します。
5. デバイスが、`<chassis>.config` ファイルを読み取り、暗号化されたダイジェストを [OTP] フィールドから読み取って、デバイスの秘密キーを使用してダイジェストを復号し、認証トークンを取得します。
6. デバイスが、AVNET/TPM1.2 SHA1 証明書認証を無効にします。
7. デバイスが、認証トークンを使用して Cisco SD-WAN Manager でそれ自体を認証し、制御接続を確立します。
8. Cisco SD-WAN Manager が、初期構成をデバイスにプッシュします。
9. Cisco SD-WAN Manager が、デバイスの SHA2 エンタープライズ証明書をプッシュし、証明書をデバイスにインストールします。
10. デバイスが、SHA2 エンタープライズ証明書を使用してそれ自体をコントローラに対して再認証し、コントローラに接続します。

考慮すべき点

- Cisco vEdge 5000 デバイスが OTP を使用して Cisco SD-WAN Validator または Cisco SD-WAN Manager で認証された後、SHA2 エンタープライズ証明書がインストールされて検証されるまで、デバイスを再起動しないでください。エンタープライズ証明書が検証される前にデバイスが再起動した場合は、ブートストラップ手順を再び開始します。
- 署名付き SHA2 エンタープライズ証明書が Cisco vEdge 5000 デバイスにインストールされ、ブートストラッププロセスが完了した後に、ソフトウェアリセット、構成リセット、または工場出荷時リセットを実行する場合は、デバイスのブートストラップを再実行します。
- Cloud-Init（暗号化 OTP）ブートストラップ構成を生成するたびに、新しい構成ファイルをブート可能 USB ドライブにダウンロードする必要があります。

前提条件

1. エンタープライズ証明書認証が設定されていることを確認します。

1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
2. [Hardware WAN Edge Certificate Authorization] をクリックします。

   （Cisco Catalyst SD-WAN Manager リリース 20.12.x 以前を使用している場合は、[Edit] をクリックします。）
3. [Enterprise Certificate (signed by Enterprise CA)] がオンになっていることを確認し、[Save] をクリックします。

2. `serial.viptela` ファイルを生成する前に、デバイスの公開キーエントリが PNP サーバーで使用できることを確認します。詳細については、「Cisco vEdge 5000 デバイスの公開キーの表示または追加」を参照してください。
3. Cisco vEdge 5000 デバイスが SHA1 証明書を使用してオーバーレイネットワークに接続されている場合は、認証に OTP、公開キー、および SHA2 エンタープライズ証明書を使用するように設定する前に、デバイスを無効にしてオーバーレイネットワークから削除する必要があります。

Cisco vEdge 5000 デバイスの公開キーの表示または追加

1. Cisco Software Central で、Cisco vEdge 5000 デバイスへのアクセスに必要なスマートアカウントおよびバーチャルアカウントを使用して **Plug and Play Connect** にログインします。
2. [Devices] リストで、Cisco vEdge 5000 デバイスのシリアル番号をクリックします。

   [Device Information] が表示されます。
3. [Device Information] ダイアログボックスで、デバイスの**公開キー**が使用可能かどうかを確認します。
4. **公開キー**を使用できない場合は、**公開キー**を追加します。
   1. [Devices] リストで、チェックボックスを使用して Cisco vEdge 5000 デバイスを選択します。
   2. [Edit] をクリックします。

      [Edit Devices] ページが表示されます。
   3. [Selected Devices] エリアで、[Public Key] 列の [view/edit] をクリックします。

      [Public Key] ダイアログボックスが表示されます。
   4. テキストボックスに公開キーを入力するか、[Browse] をクリックして公開キーを含むファイルをアップロードします。
   5. [OK] をクリックして公開キーを保存し、ダイアログボックスを閉じます。
   6. [Edit Devices] ページで、[Submit] をクリックして公開キーを Cisco vEdge 5000 デバイスにアタッチします。

ブートストラップ手順

オンサイト ブートストラップ プロセスには、ブート可能 USB ドライブからロードするブートストラップ構成ファイルの生成が含まれます。Cisco vEdge 5000 デバイスは、起動時に、構成ファイルの情報を使用してオーバーレイネットワークに接続します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]** > **[WAN Edge List]** の順に選択します。
2. [Upload WAN Edge List] をクリックします。
3. [Upload WAN Edge List] ダイアログボックスで、アップロードする Cisco vEdge 5000 シリアル番号ファイルを選択します。[Validate the uploaded vEdge list and send to controllers] を選択し、[Upload] をクリックします。

   WAN Edge リストがコントローラにアップロードされます。

   Cisco vEdge 5000 デバイスが **WAN Edge リスト**に追加されます。
4. デバイスをデバイス構成テンプレートにアタッチします。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
   2. [Device Templates] をクリックし、テンプレートを選択します。
   3. 目的のテンプレートについて、[...] をクリックし、[Attach Devices] を選択します。[Attach Devices] ダイアログボックスが開きます。
   4. [Available Devices] 列で、グループを選択し、検索して Cisco vEdge 5000 デバイスを選択します。
   5. 右向きの矢印をクリックして、デバイスを [Selected Devices] 列に移動します。
   6. [Attach] をクリックします。

      構成テンプレートはデバイス用にスケジュールされています。
5. 新しく追加されたデバイスのブートストラップ構成を生成します。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]** の順に選択します。
   2. [WAN Edge List] をクリックし、Cisco vEdge 5000 デバイスを選択します。
   3. 選択したデバイスについて、[...] をクリックし、[Generate Bootstrap Configuration] を選択します。
   4. [Generate Bootstrap Configuration] ダイアログボックスで、[Cloud-Init(Encrypted OTP)] を選択し、[OK] をクリックします。
   5. [Download] をクリックしてブートストラップ構成をダウンロードし、`<ChassisNumber>.cfg` 形式のファイル名を付けてファイルを保存します。
   6. `<ChassisNumber>.cfg` ファイルをブート可能 USB ドライブにコピーします。

（注）
- Cisco vEdge 5000 デバイスがドライブを認識して自動マウントするには、USB ドライブが FAT-32 フォーマットである必要があります。
- <ChassisNumber>.cfg ファイルを USB ドライブのホームディレクトリまたは親ディレクトリにコピーします。

6. Cisco vEdge 5000 シリアル番号ファイルおよび OTP 情報をコントローラに送信します。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** > **[WAN Edge List]** の順に選択します。
   2. [Send to Controllers] をクリックして、すべてのコントローラの WAN Edge リストを同期させます。

      デバイスシリアル番号ファイルおよび OTP 情報がコントローラに送信されます。
   3. （任意）**show orchestrator valid-vedges hardware-installed-serial-number prestaging** コマンドを使用して、コントローラの WAN Edge リストを確認します。

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number prestaging


     HARDWARE

      INSTALLED   SUBJECT

      SERIAL      SERIAL
CHASSIS NUMBER  SERIAL NUMBER                    VALIDITY  ORG
      NUMBER      NUMBER
--------------------------------------------------------------------------------
193A0122170001  deaedf5d39919454fdfcc8470eccd8d8  valid     vIPtela Inc
Regression  prestaging  N/A
```

7. Cisco SD-WAN リリース 20.3.1 以降のデフォルトイメージを使用して、Cisco vEdge 5000 デバイスの工場出荷時設定へのリセットを実行します。
8. Cisco vEdge 5000 デバイスが「稼働中」（LCD ディスプレイにステータスが「System: Up」と表示されます）のときに、<ChassisNumber>.cfg ファイルが保存された USB ドライブを挿入します。

   デバイスは、USB ドライブから <ChassisNumber>.cfg ファイルを読み取ります。組織名、Cisco SD-WAN Validator の IP アドレス、OTP トークン、およびエンタープライズルート CA は、構成ファイルから取得されます。
   1. （任意）デバイスで **show control local-properties** コマンドを発行して、構成ファイルから取得された情報を検証します。
   2. （任意）デバイスの WAN インターフェイスに DHCP を介して IP アドレスが割り当てられていない場合、静的 IP アドレスと、コントローラに到達するために必要なルーティング情報を設定します。

デバイスは、OTP を使用した認証後に Cisco SD-WAN Validator および Cisco SD-WAN Manager に接続します。

デバイスは、Cisco SD-WAN Manager 構成テンプレートからシステム IP アドレスとサイト ID を取得します。Cisco SD-WAN Manager でテンプレートが設定されていない場合は、デバイスで必要なシステム構成を設定します。

デバイスが Cisco SD-WAN Manager に接続した後に、Cisco SD-WAN Manager はエンタープライズ証明書署名要求（CSR）を取得します。Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** > **[WAN Edge List]** の順に選択すると、デバイス証明書の状態が「**CSR**」と表示されます。

9. CSR をダウンロードします。

1. Cisco SD-WAN Manager メニューから **[Configuration]** > **[Certificates]** の順に選択します。
2. 証明書に署名する Cisco vEdge 5000 デバイスを選択します。
3. 選択したデバイスについて、[...] をクリックし、[View Enterprise CSR] を選択します。
4. CSR をダウンロードするには、[Download] をクリックします。

10. 証明書をサードパーティの署名機関に送信して、署名してもらいます。

11. 証明書をデバイスにインストールするには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** > **[Controllers]** の順に選択します。

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

2. 画面の右上隅にある [Install Certificate] ボタンをクリックします。
3. [Install Certificate] 画面で、証明書を [Certificate Text] フィールドに貼り付けるか、[Select a File] をクリックしてファイルの証明書をアップロードします。
4. [Install] をクリックします。

インストールされているデバイスの証明書シリアル番号がコントローラで更新されます。

Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Certificates]** > **[WAN Edge List]** の順に選択すると、デバイス証明書の状態が「installed」と表示されます。

12. （任意）コントローラの WAN Edge リストを調べて、デバイスのシリアル番号がインストールされていることを確認します。

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number 12399910
```

```
                                                                    HARDWARE
                                                                    INSTALLED  SUBJECT
                  SERIAL                                            SERIAL     SERIAL
CHASSIS NUMBER    NUMBER    VALIDITY  ORG                           NUMBER     NUMBER
-------------------------------------------------------------------------------------
193A0122170001    18DB5D4F  valid     vIPtela Inc Regression        12399910   N/A
```

13. USB ドライブをデバイスから取り外します。

結果

- Cisco vEdge 5000 デバイスが、SHA2 エンタープライズ証明書を使用してオーバーレイネットワークに追加され、コントローラに接続されます。
- デバイスは、再起動、ソフトウェアアップグレード、または Cisco SD-WAN リリース 20.3.1 以降のリリースへのソフトウェアダウングレードの後に、インストールされた SHA2 エンタープライズ証明書を使用します。SHA1 証明書の使用は無効になります。

CLI を使用した Cisco IOS XE Catalyst SD-WAN デバイス のブートストラップファイルの生成

Cisco Catalyst SD-WAN コントローラとの接続を確立するには、デバイスに最小限の設定が必要です。ほとんどの場合、この最小限のブートストラップ設定（MBC）は、最初はプラグアンドプレイ（PnP）によって提供できます。ただし、リモートサイトで PnP を使用しないほうがよい場合など、状況によっては、デバイスをコントローラに接続できる保存済みのブートストラップ設定があると便利です。

request platform software sdwan bootstrap-config save コマンドを実行すると、デバイス設定がブートフラッシュに保存されます。このコマンドは設定を保存するためにいつでも使用できますが、その目的は、設定全体が失われたり削除されたりした場合に、デバイスがコントローラに再接続できるようにする最小限のブートストラップ設定（MBC）ファイルを保存することです。

デバイスをセットアップするときに、コントローラに接続するために必要な詳細を設定に追加し、このコマンドを使用して MBC を保存します。ファイルは次の場所に保存されます。

bootflash:/ciscosdwan.cfg

前提条件

- デバイスを認証するために、コントローラ ルート証明書が Cisco IOS XE Catalyst SD-WAN デバイス にインストールされていること。
- デバイスがそのインターフェイスの 1 つを介して WAN に物理的に接続されていること。

手順

1. Cisco IOS XE Catalyst SD-WAN デバイス で、次のように設定して、Cisco SD-WAN Manager への接続を確立します。
   - システム IP アドレス
   - ドメイン ID
   - サイト ID
   - sp-organization-name
   - organization-name
   - Cisco SD-WAN Validator の IP アドレスおよびポート番号
   - GRE または IPSEC として設定されたカプセル化を使用したトンネル

   例：

   ```
   system
   system-ip 10.0.0.10
   domain-id 1
   site-id 200
   admin-tech-on-failure
   sp-organization-name CiscoISR
   organization-name CiscoISR
   vbond 10.0.100.1 port 12346
   !
   interface Tunnel1
   no shutdown
   ip unnumbered GigabitEthernet0/1/0
   tunnel source GigabitEthernet0/1/0
   tunnel mode sdwan
   exit
   sdwan
   interface GigabitEthernet0/1/0
   tunnel-interface
   encapsulation ipsec
   exit
   exit
   commit
   ```

2. **show sdwan control connections** を使用して Cisco SD-WAN Manager、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator への接続を確認します。

3. **request platform software sdwan bootstrap-config save** コマンドを使用して、ブートストラップファイルをデバイスのブートフラッシュに保存します。

   例：

   ```
   Device#request platform software sdwan bootstrap-config save
   Saving bootstrap file 'bootflash:/ciscosdwan.cfg'...
   Done
   ```

   設定ファイルは次の場所に保存されます。

   bootflash:/ciscosdwan.cfg

ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイス のオンボード

表 *3:* 機能の履歴

機能名	リリース情報	説明
ワンタッチプロビジョニング：汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイス のオンボード	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco SD-WAN Manager で汎用ブートストラップ構成を生成し、この構成を使用して複数の Cisco IOS XE Catalyst SD-WAN デバイス をオンボードできます。汎用ブートストラップ構成でデバイスを起動すると、デバイスは要求されていない WAN エッジデバイスとして Cisco SD-WAN Manager にリストされます。オンボーディングを完了するには、Cisco SD-WAN Manager でデバイスを要求し、システムの IP アドレスとサイト ID を設定するデバイステンプレートを添付します。

汎用ブートストラップ構成の概要

Cisco IOS XE Catalyst SD-WAN デバイス を Cisco Catalyst SD-WAN オーバーレイネットワークにオンボードするには、Cisco SD-WAN Manager でブートストラップ構成を生成し、この構成でデバイスを起動します。デバイスが Cisco SD-WAN Manager に接続されたら、Cisco SD-WAN Manager GUI を使用してオンボーディングを完了します。ブートストラップ構成にはデバイス固有の構成設定が含まれているため、オンボードする必要があるデバイスごとにブートストラップ構成を生成する必要があります。Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降、汎用ブートストラップ構成を使用して、複数の Cisco IOS XE Catalyst SD-WAN デバイス をオンボードできます。

汎用ブートストラップ構成では、デバイス固有の詳細（デバイスの UUID など）が省略され、Cisco SD-WAN Validator に接続するために Cisco IOS XE Catalyst SD-WAN デバイス が使用できる設定が提供されます。デバイスが Cisco SD-WAN Validator に接続すると、デバイスは Cisco SD-WAN Manager 上の要求されていない WAN エッジデバイスとして表示されます。オンボーディングを完了するには、Cisco SD-WAN Manager でデバイスを要求し、システム IP とサイト ID を設定するデバイステンプレートを添付する必要があります。Cisco SD-WAN Manager は汎用ブートストラップ構成の一部としてデバイスにインストールされている証明書を使用してデバイスを認証します。

汎用ブートストラップ構成には、次のものが含まれます。

- 組織名
- Cisco IOS XE Catalyst SD-WAN デバイス で有効にする WAN インターフェイス
- Cisco SD-WAN Validator の IP アドレス
- デバイスを認証するための Cisco SD-WAN Manager 署名付き証明書。

汎用ブートストラップ構成を使用してデバイスをオンボードするには、デバイスをインストールするブランチネットワークに Dynamic Host Configuration Protocol（DHCP）サーバーが必要です。汎用ブートストラップ構成では、WAN インターフェイスに IP アドレスを割り当てません。代わりに、WAN インターフェイスで DHCP クライアントを有効にして、インターフェイスがブランチネットワークの DHCP サーバーから IP アドレスを取得できるようにします。

汎用ブートストラップ構成の仕組み

1. Cisco SD-WAN Manager で汎用ブートストラップ構成を生成するときに、Cisco IOS XE Catalyst SD-WAN デバイス で VPN 0（WAN）インターフェイスとして機能するインターフェイスを選択します。
2. 汎用ブートストラップ構成ファイルをデバイスのブートフラッシュにコピーし、デバイスをリセットします。リセット時に、デバイスは汎用ブートストラップ構成で初期化されます。
3. ブートストラップ構成により、指定された VPN 0 インターフェイスで DHCP クライアントが有効になります。インターフェイスは、ネットワーク内の DHCP サーバーから IP アドレスと関連する詳細を取得します。
4. VPN 0 インターフェイスを介して Cisco SD-WAN Validator に接続するデバイスは、Cisco SD-WAN Validator および Cisco SD-WAN Manager で要求されていない WAN エッジデバイスとしてリストされています。
5. Cisco SD-WAN Manager でデバイスを要求すると、Cisco SD-WAN Manager はブートストラップ構成の一部としてデバイスにインストールされた証明書を使用してデバイスを認証します。認証後、デバイスは Cisco SD-WAN Manager および Cisco SD-WAN Validator の有効な WAN エッジデバイス間にリストされます。
6. システム IP とサイト ID を含むテンプレートを添付して、デバイスにプッシュします。
7. デバイスは Cisco SD-WAN コントローラ への制御接続を確立し、オーバーレイネットワークに追加されます。

汎用ブートストラップ構成を使用した Cisco IOS XE Catalyst SD-WAN デバイス へのオンボード

1. ワンタッチプロビジョニングの有効化：
    1. Cisco SD-WAN Manager のメニューで、**[Administration]** > **[Settings]** の順に選択します。
    2. [One Touch Provisioning] が [Enabled] になっているか確認します。[Enabled] になっている場合は、ステップ 2 に進みます。

3. [One Touch Provisioning] が [Disabled] になっている場合は、[Edit] をクリックします。
4. [Enable Claim WAN Edges] 設定で、[Enabled] を選択して [Save] をクリックします。

2. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]** > **[WAN Edge List]**の順に選択します。
3. [Export Bootstrap Configuration] をクリックします。
   1. [Export Bootstrap Configuration] ダイアログボックスで、[VPN0 Interface name] を入力します。

（注） VPN 0 インターフェイス名は、Cisco IOS XE Catalyst SD-WAN デバイス モデルによって異なる場合があります。オンボードするモデルに基づいてインターフェイス名を指定します。

   2. [Generate Generic Configuration] をクリックします。
4. 汎用ブートストラップ構成ファイルを保存します。

   ファイルには `<filename>.cfg` の形式で名前が付けられます。
5. 汎用ブートストラップ構成ファイルの名前を `ciscosdwan.cfg` に変更します。
6. `ciscosdwan.cfg` ファイルをブート可能な USB ドライブまたはデバイスのブートフラッシュにコピーします。
7. USB ドライブを使用している場合は、USB ドライブをデバイスに接続します。
8. CLI で次のコマンドを発行して、デバイスソフトウェア構成をリセットします。

```
Device# request platform software sdwan config reset
Device# reload
```

（注） 設定リセットを実行すると、新しいタイプ6マスターキーが生成されます。したがって、ブートストラップ設定ファイルを保護している現在のパスワードがプレーンテキストであり、タイプ6キーが含まれていないことを確認してください。ブートストラップ設定パスワードにタイプ 6 のキーが含まれていると、デバイスのリセットが失敗します。

9. デバイスを再起動します。
   - 再起動中、デバイスはUSBドライブまたはブートフラッシュから構成ファイルを読み取り、構成を適用します。

     この構成により、VPN0インターフェイスが有効になり、インターフェイスでDHCPクライアントが初期化されます。インターフェイスは、ネットワーク内の DHCP サーバーから IP アドレスを取得します。

デバイスが Cisco SD-WAN Validator に接続し、Cisco SD-WAN Validator および Cisco SD-WAN Manager で要求されていない WAN エッジデバイスとしてリストされます。

- Cisco SD-WAN Validator で、**show orchestrator unclaimed-vedges** コマンドを使用して、要求されていない WAN エッジデバイスを表示できます。
- Cisco SD-WAN Manager で、**[Configuration]** > **[Devices]** > **[Unclaimed WAN Edges]**を選択して、要求されていない WAN エッジデバイスを表示できます。

  デバイスが要求されていない WAN エッジデバイスとしてリストされていない場合は、デバイスが Cisco SD-WAN Validator に接続できるか確認し、接続の問題を修正します。

10. Cisco SD-WAN Manager でデバイスを要求します。

Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]** > **[Unclaimed WAN Edges]**の順に選択します。

1. 要求するデバイスを選択し、[Claim Device(s)] をクリックします。

- デバイスは、[Unclaimed WAN Edges] から削除され、[WAN Edge List] にリストされます。
- Cisco SD-WAN Validator で、デバイスが有効な WAN エッジデバイスとして表示されます。**show orchestrator valid-vedges** コマンドを発行すると、有効な WAN エッジデバイスを表示できます。

11. 構成テンプレートをデバイスに添付します。

1. テンプレートにシステム IP アドレスとサイト ID が含まれていることを確認してください。

2. テンプレートをデバイスにプッシュします。

結果

デバイスが Cisco SD-WAN コントローラ に接続し、オーバーレイネットワークに追加されます。

デバイスが制御接続を確立し、オーバーレイネットワークの一部であることを確認するには、Cisco SD-WAN Manager メニューから、**[Monitor]** > **[Overview]**の順に選択し、[WAN Edges] 領域の番号をクリックします。

（注） Cisco vManage リリース 20.6.x 以前の場合：デバイスが制御接続を確立し、オーバーレイネットワークの一部であることを確認するには、Cisco SD-WAN Manager メニューから、**[Dashboard]**> **[Main Dashboard]**の順に選択し、[Summary Pane] ペインで [WAN Edge Devices] をクリックします。

汎用ブートストラップ構成を使用してオンボードされた Cisco IOS XE Catalyst SD-WAN デバイスを削除する

1. テンプレートからデバイスを切り離します。
    1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
    2. [Device Templates] をクリックし、デバイスに添付されているテンプレートを選択します。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

    3. 選択したテンプレートについて、[...] をクリックし、[Detach Devices] を選択します。
    4. [Available Devices] 列で、テンプレートから切り離すデバイスを選択します。
    5. 右向きの矢印をクリックして、デバイスを [Selected Devices] 列に移動します。
    6. [Detach] をクリックします。
2. SSH を使用して、デバイスに接続します。デバイスの SSH ターミナルから、次のコマンドを使用して VPN 0 WAN インターフェイスをシャットダウンします。

```
Device(config)# interface vpn0-interface-name
Device(config-if)# shutdown
```

3. デバイスを無効にします。
    1. Cisco SD-WAN Manager のメニューから**[Configuration]** > **[Certificates]**の順に選択します。
    2. [WAN Edge List] をクリックし、無効にするデバイスを選択します。
    3. [Validate] 列で、[Invalid] をクリックします。
    4. [OK] をクリックして、無効な状態への移行を確認します。
    5. [Send to Controllers] をクリックして、無効化されたデバイスのシャーシ番号とシリアル番号をネットワーク内のコントローラに送信します。Cisco SD-WAN Manager にプッシュ操作のステータスを示す [Push WAN Edge List] 画面が表示されます。
4. WAN エッジデバイスを削除します。
    1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]**の順に選択します。
    2. [WAN Edge List] をクリックして、削除するデバイスを選択します。
    3. 選択したデバイスについて、[...] をクリックし、[Delete WAN Edge] を選択します。
    4. [OK] をクリックして、デバイスの削除を確認します。

Cisco SD-AVC のインストール（Cisco vManage 20.1.1 以前）

（注） Cisco vManage リリース 20.3.1/Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco SD-AVC のインストールが変更されました。「Cisco SD-AVC のインストール（Cisco vManage リリース 20.3.1 以降） （22 ページ）」を参照してください。

概要

18.4 リリース以降、Cisco Catalyst SD-WAN は任意でシスコのソフトウェア定義型 Application Visibility and Control（SD-AVC）を Cisco IOS XE Catalyst SD-WAN デバイス に組み込むことができます。SD-AVC ネットワークサービスは、Cisco SD-WAN Manager 内部のコンテナとして動作します。

この機能の利点

Cisco SD-AVC は、ネットワーク内のデバイスで動作する Cisco NBAR2 およびその他のコンポーネントを使用して、次の機能を提供します。

- 可視性、分析、アプリケーション認識型ルーティング、およびアプリケーションベースのポリシー（QoS やアプリケーションベースのファイアウォールポリシーなど）のためのネットワーク アプリケーション トラフィックの認識。
- ネットワークレベルでの分析。

Cisco SD-WAN Manager の Cisco SD-AVC インストール要件

次の表に、SD-AVC のインストール要件を示します。

Cisco SD-WAN Manager インストールのシナリオ	要件
クラウドベースサーバー上の Cisco vManage 18.4（シスコのクラウド運用チームによって完全に設定された状態で提供されます）	SD-AVC パッケージは、シスコのクラウド運用チームによって事前インストールされます。
自己管理型クラウドまたはローカルサーバー上の Cisco vManage 18.4	以下の説明に従って SD-AVC パッケージをインストールします。
以前のバージョンの Cisco SD-WAN Manager から Cisco vManage 18.4 へのアップグレード	以下の説明に従って SD-AVC パッケージをインストールします。

Cisco SD-WAN Manager での SD-AVC の有効化

前提条件

- SD-AVC ネットワークサービスの最新のコンテナイメージをダウンロードします。Cisco SD-WAN Manager をホスティングしているサーバー上のアクセス可能な場所にファイルを保存します。このコンテナは手続きに必要です。コンテナをダウンロードするには、[Cisco Software Download] ページを開き、「SD-WAN」と入力します。結果から [Software-Defined WAN（SD-WAN)] を選択し、[SD-WAN] を選択します。ダウンロード可能なソフトウェアパッケージで、[SD-AVC] を選択します。
- SD-WAN トポロジに含まれるネットワーク内のルータに DNS サーバーが設定されていることを確認します。
- Cisco SD-WAN Manager が動作する仮想マシンには、SD-AVC ネットワークサービス専用で使用できる次のリソースが必要です。
  - vCPU: 4
  - RAM：5 GB
  - ストレージ：40 GB

手順

1. ダウンロードした SD-WAN イメージがお使いの Cisco SD-WAN Manager バージョンと互換性があることを確認してください。
   1. 次の API を使用して、互換性のあるイメージのチェックサムを表示します。

      https://[vManage-IP-address]/dataservice/sdavc/checksum

      例：https://10.0.0.1/dataservice/sdavc/checksum
   2. ダウンロードしたイメージのチェックサムがこのチェックサムと一致することを確認します。
2. SD-AVC 仮想サービスパッケージを Cisco SD-WAN Manager にアップロードするには、次の手順を実行します。
   1. [Cisco SD-WAN Manager] メニューから、**[Maintenance]** > **[Software Repository]**の順に選択します。
   2. [Virtual Images] をクリックし、[Upload Virtual Image] を選択して SD-AVC パッケージをアップロードします。
3. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Cluster Management]**ページの順に選択します。
4. 目的のホスト（SD-AVC を有効にする Cisco SD-WAN Manager ポータル）で、[…] をクリックし、[Edit] を選択します。

5. [Edit Cisco SD-WAN Manager] ダイアログボックスで、Cisco SD-WAN Manager ログイン情報を使用してユーザー名とパスワードを入力します。
6. [Enable SD-AVC] のチェックボックスをオンにします。[Update] をクリックします。
7. デバイスを再起動して変更をデバイスに適用する前に、確認を求めるプロンプトが Cisco SD-WAN Manager から表示されます。[OK] をクリックして確定します。
8. 再起動後、Cisco SD-WAN Manager が自動的に起動し、SD-AVC アクティベーションの進行状況が表示されます。アクティベーションが完了するまで待ちます。
9. （オプション）インストールが完了したら、Cisco SD-WAN Manager により SD-AVC 仮想サービスがインストールされ、正しく動作していることを確認できます。
    1. Cisco SD-WAN Manager メニューから、**[Administration]** > **[Cluster Management]**の順に選択します。
    2. [Service Configuration] の表の Cisco SD-WAN Manager 行で、SD-AVC に緑色のチェックマークが表示されていることを確認します。

Cisco SD-WAN Manager コマンドの詳細については、『Cisco SD-WAN Manager Command Reference』を参照してください。

Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化

Cisco IOS XE Catalyst SD-WAN デバイス で SD-AVC を有効にするには、**アプリの可視性**を有効にするローカライズされたポリシーを作成し、そのポリシーを Cisco IOS XE Catalyst SD-WAN デバイス のテンプレートに適用します。

前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス 用のテンプレートが存在すること（例：Cisco ASR 1001-X、Cisco ISR 4321）。
- TCP ポート 10501 の宛先トラフィックを許可する必要があります。

手順

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Localized Policy] をクリックします。
3. ポリシーを追加してアプリケーションを有効にするには、次の手順に従います。
    1. [ポリシーの追加（Add Policy）] をクリックします。
    2. [Policy Overview] 画面が表示されるまで、複数の画面（[Create Groups of Interest]、[Configure Forwarding Classes/QOS]、[Configure Access Control Lists]、[Configure Route Policy]）で [Next] をクリックします。
    3. [Policy Overview] 画面で、ポリシー名とポリシーの説明を入力します。

4. [Application] を選択します。
5. ポリシーを保存します。

4. ローカライズされたポリシーをデバイステンプレートに追加するには、次の手順に従います。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
   2. SD-AVC を有効にする必要があるデバイスで、[…] をクリックし、メニューから [Edit] を選択します。
   3. [Additional Templates] をクリックします。
   4. この手順の前のステップで作成したローカライズされたポリシーを追加します。
   5. [Update] をクリックして次の画面に進み、更新されたテンプレートをデバイスにプッシュします。

5. （オプション）更新をデバイスにプッシュすると、次のいずれかのコマンドを使用して、デバイスの SD-AVC のステータスを確認できます。

   ```
   show avc sd-service info summary
   ```

   または

   ```
   show avc sd-service info connectivity
   ```

Cisco SD-AVC のインストール（Cisco vManage リリース 20.3.1 以降）

Cisco vManage リリース 20.3.1 をインストールまたはアップグレードすると、Cisco SD-AVC がコンポーネントとして自動的にインストールされます。

Cisco SD-AVC の詳細については、Cisco SD-AVCを参照してください。

Cisco SD-AVC、Cisco vManage リリース 20.3.1 以降の有効化

前提条件

Cisco Catalyst SD-WANトポロジに含まれるネットワーク内のルータに DNS サーバーが設定されていることを確認します。

（注） Cisco SD-AVC は、単一の Cisco SD-WAN Manager インスタンスのみで動作する必要があります。Cisco SD-WAN Manager クラスタでは、単一の Cisco SD-WAN Manager インスタンスのみで Cisco SD-AVC を有効にします。

Cisco SD-AVC を有効にするには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、 [Administration] > [Cluster Management] の順に選択します。
2. 目的のホスト（SD-AVC を有効にするポータル）で、[…] をクリックし、[Edit] を選択します。
3. [Edit Manage] ポップアップウィンドウで、[Enable SD-AVC] のチェックボックスをオンにします。

（注） [Edit Manage] ポップアップウィンドウには、アプリケーションサーバーを無効にするオプションがあります。アプリケーションサーバーを無効にした後、この方法を使用して後で他のサービスを有効にすることはできません。アプリケーションサーバーを無効にする必要がある場合は、他の機能を有効にするのと同時にアプリケーションサーバーを無効にすることはしないでください。

4. Cisco SD-WAN Manager のログイン情報を使用して、ユーザー名とパスワードを入力します。デバイスを再起動して変更を適用します。
5. 再起動後、Cisco SD-WAN Manager が自動的に起動し、SD-AVC アクティベーションの進行状況が表示されます。アクティベーションが完了するまで待ちます。
6. （オプション）インストールが完了したら、Cisco SD-WAN Manager によりSD-AVC 仮想サービスがインストールされ、正しく動作していることを確認できます。
    1. Cisco SD-WAN Manager メニューから、 [Administration] > [Cluster Management] の順に選択します。
    2. [Service Configuration] をクリックし、テーブルの [Cisco SD-WAN Manager] 行で、SD-AVC に緑色のチェックマークが表示されていることを確認します。

Cisco IOS XE Catalyst SD-WAN デバイス での SD-AVC の有効化

Cisco IOS XE Catalyst SD-WAN デバイス で SD-AVC を有効にするには、**アプリの可視性**を有効にするローカライズされたポリシーを作成し、そのポリシーを Cisco IOS XE Catalyst SD-WAN デバイス のテンプレートに適用します。

前提条件

- Cisco IOS XE Catalyst SD-WAN デバイス 用のテンプレートが存在すること（例：Cisco ASR 1001-X、Cisco ISR 4321）。
- TCP ポート 10501 の宛先トラフィックを許可する必要があります。

手順

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Localized Policy] をクリックします。
3. ポリシーを追加してアプリケーションを有効にするには、次の手順に従います。
   1. [ポリシーの追加（Add Policy）] をクリックします。
   2. [Policy Overview] 画面が表示されるまで、複数の画面（[Create Groups of Interest]、[Configure Forwarding Classes/QOS]、[Configure Access Control Lists]、[Configure Route Policy]）で [Next] をクリックします。
   3. [Policy Overview] 画面で、ポリシー名とポリシーの説明を入力します。
   4. [Application] を選択します。
   5. ポリシーを保存します。
4. ローカライズされたポリシーをデバイステンプレートに追加するには、次の手順に従います。
   1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
   2. SD-AVC を有効にする必要があるデバイスで、[…] をクリックし、メニューから [Edit] を選択します。
   3. [Additional Templates] をクリックします。
   4. この手順の前のステップで作成したローカライズされたポリシーを追加します。
   5. [Update] をクリックして次の画面に進み、更新されたテンプレートをデバイスにプッシュします。
5. （オプション）更新をデバイスにプッシュすると、次のいずれかのコマンドを使用して、デバイスの SD-AVC のステータスを確認できます。

   ```
   show avc sd-service info summary
   ```

   または

   ```
   show avc sd-service info connectivity
   ```

Cisco SD-AVC Cloud Connector、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降の有効化

表 *4 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-AVC Cloud Connector を有効にするための新しい手順	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1	このリリースでは、**[Administration]** > **[Settings]** の [Cloud Services] オプションから Cisco SD-AVC Cloud Connector を有効にするための新しい手順が導入されています。このリリース以降、Cloud Connector を有効にするために、OTP や TAC ケースをオープンする必要はありません。

Cisco Catalyst SD-WAN Manager リリース 20.14.1 より前は、Cloud Connector を有効にするために、クライアント ID、クライアントシークレットのログイン情報、および場合によってはクラウドゲートウェイの URL と OTP が必要でした。Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降、[Cloud Services] ページを使用して Cisco SD-AVC Cloud Connector を設定できます。この機能を使用すると、SD-AVC Cloud Connector を有効にするために、OTP を取得したり、TAC ケースを個別に作成したりする必要はありません。

前提条件

Cloud Connector を有効にするには、**[Administration]** > **[Cluster Management]** で Cisco SD-AVC を有効にします。

クラウドサービスを使用した Cisco SD-AVC Cloud Connector の有効化

1. Cisco SD-WAN Manager メニューから、[Administration] > [Settings] の順に選択します。
2. [Cloud Services] をクリックします。
3. [Cloud Services] タブで [Cloud Services] を有効にします。
4. フィールドにスマートアカウントのログイン情報を入力します。
5. （任意）[Analytics] を有効にします。

（注） Cisco Catalyst SD-WAN Analytics を展開し、Cisco SD-WAN Manager によって到達可能であることを確認した場合にのみ、このオプションを有効にします。

6. [SD-AVC Cloud Connector] を有効化します。

（注） Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、クラウドサービスオプションを有効にした後で、Cloud Connector が自動的に有効になります。

7. [Save] をクリックします。

Cisco Catalyst SD-WAN Manager リリース 20.13.x を使用する Cisco SD-AVC Cloud Connector の有効化

表 *5:* 機能の履歴

機能名	リリース情報	説明
Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	Cloud onRamp for SaaS で Office 365 トラフィックを管理できるようにする場合、Microsoft によって定義された Office 365 トラフィックカテゴリに従って、ベストパスの選択を一部の Office 365 トラフィックのみに適用するか、またはすべての Office 365 トラフィックを含めるように制限できます。 Cisco SD-AVC Cloud Connector では、この機能がサポートされています。
SD-AVC Cloud Connector を有効にするための更新	Cisco vManage リリース 20.10.1	このリリース以降、Cloud Connector を有効にするには、クライアント ID とクライアントシークレットではなく、クラウドゲートウェイの URL とワンタイムパスワード（OTP）が必要です。

はじめる前に

- Cisco vManage リリース 20.10.1 以前は、Cloud Connector を有効にするには、クライアント ID とクライアントシークレットのログイン情報が必要でした。Cisco vManage リリース 20.10.1 以降は、クラウドゲートウェイの URL と OTP が必要です。OTP を使用する利点は、クライアントシークレットとは対照的に、OTP が期限切れにならないことです。さまざまなリリース、アップグレードシナリオ、およびホスティングオプションに必要なログイン情報の詳細については、次の表を参照してください。
- Cisco SD-AVC Cloud Connector は、Cloud onRamp for SaaS が Office 365 トラフィックカテゴリに従って、Office 365 トラフィックを管理するために必要なコンポーネントです。

表 *6 : SD-AVC Cloud Connector* を有効にするための要件

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
Cisco vManage リリース 20.3.1 から Cisco vManage リリース 20.9.x へ	すべてのホスティングオプション	**必要なログイン情報**： Client ID クライアントシークレット （手順で説明されているように、ログイン情報をまだ持っていない場合は、Cisco API Console ページを開いて Cloud Connector ログイン情報を作成します。） （注） Cisco SD-WAN Manager 内に SD-AVC ログイン情報の有効期限が近づいていることを示すメッセージが表示されたら、Cisco API コンソールに戻り、新しい Cloud Connector ログイン情報を作成します。 **その他の要件**： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
既存のインスタンスを以前のリリースから Cisco vManage リリース 20.10.1 にアップグレード	シスコホステッド	**必要なログイン情報：** • クラウドゲートウェイの URL： 使用： https://management-us01.sdwan.cisco.com/validate_sdavc/ • OTP： Cisco Catalyst SD-WAN Portal を使用して、OTP を取得します。詳細については、『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/self-serv-por/sdwan-ssp.html **その他の要件：** ここで説明されているように、クラスタ管理で SD-AVC を有効にします。 **注：** このシナリオでは、SD-AVC コンポーネントは以前のリリースとは異なる方法で動作します。そのため、Cisco SD-WAN Manager インスタンスで **request nms all status** コマンドを実行すると、「NMS SDAVC サーバー」コンポーネントが有効になっていないことが示されます。これは予期される動作であり、SD-AVC の問題を示すものではありません。「NMS SDAVC ゲートウェイ」コンポーネントが有効と表示されていることに注意してください。

リリース	**Cisco SD-WAN Manager** ホスティング	**Cloud Connector** を有効にするための要件
	自己管理型、パブリッククラウド、プライベートクラウド、またはオンプレミスでホスト	

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		必要なログイン情報： • アップグレード時に Cloud Connector がすでに有効になっている場合、クライアント ID とクライアントシークレットのログイン情報は、クライアントシークレットの期限が切れるまで引き続き機能します。 クライアントシークレットが期限切れになると、期限切れを示すアラームが Cisco SD-WAN Manager に表示されます。この時点で、Cloud Connector を有効にするには、クラウドゲートウェイの URL と OTP が必要です。URL の https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ を使用し、TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。 • アップグレード時に Cloud Connector が有効になっていない場合、Cloud Connector を有効にするには、クラウドゲートウェイの URL と OTP が必要です。URL の https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ を使用し、TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		その他の要件： Cloud Connector を有効にする前に、ここで説明されているように、クラスタ管理で SD-AVC を有効にします。

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
Cisco vManage リリース 20.10.1 以降の新規インストール	シスコホステッド	**必要なログイン情報：** Cloud Connector はデフォルトで有効になっており、ログイン情報を手動で入力する必要はありません。必要に応じて、Cisco SD-WAN Self-Service Portal を使用して OTP を表示できます。詳細については、『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/self-serv-por/sdwan-ssp.html **その他の要件：** ここで説明されているように、クラスタ管理で SD-AVC を有効にします。 **注：** このシナリオでは、SD-AVC コンポーネントは以前のリリースとは異なる方法で動作します。そのため、Cisco SD-WAN Manager インスタンスで **request nms all status** コマンドを実行すると、「NMS SDAVC サーバー」コンポーネントが有効になっていないことが示されます。これは予期される動作であり、SD-AVC の問題を示すものではありません。「NMS SDAVC ゲートウェイ」コンポーネントが有効と表示されていることに注意してください。
	自己管理型、パブリッククラウド、プライベートクラウド、またはオンプレミスでホスト	

リリース	Cisco SD-WAN Manager ホスティング	Cloud Connector を有効にするための要件
		必要なログイン情報： • クラウドゲートウェイの URL： https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/ を利用する • OTP： TAC ケースを開いて OTP を取得します。TAC ケースを開く方法については、このセクションの手順を参照してください。 **その他の要件**： ここで説明されているように、クラスタ管理で SD-AVC を有効にします。

Cisco SD-AVC Cloud Connector の有効化

1. Cisco SD-WAN Manager メニューから、[Administration] > [Settings] の順に選択します。
2. [SD-AVC] をクリックし、[Cloud Connector] を有効にします。

   （Cisco vManage リリース 20.10.x、Cisco vManage リリース 20.11.x、または Cisco Catalyst SD-WAN Manager リリース 20.12.x を使用している場合は、[Edit] をクリックし、[Cloud Connector] を有効にします。）

   （Cisco vManage リリース 20.9.x 以前のリリースでは、オプションは [SD-AVC Cloud Connector] と呼ばれています。これらのリリースでは、[Edit] をクリックし、[Cloud Connector] を有効にします。）

（注） Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、Cloud Connector が自動的に有効になります。

3. （この手順は Cisco vManage リリース 20.10.1 以降に適用され、Cisco SD-WAN Manager がシスコホステッドの場合は自動的に処理されます。）

   さまざまなシナリオで SD-AVC Cloud Connector を有効にするための要件の詳細については、これらの手順の前にある [Before You Begin] セクションを参照してください。そこに記載されているように、Cloud Connector を有効にする前に、クラスタ管理で SD-AVC を有効にします。

クラウドゲートウェイの URL を入力する必要がある場合は、https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/ を使用します。

Cisco Catalyst SD-WAN Portal を使用して OTP を取得する必要がある場合は、詳細について『Cisco Catalyst SD-WAN Portal Configuration Guide』を参照してください。

OTP を受け取るために TAC ケースを開く必要がある場合は、https://mycase.cloudapps.cisco.com/case を開きます。OTP を受け取るためのワークフローには、次のものが必要です。

- 資格情報。
- スマートアカウント。
- バーチャルアカウント。
- Cisco SD-WAN Manager で設定された組織名。
- Cisco SD-WAN Manager 地理的位置：南北アメリカ、欧州連合 (EU)、またはアジア太平洋（APAC）。
- テクノロジー：オンプレミスインストールには Cisco Catalyst SD-WAN On-Prem を使用し、シスコがホストするインストールには Cisco Catalyst SD-WAN- Cisco-Hosted を使用します。
- サブテクノロジー：SDWAN クラウドインフラを使用します。

4. （Cisco vManage リリース 20.9.x 以前のリリースの場合）次のログイン情報を入力します。
   - Client ID

（注） [Client ID] の（i）をクリックし、ブラウザウィンドウで [Cisco API Console] ページを開き、ログイン情報がない場合は Cloud Connector ログイン情報を作成します。https://apiconsole.cisco.com/

   - クライアントのシークレット（Client Secret）]
   - [Organization Name]：[Cisco API Console] ページの [Name of your application] フィールドに入力したわかりやすい名前を使用します。

5. （Cisco vManage リリース 20.10.1 より以前のリリース）[Affinity] の場合、Cloud Connector データを保存する地理的な場所を選択できます。ヨーロッパに所在する組織の場合、EU 一般データ保護規則（GDPR）規則に従って、場所をヨーロッパに変更することを推奨します。

6. [Telemetry] の場合、必要に応じて、テレメトリデータの収集を無効化できます。

（注） Cisco SD-WAN Manager がシスコによってクラウドでホストされている場合、このオプションは表示されず、テレメトリが自動的に有効になります。

Cisco API コンソールでのログイン情報の作成

次の手順は、Cisco API コンソールでログイン情報を作成する方法を示しています。便宜上、ここに手順が示されていますが、変更される可能性があります。

1. [Cisco API Console] ページで、シスコのログイン情報を使用してサインインします。
2. [My Apps and keys] をクリックします。新規アプリケーションの登録ページが開きます。
3. SD-AVC を登録するには、以下の手順に従います。
    1. アプリケーションの名前：わかりやすい名前を使用してください。後の手順のためにこの名前を保存します。
    2. [Application Type] 領域で、[Service] をクリックします。
    3. [Grant Type] 領域で、[Client Credentials] チェックボックスをオンにします。
    4. [Hello API] チェックボックスをオンにします。
    5. [Terms of Service] セクションで、チェックボックスをオンにして条件に同意します。
    6. [Register] をクリックします。[Cisco API Console] ページには、クライアント ID とクライアントシークレットの詳細が表示されます。このページを開いたままにして、手順を完了します。

（注） ログイン情報は 90 日後に期限切れになります。

Cisco SD-WAN Manager 内に SD-AVC ログイン情報の有効期限が近づいていることを示すメッセージが表示されたら、Cisco API コンソールに戻り、新しい Cloud Connector ログイン情報を作成します。

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

同じルータに最大 2 つの Cisco Catalyst SD-WAN イメージをインストールできます。

サポートされているハードウェア プラットフォームとインターフェイスモジュール

サポートされているハードウェア プラットフォームとインターフェイスモジュールについては、リリースノートを参照してください。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a の Cisco IOS XE Catalyst SD-WAN デバイス の場合、PnP または自動インストールプロセス完了後に .bin ファイルを使用してデバイスを起動すると、デバイスはDay-0構成で起動します。その後、デバイスが自動的にリロードして、インストールモードになります。

サポートされる暗号モジュール

ASR 1000 シリーズのルータには、以下の暗号モジュールが必要です。

- ASR 1001-HX 用 ASR 1001HX-IPSECHW
- ASR 1002-HX 用 ASR 1002HX-IPSECHW

はじめる前に

オーバーレイネットワークに IOS XE ルータを展開する前に、次の点を確認してください。

- コントローラデバイス（Cisco SD-WAN Validator、Cisco SD-WAN Manager インスタンス、およびCisco SD-WAN コントローラ）が Cisco Catalyst SD-WAN ソフトウェアリリース 18.3 を実行していること。
- オーバーレイネットワークにIOS XEルータとvEdgeルータの両方を展開する場合、vEdgeルータがリリース17.2.1以降のCisco Catalyst SD-WANソフトウェアを実行していること。これらのソフトウェアバージョンでは、vEdge と IOS XE ソフトウェアが相互運用でき、vEdge ルータと IOS XE ルータ間に BFD トンネルを確立できます。
- 同じサイトに IOS XE ルータと vEdge ルータの両方を展開する場合、vEdge ルータが Cisco Catalyst SD-WAN ソフトウェア リリース 18.3 を実行していること。
- ISR 4000 シリーズ ルータに少なくとも 4 GB の DRAM が搭載されていること。ルータには 8 GB の DRAM を搭載することをお勧めします。
- ASR 1000 Cisco SD-WAN Validator シリーズ ルータに少なくとも 8 GB の DRAM が搭載されていること。ASR 1002-HX ルータに少なくとも 16 GB の DRAM が搭載されていること。
- ルータブートフラッシュでは最小 1.5 GB のスペースが XE SD-WAN イメージに使用できます。Cisco IOX SD-WAN リリース 17.10 以降のルータブートフラッシュでは、ディスクスペースの半分以上が XE SD-WAN イメージに使用できます。
- エンタープライズルート証明書を使用してルータを認証する場合、XE SD-WAN ソフトウェアをインストールする前に、証明書がルータのブートフラッシュにコピーされていること。

- XE SD-WAN ソフトウェアをインストールする前に、サポートされていないすべてのモジュールをルータから取り外していること。サポートされるモジュールのリストについては、「サポートされるインターフェイスモジュール」および「サポートされる暗号モジュール」を参照してください。
- RP3 モジュールを搭載した Cisco ASR 1006-X の展開については、RP3 モジュールを搭載した Cisco ASR 1006-X を参照してください。
- 更新されたデバイス リストが Cisco SD-WAN Manager にアップロードされ、Cisco SD-WAN Validator に送信されていること。次の手順を実行します。
  1. システムプロンプトで **show crypto pki certificates CISCO_IDEVID_SUDI** コマンドを実行して、ルータのシャーシおよびボード ID のシリアル番号を取得します。ASR シリーズ ルータでリリース 16.6.1 以前を実行している場合は、**show sdwan certificate serial** コマンドを実行します。
  2. プラグアンドプレイ（PnP）Connect ポータルでルータのシリアル番号を追加します。詳細については、「IOS XE ルータの PnP ポータルへの追加」セクションを参照してください。
  3. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Devices]**を選択します。[Sync Smart Account] をクリックして、更新されたデバイスリストを Cisco SD-WAN Manager にダウンロードし、Cisco SD-WAN Validator に送信します。
- デバイス設定テンプレートは、Cisco SD-WAN Manager の**[Configuration]** > **[Templates]**を使用して作成され、ルータにアタッチされます。 これにより、ルータが起動時に設定を取得し、完全な制御接続を確立できるようになります。
- ルータが 250 Mbps の単方向暗号化帯域幅を超えており、HSECK9 ライセンスがまだインストールされていない場合、ライセンスファイルはルータのブートフラッシュにコピーされ、ライセンスはルータのライセンス インストール ファイル パスにインストールされます。
- ASR 1000 シリーズ、ISR 1000 シリーズ、および ISR 4000 シリーズ ルータが、次の表に示すように、必要なバージョンの ROM モニタ ソフトウェア（ROMMON）を実行していること。ルータで実行中の ROMMON のバージョンを確認するには、システムプロンプトで **show rom-monitor** コマンドまたは **show platform** コマンドを実行します。

ハードウェア プラットフォーム	必要な ROM モニタ ソフトウェア バージョン
ASR 1000 シリーズ	16.3 (2r)
ISR1000 シリーズ	16.9 (1r)
ISR4000 シリーズ	16.7 (3r)

- ISRv ルータが、次の表に示すように、CIMC および NFVIS ソフトウェアの必要最小限のバージョンを実行していること。

ハードウェア プラットフォーム	CMC	NFVIS
ISRv	3.2.4	3.8.1

Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェアのダウンロード

Cisco IOS XE Catalyst SD-WAN ソフトウェアのダウンロード

シスコのサイトから Cisco IOS XE Catalyst SD-WAN ソフトウェアをダウンロードするには、次の手順を実行します。

1. https://www.cisco.com にアクセスします。
2. 左側のメニューから [Support & Downloads] をクリックします。
3. [Products and Downloads] ページの [Downloads] 検索ボックスで、[Software-Defined WAN (SD-WAN)] を選択します。
4. [Select a Product] ページの右端のペインで、[XE SD-WAN Routers] を選択します。
5. 右端のペインから、ルータのモデルを選択します。
6. 目的のソフトウェアリリースバージョンをクリックしてダウンロードします。ソフトウェアイメージ名の形式は、router-model-ucmk9. release-number です。
7. ソフトウェアイメージをローカルネットワークの HTTP または FTP ファイルサーバーにコピーします。

Cisco IOS XE SD-WAN リリース 16.12 以前の Cisco IOS XE Catalyst SD-WAN ソフトウェアのインストール

すべての新しい Cisco IOS XE Catalyst SD-WAN デバイス は、Cisco IOS XE Catalyst SD-WAN ソフトウェアがすでにインストールされた状態で出荷されます。

既存の Cisco IOS XE Catalyst SD-WAN デバイス がある場合は、次の手順に従って Cisco IOS XE Catalyst SD-WAN ソフトウェアをインストールします。Cisco IOS XE Catalyst SD-WAN イメージを使用してルータが再起動します。

1. シスコのサイトから Cisco IOS XE Catalyst SD-WAN ソフトウェアイメージをダウンロードします。
2. ファイルサーバーからデバイスのブートフラッシュに Cisco IOS XE Catalyst SD-WAN ソフトウェアイメージをアップロードします。次に FTP の構文例を示します。

```
Device# (config)# ip ftp source-interface interface
Device# copyftp:// username:password@server-IP/file-location bootflash:
```

```
TFTP:
Device(config)# ip tftp source-interface interface
Device(config)# ip tftp blocksize 8192
Device(config)#exit
Device#copy tftp: bootflash:
SCP (assumes SSH is enabled):
Device# configure terminal
Device# (config)# ip scp server enable
FileServer$ scp filenameusername@router-IP:/filename
```

3. デバイスが管理コンソールに接続されていることを確認します。
4. デバイスのブートフラッシュに保存できる現在の構成のバックアップを作成します。

```
Device# copy run bootflash:original-xe-config
```

5. 既存の boot ステートメントをすべて削除し、構成を保存します。

```
ISR4K# (config)# no boot system ...
ISR4K# wr mem
```

6. 次の出力で、BOOT 変数が空白であることを確認します。

```
ISR4K# show bootvar
BOOT variable =
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

7. Cisco IOS XE Catalyst SD-WAN イメージを指す BOOT 変数を追加します。

```
Device(config)# boot system flash bootflash:
SDWAN-image
Device(config)# exit
ISR4K# write memory
```

8. BOOT 変数が Cisco IOS XE Catalyst SD-WAN イメージを指していることを確認します。

```
Device# show bootvar
BOOT variable =  bootflash:isr4300-ucmk9.16.10.1a.SPA.bin,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exists
Configuration register is 0x2102
Standby not ready to show bootvar
```

9. ルータから既存の構成をすべて削除します。

```
Device# write erase
```

10. config-register を 0x2102 に設定します。

```
Device# configure terminal
Deovce(config)# config-register 0x2102
Device(config)# end
```

11. config-register が 0x2102 に設定されていることと、それが次回の再起動時に 0x2102 に設定されることを確認します。

```
Device# show bootvar
```

12. ルータを再起動します。

```
ISR4K# reload
Proceed with reload? [confirm] Yes
```

```
If prompted to save the configuration, enter No. The router reboots with the XE
SD-WAN image.
```

13. 初期構成ダイアログを開始するプロンプトが表示されたら、「**No**」と入力します。

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [Yes/No]: No
```

14. 自動インストールプロセスの終了を求められたら、「**Yes**」と入力します。

```
Would you like to terminate auto-install? [Yes/No]: Yes
```

15. ログインプロンプトで、デフォルトのユーザー名およびパスワード（**admin**）を使用してログインします。

    デフォルトのパスワードは 1 回使用でき、その後は変更する必要があります。初期構成セッションがタイムアウトになったか、パスワードを変更して保存する前にセッションが中断または終了した場合、以降のログイン試行は失敗します。デバイスへのログインアクセスを復元するには、ROMMON モードのローカルコンソールからパスワードをデフォルト値にリセットする必要があります。その後、初期プロビジョニングプロセスを再開する必要があります。パスワードの復元については、デフォルトパスワードの復元（46 ページ）を参照してください。

16. PnP を停止し、Cisco IOS XE Catalyst SD-WAN パッケージのインストールを許可します。

```
ISR4K# pnpa service discovery stop
```

17. **request platform software sdwan software upgarde-confirm** を使用して、Cisco IOS XE Catalyst SD-WAN デバイスのアップグレードを設定します。

```
Router# request platform software sdwan software upgrade-confirm
Router#
*Sep 21 00:26:29.242: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install commit PACKAGE
*Sep 21 00:26:30.153: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install commit PACKAGE
Router#
```

18. **show sdwan software** の出力に、ユーザーとして CONFIRMED ステートが表示され、他の値が表示されないことを確認します。

```
Router# sh sdwan software
VERSION       ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
--------------------------------------------------------------------------------
16.12.1b.0.4  true    true     true      user       2019-09-21T00:24:22-00:00

Total Space:388M Used Space:86M Available Space:298M
```

19. **request platform software sdwan software reset** を使用して Cisco IOS XE Catalyst SD-WAN デバイスを設定します。

```
Router# request platform software sdwan software reset

*Sep 21 00:27:20.025: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install activate bootflash:isr4300-ucmk9.16.12.1b.SPA.bin
*Sep 21 00:27:43.105: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
*Sep 21 00:28:47.233: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install activate PACKAGESep 21 00:28:54.240: %PMAN-5-EXITACTION: R0/0:
pvp: Process manager
```

（注） このイメージをインストールしたら、必ず、**config-transaction** コマンドを使用して CLI 構成モードを開始してください。**config terminal** コマンドは、Cisco Catalyst SD-WAN ルータではサポートされていません。

（注） 古いイメージバージョンのフレッシュインストールへのダウングレードはサポートされていません。古いイメージの以前の既存バージョンにのみダウングレードできます。たとえば、Cisco IOS XE Catalyst SD-WAN 16.10.3 を Cisco IOS XE Catalyst SD-WAN デバイス にインストールしたことがなく、Cisco IOS XE Catalyst SD-WAN 16.11.1 リリースから Cisco IOS XE Catalyst SD-WAN 16.10.3 リリースにダウングレードしようとすると、この操作はサポートされず、予期しない動作が発生します。ただし、以前に 16.10.3 イメージをインストールしている場合は、**request platform software sdwan activate** コマンドを使用して再アクティブ化できます。

（注） データは、アップグレード時にのみ既存の Cisco Catalyst SD-WAN イメージから新しい Cisco Catalyst SD-WAN イメージに移行されます。アップグレードが完了すると、Cisco IOS XE Catalyst SD-WAN と Cisco vEdge デバイス の両方について、インストールされているイメージの異なるバージョンの間でデータが移行されることはありません。たとえば、以前に 19.2.4 をインストールしていて、20.3.2 が現在のアクティブイメージである場合、19.2.4 イメージをアクティブにすると、追加の構成が 20.3.2 から 19.2.4 に移行されません。

CLI を使用した IOS XE ルータの設定

Cisco IOS XE Catalyst SD-WAN デバイス が DHCP サーバーに接続されている場合、PnP は自動的に実行され、Cisco SD-WAN Manager は制御接続が稼働するとデバイスを自動的に設定します。制御接続が稼働しており、デバイスが検証されていることを確認するには、システムプロンプトで次のコマンドを入力します。

```
Device# show sdwan control connections
```

IOS XE ルータが DHCP サーバーに接続されていて、PnP を使用していない場合、または IOS XE ルータが WAN 上の DHCP サーバーに接続されていない場合は、次の手順に示すように、CLI を使用してルータを手動で設定します。

また、**system host-name** *hostname* コマンドを使用してホスト名を設定することもできます。ホスト名の設定は任意ですが、ホスト名はCLIのプロンプトの一部として含まれ、さまざまな Cisco SD-WAN Manager 画面でデバイスを参照するために使用されるため、設定することを推奨します。このコマンドはデバイス CLI では使用できませんが、CLI デバイステンプレートを使用している場合は使用できます。

1. 管理コンソールを使用してルータに接続します。
2. PnP を停止して、CLI へのアクセスを許可します。

```
Device# pnpa service discovery stop
```

3. コンフィギュレーション モードに入ります。

```
Device# config-transaction
Device(config)#
```

4. システム IP アドレスを設定します。

```
Device(config-system)# system-ip  ip-address
```

Cisco SD-WAN Manager は、システム IP アドレスを使用してデバイスを識別し、NMS が完全な設定をデバイスにダウンロードできるようにします。

5. デバイスが配置されているサイトの数値識別子を設定します。

```
Device(config-system)# site-id site-id
```

6. Cisco SD-WAN Validator の IP アドレスか、Cisco SD-WAN Validator を指す DNS 名を設定します。Cisco SD-WAN Validator の IP アドレスは、ルータが Cisco SD-WAN Validator に到達できるように、パブリック IP アドレスにする必要があります。

```
Device(config-system)# vbond (dns-name | ip-address)
```

7. 組織名を設定します。組織名は、オーバーレイネットワーク内のすべてのデバイスの証明書に含まれる名前です。組織名は、すべてのデバイスで同じにする必要があります。

```
Device(config-system)# organization-name name
```

8. オーバーレイ接続に使用するトンネルインターフェイスを設定します。トンネルインターフェイス ID が、Cisco SD-WAN Manager によって自動的に割り当てられる他のインターフェイス ID と競合しないようにしてください。これは、構成プレビューで確認できます。

```
Device(config)# interface Tunnel #
Device(config-if)# ip unnumbered wan-physical-interface
Device(config-if)# tunnel source wan-physical-interface
Device(config-if)# tunnel mode sdwan
```

（注）
- 構成に Cisco SD-WAN Manager **機能テンプレート**を使用している場合、トンネルインターフェイスは、使用されている WAN インターフェイスに基づいて自動的に割り当てられます。
- CLI モードから Cisco SD-WAN Manager **モード**に切り替えると、使用する WAN インターフェイスに基づき、トンネルインターフェイス番号が Cisco SD-WAN Manager によって自動的に割り当てられるため、設定したトンネルインターフェイスが変更される場合があります。トンネル番号の変更により、構成がプッシュされたときに、トンネルが停止してから再起動する可能性があります。

9. ルータが DHCP サーバーに接続されていない場合は、WAN インターフェイスの IP アドレスを設定します。

```
Device(config)# interface GigabitEthernet  #
Device(config)# ip address  ip-address mask
```

```
Device(config)# no shut
Device(config)# exit
```

10. トンネルパラメータを設定します。

```
Device(config)# sdwan
Device(config-sdwan)# interface  WAN-interface-name
Device(config-interface-interface-name)# tunnel-interface
Device(config-tunnel-interface)# color color/path-name
Device(config-tunnel-interface)# encapsulation  ipsec
```

11. ルータでIPアドレスが手動で設定されている場合は、デフォルトルートを設定します。

```
Device(config)# ip route 0.0.0.0 0.0.0.0 next-hop-ip-address
```

12. Cisco SD-WAN Validator アドレスがホスト名として定義されている場合は、DNS を設定します。

```
Device(config)# ip domain lookup
Device(config)# ip name-server dns-server-ip-address
```

13. 変更を保存して、コンフィギュレーション モードを終了します。

```
Device(config)# commit and-quit
Device# exit
```

14. エンタープライズルート CA によって署名された証明書を使用している場合は、その証明書をインストールします。

```
Device# request platform software sdwan root-cert-chain install bootflash:
certificate
```

15. 制御接続が稼働しており、ルータが検証されていることを確認します。

```
Device# show sdwan control connections

PEER    PEER PEER          SITE  DOMAIN  PEER          PEER PRIV  PEER         PEER
PUB
TYPE    PORT SYSTEM IP     ID    ID      PRIVATE IP    PORT       PUBLIC IP    PORT
    LOCAL COLOR
------------------------------------------------------------------------------------------
vsmart  dtls 192.168.1.2  10    1       172.1.1.3     12346      172.1.1.3    12346
     biz-internet
vbond   dtls -              0    0       172.1.1.4     12346      172.1.1.4    12346
     biz-internet
vmanage dtls 192.168.1.3  10    0       172.1.1.2     12346      172.1.1.2    12346
     biz-internet

                          CONTROLLER
                          GROUP
PROXY STATE  UPTIME       ID
-------------------------------------
  up         1:19:51:40   0
  up         1:19:51:45   0
  up         1:19:51:38   0
```

これで、Cisco SD-WAN Manager テンプレートを使用して、ルータで SD-WAN 機能を設定できるようになりました。

IOS XE デバイスのプラグアンドプレイポータルへの追加

表 7: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN のオンプレミスの ZTP サーバー	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、オンプレミスのプラグアンドプレイ実装のサポートが Cisco IOS XE Catalyst SD-WAN ルータに拡張されます。

プラグアンドプレイポータルにデバイスを追加するには、次の手順を実行します。

- デバイスが PNP ポータルに到達できる場合は、『Cisco Plug and Play Support Guide for Cisco Catalyst SD-WAN Products』を参照してください。
- デバイスが PNP ポータルにアクセスできない場合は、「Cisco Catalyst SD-WAN Overlay Network Bring-Up Process」の章の「Start the Enterprise ZTP Server」および「Prepare Routers for ZTP」を参照してください。

（注） デバイスが返品許可（RMA）の期限に達している場合、デバイスの詳細は Cisco PNP にあります。ただし、これらのデバイスを Cisco SD-WAN Manager の RMA リストから削除することはできません。代わりに、Cisco SD-WAN Manager 管理者は、RMA に従って、返品されたデバイスを無効としてマークできます。

Cisco IOS XE リリース 17.2 以降については、「Install and Upgrade Cisco IOS XE Release 17.2 and Later」を参照してください。

ROMMON のアップグレードまたはダウングレード

ここでは、デバイスで実行されている ROM モニタ（ROMmon）のバージョンをアップグレードまたはダウングレードする方法について説明します。ROMmon のバージョンを、「はじめる前に」に示されている必要なバージョンに変更する必要がある場合は、この手順を実行します。

デバイスで実行されている ROMmon のバージョンを判別するには、次のコマンドを入力します。

```
Device# Show rom-monitor R0
```

ROMmon をアップグレードまたはダウングレードするには、次の手順を実行します。

1. 次のいずれかの操作を実行します。
    1. SCP、FTP、TFTP、USB ドライブなどの方法を使用して、ROMmon ファイルをデバイスのブートフラッシュにロードします。

2. ルータへのアウトオブバンド管理アクセスがない場合は、次の例のように、Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送します。

```
vManage# request execute vpn 0 scp -P 830 C1100-rommon-16-1r-SPA.pkg
admin@router-ip-address:/bootflash/vmanage-admin/C1100-rommon-169-1r-SPA.pkg
```

2. 次のいずれかのアクションを実行して、ロードまたは転送した ROMmon ファイルがディレクトリ出力に表示されることを確認します。

   1. ROMmon ファイルをデバイスのブートフラッシュにロードした場合は、次のコマンドを入力します。

```
Device# dir bootflash
```

   2. Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送した場合は、次のコマンドを入力します。

```
vManage# dir bootflash:vmanage-admin
```

3. 次のコマンドを入力して config-register を 0x2102 に設定します。

```
Device# config-register 0x2102
```

4. 次の例のように、upgrade コマンドを使用して、デバイスの ROMmon ファイルをアップグレード（またはダウングレード）します。

   - ROMmon ファイルをデバイスのブートフラッシュにロードした場合の upgrade コマンドの例：

```
Device# upgrade rom-monitor filename bootflash: C1100-rommon-169-1r-SPA.pkg R0
```

   - Cisco SD-WAN Manager CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
vManage# upgrade rom-monitor filename
bootflash:vmanage-admin/C1100-rommon-169-1r-SPA.pkg R0
```

5. アップグレードに関する一連のメッセージが表示され、ルータのプロンプトが表示されたら、次のコマンドを入力してルータをリロードします。

```
Device# Reload
```

6. 次のコマンドを入力して、出力に ROMmon の新しいバージョンが表示されていることを確認します。

```
ISR4K# Show rom-monitor R0
```

工場出荷時の状態へのリセット

このセクションでは、工場出荷時設定へのリセット機能と、この機能を使用してルータを保護状態、または以前の完全に機能する状態に復元する方法について説明します。さまざまなプラットフォームでの工場出荷時設定へのリセット手順については、次を参照してください。

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ

- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco Cloud Services Router 1000V シリーズ

（注） Cisco IOS XE Catalyst SD-WAN ASR 1000 ルータで工場出荷時設定のリセットを実行するには、ルータがサブパッケージモードで起動されていることを確認してください。**show version** コマンドを実行し、システムイメージファイルの出力を確認して、起動されたイメージを特定します。

```
Device# show version
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20200303_002119_V17_X_X_XX
Cisco IOS Software [Amsterdam], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 03-Mar-20 00:29 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

2KP-CEDGE uptime is 3 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:packages.conf"
```

デフォルトパスワードの復元

Cisco IOS XE Catalyst SD-WAN デバイス のデフォルトのパスワードは admin です。このパスワードを初めて使用した後、管理者は新しいパスワードを作成する必要があります。初期構成セッションがタイムアウトになったか、新しいパスワードが作成される前にセッションが中断または終了した場合、以降のログイン試行は失敗します。この場合、デフォルトパスワードを復元する必要があります。

デバイスのデフォルトパスワードを復元するには、次の手順を実行します。

1. デバイスの電源を切り、入れなおします。
2. デバイスのローカルコンソールで、ROMMON モードを開始します。
3. 次のコマンドを入力して、config-register 値を 0x8000 に設定します。

   ```
   rommon 1 > confreg 0x8000
   ```

4. デバイスの電源を切り、入れなおすことによって、更新を有効にします。
5. ユーザー名とパスワードとして「**admin**」を使用してデバイスにログインします。

6. デバイスのローカルコンソールで、SD-WAN 構成モードを開始します。
7. 次のコマンドを入力して、config-register 値を 0x2102 に設定します。

```
Device# confreg 0x2102
```

8. デバイスのローカルコンソールで、特権 EXEC モードを開始します。
9. 次のいずれかの操作を実行します。
   - リリース 16.10.4 以降の Cisco IOS XE SD-WAN 16.10 リリース、またはリリース 16.12.2 以降の Cisco IOS XE SD-WAN 16.12 リリースの場合：

     ```
     Device# request platform software sdwan config reset
     Device# reload
     ```

   - リリース 16.10.4 より前の Cisco IOS XE SD-WAN 16.10 リリース、または 16.12.2 より前の Cisco IOS XE SD-WAN 16.12 リリースの場合：

     ```
     Device# request platform software sdwan software reset
     ```

10. デバイスが起動したら、新しい管理者パスワードを設定します。

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

この記事では、すべての Cisco vEdge デバイス（Cisco SD-WAN Manager インスタンス、Cisco Catalyst SD-WAN 制御コンポーネント、Cisco SD-WAN Validator、および vEdge ルータ）にソフトウェアをインストールする方法と、Cisco Catalyst SD-WAN ソフトウェアをすでに実行しているデバイスでソフトウェアをアップグレードする方法について説明します。

ソフトウェアイメージの署名

Cisco Catalyst SD-WAN ソフトウェアイメージはデジタル署名されており、そのイメージが正式な Cisco Catalyst SD-WAN イメージであること、およびイメージが作成および署名されてからコードが変更または破損していないことが保証されます。標準の Cisco Catalyst SD-WAN ソフトウェアイメージはすべて署名されていますが、パッチイメージは署名されていません。標準ソフトウェアイメージは3つの数値フィールド（16.1.0 など）で識別され、パッチソフトウェアイメージは 4 つの数値フィールド（16.1.0.1 など）で識別されます。

署名されたイメージには失効メカニズムが含まれているため、バグまたはセキュリティ上の欠陥により危険であることが判明したイメージは、Cisco Catalyst SD-WAN が取り消すことができます。既知の脆弱性が存在する以前に署名されたイメージをインストールしようとすると、失効メカニズムにより攻撃から保護されます。

署名されたイメージを Cisco Catalyst SD-WAN デバイスにインストールすると、署名されていないイメージをデバイスにインストールできなくなります。

ソフトウェアイメージの署名は、リリース 16.1 以降で使用できます。

ソフトウェアバージョンの互換性

コントローラデバイス（Cisco SD-WAN Manager インスタンス、Cisco SD-WAN コントローラ、および Cisco SD-WAN Validator ）のソフトウェアバージョンを、vEdge ルータを同じバージョンにアップグレードすることなく、アップグレードできます。ただし、コントローラデバイスで実行されているソフトウェアバージョンは、vEdge ルータで実行されているバージョンと互換性がある必要があります。

コントローラと vEdge ルータの互換性のあるバージョンのリストについては、リリースノートを参照してください。

（注） 同じタイプのすべてのコントローラデバイスは、同じソフトウェアバージョンを実行する必要があります。つまり、すべての Cisco SD-WAN Manager インスタンスで同じソフトウェアバージョンを実行し、すべての Cisco SD-WAN コントローラ で同じソフトウェアバージョンを実行し、すべての Cisco SD-WAN Validator で同じバージョンを実行する必要があります。

ソフトウェアのインストール

開始する前に、Cisco Catalyst SD-WAN サポートサイトからソフトウェアをダウンロードします。

最初にオーバーレイネットワークを起動するときに Cisco Catalyst SD-WAN デバイスにソフトウェアをインストールし、それらのデバイスをネットワークに追加します。

- Cisco SD-WAN Validator にソフトウェアをインストールするには、「ESXi での Cisco SD-WAN Validator VM インスタンスの作成」または「KVM での Cisco Catalyst SD-WAN Validator VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vBond.ova ファイルをインストールします。
- vEdge Cloud ルータにソフトウェアをインストールするには、「AWS での vEdge クラウド VM インスタンスの作成」、「ESXi での vEdge クラウド VM インスタンスの作成」、または「KVM での vEdge クラウド VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vEdge Cloud.ova ファイルをインストールします。
- Cisco SD-WAN Manager にソフトウェアをインストールするには、「ESXi での Cisco SD-WAN Manager VM インスタンスの作成」または「KVM での Cisco SD-WAN Manager インスタンスの作成」を参照してください。VM の作成プロセス中に、vManage.ova ファイルをインストールします。
- Cisco Catalyst SD-WAN コントローラ にソフトウェアをインストールするには、「ESXi での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成」または「KVM での Cisco Catalyst SD-WAN コントローラ VM インスタンスの作成」を参照してください。VM の作成プロセス中に、vSmart.ova ファイルをインストールします。

- ハードウェアvEdgeルータにソフトウェアをインストールするために必要なものは特にありません。すべてのvEdgeハードウェアルータは、ソフトウェアがすでにインストールされた状態で出荷されます。

ソフトウェアのアップグレード

Cisco SD-WAN Manager からオーバーレイネットワーク内にある Cisco vEdge デバイス で実行中のソフトウェアイメージをアップグレードし、新しいソフトウェアで再起動できます。これは、1つのデバイスに対して行うことも、複数のデバイスに対して同時に行うこともできます。

ソフトウェアをアップグレードするには、Cisco Catalyst SD-WAN からソフトウェアイメージを取得し、新しいソフトウェアイメージを Cisco SD-WAN Manager またはリモートサーバーにあるリポジトリに追加して、新しいソフトウェアイメージをデバイスにインストールします。[Activate and Reboot] チェックボックスをオンにすると、次の再起動がすぐに実行されます。また、次の定期的にスケジュールされているメンテナンス期間まで待つこともできます。アップグレードが失敗し、デバイスが再起動しない場合、Cisco SD-WAN Manager はデバイスを以前実行されていたソフトウェアイメージに自動的に戻します。

Cisco vEdgeデバイスのソフトウェアをアップグレードする前に、デバイスで必要なソフトウェアバージョンが実行されていることを確認します。

（注） Cisco Catalyst SD-WAN リリース 18.4.5、19.2.2、および 20.1.1 以降のリリースには、セキュリティロックアウト機能があります。これらのソフトウェアバージョン（または以降のバージョン）がデバイスにインストールされ、アクティブ化されると、デバイスにインストールされている古いイメージを削除するために30日間のタイマーが設定されます。タイマーが切れると、古いイメージは削除されます。たとえば、リリース18.4.5をインストールしてアクティブ化すると、以前にインストールされたリリース 19.2.1 イメージで 30 日間のタイマーが開始されますが、リリース 19.2.2 では開始されません。同様に、リリース 19.2.2 をインストールしてアクティブ化すると、以前にインストールされたリリース 18.4.4 イメージで 30 日間のタイマーが開始されますが、リリース 18.4.5 では開始されません。

30日間のタイマーが切れる前は、インストール済みの古いイメージを引き続きアクティブ化できます。30日間のタイマーが切れる前にデバイスが再起動すると、タイマーはリセットされます。

詳細については、『Cisco Catalyst SD-WAN Command Reference』ガイドを参照してください。

- **request software secure-boot set**：30 日間待たずに、古いイメージ* がすぐに削除されます。
- **request software secure-boot status**：インストールされている古いイメージを表示します*。
- **request software secure-boot list**：インストールされているすべての古いイメージ* のリストを出力します。

*古いイメージ＝リリース 18.4.5、19.2.2、および 20.1.1 より前のイメージ

（注） Cisco SD-WAN Manager のダウングレードはサポートされていません。Cisco SD-WAN Manager をアップグレードする前に、VMのスナップショットを作成してください。以前のCisco SD-WAN Manager リリースにロールバックするには、スナップショットに戻します。

ソフトウェアアップグレードに関する追加情報と注意事項については、リリースノートを参照してください。

ソフトウェアアップグレードのベストプラクティス

- CLI ではなく Cisco SD-WAN Manager から、ソフトウェアをアップグレードします。
- リモート Cisco SD-WAN Manager のソフトウェアイメージをアップグレードする場合は、オーバーレイネットワークがすでに稼働している必要があります。
- オーバーレイネットワーク内のすべてのデバイスをアップグレードする場合は、次の順序でアップグレードを実行する必要があります。

1. Cisco SD-WAN Manager インスタンスをアップグレードします。
2. Cisco SD-WAN Validator をアップグレードします。
3. 半分の Cisco SD-WAN コントローラ をアップグレードします。
4. アップグレードされた Cisco SD-WAN コントローラ を少なくとも 1 日（24 時間）動作させ、Cisco vEdge デバイス とオーバーレイネットワークが安定して期待どおりに動作していることを確認します。
5. 残りの Cisco SD-WAN コントローラ をアップグレードします。
6. 10% の vEdge ルータをアップグレードします。マルチルータサイトの場合、サイトごとに 1 つのルータのみをアップグレードすることをお勧めします。
7. アップグレードされた vEdge ルータを少なくとも 1 日（24 時間）動作させ、Cisco Catalyst SD-WAN デバイスとオーバーレイネットワークが安定して期待どおりに動作していることを確認します。
8. 残りの vEdge ルータをアップグレードします。

（注） Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.13.1 以降、Cisco vEdge デバイス の場合、Datagram Transport Layer Security（DTLS）の制御セッションレートは、アップグレード中のみ4000 pps に増加し、アップグレードの完了後に元の値にリセットされます。

- 新しいソフトウェアイメージがFTPサーバーにある場合は、FTPサーバーが同時ファイル転送を処理できることを確認してください。
- 新しいソフトウェアイメージが Cisco SD-WAN Manager のイメージリポジトリにある場合は、Cisco SD-WAN Manager が配置されている WAN に同時ファイル転送に十分なキャパシティがあることを確認してください。
- グループのソフトウェアアップグレード処理に Cisco SD-WAN Manager を含めることはできません。Cisco SD-WAN Manager サーバーを単体でアップグレードして再起動する必要があります。
- グループ ソフトウェア アップグレード操作では、最大 40 の Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス をアップグレードし、最大 100 の Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス を同時に再起動またはアクティブ化することができます（新しいイメージがローカルで使用可能な場合）。これらの最大数は、Cisco SD-WAN Manager がアイドル状態であり、アップグレードおよび再起動操作のみが実行されていることを前提としています。Cisco SD-WAN Manager で他の管理タスクが同時に発生すると、使用可能なセッションの数が減少します。
- ソフトウェアイメージをデフォルトのソフトウェアイメージに設定する場合は、最初にそれをアクティブにしてから、デフォルトのイメージにします。

Cisco Catalyst SD-WAN からのソフトウェアイメージの取得

オーバーレイネットワークのデバイスで実行されているソフトウェアをアップグレードするには、最初に Cisco Catalyst SD-WAN Web サイトから新しいソフトウェアパッケージを取得する必要があります。パッケージを取得するには、http://www.cisco.com/go/support にアクセスし、Cisco Catalyst SD-WAN Support にログインして、新しいリリースのソフトウェアパッケージをダウンロードします。ソフトウェアイメージをネットワーク内のFTPサーバーにダウンロードし、Cisco SD-WAN Manager からリモートホスト上のアップグレードパッケージを指定することもできます。

ソフトウェアの初期インストールの場合、リリース16.1以降のソフトウェアパッケージ名は次の形式になります。x.x.x は Cisco Catalyst SD-WAN ソフトウェア リリース バージョンを表します。各パッケージには、仮想マシンと Cisco Catalyst SD-WAN ソフトウェアが含まれています。

- vEdge Cloud ルータ
  - viptela-x.x.x-edge-genericx86-64.ova（ESXi ハイパーバイザ用）
  - viptela-edge-genericx86-64.qcow2（KVM ハイパーバイザ用）
- Cisco SD-WAN Validator
  - viptela-edge-genericx86-64.ova（ESXi ハイパーバイザ用）
  - viptela-edge-genericx86-64.qcow2（KVM ハイパーバイザ用）

- Cisco Catalyst SD-WAN コントローラ
  - viptela-smart-genericx86-64.ova（ESXi ハイパーバイザ用）
  - viptela-smart-genericx86-64.qcow2（KVM ハイパーバイザ用）
- Cisco SD-WAN Manager
  - viptela-vmanage-genericx86-64.ova（ESXi ハイパーバイザ用）
  - viptela-vmanage-genericx86-64.qcow2（KVM ハイパーバイザ用）

リリース 16.1 以降のソフトウェア アップグレード パッケージ名は次の形式になります。x.x.x はリリースバージョンを表します。文字列 mips64 および x86_64 は、基になるチップアーキテクチャを表します。

- vEdge ルータハードウェア：viptela-x.x.x-mips64.tar.gz
- Cisco SD-WAN Validator、vEdge Cloud ルータ、および Cisco Catalyst SD-WAN コントローラ：viptela-x.x.x-x86_64.tar.gz
- Cisco SD-WAN Manager：vmanage-x.x.x-x86_64.tar.gz

リリース 15.4 以前の場合、ソフトウェア アップグレード パッケージは、拡張子が .tar.bz2 のファイルにあります。vEdge 100 ルータの場合は .tar.gz です。パッケージ名の形式は次のとおりです。x.x.x はリリースバージョンを表します。文字列 mips64 および x86_64 は、基になるチップアーキテクチャを表します。

- vEdge ルータ：viptela-x.x.x-mips64.tar.bz2
- Cisco SD-WAN Validator および Cisco Catalyst SD-WAN コントローラ：viptela-x.x.x-x86_64.tar.bz2
- Cisco SD-WAN Manager：vmanage-x.x.x-x86_64.tar.bz2

リポジトリへの新しいソフトウェアイメージの追加

Cisco Catalyst SD-WAN Web サイトから新しいソフトウェアパッケージをダウンロードしたら、Cisco SD-WAN Manager リポジトリにアップロードします。ソフトウェアイメージを FTP サーバーにダウンロードした場合は、Cisco SD-WAN Manager からリモートホスト上のアップグレードパッケージを指定します。

1. [Cisco SD-WAN Manager] メニューから、**[Maintenance]** > **[Software Repository]**の順に選択します。
2.
3. [Add New Software] をクリックし、ソフトウェアイメージをダウンロードする場所を選択します。場所は次のとおりです。
   - Cisco SD-WAN Manager：ローカル Cisco SD-WAN Manager に保存するイメージを選択する場合。

- Remote Server（推奨）：リモートファイルサーバーに保存されているイメージを選択する場合。
- Remote Server – Cisco SD-WAN Manager：リモート Cisco SD-WAN Manager に保存されているイメージを選択する場合。この場所は、リリース 17.2 以降で使用できます。

4. Cisco SD-WAN Manager を選択すると、[Upload Software to Cisco SD-WAN Manager] ダイアログボックスが開きます。
   1. [Browse] をクリックしてソフトウェアイメージを選択するか、vEdge ルータ、Cisco SD-WAN コントローラ、または Cisco SD-WAN Manager のイメージをドラッグアンドドロップします。
   2. [Upload] をクリックして、イメージを Cisco SD-WAN Manager リポジトリに追加します。
5. [Remote Server] を選択すると、[Location of Software on Remote Server] ダイアログボックスが開きます。
   1. ソフトウェアイメージのバージョン番号を入力します。
   2. イメージが存在する FTP または HTTP サーバーの URL を入力します。
   3. [OK] をクリックして、リモートホスト上のソフトウェアイメージを指定します。
6. [Remote Server – Cisco SD-WAN Manager] を選択すると、[Upload Software to Cisco SD-WAN Manager] ダイアログボックスが開きます。
   1. Cisco SD-WAN Manager サーバーのホスト名を入力します。
   2. [Browse] をクリックしてソフトウェアイメージを選択するか、vEdge ルータ、Cisco SD-WAN コントローラ、または Cisco SD-WAN Manager のソフトウェアイメージをドラッグアンドドロップします。
   3. [Upload] をクリックして、イメージを Cisco SD-WAN Manager リポジトリに追加します。

追加されたソフトウェアイメージは Cisco SD-WAN Manager リポジトリテーブルに一覧表示され、デバイスにインストールできるようになります。テーブルには、イメージの名前とタイプ、更新日時、および URL が表示されます。

リストに追加されたソフトウェアバージョンを削除するには、目的のソフトウェアバージョンで [...] をクリックし、[Delete] を選択します。

ソフトウェアイメージのアップグレード

ソフトウェアイメージが Cisco SD-WAN Manager イメージリポジトリに存在している場合、デバイスにソフトウェアイメージをアップロードできます。

1. Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。
2. チェックボックスをクリックして、ソフトウェアイメージをアップグレードする 1 つ以上のデバイスを選択します。デバイスを検索するには、[Device Groups] ドロップダウンや検索ボックスを使用します。
3. [Upgrade] をクリックすると、[Software Upgrade] ダイアログボックスが開きます。
4. [Version] ドロップダウンから、インストールするソフトウェアイメージのバージョンを選択します。Cisco SD-WAN Manager とリモートサーバーがアクティブ化されます。
5. ソフトウェアイメージが Cisco SD-WAN Manager またはリモートサーバー上で使用可能かどうかを選択します。
6. ステップ 5 でリモートサーバーを選択した場合は、Cisco Catalyst SD-WAN コントローラ/Cisco SD-WAN Manager および vEdge に適切な VPN を選択し、ステップ 8 に進みます。
7. ステップ 5 で Cisco SD-WAN Manager を選択した場合は、[Activate and Reboot] チェックボックスをオンにして、新しいソフトウェアイメージを自動的にアクティブ化し、デバイスを再起動できます。（[Activate and Reboot] チェックボックスをオンにしない場合でも、新しいソフトウェアイメージはインストールされますが、デバイスでは既存のソフトウェアイメージが引き続き使用されることに注意してください。新しくインストールされたソフトウェアイメージをアクティブ化するには、以下の「新しいソフトウェアイメージのアクティブ化」を参照してください）。
8. [Upgrade] をクリックします。プログレスバーにソフトウェアアップグレードのステータスが示されます。

アップグレードが 60 分以内に正常に完了しない場合、タイムアウトになります。

Cisco SD-WAN Manager への制御接続が 15 以内に確立されなかった場合、Cisco SD-WAN Manager はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。

新しいソフトウェアイメージのアクティブ化

ソフトウェアイメージのアップロード時に [Activate and Reboot] チェックボックスをオンにする場合、[Upgrade] をクリックすると、新しいソフトウェアが自動的にアクティブになり、デバイスが再起動します。

リモートサーバーからソフトウェアイメージをアップロードした場合、または Cisco SD-WAN Manager からのソフトウェアイメージのアップロード時に [Activate and Reboot] チェックボックスをオンにしなかった場合、新しいイメージはデバイスにインストールされますが、デバイスは引き続き既存のソフトウェアイメージを使用します。新しいソフトウェアイメージをアクティブにするには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから**[Maintenance]** > **[Software Upgrade]**の順に選択します。

2. チェックボックスをクリックして、新しいソフトウェアイメージをアクティブにする 1 つ以上のデバイスを選択します。デバイスを検索するには、[Device Groups] ドロップダウンや検索ボックスを使用します。
3. [Activate] をクリックして新しいソフトウェアをアクティブにします。アクティブ化プロセスにより、デバイスが再起動され、新しくインストールされたソフトウェアにアップグレードされます。

デバイスと Cisco SD-WAN Manager の制御接続が 15 分以内に確立されなかった場合、Cisco SD-WAN Manager はデバイスを以前に実行されていたソフトウェアイメージに自動的に戻します。

ソフトウェア アップグレード アクティビティ ログの表示

各デバイスのソフトウェアアップグレードのステータスと、関連するアクティビティのログを表示するには、次の手順を実行します。

1.
2.

CLI からのソフトウェアイメージのアップグレード

デバイス上でソフトウェアイメージを直接アップグレードする必要がある場合、またはネットワークで Cisco SD-WAN Manager を使用していない場合は、ソフトウェアイメージをアップグレードするために、インストールプロセスを繰り返すか、CLI 内からソフトウェアイメージをインストールできます。

CLI 内からソフトウェアイメージをアップグレードするには、次の手順を実行します。

1. ソフトウェアのアップグレードが成功したことを確認するための制限時間を設定します。時間の範囲は 1 ～ 60 分です。

```
Device# system upgrade-confirmminutes
```

2. ソフトウェアをインストールします。

```
vEdge# request software install  url
/viptela- release -mips64.tar.bz2 [reboot] [vpn vpn-id]


vSmart# request software install url/viptela- release
-x86 _64.tar.bz2 [reboot] [vpn vpn-id]
```

次のいずれかの方法でイメージの場所を指定します。

- イメージファイルがローカルサーバー上にある場合：

  /*directory-path*/

  CLI のオートコンプリート機能を使用して、パスとファイル名を完成させることができます。

- イメージファイルが FTP サーバー上にある場合：

ftp://*hostname*/

- イメージファイルが HTTP サーバー上にある場合：

  http://*hostname*/

- イメージファイルが TFTP サーバー上にある場合：

  tftp://*hostname*/

必要に応じて、サーバーが配置されている VPN の識別子を指定します。

[reboot] オプションは、新しいソフトウェアイメージをアクティブにして、インストールの完了後にデバイスを再起動します。

3. ステップ 2 で [reboot] オプションを含めなかった場合は、新しいソフトウェアイメージをアクティブにして、デバイスを再起動します。

   ```
   Viptela# request software activate
   ```

4. アップグレード確認のための設定した制限時間内にソフトウェアアップグレードが成功したことを確認します。

   ```
   Viptela# request software upgrade-confirm
   ```

   この制限時間内にこのコマンドを発行しないと、デバイスは自動的に以前のソフトウェアイメージに戻ります。

冗長ソフトウェアイメージ

Cisco vEdge デバイスに複数のソフトウェアイメージをダウンロードして保存できます。

現在インストールされているソフトウェアバージョンを一覧表示し、現在実行されているソフトウェアイメージを確認するには、次のコマンドを使用します。

```
Viptela# show software
VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
15.4.3    true    false    false     user       2016-02-04T03:45:13-00:00
15.4.2    false   true     true      user       2015-12-06T14:01:12-00:00
```

ソフトウェアを特定のバージョンにアップグレードするには、次のコマンドを使用します。

```
Viptela# request software activate
```

CiscovEdgeデバイスの古いソフトウェアイメージへのダウングレード

CLI を使用して Cisco vEdge デバイス を以前のソフトウェアイメージにダウングレードするには、次の手順を実行します。

1. 必要に応じて、既存のソフトウェアイメージを削除して、新しいソフトウェアイメージをロードするための領域を用意します。

   ```
   vEdge# request software remove  previous-installed-build
   ```

2. ダウングレード用のソフトウェアイメージをダウンロードします。

3. ダウンロードしたイメージをインストールします。

```
vEdge# request software install desired-build
```

インストールする前にイメージをローカルストレージにコピーすることをお勧めしますが、次のいずれかの方法でイメージの場所を指定できます。

- イメージファイルがローカルサーバー上にある場合：

  /*directory-path*/

  CLI のオートコンプリート機能を使用して、パスとファイル名を完成させることができます。

- イメージファイルが FTP サーバー上にある場合：

  ftp://*hostname*/

- イメージファイルが HTTP サーバー上にある場合：

  http://*hostname*/

- イメージファイルが TFTP サーバー上にある場合：

  tftp://*hostname*/

4. インストールしたイメージをデフォルトとして設定します。

```
vEdge# request software set-default desired-build
```

5. リセットを実行します。これにより、デバイスがリセットされ、既存の構成が削除されます。デバイスはゼロデイ構成で起動します。

```
vEdge# request software reset
```

Cisco Catalyst SD-WAN Manager をホストしている仮想マシンでのメモリおよび vCPU リソースのアップグレード

次の手順を実行して、Cisco SD-WAN Manager をホストする仮想マシン（VM）上のメモリと仮想中央処理装置（vCPU）のリソースをアップグレードします。

（注） メモリまたは vCPU の増加のみが許可されます。メモリまたは vCPU をアップグレードした後にダウングレードすることはできません。

1. コマンド **show system status** を使用して、Cisco SD-WAN Manager の現在の設定を確認します。

```
vManage#show system status

Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
```

```
Version: 20.7.0-185
Build: 185


System logging to host  is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Enabled
Testbed mode:            Enabled
Engineering Signed:      True

Last reboot:             Initiated by user.
CPU-reported reboot:     Not Applicable
Boot loader version:     Not applicable
System uptime:           1 days 02 hrs 44 min 52 sec
Current time:            Sat Oct 23 22:12:10 UTC 2021

Load average:            1 minute: 14.58, 5 minutes: 12.31, 15 minutes: 10.73
Processes:               5775 total
CPU allocation:          32 total
CPU states:              31.58% user,   4.36% system,   64.06% idle
Memory usage:            65741448K total,    38096172K used,   490324K free
                         4606444K buffers,  22548508K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       15230M  3496M  10898M   24%   /
vManage storage usage:   Filesystem      Size  Used  Avail  Use%  Mounted on
                        /dev/sdb        502942M  206906M  270435M   41%   /opt/data

Personality:             vmanage
Model name:              vmanage
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Chassis serial number:   None
```

2. メモリをアップグレードするには、デバイスの電源を切ります。
3. ホスティング プラットフォームのガイドラインを使用して、VM の CPU とメモリをアップグレードします。次のアップグレードを行うことができます。

リソース	現在	アップグレード
vCPU	16	32
メモリ	32 G	64 G または 128 G
メモリ	64 G	128 G

4. デバイスの電源を入れ、メモリと CPU を確認します。

```
vManage1# show system status

Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-139
```

```
Build: 139


System logging to host  is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Enabled
Testbed mode:            Enabled
Engineering Signed:      True

Last reboot:             Initiated by user - activate 20.7.0-139.
CPU-reported reboot:     Not Applicable
Boot loader version:     Not applicable
System uptime:           16 days 17 hrs 43 min 28 sec
Current time:            Sat Oct 23 22:22:16 UTC 2021

Load average:            1 minute: 15.86, 5 minutes: 13.02, 15 minutes: 11.45
Processes:               6067 total
CPU allocation:          32 total
CPU states:              32.13% user,   4.34% system,   63.53% idle
Memory usage:            131703148K total,    88221488K used,   19285636K free
                         7022488K buffers,  17173536K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       15998M  10702M  4461M   71%   /
vManage storage usage:   Filesystem      Size  Used  Avail  Use%  Mounted on
                        /dev/sdb       10402115M  702212M  9175615M   6%   /opt/data

Personality:             vmanage
Model name:              vmanage
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Chassis serial number:   None
```

ディスクサイズの拡張

Cisco SD-WAN Manager のディスクサイズを増やすには、次の手順を実行します。

1. クラスタ内のすべての Cisco SD-WAN Manager インスタンスでデバイスの電源をオフにします。

   ```
   request nms all stop
   ```

2. Cisco SD-WAN Manager VM の電源をオフにします。
3. Cisco SD-WAN Manager VM をホストしているハイパーバイザシステムに適したツールを使用して、データ ディスク パーティションとして使用されるセカンダリパーティションのサイズを増やします。
4. Cisco SD-WAN Manager VM を起動します。
5. デバイスの電源を切ります。

   ```
   request nms all stop
   ```

6. 次のコマンドを使用して、新しいディスクサイズを使用するように Cisco SD-WAN Manager を再設定します。

```
request nms application-server resize-data-partition
```

パーティションのサイズ変更が完了するには、多少の時間がかかります。

7. 次の vshell コマンドを使用して、/opt/data ディスクのサイズが変更されたことを確認します。

```
vshell

df -hk | grep data
```

8. デバイスを再起動します。

クラスタのアップグレードプロセスの詳細については、『Cisco Catalyst SD-WAN Manager Cluster Creation and Troubleshooting guide』を参照してください。

Cisco IOS XE Catalyst SD-WAN デバイス のソフトウェア メンテナンス アップグレード

表 *8:* 機能の履歴

機能名	リリース情報	説明
ソフトウェア メンテナンス アップグレード パッケージのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、Cisco IOS XE Catalyst SD-WAN デバイス にインストール可能なソフトウェア メンテナンス アップグレード（SMU）パッケージのサポートが有効になります。SMU パッケージにより、リリース済みの Cisco IOS XE イメージにパッチ修正やセキュリティの解決策が提供されます。デベロッパーは、次のリリースで修正が利用可能になるのを待たずに、報告された問題の修正を提供するこのパッケージをビルドできます。
Cisco ISR1100 および ISR1100X シリーズ ルータの SMU サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	Cisco ISR 1100 および ISR 1100X シリーズ サービス統合型ルータ に対するサポートが追加されました。

ソフトウェア メンテナンス アップグレードについて

ソフトウェア メンテナンス アップグレード（SMU）は、リリースされたソフトウェアの重大なバグに対するポイントフィックスであり、可能な場合、ルータの中断が最小限に抑えられます。SMU は、メンテナンスリリースを置き換えるようには設計されていません。

シスコは、SMU の修正をパッケージファイル（Cisco Catalyst SD-WAN の各リリースと各コンポーネントのファイル）として提供します。パッケージには、パッケージの内容を記述するメタデータ、および報告済みの問題の修正が含まれています。

SMU イメージファイル

ソフトウェアリポジトリの各 SMU イメージファイル名には、基本イメージバージョンと修正に関連する欠陥 ID が含まれています。イメージ名の内容：

- base_image_version は、Cisco IOS XE イメージのバージョンです。
- defect_id は、SMU パッケージに修正がある欠陥の識別子です。

SMU タイプ

SMU タイプは、Cisco IOS XE Catalyst SD-WAN デバイス にインストールされた SMU パッケージの影響を表します。SMU パッケージのタイプは次のとおりです。

- ホット SMU（リロードなし）：SMU イメージのアクティブ化後に、Cisco IOS XE Catalyst SD-WAN デバイス を再起動（リロード）せずに SMU パッケージを有効にします。
- コールド SMU（リロードあり）：Cisco IOS XE Catalyst SD-WAN デバイス の再起動（リロード）後に SMU パッケージを有効にします。

ソフトウェア メンテナンス アップグレードを使用する利点

- ネットワークの問題に迅速に対応でき、テストに必要な時間と範囲も削減できます。Cisco IOS XE Catalyst SD-WAN デバイス では SMU イメージの互換性が内部的に検証されるため、互換性のない SMU パッケージはインストールできません。
- デバイスに一度に 1 つの SMU パッケージのみをインストールまたはアクティブ化して、初期実装プロセスを簡素化できます。
- Cisco SD-WAN Manager を使用してインストールするときに、同時に複数の Cisco IOS XE Catalyst SD-WAN デバイス に SMU パッケージをインストールできます。CLI を使用して複数のデバイスにSMUパッケージをインストールするには、複数のデバイスでインストールプロセスを繰り返します。

ソフトウェア メンテナンス アップグレードでサポートされるデバイス

リリース	サポートされるデバイス数
Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降	• Cisco ISR 1000 シリーズ サービス統合型ルータ • Cisco IR1101 耐環境性能 サービス統合型ルータ • Cisco ISR 4000 シリーズ サービス統合型ルータ • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco Catalyst 8500L シリーズ エッジ プラットフォーム • Cisco Catalyst 8000v シリーズ エッジプラットフォーム
Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降	Cisco ISR 1100 および ISR 1100X シリーズ サービス統合型ルータ

ソフトウェア メンテナンス アップグレード イメージの管理

SMU イメージの追加、アップグレードとアクティブ化、または非アクティブ化と削除には、Cisco SD-WAN Manager を使用します。

（注） SMU イメージをアクティブ化または非アクティブ化すると、SMU イメージによってはデバイスが再起動する場合があります。非リロード SMU タイプではデバイスの再起動はトリガーされず、リロード SMU タイプではデバイスの再起動がトリガーされます。

SMU イメージの追加、表示、およびアクティブ化

1. Cisco SD-WAN Manager ソフトウェアリポジトリを使用して SMU イメージを追加します。

   『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager「Add Software Images to Repository」手順を参照してください。

2. Cisco SD-WAN Manager ソフトウェアリポジトリを使用して SMU イメージを表示します。

   『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager「View Software Images」手順を参照してください。SMU イメージを表示するときは、次の点に注意してください。

   • [Available SMU Versions] 列には、現在の基本イメージバージョン（Cisco IOS XE イメージバージョン）で使用できる SMU イメージの数が表示されます。

- [Available SMU Versions] 列で目的のエントリをクリックして、その SMU イメージに関連付けられている欠陥を表示します。[Available SMU Versions] ダイアログボックスで、欠陥 ID、対応する SMU バージョン、および SMU タイプ（非リロードまたはリロードなど）を確認できます。
- [Available SMU Versions] ダイアログボックスで、SMU バージョンの横にある削除アイコンをクリックして、その SMU バージョンを削除します。

3. [Cisco SD-WAN Manager Software Upgrade] ウィンドウを使用して、デバイスの SMU イメージをアップグレードします。

   『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager「Upgrade the Software Image on a Device」手順を参照してください。アップグレード対象として選択する SMU イメージについて、次の点に注意してください。

   - デバイステーブルの [Available SMUs] 列には、現在の基本イメージバージョンで使用可能な SMU イメージの数が表示されます。
   - [Available SMUs] 列の下にある目的のエントリをクリックして、利用可能なすべての SMUバージョンとデバイスのアップグレードイメージのリストを表示します。[Available SMUs]ダイアログボックスで、SMUバージョン、SMUタイプ、およびSMUバージョンの状態を確認できます。

     SMU バージョンの形式は base_image_version.cdet_id です。
   - [Upgrade] ダイアログボックスで、必要に応じて [Activate and Reboot] をオンにして、SMU イメージをアクティブ化し、Cisco IOS XE Catalyst SD-WAN デバイス を自動的に再起動します。

     [Activate and Reboot] チェックボックスをオンにすると、Cisco SD-WAN Manager はデバイスに SMU イメージをインストールしてアクティブ化し、SMU タイプに基づいてリロードをトリガーします。『Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide』の Cisco SD-WAN Manager「Activate a Software Image」手順を参照してください。

   SMU イメージのアップグレードが成功すると、Cisco IOS XE Catalyst SD-WAN デバイス は対応する成功メッセージを送信します。

SMU イメージの非アクティブ化または削除

『Cisco Catalyst SD- WAN Monitor and Maintain Configuration Guide』の「Delete a Software Image」手順を使用して、SMUイメージを非アクティブ化し、デバイスからイメージを削除します。

CLI を使用したソフトウェア メンテナンス アップグレード イメージの管理

次の CLI を使用して、SMU イメージのインストール、アップグレードとアクティブ化、または非アクティブ化と削除を行います。

（注） SMUイメージがアクティブ化および非アクティブ化されると、非リロードまたはリロードSMUタイプに基づいてデバイスの再起動がトリガーされる場合があります。非リロード SMU タイプではデバイスの再起動はトリガーされませんが、リロード SMU タイプではデバイスの再起動がトリガーされます。

CLI を使用した SMU イメージのインストールとアクティブ化

1. ファイルサーバーからデバイスのブートフラッシュに SMU イメージをアップロードします。

   copy コマンドを使用して、SMU イメージをアップロードします。copy コマンドの詳細については、「Cisco IOS XE ソフトウェアのインストール」トピックのステップ 2 を参照してください。

2. SMUイメージのアクティブ化が成功したことを確認するための制限時間を設定します（まだ設定されていない場合）。

   制限時間は 1 分から 60 分に設定できます。制限時間は 15 分以上に設定することを推奨します。

   ```
   Device# config-transaction
   Device(config)# system
   Device(config-system)# upgrade-confirm minutes
   ```

3. デバイスのブートフラッシュからSMUイメージをインストールし、デバイスとSMUパッケージバージョンの互換性チェックを実行します。

   ```
   Device# request platform software sdwan smu install file-path
   ```

4. Cisco IOS XE Catalyst SD-WAN デバイス で SMU イメージをアクティブ化します。

   ```
   Device# request platform software sdwan smu activate
   build-number.smu-defect-id
   ```

5. 設定した確認用制限時間内で、SMU イメージのアップグレードを確認します。

   ```
   Device# request platform software sdwan smu upgrade-confirm
   ```

（注） **upgrade-confirm** *minutes* コマンドで指定した制限時間内にデバイスでこのコマンドを発行しないと、デバイスは SMU イメージがアクティブ化される前の状態に自動的に戻ります。

CLI を使用した SMU イメージの非アクティブ化および削除

1. SMU イメージの非アクティブ化が成功したことを確認するための制限時間を設定します（まだ設定されていない場合）。

   制限時間は 1 分から 60 分に設定できます。制限時間は 15 分以上に設定することを推奨します。

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

2. Cisco IOS XE Catalyst SD-WAN デバイス で SMU イメージを非アクティブ化します。

```
Device# request platform software sdwan smu deactivate
build-number.smu-defect-id
```

3. SMU イメージを非アクティブ化できたことを確認します。

```
Device# request platform software sdwan smu upgrade-confirm
```

（注） **upgrade-confirm** *minutes* コマンドで指定した制限時間内にデバイスでこのコマンドを発行しないと、イメージの非アクティブ化は失敗し、デバイスは SMU イメージが非アクティブ化される前の状態に自動的に戻ります。

4. Cisco IOS XE Catalyst SD-WAN デバイス から SMU イメージを削除します。

```
Device# request platform software sdwan smu remove
build-number.smu-defect-id
```

次の例は、SMU イメージ操作を管理するために使用できるコマンドを示しています。

- アップグレードをチェックし、設定を確認します。

```
show sdwan running system
```

- 確認タイマーを追加してアップグレードします。

```
config-transaction
system
upgrade-confirm 15
commit
```

- 実行コマンド：
  - **request platform software sdwan smu install bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin**
  - **request platform software sdwan smu activate 17.09.01a.0.247.CSCvq24042**
  - **request platform software sdwan smu upgrade-confirm**
  - **request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042**
  - **request platform software sdwan smu upgrade-confirm**
  - **request platform software sdwan smu remove 17.09.01a.0.247.CSCvq24042**

ソフトウェア メンテナンス アップグレードイメージのステータスの検証

Cisco SD-WAN Manager または CLI を使用して、SMU イメージのステータスを監視できます。

Cisco SD-WAN Manager を使用した SMU ステータスの監視

1. Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Software Upgrade]** の順に選択します。
2. 目的の Cisco IOS XE Catalyst SD-WAN デバイス について、[Available SMUs] の下にある SMU イメージリンク（ハイパーリンク）をクリックします。

   [Available SMUs] ダイアログボックスで、SMU イメージの状態を確認できます。

現在の基本イメージバージョン（Cisco IOS XE イメージバージョン）で使用できる SMU イメージがない場合、SMU イメージリンクは [Available SMUs] の下で使用できず、Cisco SD-WAN Manager には 0 と表示されます。

CLI を使用した SMU のステータスの確認

例 1：

以下は、SMU イメージをインストールし、アクティブにして、アップグレード（コミット）を確認した後の **show install summary** コマンドの出力例です。

```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247
SMU   I    bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin


--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

この出力は、SMU イメージがブートフラッシュ ファイル システムからインストールされ、アクティブ化されていることを示しています。[Auto abort timer] の値から、SMU イメージのロールバックの残り時間を追跡できます。この値は、自動中止タイマーの期限が切れ、デバイスがロールバックするまでの残り時間を示しています。

例 2：

次の例は、**request platform software sdwan smu deactivate** コマンドを使用して SMU イメージを非アクティブ化した後の出力を示しています。

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
smu_deactivate: START Mon Mar 5 21:54:06 PST 2021
smu_deactivate: Deactivating SMU
Executing pre scripts....
```

```
Executing pre scripts done.
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
  [1] SMU_DEACTIVATE package(s) on switch 1
  [1] Finished SMU_DEACTIVATE on switch 1
Checking status of SMU_DEACTIVATE on [1]
SMU_DEACTIVATE: Passed on [1]
Finished SMU Deactivate operation
SUCCESS: smu_deactivate 17.09.01a.0.247.CSCvq24042
```

この出力には、SMUイメージがデバイスから非アクティブ化されていることが示されています。

以下は、SMU イメージを非アクティブ化した後の **show install summary** コマンドの出力例です。

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------

IMG   C    17.09.01a.0.247
SMU   D    bootflash:
c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 00:04:57
--------------------------------------------------------------------------------
```

次の出力例は、**request platform software sdwan smu upgrade-confirm command** を使用して SMU イメージを非アクティブ化できることを確認した後に SMU イメージを非アクティブ化した出力を示しています。

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042

install_deactivate: START Thu Aug 25 17:47:10 UTC 2022
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
  [1] SMU_DEACTIVATE package(s) on R0
  [1] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation

CSCvq24042:SUCCESS
SUCCESS: install_deactivate /bootflash/c8kv_hot.bin Thu Aug 25 17:47:33 UTC 2022
```

以下は、SMU イメージを削除化した後の **show install summary** コマンドの出力例です。

```
Device# show install summary[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
```

```
IMG   C    17.09.01a.0.247

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

例 3：

以下は、SMU イメージのメタデータ（SMU タイプ、SMU ID、SMU 障害 ID など）を表示する **show install package** コマンドからの出力例です。

```
Device# show install package
bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Name: c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Version: 17.09.01a.0.247.1660805065
Platform: C8000V
Package Type: SMU
Defect ID: CSCvq24042
Package State: Inactive
Supersedes List: {}
SMU Fixes List: {}
SMU ID: 24042
SMU Type: non-reload
SMU Compatible with Version: 17.09.01a.0.247
SMUImpact:
```

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。