



サービスのプロビジョニング

- [アプリケーション](#) (1 ページ)
- [アプリケーションホスティング](#) (24 ページ)
- [Cisco Catalyst 9100 シリーズ アクセスポイントでのアプリケーションホスティング](#) (33 ページ)
- [サイト間 VPN の設定](#) (37 ページ)
- [ユーザー定義のネットワークサービスの作成](#) (39 ページ)
- [Cisco Umbrella の設定](#) (40 ページ)
- [セキュアなトンネルの設定](#) (48 ページ)

アプリケーション

ここでは、アプリケーションについて説明します。

アプリケーションの可視性について

アプリケーション可視性サービスを使用すると、組み込みアプリケーション、カスタムアプリケーション、およびアプリケーションセットを管理できます。

アプリケーション可視性サービスは、<ph conref="../../../../reuse/r_dnac_reusable_names_and_phrases.xml#id_48305/ph_dnac_name">.</ph> 内でアプリケーションスタックとしてホストされているため、特定のデバイスでコントローラベースのアプリケーション認識 (CBAR) 機能を有効にして、数千のネットワークと自社製のアプリケーションおよびネットワークトラフィックを分類することができます。

次のパッケージをインストールします。

- **[Application Policy]** : キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。
- **[Application Registry]** : アプリケーションとアプリケーションセットを表示、管理、および作成できます。

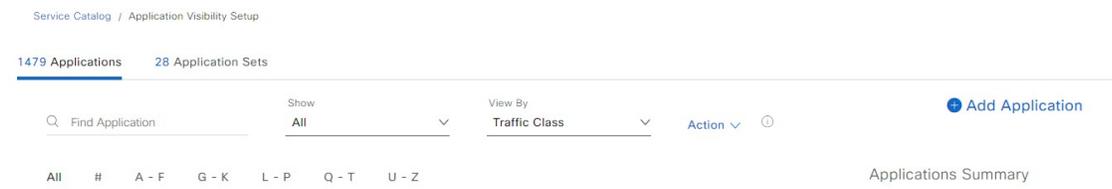
- [Application Visibility Service] : Network-Based Application Recognition (NBAR) および CBAR の技術を使用してアプリケーションを分類できます。

NBAR は、Cisco Catalyst 9000 デバイスでの最大 450 のインターフェイスのプロビジョニングをサポートしています。<ph conref="../../../../reuse/r_dnac_reusable_names_and_phrases.xml#id_48305/ph_dnac_name">を使用して無効にすることができます。</ph>のアプリケーション可視性は、この 450 インターフェイスの制限を超えません。

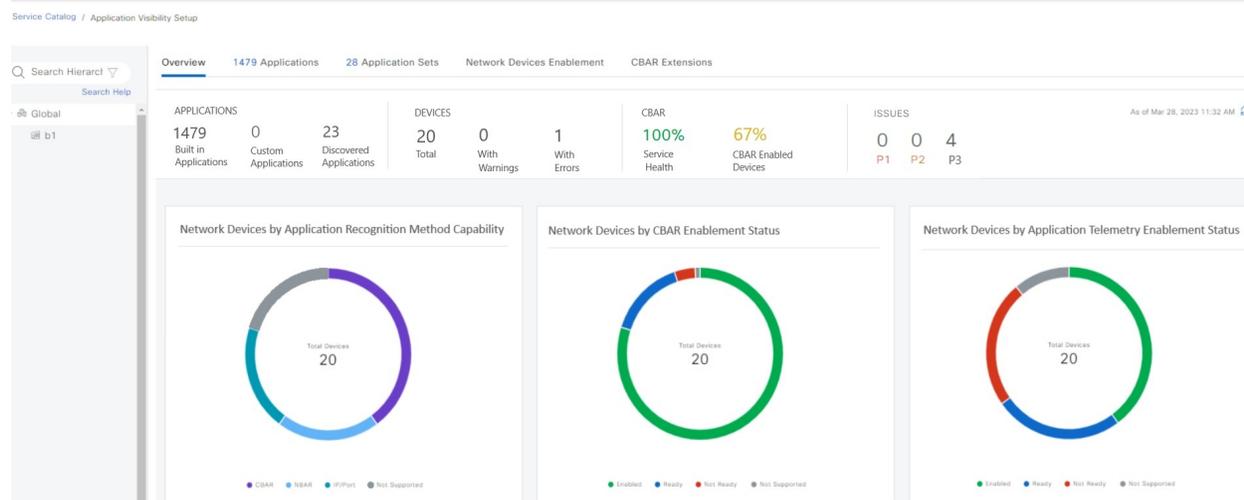


(注) 互換性を確保するには、上記のパッケージのパッケージバージョンが同じである必要があります。

アプリケーションレジストリ、またはアプリケーションレジストリとアプリケーションポリシーの両方をインストールした場合、<ph conref="../../../../reuse/r_dnac_reusable_names_and_phrases.xml#id_48305/ph_lower-case-phrase_hamburger_menu_icon">したときに、[Application] と [Application Sets] のタブが表示されます。 **プロビジョニング > アプリケーションの可視性の設定**。



アプリケーションレジストリとアプリケーション可視性サービスをインストールした場合、またはアプリケーションレジストリ、アプリケーションポリシー、およびアプリケーション可視性サービスをインストールした場合に、<ph conref="../../../../reuse/r_dnac_reusable_names_and_phrases.xml#id_48305/ph_lower-case-phrase_hamburger_menu_icon">すると、[Applications]、[Application Sets]、[Network Devices Enablement]、[CBAR Extensions] の各タブが表示されます。 **プロビジョニング > アプリケーションの可視性の設定**。



アプリケーションの可視性の設定ビュー

次の表に、[Provision] > [Services] > [Application Visibility Setup] の [Overview] タブに表示されるダッシュレットおよびチャートを示します。

アイテム	説明
アプリケーション	<p>このチャートには、Catalyst Center アプリケーション内のアプリケーションのうち、アプリケーションポリシーで使用できるアプリケーションの数が表示されます。アプリケーションは次のように分類されます。</p> <ul style="list-style-type: none"> • [Custom] : ユーザーによって追加されたアプリケーション • [Built-in]: インストールされているアプリケーション Catalyst Center • [Discovered] : さまざまな認識方法で検出され、アプリケーションレジストリにインポートされたアプリケーション <p>(注) このチャートには、CBAR が有効なデバイスでのみ観察されたアプリケーションが表示されます。</p>
デバイス	<p>デバイス、警告のあるデバイス、およびエラーのあるデバイスの総数が表示されます。</p>
CBAR	<p>このウィジェットには、すべての CBAR 対応デバイスのサービス正常性と平均正常性スコアが表示されます。デバイスに未処理のエラーまたは警告がない場合、そのデバイスは正常です。</p> <p>CBAR 正常性スコアは、すべての CBAR 対応デバイスで計算されます。</p> <p>各 CBAR 対応デバイスの CBAR 正常性を確認できます。0% の CBAR 正常性スコアは、デバイスに少なくとも1つのエラー (P1) があることを示します。50% の CBAR 正常性スコアは、デバイスにエラーはないが、少なくとも1つの警告 (P2) があることを示します。100% の CBAR 正常性スコアは、正常なデバイスを示します。</p>
問題	<p>すべての問題は、次のように優先順位によって分類されます。</p> <ul style="list-style-type: none"> • エラー (P1) • 警告 (P2) • その他 (P3) <p>[P1]、[P2]、および [P3] タブをクリックすると、デバイスの問題と修復の詳細が表示されます。</p>

アイテム	説明
アプリケーション認識方式別のネットワークデバイス	<p>このチャートには、各アプリケーション認識方式によって分類されたデバイスの数が表示されます。</p> <ul style="list-style-type: none"> • [CBAR] : CBAR 対応デバイス (ルータ、スイッチなど) • [NBAR] : NBAR ベースのデバイス (ルータ、スイッチ、シスコワイヤレスコントローラ、Cisco Catalyst 9800 シリーズワイヤレスコントローラなど) • [IP/port] : IP/ポートベースのデバイス (スイッチなど) • [Not supported] : 上記のいずれの方式でもサポートされていないデバイス
CBAR 有効化ステータス別のネットワークデバイス	<p>このチャートには、各 CBAR の準備状況ステータスのデバイス数が表示されます。</p> <ul style="list-style-type: none"> • [Enabled] : CBAR が有効になっているデバイス • [Ready] : CBAR を有効にする準備が整っているデバイス <p>(注) [Ready] ステータスの横にある情報アイコンは、それぞれのデバイスがワイヤレス対応であることを示しています。</p> <ul style="list-style-type: none"> • [Not Ready] : CBAR をサポートしているが、いくつかの問題により CBAR を有効にする準備ができていないデバイス • [Not Supported] : CBAR をサポートしていないデバイス
アプリケーションテレメトリ有効化ステータス別のネットワークデバイス	<p>このチャートには、デバイスアプリケーションテレメトリ有効化ステータスが表示されます。</p> <ul style="list-style-type: none"> • [Enabled] : アプリケーションテレメトリが有効になっているデバイス • [Ready] : アプリケーションテレメトリを有効にする準備が整っているデバイス • [Not Ready] : アプリケーションテレメトリをサポートしているが、いくつかの問題によりアプリケーションテレメトリを有効にする準備ができていないデバイス • [Not Supported] : アプリケーションテレメトリをサポートしていないデバイス

次の表に、[Network Devices Enablement] タブの [Site Devices] テーブルに表示されるデバイス情報およびステータスを示します。

カラム	説明
[Device Name]	デバイスの名前。デバイス名をクリックして、CBARサービスのステータスを表示します。
[Management IP]	デバイスの IP アドレス。
デバイス タイプ	ルータ、スイッチとハブ、ワイヤレス コントローラなど、関連するデバイスのグループ。
Site	デバイスに割り当てられているサイト。
ファブリック	デバイスが割り当てられているファブリックドメイン。
ロール (Role)	スキャンプロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Catalyst Center でデバイスロールを特定できない場合、デバイスロールは不明に設定されます。
アクティブな認識方法	デバイス認識方式 (CBAR、NBAR、IP/Port、または Not supported) が表示されます。
[OS Version]	デバイスで現在実行されている Cisco IOS ソフトウェア。
CBAR 準備状況ステータス	[CBAR Readiness Status] 列に表示されているステータスにカーソルを合わせると、対応策メッセージが表示されます。
プロトコルパックバージョン	デバイスにインストールされているプロトコルパックの現在のバージョンと、プロトコルパックの更新ステータスが表示されます。
デバイス レジストリ ステータス	デバイスとアプリケーションレジストリとの同期ステータスが表示されます。情報アイコンまたはエラーアイコンにカーソルを合わせると、同期ステータスに関する詳細が表示されます。
CBAR の展開ステータス	CBAR の展開ステータスが表示されます。 詳細については、 ネットワークデバイスでのCBARの再設定 (11 ページ) を参照してください。
サービス正常性ステータス	[Service Health Status] 列の [Issues] をクリックすると、[CBAR Service Status] ページが開きます。このページには、問題の完全なリストとデバイスのサービスステータス情報が表示されます。Cisco Catalyst 9K デバイスの名前をクリックすると、CBAR サービスのフットプリント (サービス負荷、CPU、フロー) を確認できます。
アプリケーションテレメトリ準備ステータス	アプリケーションテレメトリのデバイス準備状況が表示されません。

カラム	説明
アプリケーションテレメトリ展開ステータス	デバイスのアプリケーションテレメトリ展開ステータスが表示されます。展開が失敗した場合、リンクをクリックすると、失敗の詳細が表示されます。
Application QoS Policy	デバイスに適用されているアプリケーションポリシー。シスコワイヤレスコントローラに複数のアプリケーションポリシーがある場合は、適用されているアプリケーションポリシーの数と適用されているすべてのアプリケーションポリシーの名前が表示されます。
WAN インターフェイス	WAN インターフェイスの数が表示されます。[WAN interface details] をクリックすると、デバイスの WAN 接続設定が表示されます。
トランクインターフェイス	トランクインターフェイスの数が表示されます。[Trunk interface details] をクリックすると、デバイスのトランク接続設定が表示されます。

CBAR クラウドの設定

アプリケーション可視性サービスでは、CBAR クラウドを使用してプロトコルパックを拡充し、クラウドからデータを送受信することによって不明なアプリケーションの可視性を強化します。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision]>[Application Visibility Setup]の順に選択します。
- ステップ 2** [CBAR Extensions]>[CBAR Cloud] タブをクリックします。
- ステップ 3** クラウド認証リンクをクリックして Cisco DNA - Cloud に接続し、CBAR を有効にして、CBAR アプリケーションインテリジェンス データにアクセスします。
[System]>[Settings]>[Cloud Authentication] ウィンドウにリダイレクトされます。
- ステップ 4** Cisco DNA - Cloud でトークンを生成し、それを [Cloud Authentication] ウィンドウに入力する必要があります。[Where do I get my token Encryption Key] リンクをクリックしてトークンを生成します。
Cisco DNA - Cloud アカウントがない場合は、dna.cisco.com リンクをクリックします。
- ステップ 5** Cisco DNA - Cloud の GUI で、メニューアイコンをクリックしてから [Applications] をクリックし、[Products] を選択します。
- ステップ 6** [Region] ドロップダウンリストから、適切なリージョンを選択し、[Register] をクリックします。
- ステップ 7** [Register Product] ペインで、[Host Name/IP]、[Name]、[Description] (ある場合) などの必要な詳細を入力します。[Type] ドロップダウンリストから、Cisco DNA Center などの登録する製品の適切なタイプを選択します。[登録 (Register)] をクリックします。

(注) [Enable Cloud Access Login] チェックボックスをオンにして、Cisco DNA – Cloud から Catalyst Center への自動ログインを有効にします。

OTP の交換が自動的に行われ、Catalyst Center が新しいウィンドウで開きます。

ステップ 8 手動で接続する場合、Catalyst Center が正常に登録された後に、[OTP Generated] ダイアログボックスが表示されます。OTP をコピーするには、[Copy] をクリックし、[Close] をクリックします。

ステップ 9 [Cloud Authentication] ウィンドウに戻って接続を確立します。

- Cisco DNA Center GUI で、メニューアイコンをクリックし、[System]>[Settings]>[Cloud Authentication] の順に選択します。
- [Add OTP Key] をクリックします。
- [OTP Code] フィールドに、Cisco DNA - Cloud アプリケーションで生成してコピーした OTP を貼り付け、[Done] をクリックします。

接続が正常に確立されると、CBAR クラウドはデフォルトで有効になります。

ステップ 10 [CBAR Cloud] タブで、使用可能な **CBAR ダイナミック アプリケーション フィールド** のリストを表示できます。すべてのアプリケーションフィールドを有効にするには、[All] オプションボタンをクリックします。

(注) すべてのフィールドを選択すると、新しく導入されたアプリケーションフィールドがネットワークで自動的に有効になります。

必要なアプリケーションフィールドを有効にするには、次の手順を実行します。

- [Selected only] オプションボタンをクリックします。
- 選択するアプリケーションフィールドの横にあるチェックボックスをオンにします。
- [Apply] をクリックします。

(注) [Selected only] モードでは、新しく導入されたアプリケーションフィールドは、手動で選択するまでネットワークにインポートされません。

CBAR クラウドの有効化/無効化

始める前に

Catalyst Center と Cisco DNA-Cloud の間で接続が確立されていることを確認します。詳細については、[CBAR クラウドの設定 \(6 ページ\)](#) を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision]>[Application Visibility Setup] の順に選択します。

ステップ 2 [CBAR Extensions]>[CBAR Cloud] タブをクリックします。

ステップ 3 CBAR クラウドを有効にするには、[Enable] トグルボタンをクリックします。

ステップ4 CBAR クラウドを無効にするには、[Enable] トグルボタンを無効にして、表示されるダイアログボックスで [Yes] をクリックします。

ネットワークデバイスでの CBAR の有効化/無効化

始める前に

- デバイスがサイトに割り当てられている必要があります。
- ネットワークデバイスで CBAR を有効にする前に、CBAR クラウドを設定することをお勧めします。詳細については、[CBAR クラウドの設定（6 ページ）](#) を参照してください。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]>[Application Visibility Setup]>[Network Devices Enablement]** タブを選択します。

[Site Devices] テーブルが表示されます。すべての列を表示するには、縦の省略記号をクリックし、[All] をクリックします。

ステップ2 選択したデバイスまたはすべてのデバイスで CBAR を有効にするには、次の手順を実行します。

1. すべてのデバイスで CBAR を有効にするには、[CBAR] ドロップダウンリストから [Enable CBAR on all ready devices] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。
2. 選択したデバイスで CBAR を有効にするには、デバイス名の横にあるチェックボックスをオンにしてデバイスを選択してから、[CBAR] ドロップダウンリストから [Enable CBAR on selected devices] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。

ステップ3 選択したデバイスまたはすべてのデバイスで CBAR を無効にするには、次の手順を実行します。

1. すべてのデバイスで CBAR を無効にするには、[CBAR] ドロップダウンリストから [Disable CBAR on all devices] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。
2. 選択したデバイスで CBAR を無効にするには、デバイス名の横にあるチェックボックスをオンにしてデバイスを選択してから、[CBAR] ドロップダウンリストから [Disable CBAR on selected devices] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。

アプリケーションテレメトリの有効化/無効化

始める前に

アプリケーションテレメトリを有効にする前に、CBAR クラウドを設定することをお勧めします。詳細については、[CBAR クラウドの設定（6 ページ）](#) を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Application Visibility Setup] の順に選択します。

ステップ 2 [Network Devices Enablement] タブをクリックします。

ステップ 3 [Site Devices] テーブルで、次の手順を実行してアプリケーションテレメトリを有効にします。

1. デバイスを選択します。
2. [Application Telemetry] ドロップダウンリストから、[Enable Application Telemetry] を選択します。
3. [Enable Application Telemetry] slide-in paneで [Enable] をクリックします。

(注) デバイスの**アプリケーションテレメトリ**の展開が失敗した場合は、[Application Telemetry Deployment Status] 列のリンクをクリックして失敗の理由を表示します。

ウィンドウの下部にある「Success」というメッセージは、アプリケーションテレメトリが有効になっていることを示します。

ステップ 4 アプリケーションテレメトリを無効にするには、次の手順を実行します。

1. [Site Devices] テーブルでデバイスを選択します。
2. [Application Telemetry] ドロップダウンリストから、[Disable Application Telemetry] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。

CBAR 対応デバイスでのプロトコルパックの更新

CBAR をサポートする任意のデバイスのプロトコルパックを最新または特定のプロトコルパックにアップグレードできます。プロトコルパックを手動で更新することも、プロトコルパックの自動更新を有効にすることもできます。



- (注)
- CBAR クラウドコネクタが無効になっている場合、プロトコルパック自動更新メニューは無効になります。
 - プロトコルパック自動更新が有効になっている場合、プロトコルパック手動更新メニューは無効になります。

始める前に

- [System Settings] で Cisco ログイン情報を設定します。シスコのログイン情報の設定に関する詳細については、『[Cisco DNA Center Administrator Guide](#)』を参照してください。
- デバイスは CBAR をサポートしている必要があります。

- デバイスで CBAR が有効になっている必要があります。
- デバイスのプロトコルパックは cisco.com で使用可能である必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。

ステップ 2 **[Network Devices Enablement]** タブをクリックします。

ステップ 3 **[Site Devices]** テーブルの **[Protocol Pack Version]** 列に表示されているステータスを確認します。

[Outdated] ステータスをクリックすると、**[Update Protocol Pack]** ウィンドウに該当するプロトコルパックのリストが表示されます。

ステップ 4 **[Update Protocol Pack]** ウィンドウで、必要なプロトコルパックのバージョンに対応する **[Update]** をクリックします。

[Protocol Pack Version] カラムに **[In progress]** ステータスが表示されます。現在更新中のバージョンを表示するには、情報アイコンをクリックします。**[Protocol Pack Version]** カラムに **[Update failed]** ステータスが表示されたら、エラーアイコンをクリックして失敗の原因を確認します。

ステップ 5 すべてのデバイスまたは選択したデバイスを最新のプロトコルパックに手動で更新する場合は、次の手順を実行します。

該当するすべての CBAR 対応デバイスでプロトコルパックを更新するには、次のようにします。

- **[Update Protocol Pack]** ドロップダウンリストから、**[Update All Devices]** を選択し、後続の警告ダイアログボックスで **[Yes]** をクリックします。

選択したデバイスでプロトコルパックを更新するには、次のようにします。

- **[Site Devices]** テーブルでデバイスを選択します。
- **[Update Protocol Pack]** ドロップダウンリストから、**[Update Selected Devices]** を選択し、後続の警告ダイアログボックスで **[Yes]** をクリックします。

ファイルから選択したデバイスでプロトコルパックを更新するには、次のようにします。

- **[Site Devices]** テーブルでデバイスを選択します。
- **[Update Protocol Pack]** ドロップダウンリストから、**[Update Selected Devices From File]** を選択します。
- **[Update Protocol Pack From File]** slide-in pane で、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、**[Choose a file]** をクリックして CSV ファイルの場所を参照し、**[Open]** をクリックします。
- **[Import]** をクリックします。

ステップ 6 すべてのデバイスのプロトコルパックを自動更新する場合は、次の手順を実行します。

- **[Update Protocol Pack]** ドロップダウンリストから、**[Auto Update]** トグルボタンを有効にして、後続の警告ダイアログボックスで **[Yes]** をクリックします。

(注) デフォルトでは、すべての準備完了デバイスが自動更新に含まれます。

選択したデバイスをプロトコルパック自動更新から除外するには、次の手順を実行します。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Exclude Selected Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

選択したデバイスをプロトコルパックの自動更新に含めるには、次の手順を実行します。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Include Selected Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

ネットワークデバイスでの CBAR の再設定

[Application Visibility Setup] > [Network Devices Enablement] ウィンドウで、[Site Devices] テーブルのインターフェイスを含めたり除外したりできます。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。
 - ステップ 2** [Network Devices Enablement] タブをクリックします。
 - ステップ 3** [Site Devices] テーブルで、設定するデバイスの [CBAR Deployment status] 列で [Re-Configure] をクリックし、次の手順を実行します。
 - a) [Enable CBAR] slide-in pane で、デバイス名を検索するかデバイスを見つけて [View Interfaces] をクリックします。
 - b) 除外するインターフェイスを見つけます。
 - c) [Status] 列で、トグルボタンをクリックしてインターフェイスを無効にし、[Save] をクリックします。
 - ステップ 4** インターフェイスを含めるには、[Excluded Interfaces] を選択し、目的のインターフェイスの横にあるトグルボタンをオンにして [Save] をクリックします。
 - ステップ 5** [有効 (Enable)] をクリックします。
 - ステップ 6** [Visibility of Configurations] の設定に基づいて、使用可能なオプションを選択します。詳細については、[構成ワークフローの可視化と制御](#)を参照してください。
 - CBAR をすぐに有効にするには、[Now] オプションボタンをクリックします。
 - 将来の日付と時刻でタスクをスケジュールするには、[Later] オプションボタンをクリックして、展開する日時を定義します。
 - Catalyst Center を使用すると、構成をシスコネットワークデバイスに展開する前に確認できます。構成は、[Preview Configuration] ウィンドウから確認できます。

CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。

- ステップ 7** 前の手順で [Generate configuration preview] を選択した場合は、[Task Name] フィールドにタスク名を入力し、[Apply] をクリックします。
- ステップ 8** (任意) [Deploy] または [Discard] をクリックします。設定を展開する準備ができていない場合は、[Exit and Preview Later] をクリックします。
- ステップ 9** 前の手順で設定を展開することを選択した場合は、次の手順を実行します。
1. すぐに設定を展開するために [Now] をクリックするか、後で展開することをスケジュールするために [Later] をクリックします。
 2. 必要に応じて、デフォルトの [Task Name] を編集します。
 3. [Submit] をクリックします。

設定が正常に送信されると、成功メッセージが表示されます。

[Work Items] ウィンドウでタスクのステータスを確認できます。[Work Items] ウィンドウに移動するには、メニューアイコンをクリックして選択[Activities] > [Work Items] の順に選択します。

アプリケーションおよびアプリケーションセット

アプリケーションは、ネットワーク内で使用されているソフトウェアプログラムまたはネットワーク シグナリング プロトコルです。Catalyst Center は、約 1400 の異なるアプリケーションから成る Cisco Next Generation Network-Based Application Recognition (NBAR2) ライブラリの全アプリケーションをサポートしています。

アプリケーションは、アプリケーションセットと呼ばれる論理グループに分類されています。アプリケーションセットには、ポリシー内でのビジネスとの関連性を割り当てることができます。

アプリケーションは、同様のトラフィック処理要件が規定されている RFC4594 の定義に従い、業界標準ベースのトラフィッククラスにマッピングされています。トラフィッククラスでは、割り当てられているビジネスとの関連性グループに基づいて、アプリケーショントラフィックに適用される処理 (Differentiated Services Code Point (DSCP) マーキング、キューイング、破棄など) を定義します。

Catalyst Center に含まれていない追加のアプリケーションがある場合は、カスタム アプリケーションとして追加して、アプリケーションセットに割り当てることができます。

単方向と双方向のアプリケーショントラフィック

一部のアプリケーションは、完全な左右対称であり、接続の両端に同一の帯域幅プロビジョニングを必要とします。このようなアプリケーションのトラフィックを、双方向のトラフィックと呼びます。たとえば、100 kbps の低遅延キューイング (LLQ) が一方の音声トラフィックに割り当てられている場合、逆方向の音声トラフィックにも 100 kbps の LLQ をプロビジョニ

ングする必要があります。このシナリオは、同じ Voice over IP (VoIP) コーダ/デコーダ (コーデック) が両方の方向で使用されており、マルチキャスト保留音 (MOH) のプロビジョニングが考慮されていないことが前提となっています。ただし、ストリーミングビデオやマルチキャスト MoH などの特定のアプリケーションは、ほとんどの場合、単方向です。したがって、ブランチからキャンパスに向かう方向のトラフィックフローでは、ブランチルータでこのようなトラフィック向けの帯域幅保証をプロビジョニングするのは、不要であるばかりか非効率的となる可能性があります。

Catalyst Center では、アプリケーションが特定のポリシーに関して単方向か双方向かを指定できます。

スイッチおよびワイヤレスコントローラでは、NBAR2 やカスタムアプリケーションがデフォルトで単方向となっています。ただし、ルータでは、NBAR2 アプリケーションはデフォルトで双方向です。

カスタム アプリケーション

カスタム アプリケーションは、Catalyst Center に追加するアプリケーションです。使用可能なカスタムアプリケーションの数は、[Overview] ウィンドウで確認できます。有線デバイスについては、サーバー名、IP アドレスとポート、または URL に基づいてアプリケーションを定義できます。Cisco AireOS コントローラではなく、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してカスタムアプリケーションを定義できます。

IP アドレスとポートに従ってアプリケーションを定義する場合は、DSCP 値とポート分類を定義することもできます。

設定プロセスを簡素化するために、類似のトラフィックおよびサービスレベル要件を持つ別のアプリケーションに基づいてアプリケーションを定義できます。Catalyst Center は、他のアプリケーションのトラフィッククラス設定を、定義しているアプリケーションにコピーします。

Catalyst Center は、カスタムアプリケーションの一部として定義される場合でも、ポート番号 80、443、53、5353、および 8080 の ACL を設定しません。カスタムアプリケーションでトランスポート IP が定義されている場合、Catalyst Center はデバイス上のアプリケーションを設定します。



(注) ポリシーが展開されているときにデバイス上のカスタムアプリケーションをプログラムする場合は、そのカスタム アプリケーションを、ポリシーで定義されているいずれかのアプリケーションセットに割り当てる必要があります。

検出されたアプリケーション

検出されるアプリケーションには、Infoblox DNS サーバーなどの推奨されるカスタマイズからインポートされたアプリケーションと、推奨される未分類のアプリケーションフローからインポートされたアプリケーションがあります。

未分類のトラフィックには、CBAR 対応デバイスで識別されるフローからのトラフィックのうち、NBAR エンジンでは認識されないフローからのトラフィックが含まれます。このような場合、意味のあるビットレートを持つアプリケーションが未分類として報告され、Catalyst Center でインポートしてアプリケーションとして使用することができます。

アプリケーション可視性サービスでは、Catalyst Center を、CBAR クラウドを介して外部の信頼できるソースに接続して、未分類のトラフィックを分類したり、改善されたシグニチャを生成したりできます。

使用可能な外部の信頼できるソースは、Google Meet、ServiceNow、Sugarcrm、Telegram、SAP、Microsoft Office 365 クラウドコネクタ、Box、RingCentral、Github、Crashplan、Intuit、Workday、Zscaler、Atlassian、Amazon Chime、Zoom、Dropbox、Webex、Whatsapp、Cisco Meraki、および Salesforce です。このリストは動的です。新しいソースがクラウドに追加されると、リストが更新されます。リストを表示するには、[Application Visibility Setup] > [CBAR Extensions] > [CBAR Cloud]の順に選択します。



(注) アプリケーションを設定する前に、CBAR クラウドコネクタを設定する必要があります。

検出されたアプリケーションはアプリケーションレジストリにインポートされます。

お気に入りのアプリケーション

Catalyst Center では、他のすべてのアプリケーションよりも先に設定するアプリケーションにフラグを付けることができます。お気に入りとしてアプリケーションにフラグを付けることで、デバイス上のお気に入りのアプリケーションに対して QoS ポリシーが設定されていることを確認できるようにします。詳細については、[リソースが制限されているデバイスの処理順](#)を参照してください。

カスタムアプリケーションを作成すると、お気に入りのアプリケーションとしてマークされます。

お気に入りとしてマークできるアプリケーションの数に制限はありませんが、お気に入りのアプリケーションをごく少数にとどめると（たとえば、25 未満）、ネットワークデバイスの TCAM (Ternary Content Addressable Memory) が限られている展開で、お気に入りのアプリケーションがビジネス関連の観点から正しく処理されるようになります。

お気に入りのアプリケーションは、ビジネス関連のグループまたはトラフィッククラスに属させることが可能で、ポリシー単位ではなくシステム全体で設定されます。たとえば、お気に入りとして cisco-jabber-video アプリケーションにフラグを付けた場合、そのアプリケーションはすべてのポリシーでお気に入りのフラグが付きます。

ビジネス関連のアプリケーションだけでなく、ビジネスに関係のないアプリケーションにもお気に入りのフラグを付けられることに注意してください。たとえば、ネットワーク上に大量の望ましくない Netflix トラフィックがある場合、Netflix にお気に入りのアプリケーションとしてフラグを付けることができます (Netflix がビジネスに関係のないアプリケーションとして割り当てられている場合でも可能)。この場合、Netflix は、その他のビジネスに関係のないアプ

リケーションより先にデバイスポリシーに組み込まれるようになり、このアプリケーションを制御するビジネス上の目的が確実に実現されます。

アプリケーションおよびアプリケーションセットの設定

次のサブセクションでは、アプリケーションとアプリケーションセットのコンテキストで実行できるさまざまなタスクについて説明します。



- (注) 編集または削除できるのは、カスタムアプリケーションと検出されたアプリケーションだけです。また、一度に編集または削除できる数は、カスタムアプリケーションと検出されたアプリケーションの合計で最大100個までです。編集または削除する対象としてアプリケーションを選択した場合、選択したアプリケーションの数を除く、編集または削除が可能なアプリケーションの数を示す通知メッセージが表示されます。

アプリケーション設定の変更

既存のCBARアプリケーション、カスタムアプリケーション、検出されたアプリケーションのアプリケーションセットやトラフィッククラスを変更できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。

ステップ 2 **[Applications]** タブをクリックします。

ステップ 3 **[Search]**、**[Show]**、または**[View By]** フィールドを使用して、変更するアプリケーションを見つけます。名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 **[アプリケーション名 (Application Name)]** をクリックします。

ステップ 5 ダイアログボックスで、1つまたは両方の設定を変更します。

- **[Traffic Class]** : ドロップダウンリストからトラフィッククラスを選択します。有効なトラフィッククラスは、**BROADCAST_VIDEO**、**BULK_DATA**、**MULTIMEDIA_CONFERENCING**、**MULTIMEDIA_STREAMING**、**NETWORK_CONTROL**、**OPS_ADMIN_MGMT**、**REAL_TIME_INTERACTIVE**、**SIGNALING**、**TRANSACTIONAL_DATA**、**VOIP_TELEPHONY** です。
- **[Application Set]** : ドロップダウンリストからアプリケーションの設定を選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマソーシャルネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 6 [Save] をクリックします。

サーバー名に基づくカスタム アプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup]の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 ウィンドウの右上隅にある [Add Application] をクリックします。

ステップ 4 slide-in paneで、次のフィールドに必要な情報を入力します。

- **[Application Name]** : カスタムアプリケーションの名前。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
- **[Type]** : ユーザーがアプリケーションにアクセスするための方法。サーバー経由でアクセス可能なアプリケーションの [サーバー名 (Server Name)] を選択します。
- **[Server name]** : アプリケーションをホストするサーバーの名前。
- **[Similar To]** : 類似のトラフィック処理要件を持つアプリケーション。オプションボタンをクリックしてこのオプションを選択し、ドロップダウンリストからアプリケーションを選択します。Catalyst Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
- **[Traffic Class]** : アプリケーションが属するトラフィッククラス。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
- **[Application set]** : アプリケーションを配置するアプリケーションセット。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [Save] をクリックします。

IP アドレスおよびポートベースのカスタム アプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

- ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。
- ステップ 2 **[Application]** タブをクリックします。
- ステップ 3 **[アプリケーションの追加 (Add Application)]** をクリックします。
- ステップ 4 **[Application Name]** フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
- ステップ 5 **[種類 (Type)]** エリアで、**[サーバー IP/ポート (Server IP/Port)]** ラジオボタンをクリックして、アプリケーションが IP アドレスとポートを通じてアクセスできます。
- ステップ 6 **[DSCP]** チェックボックスをオンにして、DSCP 値を定義します。値を定義しない場合のデフォルト値は **[Best Effort]** です。ベストエフォートサービスとは原則的に、いずれの QoS も適用されないネットワークデバイスのデフォルト動作です。
- ステップ 7 **[IP/Port Classifiers]** チェックボックスをオンにして、アプリケーションの IP アドレスおよびサブネット、プロトコル、ポートまたはポート範囲を選択します。有効なプロトコルは、**[IP]**、**[TCP]**、**[UDP]**、**[TCP/UDP]** です。**[IP]** プロトコルを選択した場合は、ポート番号または範囲は定義しません。+ をクリックして、さらに分類子を追加します。
- ステップ 8 次のいずれかの方法を使用して、アプリケーショントラフィック処理要件を定義します。
 - **[Similar To]**：お使いのアプリケーションに既存のアプリケーションと同様のトラフィック処理要件がある場合は、**[Similar To]** オプションボタンをクリックし、ドロップダウンリストからアプリケーションを選択します。Catalyst Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
 - **[Traffic Class]**：アプリケーションに定義するトラフィッククラスがわかっている場合は、**[Traffic Class]** オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は **BULK_DATA**、**TRANSACTIONAL_DATA**、**OPS_ADMIN_MGMT**、**NETWORK_CONTROL**、**VOIP_TELEPHONY**、**MULTIMEDIA_CONFERENCING**、**MULTIMEDIA_STREAMING**、**BROADCAST_VIDEO**、**REAL_TIME_INTERACTIVE**、および **SIGNALING** です。
- ステップ 9 **[Application Set]** ドロップダウンリストから、アプリケーションが属するアプリケーションセットを選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ10 [Save] をクリックします。

URLに基づくカスタムアプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタムアプリケーションとして追加することができます。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup] の順に選択します。

ステップ2 [Application] タブをクリックします。

ステップ3 [アプリケーションの追加 (Add Application)] をクリックします。

[アプリケーションの追加 (Add Application)] ダイアログボックスが表示されます。

ステップ4 [アプリケーション名 (Application Name)] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大24文字の英数字を指定できます。(アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。)

ステップ5 タイプについては、[URL] オプションボタンをクリックします。

ステップ6 [Url] フィールドに、アプリケーションに到達するために使用する url を入力します。

ステップ7 トラフィック クラスの設定:

- 同様のトラフィック処理要件を持つ別のアプリケーションと同じトラフィッククラスを使用するには、オプションボタンをクリックして、ドロップダウンリストからアプリケーションを選択します。
- トラフィッククラスを指定するには、[トラフィッククラス (Traffic class)] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ8 [アプリケーションセット (Application set)] ドロップダウンリストから、アプリケーションを配置するアプリケーションセットを選択します。

ステップ9 [Save] をクリックします。

カスタムアプリケーションの編集または削除

必要な場合は、カスタムアプリケーションを変更または削除できます。



- (注) アプリケーション ポリシーによって直接参照されているカスタム アプリケーションを削除することはできません。通常、アプリケーションポリシーはアプリケーションセットを参照し、個々のアプリケーションを参照しません。ただし、ポリシーにアプリケーションの特別な定義（コンシューマまたはプロデューサの割り当てや双方向の帯域幅プロビジョニングなど）が設定されている場合、ポリシーはそのアプリケーションを直接参照します。そのため、アプリケーションを削除する前に、特別な定義を削除するか、またはアプリケーションへの参照を削除する必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。

ステップ 2 **[Application]** タブをクリックします。

ステップ 3 **[Search]**、**[Show]**、または**[View By]** フィールドを使用して、変更するアプリケーションを見つけます。名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 アプリケーションを編集するには、次の手順を実行します。

- アプリケーション名をクリックして、必要な変更を行います。フィールドの詳細については、[サーバー名に基づくカスタムアプリケーションの作成 \(16 ページ\)](#)、[IP アドレスおよびポート ベースのカスタムアプリケーションの作成 \(17 ページ\)](#)、または[URL に基づくカスタムアプリケーションの作成 \(18 ページ\)](#) を参照してください。
- [Save]** をクリックします。

または、アプリケーションを選択し、**[Actions]** ドロップダウンリストから**[Edit]** をクリックしてアプリケーションを編集します。

- (注) ポリシーを再展開しても、編集したカスタムアプリケーションは再設定されません。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

ステップ 5 アプリケーションを削除するには、アプリケーションボックスにある  をクリックし、次に **[OK]** をクリックして確定します。

または、次の手順に従ってアプリケーションを削除することもできます。

- アプリケーション名の横にあるチェックボックスをオンにします。複数のアプリケーションを選択することもできます。
- [Actions]** ドロップダウンリストから、**[Delete]** オプションをクリックします。
- [OK]** をクリックして確定します。

アプリケーションをお気に入りにする

アプリケーションをお気に入りとしてマークして、アプリケーションの QoS 設定を、他のアプリケーションの QoS 設定の前にデバイスに展開する必要があることを指定できます。お気に入りとしてマークされたアプリケーションには、その横に黄色の星が付いています。

ポリシーを追加または編集すると、お気に入りとしてマークされたアプリケーションがアプリケーションセットの上部に表示されます。

アプリケーションは、個々のポリシーベースではなくシステム全体で設定されます。詳細については、「[お気に入りのアプリケーション \(14 ページ\)](#)」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup]の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 お気に入りとしてマークするアプリケーションを特定します。

ステップ 4 スターアイコンをクリックします。

カスタム アプリケーション設定の作成

使用したいアプリケーションセットがない場合、カスタム アプリケーションセットを作成できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup]の順に選択します。

ステップ 2 [Application Sets] タブをクリックします。

ステップ 3 [Add Application Set] をクリックします。

ステップ 4 slide-in paneに、新しいアプリケーション設定の名前を入力します。

Catalyst Center で新しいアプリケーションセットが作成されますが、アプリケーションは含まれません。

ステップ 5 ドロップダウンリストから [Default Business Relevance] を選択します。デフォルトのビジネス関連性 (Default Business Relevance) は、具体的なアプリケーション QoS がない場合のビジネス関連性レベルです。このレベルは、ポリシーに割り当てられていないサイトのアシュアランスに表示されます。

ステップ 6 [Save] をクリックします。

ステップ 7 [Search] を使用して [Show] または [View By] フィールドを使用して、アプリケーション設定を見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 8 新しいアプリケーション設定に移動させるアプリケーションを見つけます。

ステップ 9 移動させるアプリケーションの横にあるチェック ボックスをオンにします。

ステップ 10 新しいアプリケーション設定にアプリケーションをドラッグアンドドロップします。

カスタムアプリケーションセットの編集または削除

必要な場合は、カスタムアプリケーションを変更または削除できます。



(注) アプリケーションポリシーによって参照されているカスタムアプリケーションセットを削除することはできません。アプリケーションセットを削除する前に、ポリシーからアプリケーションセットを削除する必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup]の順に選択します。

ステップ 2 [Application Sets] タブをクリックします。

ステップ 3 [検索 (Search)]、[表示 (Show)]、または[表示方法 (View By)] フィールドを使用して、変更するアプリケーションセットを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 次のいずれかを実行します。

- アプリケーション設定するには、アプリケーション設定に、またはアプリケーション設定からアプリケーションをドラッグアンドドロップします。[OK]をクリックして、それぞれの変更を確定します。
- アプリケーション設定を削除するには、アプリケーション設定ボックスにある  をクリックし、次に [OK] をクリックして確定します。

未分類アプリケーションの検出

Catalyst Center のアプリケーション可視性サービスは、分類済みと未分類のドメインおよびソケットに関する情報をデバイスから取得し、その情報を [Observed Traffic] チャートに表示します。アプリケーション可視性サービスによって検出された未分類のサーバー名と IP/ポートの数は、[Recommendations] の下に表示されます。

未分類のサーバー名と IP/ポートはアプリケーションレジストリに追加できます。



(注) 最大 1100 の検出されたアプリケーションをアプリケーションレジストリに追加できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Application Visibility Setup]の順に選択します。

- ステップ2 [CBAR Extensions] > [Discovered Applications] タブをクリックします。
- ステップ3 表に、未分類の検出されたサーバーまたはIP/ポートのリストが表示されます。表内で選択したサーバーまたはIP/ポートを非表示にする場合は、サーバーを選択して [Hide Ignored Applications] チェックボックスをオンにします。
- ステップ4 アプリケーションレジストリでアプリケーションとしてインポートするサーバーまたはIP/ポートを選択します。
- ステップ5 ドロップダウンリストから、必要な [Application]、[Application Set]、および [Traffic Class] を選択します。
- ステップ6 [Import] をクリックします。
- ステップ7 [Applications] タブをクリックし、[Show] ドロップダウンリストから [Discovered] を選択して、インポートされたアプリケーションを表示します。

アプリケーション可視性サービスのサポート：Catalyst Center トラフィック テレメトリ アプライアンス

Catalyst Center トラフィック テレメトリ アプライアンスは、ミラーリングされた IP ネットワークトラフィックからエンドポイントテレメトリを生成し、エンドポイントの可視性とセグメンテーションのために Catalyst Center とテレメトリデータを共有します。

Catalyst Center トラフィック テレメトリ アプライアンスで CBAR を有効にするための前提条件には、次のものが含まれます。

- デバイスをサイトに割り当てる必要があります。
- デバイスロールを [Distribution] モードに設定する必要があります。

QoS ポリシーを設定せずに、Catalyst Center トラフィック テレメトリ アプライアンスで属性セットとマップを使用してカスタムアプリケーションを設定することができます。詳細については、[アプリケーション ポリシーの作成](#)および[アプリケーション ポリシーの展開](#)を参照してください。

Infoblox アプリケーションの検出

Catalyst Center を組織の Infoblox DNS サーバーと統合して、未分類のトラフィックをサーバー名に基づいて解決することができます。

始める前に

- バージョン 1.5 以降の Infoblox WAPI が必要です。Infoblox WAPI のバージョンを確認するには、Infoblox サーバーにログインし、[Help] > [Documentation] > [WAPI Documentation] の順に選択します。
- 少なくとも読み取り専用権限を持つロールを作成し、そのロールを Infoblox ユーザーに割り当てます。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Manage Users」を参照してください。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。
- ステップ 2** **[CBAR Extensions] > [Infoblox]** タブをクリックします。
- ステップ 3** **[Infoblox]** の **[Here]** リンクをクリックして、Catalyst Center で IPAM/DNS サーバーのログイン情報を設定します。
- ステップ 4** IPAM の設定を行います。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Configure an IP Address Manager」を参照してください。
- ステップ 5** **[Infoblox]** に戻り、 をクリックして、次の設定を行います。
- **[All DNS Zones]** チェックボックスをオンにするか、**[DNS Zones to Inspect]** ドロップダウンリストから必要な DNS ゾーンを選択します。ドロップダウンリストには、Infoblox サーバーで定義されている DNS ゾーンが表示されます。
 - **[Inspect]** ドロップダウンリストから必要な検査レコードを選択します。
 - **[Read Application name from]** チェックボックスをオンにし、**[Extensible Attribute]** または **[AVC RRTYPE format]** のいずれかのオプションボタンをクリックします。**[Extensible Attribute]** オプションボタンをクリックした場合は、わかりやすいアプリケーション名を含む拡張機能属性名を入力します。
 - **[Default Traffic Class]** から、Infoblox アプリケーションを分類するためのデフォルトのトラフィッククラスを選択します。
 - **[Default Application Set]** から、Infoblox アプリケーションを分類するためのデフォルトのアプリケーションセットを選択します。
- ステップ 6** **[保存 (Save)]** をクリックします。
- ステップ 7** インポートするアプリケーションを選択し、次の手順を実行します。
- アプリケーションの名前が Infoblox サーバーで定義された名前と異なる場合は、アプリケーション名を編集します。
 - **[Infoblox]** に定義されているデフォルトのアプリケーションセットとトラフィッククラスを変更する場合は、ドロップダウンリストから必要なアプリケーションセットとトラフィッククラスを選択します。
- ステップ 8** **[Import]** をクリックします。
- ステップ 9** **[Applications]** タブをクリックして **[Show]** ドロップダウンリストから **[Discovered]** を選択し、インポートされた Infoblox アプリケーションを確認して必要に応じて編集します。
- アプリケーションのインポート後にアプリケーションのサーバー名を変更すると、**[Infoblox]** ウィンドウの **[Application Status]** 列に、アプリケーションのステータスが **[Updated]** と表示されます。**[Application Status]** 列に表示されるアプリケーション名は、アプリケーションの新しいサーバー名です。アプリケーションの古いサーバー名を表示するには、情報アイコンをクリックします。
-

検出されたアプリケーションの編集と削除

必要に応じて、検出されたアプリケーションを編集または削除できます。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [Application Visibility Setup]**の順に選択します。
- ステップ 2** [アプリケーション (Applications)] タブをクリックします。
- ステップ 3** [Search]、[Show]、[View By] のいずれかのフィールドを使用して、変更する検出済みのアプリケーションを見つけます。
- 名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。
- ステップ 4** アプリケーションを編集するには、次の手順を実行します。
- アプリケーション名をクリックして、必要な変更を行います。
- 検出済みのアプリケーションの場合、[Attribute Set] と [Traffic Class] のみを編集できます。
- [Save] をクリックします。
- ステップ 5** アプリケーションを削除するには、アプリケーションを選択し、ウィンドウの上部にある [Action] ドロップダウンリストから [Delete] オプションを選択して、その後にウィンドウに表示される警告ダイアログボックスで [OK] をクリックします。
-

アプリケーションホスティング

ここでは、アプリケーションホスティングについて説明します。

アプリケーションホスティングについて

アプリケーションホスティングを使用すると、Catalyst Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。Cisco IOS-XE ソフトウェアバージョン 16.12.1s 以降を実行している Cisco Catalyst 9300 シリーズスイッチ、Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を実行している Cisco Catalyst 9100 シリーズアクセスポイント、および Cisco IOS-XE ソフトウェアバージョン 17.1 以降を実行している Cisco Catalyst 9400 シリーズスイッチでサードパーティ製 Docker アプリケーションをホストできます。



(注) Cisco DNA Center では、ホストされるアプリケーションに割り当てられるディスク容量は 5 GB に制限されています。

アプリケーションホスティングサービスパッケージのインストールと更新

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[System] > [Software Updates]。または、クラウドアイコンをクリックし、[Go to Software Updates] リンクをクリックします。

ステップ 2 [Software Updates] ウィンドウで、次のタブを確認します。

- [Updates]：システムとアプリケーションの更新が表示されます。[System Update] では、インストールされているシステムのバージョンと、Cisco Cloud からダウンロードされ、利用可能なシステムの更新が表示されます。[Application Updates] は、Cisco Cloud からダウンロードしてインストールできる使用可能なアプリケーション、アプリケーションのサイズ、適切なアクション（ダウンロード、インストール、または更新）を示します。パッケージにカーソルを合わせると、使用可能なバージョンと基本的な説明が表示されます。
- [Installed Apps]：現在インストールされているアプリケーションパッケージが示されます。

ステップ 3 アプリケーションホスティングパッケージをダウンロードするには、[Updates] > [Application Updates] でアプリケーションホスティングの名前の横にある [Install] をクリックします。

ステップ 4 アプリケーションホスティングパッケージを更新するには、[Updates] > [Application Updates] でアプリケーションホスティングの名前の横にある [Update] をクリックします。

ステップ 5 [Installed Apps] タブでバージョンを調べて、アプリケーションが更新されていることを確認します。

(注) アプリケーションホスティングサービスパッケージをインストールしたら、いったん Catalyst Center からログアウトしてブラウザのキャッシュをクリアし、再度 Catalyst Center にログインする必要があります。

アプリケーションホスティングの前提条件

Cisco Catalyst 9000 デバイスでアプリケーションホスティングを有効にするには、次の前提条件を満たしている必要があります。

- ディスカバリの前に、デバイスの NETCONF ポートを設定します。
- アプリケーションをホストするスイッチでセキュア HTTP サーバーを設定します。
- スイッチ上の HTTPS ユーザー認証用にローカル認証サーバーまたは AAA 認証サーバーを設定します。ユーザー名およびパスワードは特権レベル 15 で設定する必要があります。

- Cisco Catalyst 9300 シリーズ スイッチが Cisco IOS XE 16.12.x 以降のバージョンを実行し、Cisco Catalyst 9400 シリーズ スイッチが Cisco IOS XE 17.1.x 以降のバージョンを実行していることを確認します。
- デバイスに着脱可能な USB SSD 外部ストレージがあることを確認します (9300 ファミリのスイッチの場合のみ)。
- スイッチ上の設定が正しいことを確認します。スイッチで WebUI を開き、HTTPS ユーザーとしてログインします。

次の例は、スイッチの動作設定を示しています。

```
prompt# sh run | sec http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
```

17.3.3 より前のリリースの Cisco IOS XE を搭載するスイッチの追加設定：

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

Cisco IOS XE 17.3.3 以降のスイッチの追加設定：

```
ip http secure-active-session-modules webui
ip http session-module-list webui NG_WEBUI
ip http session-module-list pki OPENRESTY_PKI
ip http active-session-modules pki
```

- Catalyst Center で、デバイスを手動で追加するときに HTTPS ログイン情報を設定します。アプリケーション ホスティングには、HTTPS ユーザー名、パスワード、およびポート番号が必須です。デフォルトのポート番号は 443 です。デバイスログイン情報を編集することもできます。[ネットワーク デバイス クレデンシャルの更新](#)を参照してください。すでに管理されているデバイスを編集する場合は、インベントリでそのデバイスを再同期してから、アプリケーション ホスティング関連のアクションに使用します。



(注) アプリケーション ホスティングの HA は、3 ノードの Catalyst Center クラスターではサポートされていません。

アプリケーションをホストするデバイスの準備状況の表示

スイッチにアプリケーションをインストールする前に、Cisco Catalyst 9300 シリーズ スイッチのアプリケーションをホスティングするための準備状況を確認する必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services App] > [Hosting for Switches] の順に選択します。

ステップ 2 [All Devices] をクリックします。

ステップ3 アプリケーションをホストできるデバイスのリストが表示されます。[App Hosting Status] は、デバイスがアプリケーションをホストするための準備状況を示します。[See Details] をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

アプリケーションの追加

シスコパッケージまたは Docker アプリケーションを追加できます。

始める前に

- [Cisco Package] : IOS SDK ツールを使用してアプリケーションをパッケージ化し、アプリケーションが IOS XE オペレーティングシステムと互換性を持つようにする必要があります。
- [Docker] : Docker イメージを tar ファイルとして保存する必要があります。Docker イメージを tar ファイルとして保存するには、次のコマンドを入力します。

```
docker save -o <path for generated tar file> <image name:tag>  
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します : [Provision] > [Services App] > [Hosting for Switches] の順に選択します。

ステップ2 [New Application] をクリックします。

ステップ3 ドロップダウンリストからアプリケーションとカテゴリを選択します。

ステップ4 [Select] をクリックして、アップロードするアプリケーションを選択します。

ステップ5 [Upload] をクリックします。

新しく追加されたアプリケーションは、[App Hosting] ページで確認できます。

ThousandEyes Enterprise Agent アプリケーションの自動ダウンロード

ThousandEyes Enterprise Agent アプリケーションを使用すると、ネットワークをモニターし、内部、外部、キャリア、およびインターネットネットワーク全体のネットワークトラフィックパスをリアルタイムで監視できます。ThousandEyes Enterprise Agent アプリケーションの利点は、Catalyst Center アプリケーションホスティングサービスにこのアプリケーションを手動でインポートする必要がないことです。ネットワークでスイッチおよびハブが有効になっている場合、アプリケーションホスティングサービスの開始から 10 分以内に、ThousandEyes Enterprise Agent アプリケーションが自動的にダウンロードされます。アプリケーションを手動でダウンロードするには、ThousandEyes Enterprise Agent .tar ファイルへの次のリンクをクリックします。

[thousandeyes-enterprise-agent.cat9k.tar](#)

インターネット接続がない場合は、次のコマンドを使用してコンソールからプロキシ接続を設定できます。

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

ThousandEyes Enterprise Agent アプリケーションに接続するプロキシ値を設定します。

アプリケーションの更新

Catalyst Center で追加されたアプリケーションを更新できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services App] > [Hosting for Switches]** の順に選択します。

使用可能なアプリケーションは、**[App Hosting]** ウィンドウで確認できます。

ステップ 2 更新するアプリケーションを選択します。

ステップ 3 **[Update App]** をクリックします。

ステップ 4 アップロードする新しいバージョンのアプリケーションを選択します。

ステップ 5 **[Upload]** をクリックします。

アプリケーションの起動

Catalyst Center でアプリケーションを起動できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services App] > [Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、**[Manage]** をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 起動するアプリケーションがあるデバイスを選択します。

ステップ 4 **[Actions]** ドロップダウンリストから **[Start App]** を選択します。

アプリケーションの停止

Catalyst Center でアプリケーションを停止できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services App] > [Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、**[Manage]** をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 停止するアプリケーションがあるデバイスを選択します。

ステップ4 [Actions] ドロップダウンリストから [Stop App] を選択します。

デバイスでホストされているアプリケーションの表示

始める前に

「[アプリケーションホスティングの前提条件](#)」の前提条件を満たします。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services App] > [Hosting for Switches]**の順に選択します。

ステップ2 すべてのデバイスを表示するには、右上隅の **[All Devices]** をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して **[Manage]** をクリックします。

すべてのデバイスを表示することを選択した場合、**[All Devices]** ウィンドウには、アプリケーションをホストできるデバイスに関する情報 (**[Hostname]**、**[IP Address]**、**[Image Version]**、**[App Hosting Status]**、**[Last Updated]**) が表示されます。

特定のアプリケーションのデバイスのリストを表示することを選択した場合、**[Devices]** ウィンドウには、アプリケーションをホストできるデバイスに関する次の情報 (**ホスト名**、**デバイス IP**、**アプリケーションバージョン**、**アプリケーションステータス**、**最終検知プラットフォームバージョン**、**およびアクションステータス**) が表示されます。

ステップ3 **[Devices]** ウィンドウで **[Summary]** をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。

ステップ4 アプリケーションでアクションを実行するには、**[Action]** ドロップダウンリストをクリックし、**[Start]**、**[Stop]**、**[Edit]**、**[Upgrade]**、または **[Uninstall]** を選択します。

ステップ5 インストールされているホスティングアプリケーションを表示するデバイスリンクをクリックします。

[Applications] ウィンドウには、インストールされているアプリケーションの**名前**、**バージョン**、**アプリケーションステータス**、**モニタリングアプリケーション**、**正常性**、および**詳細情報**が表示されます。

(注) **モニタリングアプリケーション**には、アプリケーションモニタリングダッシュボードへのリンクが含まれています。このリンクは、**the Catalyst Center application package controller .yaml** ファイルで提供されます。このファイルにアプリケーションダッシュボード URL が含まれていない場合、**モニタリングアプリケーション**の列 (**[Monitor App]**) は適用されません。

ステップ6 **[Details]** 列で **[View]** をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。

ステップ7 特定のアプリケーションのログをダウンロードするには、アプリケーションを選択して **[Application Logs]** をクリックします。

ステップ8 デバイスからテクニカルサポートログをダウンロードするには、**[Tech Support logs]** をクリックします。

Cisco Catalyst 9300 デバイスへのアプリケーションのインストール

Catalyst Center Cisco Catalyst 9300 シリーズ スイッチにアプリケーションをインストールできません。

始める前に

- 前提条件を満たします。詳細については、「[アプリケーション ホスティングの前提条件 \(25 ページ\)](#)」を参照してください。
- アプリケーションを Catalyst Center に追加します。詳細については、「[アプリケーションの追加 \(27 ページ\)](#)」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「[アプリケーションをホストするデバイスの準備状況の表示 \(26 ページ\)](#)」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services App] > [Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、**[Install]** をクリックします。

ステップ 3 **[Get Started]** ウィンドウで、**[Task Name]** フィールドにワークフローの一意の名前を入力し、**[Next]** をクリックします。

ステップ 4 **[Select Site]** ウィンドウで、アプリケーションを有効にするサイトを選択し、**[Next]** をクリックします。

ステップ 5 **[Select Switches]** ウィンドウで、アプリケーションのインストール先デバイスを選択し、**[Next]** をクリックします。

ステータスが **[Ready]** および **[Partially Ready]** のデバイスを選択できます。**[See Details]** をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

[Partially Ready] ステータスのデバイスの場合は、**[Readiness Check]** ウィンドウの **[Check Now]** リンクをクリックして、HTTPS ログイン情報を検証します。

[Devices] テーブルに目的のデバイスがない場合は、**[Import]** をクリックして CSV ファイルからデバイスを追加します。

ステップ 6 **[Configuration App]** ウィンドウで、以降の設定を実行します。

• **[Network Settings]** :

- **[Select Network]** ドロップダウンリストから、アプリケーションを設定する VLAN を選択します。
- **[Address Type]** ドロップダウンリストから **[Static]** または **[Dynamic]** を選択します。**[Static]** を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの **[IP Address]**、**[Gateway]**、**[Prefix/Mask]**、および **[DNS]** を入力します。

- [App Resources] : [Allocate all resources available on a device] または [Customize resource allocation] チェックボックスをオンにします。[Customize resource allocation] チェックボックスをオンにすると、[CPU]、[Memory]、および [Persistent Storage] の最大値を低い値に変更できます。
- [Custom Settings] : シスコ パッケージ アプリケーションにのみ適用されます。アプリケーションによって指定された属性の設定の詳細を入力します。
- [App Data] : アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルの特定方法については、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options] : アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 7 [Summary] ウィンドウで、アプリケーション構成の設定を確認します。

ステップ 8 (任意) [Configuration Preview] をクリックし、選択したデバイスに設定をプッシュするために使用される設定テンプレートを確認します。

ステップ 9 [Provision] をクリックします。

ステップ 10 確認ウィンドウで [Yes] をクリックして、選択したデバイスでのアプリケーションのインストールを完了します。

(注) アプリケーションをインストールすると、デバイスの Cisco IOS-XE 設定も変更されます。実行中の設定に対するこの変更は、ルータのリロード後にアプリケーションが期待どおりに機能するように、スタートアップ設定にコピーする必要があります。アプリケーションのインストールが完了したら、**テンプレートハブ**を使用して実行中の設定をスタートアップ設定にコピーします。

Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9300 シリーズ スイッチからアプリケーションをアンインストールできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します : **[Provision] > [Services App] > [Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 アンインストールするアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9300 デバイスでのアプリケーション構成の編集

Cisco Catalyst 9300 シリーズ スイッチでアプリケーションを稼働させるための設定が必要な場合は、アプリケーション設定を編集できます。

-
- ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services App] > [Hosting for Switches] の順に選択します。
 - ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。
 - ステップ 3 編集するアプリケーションがあるデバイスを選択します。
 - ステップ 4 [Actions] ドロップダウンリストから、[Edit App Config] を選択します。
-

アプリケーションの削除

Catalyst Center からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、[Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール \(31 ページ\)](#) を参照してください。

-
- ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services App] > [Hosting for Switches] の順に選択します。

ホストされている削除可能なアプリケーションは、[App Hosting] ウィンドウで確認できます。
 - ステップ 2 削除するアプリケーションを選択します。
 - ステップ 3 [Delete Application] をクリックします。
 - ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、Catalyst Center によって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。確認ダイアログボックスで [Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、[Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール \(31 ページ\)](#) を参照してください。

アプリケーションログのダウンロード

アプリケーションログは Catalyst Center からダウンロードできます。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [IoT Services]** の順に選択します。
- ステップ 2** **[All Devices]** をクリックします。
- アプリケーションをホストできるデバイスのリストが表示されます。
- ステップ 3** **[APp logs]** をクリックして、Catalyst Center からアプリケーションログをダウンロードします。
- ステップ 4** **[App Logs]** ポップアップウィンドウで、ダウンロードするアプリケーション ログ ファイルを選択し、**[Download]** をクリックします。
-

デバイス テクニカル サポート ログのダウンロード

トラブルシューティングを行うために、Catalyst Center からデバイスのテクニカルサポートのログをダウンロードできます。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [IoT Services]** の順に選択します。
- ステップ 2** **[All Devices]** をクリックします。
- アプリケーションをホストできるデバイスのリストが表示されます。
- ステップ 3** **[Tech Support logs]** をクリックして、デバイスのテクニカルサポートログをダウンロードします。
-

Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーションホスティング

ここでは、Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーションホスティングについて説明します。

Cisco Catalyst アクセスポイントでのアプリケーションホスティングについて

仮想環境への移行により、再利用可能なポータブルかつスケーラブルなアプリケーションを構築する必要性が高まりました。アプリケーションのホスティングによって、管理者には独自の

ツールやユーティリティを利用するためのプラットフォームが与えられます。ネットワークデバイスでホスティングされているアプリケーションは、さまざまな用途に利用できます。これは、既存のツールのチェーンによる自動化から、設定管理のモニタリング、統合に及びます。

アプリケーションホスティングを使用すると、Catalyst Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。このリリースでは、Cisco IOS-XE ソフトウェアバージョン 17.3 以降を搭載した Cisco Catalyst 9100 シリーズ アクセスポイントでサードパーティ製 SES-imagotag IoT Connector アプリケーションを利用できます。

Cisco Catalyst 9100 シリーズ アクセスポイントの SES-imagotag IoT Connector は、あらゆる Electronic Shelf Label (ESL) 通信に対応しています。

Cisco Catalyst 9100 シリーズ アクセスポイントでの USB のインストールと管理のアプリケーションホスティングワークフロー

始める前に

デバイスでアプリケーションホスティングを有効にするには、次の前提条件を満たしている必要があります。

- Cisco Catalyst 9100 シリーズ アクセスポイントを検出するには、NETCONF を有効にし、ポートを 830 に設定します。
- Cisco Catalyst 9100 シリーズ アクセスポイントで IP が Catalyst Center に直接到達できることを確認します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco IOS XE 17.3.x 以降のソフトウェアが実行されていることを確認します。
- Catalyst Center アプライアンスが最新の Catalyst Center ISO を実行していることを確認します。
- USB ドングルが AP に挿入されていることを確認します。これは、SES-imagotag Connector アプリケーションを実行するために必要です。

ステップ 1 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco Catalyst 9100 シリーズ アクセスポイントのアプリケーションをホスティングするための準備状況を確認してから、アプリケーションをインストールください。

詳細については、[アプリケーションをホストするデバイスの準備状況の表示 \(26 ページ\)](#) を参照してください。

ステップ 2 Catalyst Center にアプリケーションホスティングサービスをインストールします。

詳細については、[アプリケーションホスティングサービスパッケージのインストールと更新 \(25 ページ\)](#) を参照してください。

ステップ 3 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Catalyst Center に追加します。

詳細については、[ネットワーク デバイスを追加](#)を参照してください。

(注) NETCONF が有効になっていることを確認し、ポートを 830 に設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが [Managed] 状態になるまで待機する必要があります。

ステップ 4 [Network Hierarchy] ウィンドウで AP をフロアに割り当てます。

詳細については、[フロアマップでの AP の操作](#)を参照してください。

ステップ 5 USB アプリケーション (SES-imagotag コネクタ) を Catalyst Center にアップロードします。

詳細については、[アプリケーションの追加 \(27 ページ\)](#) を参照してください。

ステップ 6 IoT サービスを有効にします。

詳細については、[Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化](#)を参照してください。

ステップ 7 『Application Hosting on Catalyst APs Deployment Guide』の説明に従って、コンテナを設定します。

<https://www.cisco.com/c/en/us/products/collateral/wireless/access-points/guide-c07-744305.html>

Cisco Catalyst 9100 シリーズ アクセスポイントにインストールされているホスティング アプリケーションの表示

始める前に

前提条件が満たされていることを確認してください。詳細については、「[アプリケーションホスティングの前提条件](#)」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [IoT Services]** の順に選択します。

ステップ 2 すべてのデバイスを表示するには、右上隅の **[All Devices]** をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して **[Manage]** をクリックします。

すべてのデバイスを表示することを選択した場合、**[All Devices]** ページには、アプリケーションをホストできるデバイスに関する情報 (**[Hostname]**、**[IP Address]**、**[Image Version]**、**[App Hosting Status]**、**[Last Updated]**) が表示されます。

(注) AP の **[App Hosting Status]** が **[Ready]** の場合、AP で更新を設定するには、必要なホスト名の横にあるチェックボックスをオンにして、**[Resync]** をクリックします。

特定のアプリケーションのデバイスのリストを表示することを選択した場合、**[Devices]** ページには、アプリケーションをホストできるデバイスに関する次の情報 (**ホスト名**、**デバイス IP**、**アプリケーションバー**

ジョン、アプリケーションステータス、最終検知プラットフォームバージョン、およびアクションステータス)が表示されます。

- ステップ 3** [Devices] ページで [Summary] をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。
- ステップ 4** [Action] ドロップダウンリストをクリックして、アプリケーションを開始、停止、編集、アップグレード、およびアンインストールします。
- ステップ 5** インストールされているホスティングアプリケーションを表示するデバイスリンクをクリックします。
- [Applications] ページには、インストールされているアプリケーションの名前、バージョン、アプリケーションステータス、IP アドレス、正常性、および詳細情報が表示されます。
- ステップ 6** [Details] 列で [View] をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。
- [App Details] ウィンドウには、アプリケーションのリソースおよびネットワーク情報が表示されます。
- ステップ 7** アプリケーションログをダウンロードするには、アプリケーションログをダウンロードするアプリケーションを選択し、[Application Logs] をクリックします。
- ステップ 8** テクニカルサポートログをダウンロードするには、テクニカルサポートログをダウンロードするアプリケーションを選択し、[Tech Support Logs] をクリックします。

Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9100 シリーズ AP からアプリケーションをアンインストールできます。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [IoT Services] の順に選択します。
- ステップ 2** アプリケーションを選択し、[Manage] をクリックして、そのアプリケーションを使用するデバイスを表示します。
- ステップ 3** アンインストールするアプリケーションがあるデバイスを選択します。
- ステップ 4** [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9100 デバイスからのアプリケーションの削除

Cisco Catalyst 9100 シリーズ AP からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、「[Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール](#)」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision] > [Services] > [IoT Services]** の順に選択します。

[IoT Services] ページで使用可能なホストされたアプリケーションを表示できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Application] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、CatalystCenterによって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。[Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、「[Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール](#)」を参照してください。

サイト間 VPN の設定

サイト間 VPN を作成し、既存のサイト間 VPN を編集または削除できます。

- [サイト間 VPN の作成 \(37 ページ\)](#)
- [サイト間 VPN の編集 \(38 ページ\)](#)
- [サイト間 VPN の削除 \(39 ページ\)](#)

サイト間 VPN の作成

この手順では、サイト間 VPN を作成する方法を示します。

始める前に

- ネットワーク階層内のサイトを定義します。[ネットワーク階層の概要](#)を参照してください。
- VPN トンネルに使用する IP アドレスプールを設定します。IP アドレスプールには、少なくとも 6 つの空き IP アドレスが必要です。[IP アドレス プールを設定する](#)を参照してください。

-
- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Site to Site VPN]。
サイト間 VPN は、このほかに [Workflows] > [Site to Site VPN] ウィンドウからも作成できます。
- ステップ 2** VPN を作成するには、[Add] をクリックします。
[Choose Your Sites] ワークフローが表示されます。
- ステップ 3** [Choose Your Sites] ワークフローで、次の手順を実行します。
- 最初のフィールドに VPN 名を入力します。
 - [Site 1] ドロップダウンリストから、最初のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。
 - [Site 2] ドロップダウンリストから、2 番目のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。
- ステップ 4** [Select Networks] ウィンドウで、次を実行します。
- [Tunnel IP Pool] ドロップダウンリストから、IP アドレスプールを選択します。
 - それぞれのサイトについて、使用するサブネットの横にあるチェックボックスをオンにします。
 - (オプション) サイトのカスタムネットワークを追加する場合は、下部にある [Add Custom Networks] リンクをクリックし、必要なフィールドに入力します。
- ステップ 5** [Configure VPN] ウィンドウで、次の手順を実行します。
- 暗号化の事前共有キーを入力します。
 - 必要に応じて、暗号化アルゴリズムと整合性アルゴリズムを設定します。デフォルトの設定を使用することを推奨します。設定を変更した場合にデフォルトの選択に戻すには、[Use Cisco recommended IKEV2 & Transform Set Values] チェックボックスをオンにします。
- ステップ 6** [Summary] ウィンドウで、VPN 設定を確認します。変更するには、[Edit] をクリックします。
- ステップ 7** 続行するには、[Create VPN] をクリックします。
次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services] をクリックして [Site to Site VPN] ウィンドウに戻ると、新しく作成した VPN が表示されます。
-

サイト間 VPN の編集

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Site to Site VPN]。
- ステップ 2** 編集する VPN の横にあるチェックボックスをオンにします。
- ステップ 3** リストの上方にあるメニューバーで [Edit] をクリックします。
- ステップ 4** [Summary] ウィンドウで、VPN 設定を確認します。変更するには、[Edit] をクリックします。
- ステップ 5** [Edit VPN] をクリックして変更を送信します。

次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services] をクリックして [Site to Site VPN] 画面に戻ります。

サイト間 VPN の削除

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Site to Site VPN]。

ステップ 2 削除する VPN の横にあるチェックボックスをオンにします。

ステップ 3 リストの上方にあるメニューバーで [Delete] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 4 [Yes] をクリックして、VPN を削除することを確認します。

ユーザー定義のネットワークサービスの作成

Catalyst Center では、[Cisco User Defined Network] サービスを、[Provision] > [Service Catalog] > [Cisco User Defined Network] ページから設定できます。[Configure Cisco User Defined Network] サービスは、このほかに [Workflows] > [Configure Cisco UDN] ページからも作成できます。詳細については、「[Cisco ユーザー定義のネットワークの設定](#)」の章を参照してください。

ユーザー定義のネットワークサービスのプロビジョニングステータスの確認

この手順では、Cisco ユーザー定義のネットワークサービスのプロビジョニングステータスを [Provision] > [All Services] ウィンドウから確認する方法を示します。Cisco ユーザー定義のネットワークサービスの設定が正常に完了した後に、[Configure Cisco User Defined Network] 画面で [View Provisioning Status] ボタンをクリックする方法もあります。

始める前に

Cisco ユーザー定義のネットワークサービスを [Workflows] > [Configure Cisco User Defined Network] ウィンドウから設定してプロビジョニングします。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [All Services] > [Cisco User Defined Network] の順に選択します。

[Site Provisioning Status] ウィンドウに、サイト名、デバイス名、使用されている SSID の数、およびサイトのプロビジョニングのステータスが表示されます。

ステップ2 [Refresh] をクリックすると、最新のプロビジョニングステータスが表示されます。

ステップ3 サイト名をクリックすると、プロビジョニングされたデバイスについて、SSID の名前、ユーザー定義ネットワーク (UDN) のステータス、ユニキャストトラフィックの封じ込めなどの追加の詳細が表示されます。

ステップ4 [Activities] をクリックすると、[Scheduled Tasks] ウィンドウでスケジュールされたタスクのステータスを追跡できます。

Cisco Umbrella の設定

ここでは、Cisco Umbrella と Catalyst Center との統合について説明します。

Cisco Umbrella について

Cisco Umbrella の DNS レイヤセキュリティにより、最も迅速かつ簡単にネットワークのセキュリティを強化できます。セキュリティの可視性を向上させ、侵害されたシステムを検出します。脅威がネットワークやエンドポイントに到達する前に阻止することにより、あらゆるポートやプロトコルでネットワーク内外を問わずユーザーを保護します。

Catalyst Center は、次のデバイス上の Cisco Umbrella 設定をサポートします。

- Cisco IOS-XE ソフトウェアバージョン 16.12 以降を搭載した Cisco Catalyst 9800 シリーズワイヤレスコントローラ
- Cisco Catalyst 9100 シリーズ AP
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9200 アクセススイッチ
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9300 アクセススイッチ

Cisco Umbrella のロールベース アクセス コントロールの設定

Catalyst Center で Cisco Umbrella を設定したり、ネットワークデバイスで Cisco Umbrella をプロビジョニングしたりするには、必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成する必要があります。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Manage Users」を参照してください。

表 1: Cisco Umbrella の RBAC 権限マトリックス

機能	アクセス	権限
Cisco Umbrella の設定 Catalyst Center	[Network Design] > [Advanced Network Settings]	書き込み

機能	アクセス	権限
システム 360 での Cisco Umbrella ダッシュレットの追加	[Network Design] > [Advanced Network Settings]	書き込み
ネットワークデバイスでの Cisco Umbrella のプロビジョニング	[Network Provision] > [Provision]	書き込み
	[Network Design] > [Network Hierarchy]	読み取り
	[Network Provision] > [Inventory Management]	読み取り
	システム	読み取り
	[Network Provision] > [Scheduler]	書き込み
	[Network Services] > [Umbrella]	書き込み

Cisco Umbrella の設定 Catalyst Center

始める前に

- Cisco Umbrella アカウントを作成します。
- login.umbrella.com にログインし、API キー、レガシートークン、管理キー、シークレットなどの必要なキーを作成します。
- Cisco Umbrella ログイン URL の組織 ID をメモします。
- Cisco Umbrella でローカルバイパスドメインを作成します。
- Catalyst Center と管理しているネットワークデバイスやソフトウェアアップデートをダウンロードする Cisco cloud との間にプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。詳細については、『[Catalyst Center Administrator Guide](#)』の「Configure the Proxy」セクションを参照してください。
- Catalyst Center で Cisco Umbrella パッケージをインストールします。『[Catalyst Center Administrator Guide](#)』の「Download and Install Packages and Updates」セクションを参照してください。
- 必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成します。[Cisco Umbrella のロールベース アクセス コントロールの設定 \(40 ページ\)](#) を参照してください。



(注) IPv6 で設定された Catalyst Center クラスタに Cisco Umbrella パッケージをインストールすることはできません。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** の順に選択します。

ステップ 2 Cisco Umbrella から手動で取得した次の詳細を入力します。

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

ステップ 3 [Save] をクリックします。

Umbrella ダッシュレットの追加

[System 360] ページに [Umbrella] ダッシュレットを追加できます。[Umbrella] ダッシュレットには、Catalyst Center での Cisco Umbrella の構成ステータスが表示されます。

始める前に

Cisco Umbrella パッケージをインストールする必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[System 360]** の順に選択します。

ステップ 2 [Actions] メニューから、[Edit Dashboard] を選択し、[Add Dashlet] をクリックします。

ステップ 3 [Umbrella Dashlet] を選択し、[Add] をクリックします。

[Umbrella] ダッシュレットが [System 360] ページの [Externally Connected Systems] に表示されます。Cisco Umbrella が Catalyst Center で設定されていれば、[Umbrella] ダッシュレットにステータスが [Available] と表示され、組織 ID が表示されます。

Cisco Umbrella が Catalyst Center で設定されていない場合は、[Configure] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のフィールドに値を入力できます。[Cisco Umbrella の設定 Catalyst Center \(41 ページ\)](#) を参照してください。

Cisco Umbrella でキーが変更された場合は、[Update] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のキーを更新できます。[Cisco Umbrella の設定 Catalyst Center \(41 ページ\)](#) を参照してください。

Umbrella サービス統計ダッシュボードの表示

[Umbrella Service Stats] ダッシュボードを表示するには、左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Umbrella] の順に選択します。

ダッシュボードには、次のダッシュレットが表示されます。

- [Total Umbrella DNS Queries]：選択したサイトでブロックされた DNS クエリと許可された DNS クエリの数を示します。
- [Blocked Umbrella DNS Queries]：選択したサイトでセキュリティポリシーおよびコンテンツポリシーによってブロックされた DNS クエリの数を示します。

デフォルトでは、このダッシュレットには過去 3 時間の統計情報が表示されます。過去 24 時間または 7 日間の統計情報を表示するには、[Umbrella Service Stats] ページの左上隅にあるドロップダウンリストからその目的の時間を選択します。

ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件

ネットワークデバイスで Cisco Umbrella をプロビジョニングする前に、次の点を確認します。

- Cisco Umbrella が Catalyst Center で設定されている。
- Cisco Umbrella をプロビジョニングするデバイスについて、ワイヤレスプロビジョニングが完了している。
- SSID 設定が非ファブリックである。
- デバイスが FlexConnect モードの非ファブリック SSID として設定されている場合、AP がプロビジョニングされている。
- デバイスからダイレクトインターネットアクセスで Cisco Umbrella への接続が確立されている。
- Cisco Umbrella ルート証明書は、Catalyst Center 信頼できる証明書バンドルで入手できません。『[Cisco DNA Center Administrator Guide](#)』のトピック「Configure Trusted Certificates」を参照してください。
- デバイスの Cisco Umbrella 設定が Catalyst Center から設定されていない場合は、デバイスから Cisco Umbrella 設定を削除し、デバイスを Catalyst Center と再同期する。

ネットワークデバイスでの Cisco Umbrella のプロビジョニング

始める前に

前提条件が満たされていることを確認してください。詳細については、[ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件](#) (43 ページ) を参照してください。



(注) 組織のネットワークでの Cisco Umbrella の展開は、login.umbrella.com からのみモニタできません。

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Workflows] > [Umbrella Deployment] の順に選択します。
または、次の手順を実行します。
- 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Umbrella] の順に選択します。
 - Cisco Umbrella を展開するサイトをネットワーク階層から選択します。
 - [Select Devices] ウィンドウが表示されます。手順 4 に進んで展開ワークフローを続けます。
- ステップ 2** タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。
- ステップ 3** [Choose Site] ウィンドウが表示されます。
- a) 各サイトのデバイスの準備状況が次のステータスで示されます。
- [Eligible Devices] : Cisco Umbrella の構成に適格なデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 (43 ページ) を参照してください。
 - [Enabled Devices] : Catalyst Center からすでに設定されているデバイス。
- b) 展開するサイトを選択し、[Next] をクリックします。
- (注) 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトに同時に Cisco Umbrella を展開できます。
- ステップ 4** [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。
- ステップ 5** [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。
- a) [Select Devices] ウィンドウで、有線デバイスを選択します。
- b) [Configure Interface] ウィンドウで、次の手順を実行します。
1. 設定するポートを選択し、[Define Umbrella Interfaces] をクリックします。
 2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。
- (注) 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。
- c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択します。

- d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。
- e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

ステップ 6 [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。

- a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択します。
- b) SSID を選択し、各 SSID に必要な Cisco Umbrella ポリシーを選択します。
(注)
 - このページには、非ファブリック SSID のみが表示されます。
 - SSID は選択し、Cisco Umbrella ポリシーは選択しない場合には、デフォルトポリシーが SSID にマッピングされます。
 - 複数のポリシーを選択した場合に、ポリシーが適用される順序は、Cisco Umbrella クラウドポータルに定義されています。
- c) [Umbrella Policy Association (Wireless)] ウィンドウで、SSID に適用されるデフォルトのポリシーを確認します。

SSID に関連付けられているポリシーを変更する場合は、[Cisco Umbrella] リンクをクリックします。Catalyst Center からの Cisco Umbrella の展開が完了すると、Cisco Umbrella コンソールにネットワークアイデンティティが表示されます。Cisco IOS-XE ソフトウェアバージョン 16.xx を搭載したデバイスの場合、ネットワークアイデンティティはグローバルと表示されます。Cisco IOS-XE ソフトウェアバージョンが 16.xx 以降のデバイスの場合、ネットワークアイデンティティは、サイトと SSID 名に基づいて作成されたカスタム名として表示されます。

ステップ 7 [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。

ステップ 8 [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。

- a) [DNS Crypt] ウィンドウで、[Next] をクリックします。
- b) DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。

ステップ 9 [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。

ステップ 10 続行するには、[Deploy] をクリックします。

ステップ 11 [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。

ステップ 12 続行するには、[Apply] をクリックします。

ステップ 13 [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

デバイスの Cisco Umbrella 展開ステータスと Cisco Umbrella でのデバイス構成ステータスを確認できます。Cisco Umbrella の展開ログは [Audit Logs] ウィンドウでも確認できます。

ネットワークデバイスでの Cisco Umbrella の無効化

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Workflows] > [Umbrella Deployment] の順に選択します。
- または、次の手順を実行します。
- 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Umbrella] の順に選択します。
 - Cisco Umbrella を無効にするサイトをネットワーク階層から選択します。
 - [Select Devices] ウィンドウが表示されます。手順 4 に進んで無効化ワークフローを続けます。
- ステップ 2** タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。
- ステップ 3** [Choose Site] ウィンドウが表示されます。
- a) 各サイトのデバイスの準備状況が次のステータスで示されます。
- [Ready Devices] : Cisco Umbrella 構成の前提条件を満たしているデバイス。 [ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 \(43 ページ\)](#) を参照してください。
 - [Not Ready Devices] : 前提条件を満たしていないデバイス。
 - [Enabled Devices] : Catalyst Center からすでに設定されているデバイス。
- b) 無効にするサイトを選択し、[Next] をクリックします。
- (注) 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が無効になります。
- ステップ 4** [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。
- ステップ 5** [Select Devices] ウィンドウで、[Enabled] タブをクリックし、デバイスを選択します。
- ステップ 6** [Disable] オプションボタンをクリックし、デバイスを選択します。
- ステップ 7** [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。
- ステップ 8** 続行するには、[Deploy] をクリックします。
- ステップ 9** [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。
- ステップ 10** 続行するには、[Apply] をクリックします。
- ステップ 11** [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

ネットワークデバイスでの Cisco Umbrella 設定の更新

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：[Workflows] > [Umbrella Deployment] の順に選択します。
- または、次の手順を実行します。
- 左上隅にあるメニューアイコンをクリックして次を選択します：[Provision] > [Services] > [Umbrella] の順に選択します。
 - Cisco Umbrella 構成を更新するサイトをネットワーク階層から選択します。
 - [Select Devices] ウィンドウが表示されます。手順 4 に進んで更新ワークフローを続けます。
- ステップ 2** タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。
- ステップ 3** [Choose Site] ウィンドウが表示されます。
- a) 各サイトのデバイスの準備状況が次のステータスで示されます。
- [Ready Devices] : Cisco Umbrella 構成の前提条件を満たしているデバイス。 [ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 \(43 ページ\)](#) を参照してください。
 - [Not Ready Devices] : 前提条件を満たしていないデバイス。
 - [Enabled Devices] : Catalyst Center からすでに設定されているデバイス。
- b) 更新するサイトを選択し、[Next] をクリックします。
- (注) 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が更新されます。
- ステップ 4** [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。
- ステップ 5** [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。
- a) [Select Devices] ウィンドウで、有線デバイスを選択し、[Update] オプションボタンをクリックします。
- b) [Configure Interface] ウィンドウで、次の手順を実行します。
1. ポートを選択し、[Define Umbrella Interfaces] をクリックします。
 2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。
- (注) 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。
- c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択し、[Next] をクリックします。

- d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。
- e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

- ステップ 6** [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。
- a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択し、[Update] オプションボタンをクリックします。
 - b) [Define Umbrella Policy Map (Wireless)] ウィンドウで SSID を選択し、マッピングする Cisco Umbrella ポリシーを選択するか、SSID の選択を解除して Cisco Umbrella を無効にします。
- ステップ 7** [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。
- ステップ 8** [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。
- DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。
- ステップ 9** [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。
- ステップ 10** 続行するには、[Deploy] をクリックします。
- ステップ 11** [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。
- ステップ 12** 続行するには、[Apply] をクリックします。
- ステップ 13** [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

セキュアなトンネルの設定

Catalyst Center で VPN トンネルの設定とデプロイが行えます。これにより、コーポレートオフィスとブランチオフィスを安全に接続できます。



(注) この機能は、現在、Cisco Catalyst 9300X シリーズ スイッチでのみサポートされています。

セキュアトンネルの設定

この手順を使用して、 n 日目にセキュアトンネルを計画および展開できます。

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Secure Tunnels]** の順に選択します。
- または、**[Workflows]** > **[Create Secure Tunnel]** ウィンドウからセキュアトンネルを作成することもできます。
- ステップ 2** **[Secure Tunnel]** ウィンドウで、**[Create Secure Tunnel]** をクリックします。
- ステップ 3** タスクの概要ウィンドウが開いたら、**[Let's Do it]** をクリックして、ワークフローに直接移動します。
- ステップ 4** **[Select Tunnel Type]** ウィンドウで、**[Site To Secure Access Service Edge (SIG/SASE)]** タイルをクリックして、作成するセキュアトンネルのタイプを選択します。
- これにより、Cisco Catalyst 9300X シリーズ スイッチとセキュア インターネット ゲートウェイの間にセキュアトンネルが作成されます。
- ステップ 5** **[Select Secure Internet Gateway]** ウィンドウで、ドロップダウンリストをクリックして**セキュア インターネット ゲートウェイ**を選択します。
- 選択したセキュア インターネット ゲートウェイについて、次のいずれかを実行します。
- **[Umbrella]** : Cisco Umbrella でトンネルを作成したことを確認します。後続の手順でトンネル ID と事前共有キーが必要になります。詳細については、[Cisco Umbrella の設定 Catalyst Center \(41 ページ\)](#) を参照してください。Cisco Umbrella ポータルにトンネルが作成されている場合は、確認チェックボックスをオンにします。
 - **[Zscaler]** : Zscaler ポータルでトンネルがすでに作成されていることを確認します。Zscaler でトンネルを作成した後、選択した Cisco Catalyst 9300X シリーズ スイッチでトンネルパラメータを設定するために、事前共有キーと定義済みの FQDN が必要になります。Zscaler ポータルにトンネルが作成されている場合は、確認チェックボックスをオンにします。
- ステップ 6** **[Choose Site and Device]** ウィンドウで、サイトとトンネルのマッピングについて次の手順を実行します。
1. **[Site]** のドロップダウンリストからサイトを選択します。
 2. **[Device]** のドロップダウンリストからデバイスを選択します。
 3. **[Number of Tunnels]** のドロップダウンリストから作成するトンネルの数を選択します。
 4. Zscaler の場合、**[Tunnel Type]** のドロップダウンリストからトンネルタイプを選択します。
 5. **[Tunnel Name]** にトンネル名を入力します。
 6. **[Tunnel Source Interface]** を選択します。
 7. トンネル IP に同じインターフェイスを使用する場合は、チェックボックスをオンにします。同じインターフェイスを使用しない場合は、チェックボックスをオフにして、**[Interface]** を選択します。
 8. **[Data Center Location]** にデータセンターの位置を入力します。
- ステップ 7** **[Define Tunnel Settings]** ウィンドウで、次の手順を実行します。
1. Umbrella の場合、**[Pre-Shared Key (PSK)]** に認証用の事前共有キー (PSK) を入力します。

2. セキュア インターネット ゲートウェイの統合が完了していない場合は、次の手順を実行します。
 1. [Tunnel ID] にトンネル ID を入力し、次のいずれかを選択します。
 1. [Fully Qualified Domain Name (FQDN)] : Cisco Umbrella で生成された **トンネル ID** または Zscaler で生成された **ユーザー ID** を使用します。
 2. [IP Address] : 接続先にする IP アドレスを使用します。
3. シスコ推奨の設定を使用するには、チェックボックスをオンにします。値をカスタマイズするには、チェックボックスをオフにします。

ステップ 8 [Configure Tunnel Traffic] ウィンドウで、トラフィックをルーティングするためのオプションを次から選択します。

- [Send all traffic] : すべてのトラフィックを IPSec トンネル経由で Umbrella に送信します。
- [Send Selected Traffic] : サブネットとサブネットの入力インターフェイスを入力します。+ をクリックすると、さらにサブネットを追加できます。

ステップ 9 [Schedule Task] ウィンドウで、トンネルを今すぐ作成するか、後でスケジュールするかを選択します。[Generate CLI Preview] を選択することもできます。

ステップ 10 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 11 [Create Secure Tunnel] をクリックします。

[Done!] ウィンドウが表示されます。

ステップ 12 [View all Tunnels] タブをクリックして、トンネル作成のステータスを表示します。

この処理には、しばらく時間がかかる場合があります。[Refresh] をクリックします。トンネルが起動すると、ステータスが [Provision] から [Up] に変わります。

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。