



## 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](#) (21 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](#) (29 ページ)
- [サイト間 VPN の設定](#) (33 ページ)
- [ユーザー定義のネットワークサービスの作成](#) (35 ページ)
- [Cisco Umbrella の設定](#) (38 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、Cisco DNA Center 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。

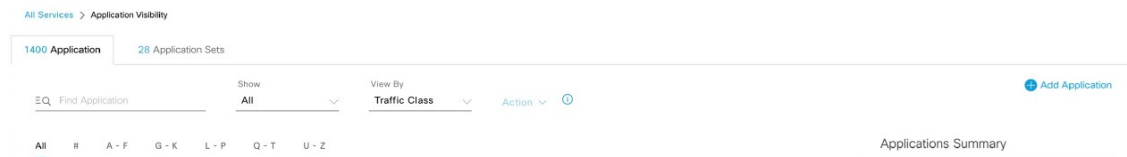
NBAR は、Cisco Catalyst 9000 デバイスでの最大 450 のインターフェイスのプロビジョニングをサポートしています。Cisco DNA Center のアプリケーション可視性は、この 450 インターフェイスの制限を超えません。

パッケージは必要に応じて任意にインストールできます。

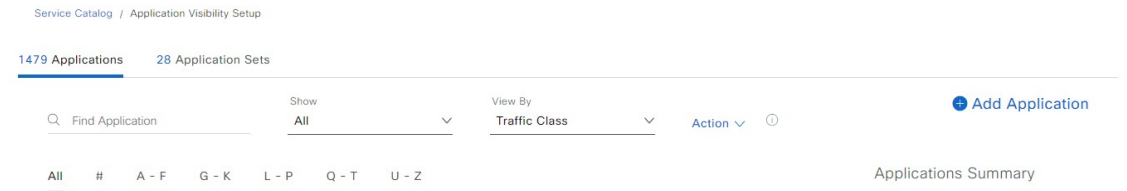


(注) 互換性を確保するには、上記のパッケージのパッケージバージョンが同じである必要があります。

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に、[Menu] アイコン (☰) をクリックして [Provision] > [Services] > [Application Visibility] の順に選択すると、[Application] タブと [Application Sets] タブが表示されます。



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、[Menu] アイコン (☰) をクリックして [Provision] > [Services] > [Application Visibility] の順に選択すると、[Application]、[Application Sets]、[Discover Applications] の各タブが表示されます。



アプリケーション可視性サービスには、次のフェーズがあります。

- Day 0 : 初回サービスの有効化。
- Day N : 継続的なモニタリングと設定の変更。

## アプリケーションの可視性サービスを有効にする Day 0 セットアップウィザード

Day 0 セットアップウィザードに従って、Cisco DNA Center でアプリケーションの可視性サービスを有効にします。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Services] > [Application Visibility] の順に選択します。

アプリケーションの可視性サービスの簡潔な概要を表示できます。

**ステップ 2** [Application Visibility] ページで [Next] をクリックします。

アプリケーションの可視性サービスを有効にするためのポップアップウィンドウが表示されます。ポップアップウィンドウで [Yes] をクリックして、Cisco DNA Center で CBAR を有効にします。

**ステップ 3** (オプション) [Enable CBAR on all Ready Devices] チェックボックスをオンにするか、[CBAR Readiness Status] が [Ready] 状態のデバイスを選択します。

CBAR を有効にする準備ができていないデバイスを選択する場合は、情報メッセージに従って [Ready] 状態に移行してからセットアップウィザードに進みます。

**ステップ 4** [Next] をクリックして、デバイスで CBAR を有効にします。

**ステップ 5** (オプション) Microsoft Office 365 クラウドコネクタなどの外部の信頼できるソースを選択すると、未分類のトラフィックの分類や、改善された署名の作成に役立ちます。

**ステップ 6** [完了 (Finish) ] をクリックします。

[Overview] ページには、アプリケーションレジストリ、デバイス認識方式、デバイスの CBAR の準備状況、過去 2、24、または 48 時間にネットワークで観察されたアプリケーション (CBAR が少なくとも 1 つのデバイスで有効になっている場合にのみ有効)、サービス正常性、および CBAR 正常性スコアのクイックビューが表示されます。

## Day-N アプリケーションの可視性ビュー

[Day-N Application Visibility] ページには、アプリケーションレジストリ、デバイス認識方式、デバイスの CBAR の準備状況、過去 2、24、または 48 時間にネットワークで観察されたアプリケーション (CBAR が少なくとも 1 つのデバイスで有効になっている場合にのみ有効)、および CBAR 正常性のクイックビューが表示されます。

次の表に、[プロビジョニング (Provision) ] > [サービス (Services) ] > [アプリケーションの可視性 (Application Visibility) ] の [概要 (Overview) ] タブに表示される情報を示します。

表 1: [Day-N Application Visibility] ビュー : チャート

グラフ	説明
レジストリ内のアプリケーション	<p>このチャートには、Cisco DNA Center アプリケーションレジストリ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"> <li>• [Custom] : ユーザーによって追加されたアプリケーション</li> <li>• [Built-in]: インストールされているアプリケーション Cisco DNA Center</li> <li>• [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</li> </ul>
ネットワークで確認されたアプリケーション	<p>このチャートには、過去 2 時間、24 時間、または 48 時間に観察されたアプリケーションが表示され、ネットワークトラフィック率が最も高いアプリケーションが一覧表示されます。</p> <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>
アクティブな認識方法によるデバイス	<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"> <li>• CBAR 対応デバイス : ルータとスイッチ</li> <li>• 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、および Cisco Catalyst 9800 シリーズワイヤレスコントローラ</li> <li>• IP/ポートベースのデバイス : スイッチ</li> <li>• サポートされていないデバイス : 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</li> </ul>
CBAR 準備状況ステータス	<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"> <li>• [Enabled] : CBAR が有効になっているデバイス</li> <li>• [Ready] : CBAR を有効にする準備が整っているデバイス</li> <li>• [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</li> <li>• [Not Supported] : CBAR をサポートしていないデバイス</li> </ul>

グラフ	説明
<b>Service Health and CBAR Health</b>	<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> <p>このウィジェットには、サービスの問題と修復 (P1、P2、および P3) も表示されます。緑色のチェックマークは、正常なサービスを示します。赤色の X マークは、少なくとも 1 つの P1 の問題を示します。警告アイコンは、少なくとも 1 つの P2 の問題を示します。P1、P2、および P3 をクリックすると、サービスの問題と修復についての詳細が表示されます。</p>
<b>CBAR 正常性の問題と修復</b>	<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"> <li>• エラー (P1)</li> <li>• 警告 (P2)</li> <li>• その他 (P3)</li> </ul> <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>

[Site Devices Table] : このテーブルには、デバイスの情報とステータスが表示されます。[Quick Filter] および [Device Table Filter] を使用して、デバイスをフィルタ処理できます。

表 2 : [Day-N Application Visibility] ビュー : [Site Devices Table]

カラム	説明
<b>[Device Name]</b>	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。
<b>[Management IP]</b>	デバイスの IP アドレス。
<b>デバイス タイプ</b>	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。
<b>Site</b>	デバイスに割り当てられているサイト。

カラム	説明
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。Cisco DNA 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。
展開ステータス	CBAR の展開ステータスが表示されます。
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。
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。

## 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。Cisco DNA 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 RFC 4594 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。

Cisco DNA 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。

Cisco DNA 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、Cisco DNA Center に追加するアプリケーションです。カスタムアプリケーションの横にはオレンジ色のバーが表示され、標準 NBAR2 アプリケーションおよびアプリケーションセットと区別されます。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。Cisco DNA 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。

Cisco DNA 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、Cisco DNA 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、Cisco DNA 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、Cisco DNA Center を Microsoft Office 365 クラウドコネクタなどの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。



---

(注) Microsoft Office 365 クラウドコネクタを設定する前に、NBAR 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

Cisco DNA 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せん。

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。

### アプリケーション設定の変更

既存の NBAR 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] > [Application] の順に選択します。

**ステップ 2** [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 3** [アプリケーション名 (Application Name)] をクリックします。

**ステップ 4** 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 5 [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

Cisco DNA 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 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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 ダイアログボックスで、次のフィールドに必要な情報を入力します。

フィールド	説明
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。
サーバー名	アプリケーションをホストするサーバーの名前。
Similar to	類似する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。Cisco DNA 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。
トラフィッククラス	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。

フィールド	説明
アプリケーションセット	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 [OK] 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

Cisco DNA 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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。Cisco DNA 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** [OK] 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

Cisco DNA 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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** [OK] 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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。

- a) 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 \(10 ページ\)](#)、[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 \(11 ページ\)](#)、または[URL に基づくカスタム アプリケーションの作成 \(12 ページ\)](#) を参照してください。
- b) [OK] をクリックします。

(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。

## 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 \(8 ページ\)](#)」を参照してください。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Services] > [Application Visibility] 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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** ダイアログ ボックスに、新しいアプリケーション設定の名前を入力します。

Cisco DNA 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** [OK] をクリックします。

**ステップ 6** [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 7** 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 8** 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 9** 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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。

## 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。

### 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](http://cisco.com) で使用可能である必要があります。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] の順に選択します。

**ステップ 2** Day-N の [Overview] ページで、下にスクロールして、[Site Devices] テーブルを表示します。

**ステップ 3** [Site Devices] テーブルの [Protocol Pack Version] カラム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、[All Devices] を選択し、後続の警告ポップアップウィンドウで [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、[Selected Devices] を選択し、後続の警告ポップアップウィンドウで [Yes] をクリックします。

## 未分類アプリケーションの検出

Cisco DNA 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] の順に選択します。

**ステップ 2** [Discover Applications] タブをクリックします。

**ステップ 3** [Recommendations] の下の [discovered server names] リンクまたは [discovered IP/Ports] リンクをクリックします。



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] > [Discovered] を選択して、インポートされたアプリケーションを確認します。

## NBAR クラウドコネクタの設定

アプリケーション可視性サービスでは、NBAR クラウドコネクタ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 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] の順に選択します。
- ステップ2 [Discover Applications] タブをクリックします。
- ステップ3 [NBAR Cloud] ウィンドウで、[Configure] をクリックします。
- ステップ4 [Configure NBAR Cloud] ウィンドウで、トグルボタンをクリックして状態を [Enable] にします。
- ステップ5 [Cisco API Console] リンクをクリックして、キーとクライアントシークレットを取得します。
- ステップ6 Cisco ログイン情報を入力して新しいブラウザタブで [Cisco API Console] を開き、次の手順を実行します。
  - a) [My Apps & Keys] タブで、[Register a New App] をクリックします。
  - b) [Register an Application] 画面の次のフィールドに入力します。
    - [Name of Your Application] : アプリケーション名を入力します。
    - [OAuth2.0 Credentials] : [Client Credentials] チェックボックスをクリックします。
    - [Select APIs] : [Hello API] チェックボックスをクリックします。
  - c) [Register] をクリックします。

登録したアプリケーションの詳細が [My Apps & Keys] タブに表示されます。
  - d) 登録したアプリケーションのキーとクライアントシークレットを [Cisco API Console] からコピーします。
- ステップ7 [Configure NBAR Cloud] ウィンドウで、コピーしたキーとクライアントシークレットを入力します。
- ステップ8 [Configure NBAR Cloud] で、次のようにフィールドを設定します。
  - a) 組織名を入力します。

- b) [Improve my network using NBAR Cloud telemetry] チェックボックスをオンにします。
- c) [NBAR classification telemetry data is being sent to region] チェックボックスで目的のロケーションを選択します。

ステップ 9 [Save] をクリックします。

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

Cisco DNA 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 Cisco DNA Center とテレメトリデータを共有します。

Cisco DNA 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：

- 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。



(注) Cisco DNA トラフィック テレメトリアプライアンスでは、アプリケーションポリシー サポートを使用できません。

## Infoblox アプリケーションの検出

Cisco DNA 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 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] の順に選択します。

ステップ 2 [Discover Applications] タブをクリックします。

ステップ 3 [Infoblox DNS Server] の [Configure] をクリックします。

- ステップ 4** [Infoblox Connector Settings] ウィンドウで [Here] リンクをクリックして、Cisco DNA 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 5** 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 6** [Infoblox Connector Settings] に戻り、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 7** [保存 (Save) ] をクリックします。
- [Poll Infoblox to Import Applications] リンクが [Recommendations] の下に表示されます。
- ステップ 8** [Poll Infoblox to Import Applications] リンクをクリックして、[Infoblox Connector Settings] で設定した DNS ゾーンからアプリケーションのリストを取得します。
- ステップ 9** 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 Connector Settings] 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 10** [Import] をクリックします。
- ステップ 11** [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 Discovered Applications] 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。

## Microsoft Office 365 クラウドコネクタを使用した未分類トラフィックの解決

Cisco DNA Center は、Microsoft Office 365 クラウドコネクタなどの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するか、または改善された署名を生成できるようにします。

### 始める前に

- Cisco DNA Center がインターネットに接続していることを確認します。
- NBAR クラウドが有効になっていることを確認します。

---

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] の順に選択します。

**ステップ 2** [Discover Applications] タブをクリックします。

**ステップ 3** [MS Office 365 Cloud] トグルボタンをクリックして、MSFT シグニチャのポーリングを有効にします。

- Microsoft Office 365 コネクタを有効にすると、コントローラは Microsoft Office 365 から新しいドメインの情報のインポートを開始し、新しいドメインに適したアプリケーションを検出します。
- 新しいセカンダリパックは、Cisco DNA Center ベースのプロトコルパックとともにインストールされ、新しいドメインが自動的にサポートされます。

---

## 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [Application Visibility] 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]、[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。

- a) 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。
- b) [OK] 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、アプリケーションのボックスで  をクリックし、[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、Cisco DNA 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 16.12.1s を搭載した Cisco Catalyst 9300 シリーズスイッチと、Cisco IOS-XE ソフトウェアバージョン 17.3.1 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 Docker アプリケーションを利用できます。

アプリケーションホスティングのアプリケーションスタックで使用されるディスク容量を制限するために、Cisco DNA Center でサポートされるアプリケーションの数は8つまでになっています。

## 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** Cisco DNA Center GUI で [Menu] アイコン () をクリックして選択します[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 Cisco DNA 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 Cisco DNA 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。

- デバイスの HTTPS ログイン情報を設定します。デバイスを手動で Cisco DNA Center に追加するときに HTTPS ログイン情報を設定するか、デバイスのログイン情報を編集できます。詳細については、「[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。
- ユーザー認証用にローカルの認証サーバーまたは AAA 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 EXEC モード（レベル 15）で設定する必要があります。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Configure Authentication and Policy Servers」を参照してください。
- 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。



(注) アプリケーションホスティングの HA は、3 ノードの Cisco DNA Center クラスタ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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [App Hosting] 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。ステータスに [Not Ready] と表示されている場合は、ステータスをクリックして理由を確認できます。

## 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] アプリケーション：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] アプリケーション：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、次のコマンドを使用します。

```
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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [IoT Services] 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 [Category] 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、Cisco DNA 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-4.1.0.cisco.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

Cisco DNA 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [IoT Services] の順に選択します。

[App Hosting] ページに使用可能なアプリケーションを表示できます。

**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 Application] をクリックします。

**ステップ 4** ドロップダウンリストからアプリケーションの [Type] と [Category] を選択します。

**ステップ 5** [Select] をクリックして、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 6** [Upload] をクリックします。

## アプリケーションの起動

Cisco DNA Center でアプリケーションを起動できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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、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** アプリケーションを起動す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

Cisco DNA Center でアプリケーションを停止できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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、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** アプリケーションを停止す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

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](#)」を参照してください。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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。
- (注)
- 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 (ホスト名、IP アドレス、アプリケーションのホスティングステータス、最終更新日) 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] 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** 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] 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、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, Cisco DNA 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、この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。
- [App Details] ウィンドウには、アプリケーションのリソース、ネットワーク、および Docker ランタイムオプション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

Cisco DNA 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す。

### 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 \(22 ページ\)](#)」を参照してください。
- アプリケーションを Cisco DNA 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 \(23 ページ\)](#)」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 \(22 ページ\)](#)」を参照してください。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [App Hosting] 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** 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。

**ステップ 4** [Configuration App] タブで次の設定を入力します。

#### • App Networking

- [Device Network] : [Select Network] 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設定する VLAN を選択します。
- [App IP address] : [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。
- [Resource Allocation] : [Allocate all resources available on a device] または [Customize resource allocation] チェックボックスをクリックします。[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。
- (オプション) [Custom Settings] : Cisco パッケージアプリケーションにのみ適用可能です。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。
- (オプション) [App Data] : アプリケーション固有のファイルを参照し、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を特定するには、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 5** [Next] をクリックして、[Confirm] 画面でアプリケーション設定を確認します。

**ステップ 6** [完了 (Finish)] をクリックします。

**ステップ 7** インストールの [Confirmation] ウィンドウで [Yes] をクリックして、選択した Cisco Catalyst 9300 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。

#### 次のタスク

アプリケーションをインストールすると、デバイスの 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正常に完了したら、**テンプレートエディタ**を使用して実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

## 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [App Hosting] 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** アプリケーションをアンインストールす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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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

Cisco DNA 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 \(27 ページ\)](#) を参照してください。

---

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Services] > [App Hosting] の順に選択します。

[App Hosting] 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、Cisco DNA 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 \(27 ページ\)](#) 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 Cisco DNA Center からダウンロードできます。

---

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[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、Cisco DNA 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、Cisco DNA 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** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[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、Cisco DNA 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 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 に設定する必要があります。
- Cisco Catalyst 9100 シリーズ アクセス ポイントでは、IP が Cisco DNA Center に直接到達できることが必要です。
- 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。
- Cisco DNA Center アプライアンスが最新の Cisco DNA 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 \(22 ページ\)](#) を参照してください。

**ステップ 2** Cisco DNA 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 \(21 ページ\)](#) 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 Cisco DNA 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、[AP の追加、配置、および削除](#)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 Cisco DNA 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（23 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](#)」を参照してください。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[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。
- (注)
- 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（ホスト名、IP アドレス、アプリケーションのホスティングステータス、最終更新日）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] 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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** アプリケーションをアンインストールす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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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、Cisco DNA 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。  
[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

この手順では、サイト間VPNを **[Provision]** > **[All Services]** ウィンドウから作成する方法を示します。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。

#### 始める前に

- ネットワーク階層内のサイトを定義します。[ネットワーク階層について](#)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** Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして選択します **[Provision]** > **[Site to Site VPN]**。
- 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** 最初のフィールドに VPN 名を入力します。
- ステップ 4** **[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。
- ステップ 5** **[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 6** **[Next]** をクリックして **[Select Networks]** 画面に進みます。
- ステップ 7** **[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。
- ステップ 8** 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。
- ステップ 9** (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 10** **[Next]** をクリックして **[Configure VPN]** 画面に進みます。

- ステップ 11** 暗号化の事前共有キーを入力します。
- ステップ 12** 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 13** [Next] をクリックして [Summary] 画面に進みます。
- ステップ 14** VPN 設定を確認し、変更が必要な場合は該当するセクションで [Edit] をクリックします。
- ステップ 15** [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] 画面に戻ると、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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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。
- [Summary] 画面が表示されます。

**ステップ 4** VPN 設定を確認し、変更が必要な場合は該当するセクションで [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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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

ここでは、Cisco DNA Center の **[Provision]** > **[Services]** ウィンドウから Cisco ユーザー定義のネットワークサービスを設定してサイトのプロビジョニングのステータスを確認する方法を示します。

## ユーザー定義のネットワークサービスの作成

この手順では、Cisco ユーザー定義のネットワークサービスを **[Provision]** > **[Services]** > **[Cisco User Defined Network]** ウィンドウから設定する方法を示します。ユーザー定義のネットワークサービスは、このほかに **[Workflows]** > **[Configure Cisco User Defined Network]** ウィンドウからも作成できます。

### 始める前に

- ネットワーク階層内のサイトを定義します。
- Cisco DNA Center Cloud アプリケーションを使用して認証トークンが生成されていることを確認します。

---

**ステップ 1** Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして選択します **[Provision]** > **[Services]** > **[Cisco User Defined Network]** の順に選択します。

**ステップ 2** ユーザー定義のネットワークサービスを作成するには、**[Add Sites]** をクリックします。

**[OK, now let's complete the connection with the cloud service]** ワークフローが表示されます。

**ステップ 3** Cisco DNA Center Cloud で生成してコピーした認証トークンを **[Authentication Token]** テキストボックスに貼り付け、**[Connect]** をクリックします。

トークンの検証に成功すると、「Connection validated, click Next to proceed」というメッセージが表示されます。

トークンの検証に失敗した場合は、**[Retry]** をクリックし、認証トークンを再度入力して **[Connect]** をクリックします。

**ステップ 4** **[Next]** をクリックして、Cisco ユーザー定義のネットワークサービスを有効にするサイトを選択します。

**ステップ 5** **[Select Sites]** ドロップダウンリストからサイトを選択します。

**ステップ 6** **[Disable User Defined Network Service]** チェックボックスをオンにすると、ユーザー定義のネットワークサービスがすべてのサイトで無効になります。

**ステップ 7** **[Next]** をクリックして、選択したサイトの SSID を選択します。

前の手順で選択したすべてのサイトについて、プロビジョニングされている非ファブリック SSID が表示されます。

**ステップ 8** **[SSID(s)]** ドロップダウンリストから SSID を選択します。

- ステップ 9** 選択した SSID のユニキャストトラフィックを制限するには、[Unicast Traffic Containment] ボタンをオンにします。
- ステップ 10** ユニキャストトラフィックの封じ込めを特定のサイトに適用するには、[Apply Individually] をクリックします。
- ステップ 11** ユニキャストトラフィックの封じ込めをすべてのサイトに適用するには、[Apply to all] をクリックします。
- ステップ 12** [Next] をクリックします。
- ステップ 13** Cisco ユーザー定義のネットワークサービスをネットワークですぐにプロビジョニングするか、後でプロビジョニングするようにスケジュールするかを選択します。
- ネットワークでの 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をすぐに行う場合は、[Now] オプションボタンをクリックし、[Next] をクリックします。
  - ネットワークでの 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を後で行うようにスケジュールする場合は、[Later] オプションボタンをクリックして日付と時刻を定義し、[Next] をクリックします。

[Configuration Summary] 画面が表示されます。

- ステップ 14** Cisco ユーザー定義のネットワークサービスの設定を確認し、変更が必要な場合は該当するセクションで [Edit] をクリックします。
- ステップ 15** [構成] をクリックします。
- 次の画面では、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。
- ステップ 16** [View Provisioning Status] をクリックして、プロビジョニングステータスを確認します。
- 詳細については、[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 \(36 ページ\)](#) 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します **[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** [Activity] 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。

## スイッチでのテレメトリの有効化

スイッチでスイッチポートアナライザ (SPAN) およびカプセル化リモート スイッチ ポートアナライザ (ERSPAN) セッションを設定して、アプリケーションアシュアランスとエンドポイント分析のために IP トラフィックを共有することができます。

### 始める前に

スイッチとトラフィック テレメトリ アプライアンス (TTA) が到達可能であり、Cisco DNA Center を介して管理されていることを確認します。スイッチは、サイトに割り当てられており、デバイスロールが [Distribution] である必要があります。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します **[Provision] > [Services] > [Service Catalog] > [Telemetry Appliance Setup]** の順に選択します。

**ステップ 2** [+ Setup] をクリックして新しいワークフローを作成します。  
[Get Started] ウィンドウが表示されます。

**ステップ 3** ワークフロー名と説明を入力します。

**ステップ 4** [Next] をクリックします。

**ステップ 5** [Choose Source Endpoint] ウィンドウで、テレメトリアプライアンスにトラフィックを送信するデバイスを選択します。

(注) スイッチとハブは、[Distribution] ロールによって管理されるワークフローでサポートされる送信元デバイスです。

**ステップ 6** [Next] をクリックします。

**ステップ 7** [Choose Destination Endpoint] ウィンドウで、宛先エンドポイントとして TTA デバイスを選択します。

(注) リストから選択できる TTA デバイスは 1 つだけです。

**ステップ 8** [Next] をクリックします。

**ステップ 9** [Choose Type for Configuration] ウィンドウで、[SPAN] または [ERSPAN] を選択します。

**ステップ 10** [Next] をクリックします。

**ステップ 11** [Choose Mapping Between Source and Destination] ウィンドウで、次の手順を実行します。

SPAN の場合 :

1. 着信トラフィックをモニタする送信元インターフェイスを選択します。
2. トラフィック テレメトリ アプライアンスが接続された、トラフィックを転送できるスイッチの宛先インターフェイスを選択します。
3. 着信トラフィックを処理するレシーバインターフェイスを選択し、分析を行います
4. [Next] をクリックします。

ERSPAN の場合 :

1. 着信トラフィックをモニタする送信元インターフェイスを選択します。
2. 着信トラフィックをフィルタ処理する VLAN を入力します。
3. 着信トラフィックを処理するレシーバインターフェイスを選択し、分析を行います
4. レシーバインターフェイスの宛先 IP を入力します。
5. レシーバインターフェイスの宛先ネットマスクを入力します。
6. [Next] をクリックします。

**ステップ 12** [Scheduler] ウィンドウで、[Now] をクリックしてただちに設定を開始するか、[Later] をクリックして特定の時間に設定をスケジュールします。

**ステップ 13** [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

**ステップ 14** [View Status] をクリックして、個々のデバイスのプロビジョニングステータスを確認します。

## Cisco Umbrella の設定

ここでは、Cisco Umbrella と Cisco DNA 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。

Cisco DNA Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco IOS-XE ソフトウェアバージョン 16.12 以降および Cisco Catalyst 9100 シリーズ アクセス ポイントで Cisco Umbrella 構成をサポートしています。

## Cisco Umbrella のロールベース アクセス コントロールの設定

Cisco DNA 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 3: 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 Cisco DNA Center	[Network Design] > [Advanced Network Settings]	書き込み
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 Cisco DNA Center

### 始める前に

- Cisco Umbrella アカウントを作成します。
- [login.umbrella.com](https://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。
- Cisco DNA 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、『[Cisco DNA Center Administrator Guide](#)』の「Configure the Proxy」セクションを参照してください。

- Cisco DNA Center で Cisco Umbrella パッケージをインストールします。『[Cisco DNA 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 \(39 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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、Cisco DNA 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** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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 Cisco DNA 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 Cisco DNA 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 Cisco DNA Center (39 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 Cisco DNA Center (39 ページ) を参照してください。

## [Umbrella Service Stats] 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、Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision]>[Services]>[Umbrella] の順に選択します。

[Umbrella Service Stats] 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、次の前提条件を満たす必要があります。

- Cisco Umbrella が Cisco DNA Center で設定されていることを確認します。
- 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ことを確認します。
- SSID 設定が非ファブリックであることを確認します。
- 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は、アクセスポイントがプロビジョニングされていることを確認します。
- デバイスの Cisco Umbrella 設定が Cisco DNA 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 Cisco DNA Center と再同期します。
- 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ことを確認します。

- Cisco Umbrella ルート証明書が Cisco DNA Center trustpool で使用可能であることを確認します。『[Cisco DNA Center Administrator Guide](#)』の「Configure Trustpool」を参照してください。

## 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

[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 \(41 ページ\)](#) を完了します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Workflows] > [Umbrella Deployment] の順に選択します。

または、次の手順を実行します。

- Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Services] > [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** [Let's Start] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Choose Site] ウィンドウが表示されます。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 \(41 ページ\)](#) を参照してください。
- [Enabled Devices] : Cisco DNA Center からすでに設定されているデバイス。

**ステップ 3** 展開するサイトを選択し、[Next] をクリックします。

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 Devices] ウィンドウで、準備が完了しているデバイスを選択し、[Next] をクリックします。

**ステップ 5** 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、Umbrella クラウドポータルに定義されています。

- ステップ 6** [Next] をクリックし、[Umbrella Policy Association] 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。Cisco DNA 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。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。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** [Next] をクリックして、Cisco Umbrella で設定されている内部ドメインを確認します。
- [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** [Next] をクリックします。
- [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。
- ステップ 9** [DNS Crypt] ウィンドウで、[Next] をクリックします。
- 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て [Next] をクリックします。
- ステップ 10** [Summary] ウィンドウで Umbrella 展開構成を確認し、変更が必要な場合は [Edit] をクリックします。
- ステップ 11** [展開 (Deploy) ] をクリックします。
- [Schedule] ウィンドウが開き、[Now] と [Later] のオプションが表示されます。
- ステップ 12** [Schedule] ウィンドウで、次のいずれかを実行します。
- 構成をすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
  - 構成を後で展開するには、[Later] オプションボタンをクリックし、[Task Name] と [Start Date and Time] を指定して [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] ページ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] ページでも確認できます。



(注) 組織のネットワークでの Cisco Umbrella の展開は、[login.umbrella.com](https://login.umbrella.com) でのみモニターできません。

## ネットワークデバイスでの Cisco Umbrella の無効化

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Workflows] > [Umbrella Deployment] の順に選択します。  
または、次の手順を実行します。
- Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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** [Let's Start] をクリックします。  
今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。  
[Choose Site] ウィンドウが表示されます。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 \(41 ページ\)](#) 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] : Cisco DNA Center からすでに設定されているデバイス。
- ステップ 3** 無効にするサイトを選択し、[Next] をクリックします。  
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、[Next] をクリックします。
- 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** [Next] をクリックします。
- ステップ 8** [Summary] ウィンドウで、[Deploy] をクリックします。
- ステップ 9** [Schedule] ウィンドウで、次のいずれかを実行します。
- 構成をすぐに無効にするには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
  - 構成を後で無効にするには、[Later] オプションボタンをクリックし、[Task Name] と [Start Date and Time] を指定して [Apply] をクリックします。
- ステップ 10** [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ページで展開ステータスを確認します。

Cisco Umbrella の展開ログは、[Audit Logs] ページで確認できます。

## ネットワークデバイスでの Cisco Umbrella 設定の更新

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[**Workflows**] > [**Umbrella Deployment**] の順に選択します。
- または、次の手順を実行します。
- Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[**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** [Let's Start] をクリックします。
- 今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。
- [Choose Site] ウィンドウが表示されます。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 (41 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。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 (41 ページ) を参照してください。
  - [Enabled Devices] : Cisco DNA Center からすでに設定されているデバイス。
- ステップ 3** 更新するサイトを選択し、[Next] をクリックします。
- 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 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 5** [Update] 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 6** [Next] をクリックします。
- ステップ 7** [Define Umbrella Policy Map] 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 8** [Summary] ウィンドウで、[Deploy] をクリックします。
- ステップ 9** [Schedule] ウィンドウで、次のいずれかを実行します。
- 構成をすぐに更新するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

- 構成を後で更新するには、[Later] オプションボタンをクリックし、[Task Name] と [Start Date and Time] を指定して [Apply] をクリックします。

**ステップ 10** [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ページで展開ステータスを確認します。

Cisco Umbrella の展開ログは、[Audit Logs] ページで確認できます。

---

## 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。