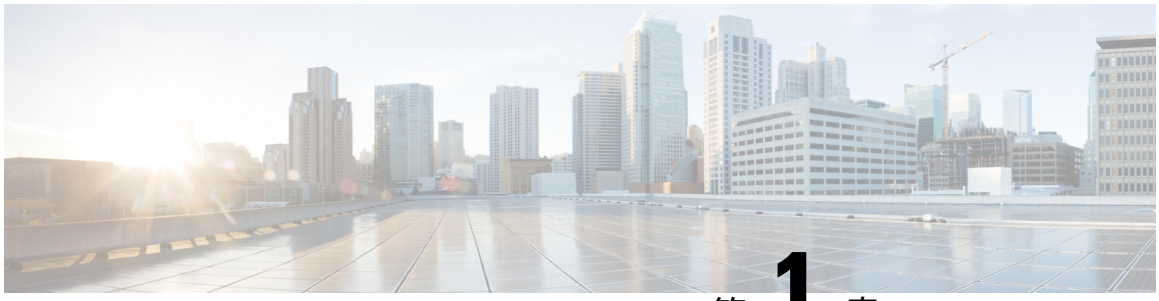
Cisco DNA Center リリース 2.2.3 ユーザーガイド

初版：2021 年 8 月 4 日

最終更新：2022 年 11 月 10 日

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

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 *1 : Cisco DNA Center* リリース *2.2.3* の新機能および機能変更

機能	説明	参照先
アプリケーションポリシーのアプリケーション QoS ポリシーとしての再ブランディング	アプリケーションポリシーのナビゲーションメニューが、**[Policy]** > **[Application]** から **[Policy]** > **[Application QoS]** に変更されました。	アプリケーション ポリシーの管理
QoS ポリシーなしでのデバイスのカスタムアプリケーションの定義	QoS ポリシーを設定せずに、Cisco DNA 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。	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 （510 ページ）
アプリケーションポリシーのサポート	アプリケーションポリシーのサポートを Cisco Catalyst IE3300 シリーズおよび IE3400 シリーズ スイッチで利用できます。	—
トポロジマップの共有	トポロジビューを他のユーザーと共有することができます。	トポロジマップレイアウトの共有
コンプライアンス	デバイスのスタートアップ構成と実行構成が一致しない場合は、[Inventory] ウィンドウの **[Action]** > **[Compliance]** で、コンプライアンスチェックを実行し、複数のデバイス間で実行構成を同期できます。	デバイスのスタートアップ設定と実行中の設定の同期

新機能および変更された機能に関する情報

機能	説明	参照先
コントローラの RADIUS プロファイリング設定	エンタープライズ SSID で RADIUS クライアント プロファイリングを有効にすることができます。	エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）
デバイス クレデンシャルの管理	ログイン情報を作成または編集したり、割り当てたり、デバイスに適用することができます。	デバイス クレデンシャルの管理
スイッチでのテレメトリの有効化	SPAN および 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。	スイッチでのテレメトリの有効化
セキュリティアドバイザリの修正バージョン	[Fixed Versions] 列が [Security Advisories] ウィンドウに追加されました。この列には、セキュリティアドバイザリの既知の最小修正済みバージョンがリストされます。この列に示されているバージョンにアップグレードすることで、デバイス上のアドバイザリを削除できます。	セキュリティアドバイザリの表示 （252 ページ）
イメージ配信サーバーのプロトコル順序の変更	イメージ配信サーバーのプロトコル順序を変更することで、ソフトウェアイメージ配信に必要なプロトコルを選択できます。プロトコルの順序は、イメージ配信サーバーで検証チェックを実行するのに役立ちます。	イメージ配信サーバーのプロトコル順序の変更
RCM クライアントの拒否	Cisco DNA Center で、ランダム MAC アドレスを使用しているクライアントがネットワークに参加できないようにします。エンタープライズ SSID とゲスト SSID を作成するときに、ランダム MAC アドレスを持つクライアントを拒否するか許可するかを選択できます。	エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ） ゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）
フラッシュクリーンアップ	ソフトウェアイメージをプロビジョニングするとき、または ISSU を使用してソフトウェアイメージをアップグレードするときに、実行中のソフトウェアイメージだけを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除できます。	ソフトウェア イメージのプロビジョニング （109 ページ） ISSU を使用したソフトウェアイメージのアップグレード
イメージ更新タスクの再試行	失敗したイメージ更新タスクについて、イメージ更新を再試行できます。	イメージ更新ステータスの表示 （112 ページ）

新機能および変更された機能に関する情報

機能	説明	参照先
ポート アクション	ポートのMACアドレスをクリアしてシャットダウンできます。error-disabled ポートをアクティブにするには、MACアドレスをクリアしてからポートをシャットダウンします。	インベントリに関する情報の表示（53 ページ）
テンプレートとモデル構成のさまざまなビュー	スイッチングまたはワイヤレスのネットワークプロファイルを作成するときに、[Cards] ビューまたは [Table] ビューでテンプレートとモデル構成を表示できます。	テンプレートのネットワークプロファイルへの関連付け （224 ページ）
AAA RADIUS 属性の新しいモデル構成設計	Cisco AireOS コントローラおよびCisco Catalyst 9800 シリーズ ワイヤレス コントローラで設定される AAA RADIUS **Called-station-id** パラメータは、ap-macaddress-ssid 属性値に制限されなくなりました。AAA RADIUS 属性のモデル構成を作成し、属性値のリストから選択できるようになりました。	AAA RADIUS 属性のモデル設定設計の作成 （228 ページ）
AAA オーバーライドの FlexConnect VLAN マッピング	FlexConnect 展開では、ローカルでスイッチされるクライアントの動的 VLAN 割り当て用に AAA オーバーライド VLAN を設定することができます。	Flex グループのネイティブ VLAN 設定 （175 ページ）
グループベースのアクセス コントロール ポリシー ダッシュボード	グループベースのアクセス コントロール ポリシー ダッシュボードでは、ネットワークアクティビティ、ポリシー関連の問題、およびトラフィックトレンドの概要を確認することができます。この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、**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。	グループベースのアクセス コントロール ポリシー ダッシュボード（266 ページ）
アクセスポイントの 802.1x 認証のサポート	プラグアンドプレイ（PnP）を使用して AP のセキュアなオンボーディングの認証設定を指定することができます。AP を要求する際、Cisco DNA Center のグローバルレベルまたはサイトレベルの階層で設定された認証設定に基づいて、PnP から 802.1x（Dot1x）サプリカントと証明書がプッシュされます。	AP の 802.1x 認証の設定

新機能および変更された機能に関する情報

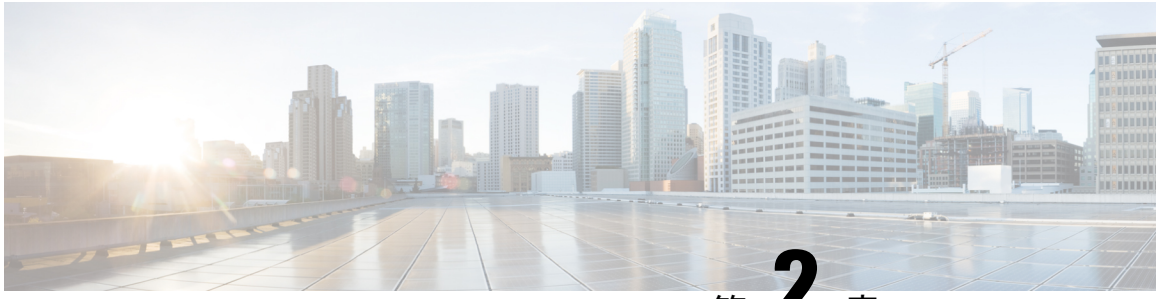
機能	説明	参照先
Locator/ID Separation Protocol Publish/Subscribe（LISP Pub/Sub）ベースのコントロールプレーン	LISP Pub/Sub コントロールプレーンを使用するようにファブリックサイトを設定することができます。LISP Pub/Sub 設定は、ネイティブ LISP サポートを提供します。これにより、LISP エンドポイント識別子のボーダーへのアドバタイズメントを処理できます。	LISP Pub/Sub の設定 （473 ページ）
範囲指定されたサブネットとファブリックゾーンのサポート	ファブリックサイトを、管理するセグメントやデバイスが少ないファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、そのボーダーとコントロールプレーンに関して親サイトに依存します。	ファブリックゾーンの設定 （482 ページ）
ワイヤレスコントローラのセキュリティ アドバイザリ サポート	セキュリティ アドバイザリ ダッシュボードでは、Cisco IOS-XE ソフトウェアを実行しているワイヤレスコントローラのセキュリティアドバイザリを確認することができます。	セキュリティアドバイザリの表示 （252 ページ）
3D ワイヤレスマップ	ワイヤレスマップを表示するための 3D モードが追加されました。 3D ワイヤレスマップを使用すると、ワイヤレスネットワークを 3D で可視化して表示できます。	ワイヤレスネットワークの 3D での可視化
テンプレートエディタの UI の拡張機能	[Template] ウィンドウでシステム変数名の入力を開始すると、関連するすべての属性がドロップダウンリストとして表示されます。 [Template Editor] ウィンドウでツリー階層を展開したり折りたたむことができます。この機能を使用すると、[Template] ウィンドウをより大きなサイズで表示できます。	—

機能	説明	参照先
メッシュ設定	アクセスポイントをルートアクセスポイントまたはメッシュアクセスポイントとして設定できます。 AireOS ワイヤレスコントローラと Cisco Catalyst 9800 ワイヤレスコントローラの両方で、許可済みアクセスポイント、ブリッジグループ名（BGN）、およびルートアクセスポイントのダウンリンクバックホールを設定できます。Cisco Catalyst 9800 ワイヤレスコントローラで、メッシュアクセスポイントの最大範囲、バックホール クライアント アクセス、およびバックホールデータレートを設定できます。	ワイヤレス メッシュ ネットワークについて WLC でのメッシュ設定の指定 AP ワークフローの設定 （554 ページ） シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （398 ページ）
ワイヤレスデバイスと国コード	Cisco DNA Center は、国コードを使用してコントローラとアクセスポイントをプロビジョニングし、[Device 360] ウィンドウにコントローラとアクセスポイントの国コード情報を表示します。	ワイヤレスデバイスと国コードについて （390 ページ）
デバイスの交換ワークフロー	このワークフローでは、障害のあるデバイスを交換するための詳細な手順が示されます。	デバイスの交換ワークフロー （557 ページ）
返品許可（RMA）での新しいデバイスのサポート	故障したデバイスを新しいデバイスに交換し、RMA ワークフローを使用して、新しいデバイスのイメージ、ライセンス、および設定を置き換えることができます。 Cisco DNA Center は、次のスイッチについてワンタッチ RMA サポートを提供します。 • シードデバイス（LAN 自動化プライマリおよびピアデバイス）など、LAN 自動化によって検出および設定されたスイッチ • ファブリックインアボックスとして構成されたデバイス（スタンドアロンのみ）	—

新機能および変更された機能に関する情報

機能	説明	参照先
Cisco AI エンドポイント分析拡張機能	Cisco AIエンドポイント分析は、エンドポイントで次の異常が検出された数と頻度に基づいて、エンドポイントにトラストスコアを割り当てます。 • AI スプーフィング検出 • プロファイルラベルの変更 • NAT モード検出 • 同時 MAC アドレス	Cisco AI エンドポイント分析の主な機能 （340 ページ）
ランダム MAC アドレスを使用するエンドポイントの検出	Cisco AIエンドポイント分析を使用すると、ランダムなMACアドレスを使用するエンドポイントを検出できます。 Cisco AI エンドポイント分析を使用すると、Cisco ISE から DUID と呼ばれる（Cisco ISE では GUID とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムで変化するMACアドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。	
非アクティブ後のエンドポイントのパージ	エンドポイント パージ ポリシーを定義して、定義された時間非アクティブだったエンドポイントをネットワークから削除できます。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。	

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



第 2 章

Cisco DNA Center について

About Cisco DNA Center

Cisco Digital Network Architecture は、設計、プロビジョニング、ネットワーク環境全体へのポリシーの適用を迅速かつ容易にする一元化された使いやすい管理機能を備えています。Cisco DNA Center GUI はネットワークを隅々まで見ることを可能にし、ネットワーク パフォーマンスの最適化およびユーザーエクスペリエンスおよびアプリケーションエクスペリエンスの最適化のためにネットワークインサイトを利用します。

ログイン

ブラウザで Cisco DNA Center のネットワーク IP アドレスを入力してアクセスします。互換性のあるブラウザについては、「Cisco DNA Center のリリースノート」を参照してください。この IP アドレスで外部ネットワークに接続します。これは、Cisco DNA Center のインストール時に設定されます。Cisco DNA Center のインストールと設定の詳細については、『Cisco DNA Center Installation Guide』を参照してください。

ログイン状態を維持するには、Cisco DNA Center を継続的に使用する必要があります。長時間非アクティブ状態が続くと、Cisco DNA Center のセッションから自動的にログアウトします。

ステップ 1 次のフォーマットで、Web ブラウザのアドレスバーにアドレスを入力します。ここで、*server-ip* は Cisco DNA Center をインストールしたサーバーの IP アドレス（またはホスト名）です。

https://*server-ip*

例：https://192.0.2.1

ネットワーク構成によっては、ブラウザを更新して Cisco DNA Center サーバーのセキュリティ証明書を信頼する必要があります。これを行うと、クライアントと Cisco DNA Center 間の接続のセキュリティが確保されます。

ステップ 2 システム管理者により割り当てられた、Cisco DNA Center のユーザー名とパスワードを入力します。Cisco DNA Center にホーム ページが表示されます。

使用しているユーザー ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じ権限を持つ他のユーザーが先にログインしていない場合、ホーム ページではなく初回セットアップ ウィザードが表示されます。詳細は、ネットワーク管理者として初回ログイン （8 ページ）を参照してください。

ステップ 3 ログアウトするには、[Menu] アイコン（☰）をクリックし、[Sign Out] を選択します。

ネットワーク管理者として初回ログイン

使用しているユーザー ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じロールを持つ他のユーザーが先にログインしていない場合は、[Get Started] ウィザードにリダイレクトされます。

このウィザードを使用すると、Cisco DNA Center から即時値をすぐに取得できます。これは複数の画面で構成され、ネットワーク デバイスの状況の検出とモニターに必要な情報を収集します。さらに、Cisco DNA Center ホームページ ダッシュ ボードを使用してネットワークの全体的な健全性を視覚化できます。

ウィザードで行うタスクと同じタスクはすべて、その他の Cisco DNA Center の機能で実行できます。ウィザードを使用しても、このような機能を使うことができます。任意の時点でウィザード全体をスキップできます。ウィザードが再び表示されることはありません。ただし、Cisco DNA Center では、同じ権限を持つユーザーがこのウィザード手順を完了するまで、このようなユーザーのログイン時に同じロールが表示され続けます。ウィザードの完了後は、Cisco DNA Center でウィザードが再度表示されることはありません。

[Get Started] ウィザードをスキップした場合でも、ホームページの右上にある [Get Started] リンクからいつでも再アクセスできます。

始める前に

ウィザードを完了するには、以下の情報が必要です。

- SYSLOG サーバーと SNMP サーバーの IP アドレス
- NetFlow サーバーの IP アドレスとポート
- ディスカバリ：開始する IP アドレス（CDP ディスカバリを選択している場合）または開始と終了の IP アドレス（範囲ディスカバリを選択している場合）
- オプション：優先される管理 IP アドレス

- デバイス CLI クレデンシャル（イネーブル パスワードなど）
- SNMP v2c クレデンシャル（read コミュニティ ストリングなど）

ステップ 1 ログイン （7 ページ）の説明に従って、通常の手順で Cisco DNA Center にログインします（まだログインしていない場合）。

初めてログインした場合は、[Get Started] ウィザードにリダイレクトされます。

ステップ 2 [Get Started] ウィザードで [Get Started] をクリックしてデバイスの検出を続行するか、または [Exit] をクリックしてホームページに戻ります。

ステップ 3 デバイス検出のネットワークプロパティを入力し、[Save & Next] をクリックします。

前の画面に戻るには、[Back] をクリックします。

ステップ 4 [Discovery Type]、[Starting IP Address]、および [CLI Credentials] を指定します。

ステップ 5 完了したら [Begin Discovery] をクリックすると Cisco DNA Center にホーム ページが表示されます。ここに、検出が完了するにつれネットワークの健全性情報が徐々に表示されていきます。

デフォルト ホームページ

ログインすると、Cisco DNA Center のホームページが表示されます。ホームページには、主要エリアとして、[Summary]**アシュアランス** 、[Network Snapshot]、[Network Configuration]、および[Tools] があります。

[Summary]**アシュアランス** エリアには次の内容が含まれます。

- [Health]：企業全体の正常性スコア（ネットワークデバイス、有線クライアント、ワイヤレスクライアントなど）が提供されます。[View Details] をクリックすると、[Overall Health] ウィンドウが表示されます。
- [Critical Issues]：P1 と P2 の問題の数が表示されます。[View Details] をクリックすると、[Open Issues] ウィンドウが表示されます。
  - [P1]：ネットワーク運用に幅広い影響を与える前に早急な対応を必要とする重大な問題。
  - [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある主要な問題。
- [Trends and Insights]：ネットワークのパフォーマンスに関するインサイトが提供されます。[View Details] をクリックすると、[Network Insights] ウィンドウが表示されます。

[Network Snapshot] エリアには次のコンポーネントが含まれます。

- [Sites]：ネットワーク上で検出されたサイトの数と、DNS サーバーおよびNTP サーバーの数が示されます。[Add Sites] をクリックすると、[Add Site] ウィンドウが表示されます。

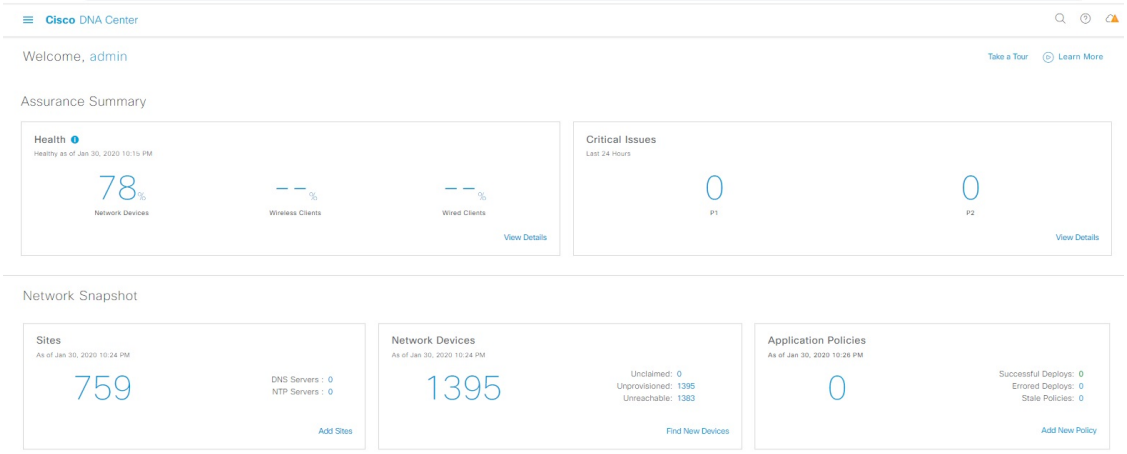
- [Network Devices]：ネットワーク上で検出されたネットワーク デバイスの数と、要求されていないデバイス、プロビジョニングされていないデバイス、および到達不能なデバイスの数が示されます。[Find New Devices] をクリックすると、[New Discovery] ウィンドウが表示されます。
- [Application policies]：ネットワーク上で検出されたアプリケーション ポリシーの数と、成功およびエラーになった展開の数を表示します。[Add New Policy] をクリックすると、[Application Policies] ウィンドウが表示されます。
- [Network Profiles]：ネットワーク上で検出されたプロファイルの数を示します。[Manage Profiles] をクリックすると、[Network Profiles] ウィンドウが表示されます。
- [Images]：ネットワーク上で検出されたイメージの数と、タグなしイメージおよび未検証イメージの数が示されます。[Import Images/SMUs] をクリックすると、[Image Repository] ウィンドウが表示されます。
- [Licensed Devices]：Cisco DNA Center ライセンスを持つデバイスの数と、スイッチ、ルータ、およびアクセスポイントの数が示されます。[Manage Licenses] をクリックすると、[License Management] ウィンドウが表示されます。

[Network Configuration] エリアには次の内容が含まれます。

- [Design]：ネットワーク全体のデバイスに適用できるネットワークの構造とフレームワーク（物理トポロジ、ネットワーク設定、デバイス タイプ プロファイルなど）を作成します。
- [Policy]：ネットワークの特定の側面（ネットワーク アクセスなど）に対する組織のビジネス目標を反映したポリシーを作成します。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワーク デバイスのさまざまなタイプ、メーカー、モデル、オペレーティング システム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。
- [Provision]：デバイスの準備と設定（サイトへのデバイスの追加、インベントリへのデバイスの割り当て、必要な設定とポリシーの展開、ファブリックドメインの作成、ファブリックへのデバイスの追加など）を行います。
- **アシュアランス**[Assurance]：ネットワーク インフラストラクチャ、アプリケーション、およびエンドユーザークライアントのパフォーマンスと正常性について、プロアクティブで予測型の実用的洞察を提供します。
- [Platform]：インテント API を使用してネットワークにプログラムでアクセスできます。最適な IT システムと統合してエンドツーエンドのソリューションを作成し、マルチベンダー デバイスのサポートを追加できます。

[Tools]：[Tools] エリアを使用して、ネットワークを設定および管理します。

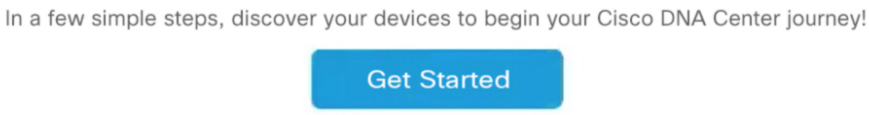
図 *1 : Cisco DNA Center* ホームページ



ホーム ページのさまざまなビュー :

使用する前に

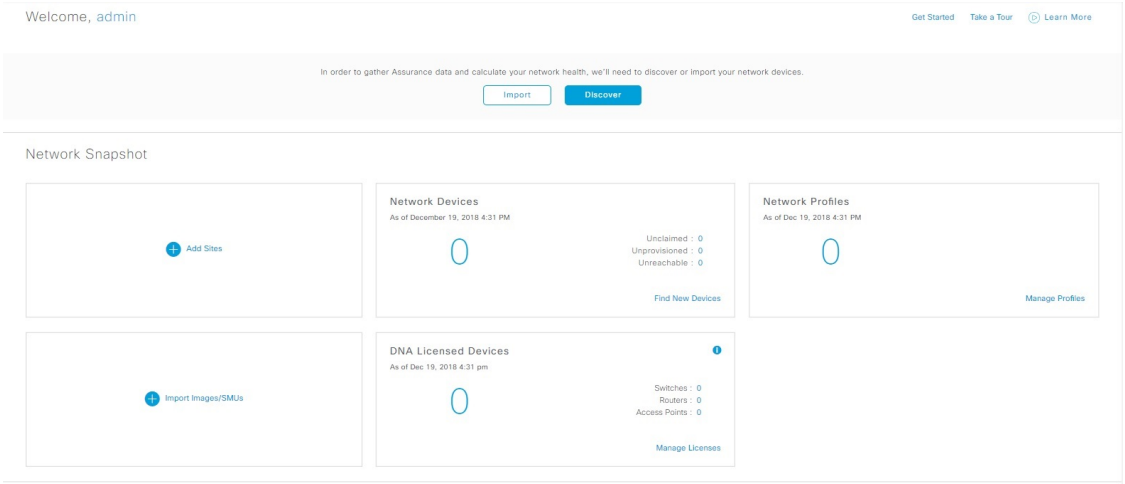
ネットワーク管理者またはシステム管理者として初めて Cisco DNA Center にログインするとき、またはシステムにデバイスが存在しない場合は、次のダッシュレットが表示されます。[Get Started] をクリックして開始ワークフローを完了し、ネットワーク内の新しいデバイスを検出します。



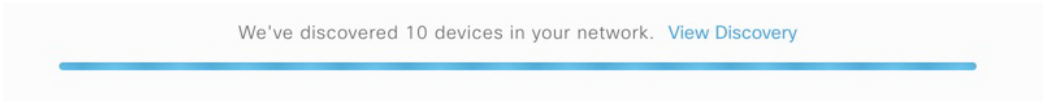
初めてオブザーバとして Cisco DNA Center にログインすると、次のメッセージが表示されます。

0 日目のホームページ

開始をスキップした場合、またはシステム内にデバイスが存在しない場合は、次のホーム ページが表示されます。



検出が進行中の場合は、[Discovery] ウィンドウへのリンクが付いた進捗状況メッセージが表示されます。



システム内にデバイスがある場合は、検出されたデバイスのネットワーク スナップショットが表示されます。

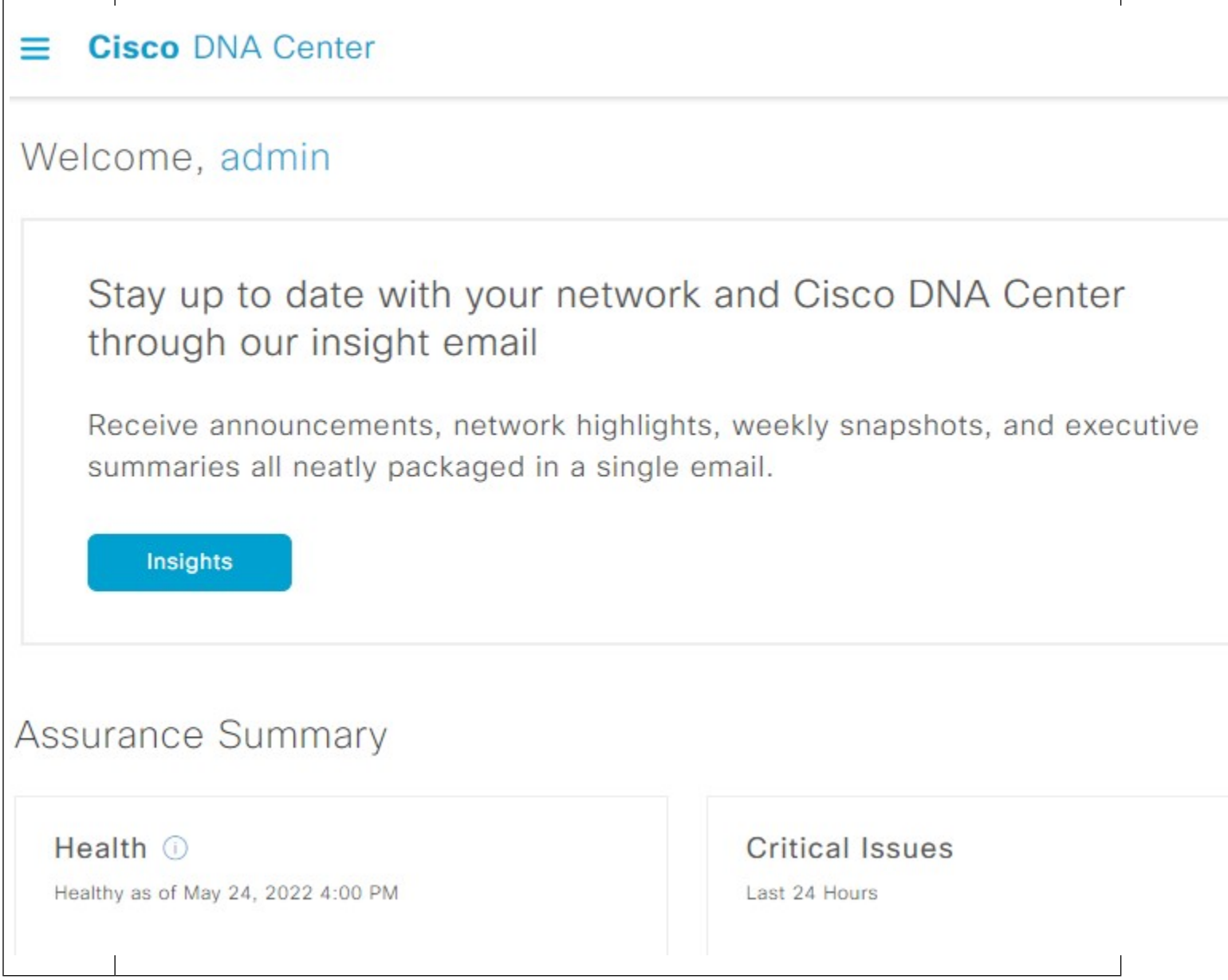
ホームページの左上隅にある [Menu] アイコン（☰）をクリックすると、次のメニューにアクセスできます。

- 設計
- ポリシー
- プロビジョニング
- 保証
- ワークフロー
- ツール
- プラットフォーム
- アクティブな状態
- システム

ホームページの右上隅と右下隅にあるアイコンをクリックして共通のタスクを実行できます。

アイコン	説明
🔍	[Search]：デバイス、ユーザー、ホスト、ハンバーガーメニューのメニュー、およびその他の項目が保存されている Cisco DNA Center データベース内の任意の場所で、それらを検索します。検索機能を使用する際のヒントについては、「グローバル検索の使用 （15 ページ）」を参照してください。

アイコン	説明
	**Help** • [About]： 現在の Cisco DNA Center のソフトウェアバージョンが表示されます。 [Release Notes] をクリックすると、別のブラウザタブでリリースノートが起動します。 [Packages] をクリックすると、システムおよびアプリケーションパッケージのバージョンが表示されます。 [Serial number] をクリックすると、Cisco DNA Center のアプライアンスのシリアル番号が表示されます。 • [API Reference]：Cisco DevNet に Cisco DNA Center プラットフォーム API のドキュメントが開きます。 • [Developer Resources]：開発者ツールにアクセスできる Cisco DevNet が開きます。 • [Help]：状況に応じたオンラインヘルプが、ブラウザの別のタブに表示されます。 • [Contact Support]：Cisco Technical Assistance Center（TAC）でサポートケースが開きます。 • [Make a Wish]：コメントや提案事項が Cisco DNA Center 製品チームに送信されます。
	[Software Updates]：利用可能なソフトウェアアップデートのリストが表示されます。[Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。

アイコン	説明
	

Cisco DNA Center を初めて使用する場合は、開始位置 （18 ページ） で使い方のヒントや提案を参照してください。

（注） デフォルトでは、入力したログイン名がウェルカム テキストに表示されます。名前を変更するには、名前のリンク（例：**admin**）をクリックします。[User Management] ウィンドウに移動し、表示名を編集できます。

グローバル検索の使用

グローバル検索機能を使用して、Cisco DNA Center の任意の場所で次のカテゴリの項目を検索します。

- **アクティビティ**：Cisco DNA Center のメニュー項目、ワークフロー、および機能を名前で検索します。
- **アプリケーション**：名前で検索します。
- **アプリケーション グループ**：名前で検索します。
- **認証テンプレート**：名前またはタイプで検索します。
- **デバイス**：収集ステータス、到達可能性ステータス、ロケーション、またはタグで検索します。
- **ファブリック**：ファブリック名で検索します。
- **ホストおよびエンドポイント**：名前、IP アドレスまたは MAC アドレスで検索します。
- **IP プール**：名前または IP アドレスでそれらを検索します。
- **ネットワーク デバイス**：名前、IP アドレス、シリアル番号、ソフトウェア バージョン、プラットフォーム、製品ファミリ、または MAC アドレスで検索します。
- **ネットワークプロファイル** ：プロファイル名で検索します。
- **ネットワーク設定**
  - **デバイスログイン情報**：名前で検索します。
  - **IP アドレスプール**：グループ名またはプールの CIDR で検索します。
  - **サービス プロバイダ プロファイル**：プロファイル名、WAN プロバイダ、またはモデルで検索します。
- **ポリシー**：名前または説明で検索します。
- **サイト**：名前で検索します。
- **トラフィックのコピー** ：名前と説明で検索します。
- **移行**：移行名で検索します。
- **ユーザー**：システム設定およびユーザーをユーザー名で検索します。大文字と小文字は区別されません。ユーザー名のサブストリング検索はサポートされていません。
- 新しいバージョンの Cisco DNA Center として別のアイテムがリリースされます。

グローバル検索を開始するには、Cisco DNA Center ページの右上隅にある アイコンをクリックします。Cisco DNA Center にポップアップグローバル検索ウィンドウが表示されます。[Search] フィールドに項目に関する識別情報を入力します。

ターゲット項目の名前、アドレス、シリアル番号、またはその他の識別情報の全体または一部を入力できます。[Search] フィールドで大文字と小文字は区別されません。任意の文字または文字の組み合わせを入力できます。

検索文字列の入力を開始すると、入力に一致する可能性がある検索ターゲットのリストが Cisco DNA Center に表示されます。複数のカテゴリの項目が検索文字列と一致する場合は、Cisco DNA Center によってカテゴリ別にソートされます。各カテゴリには最大 5 つの項目が含まれます。最初のカテゴリの最初の項目が自動的に選択され、その項目の概要情報が右側の [summary] パネルに表示されます。

必要に応じてリストをスクロールできます。提案された検索ターゲットのいずれかをクリックすると、概要パネルにその項目の情報が表示されます。カテゴリに項目が 5 つ以上ある場合は、カテゴリ名の横にある [View All] をクリックします。検索ターゲットの完全なリストからカテゴリ化されたリストに戻るには、[Go Back] をクリックします。

検索文字列にさらに多くの文字を追加すると、グローバル検索で表示されるリストが自動的に絞り込まれます。

概要パネルには、詳細へのリンクが表示されます。リンクはカテゴリおよび項目ごとに必要に応じて変わります。例：アクティビティの場合、概要パネルには Cisco DNA Center システム以外のメニュー項目およびワークフローへのリンクが表示されます。アプリケーションの場合、[Application 360] ビューが表示されます。ホスト/エンドポイントの場合は [Client 360] ビューと [Topology] ビューへのリンクが表示され、ネットワーク デバイスの場合は [Device 360] ビューと [Topology] ビューへのリンクが表示されます。

完了したら、 をクリックしてウィンドウを閉じます。

グローバル検索では、カテゴリごとに一度に 5 つの結果を表示できます。

ローカリゼーションの有効化

Cisco DNA Center の GUI 画面は、英語（デフォルト）、中国語、日本語または韓国語で表示できます。

デフォルトの言語を変更するには、次のタスクを実行します。

ステップ 1 ブラウザで、サポートされている言語（中国語、日本語、または韓国語）のいずれかにロケールを変更します。

- Google Chrome から、次の手順を実行します。

  1. 右上隅にある アイコンをクリックし、[Settings] を選択します。
  2. 下にスクロールして [Advanced] をクリックします。

3. **[Languages]** > **[Language]** ドロップダウンリストから、[Add languages] を選択します。

   [Add languages] ポップアップウィンドウが表示されます。

4. [Chinese]、[Japanese]、または [Korean] を選択して、[Add] をクリックします。

- Mozilla Firefox から、次の手順を実行します。

1. 右上隅にある ☰ アイコンをクリックし、[Options] を選択します。
2. **[Language and Appearance]** > **[Language]** エリアから、[Search for more languages] を選択します。

   [Firefox Language Settings] ポップアップウィンドウが表示されます。

3. [Select a language to add] ドロップダウンリストから、[Chinese]、[Japanese]、または [Korean] を選択します。
4. [OK] をクリックします。

ステップ 2 Cisco DNA Center にログインします。

GUI 画面は、選択した言語で表示されます。

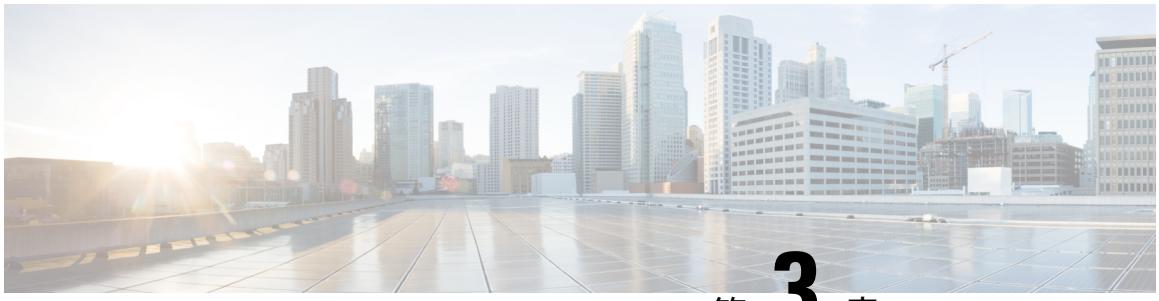
図 *2:* ローカライズされたログイン画面の例

開始位置

Cisco DNA Center の使用を開始するには、まず、サーバーがネットワーク外と通信できるように Cisco DNA Center を設定する必要があります。

設定後、現在の環境で Cisco DNA Center の使用を開始する方法を決定します。

- 既存のインフラストラクチャ：既存のインフラストラクチャ（ブラウンフィールド導入）があれば、ディスカバリを実行して開始します。ディスカバリを実行すると、すべてのデバイスが **[Inventory]** ウィンドウに表示されます。
- 新規または存在しないインフラストラクチャ：既存のインフラストラクチャがなく、ゼロから開始（新規導入）する場合は、ネットワーク階層を作成します。



第 3 章

ネットワークの検出

ディスカバリについて

ディスカバリ機能は、ネットワーク内のデバイスをスキャンし、検出されたデバイスの一覧をインベントリに送信します。

また、ディスカバリ機能は、デバイスの可制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（これらの設定がデバイスにまだ存在しない場合）。

デバイスは次の 3 つの方法で検出できます。

- Cisco Discovery Protocol（CDP）を使用し、シード IP アドレスを指定します。
- IP アドレスの範囲を指定します（最大 4096 デバイスの範囲がサポートされます）。
- Link Layer Discovery Protocol（LLDP）を使用し、シード IP アドレスを指定します。

ディスカバリ基準を設定する際は、ネットワーク検出時間を短縮するために役立つ設定があることに注意してください。

- [CDP Level] と [LLDP Level]：CDP または LLDP をディスカバリ方式として使用する場合は、CDP レベルまたはLLDP レベルを設定して、スキャンするシードデバイスからのホップ数を指定できます。デフォルトのレベル 16 では、大規模なネットワークの場合に時間がかかる可能性があります。そのため、検出する必要があるデバイスが少ない場合は、このレベルをより低い値に設定できます。

- [Subnet Filters]： IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP]：CDP、LLDP、または IP アドレスの範囲のいずれを使用する場合でも、Cisco DNA Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。

（注） Cisco SD-Access ファブリックおよび Cisco DNA アシュアランス については、デバイスのループバックアドレスを指定することをお勧めします。

どの方式を使用する場合でも、Cisco DNA Center からデバイスにアクセスできる必要があり、デバイスを検出するための特定のクレデンシャルとプロトコルを Cisco DNA Center で設定する必要があります。これらのログイン情報は、**[Design]** > **[Network Settings]** > **[Device Credentials]** ウィンドウで（または [Discovery] ウィンドウでジョブごとに）設定して保存することができます。

（注） デバイスが Hot Standby Router Protocol（HSRP）や Virtual Router Redundancy Protocol（VRRP）などのファーストホップ解決プロトコルを使用する場合、そのデバイスは、そのフローティング IP アドレスによって検出され、インベントリに追加される可能性があります。その後、HSRP または VRRP に障害が発生すると、その IP アドレスが別のデバイスに割り当てなおされる場合があります。この場合、Cisco DNA Center が分析のために取得するデータによって問題が発生する可能性があります。

検出ダッシュボード

Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Tools]** > **[Discovery]** の順に選択して、[Discovery Dashboard] を表示します。[Discovery Dashboard] には、インベントリの概要、最新のディスカバリ、ディスカバリタイプ、ディスカバリステータス、最近のディスカバリが表示されます。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- Cisco DNA Center によって検出されるデバイスの情報については、「サポート対象デバイスのリスト」を参照してください。
- Cisco DNA Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間（RTT）であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。

- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。詳細については、ディスカバリ クレデンシャル （21 ページ）を参照してください。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、設定のガイドラインと制限事項のディスカバリ （24 ページ）を参照してください。

ディスカバリ クレデンシャル

ディスカバリ クレデンシャルは、検出するデバイスに関する CLI、SNMPv2c、SNMPv3、HTTP（HTTPS）、および NETCONF 設定値です。検出を試みるデバイスの種類に基づいてクレデンシャルを指定する必要があります。

- ネットワークデバイス：CLI と SNMP のクレデンシャル。

（注） 組み込みワイヤレスコントローラなどの NETCONF 対応デバイスについては、管理者権限で SSH クレデンシャルを指定し、NETCONF ポートを選択する必要があります。

- コンピューティングデバイス（NFVIS）：CLI、SNMP、および HTTP (S) のクレデンシャル。

ネットワーク内のさまざまなデバイスが異なるクレデンシャルセットを持つことが可能であるため、Cisco DNA Center で複数のクレデンシャル セットを設定できます。ディスカバリ プロセスでは、デバイスに使用できるクレデンシャル セットが見つかるまで、ディスカバリ ジョブ用に設定されているすべてのセットで反復処理されます。

ネットワーク内の大半のデバイスに同じクレデンシャル値を使用する場合は、それらを設定して保存し、複数のディスカバリ ジョブで再利用できます。固有のクレデンシャルを使用するデバイスを検出するために、ディスカバリ ジョブの実行時にジョブ固有のディスカバリ クレデンシャルを追加できます。クレデンシャルタイプごとに最大 10 のグローバルクレデンシャルを設定し、そのうちの 5 つを定義できます。ジョブ固有のクレデンシャルを定義する必要がある場合は、クレデンシャルの種類ごとに 4 つのグローバルクレデンシャルと 1 つのジョブ固有のクレデンシャルを定義できます。

クレデンシャルと Cisco ISE のディスカバリ

Cisco ISE を認証サーバーとして使用する場合、ディスカバリ機能では、Cisco ISE をディスカバリ プロセスの一部として使用してデバイスが認証されます。デバイスが正しく検出されるように、次の注意事項に従ってください。

- 英数字4文字未満のディスカバリ クレデンシャルを使用しないでください。デバイスは英数字4文字未満のクレデンシャルを持つことができますが、Cisco ISE で許容される最短のユーザー名とパスワードは英数字4文字です。デバイス クレデンシャルが4文字未満の場合、Cisco DNA Center はデバイスのインベントリ データを収集できず、デバイスは不完全な収集状態になります。
- 同じユーザー名を持つが、異なるパスワードをもつクレデンシャルを使用しないでください (cisco/cisco123 と cisco/pw123)。Cisco DNA Center ではユーザー名が同じでありながらパスワードの異なるデバイスのディスカバリが可能ですが、Cisco ISE では許容されません。重複したユーザー名が使用されている場合、Cisco DNA Center はデバイスを認証してインベントリ データを収集することができず、デバイスは不完全な収集状態になります。

Cisco ISE を AAA サーバーとして定義する方法については、Cisco ISE またはその他の AAA サーバーの追加 （204 ページ）を参照してください。

ディスカバリ クレデンシャルのガイドラインと制約事項

Cisco DNA Center のディスカバリ クレデンシャルに関するガイドラインと制約事項は、次のとおりです。

- ディスカバリ ジョブで使用されるデバイス クレデンシャルを変更するには、ディスカバリ ジョブを編集し、使用しなくなったクレデンシャルの選択を解除する必要があります。その後、新しいクレデンシャルを追加してディスカバリを開始する必要があります。詳細については、「ディスカバリ ジョブでクレデンシャルを変更 （46 ページ）」を参照してください。
- デバイスが正常に検出された後にデバイスのクレデンシャルを変更すると、そのデバイスのその後のポーリング サイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
  - ディスカバリ ツールを使用します：
    - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 既存のディスカバリジョブを編集し、そのディスカバリジョブを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。

- 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリジョブを再作成します。または、新しいディスカバリジョブを作成します。

- デバイス認証に失敗するために進行中のディスカバリ ポーリング サイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
  - ディスカバリ ツールを使用します：
    - 現在のディスカバリ ジョブを停止または削除し、デバイスのクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 現在のディスカバリジョブを停止または削除し、既存のディスカバリジョブを編集して、そのディスカバリジョブを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
    - 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリジョブを再作成します。または、新しいディスカバリジョブを作成します。

- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。以前に検出されたデバイスのステータスは、認証の失敗を示しません。ただし、削除されたクレデンシャルの使用を試みる次回のディスカバリは失敗します。ディスカバリは、いずれかのデバイスへの接続を試みる**前**に失敗します。

ディスカバリ クレデンシャルの例

一般的なネットワークを構成するデバイスのディスカバリ要件は、非常に多岐にわたる場合があります。Cisco DNA Center では、これらの多様な要件をサポートするために、複数の検出ジョブを作成できます。たとえば、200台のデバイスで構成されるネットワークがCisco Discovery Protocol（CDP）ネイバーを形成しているとします。このネットワークでは、190台のデバイスはグローバルクレデンシャル（クレデンシャル0）を共有しており、残りのデバイスは独自のクレデンシャル（クレデンシャル 1 ～ クレデンシャル 10）を持っています。

このネットワーク内のすべてのデバイスを検出するために、Cisco DNA Center は次のタスクを実行します。

ステップ 1 クレデンシャル 0 として CLI グローバル クレデンシャルを設定します。

ステップ 2 SNMP（v2c または v3）グローバルクレデンシャルを設定します。

ステップ 3 190 台のデバイスの IP アドレス（グローバル クレデンシャルを共有する 190 台のデバイス）の 1 つとグローバル クレデンシャル 0 を使用してディスカバリ ジョブを実行します。

ステップ 4 該当するジョブ固有のクレデンシャル（クレデンシャル 1、クレデンシャル 2、クレデンシャル 3 など）を使用して、残りの 10 台のデバイスごとに 10 個の別個のディスカバリ ジョブを実行します。

ステップ 5 [Inventory] ウィンドウで結果を確認します。

優先管理 IP アドレス

Cisco DNA Center でデバイスが検出されると、デバイスの IP アドレスの 1 つが優先管理 IP アドレスとして使用されます。IP アドレスは、デバイスの組み込み管理インターフェイス、または別の物理インターフェイス、または Loopback0 のような論理インターフェイスの IP アドレスにすることができます。デバイスのループバック IP アドレスを優先管理 IP アドレスとして使用するために Cisco DNA Center を設定できます（その IP アドレスが Cisco DNA Center から到達可能である場合）。

優先管理 IP アドレスとして [Use Loopback IP] を選択した場合、Cisco DNA Center では次のように優先管理 IP アドレスが指定されます。

- デバイスに 1 つのループバック インターフェイスがある場合、Cisco DNA Center は、そのループバック インターフェイスの IP アドレスを使用します。
- デバイスに複数のループバック インターフェイスがある場合、Cisco DNA Center は、最上位の IP アドレスを持つループバック インターフェイスを使用します。
- ループバック インターフェイスがない場合、Cisco DNA Center は、最上位の IP アドレスを持つイーサネット インターフェイスを使用します（サブインターフェイスの IP アドレスは考慮されません）。
- イーサネット インターフェイスがない場合、Cisco DNA Center は、最上位の IP アドレスを持つシリアル インターフェイスを使用します

デバイスが検出された後に、**[インベントリ（Inventory）]** ウィンドウから管理 IP アドレスを更新できます。詳細については、デバイスの管理 IP アドレスの更新 （85 ページ）を参照してください。

設定のガイドラインと制限事項のディスカバリ

Cisco DNA Center による Cisco Catalyst 3000 シリーズ スイッチおよび Catalyst 6000 シリーズ スイッチの検出に関する注意事項と制約事項は、次のとおりです。

- CLI ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これは、ディスカバリ機能のために Cisco DNA Center で設定する CLI ユーザ名およびパスワードと同じです。Cisco DNA Center にはデバイスへの最高レベルのアクセス権が必要です。
- 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポート プロトコルを明示的に指定してください。この設定には、**transport input** と **transport**

output コマンドを使用してください。これらのコマンドについては、各デバイス タイプ用のコマンド リファレンス ドキュメントを参照してください。

- デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA（TACACS）ログインで設定されている場合は、Cisco DNA Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。
- Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

ディスカバリの実行

CDP を使用したネットワークの検出

Cisco Discovery Protocol（CDP）IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、IP アドレス範囲を使用したネットワークの検出 （32 ページ）およびLLDP を使用したネットワークの検出 （38 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベスト エフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで CDP を有効にします。
- ディスカバリの前提条件 （20 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 まだ表示されていない場合は [IP アドレス/範囲（IP Address/Range）] エリアを展開し、次のフィールドを設定します。

a) [ディスカバリ タイプ（Discovery Type）] で、[CDP] をクリックします。

b) [IP アドレス（IP Address）] フィールドでシード IP アドレスを入力し、Cisco DNA Centerでディスカバリ スキャンを開始します。

c) （任意）[サブネット フィルタ（Subnet Filter）] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネット マスクは、0 ～ 32 の値です。

d) [+] をクリックします。

手順 c および d を繰り返して、ディスカバリ ジョブから複数のサブネットを除外します。

e) （任意）[CDP レベル（CDP Level）] フィールドに、スキャンするシード デバイスからのホップ数を入力します。

有効値は 1 ～ 16 です。デフォルト値は 16 です。たとえば、CDP レベル 3 は、CDP がシード デバイスから最大 3 つのホップまでスキャンすることを意味します。

f) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバックインターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （24 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

（注） ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスがCisco DNA Centerから到達可能であることを確認します。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。独自のログイン情報を設定する場合は、[Save] をクリックして現在のジョブに対してのみ保存することもできれば、[Save as global settings] チェックボックスをクリックし、次に [Save] をクリックして、現在または将来のジョブに対して保存することもできます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。

b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。
c) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 *2 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *3 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *4 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *5 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意） [HTTP（S）] をクリックして、次のフィールドを設定します。

表 *6 : HTTPS* クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。

フィールド	説明
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 5 つの HTTPS 書き込みログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

h) （任意）NETCONF が有効化されているネットワークデバイスが存在する場合、[NETCONF] をクリックして、[ポート（Port）] フィールドにポート数を入力します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830（デフォルトのポート番号）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合）

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

ステップ 6 デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。

有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始する前にキャンセルするには、[Cancel] をクリックします。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（Discovery Details）] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）] ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

IP アドレス範囲を使用したネットワークの検出

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （25 ページ）およびLLDP を使用したネットワークの検出 （38 ページ）を参照してください。

始める前に

ディスカバリの前提条件 （20 ページ）で説明されているように、デバイスには必須のデバイス設定が存在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**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 まだ表示されていない場合は [IP アドレス/範囲（IP Address/Ranges）] エリアを展開し、次のフィールドを設定します。

a) [Discovery Type] で、[IP Address/Range] をクリックします。

b) [From] フィールドと [To] フィールドに、スキャンする Cisco DNA Center 最初の IP アドレスと最後の IP アドレス（IP アドレス範囲）を入力し、+ をクリックします。

検出スキャンに対して、単一の IP アドレス範囲または複数の IP アドレスを入力できます。

（注） Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

c) （任意） ステップ b を繰り返して、追加の IP アドレス範囲を入力します。

d) （任意） 検出スキャンから除外する IP アドレス/範囲またはサブネットを [Subnet Filter] フィールドに入力します。個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで *x.x.x.x* は IP アドレスを示し、*y* はサブネットマスクを示します。サブネット マスクは、0 ～ 32 の値です。

e) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバックインターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （24 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。独自のクレデンシャルを設定する場合、[保存（Save）] をクリックして現在のジョブにのみ保存できます。または、[グローバル設定として保存（Save as global settings）] チェックボックスをクリックし、次に [保存（Save）] をクリックして、現在または将来のジョブに保存できます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。

b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。

c) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 7: *CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *8 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *9 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *10 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意）[HTTP（S）] をクリックして、次のフィールドを設定します。

表 *11 : HTTPS* クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 5 つの HTTPS 書き込みログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

h) （任意）NETCONF が有効化されているネットワークデバイスが存在する場合、[NETCONF] をクリックして、[ポート（Port）] フィールドにポート数を入力します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830（デフォルトのポート番号）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合）

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

ステップ 6 （任意） デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルをクリックします。緑のチェックマークはプロトコルが選択されていることを示します。

有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（Discovery Details）] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）] ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol（LLDP）、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （25 ページ）およびIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベストエフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで LLDP を有効にします。
- ディスカバリの前提条件 （20 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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**[Tools]** > **[Discovery]**。

[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 [IP Address/Range] 領域を展開し、次のフィールドを設定します。

a) [ディスカバリ タイプ（Discovery Type）] で、[LLDP] をクリックします。

b) [IP アドレス（IP Address）] フィールドでシード IP アドレスを入力し、Cisco DNA Centerでディスカバリ スキャンを開始します。

c) （任意）[サブネット フィルタ（Subnet Filter）] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネット マスクは、0 ～ 32 の値です。

d) [+] をクリックします。

手順 c および d を繰り返して、ディスカバリ ジョブから複数のサブネットを除外します。

e) （任意）[LLDP レベル（LLDP Level）] フィールドで、スキャンするシード デバイスからのホップ数を入力します。

有効値は 1 ～ 16 です。デフォルト値は 16 です。たとえば、LLDP レベル 3 は、LLDP がシード デバイスから最大 3 つのホップをスキャンすることを意味します。

f) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） このオプションを選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は優先管理 IP アドレス （24 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

（注） ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスがCisco DNA Centerから到達可能であることを確認します。

ステップ 5 [Credentials] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。クレデンシャルを設定する場合は、[Save as global settings] チェックボックスをオンにして、将来のジョブのためにそれらを保存できます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。

b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。

c) CLI クレデンシャルの場合は、次のフィールドを設定します。

表 *12 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *13 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *14 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *15 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意） [HTTP（S）] をクリックして、次のフィールドを設定します。

表 *16 : HTTPS* クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。

フィールド	説明
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 5 つの HTTPS 書き込みログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

ステップ 6 （任意） デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（Discovery Details）] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）] ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

ディスカバリ ジョブの管理

ディスカバリ ジョブの停止および開始

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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 アクティブなディスカバリ ジョブを停止するには、次の手順を実行します。

a) **[Discoveries]** ペインで、関連するジョブを選択します。

b) [Stop] をクリックします。

ステップ 4 非アクティブなディスカバリ ジョブを再起動するには、次の手順を実行します。

a) **[Discoveries]** ペインで、関連するジョブを選択します。

b) [Re-discover] をクリックして、選択したジョブを再起動します。

ディスカバリ ジョブの編集

既存のディスカバリジョブを編集して、ジョブを再実行できます。

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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 次のフィールドを除き、ディスカバリのタイプに応じてジョブのタイプを変更できます。

- [CDP]：ディスカバリ名、ディスカバリタイプ、IP アドレス。変更可能なフィールドの詳細については、CDP を使用したネットワークの検出 （25 ページ）を参照してください。
- [IP Range]：ディスカバリ名、タイプ、IP アドレス範囲（ただし別の IP アドレス範囲を追加できます）。変更可能なフィールドの詳細については、IP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

- LLDP：ディスカバリ名、タイプ、IPアドレス。変更可能なフィールドの詳細については、LLDP を使用したネットワークの検出 （38 ページ）を参照してください。

ステップ 6 [Start] をクリックします。

ディスカバリ ジョブでクレデンシャルを変更

ディスカバリジョブで使用されるクレデンシャルを変更し、そのジョブを再実行できます。

始める前に

少なくとも 1 つのディスカバリ ジョブが必要です。

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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開します。

ステップ 6 使わないクレデンシャルを非選択状態にします。

ステップ 7 使用するクレデンシャルを設定します。

a) [クレデンシャルの追加（Add Credentials）] をクリックします。

b) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 *17 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *18 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *19 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。

フィールド	説明
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 8 [Start] をクリックします。

ディスカバリ ジョブの複製

ディスカバリジョブを複製し、そのジョブ用に定義されているすべての情報を保持できます。

始める前に

少なくとも 1 つのディスカバリ ジョブを実行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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Copy & Edit] をクリックします。

Cisco DNA Center では、「*Copy of Discovery_Job*」という名前でディスカバリジョブのコピーが作成されます。

ステップ 5 （任意） 検出ジョブの名前を変更します。

ステップ 6 新しいディスカバリ ジョブのパラメータを定義または更新します。

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[ディスカバリ（Discovery）]**ペインで、削除する検出ジョブを選択します。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

使用された設定やクレデンシャルなどの、ディスカバリ ジョブに関する情報を表示できます。実行された各ディスカバリジョブに関する履歴情報（検出されたデバイスや検出に失敗したデバイスに関する情報など）も表示できます。

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

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**[Tools]** > **[Discovery]**。[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

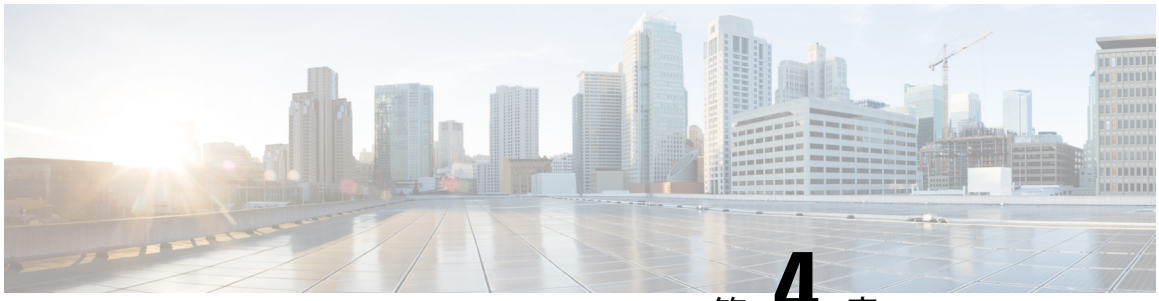
ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。もしくは、**[Search]** 機能を使用して、デバイス IP アドレスまたは名前によって、ディスカバリ ジョブを検索できます。

ステップ 4 詳細については、次の領域のひとつの隣にある下矢印をクリックします。

- [Discovery Details]：ディスカバリジョブを実行するために使用されたパラメータが表示されます。パラメータには、CDP または LLDP レベル、IP アドレス範囲、およびプロトコルの順序などの属性が含まれます。
- [Credentials]：使用されたログイン情報の名前が提供されます。
- [History]：実行された各ディスカバリジョブがリストされ、開始時刻やデバイス検出の有無などが表示されます。

  組み込みワイヤレスコントローラを正常に検出するには、NETCONF ポートを設定する必要があります。NETCONF ポートが設定されていない場合、ワイヤレスデータは収集されません。

  [Filter] 機能を使用して、IP アドレスあるいは ICMP、CLI、HTTPS、NETCOMF 値の任意の組み合わせによってデバイスを表示できます。



第 4 章

インベントリの管理

インベントリについて

インベントリ機能は、ホストの IP アドレス、MAC アドレス、およびそのデータベース内のデバイスに関するネットワーク アタッチメント ポイントなどの詳細を取得して保存します。

また、インベントリ機能は、デバイスの制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（ネットワーク設定がデバイスにまだ存在しない場合）。

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery （このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （20 ページ） を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 6 時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最高 24 時間まで変更できます。詳細については、デバイスポーリング間隔の更新（86 ページ）を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイスデータが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

インベントリと Cisco ISE の認証

Cisco ISE には、Cisco DNA Center で次の 2 つの異なる使用例があります。

- ネットワークでデバイス認証に Cisco ISE を使用する場合、Cisco DNA Center で Cisco ISE を設定する必要があります。これにより、Cisco DNA Center でデバイスをプロビジョニングする際に、ユーザーが定義した Cisco ISE サーバー情報を使用してデバイスが設定されます。また、Cisco DNA Center は Cisco ISE サーバーでデバイスを設定し、後に続くデバイスの更新プログラムについても伝えます。Cisco DNA Center での Cisco ISE の設定については、グローバル ネットワーク サーバーの設定 （204 ページ）を参照してください。

（注） Cisco ISE を使用して Cisco Catalyst 9800 シリーズ デバイスを認証する場合は、NETCONF ユーザーに権限が提供されるように Cisco ISE を設定する必要があります。

ネットワーク障害や Cisco ISE サーバーのダウンによって予定通りにデバイスが Cisco ISE サーバーで設定または更新されていない場合、Cisco DNA Center は一定の待機期間が経過した後に自動的に操作を再試行します。ただし、入力の検証エラーとして Cisco ISE から拒否されていることが障害の原因である場合、Cisco DNA Center は操作を再試行しません。

Cisco DNA Center が Cisco ISE サーバーでデバイスを設定および更新する場合、トランザクションは Cisco DNA Center の監査ログでキャプチャされます。Cisco DNA Center や Cisco ISE インベントリに関する問題のトラブルシューティングに監査ログを役立てることができます。

デバイスのプロビジョニング後、Cisco DNA Center は Cisco ISE でデバイスを認証します。Cisco ISE に到達できない（RADIUS 応答がない）場合、デバイスはローカルのログイン クレデンシャルを使用します。Cisco ISE に到達できるが Cisco ISE にデバイスが存在しない場合や、そのクレデンシャルが Cisco DNA Center で設定されたクレデンシャルと一致しない場合、デバイスはローカルのログイン クレデンシャルを使用するためにフォールバックしません。代わりに、部分的な収集状態になります。

この状態を回避するには、Cisco DNA Center を使用してデバイスをプロビジョニングする前に、必ず Cisco DNA Center で使用しているのと同じデバイス クレデンシャルで Cisco ISE のデバイスを設定します。また、有効なディスカバリ クレデンシャルを設定したことも確認してください。詳細については、ディスカバリ クレデンシャル （21 ページ）を参照してください。

- 必要に応じて、Cisco ISE を使用してデバイス グループにアクセス制御を実行できます。

インベントリに関する情報の表示

[Inventory] テーブルには、検出された各デバイスの情報が表示されます。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

テーブルで表示または非表示にする列を選択するには、 をクリックします。列の選択はセッション間では保持されない点に注意してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

[Provision]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > [Inventory] の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。次の表に、使用できる情報を記載します。

表 *20 :* インベントリ

カラム	説明
Device Name	

カラム	説明
	デバイスの名前。 デバイス名をクリックすると、デバイスの次の詳細が表示されます。 [Details]：デバイス名、到達可能性ステータス、管理性ステータス、IP アドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。 • [View Assurance 360]：360 ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 • **Interfaces** • [Ethernet Ports]（すべてのデバイスが対象）：イーサネットポートの動作ステータスと管理ステータスが表示されます。情報アイコンをクリックすると、ステータスの凡例が表示されます。 ポートのテーブルに、動作ステータス、管理ステータス、タイプ、VLAN、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [VLANs]（スイッチとハブのみが対象）：VLAN のテーブルに、VLAN ID、動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。[Search] や [Filter] のオプションをクリックして、目的の VLAN の詳細を表示できます。 • [Virtual Ports]（ワイヤレスデバイス、コントローラ、ルータのみが対象）：ポートのテーブルに、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [Hardware and Software]：デバイスのハードウェアとソフトウェアの詳細が表示されます。 • [Configuration]：show running-config コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。 この機能は、アクセスポイント (AP) とワイヤレス コントローラにはサポートされていません。したがって、これらのデバイス タイプの場合は設定データは返されません。 • [Power]：動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [Fans]：動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [Wireless Info]：プライマリとセカンダリの管理対象ロケーションが表示されます。

カラム	説明
	• [Mobility]：モビリティグループ名、RF グループ名、仮想 IP、およびモビリティ MAC アドレスが表示されます。 （注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。
IP Address	デバイスの IP アドレス。
Support Type	以下に示すデバイスのサポートレベルが表示されます。 • [Supported]：Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Unsupported]：Cisco DNA Center でテストおよび認定されていない他のすべての Cisco デバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party]：デバイスパックは、顧客/ビジネスパートナーによって構築され、認定プロセスを通過しています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡して修正を依頼する必要があります。
Reachability	以下は、さまざまなステータスのリストです。 • [Reachable]：Cisco DNA Center から SNMP、HTTP（S）、および Netconf ポーリングメカニズムを使用してデバイスに到達できます。 • [Ping Reachable]：Cisco DNA Center から ICMP ポーリングメカニズムを使用してデバイスに到達できます。SNMP、HTTP（S）、および Netconf ポーリングメカニズムでは到達できません。 • [Unreachable]：SNMP、HTTP（S）、Netconf、および ICMP のいずれのポーリングメカニズムでもデバイスに到達できません。

カラム	説明
Manageability	デバイスのステータスが次のように示されます。 • [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、Netconf ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにマウスのカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 • [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。
MAC Address	デバイスの MAC アドレス。
Image Version	デバイスで現在実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。
Serial Number	シスコ デバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している時間。
Device 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。 （注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。 • **Unknown** • **Access** • **Core** • **Distribution** • **Border Router**
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a Site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、「ネットワーク階層について （124 ページ）」を参照してください。

カラム	説明
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号（たとえば、Cisco Catalyst 4500 シリーズスイッチ）。
Resync Interval	デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、「Cisco DNA Center 管理者ガイド」を参照してください。
Last Sync Status	デバイス最終検出のスキャン状態。 • [Managed]：デバイスは完全に管理された状態です。 • [Partial Collection Failure]：デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information]（i）アイコンにマウスを合わせます。 • [Unreachable]：デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials]：デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が実行されています。

ユーザー定義フィールドの管理

ユーザー定義フィールドは、Cisco DNA Center で作成して任意のデバイスに割り当てることができるカスタムラベルです。これらのラベルを使用すると、デバイスの詳細のページにデバイスのより多くの詳細情報を表示できます。ユーザー定義フィールドを表示するには、そのフィールドをデバイスに割り当て、それに値を追加する必要があります。

ユーザー定義フィールドの作成

Cisco DNA Center では、ユーザー定義フィールドを作成し、任意のデバイスに割り当てることができます。

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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Actions] ドロップダウンリストから、**[Provision]** > **[Inventory]** > **[Manage User Defined Fields]** の順に選択します。

ステップ 3 [Manage User Defined Fields] ダイアログボックスで、[Create New Field] をクリックします。

ステップ 4 [Create New Field] ダイアログボックスで、[Field Name] フィールドと [Field Description] フィールドにユーザー定義フィールドの名前と説明を入力します。

（注） お客様の IP アドレスやお客様のデバイス名など、[Device Details] ページにまだ表示されていないデバイスの詳細をユーザー定義フィールドに追加できます。

ステップ 5 [保存（**Save**）] をクリックします。

同様に、追加のユーザー定義フィールドを作成できます。ユーザー定義フィールドはテーブルに表示されます。

ステップ 6 ユーザー定義フィールドを編集する場合は、対応する [Edit] アイコンをクリックして必要な変更を行い、[Save] をクリックします。

ステップ 7 ユーザー定義フィールドを削除する場合は、対応する [delete] アイコンをクリックし、後続の警告メッセージで [Yes] をクリックします。

デバイスへのユーザー定義フィールドの追加

始める前に

[Manage User Defined Fields] ページで少なくとも 1 つのユーザー定義フィールドを作成しておく必要があります。「ユーザー定義フィールドの作成 （58 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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 ユーザー定義フィールドを追加するデバイスの名前をクリックします。

ステップ 3 左側のペインで、[User Defined Fields] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [Field Name] ドロップダウンリストでユーザー定義フィールドを選択し、[Value] フィールドにその値を入力します。

たとえば、お客様の IP アドレスのユーザー定義フィールドを作成した場合、[Field Name] ドロップダウンリストでそのフィールドを選択し、[Value] フィールドにお客様の IP アドレスを入力します。

ステップ 6 デバイスからユーザー定義フィールドを削除する場合は、対応する [Delete] アイコンをクリックします。

ステップ 7 [Save] をクリックします。

インベントリからのトポロジマップの起動

[Inventory] ウィンドウから、検出されたデバイスのトポロジマップを起動できます。

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] > [Inventory] の順に選択します。

ステップ 2 トグルボタン  を使用して、トポロジマップビューとインベントリビューを切り替えます。トポロジマップビューには、デバイスのトポロジとプロビジョニングステータスが表示されます。各ノードをクリックすると、デバイスの詳細が表示されます。トポロジマップの詳細については、「トポロジについて」を参照してください。

（注） トポロジマップビューを折りたたむには [Collapse all] を、展開するには [expand all] をクリックします。

Cisco DNA Center インベントリ内のデバイスのタイプ

デバイスは、2 つの方法（検出されるか手動で追加される）のいずれかでインベントリに表示されます。Cisco DNA Center インベントリは、次のタイプのデバイスをサポートしています。

- **ネットワークデバイス**：サポート対象のネットワークデバイスには、シスコルータ、スイッチ、およびワイヤレスコントローラ（WLC）やアクセスポイント（AP）などのワイヤレスデバイスが含まれます。
- **計算デバイス**：サポート対象の計算デバイスには、Cisco Unified Computing System（UCS）、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、その他のデータセンターデバイスが含まれます。
- **Meraki ダッシュボード**：Cisco Meraki 製品を管理するためのシスコクラウド管理プラットフォームのダッシュボード。

サポート対象デバイスの完全なリストについては、「Cisco DNA Center Supported Devices」を参照してください。

ネットワークデバイスの管理

ネットワーク デバイスを追加

ネットワーク デバイスは、インベントリに手動で追加できます。

始める前に

ネットワークデバイスを設定していることを確認します。詳細については、「ディスカバリの前提条件 （20 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]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Type] ドロップダウン リストから、[Network Device] を選択します。

ステップ 4 [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

（注） デバイスで HSRP プロトコルを使用している場合は、仮想 IP アドレスではなく、プライマリ IP アドレスを入力する必要があります。

ステップ 5 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、[Network Settings] > [Device Credentials] ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *21 : CLI* クレデンシャル

フィールド	説明
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 6 [SNMP] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、[Network Settings] > [Device Credentials] ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

ステップ 7 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 22 : SNMPv2c のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

[V3] を選択した場合、次のフィールドを設定します。

表 *23 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 8 まだ展開されていない場合は [SNMPの再試行回数とタイムアウト（SNMP RETRIES AND TIMEOUT）] エリアを展開し、次のフィールドを設定します。

表 24 : SNMP のプロパティ

フィールド	説明
Retries	デバイスへ接続可能な試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
Timeout	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。

ステップ 9 [HTTP(S)] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、[Network Settings] > [Device Credentials] ページで作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 25 : HTTP（S）

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。

フィールド	説明
Password	ネットワーク内のデバイスのHTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Port	必要なHTTP（HTTPS）ポート番号を指定します。

ステップ 10 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONFでは、CLIプロトコルとしてSSHを設定し、SSHクレデンシャルを定義することが必要です。

ステップ 11 Cisco DNA Centerとリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

ステップ 12 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 13 [Add] をクリックします。

ネットワーク デバイス クレデンシャルの更新

選択したネットワーク デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切なRBACスコープが必要です。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するネットワーク デバイスを選択します。

ステップ 3 **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

ステップ 4 [Edit Device] ダイアログボックスで、[Type] ドロップダウンフィールドから [Network Device] を選択します（まだ選択していない場合）。

ステップ 5 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *26 : CLI* クレデンシャル

フィールド	説明
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 6 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次の手順を実行します。

ステップ 7 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *27 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

[V3] を選択した場合、次のフィールドを設定します。

表 *28 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 8 まだ展開されていない場合は [SNMPの再試行回数とタイムアウト（SNMP RETRIES AND TIMEOUT）] エリアを展開し、次のフィールドを設定します。

表 29 : SNMP のプロパティ

フィールド	説明
Retries	デバイスへ接続可能な試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。

フィールド	説明
Timeout	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。

ステップ 9 [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 30 : HTTP（S）

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。
Password	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Port	必要な HTTP（HTTPS）ポート番号を指定します。

ステップ 10 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

ステップ 11 Cisco DNA Center とリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

ステップ 12 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 13 [更新（Update）] をクリックします。

ネットワークデバイスのセキュリティフォーカス

Cisco DNA Center のセキュリティフォーカスにより、デバイスでの信頼できるチェックの結果を表示できます。

使用しているシスコのデバイスが正規の製品であり、セキュリティ侵害を受けたり物理的に変更されたりしていないことを確認するために実行されるセキュリティチェックはわずかしかありません。

デバイスアイデンティティ検証の一環として、次のチェックが実行されます。

- セキュアな固有デバイス識別子（SUDI）証明書チェーンの検証。
- デバイスの SUDI 証明書応答の署名検証。
- SUDI 証明書による製品 ID 検証。
- SUDI 証明書によるシリアル番号検証。

これらのチェックは、次の状況でトリガーされます。

- Cisco DNA Center でインベントリが収集されるたび。
- デバイスの設定を変更するとき。
- デバイスでイメージをアップグレードするとき。

次の CLI コマンドを使用して、デバイスアイデンティティ検証チェックを実行します。

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

整合性検証チェックの実行

この手順では、整合性検証チェックのステータスを確認する方法について説明します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Inventory] ドロップダウンメニューから [Security] を選択します。

ステップ 3 テーブルに示されているデバイスの詳細情報を確認します。

ステップ 4 テーブルをカスタマイズするには、テーブルの端にある縦に並んだ3つのドットをクリックし、[Add] または [Delete] を選択します。
[Integrity Verification] 列に結果が表示されます。

ステップ 5 デバイスの [Integrity Verification] 列にステータスとして [Failed] と表示されている場合は、情報アイコンをクリックして理由を表示します。

整合性検証のステータスは次のとおりです。

- [Passed]：デバイスの整合性検証に合格しました。

- [Failed]：デバイスの整合性検証に合格しませんでした。
- [Unverified]：検証を実行できませんでした。
- [Not Available]：このバージョンのデバイスまたはソフトウェアイメージが検証をサポートしていません。

計算デバイスの管理

計算デバイスの追加

計算デバイスは、インベントリに手動で追加できます。計算デバイスには、Cisco Unified Computing System（UCS）などのデバイス、Cisco Enterprise ネットワーク機能の仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、およびその他のデータセンター デバイスが含まれます。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Type] ドロップダウン リストから、[Compute Device] を選択します。

ステップ 4 [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

ステップ 5 [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *31 : HTTP（S）*

フィールド	説明
Username	HTTPS 接続の認証に使用される名前。
Password	HTTPS 接続の認証に使用されるパスワード。
Port	HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443（HTTPS の既知のポート）です。

ステップ 6 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *32 : CLI* クレデンシャル

フィールド	説明
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 7 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

ステップ 8 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *33 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

[V3] を選択した場合、次のフィールドを設定します。

表 *34 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 9 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイス ログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 10 [Add] をクリックします。

計算デバイス クレデンシャルの更新

選択した計算デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

ステップ 4 [Edit Device] ダイアログボックスの [Type] ドロップダウンリストで、[Compute Device] を選択します。

ステップ 5 まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

ステップ 6 [Username] および [Password] フィールドに、ユーザー名とパスワードを入力します。

ステップ 7 [Port] フィールドにポート番号を入力します。

ステップ 8 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [更新（Update）] をクリックします。

Meraki ダッシュ ボードの管理

Meraki ダッシュボードの統合

Meraki ダッシュボードと Cisco DNA Center を統合できます。

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]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Add Device] ダイアログボックスの [Type] ドロップダウンリストで、[Meraki Dashboard] を選択します。

ステップ 4 まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

ステップ 5 [API Key/Password] フィールドで、API キーとパスワードのログイン情報を入力し、[Get Organization details] リンクをクリックします。

ステップ 6 [Organization] ドロップダウンリストから組織のオプションを選択するか、組織名を検索します。

ステップ 7 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ステップ 8 [Add] をクリックします。

選択した組織のみで Cisco Meraki ダッシュボードとデバイスの収集が開始されます。

Meraki ダッシュボード クレデンシャルの更新

選択したデバイスの Meraki ダッシュボードログイン情報を更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

ステップ 4 [Edit Device] ダイアログボックスの [Type] ドロップダウンリストから、[Meraki Dashboard] を選択します。

ステップ 5 まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

ステップ 6 [API Key / Password] フィールドで、Meraki ダッシュボードへのアクセスに使用する API キーとパスワードのクレデンシャルを入力します。

ステップ 7 [Port] フィールドにポート番号を入力します。

ステップ 8 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [更新（Update）] をクリックします。

Firepower Management Center の管理

Firepower Management Center の統合

Firepower Management Center（FMC）を Cisco DNA Center と統合できます。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Add Device] ダイアログボックスの [Type] ドロップダウンリストで、[Firepower Management Center] を選択します。

ステップ 4 [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

ステップ 5 [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

ステップ 6 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 [Add] をクリックします。

（注） インベントリに FMC を追加すると、FMC によって管理される Firepower Threat Defense（FTD）デバイスもインベントリに自動的に追加されます。

Firepower Management Center のログイン情報の更新

Cisco DNA Center では Firepower Management Center（FMC）のログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新する FMC デバイスを選択します。

（注） FMC によって管理されている Firepower Threat Defense（FTD）デバイスを更新、編集、または削除することはできません。インベントリ内の FMC を介して FTD デバイスを管理する必要があります。

ステップ 3 **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

[Edit Device] ダイアログボックスが表示されます。

ステップ 4 [Credentials] をクリックします。

ステップ 5 [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

ステップ 6 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 [Management IP] をクリックし、[Device IP/DNS Name] フィールドにデバイスの IP アドレスまたは名前を入力します。

ステップ 8 [Resync Interval] をクリックし、再同期間隔タイプを選択します。

- [Custom]：再同期間隔を分単位で入力できます。有効な範囲は 25 ～ 1,440 分（24 時間）です。
- [Global]：デフォルトでは、再同期間隔は 1,440 分（24 時間）に設定されます。
- [Disable]：再同期間隔が無効になるかゼロに設定されます。

ステップ 9 [Role] をクリックし、[Device Role] ドロップダウンリストからロールを選択します。

ステップ 10 [更新（Update）] をクリックします。

デバイスのフィルタ

（注） フィルタを削除または変更するには、[リセット（Reset）] をクリックします。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Filter] をクリックします。

次のタイプのフィルタを使用できます。

- クイック フィルタ
- 拡張フィルタ
- 最近のフィルタ

[Quick Filter]：このフィルタでは、次の項目に基づいてデバイスの詳細を取得できます。

- **Device Family**
- **Device Role**
- **Last Sync Status**
- **Provision Status**
- **Credential Status**
- **OS Updated Status**
- **Image Needs Update**
- **Image Pre Check Status**
- **Support Type**

[Advanced Filters]：このフィルタでは、[Contains]、[Starts With]、[Ends With]、[Equals]、[Does not contains] などの演算子と正規表現を使用してフィルタ基準を設定し、その条件に基づいてデバイスの詳細を絞り込むことができます。たとえば、ドロップダウンリストからフィルタパターン（テーブル列名ごと）と演算子を選択できます。さらに、使用可能なデータに基づいてフィルタ基準の値を入力する必要があります。

[Recent Filters]：このフィルタでは、最近使用したフィルタが表示されます。フィルタ基準を保存するには、[RECENT] から [SAVED] にフィルタをドラッグアンドドロップします。

ステップ 3 選択したフィルタのフィールドに適切な値を入力します。たとえば、[Device Name] フィルタであれば、デバイスの名前を入力します。

Cisco DNA Center その他のフィールドに値を入力すると、オートコンプリート値が提示されます。推奨されるいずれかの値を選択するか、または値の入力を終了します。

これらのフィルタにワイルドカード（アスタリスク）を使用することもできます。たとえば、文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。その後、Enter を押します。

ステップ 4 [Apply] をクリックして情報をフィルタします。

[Devices] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

（注） フィルタごとに複数のフィルタ タイプと複数の値を使用できます。

ステップ 5 （オプション）必要に応じて、フィルタを追加します。

フィルタを削除するには、対応するフィルタ値の横にある [x] アイコンをクリックします。

インベントリ内のデバイスの管理

ここでは、[Inventory] ウィンドウを使用して、サイトにデバイスを割り当て、デバイスタグを管理する方法について説明します。

デバイスをサイトに追加する

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。

ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドイン ペインが表示されます。

ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。

ステップ 6 [Save] をクリックします。

ステップ 7 （任意） 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。

ステップ 8 [**Assign**] をクリックします。

ステップ 9 サイトにデバイスを割り当てるときにデバイスの可制御性が有効になっていると、ワークフローが自動的にトリガーされ、サイトからデバイスにデバイス設定がプッシュされます。
[Focus] ドロップダウンリストから [Provision] を選択し、[Provision Status] 列の [See Details] をクリックします。デバイスの可制御性を有効にしている場合、デバイスにプッシュされる設定が別のウィンドウに表示されます。

デバイスのタグ付け

デバイスタグは属性またはルールに基づいてデバイスをグループ化することができます。単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[プロビジョン（Provision）]ウィンドウのデバイスに対してタグを追加したり、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] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、[Tag Device] をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力します。

- 新しいタグを作成している場合は、[新規タグの作成（Create New Tag）] をクリックします。ルールを使用して新規タグを作成することもできます。詳細については、「ルールを使用してデバイスにタグ付けする （81 ページ）」を参照してください。
- 既存のタグを使用する場合は、一覧からタグを選択して、[Apply] をクリックします。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

ステップ 4 デバイスからタグを削除するには、以下のいずれか 1 つを行います。

- Click **Create New Tag**, unselect all tags, and then click **APply**.
- タグアイコンまたはタグ名にカーソルを合わせて、[X] をクリックし、デバイスからタグの関連付けを解除します。

ルールを使用してデバイスにタグ付けする

ルールを定義するタグに基づいてデバイスをグループ化することができます。ルールを定義するとき、Cisco DNA Center は指定したルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリ、デバイスシリーズ、IP アドレス、ロケーション、またはバージョンに基づくことができます。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの隣のチェックボックスをオンにして、**[デバイスのタグ付け（Tag Device）]** をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力し、[ルールによる新規タグの作成（Create New Tag with Rule）] をクリックします。

[新規 VRF の作成（Create New VRF）] ウィンドウが表示されます。

[タグ付きデバイスの合計数（Total Devices Tagged Count）] の下の [手動で追加（Manually Added）] フィールドは、ステップ 2 で選択されたデバイスの合計数を示します。

ステップ 4 [条件の追加（Add Condition）] をクリックして、ルールに必要なフィールドに記入します。

[一致するデバイス（Matching Devices）] の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- *And* 条件— [条件の追加（Add Condition）] リンクをクリックします。**And** が条件の上に表示されます。
- *Or* 条件—既存の条件の隣の追加アイコン (+) をクリックします。**Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、指定したルールに一致するインベントリのデバイス数を反映して一致するデバイス数が変更されます。デバイス数でクリックして、ルールと一致するデバイスを表示できます。

ステップ 5 [保存（Save）] をクリックして、定義されたルールと共にタグを保存します。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義したruleと一致する場合、タグは自動的にデバイスに適用されます。

デバイスタグの編集

以前に作成したデバイスタグを編集できます。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

[デバイス名（Device Name）] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。

ステップ 2 デバイスを選択しないで、 [デバイスのタグ付け（Tag Device）] をクリックします。

以前に作成されたタグがリストされます。

ステップ 3 編集するタグをマウスオーバーして、タグ名の隣の鉛筆アイコンをクリックします。

代わりに、**[Tag Device]** > **[View All Tags]** の順に選択してから、編集するタグの横にある鉛筆アイコンをクリックすることもできます。

ステップ 4 タグを変更し、 [保存（Save）] をクリックして変更を保存します。

タグの削除

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

始める前に

デバイスに（ルールを使用して）静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。

デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 デバイスを選択しないで、**[Tag Device]** > **[Manage Tags]** の順に選択します。

ステップ 3 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。

ステップ 4 警告メッセージが表示されたら、[Yes] をクリックします。

タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージが生成されます。デバイスまたはテンプレートに関連付けられているタグを除去し、タグを削除します。

インベントリインサイト

[Inventory Insights] ウィンドウには、他の直接接続されたデバイスと設定が一致しないデバイスが表示されます。また、Cisco DNA Center のベストプラクティスの推奨事項と比較して、誤って設定されたデバイスも表示されます。Cisco DNA Center では、次のインサイトと推奨されるアクションが提供されます。

- 速度/デュプレックス設定の不一致
- VLAN の不一致

速度/デュプレックス設定の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる速度とデュプレックス値が設定されているデバイスが表示されます。

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]** > **[Network Devices]** > **[Inventory Insights]** の順に選択します。

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [Speed/Duplex settings mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

[Speed/Duplex settings mismatch] ウィンドウでは、速度とデュプレックスの不一致が強調表示されます。

ステップ 4 推奨アクションに従って、デバイス設定に必要な変更を加えます。

VLAN の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる VLAN が設定されているデバイスが表示されます。

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]** > **[Network Devices]** > **[Inventory Insights]** の順に選択します。

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [VLAN Mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

[VLAN Mismatch] ウィンドウに、許可された VLAN とネイティブ VLAN の不一致が強調表示されます。

ステップ 4 推奨アクションに従って、デバイス設定に必要な変更を加えます。

デバイスのロールの変更（インベントリ）

ディスカバリ プロセスに、Cisco DNA Center は検出された各デバイスにロールを割り当てます。デバイスのロールは、デバイスを特定してグループ化するためと、トポロジツールでネットワーク トポロジ マップのデバイスの配置を決定するために使用されます。最上位の層は、インターネットです。最下層のデバイスは、次のロールのいずれかに割り当てられます。

表 *35 :* デバイスのロールとトポロジの位置

トポロジの位置	デバイス ロール
階層 1	インターネット（設定不可）
階層 2	[Border Router]
階層 3	コア

トポロジの位置	デバイス ロール
階層 4	Distribution
階層 5	アクセス
階層 6	不明（Unknown）

（注） **アクセス**ロールをデバイスに割り当てると、IP デバイストラッキング（IPDT）が設定されるか、サイトの IPDT 設定に基づいてデバイスから削除されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 Locate the device whose role you want to change, click the pencil icon under the **Device Role** column, and choose a role from the **Update Device Role** dialog box. 有効な選択肢は、[Unknown] 、[Access] 、[Core] 、[Distribution] 、または [Border Router] です。

デバイスロールは次の手順で、[Edit Device] ダイアログボックスでも更新できます。

- ロールを変更するデバイスを選択します。
- **[Actions]** > **[Inventory]** > **[Edit Device]** の順に選択します。
- **[Role]** タブをクリックし、**[Device Role]** ドロップダウンリストから適切なロールを選択します。

（注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。

デバイスの管理 IP アドレスの更新

デバイスの管理 IP アドレスを更新することができます。

（注） 複数のデバイスを同時に更新することはできません。また、Meraki デバイスの管理 IP アドレスは更新できません。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウンリストから **[インベントリ（Inventory）]** > **[デバイスの編集（Edit Device）]** の順に選択します。

[Edit Device] ダイアログボックスが表示されます。

ステップ 4 **[IP の管理（Management IP）]** タブをクリックし、**[デバイス IP/DNS 名（Device IP/DNS Name）]** フィールドに新しい管理 IP アドレスを入力します。

（注） 新しい管理 IP アドレスが Cisco DNA Center から到達可能であり、デバイス クレデンシャルが正しいことを確認します。そうでない場合、デバイスが管理対象外状態になる可能性があります。

次のタスク

デバイスを再プロビジョニングして、送信元インターフェイスの設定を更新します。

デバイスポーリング間隔の更新

[System] > **[Settings]** > **[Network Resync Interval]** の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 更新するデバイスを選択します。

ステップ 3 [Update Polling Interval] をクリックします

ステップ 4 [Update Resync Interval] ダイアログボックスの [Status] フィールドで、[Enabled] をクリックしてポーリングを有効にするか、[Disabled] をクリックしてポーリングを無効にします。

ステップ 5 [Polling Time] フィールドには、継続的なポーリングサイクルの間隔（分単位）を入力します。有効な値は、25 ～ 1,440 分（24 時間）です。

（注） デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco DNA Center は引き続きデバイス固有のポーリング時間を使用します。

ステップ 6 [更新（Update）] をクリックします。

デバイス情報の再同期

選択したデバイスのデバイス情報は、再同期間隔の構成にかかわらず、ただちに再同期できます。同時に最大 40 台のデバイスを再同期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**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 関連する情報を収集するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから [Inventory] > [Resync Device] の順に選択します。 >

ステップ 4 [OK] をクリックします。

ネットワーク デバイスの削除

デバイスがまだサイトに追加されていない場合に限り、Cisco DNA Center データベースからデバイスを削除できます。

インベントリからワイヤレスセンサーを削除すると、センサーは工場出荷時のデフォルト状態にリセットされるため、再接続すると現在の構成が採用されます。

始める前に

この手順を実行するには、管理者（ROLE_ADMIN）権限、およびすべてのデバイスへのアクセス権（[RBAC Scope] を [ALL] に設定）が必要です。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

（注） さらにチェック ボックスをオンにして複数のデバイスを選択できますが、リストの上部にあるチェック ボックスをクリックしてすべてのデバイスを選択できます。

ステップ 3 [Actions] ドロップダウンリストから [Inventory] > [Delete Device] > の順に選択します。

ステップ 4 [Warning] ウィンドウで、[Config Clean-Up] チェックボックスをオンにして、選択したデバイスからネットワーク設定およびテレメトリ設定を削除します。

ステップ 5 [OK] をクリックして、アクションを確認します。

コマンド ランナーを起動（インベントリ）

[Inventory] ウィンドウで選択したデバイスのコマンド ランナー アプリケーションを起動することができます。

始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、Cisco DNA Center 管理者ガイド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]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 コマンドを実行するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[Others]** > **[Launch Command Runner]** の順に選択します。

実行可能なコマンドの詳細、およびこれらのコマンドの実行方法については、デバイスの診断コマンドを実行 （207 ページ）を参照してください。

Run コマンドを使用したデバイスの到達可能性の問題のトラブルシューティング

[Inventory] ウィンドウから [Run Commands] ウィンドウを起動し、ping、traceroute、snmpget などのプラットフォームコマンドを実行して、デバイス到達可能性の問題をトラブルシューティングできます。

（注） Cisco DNA Center クラスタでプラットフォームコマンドを直接実行する場合は、[Run Commands] を起動する前にデバイスを選択しないでください。そうしないと、プラットフォームではなくそのデバイスに対してコマンドが実行されます。

始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、Cisco DNA Center 管理者ガイド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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 [Actions] ドロップダウンリストから、**[Others]** > **[Run Commands]** の順に選択します。

man を入力すると、現在サポートされているコマンドおよびショートカットのリストをいつでも取得できます。

CSV ファイルを使用したデバイス設定のインポート/エクスポート

CSV ファイルのインポート

CSV ファイルを使用して、別のソースから Cisco DNA Center にデバイスの設定やサイトをインポートできます。サンプルテンプレートをダウンロードする場合は、[Provision Devices] ページに移動し、**[Actions]** > **[Inventory]** > **[Import Inventory]** を選択します。[Download Template] をクリックして、サンプル CSV ファイルテンプレートをダウンロードします。

CSV ファイルを使用してデバイスまたはサイト設定をインポートする場合、Cisco DNA Center がデバイスをどれだけ管理できるのかは CSV ファイルに指定する情報に依存します。CLI ユーザー名、パスワード、およびイネーブルパスワードの値を指定しない場合、Cisco DNA Center

の機能が制限され、デバイス設定の変更、デバイス ソフトウェア イメージの更新、および他の重要な機能の実行ができません。

CSV ファイルでクレデンシャル プロファイルを指定し、対応するクレデンシャルをデバイスのセットに適用できます。クレデンシャル プロファイルを指定して、CSV ファイルに手動で値も入力する場合、手動入力されたクレデンシャルが優先され、デバイスは手動入力されたクレデンシャルとクレデンシャル プロファイルの組み合わせに基づいて管理されます。たとえば、手動で入力した SNMP ログイン情報に加えて、SNMP および SSH または Telnet のログイン情報を含むログイン情報プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP ログイン情報とログイン情報プロファイル内の SSH または Telnet ログイン情報に基づいて管理されます。Telnet は非推奨です。

（注） また、指定したプロトコルに対応するフィールドにも値を入力する必要があります。たとえば、SNMPv3 を指定した場合、SNMPv3 のユーザー名や認証パスワードなど、サンプルの CSV ファイルの SNMPV3 フィールドに値を指定する必要があります。

Cisco DNA Center の部分的なインベントリ収集の場合は、CSV ファイルに次の値を指定する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値

Cisco DNA Center の完全なインベントリ収集では、CSV ファイルに以下の値を提供する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値
- Protocol
- CLI ユーザー名
- CLI パスワード

- CLI イネーブル パスワード
- CLI タイムアウト値

CSV ファイル エクスポート

Cisco DNA Center では、すべてまたは選択したデバイスを含む CSV ファイルをインベントリに作成できます。このファイルを作成するには、ファイルに含まれる設定データを保護するパスワードを入力する必要があります。

CSV ファイルからのデバイス設定のインポート

CSV ファイルからデバイス設定をインポートできます。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Actions] ドロップダウンリストから、[Inventory] > [Import Inventory] > を選択してデバイスのログイン情報をインポートします。

ステップ 3 [Bulk Import] ダイアログボックスのボックスエリアに CSV ファイルをドラッグアンドドロップするか、点線のボックスエリアをクリックして CSV ファイルを参照します。

ステップ 4 **[インポート (Import)]** をクリックします。

デバイスデータのエクスポート

選択したデバイスに関する特定のデータを CSV ファイルにエクスポートできます。CSV ファイルは圧縮されます。[Export] をクリックして、フィルタ処理されたデバイスまたはすべてのデバイスのデータをエクスポートします。

⚠

注意 CSV ファイルにはエクスポートされたデバイスに関する機密情報が含まれているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 特定のデバイスのみの構成情報をエクスポートするには、含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、デバイスリストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Inventory] > [Export Inventory] > を選択してデバイス設定をエクスポートします。

[Export Inventory] ダイアログボックスが表示されます。

ステップ 4 **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

ステップ 5 確認のために暗号化パスワードをもう一度入力します。

ステップ 6 [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

ステップ 7 [Export] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

デバイスのクレデンシャルのエクスポート

デバイスのクレデンシャル CSV ファイルにエクスポートできます。不要なアクセスからファイルを保護するために、パスワードを設定する必要があります。ファイルを開くことができるように、受信者にパスワードを提供する必要があります。

⚠

注意 CSV ファイルにはエクスポートされたデバイスのすべてのクレデンシャルがリストされているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 CSV ファイルに含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、リストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから **[Inventory]** > **[Export Inventory]** を選択します。

[Export] ダイアログボックスが表示されます。

ステップ 4 [Select Export Type] で、[Credentials] オプションボタンをクリックします。

ステップ 5 [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

ステップ 6 **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

ステップ 7 暗号化パスワードを確認し、[エクスポート（Export）] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

故障したデバイスの交換

ネットワーク内で障害が発生したデバイスを交換することは、デバイスのライフサイクル管理の重要な部分です。Cisco DNA Center の返品許可（RMA）ワークフローにより、障害が発生したデバイスを迅速に交換できるため、生産性が向上し、運用コストが減少します。RMA では、ルータ、スイッチ、および AP を共通のワークフローに従って交換できます。

ルータおよびスイッチで RMA ワークフローを使用すると、ソフトウェアイメージ、構成、およびライセンスが、障害が発生したデバイスから交換用デバイスに復元されます。ワイヤレス AP の場合、交換用デバイスは同じサイトに割り当てられ、プライマリワイヤレス LAN コントローラ、RF プロファイル、および AP グループ設定でプロビジョニングされ、障害が発生した AP と同じ Cisco DNA Center のフロアマップの場所に配置されます。

（注） **デバイス交換**ワークフローを使用して、故障したデバイスを交換することもできます。詳細については、デバイスの交換ワークフロー （557 ページ）を参照してください。

始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

ステップ 1 故障したデバイスを交換対象としてマークするには、次の手順を実行します。

a) Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

b) 交換する故障したデバイスを選択します。

c) [Actions] ドロップダウンリストから、**[Inventory]** > **[Device Replacement]** > **[Mark Device for Replacement]** を選択します。

d) [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

（注） ファブリックデバイスのシームレスな交換を実現するために、DHCP サーバーがネイバーデバイスで設定されます。これは、PnP でデバイスを Cisco DNA Center にオンボードするために、交換用デバイスに IP アドレスを割り当てるために必要です。この DHCP サーバーは、故障したデバイスが正常に交換されると削除されます。

障害のあるデバイスからの最新の構成変更は、RMA ワークフロー中に交換後のデバイスにプッシュされます。

e) [Inventory] ドロップダウンリストから、[Marked for Replacement] を選択します。

交換用としてマークされたデバイスのリストが表示されます。

f) （任意） デバイスを交換しない場合は、デバイスを選択して、**[Actions]** > **[Unmark for Replacement]** を選択します。

ステップ 2 （任意） デバイスを交換するには、次の手順を実行します。

a) 交換するデバイスを選択し、**[Actions]** > **[Replace Device]** を選択します。

b) [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

c) （任意） 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。

1. [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
2. [Add New Device] ウィンドウで、デバイスの**シリアル番号**を入力し、[Add New Device] をクリックします。

または

1. [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。
2. [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。

d) [Next] をクリックします。

e) [Schedule Replace] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時間でのデバイスの交換をスケジュールします。

交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時間でのデバイスの交換をスケジュールすることは可能です。

f) [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。

g) [Next] をクリックして [Summary] ウィンドウで詳細情報を確認します。

h) [Summary] ウィンドウで、次の手順を実行します。

1. 前の手順で選択したデバイスタイプ、故障したデバイス、または交換用デバイスを変更する場合は、[Edit] をクリックします。
2. [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。
3. [置換（Replace）] をクリックします。

i) [Click Monitor Replacement Status] をクリックして [Provision] ウィンドウの [Mark for Replacement] ビューに移動します。

j) 交換用デバイスの [Replace Status] をクリックすると、次のように RMA ワークフローの進捗状況が表示されます。

- （PnP）交換用デバイスを請求します。
- 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
- ライセンスを展開する。
- VLAN 構成をプロビジョニングします。
- スタートアップ構成をプロビジョニングします。
- 交換用デバイスをリロードします。
- 交換用デバイスの到達可能性を確認します。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- 交換用デバイスを同期します。
- 故障したデバイスを CSSM から削除します。
- 交換用デバイスを CSSM に追加します。
- PKI 証明書を失効化して作成します。
- Cisco ISE を更新します。
- 障害のあるデバイスを削除します。

ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

k) エラーメッセージが表示された場合は、エラーリンクをクリックします。

l) [Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

（注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

デバイスを交換対象としてマーキングする先行タスクと、デバイスを交換するタスクは、異なるタイミングで実行できます。

障害のあるアクセスポイントの交換

AP の RMA 機能を使用して、障害のある AP をデバイスインベントリに登録されている交換用 AP に交換できます。

始める前に

- AP の返品許可（RMA）機能では、同等の交換のみをサポートしています。モデル番号と PID が障害のある AP と同じ交換用 AP を用意する必要があります。
- 交換用 AP を障害のある AP と同じ シスコ ワイヤレス コントローラに接続しておく必要があります。
- ワイヤレスコントローラとして機能する Cisco Mobility Express AP は、交換用 AP の候補ではありません。
- 障害のある AP のソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換用デバイスにマークを付ける必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用 AP がプロビジョニング状態である必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。

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]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 交換する障害のあるデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Device Replacement]** > **[Mark Device for Replacement]** の順に選択します。

ステップ 4 [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

成功したことを示す「`Device(s) Marked for Replacement Successfully`」というメッセージが表示されます。

ステップ 5 [Replace Device] ウィンドウで、障害のあるデバイスと利用可能な交換用デバイスの詳細を確認します。

ステップ 6 [Available Replacement Devices] テーブルで、交換用デバイスの名前の横にあるオプションボタンをクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 [Replacement Summary] を確認し、[Next] をクリックします。

ステップ 9 デバイスを今すぐ交換するか、後で交換を行うようスケジュールするかを選択し、[Submit] をクリックします。

RMA ワークフローが開始されます。

ステップ 10 交換ステータスをモニターするには、[What's Next] で [Monitor Replacement Status] をクリックします。

[Mark For Replacement] ウィンドウに、交換用としてマークされているデバイスのリストが表示されます。

[Replace Status] 列で交換のステータスを確認します。当初は [In-Progress] と表示されます。

ステップ 11 [Replace Status] 列の [In-Progress] をクリックします。

[Replace Status] タブには、デバイス交換の一環として Cisco DNA Center で実行されるさまざまな手順が表示されます。

ステップ 12 [Marked for Replacement] ウィンドウで、[Refresh] をクリックしてから [Replacement History] をクリックして交換のステータスを確認します。

ステップ 13 障害のあるデバイスが正常に交換されていれば、[Replacement History] ウィンドウの [Replace] 列に [Replaced] と表示されます。

ステップ 14 （オプション）デバイスを交換しない場合は、デバイスを選択し、**[Actions]** > **[Unmark for Replacement]** の順に選択します。

Cisco DNA Center での RMA ワークフローの制限事項

- RMA は、類似デバイスの交換のみサポートしています。たとえば Cisco Catalyst 3650 スイッチは、別の Cisco Catalyst 3650 スイッチとのみ交換できます。また、故障したデバイスと交換用デバイスのプラットフォーム ID も同じである必要があります。
- RMA は、以下を除くすべてのスイッチ、ルータ、および Cisco SD-Access デバイスの交換をサポートします。
  - クラシックおよびポリシー拡張ノード
  - ワイヤレスコントローラが組み込まれたデバイス
  - ワイヤレスコントローラ（WLC）
  - Catalyst 9400、Catalyst 9600、Catalyst 4500e、Catalyst 6500、Catalyst 6800、Nexus 7700 シリーズ スイッチなど、シャーシベースのスイッチ
  - スイッチスタック（ハードウェアスタッキングおよび SVL スタッキング）
  - シングルおよびデュアル スーパーバイザ エンジンを搭載したデバイス

- サードパーティの証明書を持つデバイス
- 外部 SCEP ブローカ PKI 証明書を持つデバイス

- RMA ワークフローでは、次の場合にのみデバイスの交換が可能です。
  - 障害のあるデバイスと交換用デバイスの両方に同じ拡張カードが搭載されている。
  - 両方のデバイスのポート数が拡張カードによって変わらない。
  - 障害のあるデバイスは、Cisco DNA Center によって静的 IP で管理されます（RMA は、Cisco DNA Center によって DHCP IP で管理されるデバイスではサポートされません）。

- 交換用デバイスが、障害のあるデバイスが接続されていたポートと同じポートに接続されていることを確認してください。
- ファブリックデバイスのシームレスな交換を実現するために、DHCP サーバーがネイバーデバイスで設定されます。これは、PnP でデバイスを Cisco DNA Center にオンボードするために、交換用デバイスに IP アドレスを割り当てるために必要です。これは、/30 ネットワークでのみサポートされます。他のネットワークの場合は、ユーザーが、交換用デバイスに IP を手動で割り当て、デバイスを Cisco DNA Center にオンボードにする必要があります。
- Cisco DNA Center レガシーライセンスの導入はサポートされていません。

  RMA ワークフローにより、CSSM から故障したデバイスの登録が解除され、交換用デバイスが CSSM に登録されます。

  - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 よりも前のバージョンの場合、[License Details] ウィンドウにはネットワークと機能のライセンスの詳細が表示されず、警告メッセージも表示されません。そのため、障害のあるデバイスに設定されているレガシー ネットワーク ライセンスを確認し、交換用デバイスに同じレガシー ネットワーク ライセンスを手動で適用する必要があります。
  - 故障したデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 以降の場合は、[License Details] ウィンドウにネットワークライセンスの詳細（**レガシー**、**ネットワーク**など）と機能ライセンス（IP Base、IP Service、LAN Base など）が表示されます。障害のあるデバイスを交換対象としてマークしている際に、次の警告メッセージが表示されます。

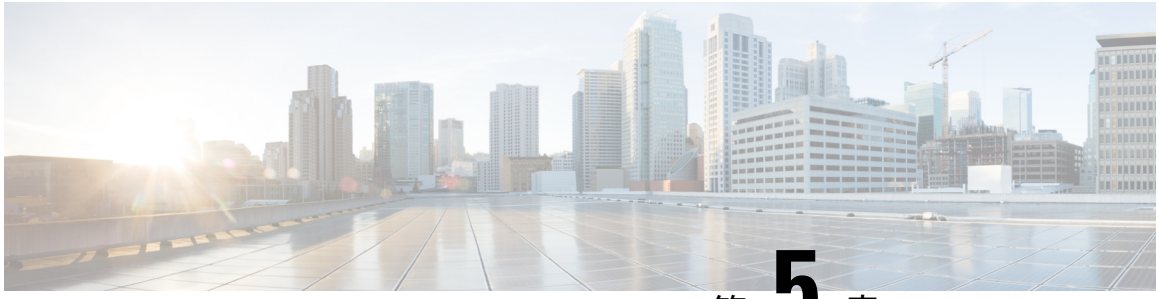
    ```
    Some of the faulty devices don't have a Cisco DNA license. Please
    ensure your replacement device has the same Legacy license of
    the faulty device enabled.
    ```

  - 交換用デバイスと障害のあるデバイスのレガシー ネットワーク ライセンスが一致しない場合は、ライセンスの展開中に次のエラーメッセージが表示されます。

    ```
    Cisco DNA Center doesn't support legacy license deployment.
    ```

    そのため、交換用デバイスで障害のあるデバイスのライセンスを手動で更新し、再同期してから続行してください。

- 交換用デバイスが PnP DHCP 機能によってオンボードされる場合は、リロードのたびにデバイスが同じ IP アドレスを取得し、DHCP のリースタイムアウトが 2 時間を超えていることを確認してください。



第 5 章

ソフトウェア イメージの管理

イメージ リポジトリについて

Cisco DNA Center は、ネットワークにあるデバイスのすべてのソフトウェアイメージとソフトウェア メンテナンス アップデート（SMU）、サブパッケージ、ROMMON イメージなどを保存します。イメージ リポジトリには次の機能があります。

- イメージリポジトリ：Cisco DNA Center はイメージタイプとバージョンに応じて、固有のソフトウェアイメージをすべて保存します。ユーザーはソフトウェアイメージの表示、インポート、および削除ができます。
- プロビジョニング：ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。

イメージリポジトリ機能を使用する前に、Cisco Catalyst 3000、4000、および 6000 などの古いデバイスで Transport Layer Security（TLS）プロトコルを有効にする必要があります。システムアップグレード後は、TLS を再度有効にする必要があります。詳細については、『Cisco DNA Center 管理者ガイド』[英語] の「Cisco DNA Center のセキュリティの構成」を参照してください。

ソフトウェア イメージの整合性検証

整合性検証アプリケーションでは、デバイスの感染を示す予期しない変更や無効な値がないか、Cisco DNA Center に格納されたソフトウェア イメージをモニターします。システムは、インポートプロセス中に、インポートしているイメージのソフトウェアおよびハードウェア プラットフォームのチェックサム値と、Known Good Values（KGV）ファイルのプラットフォームで識別されたチェックサム値を比較して、2 つの値の一致を確認することで、イメージの整合性を決定します。

整合性検証アプリケーションで現在の KGV ファイルを使用して選択したソフトウェアイメージを検証できない場合は、[Image Repository] ウィンドウにメッセージが表示されます。整合性検証アプリケーションおよび KGV ファイルのインポートの詳細については、*Cisco Digital Network Architecture Center* 管理者ガイド [英語] を参照してください。

ソフトウェア イメージの表示

ディスカバリを実行するか、手動でデバイスを追加した後、Cisco DNA Center は、デバイスのソフトウェア イメージ、SMU、およびサブパッケージに関する情報を自動的に保存します。

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**[Design]** > **[Image Repository]**。

ソフトウェアイメージは、デバイスタイプに基づいて編成され、表示されます。デフォルトでは、物理デバイス用のソフトウェア イメージが表示されます。仮想デバイスのソフトウェアイメージを表示するには、[Virtual] タブをクリックします。

（注） cisco.com のログイン情報が設定されていない場合、警告アラートが表示されます。

ステップ 2 [Family] 列で、下向き矢印をクリックすると、指定されたデバイスタイプファミリのすべてのソフトウェアイメージを表示できます。[Device(s)] 列には、[Image Name] フィールドで示された特定のイメージを使用しているデバイス数が示されます。デバイスの番号をクリックすると、そのイメージを使用しているデバイスが表示されます。

ステップ 3 [Version] 列で、[Add On] リンクをクリックすると、適用可能な [SMUs]、[Subpackages]、[ROMMON]、[APSP]、および基本イメージの [APDP] アップグレードが表示されます。

サブパッケージは、既存の基本イメージに追加できる追加の機能です。ここには、イメージファミリと基本イメージのバージョンに一致するサブパッケージバージョンが表示されます。

AP サービスパック（APSP）と AP デバイスパック（APDP）は、ワイヤレスコントローラに関連付けられた AP をアプグレードするためのイメージです。

- 新しい AP ハードウェアモデルが導入されると、既存のワイヤレスネットワークへの接続に APDP が使用されます。
- 関連付けられた AP の場合、重要な AP バグ修正が APSP によって適用されます。

（注） いずれかの SMU をゴールデンとしてタグ付けすると、基本イメージがインストールされたときに、それが自動的に有効化されます。

サブパッケージはゴールデンとしてタグ付けすることはできません。

ROMMON のアップグレードでは、cisco.com の設定が必須です。デバイスが追加されると、該当するデバイスの最新の ROMMON の詳細が cisco.com から取得されます。また、基本イメージのインポートまたは基本イメージのタグ付けがある場合、ROMMON イメージが cisco.com から自動的にダウンロードされます。

ステップ 4 [Advisory] 列で、[Critical] または [High] のアドバイザリの数をクリックして、特定のソフトウェアイメージのアドバイザリを表示します。

[Image Advisory] スライドインペインには、ソフトウェアイメージの**ファミリ名**、**バージョン**、および**アドバイザリ**が表示されます。アドバイザリは、[Critical]、[High]、[Medium]、[Low]、および [Informational] に分類されます。

[CRITICAL]、[HIGH]、または [MEDIUM] をクリックして、各カテゴリに固有のアドバイザリを表示します。

アドバイザリを修正するには、次の手順を実行します。

a) [Fix Advisories] をクリックします。
[Image Update] ウィンドウが表示されます。

b) デバイスを更新する推奨ソフトウェアイメージを選択します。

推奨されるソフトウェアイメージがイメージリポジトリにない場合は、cisco.com からダウンロードできます。

c) [Download and Mark Golden] をクリックします。

d) [Download Image] ダイアログボックスで、次のいずれかを実行します。

- [Mark the image as gold after download] チェックボックスをオン（デフォルト）のままにします。その後、[Download] をクリックします。ソフトウェアイメージがダウンロードされ、ゴールデンとしてマークされます。
- [Mark the image as golden after download] チェックボックスをオフにし、[Download] をクリックします。ソフトウェアイメージがリポジトリにダウンロードされますが、ゴールデンとはマークされません。

e) [OK] をクリックします。
ソフトウェアイメージがダウンロードされます。[Show Tasks] で進捗状況を確認することができます。

ステップ 5 [Device Role] 列で、これがゴールデン ソフトウェア イメージであることを示すデバイスロールを選択します。詳細については、ゴールデン ソフトウェアのイメージについて （107 ページ）およびゴールデン ソフトウェア イメージの指定 （107 ページ）を参照してください。

推奨されるソフトウェア イメージの使用

Cisco DNA Center は、管理しているデバイスの Cisco 推奨のソフトウェア イメージを表示します。ユーザーはそこから選択できます。

（注） シスコが推奨する最新のソフトウェアイメージのみ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（≡）をクリックして選択します**[System]** > **[Settings]** > **[Cisco.com Credentials]** の順に選択します。

ステップ 2 cisco.com に接続するための正しいログイン情報が入力されていることを確認します。

ステップ 3 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Image Repository]**。

Cisco DNA Center は、デバイス タイプに従って Cisco 推奨のソフトウェア イメージを表示します。

ステップ 4 推奨のイメージをゴールデンとして指定します。詳細については、「ゴールデン ソフトウェア イメージの指定 （107 ページ）」を参照してください。

Cisco 推奨のイメージをゴールデンとして指定すると、Cisco DNA Center はそのイメージを cisco.com から自動的にダウンロードします。

ステップ 5 推奨のソフトウェア イメージをネットワーク内のデバイスにプッシュします。詳細については、「ソフトウェア イメージのプロビジョニング （109 ページ）」を参照してください。

ソフトウェア イメージのインポート

ローカル コンピュータまたはURL から、ソフトウェア イメージおよびソフトウェア イメージ更新プログラムをインポートできます。

インポートされたイメージは、特定のデバイスファミリに存在するさまざまなスーパーバイザに基づいて分類されます。異なるスーパーバイザによる分類では、Catalyst 9400 シリーズ ファミリのみがサポートされます。

FTP を使用して FTP サーバからイメージをインポートする場合は、FTP 標準を使用します。

```
ftp://username:password@ip_or_hostname/path
```

ステップ 1 [Design] > [Image Repository]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します。

ステップ 2 [Import] をクリックします。

ステップ 3 **[Choose File]**をクリックして、ローカルに保存されているソフトウェアイメージまたはソフトウェアイメージ更新プログラムに移動するか、[Enter image URL] をクリックしてソフトウェア イメージまたはソフトウェア イメージ更新プログラムのインポート元となる HTTP または FTP ソースを指定します。

ステップ 4 インポートするイメージがサードパーティ（シスコ以外）ベンダー向けの場合、**[Source]** で **[Third Party]** を選択します。次に **[Application Type]** を選択して、デバイスの **[Family]** を示し、**[Vendor]** を特定します。

ステップ 5 [Import] をクリックします。

ウィンドウにインポートの進行が表示されます。

ステップ 6 **[タスクの表示（Show Tasks）]** をクリックして、イメージが正常にインポートされたことを確認します。

SMU をインポートした場合、Cisco DNA Center は自動的に SMU を適切なソフトウェア イメージに適用し、対応するソフトウェア イメージの下に **[Add-On]** リンクが表示されます。

ステップ 7 **[Add-On]** リンクをクリックすると、SMU が表示されます。

ステップ 8 [Device Role] フィールドで、この SMU をゴールデンとしてマークするロールを選択します。詳細については、「ゴールデン ソフトウェア イメージの指定 （107 ページ）」を参照してください。

SMU をゴールデンとしてマークするには、事前に対応するソフトウェア イメージをゴールデンとしてマークしている必要があります。

デバイスファミリへのソフトウェアイメージの割り当て

ソフトウェアイメージをインポートした後、使用可能なデバイスファミリに割り当てたり割り当てを解除したりできます。インポートしたイメージは、いつでも複数のデバイスに割り当てることができます。

インポートしたソフトウェアイメージをデバイスファミリに割り当てるには、次の手順を実行します。

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**[Design]** > **[Image Repository]**。

ステップ 2 [Imported Images] をクリックします。

ステップ 3 [Assign] リンクをクリックします。

ステップ 4 [Assign Device Family] ウィンドウで、[Device Series from Cisco.com] または [All Device Series] を選択し、イメージのマッピング先の [Assign] リンクをクリックします。

ステップ 5 グローバル階層から適切なサイトを選択して [Assign] をクリックし、[Save] をクリックします。

ステップ 6 イメージの割り当てを解除するには、グローバル階層からサイトを選択し、[Action] 列の [Unassign] リンクをクリックします。

ソフトウェアイメージがデバイスファミリに割り当てられ、そのイメージを使用しているデバイスの数が [Using Image] 列に表示されます。イメージを割り当てたら、そのイメージをゴールデンイメージとしてマークできます。「ゴールデン ソフトウェア イメージの指定」を参照してください。

デバイスファミリがゴールデンイメージとしてマークされている場合、そのイメージをデバイスファミリから削除することはできません。

（注） PnP デバイスでは、デバイスが使用可能になる前に、ソフトウェアイメージをインポートしてデバイスファミリに割り当てることができます。また、イメージをゴールデンイメージとしてマークすることもできます。デバイスがインベントリで使用可能になると、そのデバイスファミリに割り当てられたイメージが、そのデバイスファミリの新しく追加されたデバイスに自動的に割り当てられます。

イメージがインポートされ、Cisco DNA Center に cisco.com ログイン情報が追加されると、Cisco DNA Center はイメージに適用可能なデバイスファミリのリストを提供します。リストから、必要なデバイスファミリを選択できます。

イメージが cisco.com で使用できない場合、またはログイン情報が Cisco DNA Center に追加されていない場合は、そのイメージに適したデバイスファミリを設計する必要があります。

デバイスのソフトウェアイメージをインストールモードでアップロード

[イメージリポジトリ（Image Repository）] ページでは、ソフトウェア イメージがインストール モードの状態として表示されることがあります。デバイスがインストール モードの場合、Cisco DNA Center は、ソフトウェア イメージをデバイスから直接アップロードできません。デバイスがインストール モードのときは、次の手順で示すように、最初に手動でソフトウェア イメージを Cisco DNA Center リポジトリへアップロードしてから、イメージをゴールデンとしてマーキングします。

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**[Design]** > **[Image Repository]**。

ステップ 2 [Image Name] カラムで、[Install Mode] で実行中のデバイスのソフトウェアイメージを検索します。

ステップ 3 [インポート（Import）] をクリックして、インストール モードであるイメージのバイナリ ソフトウェア イメージ ファイルをアップロードします。

ステップ 4 [ファイルの選択（Choose File）] をクリックしてローカルに保存されているソフトウェア イメージへ移動するか、または [イメージのURLを入力（Enter image URL）] でソフトウェア イメージのインポート元となる HTTP または FTP を指定します。

ステップ 5 [Import] をクリックします。

ウィンドウにインポートの進行が表示されます。

ステップ 6 [タスクの表示（Show Tasks）] をクリックして、インポートしたソフトウェア イメージが、正常にインポートされ、Cisco DNA Center リポジトリに追加されたことを示す緑色であることを確認します。

ステップ 7 [Refresh] をクリックします。

[イメージリポジトリ（Image Repository）] ウィンドウを更新します。Cisco DNA Center にソフトウェア イメージが表示され、[ゴールデンイメージ（Golden Image）] および [デバイスロール（Device Role）] 列がグレー表示ではなくなります。

ゴールデン ソフトウェアのイメージについて

Cisco DNA Center では、ソフトウェア イメージと SMU をゴールデンとして指定できます。ゴールデン ソフトウェア イメージや SMU は、特定のデバイス タイプのコンプライアンス要件を満たす検証済みのイメージです。ソフトウェア イメージや SMU をゴールデンとして指定すると、反復的な設定変更の必要がなくなることで時間を節約でき、デバイス間の一貫性を確保できます。標準化されたイメージを作成するために、イメージと対応する SMU をゴールデンとして指定できます。特定のデバイス ロールのゴールデン イメージを指定することもできます。たとえば、Cisco 4431 統合サービス ルータ デバイス ファミリのイメージがある場合、アクセス ロールだけを持つ Cisco 4431 デバイスに対するゴールデン イメージを追加で指定できます。

対応するイメージもゴールデンとしてマークされていない限り、SMUをゴールデンとしてマークすることはできません。

ゴールデン ソフトウェア イメージの指定

デバイス ファミリまたは特定のデバイス ロールに対するゴールデン ソフトウェア イメージを指定することができます。デバイスロールは、ネットワークにおける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。

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**[Design]** > **[Image Repository]**。

デバイス タイプに従ってソフトウェア イメージが表示されます。

ステップ 2 **[ファミリ（Family）]** 列で、ゴールデン イメージを指定するデバイス ファミリを選択します。

ステップ 3 **[イメージ名（Image Name）]** 列で、ゴールデン イメージとして指定するソフトウェア イメージを選択します。

ステップ 4 **[デバイス ロール（Device Role）]** 列で、ゴールデン イメージを指定するデバイス ロールを選択します。同じデバイス ファミリのデバイスを所有していたとしても、各デバイス ロールに異なるゴールデン イメージを指定することができます。物理イメージのデバイス ロールのみ選択できます。仮想イメージは選択できないことに注意してください。

ゴールデン イメージとして指定したソフトウェア イメージが Cisco DNA Center リポジトリにアップロードされていない場合は、このプロセスには多少時間がかかります。**[イメージ リポジトリ (Image Repository)]** ページの **[アクション (Action)]** 列で、ゴミ箱アイコンがグレー表示されている場合、イメージはまだ Cisco DNA Center リポジトリにアップロードされていません。Cisco DNA Center では最初にソフトウェア イメージをリポジトリにアップロードする必要があります。その後、イメージをゴールデンとしてマークするこ

とができます。ソフトウェア イメージが **[アクション（Action）]** 列のアクティブなごみ箱アイコンで示された Cisco DNA Center リポジトリに既にアップロードされている場合、ゴールデン イメージを特定するプロセスはより速く完了します。

イメージ配信サーバの設定

イメージ配信サーバは、ストレージとソフトウェアの配布に役立ちます。ソフトウェアイメージ配信用の外部イメージ配信サーバを設定したり、新しく追加されたイメージ配信サーバに 1 つ以上のプロトコルを設定したりできます。

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]** > **[Settings]** > **[Device Settings]** の順に選択します。

ステップ 2 [Device Settings] ドロップダウンリストから、[Image Distribution Servers] を選択します。

ステップ 3 [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバのホスト、ユーザ名、SFTP、SCP、および接続の詳細が表示されます。

ステップ 4 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server] スライドインペインが表示されます。

ステップ 5 イメージ配信サーバについて、次の項目を設定します。

- [Host]：イメージ配信サーバのホスト名または IP アドレス。
- [Root Location]：ファイル転送にルートディレクトリを使用する場合は、[Use root directory for file transfers] チェックボックスをオンにします。それ以外の場合は、[Use root directory for file transfers] チェックボックスをオフにしてルートの場所を入力します。

  （注） Cisco AireOS コントローラの場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [SFTP and SCP] を展開します。
- [Username]：イメージ配信サーバへのログインに使用される名前。ユーザには、サーバの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [パスワード]：イメージ配信サーバへのログインに使用されるパスワード。
- [ポート番号]：イメージ配信サーバが実行されているポート番号。

ステップ 6 [**Save**] をクリックします。

ステップ 7 設定を編集するには、[Action] 列で対応するイメージ配信サーバの [Edit] アイコンをクリックし、[Edit] ウィンドウで必要な変更を行って [Save] をクリックします。

ステップ 8 イメージ配信サーバを削除するには、[Action] 列で対応するイメージ配信サーバの [Delete] アイコンをクリックし、[Delete] をクリックします。

サイトへのイメージ配信サーバの追加

地理的に異なる地域にある SFTP サーバを、サイト、ビルディング、およびフロアに関連付けることができます。ネットワーク階層内のすべてのデバイスは、ネットワークのアップグレードの際、関連付けられたイメージ配信サーバを使用します。

始める前に

イメージ配信サーバを設定する必要があります。『イメージ配信サーバの設定（108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**[Design]** > **[Network settings]**。

ステップ 2 左ペインで、イメージ配信サーバを関連付けるサイトを選択します。

ステップ 3 [サーバの追加（Add Servers）] をクリックします。

ステップ 4 [Add Servers] ウィンドウで、[Image Distribution] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Primary] ドロップダウンリストをクリックし、プライマリとして設定するイメージ配信サーバを選択します。

ステップ 7 [Secondary] ドロップダウンリストをクリックし、セカンダリとして設定するイメージ配信サーバを選択します。

ステップ 8 [Save] をクリックします。

ソフトウェア イメージのプロビジョニング

ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。ソフトウェアイメージをデバイスにプッシュする前に、Cisco DNA Center はデバイス管理ステータスの確認、ディスク容量の確認など、デバイスのアップグレード準備の事前チェックを実行します。事前チェックに失敗した場合は、ソフトウェアイメージの更新を実行できません。デバイスのソフトウェア イメージをアップグレード後、 Cisco DNA Center は CPU 使用率、ルート サマリなどを確認し、イメージのアップグレード後にネットワークの状態が変更されていないことを保証します。

（注） 複数のデバイスに対して事前チェックを実行できます。

Cisco DNA Center は、各デバイスのソフトウェア イメージを、その固有のデバイス タイプに対してゴールデンと指定したイメージと比較します。デバイスのソフトウェアイメージとゴールデンイメージに違いがある場合、Cisco DNA Center はデバイスのソフトウェアイメージを無効とします。これらのデバイスに対するアップグレード準備の事前チェックがトリガーされます。すべての事前チェックをクリアしたら、新しいイメージをデバイスに配信（コピー）し、有効化（新しいイメージを実行中のイメージにすることが）できます。新しいイメージの有効化には、デバイスの再起動が必要です。再起動によって現在のネットワークアクティビティが中断される可能性があるため、後でプロセスをスケジュールすることができます。

そのデバイスタイプにゴールデンイメージを指定していない場合、そのデバイスのイメージは更新できません。『ゴールデン ソフトウェア イメージの指定 （107 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]** > **[Devices]** > **[Inventory]**。

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択します。イメージをアップグレードするデバイスを選択します。

（注） デバイスの事前チェックに成功したら、[OS Image] カラムの [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのマークが赤色に変わり、そのデバイスの OS イメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。

デバイスのアップグレードの準備の事前チェック リスト （112 ページ） を参照してください。

ステップ 3 **[Actions]** ドロップダウンリストから、**[Software Images]** > **[Update Image]** を選択します。

ステップ 4 [Distribute]：[Now] をクリックしてすぐに配信を開始するか、[Later] をクリックして特定の時間に配信のスケジュールを設定します。

（注）
- 外部イメージ配信サーバをネットワーク階層に関連付けている場合、ネットワーク階層下のすべてのデバイスへのイメージ配信は、イメージ配信サーバから行われます。サイトへのイメージ配信サーバの追加 （109 ページ）を参照してください。
- 選択したデバイスに既にイメージが配信されている場合、配信プロセスはスキップされ、イメージの有効化のみ可能になります。
- [SWIM Events for ITSM (ServiceNow)] バンドルが有効になっている場合は、後でイメージを更新（配布およびアクティブ化）する必要があります。イメージを更新するために [Now] をクリックしないでください。ここでイメージを更新する必要がある場合は、まずバンドルとその統合ワークフロー（ServiceNowでのイメージ更新スケジュールの承認）を無効にする必要があります。バンドルにアクセスするには、[Platform]、[Manage]、[Bundles]、[SWIM Events for ITSM（ServiceNow）] の順にクリックします。[SWIM Events for ITSM（ServiceNow）] ウィンドウの [Disable] ボタンをクリックします。バンドルとワークフローを無効にするプロセスには数秒かかるため、イメージの更新に進む前に数秒待ちます。

ステップ 5 **[Next]** をクリックします。

ステップ 6 [Activate]：[Now] をクリックして直ちに有効化を開始するか、[Later] をクリックして特定の時間に有効化をスケジュールします。

（注） 今は配信プロセスのみを実行する場合、この手順をスキップすることができます。

ステップ 7 （任意）[Initiate image activation right after distribution is completed successfully] チェックボックスをオンにします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Checks]：現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。

b) オンとオフを切り替えるトグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。

c) 新しいカスタム事前チェックと事後チェックをステージごとに追加するには、次の手順を実行します。

- [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウン矢印をクリックし、必要に応じて事前か事後またはその両方を選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。[Additional Criteria] 領域を展開し、[Distribution] か [Activation] または両方の操作段階を選択します。
- [Additional Criteria] 領域で、[Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。

d) [**保存（Save）**] をクリックします。

e) カスタムチェックを編集する場合は、対応するその他のアイコンをクリックし、[Edit] を選択します。

f) 必要な変更を行って、**[保存（Save）]** をクリックします。

g) カスタムチェックを削除する場合は、対応するその他のアイコンをクリックし、[Delete] を選択します。

h) [Confirm Delete] メッセージで [Delete] をクリックします。

ステップ 10 **[確認（Confirm）]**：[確認（Confirm）] をクリックして、更新を確認します。

更新のステータスは、[OS の更新ステータス（OS Update Status）] 列で確認できます。このカラムが表示されない場合は、 をクリックして、[OS Update Status] を選択します。

[See Details] リンクをクリックすると、イメージ更新ステータスの詳細を表示できます。

デバイスのアップグレードの準備の事前チェック リスト

事前チェック	説明
ファイル転送のチェック	HTTPS と SCP を通じてデバイスに到達できるかどうかをチェックします。 プロトコルのデフォルトの順序は、HTTPSが先で、SCP はその後です。
NTP クロックのチェック	デバイスの時間と Cisco DNA Center の時間を比較して、Cisco DNA Center 証明書が正常にインストールされていることを確認します。
フラッシュのチェック	更新に十分なディスク容量があるかどうか確認します。十分なディスク容量がない場合、警告またはエラー メッセージが返されます。自動フラッシュ クリーンアップでサポートされるデバイスとファイルの削除方法については、自動フラッシュクリーンアップを参照してください。
設定レジスタのチェック	設定レジスタの値を確認します。
暗号化 RSA チェック	RSA 証明書がインストールされているかどうかチェックします。
暗号化 TLS のチェック	デバイスが TLS 1.2 をサポートしているかどうかチェックします。
IP ドメイン名のチェック	ドメイン名が設定されているかどうかチェックします。
スタートアップ設定のチェック	このデバイス用のスタートアップ設定があるかどうかを確認します。
NFVIS Flash のチェック	NFVIS デバイスでゴールデンイメージをアップグレードする準備ができているかどうかを確認します。
サービス契約のチェック	デバイスに有効なライセンスがあるかどうかを確認します。

イメージ更新ステータスの表示

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]** > **[Devices]** > **[Inventory]**。

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択します。

デフォルトでは、[Image Update Status] ウィンドウに最近のすべてのイメージ更新タスクが表示されます。下矢印をクリックし、[Failed]、[In-progress]、[Success] のいずれかのタスクを選択できます。

ステップ 4 各タスクに対応する下矢印をクリックし、次の手順を実行してタスクの詳細を表示します。

a) [Show Scripts] をクリックして、事前チェックと事後チェックのステータスを表示します。
b) [View] をクリックして、事前チェックと事後チェックの詳細を表示します。

c) [View Diff] をクリックして、事前チェックと事後チェックの差異を表示します。

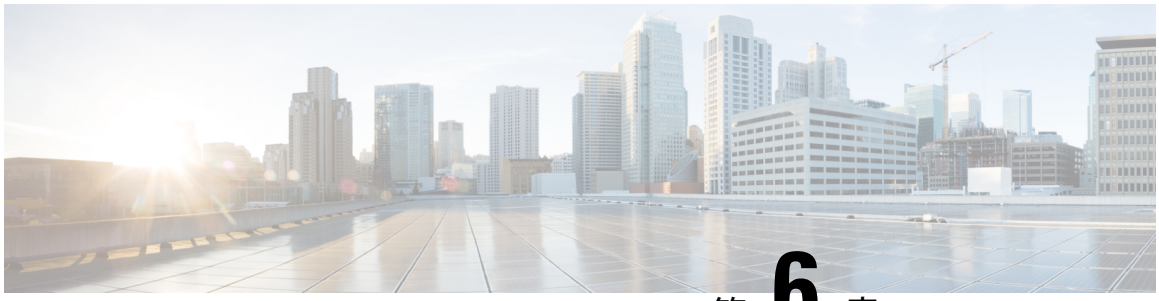
自動フラッシュクリーンアップ

デバイスのアップグレード準備の事前チェックの間、フラッシュのチェックにより、新しいイメージをコピーするための十分なスペースがデバイスにあるかどうかが確認されます。スペースが十分でない場合：

- **自動フラッシュクリーンアップをサポートしているデバイスの場合**：フラッシュのチェックが失敗し、警告メッセージが表示されます。このようなデバイスの場合、十分なスペースを作成するために、イメージの配信プロセス中に自動クリーンアッププロセスが試行されます。自動フラッシュクリーンアップの一環として、Cisco DNA Center は未使用の .bin、.pkg、および .conf ファイルを特定し、デバイスに十分な空き領域ができるまでそれらのファイルの削除を繰り返します。イメージの配信はフラッシュクリーンアップ後に試行されます。削除されたファイルは **[システム（System）]** > **[監査ログ（Audit Logs）]** で確認できます。

（注） 自動フラッシュクリーンアップは、Nexus スイッチとワイヤレスコントローラを除くすべてのデバイスでサポートされています。

- **自動フラッシュクリーンアップをサポートしていないデバイスの場合**：フラッシュのチェックが失敗し、エラーメッセージが表示されます。イメージのアップグレードを開始する前に、デバイスのフラッシュからファイルを削除して、必要なスペースを作成できます。



第 6 章

ネットワーク トポロジを表示

トポロジについて

[Topology] ウィンドウはネットワークのグラフィック ビューを表示します。Cisco DNA Center は、ユーザーが設定したディスカバリ設定を使用してネットワーク内のデバイスを検出して、デバイス ロールを割り当てます。検出中に割り当てられた（またはデバイス インベントリ内で変更された）デバイス ロールに基づいて、Cisco DNA Center は詳細なデバイス レベルのデータを使用して物理トポロジ マップを作成します。

トポロジ マップを使用すると、次のことができます。

- 選択したエリア、サイト、ビルディング、またはフロアのトポロジを表示する。
- 詳細なデバイス情報を表示する。
- 詳細なリンク情報を表示する。
- 特定のレイヤ 2 VLAN に基づいてデバイスをフィルタ処理する。
- レイヤ 3 プロトコル（Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、スタティック ルーティング）に基づいてデバイスをフィルタ処理する。
- Virtual Routing and Forwarding（VRF）機能を使用してデバイスをフィルタ処理する。

- トポロジ マップにデバイスをピン留めする
- トポロジ マップ レイアウトの保存
- トポロジ マップ レイアウトを開く
- トポロジ レイアウト全体のスクリーンショットを PNG 形式でエクスポートする。

エリア、サイト、ビルディング、フロアのトポロジを表示

エリア、サイト、ビルディングまたはフロアのトポロジを表示できます。

始める前に

- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ネットワーク階層を定義し、ビルディングまたはその内部のフロアにデバイスをプロビジョニングしている必要があります。

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[Tools] > [Topology] の順に選択します。

ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 トグルボタン  を使用して、地理的マップビューとレイヤ2マップビューを切り替えます。

地理的マップビューにサイトが表示されます。近いサイトがグループ化され、グループ内のサイト数とともに示されます。デバイスの正常性は異なる色で示されます。サイトの上にカーソルを移動すると、デバイスの正常性の詳細が表示されます。

右上隅の [Search] フィールドを使用して、地理的マップビューのビルディング、およびレイヤ 2 マップビューのデバイスを検索できます。

（注）
- 右下隅にあるアイコン ⓘ をクリックすると凡例が開き、トポロジマップで利用可能なショートカットキーが表示されます。
- [Toggle Annotate] アイコンをクリックして、レイヤ 2 マップに注釈を描画します。[export] アイコンをクリックして、トポロジマップを注釈とともにエクスポートできます。

ステップ 4 [Take a Tour] をクリックすると、[Topology] ページで使用できるさまざまなオプションの詳細を確認できます。

トポロジ マップでデバイスをフィルタリング

次のいずれかの属性に基づいてデバイスをフィルタ処理できます。

- VLAN
- Routing
- VRF
- タギング

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 [Filter] をクリックします。

（注） [Filter] を表示できない場合は、左側のツリービューメニューでサイトをクリックします。

ステップ 3 次のいずれかを実行します。

- [VLAN] ドロップダウン リストから表示する VLAN を選択します。
- [ルーティング（Routing）] ドロップダウン リストから目的のプロトコルを選択します。
- [VRF] ドロップダウン リストから表示する VRF を選択します。
- [View All Tags] をクリックして、表示するタグを選択します。選択したタグに関連付けられているデバイスが強調表示されます。新しいタグを作成するには、次の手順を実行します。

a) [Create New Tag] をクリックします。
b) [Tag Name] にタグ名を入力します。
c) **[Save]** をクリックします。

また、次の手順を実行して、デバイスをタグに関連付けることもできます。

a) デバイスをクリックします。
b) [Tag Device] をクリックします。
c) デバイスを関連付けるタグを選択します。
d) [Apply] をクリックします。

デバイス情報の表示

デバイス名、IP アドレス、およびデバイスのソフトウェア バージョンを表示することができます。

（注） **[トポロジ（Topology）]** ウィンドウでアクセス可能なデバイス情報には、**[デバイス インベントリ（Device Inventory）]** ウィンドウでもアクセス可能です。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 トポロジ エリアで、興味のあるデバイスまたはデバイス グループにマウス オーバーします。

（注） デバイス グループには、含まれているデバイスの数と種類がラベル付けされています。スイッチにホストがある場合、青い矢印がスイッチの下に表示されます。青い矢印をクリックすると、ホストが表示されます。

ステップ 4 [Display] をクリックして以下の項目を有効にすると、デバイスの詳細が表示されます。項目の横にあるアイコンにカーソルを合わせると、詳細情報を確認できます。

- [Device Health]：デバイスの正常性が表示されます。
- [Link Health]：デバイス間のリンクの正常性が表示されます。
- [License status]：デバイスのライセンスステータスが表示されます。デバイスのライセンスが期限切れに近づくと、強調表示され、デバイスの横に警告アイコンが表示されます。強調表示されたデバイスをクリックすると、そのライセンスの詳細が表示されます。
- [Device IP]：デバイスラベルの下にデバイスの IP アドレスが表示されます。
- [Device Suffixes]：デバイスのフルネームが、サフィックスと一緒に表示されます。

リンク情報の表示

トポロジマップ内のリンクに関する情報を表示できます。単純なリンクの場合は、1つのリンクの情報が表示されます。集約されたリンクの場合は、基本となるすべてのリンクのリストが表示されます。情報には、インターフェイス名、その速度、およびその IP アドレスが含まれます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 興味のあるリンクにカーソルを合わせます。

ステップ 4 [Display] をクリックして、[Link Health] を有効にします。

ダウンリンクは赤色で表示されます。リンクを削除する場合は、削除するリンクを選択して [Delete] をクリックします。次の手順を実行して、リンクをアップさせることができます。

a) デバイスにログインします。
b) インターフェイスをイネーブルにします。
c) [Inventory] ページでデバイスを再同期します。

トポロジ マップにデバイスをピン留めする

デバイスをグループ化または集約して、マップ上に表示するスペースを削減できます。ただし、グループからデバイスを区別する必要がある場合があります。これは、デバイスをマップにピン留めすることで可能になります。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 次のいずれかを実行します。

- デバイスをピン留めするには、デバイス グループをクリックして、デバイス名の左にあるピンのアイコンをクリックします。
- すべてのデバイスをピン留めするには、デバイス グループをクリックして、ダイアログボックスで、[すべてピン留め（Pin All）] をクリックします。

（注） グループをダブルクリックすると、グループ内のデバイスのピン留めが解除されます。

サイトへのデバイスの割り当て

デバイスは、トポロジ マップを使用して、特定のサイトに割り当てることができます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 左側のペインの [未割り当てのデバイス（Unassigned Devices）] をクリックします。未割り当てのデバイスはすべて、トポロジ領域に表示されます。

ステップ 3 サイトの割り当て先となるデバイスをクリックします。デバイスの詳細がポップアップウィンドウに表示されます。[Assign devices to:] セクションで、[choose the location] ドロップダウンリストをクリックして場所を選択します。

ステップ 4 （オプション）サイトを選択したデバイスにのみ割り当て、接続済みの（ダウンストリーム）デバイスには割り当てない場合、[Auto-assign unclaimed downstream devices] チェックボックスのチェックを外します。

ステップ 5 [**Assign**] をクリックします。

トポロジ マップ レイアウトの保存

Cisco DNA Center には Cisco 推奨のトポロジ レイアウトがあり、トポロジ ツールを開いたときにこれがデフォルトで表示されます。複数のレイアウトをカスタマイズし、後で確認するために保存できます。またレイアウトの 1 つを、トポロジマップを開いたときに表示されるデフォルトとして設定することもできます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2 [Custom View] をクリックします。

ステップ 3 [表示タイトルの入力（Enter View Title）] フィールドに、カスタマイズしたマップの名前を入力します。

ステップ 4 **[Save]** をクリックします。

ステップ 5 （任意） カスタマイズしたマップをデフォルトとして設定するには、[Make Default] をクリックします。

トポロジ マップ レイアウトを開く

以前に保存したトポロジ マップを開くことができます。

始める前に

トポロジ マップ レイアウトが保存済み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[Tools] > [Topology] の順に選択します。

ステップ 2 [Custom View] をクリックします。

ステップ 3 表示するマップの名前をクリックします。

トポロジのレイアウトをエクスポート

完全なトポロジレイアウトのスナップショットをエクスポートできます。スナップショットは、SVG、PDF、PNG ファイルとしてローカル マシンにダウンロードされます。

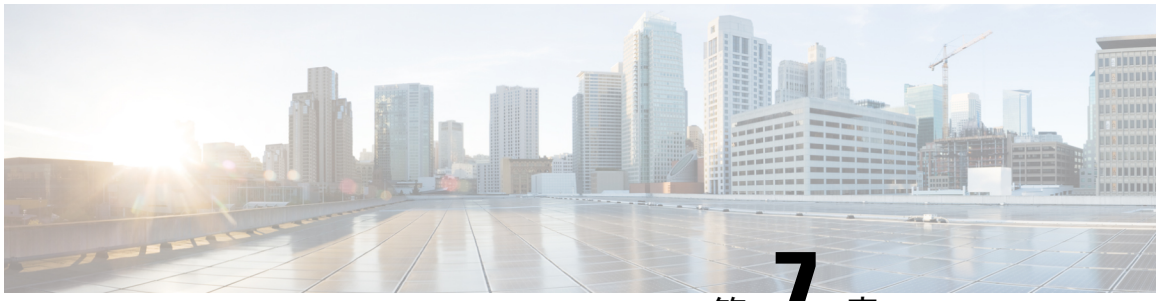
始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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[Tools] > [Topology] の順に選択します。

ステップ 2  （このアイコンは [トポロジのエクスポート（Export Topology）]) をクリックします。

ステップ 3 ファイル形式を選択し、[エクスポート（Export）] をクリックします。



第 7 章

ネットワーク階層と設定を設計

新しいネットワーク インフラストラクチャの設計

[Design]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、「ディスカバリについて （19 ページ）」を参照してください。

これらのタスクは、[Design] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。詳細については、ネットワーク階層のサイトの作成 （125 ページ）を参照してください。

ステップ 2 グローバル ネットワーク設定を定義します。詳細については、グローバルネットワーク設定の管理 （184 ページ）を参照してください。

ステップ 3 ネットワーク プロファイルを定義します。

ネットワーク階層について

ネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層には、ビルディングやエリアを含むサイトを含めることができます。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。

ネットワーク階層は、次の事前設定された階層をもちます。

- [エリア（Areas）] や [サイト（Sites）] には、物理的なアドレス（例、米国）はありません。エリアは最大の要素だと考えることができます。エリアにはビルディングとサブエリアを含めることができます。たとえば、米国というエリアには、カリフォルニアというサブエリアが含まれ、カリフォルニアというサブエリアにはサンノゼというサブエリアが含まれることができます。
- [ビルディング（Buildings）] には物理アドレスがあり、フロアとフロア プランが含まれています。ビルディングを作成する場合、物理アドレスおよび緯度と経度の座標を指定する必要があります。ビルディングにエリアを含めることはできません。ビルディングを作成することで、特定のエリアに設定を適用できます。
- [フロア（Floors）] は建物内にあり、キュービクル、壁に囲まれたオフィス、配線クローゼットなどで構成されています。フロアはビルディングにのみ追加できます。

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、「ネットワーク階層のサイトの作成 （125 ページ）」を参照してください。

- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、既存のサイト階層をアップロード （127 ページ）を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

- マップのイメージファイルを .jpg、.gif、.png、.pdf、.dxf、.dwg などの形式で保存できるグラフィカル アプリケーションを使用します。
- イメージ画像の寸法が、キャンパスマップに追加する予定のすべてのビルディングと屋外領域の合計寸法よりも大きいことを確認します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージを完全な定義でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。

ネットワーク階層のサイトの作成

Cisco DNA Center では、物理サイトを簡単に定義し、それらのサイトの共有リソースを特定することができます。[Design] エリアは、直観的な操作のために階層型になっており、デバイスをプロビジョニングするときに同じリソースを複数の場所で再定義する必要がありません。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。ネットワーク階層には、複数のサイト、ビルディング、およびエリアを追加できます。プロビジョニング機能を使用する前に、少なくとも 1 つのサイトを作成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**[Design]** > **[Network Hierarchy]**。

結果：世界地図が右側のペインに表示されます。

ステップ 2 マップツールバーから [+ Add Site] をクリックし、[Add Area] を選択します。

（注） 左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。

ステップ 3 [Area Name] フィールドにサイトの名前を入力します。

ステップ 4 [Parent] ドロップダウンリストから、親ノードを選択します。

（注） デフォルトでは、**[グローバル（Global）]** が親ノードです。

ステップ 5 [Add]をクリックします。

結果：左側ペインの親ノードにサイトが作成されます。

Cisco Prime Infrastructure からサイト階層をエクスポートしてCiscoDNACenterにインポート

ネットワーク階層はネットワークの地理的な場所を表します。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、Cisco DNA Center にインポートして、新しいネットワーク階層の作成に費やす時間と労力を削減できます。

これは、ロケーショングループまたはサイト情報を含む CSV ファイルと、ネットワーク階層内のさまざまなフロアマップを含むマップアーカイブファイルとして、Cisco Prime Infrastructure から 2 つのファイルをエクスポートするために必要な単純なプロセスです。

この手順では、Cisco Prime Infrastructure から Cisco DNA Center に既存のサイト階層をエクスポートする方法について説明します。Cisco Prime Infrastructure リリース 3.2 以降からサイト階層をエクスポートできます。

始める前に

- インベントリにシスコ ワイヤレス コントローラおよび AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。
- Cisco Prime Infrastructure にあるサイトを Cisco DNA Center で手動作成した場合は、Cisco DNA Center にインポートする前にそれらのサイトを手動で削除する必要があります。

ステップ 1 Cisco Prime Infrastructure からワークステーションに CSV ファイルとしてロケーショングループをエクスポートします。Cisco Prime Infrastructure で、**[Inventory]** > **[Group Management]** > **[Network Device Groups]** の順に選択します。

ステップ 2 [Device Groups] ウィンドウで、[Export Groups] をクリックします。

ステップ 3 [Export Groups] ダイアログボックスで、[APIC-EM] オプションボタンをクリックして CSV ファイルをダウンロードし、[OK] をクリックします。

（注） CSV ファイルがダウンロードされるまで待ちます。CSV ファイルには、さまざまなサイト、ビルディング、およびフロアの地理的場所と、ネットワーク内の階層に関する情報が含まれています。

ステップ 4 **[Maps]** > **[Wireless Maps]** > **[Site Maps (New)]** を選択することにより、Cisco Prime Infrastructure からマップをエクスポートします。

（注） これにより、フロア寸法などのマップ情報と Cisco Prime Infrastructure の各フロアに適用されている無線周波数（RF）減衰モデルなどのキャリブレーション情報がダウンロードされます。

ステップ 5 **[エクスポート（Export）]** ドロップダウン リストから **[マップ アーカイブ（Map Archive）]** を選択します。

結果：[Export Map Archive] ウィンドウが表示され、デフォルトで [Select Sites] ウィンドウが表示されます。

ステップ 6 エクスポートする特定のサイト、キャンパス、ビルディング、またはフロアのチェックボックスをオンにします。すべてのマップをエクスポートする場合は、[Select All] チェックボックスをオンにします。

ステップ 7 [Map Information] と [Calibration Information] が選択されているかどうかを確認します。必ずオプション 1 つを選択する必要があります。選択されていない場合は、[Map Information] および [Calibration Information] に対して [On] ボタンをクリックします。

- [Map Information] を選択すると、長さ、幅、高さなどのフロアの寸法がエクスポートされます。また、フロアマップ上に配置された AP に関する詳細、および Cisco Prime Infrastructure 内のフロアマップ上にオーバーレイされた障害物とエリアもエクスポートされます。
- [Calibration Information] を選択すると、Cisco Prime Infrastructure の各フロアに適用されている RF 減衰モデルがエクスポートされます。既存のキャリブレーションデータを Cisco Prime Infrastructure からエクスポートすることをお勧めします。それ以外の場合は、Cisco DNA Center でキャリブレーションの詳細を手動で入力する必要があります。

ステップ 8 [マップアーカイブを生成（Generate Map Archive）] をクリックします。

結果：ネットワーク階層内のさまざまなフロアマップを含む tar ファイルが作成され、お使いのワークステーションに保存されます。

ステップ 9 サイト階層を Cisco DNA Center にインポートするには、次の手順を実行します。

a) Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]** の順に選択します。

b) マップツールバーから [Import] をクリックし、[Import Sites] を選択します。

ステップ 10 [Import Sites] ウィンドウで、Cisco Prime Infrastructure のロケーショングループの CSV ファイルをドラッグアンドドロップします。

ステップ 11 [インポート（Import）] をクリックします。

ステップ 12 マップツールバーから [Import] をクリックして [Import Maps] を選択することにより、フロアマップおよび関連するマップ情報を含むマップアーカイブファイルをインポートします。

ステップ 13 [Import Maps] ウィンドウで、マップアーカイブファイルをドラッグアンドドロップします。

ステップ 14 **[インポート (Import)]** をクリックします。

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップ アーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。Cisco Prime Infrastructure からのマップのエクスポートについては、マップアーカイブのエクスポート（128 ページ）を参照してください。

（注） マップアーカイブファイルを Cisco DNA Center にインポートする前に、シスコ ワイヤレスコントローラや関連付けられている AP などのデバイスが検出され、Cisco DNA Center インベントリページに一覧になっていることを確認してください。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 ツールバーから [Import] をクリックし、[Import Sites] を選択します。

ステップ 3 CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、[Import] をクリックします。

（注） 既存の CSV ファイルがない場合は、**[テンプレートをダウンロード（Download Template）]** をクリックして、編集可能なCSVファイルをダウンロードして、その後、アップロードすることができます。

ステップ 4 Cisco Prime Infrastructure マップ tar.gz アーカイブファイルをインポートするには**[Import]** > **[Map Import]**を選択します。

ステップ 5 [Import Site Hierarchy Archive] ダイアログボックスのボックスエリアにマップアーカイブファイルをドラッグしてドロップします。

ステップ 6 **[保存]** を選択してファイルをアップロードします。

結果：[Import Preview] ウィンドウが表示され、インポートされたファイルが示されます。

マップ アーカイブのエクスポート

Cisco Prime Infrastructure からマップ アーカイブ ファイルをエクスポートし、それらを Cisco DNA Center にインポートできます。

ステップ 1 Cisco Prime Infrastructure のユーザーインターフェイスから、**[マップ（Map）]**>**[ワイヤレス マップ（Wireless Maps）]** > **[サイト マップ（新規）（Site Maps (New)）]**を選択します。

ステップ 2 **[エクスポート（Export）]** ドロップダウン リストから **[マップ アーカイブ（Map Archive）]** を選択します。

ステップ 3 [サイトの選択（Select Sites）] ウィンドウで、次のように設定します。マップ アーカイブに含めるマップ情報またはキャリブレーション情報を選択できます。

- マップ情報（Map Information）：アーカイブにマップ情報を含めるには、**オンまたはオフ** ボタンをクリックします。
- キャリブレーション情報（Calibration Information）：キャリブレーション情報をエクスポートするには、**オンまたはオフ** ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] オプション ボタンか、または [すべてのキャリブレーション情報（All Calibration Information）] オプション ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] を選択すると、選択したサイト マップのキャリブ

レーション情報がエクスポートされます。[すべてのキャリブレーション情報（All Calibration Information）] を選択すると、選択したマップとともに、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。

- 左側のペインの [サイト（Sites）] で、エクスポートするサイト、キャンパス、ビルディング フロア、または屋外領域の 1 つ以上のチェックボックスをオンにします。すべてのマップをエクスポートするには、[Select All] チェックボックスをオンにします。

ステップ 4 [マップアーカイブを生成（Generate Map Archive）] をクリックします。「データをエクスポートしています（`Exporting data is in progress`）」というメッセージが表示されます。
tar ファイルが作成され、ローカル マシンに保存されます。

ステップ 5 [Done] をクリックします。

グローバルマップアーカイブのエクスポート

ネットワーク全体のグローバルな階層マップをエクスポートできます。階層マップからアーカイブファイルにダウンロードするサイト、ビルディング、フロアの階層を選択することもできます。マップアーカイブファイルには、日時、フロアの数、APなどのデータが格納されます。

始める前に

次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**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[Design] > [Network Hierarchy] の順に選択します。

ステップ 2 ネットワーク全体のマップをエクスポートするには、**[Export]** > **[Export Maps]** の順に選択します。あるいは、左側のペインで目的のサイト、ビルディング、またはフロアの横にある歯車アイコンをクリックし、[Export Maps] を選択します。

- サイトを選択して [Export Maps] をクリックすると、すべてのサブサイト、ビルディング、およびフロアを含むサイトマップがエクスポートされます。
- ビルディングを選択して [Export Maps] をクリックすると、すべてのフロアを含むビルディングマップがエクスポートされます。
- フロアを選択して [Export Maps] をクリックすると、選択したフロアのフロアマップのみがエクスポートされます。

ステップ 3 [Export Maps Archive] ウィンドウで、次のいずれかを実行します。

- [File Name] フィールドにファイル名を入力し、[Export] をクリックして、[OK] をクリックします。

  選択したマップのアーカイブファイルを含む新しい tar ファイルが作成されてコンピュータに保存されます。

- [File Name] フィールドに既存のファイル名を入力し、[Click to select] リンクをクリックしてコンピュータから既存のファイルを選択します。[OK] をクリックします。

マップが選択したファイルにアーカイブされてコンピュータに保存されます。

ネットワーク階層の検索

ネットワーク階層を検索し、サイト、ビルディング、またはエリアをすばやく見つけることができます。これは、多くのサイトやエリア、ビルディングを追加した後に特に役立ちます。

ツリー階層を検索するには、左ペインの **[階層の検索（Find Hierarchy）]** で、検索するサイト、ビルディング、フロア名の名称の一部または正式名称をのどちらかを入力します。

結果：ツリー階層が、検索フィールドに入力したテキストに基づいてフィルタ処理されます。

サイトの編集

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**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のツリー ペインで、編集するサイトに移動します。
ステップ 3 サイトの横にある歯車アイコン ⚙ をクリックし、[サイトの編集（Edit Site）] を選択します。
ステップ 4 必要な変更を行って、[更新（Update）] をクリックします。

サイトの削除

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**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Delete Area] を選択します。
ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

建物の追加

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**[Design]** > **[Network Hierarchy]**。
ステップ 2 [Network Hierarchy] ウィンドウで、**[+Add Site]** > **[Add Building]** をクリックします。

（注） または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Building] を選択することもできます。

ステップ 3 [Add Building] ポップアップで建物の詳細を追加します。

a) [Building Name] フィールドに建物の名前を入力します。

（注） 建物名には、（”、&、?、'、/、<、>）を除く、すべての特殊文字を' / < >.

b) [Parent] ドロップダウンリストから、親ノードを選択します。

（注） デフォルトでは、**[グローバル（Global）]** が親ノードです。

c) [Address] フィールドにアドレスを入力します。

（注） また、マップをクリックしてアドレスを入力することもできます。アドレスを追加すると、[Longitude] および [Latitude] の座標フィールドが自動的に設定されます。経度と緯度の座標を手動で変更して、アドレスを変更できます。

ステップ 4 [Add] をクリックします。

結果：左側ペインの親サイトに建物が作成され、表示されます。

ビルディングの編集

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のツリー ペインで、編集するビルディングに移動します。

ステップ 3 ビルディングの横にある歯車アイコン ⚙ をクリックし、[ビルディングの編集（Edit Building）] を選択します。

ステップ 4 [ビルディングの編集（Edit Building）] ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

ビルディングの削除

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Delete Building] を選択します。

ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

（注） ビルディングを削除すると、そのコンテナマップもすべて削除されます。AP は、削除されたマップから未割り当ての状態に移動します。

ビルディングへのフロアの追加

ビルディングを追加したら、フロアを作成し、フロア マップをアップロードします。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 [グローバル（Global）] サイトと以前に作成した領域を展開し、以前に作成したすべてのビルディングを確認します。

ステップ 3 フロアを追加するビルディングの横にある歯車アイコン⚙をクリックし、次に [フロアを追加（Add Floor）] をクリックします。

ステップ 4 フロアの名前を入力します。フロア名には 21 文字の制限があります。フロア名は文字またはハイフン（-）で始める必要があり、最初の文字に続く文字列は、次の 1 つ以上を含めることができます。

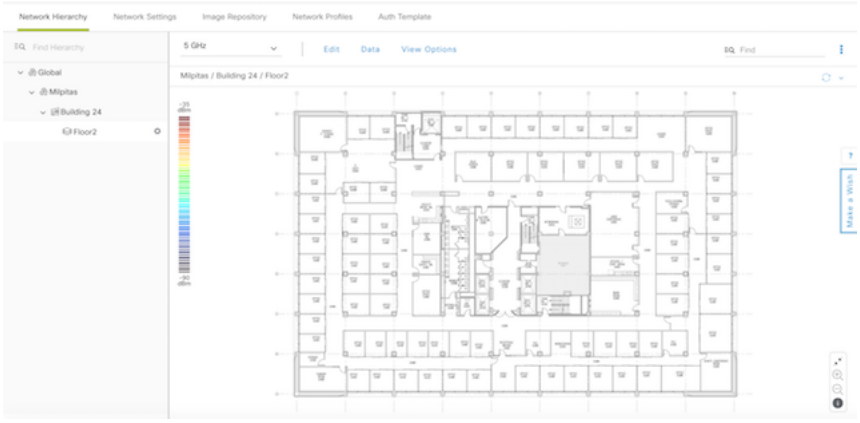
- 大文字または小文字、またはその両方
- 数字
- アンダースコア（_）
- ハイフン（-）
- ピリオド(.)
- スペース ( )

ステップ 5 [タイプ（RFモデル）（Type（RF Model））] ドロップダウン リストから無線周波数（RF）モデルを選択して、フロアのタイプを定義します（[屋内天井高（Indoor High Ceiling）]、[屋外オープンスペース（Outdoor Open Space）]、[乾式壁オフィスのみ（Drywall Office Only）]、および [キューブと壁で囲まれたオフィス（Cubes And Walled Offices）]）。これにより、フロアがオープンスペースであるか、乾式壁のオフィスであるかなどを定義します。選択した RF モデルに基づいて、ワイヤレス信号強度、ヒートマップの分布が計算されます。

ステップ 6 フロア プランをマップにドラッグしたり、ファイルをアップロードしたりできます。Cisco DNA Center は、.jpg、.gif、.png、dxf、および .dwg の各ファイル タイプをサポートしています。

マップをインポートした後は、必ず [オーバーレイの可視性（Overlay Visibility）] を [ON] にしてください（[フロア（Floor）]>[表示オプション（View Option）]>[オーバーレイ（Overlays）]）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

図 *3 :* フロア プランの例



ステップ 7 [Add] をクリックします。

フロアの編集

フロアを追加したら、フロア上にある障害物、エリア、および AP が含まれるようにフロアマップを編集できます。

ステップ 1 [Menu] アイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**の順に選択します。
ステップ 2 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせて、[Edit Floor] を選択します。
ステップ 3 [Edit Floor] ポップアップで、必要な変更を行います。
ステップ 4 [Update] をクリックして変更を保存します。

フロア マップのモニターリング

[Floor View] ナビゲーションウィンドウでは、次のような複数のマップ機能にアクセスできます。

- フロア マップ ウィンドウの右上隅にある [Find] 機能を使用して、AP、センサー、クライアントなど特定のフロア要素を検索します。検索基準に一致する要素は、右側のペインでテーブルとともにフロアマップに表示されます。マウスをテーブルの上に置くと、フロアマップ上の検索要素が接続線で示されます。
- フロア マップ ウィンドウの右上隅にある ⋮ アイコンをクリックして、次の作業を行います。
  - フロア プランを PDF としてエクスポートします。
  - フロア マップで距離を測定します。

- スケールを設定してフロア面積を変更します。

- フロア マップ ウィンドウの右下隅にある アイコンをクリックして、場所をズームインします。ズームレベルは画像の解像度によって異なります。高解像度画像では、より高いズーム レベルを使用できます。各ズーム レベルはさまざまなスケールで表示される各種スタイルマップで構成されていて、対応する詳細が表示されます。マップの中にはスケールを小さくしても大きくしても同じ状態のマップもあります。
- アイコンをクリックすると、広範囲のマップが表示されます。
- アイコンをクリックすると、マップ アイコンの凡例が表示されます。

フロア要素とオーバーレイの編集

フロア領域で使用できる **[編集（Edit）]** オプションにより、次の操作を実行できます。

- 次のフロア要素を追加、配置、および削除します。
  - アクセス ポイント（Access Points）
  - Sensor
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。
  - カバレッジ エリア
  - 障害物
  - ロケーション リージョン
  - Rails
  - マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿って AP を設置します。このようなカバレッジ領域の中心に設置された AP からは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイス ロケーションのスナップショットが他と異なるように、それらを交互にずらします。

- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。

AP の追加、配置、および削除

Cisco DNA Center Cisco DNA Center によって、カバレッジエリアの無線周波数（RF）信号の相対強度を表示する全体マップのヒートマップが計算されます。このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値に過ぎません。

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。「ディスカバリについて （19 ページ）」を参照してください。

Cisco DNA Center Cisco DNA Center では、次の 802.11ax AP がサポートされています。

- Cisco Catalyst 9120 アクセス ポイント
- Cisco Catalyst 9117 アクセス ポイント
- Cisco Catalyst 9115 アクセス ポイント
- Cisco Catalyst 9100 アクセスポイント

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [Add Aps] ウィンドウで、アクセスポイントのチェックボックスをオンにして AP を一括で選択し、[Add Selected] をクリックします。または、アクセスポイントの横にある [Add] をクリックします。

（注） 使用可能な検索オプションを使用して、アクセスポイントを検索できます。[フィルタ（Filter）] フィールドを使用し、AP 名、MAC アドレス、モデル、シスコ ワイヤレス コントローラのいずれかを使ってアクセス ポイントを検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）] をクリックして、フロア領域に 1 つ以上の AP を追加します。

ステップ 6 フロア領域に AP を割り当てたら、[APの追加（Add APs）] ウィンドウを閉じます。

ステップ 7 新しく追加した AP はフロア マップの右上隅に表示されます。

ステップ 8 [アクセスポイント（Access Points）] の横にある[フロア要素（Floor Elements）] ペインで、 [位置（Position）] をクリックして AP をマップに正しく配置します。

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細（Selected AP Details）] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセスポイントをドラッグすると、その水平（x）と垂直（y）の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセスポイントの詳細が表示されます。[選択したAPの詳細（Selected AP Details）] ウィンドウには、次の情報が表示されます。
  - [Position by 3 points]：フロアマップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
    1. [3ポイントによる位置付け（Position by 3 points）] をクリックします。
    2. ポイントを定義するには、フロア マップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[距離の設定（Set Distance）] をクリックします。
    3. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。
  - [Position by 2 Walls]：フロアマップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。
    1. [2つの壁による位置付け（Position by 2 Walls）] をクリックします。
    2. 最初の壁を定義するには、フロア マップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[Set Distance] をクリックします。
    3. 2 番目の壁を同様の方法で定義し、[保存（Save）] をクリックします。

       AP が、壁の間の定義された距離に従って自動的に配置されます。
  - [AP Name]：AP 名が表示されます。
  - [AP Model]：選択したアクセスポイントの AP モデルを示します。
  - [MAC Address]：MAC アドレスが表示されます。
  - [x]：マップの水平スパンをフィート単位で示します。
  - [y]：マップの垂直スパンをフィート単位で示します。
  - [AP Height）]：アクセスポイントの高さを示します。
  - [Protocol]：このアクセス ポイントのプロトコル：[802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
  - [Antenna]：このアクセスポイントのアンテナタイプ。

（注） 外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP がマップに表示されません。

- [Antenna Image]：AP イメージが表示されます。
- [Antenna Orientation]：[Azimuth] と [Elevation] の方向の度数を示します。
- [Azimuth]：全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

  方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Cisco DNA Center では、北は 0 または 360 度で、東は 90 度です。

ステップ 9 アクセス ポイントの設定と調整が完了したら、[保存（Save）] をクリックします。

AP の新しい位置に基づいてヒートマップが生成されます。

Cisco Connected Mobile experience（CMX）が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。『Cisco CMX 設定の作成 （173 ページ）』を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[Delete APs] ウィンドウが表示され、割り当てられて設定されたすべてのアクセスポイントが一覧表示されます。

ステップ 11 削除するアクセス ポイントの横にあるチェック ボックスをオンにし、[選択済みの削除（Delete Selected）] をクリックします。

- すべてのアクセスポイントを削除するには、[Select All] をクリックし、[Delete Selected] をクリックします。
- フロアからアクセス ポイントを削除するには、[削除（Delete）] アイコンをクリックします。
- [Quick Filter] を使用し、AP 名、MAC アドレス、モデル、コントローラのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果が表に表示されます。[削除（Delete）] アイコンをクリックしてフロア領域から AP を削除します。

Cisco Prime Infrastructure から一括 AP をエクスポートして Cisco DNA Center にインポートする

Cisco DNA Center では、アクセスポイントのコレクションをフロアマップにインポート、割り当て、および配置できます。Cisco Prime Infrastructure にアクセスポイントの既存のコレクションがある場合は、それを Cisco DNA Center にインポートすると、フロアマップへのアクセスポイントのインポート、割り当て、および配置に費やす時間と労力を節約できます。

この手順では、Cisco Prime Infrastructure からアクセスポイントの既存のコレクションをエクスポートして Cisco DNA Center にインポートする方法について説明します。

始める前に

- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。
- インベントリに AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。
- サイト、ビルディング、およびフロアは、サイト階層に存在する必要があります。

ステップ 1 一括 AP 位置を CSV ファイルとして Cisco Prime Infrastructure からワークステーションにエクスポートします。

ステップ 2 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します **[Design]** > **[Network Hierarchy]**。

ステップ 3 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Import Bulk AP] を選択します。

ステップ 4 [Import Bulk AP] ポップアップウィンドウで、AP ファイルをドラッグアンドドロップするか、[Choose a file] をクリックしてワークステーションからファイルを選択します。

（注）
- Prime テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Prime Template] をクリックして、Prime テンプレートをワークステーションにエクスポートします。Prime テンプレートは、ネストされたファイルをサポートしていません。
- Cisco DNA テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Template] をクリックして、Cisco DNA テンプレートをワークステーションにエクスポートします。Cisco DNA テンプレートは、ネストされたファイルをサポートしています。

CSV ファイルがダウンロードされるまで待ちます。CSV ファイルには、ネットワーク内のさまざまなサイトの AP 位置に関する情報が含まれています。

ステップ 5 [Import] をクリックします。

結果：[Import Summary] ウィンドウが表示されます。

- [Information] タブに、正常にインポートされた AP のリストが表示されます。
- [Warning] タブをクリックすると、警告のリストが表示されます。
- [Error] タブをクリックすると、エラーのリストが表示されます。

AP のクイック ビュー

フロアマップ上の AP アイコンにカーソルを合わせると、AP の詳細、Rx ネイバーの情報、クライアントの情報、およびデバイス 360 の情報が表示されます。

- [Info] をクリックすると、次の AP の詳細が表示されます。

- [Associated]：AP が関連付けられているかどうかを示します。
- [Name]：AP 名。
- [MAC Address]：AP の MAC アドレス。
- [Model]：AP モデル番号。
- [Admin/Mode]：AP モードの管理ステータス。
- [Type]：無線タイプ。
- [OP/Admin]：動作ステータスおよび AP モード。
- [Channel]：AP のチャネル番号。
- [Antenna]：アンテナ名。
- [Azimuth]：アンテナの方向。

- [Rx Neighbors] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネイバーが接続回線とともに表示されます。また、フロア マップには AP が関連付けられているかどうかも AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコ ワイヤレス コントローラ）の 360 度ビューが表示されます。

（注） デバイス 360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。

センサーの追加、配置、および削除

（注） インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco Aironet 1800s アクティブセンサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。

センサーデバイスは AP 1800s センサー専用です。Cisco Aironet 1800s アクティブセンサーは、PnP を使用してブートストラップされます。アシュアランス サーバーに到達可能かどうかの詳細情報を取得してから アシュアランス サーバーと直接通信します。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 フロア プランの上にある [編集（Edit）] をクリックします。

ステップ 4 [センサー（Sensors）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [Add Sensors] ウィンドウで、追加するセンサーのチェックボックスをオンにするか、またはセンサー行の横にある [Add] をクリックしてセンサーを追加します。

（注） 検索オプションを使用して、特定のセンサーを検索できます。[Filter] フィールドを使用し、センサーの名前、MACアドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）]をクリックして、フロア領域に 1 つ以上のセンサーを追加します。

ステップ 6 フロア マップへセンサーを割り当てたら、[センサーの追加（Add Sensors）] ウィンドウを閉じます。新しく追加したセンサーはフロア マップの右上隅に表示されます。

ステップ 7 センサーを正しく設定するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[位置（Position）] をクリックして、マップに正しくセットします。

ステップ 8 センサーの設定と調整が完了したら、[保存（Save）] をクリックします。

ステップ 9 センサーを削除するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[削除（Delete）] をクリックします。
[Delete Sensors] ウィンドウには、割り当てられて設定されたすべてのセンサーが一覧表示されます。

ステップ 10 削除するセンサーのチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのセンサーを削除するには、[すべて選択（Select All）]をクリックし、[選択済みの削除（Delete Selected）] をクリックします。
- フロアからセンサーを削除するには、そのセンサーの横にある [削除（Delete）]アイコンをクリックします。
- [Quick Filter] を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[削除（Delete）] アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。

カバレッジ エリアの追加

既定では、フロア領域やビルディング マップの一部として定義されている外部エリアが無線カバレッジ エリアと見なされます。

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、マップ エディタを使用してカバレッジ領域または多角形の領域を描画できます。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインでビルディングのフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Coverage Areas] トグルをクリックします。

ステップ 5 マップの左側のペインから、[Coverage Area] アイコンをクリックします。

ステップ 6 [Coverage Area] ポップアップウィンドウで、フィールドにカバレッジエリアの名前を入力し、[Add Coverage] をクリックします。

ステップ 7 描画ツールを使用して、カバレッジエリアの形状を作成します。

a) マップをクリックしてポイントを作成し、引き続きポイントを作成してカバレッジエリアの形状を定義します。

（注） カバレッジエリアの形状には、少なくとも 3 つのポイントが必要です。

b) 任意のポイントをクリックしてドラッグすると、カバレッジエリアの形状を定義し直すことができます。

c) ダブルクリックして描画ツールを終了し、カバレッジエリアの形状を確定します。

ステップ 8 カバレッジエリアの作成が完了したら、マップツールバーの [Save] をクリックします。

ステップ 9 カバレッジエリアを編集するには、次の手順を実行します。

a) マップツールバーから、[Add/Edit] をクリックします。

b) マップツールバーから、[Coverage Areas] トグルをクリックします。

c) カバレッジエリアのポイントをクリックしてドラッグすると、形状を定義し直すことができます。

d) カバレッジエリアの名前を編集するには、カバレッジエリアを右クリックして [Edit] を選択します。

e) 編集が完了したら、マップツールバーの [Save] をクリックします。

ステップ 10 カバレッジエリアを削除するには、次の手順を実行します。

a) マップツールバーから、[Add/Edit] をクリックします。

b) マップツールバーから、[Coverage Areas] トグルをクリックします。

c) カバレッジエリアを右クリックし、[Delete] を選択します。

d) 削除が完了したら、マップツールバーの [Save] をクリックします。

障害物の作成

アクセス ポイントの RF 予測ヒートマップを計算する際に考慮するための障害を作成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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 [Obstacles] の横にある [Overlays] パネルで、[Add] をクリックします。

ステップ 5 [Obstacle Creation] ダイアログ ボックスで、[Obstacle Type] ドロップダウン リストから障害のタイプを選択します。作成可能な障害のタイプは、[Thick Wall]、[Light Wall]、[Heavy Door]、[Light Door]、[Cubicle]、および [Glass] です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。

ステップ 6 [Add Obstacle] をクリックします。

ステップ 7 障害物を作成する領域に描画ツールを移動します。

ステップ 8 描画ツールをクリックして、描線を開始および停止します。

ステップ 9 エリアの輪郭を描画したら、そのエリアをダブルクリックして強調表示します。

ステップ 10 表示される [障害の作成（Obstacle Creation）] ウィンドウで [完了（Done）] をクリックします。

ステップ 11 [Save] をクリックして、障害をフロア マップに保存します。

ステップ 12 障害を編集するには、[Obstacles] の隣にある [Overlays] パネルで、[Edit] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 13 変更が完了したら、[Save] をクリックします。

ステップ 14 障害を削除するには、[Obstacles] の隣にある [Overlays] パネルで、[Delete] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 15 障害にマウス カーソルを合わせ、クリックして削除します。

ステップ 16 [Save] をクリックします。

ロケーション リージョンの作成

包含領域および除外領域を作成して、フロア上のロケーション計算の精度をさらに高めることができます。計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

フロア マップ上に包含領域と除外領域を配置するためのガイドライン

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。
- フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロア領域が作成されるときに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。
- フロア領域に複数の除外領域を定義することができます。

フロア上の包含リージョンの定義

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 [Overlays] パネルで、[Location Regions] の横にある [Add] をクリックします。

ステップ 4 **[ロケーション リージョンの作成（Location Region Creation）]** ダイアログ ウィンドウで、**[包含タイプ（Inclusion Type）]** ドロップダウン リストからオプションを選択します。

ステップ 5 **[位置領域の追加（Add Location Region）]** をクリックします。

包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 6 包含領域の定義を開始するには、描画ツールをマップ上の開始ポイントに移動して、1回クリックします。

ステップ 7 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。

再びクリックすると、次の境界線を定義できます。

ステップ 8 領域の輪郭が描画されるまでステップ 7 を繰り返したら、描画アイコンをダブルクリックします。

水色の実線によって包含領域が定義されます。

ステップ 9 [Save] をクリックします。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。原則として、除外領域は包含領域の境界内に定義されます。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで建物のフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Location Regions] トグルをクリックします。

ステップ 5 マップの左側のペインから、[Exclusion] アイコンをクリックします。

ステップ 6 描画ツールを使用して除外領域を作成します。

- マップをクリックしてポイントを作成し、除外領域の形状ができるまでポイントの作成を続けます。
- 形状を完成させるには、左側のペインで [Exclusion] アイコンをクリックして、描画モードを終了します。または、マップをダブルクリックして形状を確定することもできます。形状をキャンセルする場合は、マップ上で右クリックします。
- 既存の除外領域を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の除外領域を削除するには、形状を右クリックして [Delete] を選択します。

ステップ 7 除外領域の作成が完了したら、マップツールバーの [Save] をクリックします。

ロケーション リージョンの編集

ステップ 1 **[Overlays]** パネルで、**[Location Regions]** の横にある **[Edit]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 必要な変更を行って、**[Save]** をクリックします。

ロケーション リージョンの削除

ステップ 1 **[Overlays]**パネルで、**[Location Regions]** の横にある **[Delete]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 削除する領域の上にマウスのカーソルを合わせ、**[Delete]** をクリックします。

ステップ 3 [Save] をクリックします。

レールの作成

フロア上にコンベヤベルトを表すレールラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算をさらにサポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクライアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

スナップ幅領域は、フィートまたはメートル（ユーザー定義）単位で定義され、レールの片側（東および西、または北および南）からモニターされる距離を表します。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 [Rails] の横にある [Overlays] パネルで、[Add] をクリックします。

ステップ 5 レールのスナップ幅（フィートまたはメートル）を入力し、[Add Rail] をクリックします。

描画アイコンが表示されます。

ステップ 6 レール ラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。

ステップ 7 フロア マップ上にレール ラインを描画したら、描画アイコンを 2 回クリックします。レールラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

ステップ 8 [Save] をクリックします。

ステップ 9 [Overlays] パネルで、[Rails] の横にある [Edit] をクリックします。

使用可能なレールがマップ上で強調表示されます。

ステップ 10 変更を加えて、[Save] をクリックします。

ステップ 11 [Overlays] パネルで、[Rails] の横にある [Delete] をクリックします。

使用可能なすべてのレール ラインがマップ上で強調表示されます。

ステップ 12 削除するレールラインの上にマウスのカーソルを合わせ、[delete] をクリックします。

ステップ 13 [Save] をクリックします。

マーカーの配置

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[追加（Add）]** をクリックします。

描画アイコンが表示されます。

ステップ 5 マーカーの名前を入力し、[マーカーの追加（Add Marker）] をクリックします。

ステップ 6 描画アイコンをクリックし、マーカーをマップ上に配置します。

ステップ 7 **[Save]** をクリックします。

ステップ 8 [オーバーレイ（Overlays）] パネルで、[マーカー（Markers）] の横にある [編集（Edit）] をクリックします。

使用可能なマーカーがマップ上で強調表示されます。

ステップ 9 変更を加えて、[保存（Save）] をクリックします。

ステップ 10 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[削除（Delete）]** をクリックします。

使用可能なすべてのマーカーがマップ上で強調表示されます。

ステップ 11 削除するマーカーの上にマウスのカーソルを合わせ、[Delete] をクリックします。

ステップ 12 [Save] をクリックします。

フロア ビュー オプション

中央のペインのフロア プランの上にある **[View Options]** をクリックします。フロア マップと [Access Points]、[Sensor]、[Overlay Objects]、[Map Properties]、および [Global Map Properties]の各パネルが右側のペインに表示されます。

フロアマップの外観を変更するには、さまざまなパラメータを選択または選択解除します。たとえば、フロアマップ上のアクセス ポイント情報だけを表示する場合は、[Access Point] チェックボックスをオンにします。各パネルを展開して、各フロア要素で使用可能なさまざまな設定を構成できます。

アクセス ポイントの表示オプション

[Access Points] の横にある [On/Off] ボタンをクリックして、アクセスポイントをマップ上に表示します。[アクセスポイント（Access Points）] パネルを展開して、次の設定を行います。

- [表示ラベル（Display Label）]：ドロップダウン リストから、AP に関してフロア マップに表示するテキスト ラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - [なし（None）]：選択したアクセス ポイントに関してラベルが表示されません。
  - [名前（Name）]：AP 名。
  - [AP MAC アドレス（AP MAC Address）]：AP の MAC アドレス。
  - [コントローラIP（Controller IP）]：アクセス ポイントが接続されているシスコ ワイヤレス コントローラの IP アドレス。
  - [無線 MAC アドレス（Radio MAC Address）]：無線 MAC アドレス。
  - **IP Address**
  - [チャネル（Channel）]：Cisco Radio のチャネル番号または [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
  - [カバレッジホール（Coverage Holes）]：クライアントが接続を失うまで信号が弱まったクライアントのパーセンテージ。接続されていないアクセス ポイントについては [使用不可（Unavailable）]、monitor-only モードのアクセス ポイントについては [MonitorOnly] と表示されます。
  - [送信電力（TX Power）]：現在の Cisco Radio の送信電力レベル（1 が高い）または [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。無線帯域を変更すると、マップ上の情報もそれに応じて変更されます。

    電力レベルはアクセス ポイントのタイプによって異なります。1000 シリーズの AP では 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。
  - [チャネルおよび送信電力（Channel and Tx Power）]：チャネルと送信電力レベルまたは [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
  - [使用率（Utilization）]：関連付けられたクライアント デバイスで使用されている帯域幅のパーセンテージ（受信、送信、およびチャネル使用率を含む）。アソシエーションを解除されたアクセス ポイントでは **[Unavailable]**、monitor-only モードのアクセス ポイントでは **[MonitorOnly]** が表示されます。
  - [送信使用率（Tx Utilization）]：指定されたインターフェイスの送信（Tx）使用率。
  - [受信使用率（Rx Utilization）]：指定されたインターフェイスの受信（Rx）使用率。
  - [チャネル使用率（Ch Utilization）]：指定されたアクセス ポイントのチャネル使用率。
  - **関連付けられたClients**）]：関連付けられたクライアントの総数。

- [デュアルバンド無線（Dual-Band Radios）]：Cisco Aironet 2800 および 3800 シリーズ アクセス ポイント上の XOR デュアルバンド無線を識別してマークします。
- [ヘルス スコア（Health Score）]：AP のヘルス スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**

- [ヒートマップ タイプ（Heatmap Type）]：ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI予測モデル、アンテナの方向、およびAP送信電力に基づいて計算されます。[ヒートマップ タイプ（Heatmap Type）] ドロップダウンリストから、ヒートマップのタイプ（[なし（None）] または [カバレッジ（Coverage）]）を選択してください。
  - **None**
  - [カバレッジ（Coverage）]：フロア プランにモニター モード アクセス ポイントがある場合は、カバレッジヒートマップを選択できます。カバレッジヒートマップでは、モニター モード アクセス ポイントは除外されます。
- [ヒートマップの不透明度（%）（Heatmap Opacity (%)）]：スライダを 0 ～ 100 の範囲でドラッグして、ヒートマップの不透明度を設定します。
- [RSSIカットオフ（dBm）（RSSI Cut off (dBm)）]：スライダをドラッグして RSSI カットオフ レベルを設定します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [マップの不透明度（%）（Map Opacity (%)）]：スライダをドラッグしてマップの不透明度を設定します。

AP の詳細はすぐにマップに反映されます。マップ上の APアイコンにカーソルを合わせると、AP の詳細、RX ネイバーの詳細、クライアントの詳細、およびスイッチの情報が表示されます。

センサーオプションの表示

[Sensors] ボタンをクリックすると、マップ上にセンサーが表示されます。[Sensors] パネルを展開して、次の設定を行います。

- [Display Label]：ドロップダウンリストから、選択したアクセスポイントに関してフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - [None]
  - [Name]：センサー名。
  - [Sensor MAC Address]：センサーの MAC アドレス。

オーバーレイ オブジェクトの表示オプション

オーバーレイオブジェクト をこれらの設定を構成するパネルに展開します。[On]/[Off] ボタンを使用して、これらのオーバーレイオブジェクトをマップ上に表示します。

- [Coverage Areas]
- [Location Regions]
- [Obstacles]
- [Rails]
- [Markers]

スイッチの表示オプション

スイッチの横にある [On]/[Off] ボタンをクリックすると、そのスイッチで使用できる AP のリストがマップ上に表示されます。

[Switch] パネルを展開して、表示ラベルの設定を行います。

- [Display Label]：ドロップダウンリストから、選択したスイッチのフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - なし
  - 名前
  - スイッチMACアドレス
  - AP 数
  - クライアント数
  - SSID の数

選択したスイッチの AP の詳細がマップにすぐに反映されます。マップでスイッチのアイコンにカーソルを合わせると、スイッチの詳細が表示されます。

スイッチ名をクリックすると、次の詳細が表示されます。

- スイッチ MAS アドレス
- AP 数
- クライアント数
- SSID の数
- ヒートマップ：対応するオプションボタンをクリックして、すべての AP、特定のスイッチに属する AP、または他のスイッチに属する AP のヒートマップを表示できます。
- 所有している AP：このスイッチに属する AP のリストが表示されます。

マップ プロパティの設定

[Map Properties] パネルを展開して、以下を構成します。

- [Auto Refresh]：間隔のドロップダウンリストを使用して、データベースからマップデータを更新する頻度を設定できます。[Auto Refresh] ドロップダウンリストから、時間間隔（[None]、[1 min]、[2 mins]、[5 mins]、または [15 mins]）を設定してください。

グローバルマッププロパティの設定

[Global Map Properties] パネルを展開し、次のように設定します。

- [Unit of Measure]：ドロップダウンリストを使用して、マップの寸法測定値を [Feet] または [Meters] のいずれかに設定します。

フロアマップでのワイヤレス干渉源の特定

Cisco DNA Center は、干渉を検出し、フロアマップ上の特定の帯域に対する干渉源を無効にします。2.4 GHz 帯域に干渉があると、802.11 ワイヤレスネットワークのネットワークトラフィックが中断します。

Cisco DNA Center は、干渉源の場所、影響範囲、および強度を特定します。

この手順では、フロアマップ上のネットワーク干渉源を特定する方法を示します。

始める前に

Cisco Connected Mobile Experiences（CMX）または Cisco DNA Spaces が Cisco DNA Center と同期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**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで建物のフロアをクリックします。

ステップ 3 フロアの横にある省略記号のアイコン ••• にカーソルを合わせ、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

（注） （オプション）世界地図で、フロアにカーソルを合わせ、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

ステップ 4 [Network Hierarchy] ウィンドウで、[View Options] をクリックします。

ステップ 5 [View Options] ウィンドウで下にスクロールし、[Interferers] トグルをクリックして、干渉源がフロアマップに表示されるようにします。

ステップ 6 [Interferers] カテゴリを展開し、[Show Zone of Impact] トグルをクリックして、干渉源の影響ゾーンがフロアマップに表示されるようにします。

（注） デフォルトでは、[Zone of Impact] は無効になっています。

ステップ 7 フロアマップで、干渉源のアイコンにカーソルを合わせ、影響を受けるチャネルをクリックして干渉源デバイスの詳細情報を確認します。

データのフィルタリング

アクセスポイントデータのフィルタ処理

右側のペインの [Filters] パネルの下にある [Access Point] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。
- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップ上に表示するアクセスポイントの識別子を選択します。
  - アクセス ポイントをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のアクセス ポイントを表示するには、表示されたテーブル内でアクセス ポイントのチェック ボックスをオンにし、[マップ上で選択を表示（Show Selected on Maps）] をクリックします。

テーブルの検索結果にカーソルを合わせると、AP の位置がマップ上に線でマークされます。

センサーデータのフィルタ処理

右側のペインの [Filters] パネルの下にある [Sensor] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。
- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップで表示するセンサーの識別子（名前および MAC アドレス）を選択します。
  - センサーをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のセンサーを表示するには、表示されたテーブ

ル内でセンサーのチェックボックスをオンにし、[Show Selected on Maps] をクリックします。

テーブルの検索結果にカーソルを合わせると、センサーの位置がマップ上に線でマークされます。

ゼロデイ Ekahau 計画ワークフロー

始める前に

Ekahau Pro ツールを使用すると、フロアレイアウト、AP の場所、障害物など、企業の完全なネットワーク計画を作成できます。フロアレイアウトを作成した後、シミュレートされたネットワーク計画と実際のサイト調査データを、Cisco DNA Center が使用可能な形式にエクスポートできます。Ekahau プロジェクトファイルを Cisco DNA Center にインポートして、さらに計画を立てることができます。

Ekahau Pro ツールバージョン 10.2 では、サイト階層を自動的に作成し、それをプロジェクトファイルとして保存して、Cisco DNA Center にインポートできます。

ステップ 1 Ekahau Pro ツールでフロアレイアウトを計画します。

- ビルディングとフロアを作成します。

  Ekahau Pro ツールでビルディングを作成することは必須ではありません。

- フロアプランをインポートします。
- 計画された AP または仮定の AP を追加します。
- ビルディングの座標を追加します。
- サイト名を定義します。

  ここで指定した AP 名は、ワイヤレスコントローラ の設定中に、シスコ ワイヤレス コントローラ の AP 名を更新するために使用されます。

- 障害物を追加します。
- プロジェクトを PDF としてエクスポートします。

ステップ 2 フロアレイアウトで設計された場所に計画された AP を展開します。

- 物理 AP は、フロアレイアウトで指定された設計済みの場所に取り付けられます。計画された AP の MAC アドレスが、物理 AP の MAC アドレスで更新されます。
- 物理 AP は、目的 ワイヤレスコントローラ の VLAN に接続されています。

ステップ 3 シスコ ワイヤレス コントローラを設定します。

- 検出されたシスコ ワイヤレス コントローラ と AP が [Inventory] ウィンドウにリストされるように、**検出**ジョブを実行して、ワイヤレスコントローラネットワーク内の とアクセスポイントを検出します。
- フロアプランニング中に Ekahau Pro プロジェクトで指定された AP 名を使用して、ワイヤレスコントローラ の AP 名を更新します。

ステップ 4 Ekahau プロジェクトを Cisco DNA Center にインポートします。

ステップ 5 計画された AP を Cisco DNA Center の実際 AP にマッピングします。

Cisco DNA Center への Ekahau プロジェクトのインポート

ステップ 1 [Menu] アイコン ☰ をクリックして、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

（注） 詳細については、ネットワーク階層のサイトの作成 （125ページ）、建物の追加 （130ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

フロアを追加する際には、必ず、Ekahau プロジェクトで指定されたものと同じ名前でフロアを作成してください。

ステップ 3 左側のペインで、Ekahau プロジェクトをインポートするサイトの横にある省略記号 ••• のアイコンにカーソルを合わせて、[Import Ekahau Project] を選択します。

結果：[Import Ekahau Project] ダイアログボックスが表示されます。

ステップ 4 [Import Ekahau Project] ダイアログボックスのボックスエリアに ESX ファイルをドラッグアンドドロップするか、または [click to select] リンクをクリックして ESX ファイルを参照します。

（注） インポートが成功すると、各計画された AP は、AP 名を使用してインベントリ内の既存の実際の AP にマッピングされます。計画された AP は、フロアマップ上にアイコン [P] とともに表示されます。たとえば、計画済みの AP の名前が SJC01-02-AP-B-1 の場合、インポートプロセスでは同じ名前の実際の AP が検索されます。

ステップ 5 インベントリで AP が見つからず、マッピングが解除されたままの場合、計画された AP はフロア上に保持されます。

不一致の理由を表示するには、フロアマップ上の計画された AP アイコンの上にカーソルを置いて、[Import History] をクリックします。

次の試行は、計画された AP を実際の AP にマッピングするために行われます。

- 新たに検出された AP が計画された AP と一致する場合、計画された AP は検出された実際の AP で置き換えられます。
- 計画された AP がマッピング解除されたままの場合は、計画された AP を実際の AP で手動で置き換えて、失敗の原因を示すことができます。

ステップ 6 実際の AP に計画された AP を手動で割り当てるには、フロアマップ上の計画された AP アイコンの上にカーソルを合わせて、[Assign] > [Assign] > をクリックします。

結果：[Assign Planned APs] パネルが表示されます。

ステップ 7 [Assign Planned APs] パネルで、AP 名、AP タイプ、またはすべての AP によって計画された AP を実際の AP にマッピングします。

ステップ 8 AP 名の横にあるオプションボタンを選択し、[Assign] をクリックして、計画済みの AP を手動で割り当てます。

ステップ 9 [Save] をクリックします。

インタラクティブ フロア プランニングについて

インタラクティブ プランニングは、計画された AP または仮想 AP や障害物をラスターイメージや CAD フロアプランで描画することによって、フロアレイアウトのプランを支援します。フロアマップを PDF としてエクスポートして、AP を設置している技術者と共有できます。フロアの描画は、技術者がフロアのレイアウトと正確な AP の設置場所を可視化するのに役に立ちます。

インタラクティブ フロア プランニングにより、次のことが可能になります。

- キャンバスとしてラスターまたは CAD フロアプランを使用してフロアレイアウトを作成する。
- 信号カバレッジ要件に基づいて、計画された AP または仮想 AP をフロアマップに配置する。これらの仮想 AP または計画された AP は、Cisco DNA Center によってまだインストールまたは検出されていません。
- アンテナのタイプと方向を割り当てる。
- 信号の減衰に影響を与える壁や棚などの障害物をフロアに描画する。
- すべての AP を順番に計画する。
- フロアマップを PDF としてエクスポートする。

インタラクティブ フロア プランニング

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

ステップ 3 左側のメニューで、フロアを選択します。

選択したフロアに計画された AP と障害物を描画できます。

ステップ 4 中央のペインのフロア プランの上にある **[編集（Edit）]** をクリックします。

ステップ 5 [Floor Elements] パネルで、[Planned Access Points] の横にある [Add] をクリックします。

[Add Planned AP] ウィンドウが表示されます。

ステップ 6 [AP Name] テキストボックスに、計画された AP の名前を入力します。

ステップ 7 （オプション）[MAC Address] テキストボックスに、計画された AP の MAC アドレスを入力します。

ステップ 8 [AP Model] ドロップダウンリストから、AP モデルを選択します。

ステップ 9 [x] および [y] テキストボックスには、マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。

ステップ 10 [Ap Height] テキストボックスに、AP の高さを入力します。

ステップ 11 [Radio band] タブをクリックして、アンテナタイプ、方位角、および垂直面の方向を設定します。

ステップ 12 [Antenna] ドロップダウンリストから、この AP の適切なアンテナタイプを選択します。

アンテナイメージは、選択されたアンテナを反映しています。

ステップ 13 アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

ステップ 14 **[Save]** をクリックします。

新しく追加された計画された AP がフロアマップに表示されます。

ステップ 15 水平方向と垂直方向のスパン（つまり、x 座標と y 座標）を指定していない場合、計画された AP はフロアマップの右上隅に表示されます。

ステップ 16 マップ上の適切な場所にドラッグアンドドロップして、計画された AP をマップに正しく配置します。

ステップ 17 **[Save]** をクリックします。

ステップ 18 計画可能な次の AP は、フロアマップの右上隅に表示されます。

ステップ 19 次の AP を計画するには、ステップ 6 ～ 14 を繰り返します。

ステップ 20 障害物を描画するには、[Overlays] パネルで [Obstacles] の横にある [Add] をクリックします。

詳細については、「障害物の作成 （141 ページ）」を参照してください。

ステップ 21 フロアプランを PDF としてエクスポートするには 、[Network Hierarchy] ウィンドウの右上隅にある アイコンをクリックし、[Export] を選択します。

ステップ 22 [Export] ウィンドウで PDF としてエクスポートするには、[PDF] チェックボックスをオンにします。

ステップ 23 [エクスポート（Export）] をクリックします。

ODF が作成され、ローカルマシンにダウンロードされます。PDF には、設定した計画された AP の詳細とともにフロアマップが含まれています。計画された AP は、AP モデルに基づいて一覧表示されます。

APモデルカタログを使用したフロアマップへの計画済みアクセスポイントの配置

AP モデルカタログ機能を使用すると、フロア上の 1 つの AP を AP モデル、アンテナタイプ、方位角、および垂直面の方向で設定し、同じモデルタイプに属する残りの AP にその構成を複製できます。

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**[Design]** > **[Network Hierarchy]**。

ステップ 2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

ステップ 3 左側のペインでビルディングのフロアをクリックします。

（注） 選択したフロアに計画された AP と障害物を描画できます。

ステップ 4 マップの左側のペインにある [AP Models] エリアで、追加する計画済み AP の AP モデルをクリックします。

（注） AP モデルがリストにない場合は、[Add Model] をクリックして、リストに追加する AP モデルを選択します。

ステップ 5 描画ツールを使用して、フロアマップ上の位置をクリックして計画済み AP を追加します。

結果：選択したモデルの計画済み AP がフロアマップに追加され、右側に [Edit Planned AP] スライドインペインが表示されます。このペインには、デフォルトで AP 名が追加されます。

ステップ 6 [Edit Planned AP] スライドインペインで、[AP Name] フィールドの横にある歯車のアイコンをクリックします。

結果：[Name pattern] ダイアログボックスが表示されます。

ステップ 7 最初の AP をフロアに追加するときは、SJC-BLD21-FL2-AP #### などの有効な名前パターンを入力してから、[Set name pattern] をクリックするようにしてください。

（注） 計画済み AP は Cisco DNA Center 内で一意である必要があるため、名前パターンでフロアを識別できるようにします。

名前パターンの #### は、[AP Name] の番号に置き換えられます（SJC-BLD21-FL2-AP0001 や SJC-BLD21-FL2-AP0002 など）。

ステップ 8 [Edit Planned AP] スライドインペインの [Antenna] ドロップダウンリストから、AP の各無線スロットに適切なアンテナタイプを選択します。

（注） アンテナイメージは、選択されたアンテナを反映しています。

ステップ 9 アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

ステップ 10 作成した AP と同じ AP プロパティを持つ別の AP を追加するには、その新しい AP を配置するフロアマップ内の場所をクリックします。

結果：BLD1-AP0002-TX のように、新しい AP のアイコンがマップに表示されます。すべてのプロパティが継承され、AP 名が付加されています。

ステップ 11 同じプロパティを持ち、AP 名が付加された AP をさらに追加するには、フロアマップをクリックします。

ステップ 12 フロアマップへの AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。

ステップ 13 AP を配置するには、AP をフロアマップ内の適切な場所にドラッグアンドドロップします。

ステップ 14 計画済み AP を削除するには、AP のアイコンを右クリックし、[Delete] をクリックします。

ステップ 15 計画済み AP を編集するには、AP のアイコンを右クリックし、[Edit] をクリックします。

ステップ 16 計画済み AP の追加が完了したら、マップツールバーの [Save] をクリックします。

グローバル ワイヤレス設定の構成

グローバル ワイヤレス ネットワーク設定には、サービスセット識別子（SSID）、ワイヤレス インターフェイス、ワイヤレス無線周波数（RF）、およびセンサーの設定が含まれます。

（注） ワイヤレス センサー デバイス プロファイルの作成は、Cisco Aironet 1800s アクティブセンサーデバイスにのみ適用されます。

エンタープライズ ワイヤレス ネットワーク用 SSID の作成

次の手順では、エンタープライズ ワイヤレス ネットワークに SSID を設定する方法を説明しています。

（注） SSID は、グローバルレベルで作成されます。サイト、ビルディング、フロアは、グローバルレベルから設定が継承されます。

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**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] が選択されていることを確認します。

ステップ 4 [SSID] テーブルから、Add にカーソルを合わせて、[Enterprise] を選択します。

結果：**ワイヤレス SSID** ワークフローが表示されます。

ステップ 5 [Basic Settings] の手順を完了します。

a) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

b) [Wireless Option] で、ワイヤレス帯域設定を選択します。

- [Dual band operation (2.4 GHz and 5 GHz)]：WLAN は 2.4 GHz と 5 GHz に対して作成されます。デフォルトでは、帯域選択は無効になっています。
- [Dual band operation with band select]：WLAN が 2.4 GHz および 5 GHz 用に作成され、バンドセレクトが有効になります。
- [5 GHz only]：WLAN が 5 GHz 用に作成され、バンドセレクトが無効になります。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトが無効になります。

c) [Type of Enterprise Network] で、ワイヤレスネットワークでの Quality of Service（QoS）のプロビジョニング方法を選択します。

- [Voice and Data]：QoS が音声およびデータトラフィックに対して最適化されます。
- [Data Only]：QoS はワイヤレス データ トラフィックに対してのみ最適化されます。

d) [SSID STATE] で、次の設定をカスタマイズします。

- [Admin Status]：管理ステータスを有効または無効にするには、このトグルを使用します。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルを使用します。

ステップ 6 [Security Settings] の手順を完了します。

a) [Level of Security] で、このネットワークの暗号化および認証タイプを選択します。

（注） サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。

- [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA2] チェックボックスが有効になっています。

  （注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。

  WPA3 は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

- [Personal]：[Personal] を選択した場合は、[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバー間のペアワイズマスターキー（PMK）として使用されます。

（注） WPA3-Personal は、パスワードベースの堅牢な認証を提供することによって、個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

WPA2 パーソナルの場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、事前共有キーのオーバーライド （161 ページ）を参照してください。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアな SSID にリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、最小限のセキュリティを提供します。

  （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

  オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

b) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、「エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定」を参照してください。

c) 次のチェックボックスの 1 つ以上をオンにします。

- [Fast Lane]：このネットワークで fastlane 機能を有効にするには、このチェックボックスをオンにします。

  （注） fastlane を有効にすると、最適化されたレベルのワイヤレス接続と enhanced Quality of Service（QoS）を受信するように IOS デバイスを設定できます。

- [Identity PSK]（個人レイヤ 2 セキュリティ用）：SSID 内の個人またはユーザーグループのために作成できる一意の事前共有キーを有効にするには、このチェックボックスをオンにします。
- [MAC Filtering]：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

  （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。

d) [Next] をクリックします。

ステップ 7 [Advance Settings] の手順を完了します。

a) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

  （注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。

b) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] 設定を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

c) [11K] で、次の設定を指定します。

- [Neighbor List]：11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるようにするには、このチェックボックスをオンにします。

  （注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバーAPのリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。

  （注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。

  （注） ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続から除外します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

d) [11v BSS Transition Support] で、次の設定を指定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

  （注） BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントを関連付け解除しないタイムフレームです。

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウトを設定するには、このチェックボックスをオンにします。

  （注） クライアントが送信するデータがユーザーアイドルタイムアウト内で指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは別のタイムアウト期間中に更新します。

  デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

- [Directed Multicast Service]：Directed Multicast Service を有効にするには、このチェックボックスをオンにします。

  （注） デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するように AP に要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

e) [Radius Client Profiling] で、このトグルを使用して WLAN での RADIUS プロファイリングを有効または無効にします。

（注） この機能を有効にするには、1 つ以上の AAA/PSN サーバーが必要です。

f) [Next] をクリックします。

ステップ 8 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインで、プロファイルをクリックします。

b) プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。

- [Profile Name]：ワイヤレスプロファイルの名前を入力します。
- [Fabric]：SSID がファブリックか非ファブリックかを指定します。

  （注） ファブリック SSID は、ソフトウェア定義型アクセス（SD-Access）の一部であるワイヤレスネットワークです。ファブリック SSID を使用する場合は、SD アクセスが必須です。非ファブリックは、SD アクセスを必要としない従来のワイヤレスネットワークです。

非ファブリック SSID の場合は、次の設定を選択します。

- [Interface]：[Interface Management] ドロップダウンリストをクリックしてインターフェイスを選択するか、プラスアイコン をクリックして新しいワイヤレスインターフェイスを追加します。

  （注） これは、ワイヤレスインターフェイスに関連付けられている VLAN ID です。

- [VLAN Group]：[VLAN Group Name] ドロップダウンリストをクリックして VLAN グループを選択するか、プラスアイコン をクリックして VLAN グループを追加します。

- [Do you need Anchor for this SSID?]：SSID をアンカーにするかどうかを選択します。
- [Flex Connect Local Switching]：WLAN のローカルスイッチングを有効にするには、チェックボックスをオンにします。ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect AP がデータパケットをローカルにスイッチできます。

  （注） SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされている特定のフロア上のすべての AP が FlexConnect モードに切り替わります。

c) [Associate Profile] をクリックして、プロファイルを選択します。
d) [Next] をクリックします。

ステップ 9 [Summary] の手順を確認します。変更が必要な場合は、[Edit] をクリックします。

ステップ 10 SSID の設定を保存するには、[Save] をクリックします。

結果：SSID が作成されます。

事前共有キーのオーバーライド

SSID はグローバル階層に作成されます。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロア レベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルでPSKをオーバーライドすると、後続のフロアは新しい設定を継承します。

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**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 左側のメニューで、PSK を編集するサイト、ビルディング、またはフロアを選択します。

ステップ 3 [Enterprise Wireless] の下の [Passphrase] フィールドをクリックし、PSK SSID の新しいパスフレーズを入力します。

ステップ 4 **[保存（Save）]** をクリックします。

「Passphrase for the SSID(s) updated successfully」という成功メッセージが表示されます。

SSID の横にある検証アイコン にカーソルを合わせると、この設定の継承元が表示されます。

ステップ 5 PSK オーバーライドをリセットするには、サイト、ビルディング、またはフロアの PSK SSID のチェックボックスをオンにして、[削除(Delete)] をクリックします。PSK はグローバルパスフレーズ値にリセットされます。

ゲスト ワイヤレス ネットワークの SSID の作成

この手順では、ゲスト ワイヤレス ネットワークの SSID を作成する方法について説明します。

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**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 [Guest Wireless] の下で、[Add] をクリックして、新しい SSID を作成します。

[Create a Guest Wireless Network] ウィンドウが表示されます。

ステップ 3 [Wireless Network Name (SSID)] フィールドに、作成するゲスト SSID の一意の名前を入力します。

名前には、1 つのスペースを含めて、最大 32 文字の英数字を使用できます。< および / を除くすべての特殊文字を使用できます。

. および * のサブストリングの組み合わせは使用できません。

ステップ 4 [SSID STATE] で、次のように設定します。

- [Admin Status] ボタンをオフにして、管理ステータスを無効にします。
- 範囲内のすべてのワイヤレスクライアントに SSID を表示しない場合は、[Broadcast SSID] ボタンをオフにします。[Broadcast SSID] をオフにすると、この SSID に接続しようとしているクライアントで SSID が非表示になり、ワイヤレス インフラストラクチャの不要な負荷が軽減されます。

ステップ 5 [Level Of Security] の下で、レイヤ 2 およびレイヤ 3 セキュリティポリシーを設定します。

ステップ 6 [L2 Security] の下で、このネットワークの暗号化および認証タイプを設定します。

ステップ 7 [Enterprise]、[Personal]、[Open Secured]、[Open] のいずれかのオプションボタンをクリックして、対応するセキュリティ認証を設定します。

- [Enterprise]：**WPA2** と **WPA3** の両方のセキュリティ認証タイプを設定するには、それぞれのチェックボックスをオンにします。デフォルトでは、[WPA2] チェックボックスが有効になっています。

  Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。Fast transition は、エンタープライズ WPA2 SSID に適用できます。

  WPA3 セキュリティ認証は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

- [Personal]：**WPA2** と **WPA3** の両方を設定したり、**WPA2** と **WPA3** を個別に設定したりするには、それぞれのチェックボックスをオンにします。

  WPA3 パーソナルセキュリティ認証は、パスワードベースの堅牢な認証を提供することによって個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

  [Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、オープン SSID に関連付けるためのオープン SSID を選択します。関連付けにより、オープン SSID が保護されます。オープンでセキュアな SSID に関連付ける前に、オープン SSID が作成されている必要があります。

  （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

ステップ 8 [L3 Security] の下で、このゲストネットワークの暗号化および認証のタイプを [Web Policy] と [Open] から選択します。

ステップ 9 オープンなポリシーはセキュリティを提供しません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

ステップ 10 [Web Policy] を選択した場合、認証サーバーを [ISE Authentication]、[Web Authentication]、または [Web Passthrough] として設定する必要があります。

[Web Policy] の暗号化と認証タイプは、レイヤ 3 のセキュリティを強化します。

- 外部 Web 認証（EWA）では、セキュリティレベルとして [L3 Security] の下の [Web Policy] オプションボタンをクリックし、認証サーバーとして [Authentication] ドロップダウンリストから [Web Authentication External] をクリックします。
- 中央 Web 認証（CWA）では、セキュリティレベルとして [L3 Security] の下の [Web Policy] をクリックし、認証サーバーとして [Authentication] ドロップダウンリストから [ISE Authentication] をクリックします。

ステップ 11 [Authentication Server] で、SSID の認証サーバーを設定できます。

ステップ 12 [ISE Authentication] を選択した場合は、[WHAT KIND OF PORTAL ARE YOU CREATING TODAY ?] ドロップダウンリストから、作成するポータルのタイプを選択します。

- [SelfRegistered]：ゲストは自己登録ゲストポータルにリダイレクトされ、情報を提供して登録して、自動的にアカウントを作成します。
- [HotSpot]：ゲストはログイン情報なしでネットワークにアクセスできます。

[WHERE WILL YOUR GUESTS REDIRECT AFTER SUCCESSFUL AUTHENTICATION ?] ドロップダウンリストから、認証の成功後にゲストをリダイレクトする場所を選択します。

- [Success page]：ゲストは [Authentication Success] ウィンドウにリダイレクトされます。

- [Original URL]：ゲストは最初にリクエストした URL にリダイレクトされます。
- [Custom URL]：ゲストはここで特定されたカスタム URL にリダイレクトされます。[Redirect URL] フィールドにリダイレクト URL を入力します。

  SSID を作成したので、それをワイヤレス プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

ステップ 13 [Web Authentication] または [Web Passthrough] を選択した場合は、認証タイプとして [Internal] または [External] を設定します。

レイヤ 3 セキュリティ方式である Web 認証（Web Auth）を使用すると、クライアントは、何らかの認証方式に合格するまでの間、Dynamic Host Configuration Protocol（DHCP）およびドメインネームシステム（DNS）のトラフィックを通過させることができます。

Web パススルーは、ゲストアクセスに使用されるソリューションであり、認証ログイン情報は必要ありません。Web パススルーでは、ワイヤレスユーザーがインターネットを初めて使用するときに、使用ポリシーページにリダイレクトされます。ポリシーを承認すると、ユーザーはインターネットを参照できます。

- [Authentication Server] ドロップダウンリストから [Web Authentication Internal] または [Web Passthrough Internal] を選択した場合、ページは シスコ ワイヤレス コントローラによって再構築されます。
- [Authentication Server] ドロップダウンリストから [Web Authentication External] または [Web Passthrough External] を選択した場合、クライアントは指定した URL にリダイレクトされます。[Web Auth Url] フィールドにリダイレクト URL を入力する必要があります。

ステップ 14 [TIMEOUT SETTINGS FOR SLEEPING CLIENTS] の下で、スリープ状態のクライアントの認証を設定します。[Always authenticate] または [Authenticate after] を選択できます。

Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ～ 43200 分、デフォルトは 720 分です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープ タイマーは、アイドルタイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープ タイマーに設定された時間より短い場合、クライアントのライフタイムがスリープ時間として使用されます。

- スリープ状態のクライアントの認証を有効にするには、[Always authenticate] オプションボタンをクリックします。
- [Authenticate after] オプションボタンをクリックし、再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間を入力します。有効な範囲は 10 ～ 43200 分、デフォルト期間は 720 分です。

ステップ 15 次の内容を設定するには、[Show Advanced Settings] をクリックします。

ステップ 16 [Client Exclusion] チェックボックスをオンにして、[in (secs)] フィールドにクライアント除外タイマーの設定値を入力します。

ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続対象から除外するため、除外タイマーが期限切れになるまで、クライアントはネットワークに接続できません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。指定できる範囲は 0 ～ 2147483647 秒です。

ステップ 17 [Session Timeout] チェックボックスをオンにして、値（秒）を入力します。

セッションタイムアウトとは、クライアントセッションがアクティブである最大時間を指します。この時間が経過すると再認証を受ける必要があります。デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。値の範囲は 300 ～ 86400 秒です。

ステップ 18 Under **MFP Client Protection**, click one of the radio buttons: **Optional**, **Required**, and **Disabled**.

管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、アクセスポイントとクライアントとの間で送受信される、保護および暗号化されていない802.11管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは [Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 にも設定されている場合）にのみ、クライアントはアソシエーションを許可されます。

ステップ 19 [11k] で [Neighbor List] チェックボックスをオンにすると、その 11k 対応クライアントは、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できます。

ローミングを容易にするため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。同じ WLAN にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して、AP は応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

ステップ 20 [11v BSS Transition Support] で、次のように設定します。

ステップ 21 [BSS Max Idle Service] チェックボックスをオンにして、アイドル期間タイマー値を設定します。アイドル期間タイマー値は、APからクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントを関連付け解除しないタイムフレームです。

ステップ 22 [Client User Idle Timeout] チェックボックスをオンにして、[Client User Idle Timeout] フィールドに WLAN のユーザーアイドルタイムアウトの設定値を入力します。

クライアントが送信するデータがユーザーアイドルタイムアウト内で指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは次のタイムアウト期間中に更新されます。

デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザーアイドルタイムアウト付きで有効になります。

ステップ 23 [Directed Multicast Service] チェックボックスをオンにして、Directed Multicast Service を有効にします。

デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するように AP に要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

ステップ 24 [Next] をクリックします。

[ワイヤレス プロファイル（Wireless Profiles）] ウィンドウが表示されます。

ステップ 25 既存のワイヤレスプロファイルがない場合は、[Wireless Profiles] ウィンドウで [Add] をクリックして、新しいワイヤレスプロファイルを作成します。

ステップ 26 [Wireless Profile Name] フィールドにプロファイル名を入力します。

ステップ 27 [ファブリック（Fabric）] の隣にある [はい（Yes）] または [いいえ（No）] ラジオ ボタンを選択して、SSID がファブリックであるか、そうでないかを指定します。

ファブリック SSID は、ソフトウェア定義型アクセス (SD アクセス) の一部であるワイヤレスネットワークです。SDアクセスは、有線およびワイヤレスネットワークの設定、ポリシー、およびトラブルシューティングを自動化し、簡素化するソリューションです。ファブリック SSID を使用する場合は、SDA を使用することが必須です。非ファブリックは、SDアクセスを必要としない従来のワイヤレスネットワークです。

ステップ 28 ゲスト SSID をゲスト アンカーにする場合、[このゲスト SSID にゲスト アンカーが必要ですか（Do you need a Guest Anchor for this guest SSID）] の隣にある [はい（Yes）] または [いいえ（No）] ラジオ ボタンをクリックします。

ゲスト SSID をゲストアンカーにするには、[Yes] をクリックします。

ステップ 29 [Select Interface] ドロップダウンリストからインターフェイスを選択するか、[+] をクリックして新しいワイヤレスインターフェイスを作成します。

これは、ワイヤレス インターフェイスに関連付けられている VLAN ID です。

ステップ 30 [No] をクリックした場合は、[Flex Connect Local Switching] チェックボックスをオンにして、FlexConnect モードを有効にします。FlexConnect を選択すると、トラフィックがローカルに切り替わります。設定に基づき、プロファイルはサイトおよび内部的に作成された Flex グループに適用されます。

ステップ 31 [Local to VLAN] フィールドに VLAN ID の値を入力します。

ステップ 32 このプロファイルをサイトに割り当てるには、[Sites] をクリックします。

ステップ 33 [Sites] ウィンドウで、このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにして、[OK] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、すべての子が親サイトから設定を継承します。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 34 [+ Add Model Config] をクリックして、モデル設定設計をワイヤレスプロファイルに関連付けます。

[Add Model Config] ウィンドウが表示されます。

ステップ 35 [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[Search...] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 36 [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。

ステップ 37 [Add] をクリックします。

ステップ 38 [Save] をクリックします。

[Wireless Profiles] ウィンドウに、作成したプロファイルが表示されます。

ステップ 39 SSID をワイヤレスプロファイルに関連付けるには、[Wireless Profiles] ウィンドウで、[Profile Name] チェックボックスをオンにして SSID を関連付けてから、[Next] をクリックします。
[ポータルのカスタマイズ（Portal Customization）] ウィンドウが表示され、ゲスト ポータルに SSID を割り当てることができます。

ステップ 40 [Portal Customization] ウィンドウで [Add] をクリックして、ゲストポータルを作成します。

[ポータル ビルダー（Portal Builder）] ウィンドウが表示されます。

ステップ 41 左側のメニューで [ページ コンテンツ（Page Content）] を展開し、さまざまな変数を組み込みます。

ステップ 42 ポータル テンプレート ウィンドウに変数をドラッグ アンド ドロップし、それらを編集します。

- [Login] ページの変数は次のとおりです。
  - **Access Code**
  - **Header Text**
  - **AUP**
  - **Text Field**
- [Registration] ページの変数は次のとおりです。
  - **[名（First Name）]**
  - **姓（Last Name）**
  - **Phone Number**
  - **会社（Company）**
  - **SMS プロバイダ（SMS Provider）**
  - **Person being visited**
  - **Reason for a visit**
  - **Header text**
  - **[User Name]**
  - **電子メール アドレス（Email Address）**
  - **AUP**
- [Registration Success] ページの変数は次のとおりです。
  - **Account Created**
  - **Header texts**

- [成功（Success）] ページの変数：**テキストフィールド**です。

ステップ 43 ポータルのデフォルト カラー スキームをカスタマイズするには、左側のメニューで [色（Color）] を展開し、色を変更します。

ステップ 44 フォントをカスタマイズするには、左側のメニューで [フォント（Font）] を展開し、フォントを変更します。

ステップ 45 **[Save]** をクリックします。

[ポータルのカスタマイズ（Portal Customization）] ページに作成したポータルが表示されます。

ステップ 46 [Portals] の下で、[Portal Name] の横にあるオプションボタンをクリックし、ゲストポータルに SSID を割り当てます。

ステップ 47 [完了（Finish）] をクリックします。

ワイヤレスインターフェイスの作成

非ファブリック展開でのみワイヤレスインターフェイスを作成できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network settings]**。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで [Global] が選択されていることを確認します。

ステップ 4 [Wireless Interfaces] テーブルで、[+Add] をクリックします。

ステップ 5 [Create a Wireless Interface] スライドペインでワイヤレスインターフェイスの設定を指定します。

a) [Interface Name] フィールドに、動的なインターフェイスの名前を入力します。

b) [VLAN ID] フィールドに、このインターフェイスの VLAN ID を入力します。

ステップ 6 [**保存（Save**）] をクリックします。

結果：ワイヤレスインターフェイスが作成され、[Wireless Interfaces] テーブルに表示されます。

ワイヤレス無線周波数プロファイルの作成

デフォルトの無線周波数プロファイル（低、標準、高）を使用することも、カスタムの無線周波数プロファイルを作成することもできます。

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**[Design]** > **[Network Settings]** > **[Wireless]**。

ステップ 2 **[ワイヤレス無線周波数プロファイル（Wireless Radio Frequency Profile）]** の下で、**[+ RF を追加（+Add RF）]**をクリックします。

[ワイヤレス無線周波数（Wireless Radio Frequency）] ウィンドウが表示されます。

ステップ 3 [プロファイル名（Profile Name）] テキスト ボックスに、RF プロファイル名を入力します。

ステップ 4 **[オン（On）]/[オフ（Off）]** ボタンを使用して、**[2.4 GHz]** または **[5 GHz]** のいずれかの無線バンドを選択します。無線のうちの 1 つを無効にした場合、この AP プロファイルを設定しようとしている AP の基本の無線が無効になります。

ステップ 5 [2.4 GHz] 無線タイプでは、次を設定します。

- [Parent Profile] で、[High]、[Medium（Typica）]、[Low]、[Custom] のいずれかを選択します。（[データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドは、選択された親プロファイルによって変更されます。たとえば、[High] を選択した場合、2.4 GHz のデバイスで使用可能なプロファイル設定が追加されます。保存された [データレート（Data Rate）] および [Tx設定（Tx Configuration）] で設定を変更すると、[親プロファイル（Parent Profile）] は自動的に [カスタム（Custom）] に変更されます。）選択したカスタム プロファイルに対してのみ、新しい RF プロファイルが作成されることに注意してください。

  （注） [低（Low）]、[中（標準）（Medium (Typical)）]、および [高（High）] は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、デバイスにあるそれぞれの RF プロファイルが使用され、新しい RF プロファイルは Cisco DNA Center で作成されません。

- [DCA] は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。
  - **[すべて選択（Select All）]** チェック ボックスをオンにして、DCA チャネル **[1]**、**[6]**、および **[11]** を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
  - **[詳細オプション（Advanced Options）]** の下で **[詳細設定を表示（Show Advanced）]** をクリックし、チャネル番号を選択します。[Select All] チェックボックスをオンにして、[Advanced Options] の下にある DCA チャネルを選択するか、個々のチャネル番号の横にあるチェックボックスをオンにします。B プロファイルで使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

    （注） シスコ ワイヤレス コントローラでこれらのチャネルをグローバルに設定する必要があります。

- アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
- [Tx電力構成（Tx Power Configuration）] で、AP の電力レベルと電力しきい値を設定できます。
  - **電力レベル**：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は-10 ～ 30 dBm で、デフォルトは -10 dBM です。
  - **電力しきい値**：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値（Power Threshold）] スライダを使用して電力値を

増減させ、APをより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 dBM ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。

- RX SOP：レシーバのパケット検出開始しきい値（RX SOP）は、APの無線がパケットを復調してデコードするdBm単位のWi-Fi信号レベルを決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

ステップ 6 [5 GHz] 無線タイプでは、次を設定します。

- **[親プロファイル（Parent Profile）]** ドロップダウン リストから、**[高（High）]**、**[中（標準）（Medium (Typical)）]**、**[低（Low）]**、または **[カスタム（Custom）]** を選択します。（[データレート（Data Rate）]および[Tx設定（Tx Configuration）]フィールドは、選択された親プロファイルによって変更されます。たとえば、[高（High）]を選択した場合、2.4 GHzのデバイスで使用可能な設定が追加されます。保存された [データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドで設定を変更すると、[親プロファイル（Parent Profile）] は自動的に [カスタム（Custom）] に変更されます。）選択したカスタム プロファイルに対してのみ、新しい RF プロファイルが作成されます。

  （注） [低（Low）]、[中（標準）（Medium (Typical)）]、および [高（High）] は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、すでにデバイスにあるそれぞれの RF プロファイルが使用され、新しい RF プロファイルは Cisco DNA Center で作成されません。

- [チャネル幅（Channel Width）] ドロップダウン リストから、チャネル帯域幅オプションを 1 つ選択します：[最適（Best）]、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [最適（Best）]。
- [DCA チャネル（DCA Channel）] を設定して、チャネルの割り当てを管理します。

  （注） シスコ ワイヤレス コントローラでこれらのチャネルをグローバルに設定する必要があります。

  - [UNNI-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。[UNII-1 36-48] チェック ボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェック ボックスをオンにして、個別に選択します。
  - [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。[UNII-2 52-144] チェック ボックスをオンにしてすべてのチャネルを含めるか、1 つまたは複数のチャネルのチェック ボックスをオンにして、個別に選択します。
  - [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。[UNII-3 149-165] チェック ボックスをオンにしてすべてのチャネルを含めるか、1 つまたは複数のチャネルのチェック ボックスをオンにして、個別に選択します。

- アクセスポイントとクライアント間でデータを送信できるレートを設定するには、[データレート（Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。
- [Tx電力構成（Tx Power Configuration）] で、AP の電力レベルと電力しきい値を設定できます。

- **電力レベル**：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は-10 ～ 30 dBm で、デフォルトは -10 dBM です。
- **電力しきい値**：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値（Power Threshold）] スライダを使用して電力値を増減させ、APをより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 dBM ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
- RX SOP：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウンリストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

ステップ 7 **[Save]** をクリックします。

ステップ 8 プロファイルをデフォルトの RF プロファイルとしてマークするには、[Profile Name] チェックボックスをオンにし、[Mark Default] をクリックします。

ステップ 9 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

バックホールの設定の管理

ワイヤレスセンサのバックホール設定を表示、作成、管理するには、次の手順を実行します。ワイヤレスセンサーには、Cisco DNA Center と通信するためのバックホール SSID が必要です。

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**[Assurance]** > **[Manage]** > **[Sensors]** の順に選択します。

結果：[Sensor List] ウィンドウが表示されます。

ステップ 2 [Settings] タブにカーソルを合わせ、[Backhaul Settings] を選択します。

ステップ 3 バックホール SSID を追加および管理するには、次の手順を実行します。

a) [Add Backhaul] をクリックします。

[Create Sensor Backhaul SSID Assignment] ウィンドウが表示され、[Wired Backhaul] と [Wireless Backhaul] の 2 つの領域が表示されます。

b) [Settings name] フィールドでバックホール SSID の名前を入力します。

c) [Wired Backhaul] 領域で、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - **802.1x EAP**：Extensible Authentication Protocol（EAP）を有線 LAN で渡すために使用される規格。

- **Open**：セキュリティまたは認証は使用されません。

- [EAP Method]：[802.1x EAP] を選択した場合は、ドロップダウンリストからユーザ認証に次のいずれかの EAP 方式を選択する必要があります。
  - [EAP-FAST]：指定されたフィールドにユーザ名とパスワードを入力します。
  - [PEAP-MSCHAPv2]：指定されたフィールドにユーザ名とパスワードを入力します。
  - [EAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。
  - [PEAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll using SCEP] を選択します。

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name (SSID)] 領域で、ワイヤレスネットワーク（SSID）を選択し、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - [WPA2 Enterprise]：拡張可能認証プロトコル（EAP）（802.1x）を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワークユーザを認証および承認します。
  - [WPA2-Personal]：パスフレーズまたは事前共有キー（PSK）を使用して、良好なセキュリティを実現します。ワイヤレスネットワークにアクセスするパスキーがあれば誰でも使用できます。

    [WPA2パーソナル（WPA2 Personal）] を選択した場合は、[パスフレーズ（Passphrase）] テキストボックスにパスフレーズを入力します。
  - [PSK Format]：使用可能な事前共有キーの形式は次のとおりです。
    - [ASCII]：ASCII PSK パスフレーズをサポートします。
    - [HEX]：64 文字の HEX キー PSK パスワードをサポートします。
  - **Open**：セキュリティまたは認証は使用されません。

e) [**保存（Save）**] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。
b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

Cisco Connected Mobile Experiences の統合について

Cisco DNA Center ワイヤレスマップのためのコネクテッドモバイルエクスペリエンス（CMX）の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディング レベルで CMX を割り当てることができ、小企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX 設定の作成

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]** > **[CMX Servers]** の順に選択します。

[CMX Servers] ウィンドウが表示されます。

ステップ 2 [Add] をクリックします。

[Add CMX Servers] ウィンドウが表示されます。

ステップ 3 [IP Address] フィールドに、CMX Web GUI の有効な IP アドレスを入力します。

ステップ 4 [User Name] および [Password] フィールドに、CMX Web GUI のユーザー名とパスワードのログイン情報を入力します。

ステップ 5 [SSH User Name] および [SSH Password] フィールドに、CMX 管理者のユーザー名とパスワードのログイン情報を入力します。

（注） CMX が到達可能であることを確認してください。

ステップ 6 [Add]をクリックします。

CMX サーバーが正常に追加されました。

ステップ 7 CMXサーバーをサイト、建物、またはフロアに割り当てるには、[Menu]アイコンをクリックし、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 8 左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。

ステップ 9 [CMX Servers] の下で、[CMX Servers] ドロップダウンリストから CMX サーバーを選択します。

ステップ 10 [Save] をクリックします。

[Create CMX Settings] ページが表示されます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

フロアマップでは、次のことを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] タブで表示されます。詳細については、各タブをクリックしてください。[デバイス 360（Device 360）] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアント デバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイド バーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

ステップ 11 変更を加えたときに CMX がダウンした場合は、手動で同期する必要があります。同期するには、[Network Hierarchy] ページで、左側のツリーペインで変更を加えたビルディングやフロアの隣にある歯車アイコンをクリックし、[Sync with CMX] を選択して、変更を手動でプッシュします。

ステップ 12 CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) 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]** > **[CMX Servers]** の順に選択します。
b) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
c) 削除する CMX サーバーを選択し、[Delete] をクリックします。
d) [OK] をクリックして削除を実行します。

CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web GUI にログインできるか確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX UI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントが Cisco DNA Center フロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブになっているか確認します。

- CMX GUI でフロアマップにクライアントが表示されるか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```

Flex グループのネイティブ VLAN 設定

ネイティブ VLAN は、AP と シスコ ワイヤレス コントローラ 間の管理トラフィックを伝送します。この機能を使用すると、Cisco DNA Center ユーザー インターフェイスを介してサイトの VLAN を設定できます。グローバル レベルでネイティブ VLAN を設定し、サイト、ビルディング、またはフロア レベルでオーバーライドできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Settings]** > **[Wireless]**。

ステップ 2 グローバル レベルでネイティブ VLAN を設定する場合、左ペインで [グローバル（Global）] を選択します。

ステップ 3 [ネイティブVLAN（Native VLAN）] の下の [VLAN] テキスト ボックスに、VLAN ID の値を入力します。有効な範囲は 1 ～ 4094 です。

ステップ 4 **[Save]** をクリックします。

ステップ 5 SSID を設定し、ワイヤレス ネットワーク プロファイルを作成します。**[設計（Design）]** > **[ネットワークの設定（Network Settings）]** > **[ワイヤレス（Wireless）]** ページの [FlexConnect ローカル スイッチング（FlexConnect Local Switching）] チェック ボックスがオンになっていることを確認します。詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）を参照してください。

ステップ 6 保存済みの VLAN ID を ワイヤレスコントローラ で設定するには、ワイヤレスコントローラ を [プロビジョニング（Provision）] ページでプロビジョニングする必要があります。詳細については、「Cisco AireOS コントローラのプロビジョニング （391 ページ）」を参照してください。

ステップ 7 ワイヤレスコントローラ のプロビジョニング後に、コントローラに関連付けられている AP をプロビジョニングする必要があります。詳細については、「#unique_194」を参照してください。

ステップ 8 サイト、ビルディング、またはフロア レベルでネイティブ VLAN をオーバーライドするには、左側のツリー ビュー メニューでサイト、ビルディングまたはフロアを選択します。

ステップ 9 [ネイティブVLAN（Native VLAN）] の下で、VLAN ID の値を入力します。

ステップ 10 ワイヤレスコントローラ および関連付けられているアクセス ポイントを再プロビジョニングします。

ネットワーク プロファイルの作成

[設計（Design）] > [ネットワークプロファイル（Network Profiles）] の順に進み、[プロファイルの追加（Add Profile）] をクリックして次の要素向けのネットワークプロファイルを作成します。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します >

- ルーティングと NFV
- スイッチング
- ワイヤレス

NFVIS 用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ENCS 統合スイッチを設定します。

（注） このオプションは、ENCS 5400 デバイスでのみ使用できます。

3. カスタム構成を作成します。
4. プロファイルの概要を表示します。

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**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [+Add Profile] をクリックし、[NFVIS] を選択します。

ステップ 3 [ルータWAN構成（Router WAN Configuration）] ウィンドウが表示されます。

- [名前（Name）] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダと 2 つのデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、「サービス プロバイダ プロファイルの設定 （203 ページ）」を参照してください。
- ドロップダウンリストから [Device Type]デバイスタイプを選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。選択内容は、ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。

- デバイスごとに 1 つ以上の回線リンクを有効にするには、[O] をクリックし、[Connect] の横のチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。
- [+サービスの追加（+Add Services）] をクリックして、プロファイルにサービスを追加します。[サービスの追加（Add Services）] ウィンドウが表示されます。[Router]、[Firewall]、[Application] のいずれかのアイコンをクリックして図にドラッグします。選択内容に基づいて、デフォルトのネットワーク接続が自動的に作成されます。または、[Custom- Net] を選択して、プロファイルにカスタムサービスまたはネットワークを追加することもできます。

  ルータを設定するには、ルータをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[Profile] を選択します。詳細については、「ソフトウェア イメージのインポート （104 ページ）」を参照してください。[vNIC Mapping] のフィールドを必要に応じて設定します。

  ファイアウォールを設定するには、ファイアウォールをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[Profile] を選択します。[Type] のドロップダウンリストは、システムにインストールされているファイアウォールプラグインに基づいて入力されます。[vNIC Mapping] のフィールドを必要に応じて設定します。

  アプリケーションを設定するには、アプリケーションをクリックして [Configuration] を選択します。ドロップダウンリストから [Type]、[Image]、[Profile] を選択します。[Type] のドロップダウンリストは、システムにインストールされているアプリケーションプラグインに基づいて入力されます。[vNIC Mapping] のフィールドを必要に応じて設定します。

  カスタムネットワークを設定するには、[custom-net interface] をクリックします。[Connect from] を選択し、カスタムネットワークを追加するノードをクリックして [Connect to] を選択します。[custom-net] をクリックし、[Add Configuration] を選択します。[Network Mode] を選択し、[VLAN] に VLAN ID を入力します。

  [Save] をクリックします。
- **[Next]** をクリックします。

ステップ 4 ENCS デバイスを選択した場合は、[ENCS Integrated Switch Configuration] ページが表示されます。

- [+Add Row] をクリックします。ドロップダウンリストから、[Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- **[Next]** をクリックします。

ステップ 5 [カスタム構成（Custom Configuration）] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ページでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template(s)] または [Day-N Templates] タブを選択します。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタ処理されます。

- **[Next]** をクリックします。

ステップ 6 **[概要（Summary）]** ページが表示されます。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項がこのページで提供されます。

- **[Save]** をクリックします。

ステップ 7 [ネットワークプロファイル（Network Profiles）] ページが表示されます。

[サイトの割り当て（Assign Sites）] をクリックして、ネットワーク プロファイルにサイトを割り当てます。詳細については、ネットワーク階層のサイトの作成 （125 ページ）を参照してください。

ルーティング用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ルータ LAN を設定します。
3. 統合スイッチ構成を設定します。
4. カスタム構成を作成します。
5. プロファイルの概要を表示します。

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**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [+Add Profile] をクリックし、[Routing] を選択します。

ステップ 3 [ルータWAN構成（Router WAN Configuration）] ウィンドウが表示されます。

- [名前（Name）] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダと 10 つのデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、「サービス プロバイダ プロファイルの設定 （203 ページ）」を参照してください。
- ドロップダウンリストから [Device Type]デバイスタイプを選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。2 つ以上のデバイスが同じタイプの場合は、デバイスタグを使用します。すべてのデバイスが異なるタイプの場合、デバイスタグはオプションです。選択内容は、ネットワークプ

ロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。

- デバイスごとに 1 つ以上の回線リンクを有効にするには、[O] をクリックし、[Connect] の横のチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。

  複数のサービスプロバイダを選択した場合は、プライマリインターフェイスをギガビットイーサネットとして、セカンダリをセルラーとして、または両方のインターフェイスをギガビットイーサネットとして選択できます。また、プライマリインターフェイスをセルラーとして、セカンダリインターフェイスをギガビットイーサネットとして選択することもできます。

  （注） Cisco 1100 シリーズ サービス統合型ルータ、Cisco 4200 シリーズ サービス統合型ルータ、Cisco 4300 シリーズ サービス統合型ルータ、および Cisco 4400 シリーズ サービス統合型ルータのみが、セルラーインターフェイスをサポートしています。

- **[次へ (Next)]** をクリックします。

ステップ 4 [ルータWAN構成（Router WAN Configuration）] ページが表示されます。

- [Configure Connection] オプションボタンをクリックし、[L2] または [L3]、あるいはその両方を選択します。
- [L2] を選択した場合は、ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- [L3] を選択した場合は、ドロップダウンリストから [Protocol Routing] を選択し、[Protocol Qualifier] を入力します。

[Skip] をクリックして、設定をスキップできます。

- **[次へ (Next)]** をクリックします。

ステップ 5 [Integrated Switch Configuration] ページが表示されます。

統合スイッチの設定では、新しい VLAN を追加したり、ルータの LAN 設定で選択した以前の設定を保持したりすることができます。

- 1 つ以上の新しい VLAN を追加するには、[+] をクリックします。
- VLAN を削除するには、[x] をクリックします。
- [Next] をクリックします。

（注） Switchport インターフェイスのサポートは、Cisco 1100 シリーズおよび Cisco 4000 シリーズ サービス統合型ルータでのみ使用できます。

ステップ 6 [カスタム構成（Custom Configuration）] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ページでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template(s)] または [Day-N Templates] タブをクリックします。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタ処理されます。
- [Next] をクリックします。

ステップ 7 [Summary] ページで、[Save] をクリックします。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項が提供されます。

ステップ 8 [ネットワークプロファイル（Network Profiles）] ページが表示されます。

[サイトの割り当て（Assign Sites）] をクリックして、ネットワークプロファイルにサイトを割り当てます。詳細については、ネットワーク階層のサイトの作成 （125 ページ）を参照してください。

スイッチ用のネットワークプロファイルの作成

スイッチングプロファイルには、次の 2 つのタイプの設定テンプレートを適用できます。

- オンボーディングテンプレート
- Day N テンプレート

始める前に

デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。『デバイス設定の変更を自動化するテンプレートの作成 （209 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**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [+Add Profile] をクリックし、[Switching] を選択します。

ステップ 3 [Switching profile] ウィンドウで、[Profile Name] テキストボックスにプロファイル名を入力します。

作成するテンプレートのタイプに応じて、[OnBoarding Template(s)] または [Day-N Template(s)] を選クリックします。

- [追加（Add）] をクリックします。
- [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。

- ドロップダウンリストから [Tag Name] を選択します。この手順は任意です。選択したタグがすでにテンプレートに関連付けられている場合は、そのテンプレートのみが [Template] ドロップダウンリストで使用できます。
- ドロップダウンリストから [Device Type] を選択します。
- ドロップダウンリストから [Template] を選択します。すでに作成済みの [Onboarding Configuration] テンプレートを選択できます。

ステップ 4 **[Save]** をクリックします。

スイッチに設定されているプロファイルは、スイッチのプロビジョニング時に適用されます。サイトを有効にするには、サイトにネットワークプロファイルを追加する必要があります。

ワイヤレス用のネットワークプロファイルの作成

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**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [+Add Profile] をクリックし、[Wireless] を選択します。

ワイヤレス ネットワーク プロファイルを割り当てる前に、**[Design]** > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID を作成していることを確認します。

ステップ 3 [Add a Network Profile] ウィンドウで、[Profile Name] テキストボックスに有効なプロファイル名を入力します。

ステップ 4 [+ SSIDの追加（+ Add SSID）] をクリックします。

作成した SSID が入力されます。

ステップ 5 [SSID] ドロップダウン リストで、[SSID] を選択します。

SSID タイプが表示されます。

ステップ 6 [Yes] または [No] を選択して、SSID がファブリックであるか、非ファブリックであるかを指定します。

ステップ 7 非ファブリック SSID を作成する場合は、[No] を選択して次のパラメータを設定します。

ステップ 8 [Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ create a new wireless interface] をクリックして新しいワイヤレスインターフェイスを作成します。

ステップ 9 [Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。

ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect アクセスポイントがデータパケットをローカルにスイッチできます。

ステップ 10 ワイヤレスインターフェイスに関連付けられている VLAN ID は、選択したインターフェイス名に基づいて自動的に入力されます。

VLAN ID を変更する場合は、[Local to VLAN] テキストボックスに VLAN ID の新しい値を入力します。

ステップ 11 [+ Add Model Config] をクリックして、モデル設定設計をネットワークプロファイルに追加します。

[Add Model Config] ウィンドウが表示されます。

ステップ 12 [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[search] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 13 [Wireless] を展開し、このワイヤレスプロファイルに関連付けるモデル設定設計を選択します。

ステップ 14 [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。

ステップ 15 [Add] をクリックします。

関連付けられたモデル設定が [Add a Network Profile] ウィンドウの [Attach Model Config] 領域に表示されます。

ステップ 16 テンプレートをネットワークプロファイルに関連付けるには、[Attach Template(s)] 領域の下にある [Add] をクリックします。

ステップ 17 [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[search] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

ステップ 18 [Device Tag] と [Template] のドロップダウンリストから、デバイスタグとテンプレートを選択できます。

テンプレートではタグを使用できます。これを使用するのは、デバイスタグに基づいて同じデバイスタイプに対して異なるテンプレートをプッシュする必要がある場合だけです。

ステップ 19 [Add]をクリックします。

[Wireless Profiles] ウィンドウに、作成したプロファイルが表示されます。

ステップ 20 [Save] をクリックして、ネットワークプロファイルを追加します。

新しく追加されたネットワークプロファイルが、**[Design]** > **[Network Profiles]** ページに表示されます。

ステップ 21 このプロファイルをサイトに割り当てるには、[Assign Sites] をクリックします。

ステップ 22 [Add Sites To Profile] ウィンドウで、サイトの横にあるチェックボックスをオンにしてこのプロファイルを関連付けます。

親ノードまたは個々のサイトを選択できます。親サイトを選択すると、その親ノードの下にある子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 23 [Save] をクリックします。

ネットワークプロファイルの AP グループ、Flex グループ、およびサイトタグの事前プロビジョニング

Cisco DNA Center では、ネットワークプロファイルに AP グループ、Flex グループ、およびサイトタグを事前プロビジョニングできます。事前プロビジョニングすると、反復的な構成変更の必要がなくなることで AP プロビジョニング時の時間を節約でき、デバイス間の一貫性を確保できます。

- AP グループ構成は、AireOS イメージを実行するワイヤレス LAN コントローラに適用できます。
- Flex グループ構成は、AireOS イメージを実行するワイヤレス LAN コントローラに適用できます。
- サイトタグ構成は、Catalyst 9800 シリーズ ワイヤレス コントローラに適用できます

始める前に

AP グループ、Flex グループ、およびサイトタグを作成できるようにするには、ネットワークプロファイルを作成し、そのネットワークプロファイルにサイト（フロア）を割り当てる必要があります。

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**[Design]** > **[Network Profiles]** の順に選択します。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Show Advanced Settings] をクリックします。

ステップ 4 ネットワークプロファイルに AP グループを作成するには、[AP Group] を展開し、[+ Create an AP Group] をクリックします。

[Create an AP Group] ウィンドウが表示されます。

ステップ 5 [AP Group Name] フィールドに、AP グループ名を入力します。

ステップ 6 [RF Profile] ドロップダウンリストから、RF プロファイルを選択します。

オプションは、[High]、[Typical]、[Low]、[custom_rf_profile2]、および [rf_prof1_custom] です。

ステップ 7 [Select Sites] フィールドで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

ステップ 8 （オプション）[Save & Add another] をクリックして別の AP グループを追加します。

ステップ 9 **[保存（Save）]** をクリックします。

AP グループは、[Edit Network Profile] ウィンドウの [AP Group] 領域で選択した RF プロファイルに基づいて作成されます。

ステップ 10 ネットワークプロファイルで Flex グループを有効にするには、[Flex Connect Local Switching] チェックボックスをオンにし、[Local to VLAN] テキストボックスに VLAN ID を定義して、非ファブリック SSID を Flex ベースの SSID としてマークします。

[Flex Group] オプションは、[View Advanced Settings] で有効になります。

ステップ 11 ネットワークプロファイルに Flex グループを作成するには、[Flex Group] を展開し、[+ Create Flex Group] をクリックします。

[Create Flex Group] ウィンドウが表示されます。

ステップ 12 [Flex Group] フィールドに、Flex グループ名を入力します。

ステップ 13 [Select Sites] フィールドで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

ステップ 14 （オプション）[Save & Add another] をクリックして別の Flex グループを追加します。

ステップ 15 **[保存（Save）]** をクリックします。

Flex グループは、[Edit Network Profile] ウィンドウの [Flex Group] 領域に作成されます。

ステップ 16 ネットワークプロファイルにサイトタグを作成するには、[Site Tag] を展開し、[+ Create a Site Tag] をクリックします。

[Create a Site Tag] ウィンドウが表示されます。

ステップ 17 [Site Tag] フィールドに、サイトタグ名を入力します。

ステップ 18 [Flex Profile Name] 名前フィールドに、Flex プロファイル名を入力します。

（注） [Flex Profile Name] 名前フィールドを有効にするには、[Edit Network Profile] ウィンドウの [Flex Connect Local Switching] チェックボックスをオンにします。

ステップ 19 [Select Sites] フィールドで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

ステップ 20 （オプション）[Save & Add another] をクリックして別のサイトタグを追加します。

ステップ 21 **[保存（Save）]** をクリックします。

サイトタグは、[Edit Network Profile] ウィンドウの [Site Tag] 領域の下に作成されます。

グローバルネットワーク設定の管理

ネットワーク全体のデフォルトになるネットワーク設定を作成できます。ネットワーク内の設定を定義可能な主なエリアは次の 2 つです。

- [Global settings]：ここで定義されている設定はネットワーク全体に適用されます。DHCP、DNS、AAA、NTP などのサーバー、IP アドレスプール、デバイス クレデンシャル プロファイル、Syslog、トラップ、Netflow などのテレメトリの設定が含まれます。

- [Site settings]：ここで定義されている設定はグローバル設定をオーバーライドします。また、サーバー、IPアドレスプール、デバイスのログイン情報プロファイルの設定を含めることができます。

（注） アクティブなファブリックで使用されているネットワーク設定の変更はサポートされていません。それらのネットワーク設定には、サイト階層、IP プールの名前変更など複数の機能が含まれます。

（注） 一部のネットワーク設定は、デバイスの可制御性機能を使用してデバイスに自動的に設定できます。Cisco DNA Centerによるデバイスの設定または更新時に、トランザクションが Cisco DNA Center の監査ログにキャプチャされます。監査ログを使用すると、変更を追跡し、問題をトラブルシューティングするのに役立ちます。

[Design] > **[Network Settings]** の順に選択して該当するタブをクリックし、次のグローバルネットワーク設定を定義できます。

- AAA、DHCP、DNS サーバーなどのネットワーク サーバー：詳細については、グローバル ネットワーク サーバーの設定 （204 ページ）を参照してください。
- CLI、SNMP、HTTP（S）などのデバイス クレデンシャル：詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、およびグローバル HTTPS クレデンシャルの設定 （193 ページ）を参照してください。
- IP アドレス プール：詳細については、IP アドレス プールを設定する （197 ページ）を参照してください。
- SSID、ワイヤレス インターフェイス、および無線周波数プロファイルなどのワイヤレス設定：詳細については、グローバル ワイヤレス設定の構成 （156 ページ）を参照してください。
- テレメトリを使用して、syslog、SNMP、NetFlow コレクタサーバーなどのグローバルテレメトリ設定を構成します。

デバイス クレデンシャルについて

デバイスクレデンシャルとは、ネットワークデバイスに設定されている CLI、SNMP、HTTPS クレデンシャルを指します。Cisco DNA Center では、これらのクレデンシャルを使用してネットワーク内のデバイスに関する情報を検出および収集します。Cisco DNA Center では、ほとんどのデバイスが使用するクレデンシャルを指定できるため、ディスカバリ ジョブを実行するたびにクレデンシャルを入力する必要はありません。設定したクレデンシャルは、[ディスカバリ（Discovery）] ツールで使用可能になります。

CLI クレデンシャル

ディスカバリ ジョブを実行するには、Cisco DNA Center でネットワーク デバイスの CLI クレデンシャルを設定する必要があります。

これらのクレデンシャルは、ネットワークデバイスの CLI にログインするために Cisco DNA Center によって使用されます。Cisco DNA Centerは、これらのクレデンシャルを使用して、ネットワークデバイスに関する情報を検出し、収集します。ディスカバリ プロセスの実行時に、Cisco DNA Center は CLI ユーザー名とパスワードを使用してネットワーク デバイスにログインし、**show** コマンドを実行してデバイスのステータスや設定情報を収集します。また、**clear** コマンドやその他のコマンドを実行して、デバイスの設定に保存されていないアクションを実行することもあります。

（注） Cisco DNA Center の実装では、ユーザー名だけがクリアテキストで提供されます。

SNMPv2c のクレデンシャル

簡易ネットワーク管理プロトコル（SNMP）は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供します。SNMP は、ネットワーク デバイスをモニターおよび管理するために標準化されたフレームワークと共通言語を提供しています。

SNMPv2c は SNMPv2 に代わるコミュニティ ストリング ベースの管理フレームワークです。SNMPv2c では、認証および暗号化が行われません（noAuthNoPriv セキュリティ レベル）。代わりに、クリアテキストで通常提供されるパスワード タイプとして、コミュニティ ストリングを使用します。

（注） Cisco DNA Center の実装では、セキュリティの理由から SNMP コミュニティ ストリングはクリアテキストで提供されません。

ディスカバリ機能を使用してネットワーク デバイスを検出する前に、SNMPv2c コミュニティ ストリング値を設定する必要があります。設定する SNMPv2c コミュニティ ストリング値は、ネットワーク デバイスで設定された SNMPv2c 値と一致している必要があります。Cisco DNA Center では、最大 5 つの read コミュニティ ストリングと 5 つの write コミュニティ ストリングを設定できます。

ネットワークで SNMPv2 を使用している場合、最善の結果を実現するには Read Only（RO）コミュニティ ストリング値と Read/Write（RW）コミュニティ ストリング値の両方を指定します。両方を指定できない場合は、RO 値を指定することを推奨します。RO 値を指定しなければ、Cisco DNA Center はデフォルトの RO コミュニティ ストリングの *public* を使用してデバイスを検出しようとします。RW 値のみを指定すると、ディスカバリで RW 値が RO 値として使用されます。

プラグアンドプレイの場合は、SNMPv2c の読み取り専用と読み取り/書き込みの両方のログイン情報を指定する必要があります。

SNMPv3 のクレデンシャル

ディスカバリを使用するために設定する SNMPv3 値は、ネットワーク デバイスで設定された SNMPv3 値と一致している必要があります。最大 5 つの SNMPv3 値を設定できます。

SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージが有効な送信元からのものかどうかを判別します。
- 暗号化：パケットコンテンツのスクランブルによって、不正な送信元から認識できないようにします。

SNMPv3 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティ モデルは、ユーザーおよびユーザー ロール向けに設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティモデル内のさまざまなセキュリティレベルは、次のとおりです。

- [noAuthNoPriv]：認証も暗号化も実行しないセキュリティレベル
- [AuthNoPriv]：認証は実行するが、暗号化を実行しないセキュリティレベル
- [AuthPriv]：認証と暗号化の両方を実行するセキュリティレベル

次の表に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 *36 : SNMPv3* セキュリティ モデルおよびセキュリティ レベル

レベル	認証	暗号化	結果
noAuthNoPriv	ユーザー名	未対応	ユーザ名の照合を使用して認証します。
AuthNoPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	なし	ハッシュメッセージ認証コード-セキュアハッシュ アルゴリズム（HMAC-SHA）に基づく認証を提供します。

レベル	認証	暗号化	結果
AuthPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	次のいずれかを行います。 • CBC-DES • CBC-AES-128	HMAC-MD5 または HMAC-SHA に基づく認証を提供します。 暗号ブロック連鎖（CBC）DES（DES-56）標準または CBC モードの AES 暗号化に基づいた認証に加え、データ暗号規格（DES）の 56 ビット暗号化を提供します。

セキュリティレベルは、SNMPv3 ユーザーとそのユーザーが属する SNMPv3 グループで同じである必要があります。SNMPv3 ユーザーとそのユーザーの SNMPv3 グループのセキュリティレベルが異なる場合に、Cisco DNA Center が SNMPv3 トラップホストを設定すると、デバイスの SNMP 到達可能性が阻害される可能性があります。

HTTPS クレデンシャル

HTTPS は、特殊な PKI 証明書ストアに基づく HTTP のセキュア バージョンです。

グローバル デバイス クレデンシャルについて

「グローバル デバイス クレデンシャル」とは、ネットワーク内のデバイスに関する情報を検出して収集するために Cisco DNA Center で使用される共通の CLI、SNMP、および HTTPS クレデンシャルを指します。Cisco DNA Center は、グローバル クレデンシャルを使用して設定済みデバイス クレデンシャルを共有するネットワーク内のデバイスを認証し、アクセスします。グローバル デバイス クレデンシャルの追加、編集、および削除することができます。また、グローバル サイトまたは特定のサイトにクレデンシャルを関連付けることもできます。

グローバル CLI クレデンシャルの設定

最大 5 つのグローバル CLIクレデンシャルを設定して保存できます。

ステップ 1 [Design] > [Network Settings] > [Device Credentials]。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > >

ステップ 2 グローバル サイトを選択した状態で、[CLI Credentials] エリアで [Add] をクリックします。

ステップ 3 次のフィールドに情報を入力します。

表 *37 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。

フィールド	説明
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 4 **[保存（Save）]** をクリックします。

サイトにクレデンシャルを適用するには、左側の階層にあるサイトをクリックし、クレデンシャルの横にあるボタンを選択して、[Save] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（Time Zone）] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル SNMPv2c クレデンシャルの設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv2c クレデンシャルを設定できます。

（注） プラグアンドプレイの場合は、SNMPv2c の読み取り専用と読み取り/書き込みの両方のクレデンシャルを指定する必要があります。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [Design] > [Network Settings] > [Device Credentials]。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します> >

ステップ 2 グローバル サイトを選択した状態で、[SNMP Credentials] エリアで [Add] をクリックします。

ステップ 3 [Type] で、[SNMP v2c] をクリックし、次の情報を入力します。

表 *38 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行（Now）] ラジオ ボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（Time Zone）] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル SNMPv3 クレデンシャルの設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv3 クレデンシャルを設定できます。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [設計（Design）] > [ネットワーク設定（Network Settings）] > [デバイスクレデンシャル（Device Credentials）]。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します> >

ステップ 2 グローバル サイトを選択した状態で、[SNMP Credentials] エリアで [Add] をクリックします。

ステップ 3 [タイプ（Type）] で、**[SNMP v3]** をクリックし、次の情報を入力します。

表 *39 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	SNMPv3を使用するデバイスから情報にアクセスする際に使用するSNMPv3パスワード。これらのパスワード（またはパスフレーズ）は、8文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用されるSNMPv3プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行（Now）]ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（Time Zone）] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル HTTPS クレデンシャルの設定

ステップ 1 [Design] > [Network Settings] > [Device Credentials]。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します > >

ステップ 2 グローバル サイトを選択した状態で、[HTTPS Credentials] エリアで [Add] をクリックします。

ステップ 3 次の情報を入力します。

表 *40 : HTTPS* クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 5 つの HTTPS 書き込みログイン情報を設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [タイム ゾーン（Time Zone）] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバルデバイスのログイン情報の編集に関する注意事項

既存のグローバル デバイス クレデンシャルの編集に関する注意事項と制約事項は、次のとおりです。

- Cisco DNA Center グローバル デバイス クレデンシャルを編集、保存、および適用する際は、次のプロセスが使用されます。

  1. Cisco DNA Center からローカル認証を持つデバイスにログイン情報がプッシュされます。ローカル認証では、ログイン情報の変更が適用され、Cisco DNA Center はこれらのログイン情報を使用してデバイスを管理します。

     （AAA サーバーが継承または設定されたサイトにあるデバイスには、Cisco DNA Center から CLI ログイン情報の変更はプッシュされません。AAA 認証では、ログイン情報の変更は適用されません。Cisco DNA Center は、同じログイン情報が AAA サーバーに存在する場合にのみ、これらのログイン情報を使用してデバイスを管理します）

  2. クレデンシャルがデバイスに正常にプッシュされると、Cisco DNA Center は新しいクレデンシャルを使用してデバイスに到達できることを確認します。

（注） この手順に失敗すると、Cisco DNA Center が新しいクレデンシャルをデバイスにプッシュしていても、インベントリでは古いクレデンシャルを使用してデバイスが管理されます。この場合、既存のログイン情報を更新すると、**[Provision]** > **[Inventory]** ウィンドウでデバイスが管理対象外であると示される可能性があります。

  3. 新しいクレデンシャルを使用してデバイスに正常に到達すると、Cisco DNA Center のインベントリは、新しいクレデンシャルを使用してデバイスの管理を開始します。

- サイトには、SNMPv2c クレデンシャルと SNMPv3 クレデンシャルを使用するデバイスを含めることができます。SNMPv2c または SNMPv3 のグローバル クレデンシャルを編集して保存すると、Cisco DNA Center はその変更をデバイスにプッシュし、そのクレデンシャルを有効にします。たとえば、SNMPv2c を使用するデバイスがあるのに、SNMPv3 のグローバル クレデンシャルを編集して保存すると、Cisco DNA Center は関連付けられたサイトのすべてのデバイスに新しい SNMPv3 のクレデンシャルをプッシュして、そのクレデンシャルを有効にします。つまり、以前は SNMPv2c が有効になっていたデバイスを含め、すべてのデバイスが SNMPv3 を使用して管理されるようになります。
- 混乱が生じないようにするために、CLI ログイン情報を編集する際は [User Name] を変更してください。これにより、新しい CLI クレデンシャルが作成され、既存の CLI クレデンシャルは変更されません。

グローバル デバイス クレデンシャルの編集

準備が整うまで、Cisco DNA Center でクレデンシャルの変更を適用せずに、グローバル デバイス クレデンシャルを編集および保存できます。変更の適用を決定すると、Cisco DNA Center は、変更したデバイス クレデンシャルを参照するすべてのサイトを検索し、すべてのデバイスに変更をプッシュします。

新しいグローバル デバイス クレデンシャルを更新または作成できますが、Cisco DNA Center はデバイスからクレデンシャルを削除することはありません。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコンをクリックし、**[Design]** > **[Network Settings]** > **[Device Credentials]** の順に選択します。

ステップ 2 グローバルサイトを選択した状態で、[Manage Credentials] をクリックし、変更するデバイスクレデンシャルのチェックボックスをオンにして、**[Actions]** > **[Actions]**を選択します。

ステップ 3 [Edit Credentials] ダイアログボックスで、変更を加えて、[Save] をクリックします。

（注） CLI パスワードログイン情報には、*ASCII* 印刷可能文字（文字コード 32 ー 127。https://en.wikipedia.org/wiki/ASCII#Printable_characters を参照）だけを使用できます。

ステップ 4 クレデンシャルタイルで、[Apply] をクリックします。

ステップ 5 [Apply Credentials] ダイアログボックスで、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールするかを選択します。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 後で更新をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックして更新の日時を定義し、[適用（Apply）] をクリックします。

（注） [タイム ゾーン（Time Zone）] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

ステータスメッセージに、デバイスログイン情報の変更が成功したか、失敗したかが示されます。

ステップ 6 クレデンシャル変更のステータスを表示するには、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[クレデンシャル ステータス（Credential Status）] 列に、次のいずれかのステータスが表示されます。

- [Success]：Cisco DNA Center はログイン情報の変更を正常に適用しました。
- [Failed]：Cisco DNA Center はログイン情報の変更を適用できませんでした。失敗したログイン情報の変更とその理由に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。
- [Not Applicable]：ログイン情報はデバイスタイプに適用できません。

複数のクレデンシャル（CLI、SNMP、HTTPS など）を編集して保存した場合、がいずれかのクレデンシャルを適用できなかったときには、[クレデンシャルステータス（Credential Status）] 列に [失敗（Failed）] と表示されます。Cisco DNA Center 失敗したログイン情報の変更に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。

デバイス クレデンシャルのサイトへの関連付け

グローバルサイトを作成するサイトは、グローバルなデバイスのクレデンシャルを継承できます。または特定サイトの別のデバイスのクレデンシャルを作成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**[Design]** > **[Network Settings]** > **[Device Credentials]**。

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 選択したサイトに関連付けるクレデンシャルを選択し、次に **[保存（Save）]** をクリックします。

デバイスのクレデンシャルとサイトとの関連付けが正常に成功したことを示すメッセージが、画面の下部に表示されます。

ステップ 4 **[リセット（Reset）]** をクリックして、画面上のエントリをクリアします。

IP アドレス プールを設定する

Cisco DNA Center IPv4 と IPv6 のデュアルスタック IP プールがサポートされています。

IPv4 および IPv6 アドレスプールは手動で設定できます。

Cisco DNA Center を外部 IP アドレス マネージャと通信するように設定することもできます。詳細については、Cisco DNA Center 管理者ガイド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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Add] をクリックし、[Add IP Pool] ウィンドウの必須入力フィールドをすべて入力します。

Cisco DNA Center が外部の IP アドレスマネージャと通信するように設定した場合、外部 IP アドレスマネージャの既存の IP アドレスプールと重複する IP プールを作成することはできません。

ステップ 3 **[Save]** をクリックします。

新しく追加されたプールが IP アドレスプールテーブルに表示されます。IPv4 または IPv6 のアドレスプールのみを表示する場合は、[SUBNET TYPE] 領域で [IPv4] または [IPv6] オプションをクリックします。

（注） IP アドレス プールを編集して、DHCP を変更すると、その IP アドレス プールを使用してデバイスを再設定する必要はありません。

IP アドレスマネージャから IP アドレスプールをインポートする

Bluecat または Infoblox から IP アドレスプールをインポートできます。

（注） IP アドレスプールはサブプールを持つことができず、IP アドレスプールから割り当てられた IP アドレスを持つことはできません。

外部 IP アドレスマネージャ（IPAM）と通信するには Cisco DNA Center を設定する必要があります。詳細については、Cisco DNA Center 管理者ガイド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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from IPAM Server] を選択し、必須フィールドに値を入力します。

ステップ 3 CIDR を入力し、**[Retrieve]** をクリックして、インポートできる IP プールのリストを取得します。

ステップ 4 [Select All] をクリックするか、またはインポートする IP アドレスプールを選択して [Import] をクリックします。

CSV ファイルから IP アドレスプールをインポートする

CSV ファイルから IP アドレスプールをインポートできます。

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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from CSV File] を選択します。

ステップ 3 [Download Template] をクリックして最新のサンプルファイルをダウンロードします。

ステップ 4 ファイルに IP アドレスプールを追加して、ファイルを保存します。

ステップ 5 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

a) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。

b) **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 6 **[インポート (Import)]** をクリックします。

IP プールの予約

始める前に

1 つまたは複数の IP アドレスプールが作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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [hierarchy] ペインを展開し、サイトを選択します。

ステップ 3 [Reserve] をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。LAN 自動化の場合は、**LAN** を選択します。次のオプションがあります。
  - [LAN]：該当する VNF とアンダーレイの LAN インターフェイスに IP アドレスを割り当てます。
  - [Management]：IP アドレスを管理インターフェイスに割り当てます。管理ネットワークは、VNF 管理用に VNF に接続される専用ネットワークです。
  - [Service]：IP アドレスをサービスインターフェイスに割り当てます。サービスネットワークは、VNF 内の通信に使用されます。
  - [WAN]：UCS-E プロビジョニングの場合は NFVIS に IP アドレスを割り当てます。
  - [Generic]：他のすべてのネットワークタイプで使用されます。
- [IP Address Space]：すべてまたは一部の IP アドレスを予約する IPv4 および IPv6 アドレスプール。
- **CIDR Prefix/Number of IP Addresses**：IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. IPv6 IP プールの [CIDR Prefix] として \64 を選択すると、[SLAAC] オプションがオンになります。（[SLAAC] が選択されている場合、デバイスは DHCP サーバーを必要とせずに、自動的に IP アドレスを獲得します）。
- [Gateway]：ゲートウェイ IP アドレス。
- [DHCP Servers]：DHCP サーバーの IP アドレス。
- [DNS Servers]：DNS サーバーのアドレス。

ステップ 4 [予約（Reserve）] をクリックします。

IPv4 と IPv6 の両方のアドレスプールを予約している場合（ファブリックがデュアルスタック IP プールでプロビジョニングされている場合）で、IPv6 プールがすでに VN に接続されているときは、シングルスタック IP プールに戻すことはできません。

ただし、IPv6 プールが VN に接続されていない場合は、デュアルスタック IPv6 プールからシングルスタック IPv4 プールにダウングレードできます。シングルスタックにダウングレードするには、[IP Address Pools] ウィンドウで、デュアルスタック IP プールの [Edit] をクリックします。[Edit IP Pool] ウィンドウで、[IPv6] チェックボックスをオフにして、[Save] をクリックします。

IP プールの編集

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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括で編集するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Edit All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

c) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

ステップ 4 目的の IP プールのみを編集するには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Edit Selected] をクリックします。

選択した IP プールに対応する [Edit] をクリックすることもできます。

b) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

IP プールの削除

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**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括で削除するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Delete All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

ステップ 4 目的の IP プールのみを削除するには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Delete Selected] をクリックします。

選択した IP プールに対応する [Delete] をクリックすることもできます。

b) [Warning] メッセージで [Yes] をクリックします。

IP プールの複製

サイトレベルで既存の IP プールを複製できます。IP プールを複製すると、DHCP サーバーと DNS サーバーの IP アドレスが自動的に入力されます。

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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 階層ツリーを展開し、サイトを選択します。

ステップ 3 目的の IP プールを見つけ、[Actions] 領域で [Clone] をクリックします。

ステップ 4 [Clone IP Pool] ウィンドウで、次の手順を実行します。

a) 必要に応じて、プール名を編集します（タイプ、IP アドレス空間、またはグローバルプール値は、複製元のプールから継承されるため編集できません）。

b) 必要に応じて、CIRD プレフィックス値を編集します。

c) [Clone] をクリックします。

IP プールのリリース

サイトレベルで予約されているシングルスタックおよびデュアルスタックプールをリリースできます。

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**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括でリリースするには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Release All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

c) プロンプトで [Release] をクリックします。

ステップ 4 目的の IP プールのみをリリースするには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Release Selected] をクリックします。

b) プロンプトで [Release] をクリックします。

IP アドレスプールの表示

この手順では、テーブルビューとツリービューで 10 個以上の IP アドレスプールを表示する方法を示します。

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**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 トグルボタンを使用して、テーブルビューとツリービューを切り替えます。

- IP プールが 10 個以上の場合は、デフォルトではテーブルビューにプールが表示されます。
- IP プールが 10 個未満の場合は、デフォルトではツリービューにプールが表示されます。

（注） テーブルマップビューとツリーマップビューの切り替えは、UI でのユーザーの選択ではなくプール数に基づきます。

ツリービューは、グローバルプールとサイトプールに適用されます。

ステップ 4 [IP Address Pools] テーブルビューには、[Name]、[Type]、[IPv4 Subnet]、[IPv4 Used]、[IPv6 Subnet]、[IPv6 Used]、および [Actions] に基づいてIP アドレスプールのリストが表示されます。

（注）
- [IPv4 Used] および [IPv6 Used] の横にある [i] アイコンにカーソルを合わせます。[IPv4 Used]、[IPv6 Used]、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールに関する詳細情報を示すツールチップが表示されます。
- [IPv4] 列と [IPv6] 列で、特定の IP アドレスプールに対応する [IPv4] と [IPv6] の使用率の横にある [i] アイコンにカーソルを合わせます。ツールチップには、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールの割合が表示されます。

ステップ 5 テーブルビューで [IPv4] または [Dual-Stack] のアドレスプールのみを表示する場合は、[Sbunet Type] エリアで [IPv4 only] または [Dual-Stack] オプションをクリックします。

ステップ 6 ツリービューで、目的の IP アドレスプールにカーソルを合わせてクリックすると、次の情報を含むスライドインペインが表示されます。

- IP アドレスプールのサブネットタイプ。
- それぞれのプール下にある使用可能な IP アドレスと [Pool CIDR]、[Gateway]、[DHCP Server(s)]、および [DNS Server(s)] の割合。
- 各プールで使用されている IP アドレスの割合。

ステップ 7 [Used] エリアで、[Assigned] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てられた IP アドレスのリストが表示されます。

ステップ 8 [Unassignable] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てることができない未割り当て IP アドレスのリストが表示されます。

ステップ 9 [Edit] をクリックして、IP アドレスプールを編集します。

ステップ 10 [Release] をクリックして、IP アドレスプールを解放します。

（注）
- グローバルプールのサイドバーでは、特定のプールについて、すべての子プールにおける使用状況を確認できます。
- グローバル IP アドレスプールとサイト IP アドレスプールには、ブロックリストに登録された IP アドレスを設定できます。
- サブプールにはブロックリストに登録された IP アドレスを含めることはできません。
  - Cisco DNA Center は、ブロックリストに登録された IP アドレスが含まれている場合、CIDR アドレスプールの IP アドレスプール作成要求を拒否します。
  - 次の空き IP アドレスプール要求では、Cisco DNA Center はブロックリストに登録された IP アドレスをスキップして、次の IP アドレス空きプールを見つけます。

ステップ 11 （オプション）テーブルデータをエクスポートするには、サイドバーで [Export] をクリックします。

サービス プロバイダ プロファイルの設定

特定の WAN プロバイダのサービス クラスを定義するサービス プロバイダ（SP）プロファイルを作成することができます。サービスモデルには、4 クラス、5 クラス、6 クラス、および 8 クラスを定義できます。SP プロファイルの作成後、アプリケーションポリシーの範囲内（必要に応じてインターフェイスのサブラインレート設定を含む）のアプリケーションポリシーと WAN インターフェイスにそのプロファイルを割り当てることができます。

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**[Design]** > **[Network Settings]** > **[SP Profiles]** の順に選択します。

ステップ 2 **[Qos]** 領域で、**[追加（Add）]** をクリックします。

ステップ 3 **[プロファイル名（Profile Name）]**フィールドに、SP プロファイルの名前を入力します。

ステップ 4 [WAN Provider] ドロップダウンリストから、新しいサービスプロバイダを入力するか、既存のプロバイダを選択します。

ステップ 5 [Model] ドロップダウンリストから、クラスモデル（[4 class]、[5 class]、[6 class]、および [8 class]）のいずれかを選択します。

これらのクラスの詳細については、サービス プロバイダのプロファイル（305 ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

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**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP サーバー（DHCP Server）]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS サーバー（DNS Server）]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

Cisco ISE またはその他の AAA サーバーの追加

Cisco Identity Services Engine（ISE）サーバーまたはその他の同様の AAA サーバーを、ネットワーク、クライアント、およびエンドポイント認証のためにサイトまたはグローバル レベルで定義することができます。ネットワーク認証では、RADIUS および TACACS プロトコルがサポートされています。クライアントとエンドポイント認証では、RADIUS のみがサポートされます。Cisco DNA Center あたり、1 つの Cisco ISE のみサポートされます。

マルチ ISE 設定をサポートするために、RADIUS または TACACS サーバーグループの下に送信元インターフェイスを設定できます。各 Cisco ISE ISE クラスタには独自のサーバーグループがあります。RADIUS サーバーと TACACS サーバーに使用される送信元インターフェイスは、次のように決定されます。

- デバイスに Loopback0 インターフェイスが設定されている場合、Loopback0 は送信元インターフェイスとして設定されます。

- それ以外の場合は、Cisco DNA Center を管理 IP として使用するインターフェイスが送信元インターフェイスとして設定されます。

あるサイトに Cisco ISEサーバーを設定すると、サイトに割り当てられているデバイスは、対応する Cisco ISE サーバーで、自動的に a /32 マスクに更新されます。その後、Cisco ISE でこれらのデバイスに変更が行われると、Cisco DNA Center に自動的に送信されます。

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**[Design]** > **[Network Settings]** > **[Network]**。

ステップ 2 [サーバーの追加（Add Servers）] をクリックして AAA サーバーを追加します。

ステップ 3 [サーバーの追加（Add Servers）] ウィンドウで、[AAA] チェック ボックスをオンにし、[OK] をクリックします。

ステップ 4 AAA サーバーをネットワークユーザー、クライアント/エンドポイントユーザー、またはその両方に設定します。

ステップ 5 [Network] または [Client/Endpoint] チェックボックスをオンにし、AAA サーバーのサーバーとプロトコルを設定します。

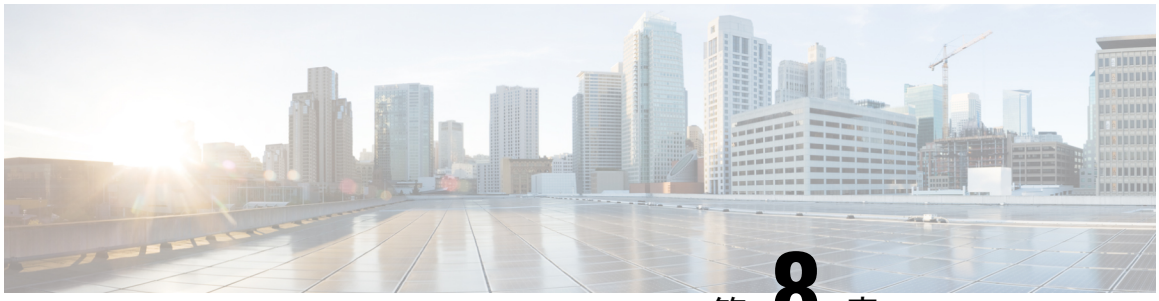
ステップ 6 認証と認可のための [Servers] を選択します（[ISE] または [AAA]）。

- [ISE] を選択した場合は、次のように設定します。
  - [ネットワーク] ドロップダウンリストから、Cisco ISE サーバーの IP アドレスを選択します。[Network] ドロップダウンリストには、Cisco DNA Center のホームページの [System Settings] に登録されている 、Cisco ISE サーバーのすべての IP アドレスが含まれています。Cisco ISE の IP を選択すると、選択した Cisco ISE のポリシーサービスノード（PSN）の IP アドレスを持つプライマリおよび追加 IP アドレスのドロップダウンリストが表示されます。AAA サーバーの IP アドレスを入力することも、[IP Address (Primary)] と [IP Address (Additional)] ドロップダウンリストから PSN IP アドレスを選択することもできます。
  - [Protocol] を選択します（[RADIUS] または [TACACS]）。

    （注） 特定の WLC の物理サイトと管理サイトの AAA 設定が一致する必要があります。一致しない場合、プロビジョニングは失敗します。

- [AAA] を選択した場合は、次のように設定します。
  - AAA サーバーの IP アドレスを入力することも、[IP Address（Primary] および [IP Address（Additional] ドロップダウンリストから IP アドレスを選択することもできます。これらのドロップダウンリストには、[System Settings] で登録されている Cisco ISE 以外の AAA サーバーが含まれています。

ステップ 7 [Save] をクリックします。



第 8 章

デバイスの診断コマンドを実行

コマンドランナーについて

コマンドランナー ツールでは、選択したデバイスに診断CLI コマンドを送信できます。現在、**show** とその他の読み取り専用コマンドが許可されています。

デバイスの診断コマンドを実行

コマンド ランナーを使用すると、選択したデバイスで診断 CLI コマンドを実行し、結果のコマンド出力を表示できます。コマンドランナーは、スタンドアロン端末の一部として使用可能なショートカットのサブセットのみをサポートします。

始める前に

コマンドランナーの使用を開始するには、次の手順を実行します。

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]** > **[Installed Apps]** の順に選択します。
2. [Command Runner] アプリケーションを検索し、[Install] をクリックします。
3. インストール後、ディスカバリ ジョブを実行し、デバイスに Cisco DNA Center を入力します。これらデバイスの一覧が表示され、ここから診断 CLI コマンドを実行します。

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**[Tools]** > **[Command Runner]** の順に選択します。

[コマンド ランナー（Command Runner）] ウィンドウが表示されます。

デバイスの診断コマンドを実行

ステップ 2 [Search] フィールドで、ドロップダウン矢印をクリックして、[Device IP] または [Device Name] で検索します。

ステップ 3 診断 CLI コマンドを実行するデバイス（複数可）を選択します。

選択した [デバイス一覧（Device List）] が表示されます。

ステップ 4 （任意） リストに追加する別のデバイスを選択します。到達可能なデバイスを 20 台まで選択できます。

（注） デバイス一覧にはインベントリで利用可能なデバイスがすべて表示されますが、コマンド ランナーはワイヤレス アクセス ポイント デバイスおよび Cisco Meraki デバイスではサポートされていません。アクセス ポイント デバイスまたは Cisco Meraki デバイスを選択すると、コマンドが実行されないという警告メッセージが表示されます。

ステップ 5 [Select/Enter commands] フィールドに CLI コマンドを入力し、[Add] をクリックします。

コマンドランナーでは、先行入力がサポートされています。入力を開始すると、選択可能なコマンドがコマンドランナーによって表示されます。新しい有効なコマンドを入力することもできます。

ステップ 6 [コマンドの実行（Run Command(s)）] をクリックします。

成功すると、「コマンドは正常に実行されました」 というメッセージが表示されます。

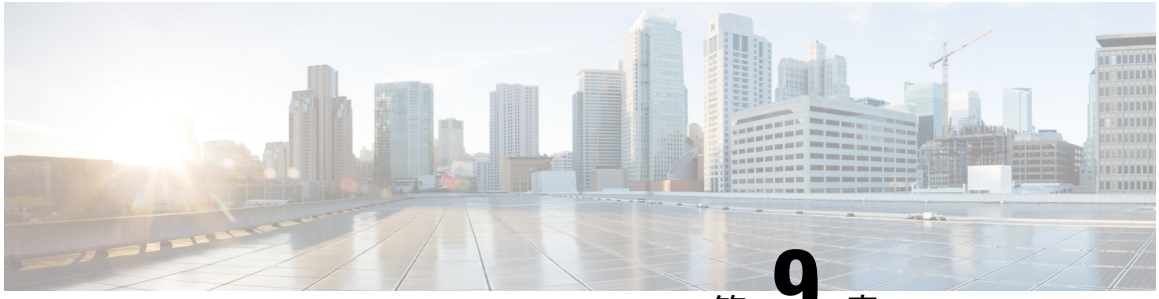
ステップ 7 コマンド出力を表示するには、デバイスの下に表示されているコマンドをクリックします。

（注） [Command Runner] ウィンドウにすべてのコマンド出力が表示されます。パスワードなどの機密情報は、コマンド出力でマスクされます。

ステップ 8 （任意） [Export all CLI Output] をクリックすると、コマンド出力をテキストファイルにエクスポートしてローカルに保存できます。

ステップ 9 [Go Back] をクリックすると前のウィンドウに戻ります。

（注） 必要に応じて、デバイス名の横にある [x] をクリックすると、デバイス一覧からデバイスが削除されます。同様に、コマンドの横にある [x] をクリックすると、コマンド一覧からコマンドが削除されます。



第 9 章

デバイス設定の変更を自動化するテンプレートの作成

テンプレート エディタについて

Cisco DNA Center Cisco DNA Center には、CLI テンプレートを作成するためのテンプレートエディタと呼ばれるインタラクティブなエディタがあります。パラメータ化された要素または変数を使用して、事前に定義された設定で簡単にテンプレートを設計できます。テンプレートを作成したら、そのテンプレートを再度使用して、ネットワーク内の任意の場所に設定されている 1 つ以上のサイトにデバイスを展開できます。

テンプレートエディタを使用すると、次のことができます。

- テンプレートの作成、編集、および削除
- インタラクティブ コマンドの追加
- テンプレート内のエラーの検証
- 追跡のためのテンプレートのバージョン管理
- テンプレートのシミュレーション

プロジェクトの作成

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、⊕ > **[プロジェクトの作成（Create Project)）]** の順にクリックします。

[Add New Project] スライドインペインが表示されます。

ステップ 3 [Name] フィールドに、プロジェクトの名前を入力します。

ステップ 4 （任意） [Description] フィールドに、プロジェクトの説明を入力します。

ステップ 5 [Add] をクリックします。

プロジェクトが作成され、左側のペインに表示されます。

テンプレートの作成

テンプレートは、パラメータ要素と変数を使用して構成を簡単に事前定義する方法を提供します。テンプレートにより、管理者は複数のネットワークデバイスを一貫して設定するのに使用する CLI コマンドの設定を定義できるようになり、展開時間を短縮できます。テンプレートの変数を使用すると、デバイスごとに特定の設定をカスタマイズできます。

標準テンプレートの作成

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**[Tools]** > **[Template Editor]** の順に選択します。

デフォルトでは、[Onboarding Configuration] プロジェクトは、day-0 テンプレートの作成に使用できます。独自のカスタムプロジェクトを作成できます。カスタムプロジェクトで作成されたテンプレートは、day-N テンプレートとして分類されます。

ステップ 2 左側のペインで、テンプレートを作成するプロジェクトを選択します。

ステップ 3 左側のペインで、歯車アイコン ⚙ > **[Add Templates]** の順にクリックします。

または、左側のペインで ⊕ > **[Add Templates]** をクリックします。

（注） day-0 用に作成したテンプレートは、day-N にも適用できます。

ステップ 4 [Add New Template] ウィンドウでは、デフォルトで [Regular Template] が選択されています。

ステップ 5 [Template Language] の選択で、[Velocity] または [Jinja] のいずれかのオプションボタンをクリックして、テンプレートの内容を作成するために使用する言語を選択します。

ステップ 6 [Name] フィールドにテンプレートの一意の名前を入力します。

ステップ 7 [Project Name] ドロップダウンリストからプロジェクトを選択します。

[Add Templates] パスから移動してきた場合、ドロップダウンリストが有効になっています。 >

プロジェクトを選択した後に左側のペインで歯車アイコン > **[Add Templates]** の順に選択した場合、ドロップダウンリストは無効になります。

ステップ 8 [Description] フィールドにテンプレートの説明を入力します。

ステップ 9 [Tags] ドロップダウンリストからテンプレートのタグ名を選択します。

タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

（注） タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に次のエラーが表示されます。「デバイスを選択できません。テンプレートとの互換性がありません（Cannot select the device. Not compatible with template.）」。

ステップ 10 [Edit] をクリックして、このテンプレートに適用するデバイスタイプを選択します。

[Select Device Type(s)] ウィンドウが表示されます。デフォルトでは、すべてのデバイスタイプが表示されます。

- [Find] 機能でデバイス名を入力してデバイスをすばやく検索するか、またはデバイスタイプを展開してからテンプレートに適用するデバイスタイプの横にあるチェックボックスをオンにします。

  選択済みのデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。

階層構造から選択するデバイスタイプには、さまざまな細かいレベルがあります。展開時にデバイスタイプを使用して、指定したデバイスタイプの条件に一致するデバイスをテンプレートが確実に展開できるようにします。これにより、特定のデバイスモデルに対して専用のテンプレートを作成できます。

テンプレートエディタには、デバイスの製品 ID（PID）は表示されません。代わりに、デバイスのシリーズとモデルの説明が表示されます。Cisco.com を使用すると、PID に基づいたデバイスデータシートの検索、デバイスシリーズとモデルの説明の検索、適切なデバイスタイプの選択を実行できます。

ステップ 11 デバイスタイプを選択したら、[Back to Add New Template] をクリックします。

ステップ 12 [Software Type] ドロップダウンリストから、ソフトウェアタイプとして、[IOS]、[IOS XE]、[IOS XR]、[NX-OS]、[Cisco Controller]、[Wide Area Application Services]、[Adaptive Security Appliance]、[NFV-OS]、[Others] を選択します。

シスコ ワイヤレス コントローラのサポート対象ソフトウェアバージョンおよびサポートされている最小バージョンの詳細については、「Cisco DNA Center Supported Devices」を参照してください。

たとえば、ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

ステップ 13 [Software Version] フィールドにソフトウェアのバージョンを入力します。プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されているのと同じソフトウェアバージョンがあるか確認します。不一致がある場合、プロビジョニングはテンプレートをスキップします。

ステップ 14 [Add]をクリックします。

テンプレートが作成され、左側のペインの選択したプロジェクトの下に表示されます。

ステップ 15 左側のペインで作成したテンプレートを選択して、テンプレートの内容を編集することができます。テンプレートの内容の編集の詳細については、テンプレートの編集 （215 ページ）を参照してください。

ブロックリストコマンド

ブロックリストコマンドは、ブロックリストカテゴリに追加されるコマンドです。これらのコマンドは、Cisco DNA Center アプリケーションを介してのみ使用できます。テンプレートでブラックリストコマンドを使用すると、テンプレートに警告が表示されます。この場合、一部の Cisco DNA Center プロビジョニング アプリケーションと競合している可能性があります。

このリリースでサポートされるブロックリストコマンドを次に示します。

- Router LISP は、Cisco Catalyst 1000 シリーズ スイッチ、Cisco Catalyst 3000 シリーズ スイッチ、Cisco Catalyst 4000 シリーズ スイッチ、および Cisco Catalyst 6000 シリーズ スイッチでサポートされます。
- Hostname は、Cisco サービス統合型仮想ルータ（ISRv）および Cisco 適応型セキュリティ仮想アプライアンス（ASAv）でサポートされます。

サンプル テンプレート

テンプレートの変数を作成する際は、次のサンプルテンプレートを参照してください。

ホスト名を設定します

```
hostname$name
```

インターフェイスの設定

```
interface $interfaceName
description $description
```

シスコ ワイヤレス コントローラでの NTP の設定

```
config time ntp interval $interval
```

複合テンプレートの作成

2つ以上の標準テンプレートは、連続した複合テンプレートにまとめられます。一連のテンプレートに対し、デバイスに集合的に適用される連続的な複合テンプレートを作成できます。たとえば、ブランチを展開するときに、ブランチルータの最小設定を指定する必要があります。作成したすべてのテンプレートは、単一の複合テンプレートに追加できます。これは、ブラン

チルータに必要なすべての個々のテンプレートを集約したものです。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。

（注） 複合テンプレートには、コミットされたテンプレートのみを追加できます。

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

ステップ 2 左側のペインで、テンプレートを作成するプロジェクトを選択します。

ステップ 3 左側のペインで、歯車アイコン ⚙ > **[Add Templates]** の順にクリックします。

[Add New Template] スライドインペインが表示されます。

ステップ 4 複合テンプレートの設定を指定します。

a) [Template Type] で、複合テンプレートの [Composite Sequence] を選択します。

b) [Template Language] については、テンプレートのコンテンツに使用する言語（[Velocity] または [Jinja]）を選択します。

c) [Name] フィールドにテンプレートの一意の名前を入力します。

d) （任意） [Description] フィールドにテンプレートの説明を入力します。

e) [Tags] フィールドで、ドロップダウンリストをクリックし、テンプレートのタグを選択します。

（注） タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に「Cannot select the device. Not compatible with template.」というエラーメッセージが表示されます。

f) [Device Type(s)] については、[Edit] をクリックし、このテンプレートを適用するデバイスタイプを選択します。

[Select Device Type(s)] スライドインペインが表示されます。デフォルトでは、すべてのデバイスタイプが表示されます。

（注）
- [Select Device Type(s)] スライドペインでは、[Full Device List] ビューと [Favorite Devices] ビューを切り替えることができます。
- [Full Device List] ビューでは、デバイスタイプ階層の各デバイスモデルがアルファベット順に並べ替えられます。

- [Find] 機能でデバイス名を入力してデバイスをすばやく検索するか、またはデバイスタイプを展開してからテンプレートに適用するデバイスタイプの横にあるチェックボックスをオンにします。

  選択済みのデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。

g) 階層で、デバイスタイプを展開し、お気に入りとしてマークするデバイスモデルの横に表示される星のマークをクリックします。

（注） [Favorite Devices] ビューに切り替えて、お気に入りのマークが付いたデバイスモデルのリストを表示することができます。

h) デバイスタイプを選択したら、[Back to Add New Template] をクリックします。

i) [Software Type] については、ドロップダウンリストをクリックし、ソフトウェアのタイプを選択します。

（注） ソフトウェアタイプに固有のコマンドがある場合は、特定のソフトウェアタイプ（IOS XE や IOS XR など）を選択できます。ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

j) [Software Version] フィールドにソフトウェアのバージョンを入力します。

（注） プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されているのと同様のソフトウェアバージョンがあるか確認します。不一致がある場合、プロビジョニングはテンプレートをスキップします。

ステップ 5 [Add]をクリックします。

複合テンプレートが作成され、左側のペインの選択したプロジェクトの下に表示されます。

ステップ 6 左側のビューペインで作成した複合テンプレートをクリックします。

ステップ 7 [Template Editor] ウィンドウで、左側のペインからテンプレートを順番にドラッグアンドドロップします。

テンプレートは順序付けされた順序に基づいて導入されます。[テンプレートエディタ（Template Editor）] ウィンドウでテンプレートの順序を変更できます。

（注） デフォルトでは、[View] フィルタで [Applicable] オプションが選択されています。複合テンプレートに追加できる適用可能なテンプレートのみが [Template Editor] ウィンドウに表示されます。[View] フィルタで [All] オプションを選択すると、[Template Editor] ウィンドウにすべてのテンプレートを表示できます。[All] オプションビューでは、選択したデバイスタイプとソフトウェアバージョンに一致するテンプレートがプラスアイコンでマークされます。

複合テンプレートと同じデバイスタイプ、ソフトウェアタイプ、およびソフトウェアバージョンを持つテンプレートをドラッグアンドドロップできます。

ステップ 8 最初のテンプレートで障害が発生した場合に展開プロセスをキャンセルするには、[Template Editor] ウィンドウで最初のテンプレートを選択し、[Abort sequence on targets if deployment fails] チェックボックスをオンにします。

ステップ 9 **[Actions]** ドロップダウンリストで、**[Commit]** を選択してテンプレートのコンテンツをコミットします。

テンプレートの編集

テンプレートを作成したら、テンプレートを編集して内容を記述できます。

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**[Tools]** > **[Template Editor]** の順に選択します。

ステップ 2 左側のペインで、編集するテンプレートを選択します。

[Template Editor] ウィンドウが表示されます。

ステップ 3 [テンプレート エディタ（Template Editor）] ウィンドウで、テンプレートのコンテンツを入力します。単一行設定または複数選択設定を含むテンプレートを使用できます。

ステップ 4 [Template Language] から、内容の記述に使用する言語を選択します。

- [Velocity]：Velocity Template Language（VTL）を使用します。詳細については、http://velocity.apache.org/engine/devel/vtl-reference.htmlを参照してください。

  Velocity テンプレートフレームワークでは、数字で始まる変数の使用が制限されます。変数名の先頭は数字ではなく文字にしてください。

  （注） Velocity テンプレートの使用中は、ドル記号（$）を使用しないでください。ドル記号（$）を使用すると、その後ろの値は変数として扱われます。たとえば、パスワードを「$a123$q1ups1$va112」として設定すると、テンプレートエディタはこれを変数「a123」、「q1ups」、および「va112」として扱います。この問題を回避するために、Velocity テンプレートによるテキスト処理に合わせて Linux シェルスタイルを使用してください。

  （注） Velocity テンプレートでは、変数を宣言する場合にのみドル（$）記号を使用してください。

- [Jinja]：Jinja 言語を使用します。詳細については、https://www.palletsprojects.com/p/jinja/を参照してください。

ステップ 5 [Actions] ドロップダウンリストから [Check for errors] を選択してテンプレートを検証します。

Cisco DNA Center 次のエラーをチェックし、報告します。

- 言語構文エラー。
- ブラックリストコマンドとの競合。詳細については、ブロックリストコマンドを参照してください。

ステップ 6 [Actions] ドロップダウンリストから、[Save] を選択します。

テンプレートを保存後、Cisco DNA Center がテンプレート内のすべてのエラーをチェックします。構文エラーがある場合、テンプレートの内容は保存されず、テンプレートで定義されているすべての入力変数が保存プロセス中に自動的に識別されます。ローカルの値（ループ用に使用され、セットを通じて割り当てられる変数など）は無視されます。

ステップ 7 [Actions] ドロップダウンリストから、[Commit] を選択します。

（注） ネットワーク プロファイルにコミットされたテンプレートのみを関連付けることができます。

テンプレートのシミュレーション

インタラクティブ テンプレート シミュレーションを使用すると、変数にテストデータを指定することで、変数をデバイスに送信する前に、テンプレートのCLI生成をシミュレーションすることができます。テストシミュレーションの結果を保存し、必要に応じてそれらを後で使用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 >

ステップ 2 左側のペインで、編集するテンプレートを選択します。

[Template Editor] ウィンドウが表示されます。

ステップ 3 右上隅にある [Simulator Editor] アイコンをクリックし、コマンドのシミュレーションを実行します。

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

[Simulation Input] フォームが表示されます。

ステップ 5 [Simulation Name name] フィールドにシミュレーションの名前を入力します。

（注） テンプレートに暗黙的な変数がある場合、[edit] リンクをクリックし、[Simulation Input] フォームでデバイスまたはサイトを選択して、バインディングに基づいて実際のデバイスに対してシミュレーションを実行できます。

ステップ 6 [シミュレーション入力（Simulation Input）] フォームの必須フィールドを入力し、[実行（Run）] をクリックします。

結果は、[テンプレート プレビュー（Template Preview）] ウィンドウに表示されます。

テンプレートのエクスポート

テンプレートまたは複数のテンプレートを JSON フォーマットで 1 つのファイルにエクスポートできます。

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、エクスポートするテンプレートを選択します。[Export] を選択します。⚙ >

- 1 つのプロジェクトの下に複数のテンプレートをエクスポートするには、左側のペインでプロジェクトを選択し、⚙ > **の [Export Template (s)] を選択します。**

[Export Template(s)] ウィンドウからテンプレートを選択し、[Export] をクリックします。

- 異なるプロジェクトの下に複数のテンプレートをエクスポートするには、左側のペインで の [Export Project(s)] をクリックします。

  [Export Project(s)] ウィンドウからエクスポートするテンプレートを選択し、[Export] をクリックします。

ステップ 3 プロンプトが表示されたら、[Save] をクリックします。

テンプレートの最新バージョンがエクスポートされます。

テンプレートの以前のバージョンをエクスポートするには、[Actions] > [Show History] > [View] からテンプレートを開きます。

[Actions] > [Export] の順にクリックします。

テンプレートのインポート

プロジェクトの下に 1 つまたは複数のテンプレートをインポートできます。

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、テンプレートをインポートするプロジェクトを選択します。 の [Import Template(s)] を選択します。 >

ステップ 3 [Import Template(s)] ウィンドウで [Select a File from your computer] をクリックし、JSON テンプレートファイルの場所を参照します。

ステップ 4 JSON ファイルを選択し、[Open] をクリックします。

テンプレートは、選択したプロジェクトの下にインポートされます。同じ名前のテンプレートが存在する場合、Cisco DNA Center はエラーメッセージを表示し、テンプレートをインポートしません。

（注） 既存のものと同じ名前のテンプレートをインポートするには、[Import Template(s)] ウィンドウの [Create new version of imported template/project when template/project with the same name already exists in the hierarchy] チェックボックスをオンにします。

このオプションを選択すると、既存のテンプレートの新しいバージョンが作成されます。

テンプレートの複製

テンプレートのコピーを作成して、その一部を再利用することができます。

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、エクスポートするテンプレートを選択します。[複製（Clone）]⚙ > を選択します。

ステップ 3 [Clone template] ウィンドウの [Name] フィールドに、複製されたテンプレートの名前を入力します。

ステップ 4 [Project Name] ドロップダウンリストからプロジェクトを選択します。

ステップ 5 [Clone] をクリックします。

ステップ 6 複製されたテンプレートを確定するには、ウィンドウの左ペインからテンプレートを選択し、[Actions] > [Commit] をクリックします。

テンプレートの最新バージョンが複製されます。

テンプレートの以前のバージョンを複製するには、[Actions] > [Show History] > [View] からテンプレートを開きます。

[Actions] > [Clone] をクリックします。

プロジェクトのエクスポート

プロジェクトまたは複数のプロジェクト (テンプレートを含む) を JSON フォーマットの 1 つのファイルにエクスポートできます。

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、エクスポートするプロジェクトを選択します。の [Export Project] を選択します。⚙ >

プロジェクトを一括してエクスポートするには、左側のペインで⊕ > **の [Export Project (s)] をクリックします。**

エクスポートするプロジェクトを選択し、[Export] をクリックします。

ステップ 3 プロンプトが表示されたら、[Save] をクリックします。

プロジェクトのインポート

テンプレートを使用して、1 つまたは複数のプロジェクトを Cisco DNA Center テンプレートエディタにインポートできます。

ステップ 1 [Tools] > [Template Editor]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > を選択します。

ステップ 2 左側のペインで、[Import Project(s)] > をクリックします。

ステップ 3 [Import Project(s)] ウィンドウで [Select a File from your computer] をクリックし、JSON プロジェクトファイルの場所を参照します。

ステップ 4 JSON ファイルを選択し、[Open] をクリックします。

プロジェクトとそのテンプレートがインポートされます。同じ名前のプロジェクトが存在する場合、Cisco DNA Center はエラーメッセージを表示し、プロジェクトをインポートしません。

（注） 既存のものと同じ名前のプロジェクトをインポートするには、[Import project(s)] ウィンドウの [Create new version of imported template/project when template/project with the same name already exists in the hierarchy] チェックボックスをオンにします。

このオプションを選択すると、既存のプロジェクトの新しいバージョンが作成されます。

テンプレート フォーム エディタ

テンプレート フォーム エディタは、追加のメタデータ情報をテンプレート内のテンプレート変数に追加するために使用します。またフォームエディタを使用して、最大長や範囲などの変数の検証を提供することもできます。

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**[Tools]** > **[Template Editor]** の順に選択します。

ステップ 2 左側のペインで、プロジェクトを展開し、テンプレートをクリックします。

テンプレートが表示されます。

ステップ 3 [Form Editor] トグル  をクリックします。

フォームエディタでは、テンプレート変数にメタデータを追加できます。テンプレートで識別されたすべての変数が表示されます。以下のメタデータを設定できます。

- 文字列を変数として考慮しない場合は、変数を選択し、[Not a Variable] チェックボックスをオンにします。
- [Field Name] テキストボックスに、フィールド名を入力します。これは、プロビジョニング中に各変数の UI ウィジェットに使用されるラベルです。
- [ツールチップ（Tooltip）] テキスト ボックスに、各変数に表示されるツールチップのテキストを入力します。
- [デフォルト値（Default Value）] テキスト ボックスに、デフォルト値を入力します。この値は、プロビジョニング中にデフォルト値として表示されます。
- [説明文（Instructional Text）] テキスト ボックスに、任意の説明文を入力します。説明文は UI ウィジェット内に表示されます（たとえば、**「ここにホスト名を入力してください」**など）。ユーザーが

テキストを入力するためにウィジェットをクリックすると、ウィジェット内のテキストは消去されます。

- [データタイプ（Data Type）] ドロップダウンリストから、データタイプ：[文字列（String）]、[整数（Integer）]、[IP アドレス（IP Address）]、または [MAC アドレス（Mac Address）] を選択します。
- これがプロビジョニング中に必要な変数の場合、[必須（Required）] チェック ボックスにチェックを付けます。デフォルトでは、すべての変数に [必須（Required）] マークが付いています。これはつまり、プロビジョニング時にこの変数の値を入力する必要があることを意味します。パラメータに [Required] マークがなく、このパラメータに何も値を渡さない場合は、実行時に空の文字列に置換されます。変数の不足は、コマンドの失敗につながります。また、構文上正しくない可能性があります。[Required] マークが付いていない変数に基づいてコマンド全体をオプションにしたい場合は、テンプレートで **if-else** ブロックを使用します。
- [表示タイプ（Display Type）] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプ：[テキスト フィールド（Text Field）]、[単一選択（Single Select）]、または [複数選択 （Multi Select）] を選択します。
- [最大文字数 （Maximum Characters）] テキスト ボックスに、入力できる最大文字数を入力します。これは文字列データタイプの場合にのみ適用可能です。

ステップ 4 メタデータ情報を設定したら、[Actions] ドロップダウンリストから [Save] を選択します。

ステップ 5 テンプレートを保存したら、バージョンを付ける必要があります。テンプレートは、変更を加えるたびにバージョンを付ける必要があります。[Actions] ドロップダウンリストから、[Commit] を選択します。[コミット（Commit）] ウィンドウが表示されます。[コミット メモ（Commit Note）] テキスト ボックスに、コミットのメモを入力することができます。バージョン番号はシステムによって自動的に生成されます。

ステップ 6 履歴を表示するには、[アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。以前作成してバージョンを付けたテンプレートが表示されます。

ポップアップウィンドウが表示されます。

- 古いバージョンのコンテンツを表示するには、ポップアップ ウィンドウの [表示（View）] をクリックします。
- テンプレートを編集するには、ポップアップ ウィンドウの [編集（Edit）] をクリックします。

変数バインド

テンプレートを作成する場合、コンテキストに合わせて置き換わる変数を指定できます。これらの変数の多くは、[Template Editor] ドロップダウンリストで使用できます。

テンプレートエディタには、編集中または入力フォーム機能拡張（DHCP サーバー、DNS サーバー、syslog サーバーなど）から、ソースオブジェクト値を使用してテンプレートで変数をバインドまたは使用するオプションがあります。

一部の変数については、対応するソースに常にバインドされ、動作を変更することはできません。[Code Editor] または [Form Editor] ウィンドウでテンプレートの名前の横にある ⓘ アイコンをクリックすると、暗黙の変数のリストを表示できます。

事前定義済みのオブジェクト値は、次のいずれかにすることができます。

- インベントリ
  - デバイス オブジェクト
  - インターフェイス オブジェクト
- [Common Settings]：**[Design]** > **[Network Settings]** > **[Network]** で利用可能な設定。共通設定の変数バインドによって、デバイスが属するサイトに基づいた値が解決されます。

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**[Tools]** > **[Template Editor]** の順に選択します。

ステップ 2 テンプレートを選択し、[Input Form] アイコンをクリックして、テンプレート内の変数をネットワーク設定にバインドします。

ステップ 3 変数をネットワーク設定にバインドするには、[Input Form] ペインで変数を選択し、[Required] チェックボックスをオンにします。

ステップ 4 [Display] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプを選択します。[Text Field]、[Single Select]、または [Multi Select]。

ステップ 5 変数をネットワーク設定にバインドするには、[Input Form] で各変数を選択し、[Content] の下の [Bind to Source] チェックボックスをオンにします。

- それぞれのドロップダウンリストで、[Source]、[Entity]、および [Attributes] を選択します。
- ソースタイプが [CommonSettings] の場合は、次のエンティティのいずれかを選択します。[dhcp.server]、[syslog.server]、[snmp.trap.receiver]、[ntp.server]、[timezone.site]、[device.banner]、[dns.server]、[netflow.collector]。

  [dns.server] または [netflow.collector] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。
- ソースタイプが [NetworkProfile] の場合、エンティティタイプとして [SSID] を選択します。入力される SSID エンティティは、[Design] > [Network Profile] で定義されます。 > バインドにより、SSID 名、サイト、および SSID カテゴリの組み合わせであるわかりやすい SSID 名が生成されます。[Attributes] ドロップダウンリストから、[wlanid] を選択します。この属性は、テンプレートのプロビジョニング時の高度な CLI 設定中に使用されます。
- ソースタイプが [Inventory] の場合、次のいずれかのエンティティを選択します。[Device]、[Interface]、[AP Group]、[Flex Group]、[Wlan]、[Policy Profile]、[Flex Profile]。エンティティタイプ [Device] および [Interface] の場合、[Attribute] ドロップダウンリストにデバイスまたはインターフェイスの属性が表示されます。変数は、テンプレートを適用するデバイスで設定されている AP グループと Flex グループの名前を解決します。

[Device]、[Interface]、または [Wlan] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。

変数を共通設定にバインドしたら、テンプレートをワイヤレスプロファイルに割り当て、テンプレートをプロビジョニングするときに、**[Network Settings]** > **[Network]** の下で定義したすべてのネットワーク設定がドロップダウンリストに表示されます。これらの属性は、ネットワークの設計時に **[Network Settings]** > **[Network]** の下で定義する必要があります。

特別なキーワード

テンプレートを通じて実行されるすべてのコマンドは、常に **config t** モードになります。そのため、テンプレートで明示的に **enable or config t** コマンドを指定する必要はありません。

Day-0 テンプレートは特別なキーワードをサポートしていません。

イネーブル モード コマンド

config t コマンドの他に任意のコマンドを実行する場合は、**#MODE_ENABLE** コマンドを指定します。

次の構文を使用して、CLI テンプレートに **enable mode** コマンドを追加します。

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

インタラクティブコマンド

ユーザー入力が必要なコマンドを実行する場合は、**#INTERACTIVE** を指定します。

インタラクティブコマンドには、コマンドの実行後に入力する必要がある入力が含まれています。[CLI Content] 領域にインタラクティブ コマンドを入力するには、次の構文を使用します。

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question
2<R>command response 2
```

ここで、**<IQ>** および **<R>** タグは、デバイスに表示される内容に対して提供されるテキストを評価します。

インタラクティブな質問では、正規表現を使用して、デバイスから受け取ったテキストが入力されたテキストと類似しているかどうかを検証します。**<IQ><R>** タグに入力された正規表現が見つかった場合は、インタラクティブな質問が検証を通過し、出力テキストの一部が表示されます。つまり、質問の一部を入力する必要がありますが、質問全体を入力する必要はありません。**<IQ>**と **<R>** タグの間に「Yes」または「No」を入力するだけで十分ですが、デバイスからの質問の出力に「Yes」または「No」のテキストが表示されていることを確認する必要があります。これを行う最善の方法は、デバイスでコマンドを実行し、出力を確認することです。さらに、入力された正規表現のメタ文字または改行が適切に使用されるか、完全に回避さ

れることを確認する必要があります。一般的な正規表現のメタ文字は **です。( ) [ ] { } |* + ? \ $ ^: &**。

たとえば、次のコマンドには、メタ文字と改行を含む出力があります。

```
Switch(config)# no crypto pki trustpoint DNAC-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
 Certificate Authority
Are you sure you want to do this? [yes/no]:
```

テンプレートにこれを入力するには、メタ文字または改行がない部分を選択する必要があります。ここでは、使用可能なものの例をいくつか紹介します。

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

ここで、**<IQ>** タグおよび **<R>** タグは大文字と小文字を区別し、大文字で入力する必要があります。

（注） 応答後にインタラクティブな質問に対応するとき、改行文字が必要ない場合は **<SF>** タグを入力する必要があります。**<SF>** タグの前にスペースを 1 つ含めます。**<SF>** タグを入力すると、**</SF>** タグが自動的にポップアップ表示されます。**</SF >** タグは不要なため削除できます。

次に例を示します。

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

インタラクティブ イネーブル モード コマンドの組み合わせ

次の構文を使用して、インタラクティブな **Enable Mode** コマンドを結合します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#ENDS_END_ENABLE
```

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

複数行コマンド

CLI テンプレートで複数行をラップする場合は、**MLTCMD** タグを使用します。そうしなければ、コマンドは 1 行ずつデバイスに送信されます。[CLI Content] 領域にマルチライン コマンドを入力するには、次の構文を使用します。

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- ここで、**<MLTCMD>** および **</MLTCMD>** は大文字と小文字を区別し、大文字で入力する必要があります。
- 複数行のコマンドは、**<MLTCMD>** タグと **</MLTCMD>** タグの間に挿入する必要があります。
- タグをスペースで開始することはできません。
- 1 行に **<MLTCMD>** タグと **</MLTCMD>** タグを使用することはできません。

テンプレートのネットワークプロファイルへの関連付け

始める前に

テンプレートをプロビジョニングする前に、テンプレートがネットワークプロファイルに関連付けられており、そのプロファイルがサイトに割り当てられていることを確認してください。

プロビジョニング中にデバイスが特定のサイトに割り当てられると、ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

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**[Design]** > **[Network Profiles]** の順に選択し、[Add Profile] をクリックします。

次のタイプのプロファイルを使用できます。

- [Firewall]：ファイアウォール プロファイルの作成時にこれを選択します。
- [NFVIS]：NFV プロファイルの作成時にこれを選択します。
- [Routing]：ルーティングプロファイルの作成時にこれを選択します。
- [Switching]：スイッチングプロファイルの作成時にこれを選択します。
    - 必要に応じて、[Onboarding Templates] または [Day-N Templates] をクリックします。

- **プロファイル名**を入力します。
- [+Add Template] をクリックして、[Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、およびテンプレートを選択します。

  必要なテンプレートが見つからない場合は、テンプレートエディタで新しいテンプレートを作成できます。標準テンプレートの作成 （210 ページ）を参照してください。
- [**保存（Save）**] をクリックします。

- [Telemetry Appliance]：Cisco DNA トラフィック テレメトリ アプライアンス プロファイルの作成時にこれをクリックします。
- [Wireless]：ワイヤレスプロファイルの作成時にこれをクリックします。ワイヤレス ネットワーク プロファイルを割り当てる前に、ワイヤレス SSID が作成されていることを確認してください。
  - **プロファイル名**を入力します。
  - [+ SSIDの追加（+ Add SSID）] をクリックします。**[Network Settings]** > **[Wireless]** の下で作成されたこれらの SSID が追加されます。
  - [Attach Template(s)] で、[Template] ドロップダウンリストからプロビジョニングするテンプレートを選択します。
  - **[Save]** をクリックします。

（注） スイッチングプロファイルとワイヤレスプロファイルは、[Cards] ビューおよび [Table] ビューで表示できます。

ステップ 2 [ネットワーク プロファイル（Network Profiles）] ページには、次のリストが表示されます。

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- [Sites]：[Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 3 Day-N プロビジョニングの場合は、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

a) プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。
b) [Actions] ドロップダウンリストから、[Provision] を選択します。
c) [サイトの割り当て（Assign Site）] ウィンドウで、プロファイルが添付されたサイトを割り当てます。
d) [Choose a Site] フィールドで、コントローラと関連付けるサイトの名前を入力するか、[Choose a Site] ドロップダウンリストから選択します。
e) **[次へ (Next)]** をクリックします。
f) [設定（Configuration）] ウィンドウが表示されます。[管理対象 AP ロケーション（Managed AP Locations）] フィールドで、このコントローラによって管理される AP の場所を入力します。サイトの変更、削除、または再割り当てができます。これはワイヤレスプロファイルにのみ適用可能です。
g) [Next] をクリックします。

h) **[Advanced Configuration（詳細設定）]** ウィンドウが表示されます。ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

- テンプレート内のインテントからの構成を上書きして、変更を上書きする場合は、[Provision these templates even if they have been deployed before] チェックボックスをオンにします（このオプションは、デフォルトで無効です）。
- [Copy running config to startup config] オプションはデフォルトで有効になっています。つまり、テンプレート構成を展開した後、write mem が適用されます。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適用しない場合は、このチェック ボックスをオフにする必要があります。
- [Find] 機能を使用し、デバイス名を入力してすばやくデバイスを検索するか、左側のペインでテンプレートフォルダを展開してテンプレートを選択します。右側のペインで、送信元にバインドされている属性の値を選択します。
- テンプレートを導入する間にテンプレートの変数を CSV ファイルにエクスポートするには、右側のペインで [エクスポート（Export）] をクリックします。CSV ファイルを使用して変数設定に必要な変更を加え、右側のペインで [Import] をクリックすると、後でそれを Cisco DNA Center にインポートできます。

i) [次へ（Next）] をクリックしてテンプレートを導入します。

j) テンプレートを今すぐ展開する場合は [Now] を選択します。または、後で展開するようにスケジュールすることを選択します。
展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

ステップ 4 [Export Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をエクスポートします。

ステップ 5 [Import Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をインポートします。

ステップ 6 Day-0 プロビジョニングの場合は、**[Provision]** > **[Network Devices]** > **[Plug and Play]** の順に選択します。

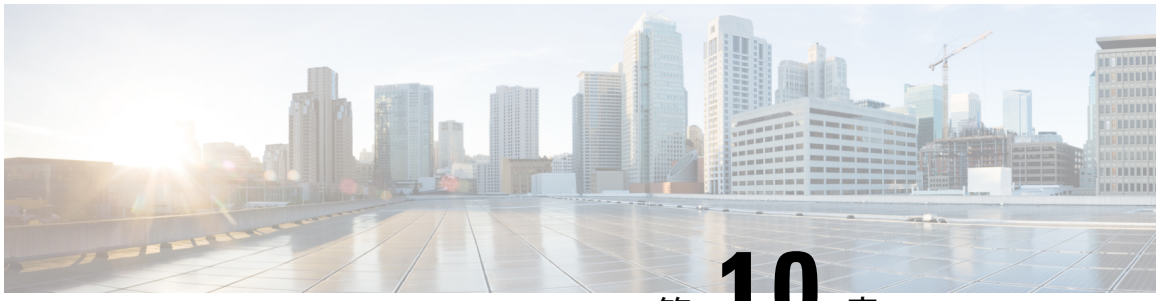
a) デバイスを選択し、[Actions] ドロップダウンリストから [Claim] をクリックします。

b) [Next] をクリックし、[Site Assignment] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

c) [Next] をクリックし、[Configuration] ウィンドウで、イメージと Day-0 テンプレートを選択します。

d) [Next] をクリックし、[Advanced Configuration] ウィンドウで場所を入力します。

e) [Next] をクリックして、[Device Details]、[Image Details]、[Day-0 Configuration Preview]、および [Template CLI Preview] を表示します。



第 10 章

設計モデルの設定

モデル設定エディタの概要

モデル設定では、プロビジョニングするアプリケーションにカプセル化される Cisco Validated Design（CVD）の高度なカスタマイズを定義できます。モデル設定は、高レベルのサービスインテントとデバイス固有の CLI テンプレートとともにネットワークデバイスに展開できる、モデルベースの検出可能かつカスタマイズ可能な構成機能のセットです。

モデル設定機能は、複雑なデバイス構成を抽象化し、デバイス固有の CLI の代わりに直感的な GUI を使用してカスタマイズ可能なネットワーク構成を容易にすることにより、ネットワークのプロビジョニングを簡素化します。共通の設計は、統一された方法で、さまざまなデバイスハードウェア プラットフォームとソフトウェアタイプに展開されます。展開時に、Cisco DNA Center インフラストラクチャは、抽出された設計を自動的に検証してデバイス固有の CLI コマンドに変換します。

モデル設定設計をプロビジョニングするには、次の手順を実行します。

1. [Model Config Editor] ウィンドウ（[Menu] アイコン（☰）から **[Tools]** > **[Model Config Editor]** の順に選択）を使用して、新しいモデル設定設計を作成します。
2. モデル設定設計をさまざまなネットワークプロファイルに適用します。
3. プロビジョニング ワークフローを使用して、ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスに適用します。

サポートされているモデル設定設計タイプ

Cisco DNA Center では、次のタイプのワイヤレスモデル設定設計がサポートされています。

- AAA RADIUS 属性
- 高度な SSID 構成
- CleanAir 構成
- Dot11ax 構成
- グローバル IPv6 構成
- マルチキャストの設定

AAA RADIUS 属性のモデル設定設計の作成

Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの **Called-station-id** パラメータ値を定義するには、「**AAA RADIUS 属性設定**」モデル設定を使用します。

「**Default AAA_Radius_Attributes_Configuration**」により、called-station ID が **ap-macaddress-ssid** として定義されます。このデフォルトのモデル設定は編集または削除できません。ただし、特定のネットワーク設計用にカスタムモデル設定を作成することができます。

この手順では、新しい**AAA RADIUS 属性設定**モデル設定を作成する方法について説明します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [AAA Radius Attributes Configuration] を選択します。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

[Add Called-station-id] スライドインペインが表示されます。

ステップ 4 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 5 [Called-station-id] ドロップダウンリストから、次の属性値のいずれかを選択します。

- **ap-ethmac-only**
- **ap-ethmac-ssid**
- **ap-group-name**

- **ap-label-address**
- **ap-label-address-ssid**
- **ap-location**
- **ap-macaddress**
- **ap-macaddress-ssid**
- **ap-name**
- **ap-name-ssid**
- **ipaddress**
- **macaddress**
- **vlan-id**

ステップ 6 [保存（**Save**）] をクリックします。

[Design Instances] ウィンドウに新しい設計インスタンスが表示されます。

ステップ 7 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 8 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成 （181 ページ）を参照してください。

ステップ 9 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）またはCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （429 ページ）を参照してください。

高度な SSID のモデル設定設計の作成

SSID は、WLAN に基づいてインターフェイスまたはインターフェイスグループに関連付けられます。WLAN で、セキュリティ、Quality of Service（QoS）、無線ポリシーなど、ワイヤレスネットワークのパラメータが設定されます。ワイヤレスコントローラごとに最大 512 個の WLAN を設定できます。

デバイスの高度なサービスセット識別子（SSID）パラメータの設定には、高度な SSID モデル設定を使用します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Advanced SSID Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Advanced SSID Design] チェックボックスをオンにして、デフォルトの拡張 SSID 設計を使用します。

（注） デフォルトの高度な SSID 設計を編集または削除することはできません。

ステップ 4 [Design Instances] ペインで [Add Design] をクリックします。

[Add Advanced SSID Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 6 [General] タブで、[Peer-to-Peer Blocking] ドロップダウンリストをクリックして、ピアツーピアブロッキングのオプションを選択します。

ピアツーピアブロッキングは、個々の WLAN に適用されます。クライアントは、それぞれが関連付けられている WLAN からピアツーピアブロッキング設定を継承します。ピアツーピアブロッキングを使用すると、トラフィックの転送方法を細かく制御できます。

- [DISABLE]：ピアツーピアブロッキングを無効にし、可能な場合はワイヤレスコントローラ内においてローカルでトラフィックを転送し ます。
- [DROP]：ワイヤレスコントローラでクライアントパケットを破棄します。
- [FORWARD UP]：クライアントパケットをアップストリームの VLAN に転送します。これらのパケットに対して行われる動作は、ワイヤレスコントローラよりも上流にあるデバイスにより決定されます。このデバイスは、ルータまたはレイヤ 3 スイッチのいずれかになります。
- [ALLOW PVT GROUP]：事前共有キー（PSK）クライアントにのみ適用されます。送信元と宛先のクライアントデバイスに関連付けられている Identity PSK（IPSK）タグに基づいてトラフィックが転送されます。

ステップ 7 パッシブクライアント機能を有効にするには、[Passive Client Enable] トグルボタンをクリックします。

パッシブクライアントとは、固定 IP アドレスが設定されている、スケールやプリンタなどのワイヤレスデバイスです。これらのクライアントは、アクセスポイントとの関連付けの際に IP 情報（IP アドレス、サブネットマスク、ゲートウェイ情報など）を送信しません。その結果、パッシブクライアントが使用された場合、それらのクライアントが DHCP を使用しない限り、ワイヤレスコントローラではその IP アドレスは認識されません。

ステップ 8 WLAN の経由ローミング予測リストを設定するには、[Assisted Roaming Prediction Optimization] トグルボタンをクリックします。

ステップ 9 デュアル無線バンドのネイバーリストを設定するには、[Neighbor List Dual Band] トグルボタンをクリックします。

ステップ 10 WLAN で SNMP NAC サポートを有効にするには、[Network Admission Control (NAC-SNMP)] トグルボタンをクリックします。

ステップ 11 WLAN で RADIUS NAC サポートを有効にするには、[Network Admission Control (NAC-Radius)] トグルボタンをクリックします。

ステップ 12 [DHCP Required] ドロップダウンリストで、RUN 状態（クライアントからのトラフィックがワイヤレスコントローラを通過できる状態）になるために DHCP 要求が必要かどうかに応じて、[Yes] または [No] のいずれかを選択します。

ステップ 13 [DHCP Server] を展開し、[IP Address] フィールドに DHCP サーバーの IP アドレスを入力します。

ステップ 14 FlexConnect ローカル認証を有効にするには、[FlexConnect Local Authentication] トグルボタンをクリックします。

ステップ 15 [NAS ID] フィールドにネットワークアクセスサーバー識別子を入力します。

ステップ 16 [Client Data Rates] をクリックし、次の各フィールドに値を入力して、クライアントごとにクライアントデータレート制限を設定します。

- Average Downstream Data Rate Per Client (kbps)
- Burst Downstream Data Rate Per Client (kbps)
- Average Downstream Real-Time Rate Per Client (kbps)
- Burst Downstream Real-Time Rate Per Client (kbps)
- Average Upstream Data Rate Per Client (kbps)
- Burst Upstream Data Rate Per Client (kbps)
- Average Upstream Real-Time Rate Per Client (kbps)
- Burst Upstream Real-Time Rate Per Client (kbps)

ステップ 17 [SSID Data Rate] をクリックし、次の各フィールドに値を入力して、SSID ごとに SSID データレート制限を設定します。

- Average Upstream Data Rate Per SSID (kbps)
- Burst Upstream Data Rate Per SSID (kbps)
- Average Upstream Real-Time Rate Per SSID (kbps)
- Burst Upstream Real-Time Rate Per SSID (kbps)
- Average Downstream Data Rate Per SSID (kbps)
- Burst Downstream Data Rate Per SSID (kbps)
- Average Downstream Real-Time Rate Per SSID (kbps)
- Burst Downstream Real-Time Rate Per SSID (kbps)

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にあるロック記号をクリックします。

ステップ 18 [802.11ax Configuration] をクリックし、802.11ax BSS 設定のパラメータを設定します。トグルボタンを使用して次の設定パラメータを有効または無効にすることができます。

- BSS ターゲット起動時間
- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にあるロック記号をクリックします。

ステップ 19 **[保存（Save）]** をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Advanced SSID Configuration - Model Config] 領域に表示されます。

ステップ 20 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 21 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（181 ページ）を参照してください。

ステップ 22 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）を参照してください。

Cisco CleanAir の設計の作成

CleanAir は、共有ワイヤレススペクトラムに関する問題に予防的に対応するスペクトルインテリジェンス ソリューションです。この機能を使用すると、共有スペクトラムの全ユーザーを確認できます（ネイティブデバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルをステアリングして干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と無線周波数（RF）の可視性を提供します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定機能の名前を入力して検索するか、[Wireless] モデル設定を展開して [CleanAir Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default CleanAir 802.11a Design] または [Default CleanAir 802.11b Design] チェックボックスをオンにして、デフォルトの CleanAir 設計を使用します。

（注） [Default CleanAir 802.11a Design] または [Default CleanAir 802.11b Design] は編集および削除できません。

ステップ 4 [Design Instances] ウィンドウで、[Add] をクリックします。

[Add CleanAir Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドに設計の名前を入力します。

ステップ 6 [Radio Band] ドロップダウンリストから [2.4 GHz] または [5 GHz] を選択します。

ステップ 7 [CleanAir Enable] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で CleanAir 機能を有効にします。

[CleanAir Enable] トグルボタンが有効になっている場合は、そのトグルボタンをクリックしてスペクトル干渉を シスコ ワイヤレス コントローラ で検出しないようにします。

ステップ 8 [CleanAir Device Reporting Enable] トグルボタンをクリックして、干渉源が検出された場合に CleanAir システムから報告されるようにします。

[CleanAir Device Reporting Enable] トグルボタンが有効になっている場合は、トグルボタンをクリックして干渉源が シスコ ワイヤレス コントローラ から報告されないようにします。

ステップ 9 CleanAir で検出できる永続型デバイスに関する情報を伝達できるように、[Persistent Device Propagation] トグルボックスをオンにします。

永続型デバイスの伝達を有効にすると、同じシスコ ワイヤレス コントローラに接続されているネイバー AP に永続型デバイスの情報を伝達できます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。

ステップ 10 [Enable Interferers Features] を展開し、CleanAir システムで検出および報告する必要がある干渉源の横にあるチェックボックスをオンにします。

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect

- Generic TDD
- Generic Waveform
- Jammer
- 電子レンジ
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- ビデオ
- Wimax Fixed
- Wimax Mobile
- XBox

ステップ 11 [CleanAir Description] フィールドに説明を入力します。

ステップ 12 [Apply] をクリックします。
作成した設計インスタンスが [Design Instances] ウィンドウの [CleanAir Configuration - Model Configs] 領域に表示されます。

ステップ 13 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 14 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（181 ページ）を参照してください。

ステップ 15 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）を参照してください。

Dot11ax 設定のモデル設定設計の作成

Cisco DNA Center の Dot11ax モデル設定機能により、デバイスの Dot11ax パラメータが設定されます。

Dot11ax 設定には、高効率（HE）ワイヤレスとも呼ばれる 802.11ax ワイヤレス仕様標準が含まれます。Dot11ax は 2.4 GHz と 5 GHz のデュアルバンドテクノロジーです。Dot11ax 設定パラメータは、Wi-Fi 6 をサポートしている Cisco Catalyst 9100 シリーズ アクセスポイントでのみ設定できます。

（注） BSS カラーは、重複する基本サービスセット（OBSS）を識別するために使用されます。BSS 設定は、Wi-Fi 6 対応アクセスポイントでのみプッシュされます。Cisco Catalyst 9100 シリーズ アクセスポイントは、高密度の高解像度アプリケーションに最適な次世代の Wi-Fi 802.11ax アクセスポイントです。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力するか、[Wireless] を展開して [Dot11ax Configuration] を選択することで、モデル設定を検索できます。

ステップ 3 [Design Instances] ペインで [Default Dot11ax Design] チェックボックスをオンにしてデフォルトの Dot11ax 設計を使用します。

（注） [Default dot11ax Design] の値は編集および削除できません。

ステップ 4 [Design Instances] ウィンドウで、[Add Design] をクリックします。

[Add Dot11ax Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 6 [BSS Color] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で BSS カラー機能を有効にします。デフォルト値は [disabled] です。

ステップ 7 [Target Wakeup Time] トグルボタンをクリックしてターゲットのウェイクアップ時間を有効にします。デフォルト値は [disabled] です。

ステップ 8 [Radio Band] ドロップダウンリストから 2.4 GHz または 5 GHz の無線帯域を選択します。

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、各プロパティの横にあるロック記号をクリックします。

ステップ 9 [保存（**Save**）] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Dot11ax Configuration - Model Configs] エリアに表示されます。

ステップ 10 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 11 アクセスポイントに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。詳細については、「ワイヤレス用のネットワークプロファイルの作成」を参照してください。

ステップ 12 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）を参照してください。

マルチキャストのモデル設定設計の作成

デバイスでマルチキャストパラメータを設定するには、マルチキャストモデル設定機能を使用します。

ネットワークがパケットのマルチキャストをサポートしている場合は、シスコ ワイヤレス コントローラが使用するマルチキャストの方法を設定できます。ワイヤレスコントローラは次のいずれかのモードでマルチキャストを実行します。

- ユニキャストモード：このモードでは、ワイヤレスコントローラは、ワイヤレスコントローラに関連付けられているすべてのアクセスポイントにすべてのマルチキャストパケットをユニキャストします。このモードはそれほど効率的ではありませんが、マルチキャストをサポートしていないネットワークでは必要です。
- マルチキャストモード：このモードでは、ワイヤレスコントローラはマルチキャストパケットを CAPWAP マルチキャストグループに送信します。この方法では、ワイヤレスコントローラプロセッサのオーバーヘッドが軽減され、パケットレプリケーションの処理がネットワークに移されます。これは、ユニキャストを使った方法より効率的です。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Multicast Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Multicast Design] チェックボックスをオンにして、デフォルトのマルチキャスト設計を使用します。

（注） [Default Multicast Design] の値を編集および削除することはできません。

ステップ 4 [Design Instances] ウィンドウで [Add Design] をクリックします。

[Add Multicast Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 6 [Enable Global Multicast Mode] トグルボタンをクリックして、マルチキャストパケットの送信を設定します。デフォルト値は [disabled] です。

ステップ 7 [AP Multicast Mode] ドロップダウンリストから、[UNICAST] または [MULTICAST] のいずれかを選択します。

- ワイヤレスコントローラからユニキャスト方式でパケットをブロードキャストするように設定するには、[UNICAST] を選択します。
- ワイヤレスコントローラからマルチキャスト方式でCAPWAPマルチキャストグループにパケットをブロードキャストするように設定するには、[MULTICAST] を選択します。

ステップ 8 [IPV4 Multicast Group Address] を展開し、[IP Address] フィールドに IPv4 マルチキャストアドレスを入力します。

ステップ 9 [IPV6 Multicast Group Address] を展開し、[IP Address] フィールドに IPv6 マルチキャストアドレスを入力します。

ステップ 10 [Apply] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Multicast - Model Config] 領域に表示されます。

ステップ 11 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。

変更を加えたら、[Save] をクリックします。

ステップ 12 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。

Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（181 ページ）を参照してください。

ステップ 13 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）を参照してください。

グローバル IPv6 の設計の作成

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Global IPV6 Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Global IPv6 Design] チェックボックスをオンにして、デフォルトのグローバル IPV6 設計を使用します。

（注） [Default Global IPv6 Design] は編集も削除もできません。

ステップ 4 [Design Instances] ウィンドウで、[Add Design] をクリックします。

[Add Global IPV6 Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 6 [Global IPV6 Config] トグルボタンをクリックして、IPv6 をデバイスでグローバルに有効にします。

ステップ 7 [Apply] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Global IPV6 Configuration - Model Config] 領域に表示されます。

ステップ 8 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 9 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（181 ページ）を参照してください。

ステップ 10 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）を参照してください。

レガシーデバイスからの設計の検出と作成

モデル設定エディタを使用して手動で設計を作成する代わりに、[Discover Model Configs] 機能を使用して使用可能な既存のモデル設定の設計をレガシーデバイスから検出し、それらをテンプレートとして使用して新しい設計を作成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**[Tools]** > **[Model Config Editor]** の順に選択します。

ステップ 2 [Discovery] タブをクリックします。

[Inventory] ウィンドウにある使用可能な検出済みデバイスのリストが表示されます。

ステップ 3 デバイス名の横にあるオプションボタンをクリックし、[Discover Model Configs] をクリックします。

ステップ 4 右側のペインで、[Wireless] を展開し、モデル設定の設計タイプを選択します。

選択したモデル設定のタイプで使用可能な設定が表示されます。たとえば、[Wireless] の [CleanAir Configuration] を選択した場合、CleanAir についての使用可能な設定が表示されます。

ステップ 5 新しい設計を作成するためのテンプレートとして使用する設定の横にあるオプションボタンをクリックし、[Create Design] をクリックします。

ステップ 6 表示されるウィンドウで、必要な変更を行ってから [Save] をクリックします。

第 11 章

テレメトリの設定

アプリケーションテレメトリについて

アプリケーションテレメトリを使用すると、デバイスの正常性をモニターおよび評価するためのグローバルネットワーク設定を構成できます。

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定

Cisco DNA Center では、デバイスを特定のサイトに割り当てる際のグローバルネットワーク設定を構成できます。テレメトリを使用すると、ネットワークデバイスがポーリングされ、SNMP サーバー、syslog サーバー、NetFlow コレクタ、または有線クライアントの設定に従ってテレメトリデータが収集されます。

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『ネットワーク階層のサイトの作成（125 ページ）』を参照してください。

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

ステップ 2 [NMP Traps] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Cisco DNA Center as SNMP trap server] チェックボックスをオンにします。

b) [Add an external SNMP trap server] チェックボックスをオンにし、外部 SNMP トラップサーバーの IP アドレスを入力します。

選択したサーバーによってネットワークデバイスから SNMP トラップとメッセージが収集されます。

ステップ 3 [Syslogs] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Use Cisco DNA Center as syslog server] チェックボックスをオンにします。

b) [Add an external syslog server] チェックボックスをオンにし、外部 syslog サーバーの IP アドレスを入力します。

ステップ 4 [NetFlow] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Use Cisco DNA Center as NetFlow collector server] チェックボックスをオンにします。

デバイスインターフェイスの NetFlow の構成は、デバイスでアプリケーションテレメトリを有効にした場合にのみ完了します。NetFlow の宛先サーバーをデバイスに設定するには、サイトレベルで NetFlow コレクタを選択します。

b) [Add an external NetFlow collector server] チェックボックスをオンにし、NetFlow コレクタサーバーの IP アドレスとポート番号を入力します。

選択したサーバーがネットワークデバイスからの NetFlow エクスポートの宛先サーバーになります。NetFlow コレクタが選択されていない場合、アプリケーションテレメトリは有効になりません。

ステップ 5 [Wired Client Data Collection] 領域を展開し、[Monitor wired clients] チェックボックスをオンにします。

この選択により、サイトのアクセスデバイスで IP デバイストラッキング（IPDT）がオンになります。

デフォルトでは、サイトの IPDT は無効になっています。

ステップ 6 [Save] をクリックします。

デバイスでのアプリケーションテレメトリ有効化の基準

Cisco DNA Center では、新しい自動選択アルゴリズムに基づいてインターフェイスと WLAN を選択し、該当するすべてのインターフェイスと WLAN でアプリケーションテレメトリを自動的に有効にします。

アプリケーションテレメトリは、Cisco DNA Center を介してプロビジョニングされた WLAN にプッシュされます。

（注）
- 従来のタギングベースのアルゴリズムがサポートされ、インターフェイスまたは WLAN の新しい自動選択アルゴリズムよりも優先されます。
- 自動選択アルゴリズムからタギングベースのアルゴリズムに切り替える場合は、タグ付き SSID をデバイスに対してプロビジョニングする前にテレメトリを無効にする必要があります。

次の表に、サポートされているすべてのプラットフォームについて、従来のタギングベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムに基づくインターフェイスと WLAN の選択基準を示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Router	• インターフェイスの説明に **lan** キーワードが含まれている。[12] • インターフェイスが物理インターフェイスである。 • インターフェイスに管理 IP アドレス以外の IP アドレスがある。	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれでもない。 • WAN （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。 このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。 ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。 • ループバック • 管理インターフェイス：IGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

スイッチ	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2]
	• スイッチポートがアクセスポートとして設定されている。
	• スイッチポートに **switch-mode access** コマンドが設定されている。
		• インターフェイスが物理インターフェイスである。
		• アクセスポートにネイバーがない。
		• インターフェイスが次のいずれでもない。
		  • 管理インターフェイス：FASTETHERNET0、FASTETHERNET1、GIGABITETHERNET0/0、MGMT0
		  • LOOPBACK0、Bluetooth、App Gigabit、WPAN、Cellular、Async
		  • VSL インターフェイス

Cisco AireOS コントローラ	• WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	• ゲスト SSID ではない。
		  • WLAN がゲストタイプとして設定されていない。
		  • SSID の名前に **guest** キーワードが含まれていない。
		• SSID がローカルモードで設定されている。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS リリース 16.12.1 以降	• WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]
	• WLAN がローカルモードで設定されている。
		• ゲスト SSID ではない。
		  • WLAN がゲストタイプとして設定されていない。
		  • SSID の名前に **guest** キーワードが含まれていない。
		• SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべての SSID がローカルモードの場合、最適化 APM レコードが設定されます。

	（注） テレメトリ設定を更新する場合は、テレメトリを無効にしてから、設定の変更後にテレメトリを有効にする必要があります。	

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Cisco DNA トラフィック テレメトリ アプライアンス と最適化 APM プロファイルおよび IOS リリース 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

[1] **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。
[2] ネットワークデバイスを再同期して、**lan** インターフェイスの説明を読み取ります。

アプリケーションテレメトリ設定のプロビジョニング

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定（241 ページ） の説明に従って、グローバルテレメトリ設定を構成します。

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]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、建物、またはフロアを選択します。

ステップ 2 プロビジョニングするデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Telemetry] を選択し、次のいずれかを実行します。

（注） アプリケーションテレメトリのオプションは、Cisco DNA Center からのアプリケーションテレメトリの有効化がデバイスでサポートされている場合にのみ有効になります。

a) [Enable Application Telemetry]：選択したデバイスでアプリケーションテレメトリを設定します。
b) [Disable Application Telemetry]：選択したデバイスからアプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

[Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で

[Application Telemetry] 列が表示されない場合は、列見出しの右端にある [More] アイコン（⋮）をクリックし、[Application Telemetry] チェックボックスをオンにします。

新しいクラスタ仮想IPアドレスを使用するためのテレメトリ設定の更新

Cisco DNA Centerアプリケーションテレメトリを使用してデバイスデータをモニターし、Cisco DNA Center クラスタ仮想 IP アドレス（VIP）を変更する必要がある場合は、次の手順を実行して VIP を変更し、ノードテレメトリデータが新しい VIP に送信されることを確認します。

始める前に

- 使用している Cisco DNA Center のバージョンを確認します。それには、Cisco DNA Center GUI にログインし、[About] オプションを選択して Cisco DNA Center のバージョン番号を表示します。
- SSH クライアントソフトウェアを入手します。
- Cisco DNA Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスを特定します。ポート 2222 上のこのアドレスを使用してアプライアンスにログインします。このポートを特定するには、『Cisco DNA Center Installation Guide』の「Front and Rear Panels」の項にある背面パネルの図を参照してください。
- プライマリノードに設定されている Linux ユーザー名（**maglev**）とパスワードを取得します。
- 割り当てるクラスタ VIP を特定します。クラスタ VIP は、『Cisco DNA Center Installation Guide』の「Required IP Addresses and Subnets」セクションで説明されている要件に準拠している必要があります。

ステップ 1 Cisco DNA Center GUI にアクセスし、次の手順に従ってすべてのサイトでアプリケーションテレメトリを無効にします。

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、建物、またはフロアを選択します。

b) 現在モニターしているすべてのサイトとデバイスを選択します。

c) [Actions] ドロップダウンリストから、[Telemetry] > [Disable Application Telemetry] の順に選択します。

d) サイトとデバイスでテレメトリが無効になったことが示されるまで待ちます。

ステップ 2 アプライアンス構成ウィザードを使用して、次のようにクラスタ VIP を変更します。

a) SSH クライアントを使用して、Cisco DNA Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスにログインします。ポート 2222 にログインしていることを確認します。
b) プロンプトが表示されたら、Linux のユーザー名とパスワードを入力します。
c) 次のコマンドを入力すると、プライマリノード上で構成ウィザードにアクセスできます。

```
$ sudo maglev-config update
```

Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。

d) クラスタ仮想 IP の入力を求める画面が表示されるまで [Next] を繰り返しクリックします。新しいクラスタ VIP を入力し、以降のすべての画面で [Next] をクリックしてウィザードを終了します。

設定したインターフェイスごとに 1 つの仮想 IP を設定する必要があります。**sudo maglev-config update** コマンドを入力して、設定したインターフェイスごとに 1 つの VIP を入力するよう指示されるようにウィザードを設定することを推奨します。

最後の画面に到達すると、変更を適用する準備ができたことを示すメッセージが表示されます。

e) [proceed] をクリックして、クラスタ VIP の変更を適用します。

設定プロセスの最後に成功メッセージが表示され、SSH プロンプトに復帰します。

ステップ 3 SSH プロンプトで次の一連のコマンドを入力して、必要な Cisco DNA Center サービスを再起動します。

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

ステップ 4 すべてのサービスが再起動するまで待ちます。次のコマンドを入力して、再起動の進行状況をモニターリングできます。必要に応じて、使用している Cisco DNA Center のバージョンが属するリリーストレインに適したサービス名に置き換えてください。

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

必要なすべてのサービスが実行されている場合は、次のようなコマンド出力が表示され、正常に再起動した各サービスの実行ステータスが表示されます。

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp   collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>   <IP>
ndp   collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>   <IP>
ndp   collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>   <IP>
```

ステップ 5 Cisco DNA Center GUI にアクセスし、次の手順に従ってすべてのノードでアプリケーションテレメトリを有効にします。

a) Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Inventory]** > **[Provision]** の順に選択します。
b) モニターするすべてのサイトとデバイスを選択します。
c) [Actions] ドロップダウンリストから、[Telemetry] > [Enable Application Telemetry] の順に選択します。
d) サイトとデバイスでテレメトリが有効になったことが示されるまで待ちます。

テレメトリを使用したデバイス設定の更新

デバイスの可制御性が有効か無効かに関係なく、デバイスに構成の変更をプッシュできます。

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]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

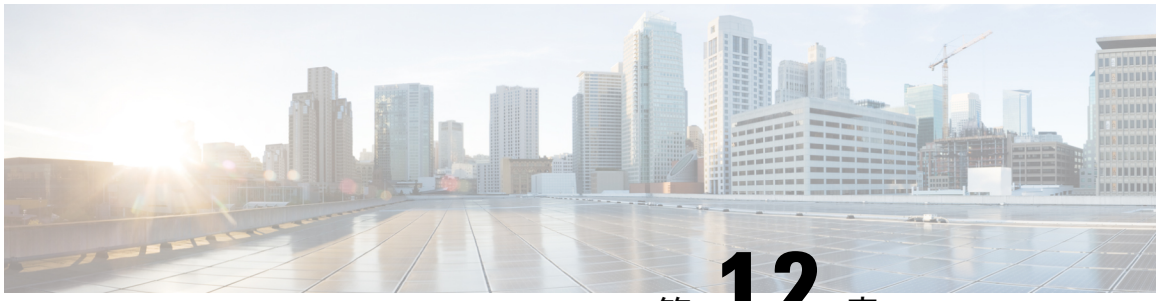
ステップ 2 構成の変更を反映するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[Telemetry]** > **[Update Telemetry Settings]** の順に選択します。

ステップ 4 [Update Telemetry Settings] ウィンドウで、次の手順を実行します。

- （オプション）構成の変更をデバイスにプッシュするには、[Force Configuration Push] チェックボックスをオンにします。構成に変更がない場合は、既存の構成がデバイスに再度プッシュされます。
- [Next] をクリックします。
- [Now] オプションボタンをクリックするか、[Later] オプションボタンをクリックしてテレメトリ設定を更新する日付と時刻を指定します。

ステップ 5 [Apply] をクリックします。



第 12 章

ネットワーク セキュリティ アドバイザリの識別

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team（PSIRTT; プロダクト セキュリティ インシデント レスポンス チーム）は、シスコ製品セキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、シスコのセキュリティアドバイザリとアラートを推奨します。

セキュリティ アドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Cisco DNA Center 内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

前提条件

セキュリティ アドバイザリ ツールを使用するには、機械推論パッケージをインストールする必要があります。『Cisco DNA Center Administrator Guide』の「*Download and Install Packages and Updates*」を参照してください。

オブザーバとして Cisco DNA Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

セキュリティアドバイザリの表示

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

Cisco DNA Center では、セキュリティの問題を特定して自動分析を改善するためにナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

a) Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[System]** > **[Settings]** > **[Machine Reasoning Knowledge Base]** の順に選択します。

b) [Import] をクリックするか、[Download] をクリックして最新の使用可能なナレッジベースをダウンロードしてから [Import] をクリックします。

c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

（注）
- セキュリティアドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
- [Overview] タブのセキュリティアドバイザリのグラフィックには、[Critical]、[High]、[Medium]、[Low]、[Informational] など、ネットワークに対するそれぞれの影響の割合が表示されます。
- セキュリティアドバイザリ スキャンは、サポートされている最小ソフトウェアバージョン以上を実行しているルータおよびスイッチでのみ使用できます。詳細については、「Cisco DNA Center Supported Devices」を参照してください。
- 表示されるセキュリティアドバイザリは、「シスコのセキュリティ脆弱性ポリシー」に基づいています。

次の表に、使用できる情報を記載します。

カラム	説明
アドバイザリ ID	ネットワークで検出されたセキュリティアドバイザリの ID。ID をクリックして、それぞれのアドバイザリ Web ページに移動します。
アドバイザリタイトル	ネットワークデバイスに適用可能なセキュリティ脆弱性アドバイザリの名前。
CVSS スコア	共通脆弱性評価システム（CVSS）モデルに基づいて評価されたスコア。
Impact	脆弱性がネットワークに及ぼす影響。

カラム	説明
CVE	脆弱性の Common Vulnerabilities and Exposures（CVE）識別子。
デバイス	脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
Match Type	検出された脆弱性が [Image Version] の一致と [Configuration] の一致のどちらに基づくかを示します。
検出以降の期間（日数)	脆弱性が検出されてからの経過日数。
Last updated	アドバイザリが最後に更新された日付。

ステップ 3 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。

b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、デバイスに一致するすべてのアドバイザリが表示されます。

デバイスの横にあるロックアイコンは、デバイスに適用可能な 1 つ以上のアドバイザリがあることを示します。

ステップ 4 いつでも [Scan Network] をクリックすれば、表示された結果を更新できます。

セキュリティアドバイザリスキャンのスケジュール設定

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

[Scan Network] ウィンドウが表示されます。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 スキャンを後で実行するように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、日付と時刻を指定します。

ステップ 5 [Time Zone] ドロップダウンリストを使用して、スキャンのスケジュール設定に使用するタイムゾーンを選択します。

ステップ 6 繰り返しオプションとして [None]（デフォルト）、[Daily]、[Weekly] のいずれかを選択します。

ステップ 7 [Run at Interval] フィールドに、スキャンの繰り返しの間隔（日または週の数）を入力します。

ステップ 8 （オプション）スケジュールの終了日や終了までの回数を指定する場合は、[Set Schedule End] チェックボックスをオンにします。

a) スキャン終了日をスケジュールするには、[End Date] オプションボタンをクリックし、日付と時刻を定義します。

b) スキャンの繰り返し回数を定義するには、[End After] オプションボタンをクリックします。

ステップ 9 [Schedule] をクリックします。

ステップ 10 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Activity]** > **[Tasks]** の順に選択して、スキャンのスケジュールと繰り返しを確認します。

（注） Cisco DNA Center ユーザーは、シスコによるテレメトリの収集を許可するかどうかを選択できます。収集されたテレメトリは、ユーザーが使用している機能の開発に役立てられます。収集を許可すると、cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、ネットワーク デバイス インベントリ、およびソフトウェア利用資格の情報が収集されます。テレメトリは、アプリケーションごとや機能ごとではなく、Cisco DNA Center 全体について開示されます。収集されるデータの詳しいリストについては、「*Cisco DNA Center のデータシート*」を参照してください。

セキュリティ アドバイザリ スキャンの実行時に収集されるテレメトリデータは次のとおりです。

- ナレッジパッケージの自動更新が設定されているかどうか。
- 繰り返しのスキャンおよび繰り返しのレポートが設定されているかどうか。
- 実行されたレポートの数。
- ソフトウェアのバージョンと設定に基づいて一致するセキュリティアドバイザリがあるデバイスの数。
- 各スキャンの受理と拒否の数。
- 検索で入力された手動設定とそれに関連するアドバイザリ。
- ソフトウェアのバージョンと設定（製品ファミリを含む）が一致するアドバイザリの数。
- 他のカテゴリ（アドバイザリなし、不明、サポート対象外）に基づくデバイスの数。
- スキャンの成功、失敗、終了の数。
- 平均スキャン時間。

アドバイザリに対するデバイスの表示/非表示

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを非表示にするアドバイザリに対応するデバイス数をクリックします。

[Active] タブには、これらのアドバイザリが発行されたデバイスの数が表示されます。

c) 非表示にするデバイスを選択し、[Suppress Device] をクリックします。

非表示にしたデバイスは、[Suppressed] タブで確認できます。

d) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

ステップ 5 デバイスをアドバイザリに復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを再表示するアドバイザリに対応するデバイス数をクリックします。

c) [Suppressed] タブをクリックして、非表示のデバイスを表示します。

d) 再表示するデバイスを選択し、[Mark as Active] をクリックします。

復元されたデバイスは、[Active] タブで確認できます。

e) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

デバイスに対するアドバイザリの表示/非表示

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。

b) [Advisories] 列で、アドバイザリを非表示にするデバイスに対応するアドバイザリカウントをクリックします。

[Active] タブには、このデバイスに対して発行されたアドバイザリの数が表示されます。

c) 非表示にするアドバイザリを選択し、[Suppress Advisory] をクリックします。

非表示のアドバイザリは、[Suppressed] タブで確認できます。

d) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

ステップ 5 デバイスのアドバイザリを復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。

b) [Advisories] 列で、アドバイザリを再表示するデバイスに対応するアドバイザリカウントをクリックします。

c) [Suppressed] タブをクリックして、非表示のアドバイザリを表示します。

d) 再表示するアドバイザリを選択し、[Mark as Active] をクリックします。

復元されたアドバイザリは、[Active] タブで確認できます。

e) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

一致パターンの追加

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンがアドバイザリに追加されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの AND/OR の定義

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、次の手順を実行します。

a) [CONDITIONS] テキストボックスに条件を入力し、[Add] アイコンをクリックします。

b) ドロップダウンリストから、[AND] または [OR] を選択し、次の条件を入力します。

c) 条件を削除する場合は、[Remove] アイコンをクリックします。

d) **[保存（Save）]** をクリックします。
一致パターンがアドバイザリに追加されます。

ステップ 6 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの編集

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**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンが変更されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの削除

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**[Tools]** > **[Security Advisories]** の順に選択します。

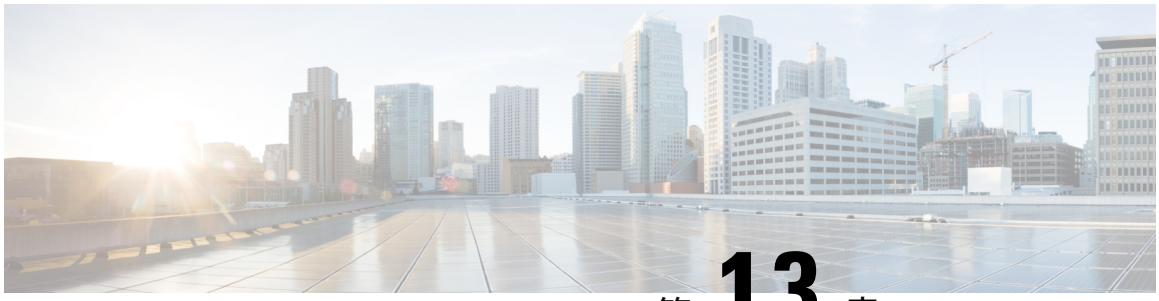
ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[Delete] をクリックします。

一致パターンが削除されます。



第 13 章

ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング

ネットワーク推論機能について

ネットワーク推論機能ツールを使用すると、ネットワークのさまざまな問題を迅速にトラブルシューティングできます。Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Tools]** > **[Network Reasoner]** の順に選択すると、ネットワーク推論機能ダッシュボードが起動します。ネットワーク推論機能ダッシュボードには、ネットワークの問題を事前にトラブルシューティングできる個別のワークフローが用意されています。ダッシュボードには、ワークフローに関する簡単な説明、過去 24 時間に影響を受けたデバイスの数、およびワークフローをネットワークで実行した場合の影響が表示されます。

（注） ネットワーク推論機能を使用するには機械推論パッケージをインストールする必要があり、インストールされていないと [Tools] メニューに表示されません。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

ネットワーク推論機能ダッシュボード

Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Tools]** > **[Network Reasoner]** の順に選択します。ネットワーク推論機能ダッシュボードに次のワークフローが表

示され、ワークフローの説明、過去24時間に影響を受けたデバイスの数、ワークフローをネットワークで実行した場合の影響などが示されます。

- [CPU Utilization]：デバイスで CPU 使用率が高くなっている原因をトラブルシューティングします。
- [Interface Down]：デバイスでインターフェイスが停止している原因をトラブルシューティングします。
- [Power Supply]：デバイスの電源に関する問題の根本原因を特定します。
- [Ping Device]：送信元ネットワークのデバイスからターゲットネットワークのデバイスへの IP 接続に関する問題の原因をトラブルシューティングします。

CPU 使用率が高い場合のトラブルシューティング

CPU 使用率のトラブルシューティングは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ

始める前に

- 機械推論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」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」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**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [CPU Utilization] タブをクリックします。

[CPU Utilization] ページには、過去 24 時間の CPU 使用率の高いデバイスがフィルタ処理されて一覧表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、[CPU Utilization Threshold] にチェックする使用率を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

（注） 次のプロセスが確認されると、詳細な分析の対象となります。

- [MATM Process Group]：MATM RP Shim、NGWC Learning、VMATM Callback
- [IOSXE Process Group]：IP Input、ARP Input、IOSXE-RP Punt Se、SISF Main Thread、DAI Packet、ARP Snoop

[CPU Utilization] ウィンドウが表示され、選択したデバイスの CPU 使用率が高い原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、CPU の消費が多いプロセスとその使用率を確認します。

ステップ 9 それぞれのプロセスについて、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティングプロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

電源障害のトラブルシューティング

電源トラブルシューティング ワークフローは、ソフトウェアバージョン 16.6.1 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論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」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」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**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Power Supply] タブをクリックします。

[Power Supply] ページに、過去 24 時間に電源障害が発生したデバイスのフィルタ処理されたリストが表示されます。

インベントリ内のすべてのデバイスのリストを表示するには、[All] をクリックします。ワークフローを実行する任意のデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力してデバイスをフィルタ処理します。

ステップ 4 [Troubleshoot] をクリックします。

[Power Supply] ウィンドウが開き、選択したデバイスの電源障害の原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 5 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 6 [Conclusion] タブをクリックして、選択したデバイスの電源の [Stack Identifier]、[Product ID]、[Serial Number]、および [Status] の情報と推奨されるアクションを確認します。

ステップ 7 それぞれのスタック識別子について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 8 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） MRE では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

インターフェイスが停止した場合のトラブルシューティング

インターフェイス ダウン トラブルシューティング ワークフローは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論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」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」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**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Interface Down] タブをクリックします。

[Interface Down] ページには、過去 24 時間にインターフェイスが停止したデバイスがフィルタ処理されて一覧表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、問題が疑われるインターフェイスの名前を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

[Interface Down] ウィンドウが開き、選択したデバイスのインターフェイスが停止する原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、インターフェイスが停止する問題についての考えられる根本原因と推奨されるアクションを確認します。

ステップ 9 それぞれの根本原因分析について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） MRE では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

デバイスの IP 接続のトラブルシューティング

ping はシンプルなコマンドであるため、すべてのネットワークデバイスで IP 接続のトラブルシューティングをサポートできます。

始める前に

- 機械推論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」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」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**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、[Ping Device] をクリックします。

ステップ 3 [Devices] ウィンドウで、デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、[Target IP Address] に値を入力し、[Run Machine Reasoning] をクリックします。

ステップ 5 [View Details] をクリックして、ping ステータスを確認します。

第 14 章

ポリシーの設定

ポリシーの概要

Cisco DNA Center を使用すると、ネットワークの特定の側面（ネットワークアクセスなど）に対する組織のビジネス目標を反映したポリシーを作成できます。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワークデバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。

Cisco DNA Center を使用して、仮想ネットワーク、アクセス コントロール ポリシー、トラフィック コピー ポリシー、およびアプリケーション ポリシーを作成できます。

グループベースのアクセスコントロール

Cisco DNA Center は、次の 2 つの方法で Software-Defined Access を実装します。

- 仮想ネットワーク（VN）は、たとえば、企業のネットワークから IoT デバイスを分離するといった、マクロレベルのセグメンテーションを提供します。
- グループベースのポリシーは、たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御するといった、マイクロレベルのセグメンテーションを提供します。

グループベースのアクセス コントロール ポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセス制御機能。
- きめ細かいアクセス制御。
- スケーラブルグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセス コントロール ポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてスケーラブルグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセス コントロール ポリシーを展開するための拡張機能を提供します。
- アイデンティティまたはネットワーク アドミッション コントロール（NAC）アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが、Cisco ISE に移行したいユーザーに対して、Cisco Identity Services Engine（Cisco ISE）への簡単な移行パスを提供します。

Cisco DNA Center での IP プール、サイト、および仮想ネットワークの作成方法については、Cisco DNA Center のユーザーガイドを参照してください。

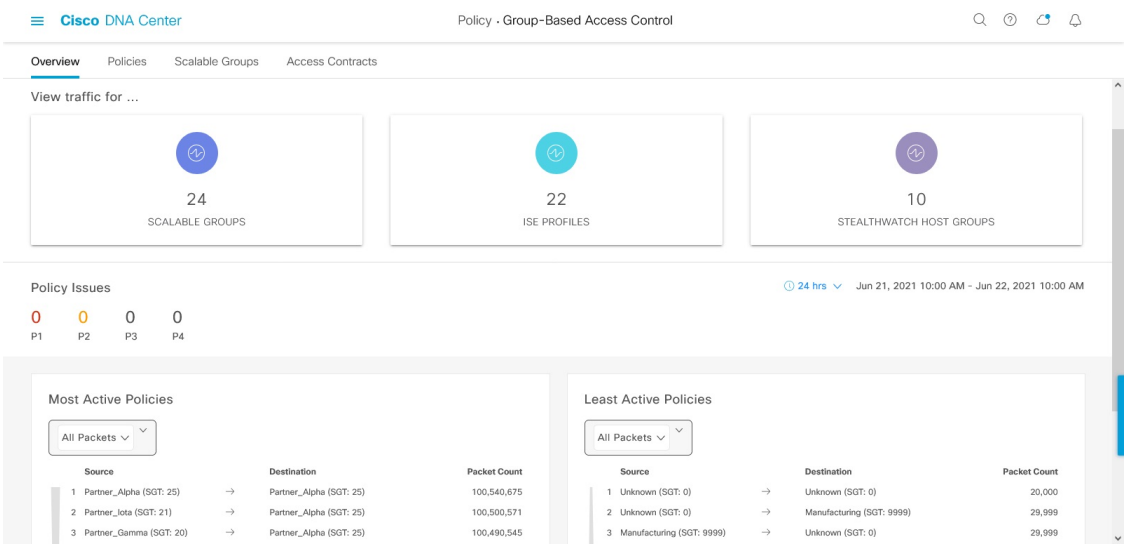
Cisco DNA Center for Cisco ISE の設定の詳細については、Cisco DNA Center のインストールガイドを参照してください。

Cisco ISE for Cisco DNA Center の設定の詳細については、Cisco Identity Services Engine 管理者ガイド [英語] を参照してください。

グループベースのアクセス コントロール ポリシー ダッシュボード

グループベースのアクセスコントロールポリシーダッシュボードでは、ネットワークアクティビティ、ポリシー関連の問題、およびトラフィックトレンドの概要が提供されます。この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**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。

図 *4*: グループベースのアクセス コントロール ポリシー ダッシュボード



このダッシュボードでは、次の詳細方法を表示できます。

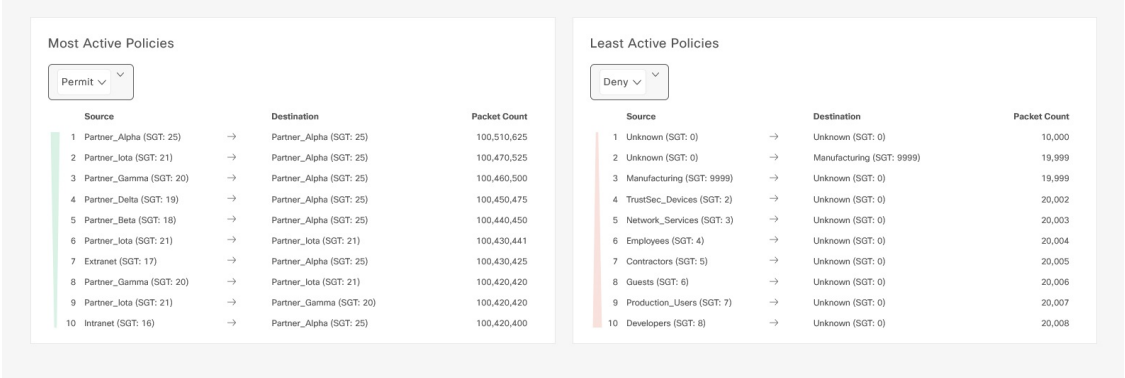
- [View Traffic]：スケーラブルグループ、Cisco ISE プロファイル、および Stealthwatch ホストグループのトラフィックを表示できます。このデータを表示するには、グループベースポリシー分析パッケージをインストールする必要があります。グループベースポリシー分析で提供される分析情報により、新しいアクセスコントロールの導入による影響を評価するために、資産間の通信を可視化してグループベースポリシーを作成したり、そのポリシーで許可する必要があるプロトコルを正確に特定することができます。シスコのグループベースポリシー分析では、ネットワーク上のアセットのグループとそれらの通信に関する情報が集約されます。詳細については、シスコのグループベースポリシー分析（279ページ）を参照してください。

- [View Policy-Related Issues]：ポリシー関連の問題の数が表示されます。数をクリックすると詳細情報が表示されます。新しいブラウザタブで [Assurance Issues] ダッシュボードが開きます。ここで、詳細情報を確認できます。

  このポリシー関連の問題のビューは、現在選択されている期間に関するものであることに注意してください。必要に応じて、時間セレクタを使用して時間枠を調整します。

- [View Most Active and Least Active Policies]：最もアクティブなポリシーと最もアクティブでないポリシーの詳細情報が提供されます。デフォルトでは、このビューは、各ポリシー（各送信元/宛先グループペア）に関してネットワークで確認されたパケットの総数に基づいています。ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。ドロップされたパケットのオプションを使用すると、ポリシーベースのドロップが最もアクティブに実行されているポリシーを確認することができます。

図 *5:*最もアクティブなポリシーのダッシュレットと最もアクティブでないポリシーのダッシュレット



このポリシーアクティビティのビューは、現在選択されている期間に関するものであることに注意してください。必要に応じて、時間セレクタを使用して時間枠を調整します。

グループベースのアクセス コントロール ポリシー

アクセスコントロールポリシーは、送信元スケーラブルグループから宛先スケーラブルグループに渡すことができるネットワークトラフィックを定義します。

- **スケーラブルグループ**：ユーザー、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。スケーラブルグループは、アクセス コントロール ポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、スケーラブルグループを仮想ネットワークに関連付けることができます。

- **契約**：アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワーク アプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。他のルールが一致しない場合、デフォルトアクションでは Catch All ルールが使用されます。

- **グループベースのアクセスコントロールポリシー**：グループベースのアクセスコントロールポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約は、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは単方向です。

  スケーラブルグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザーがアクセスできるネットワークリ

ソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。「財務サーバー」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

送信元と宛先のスケーラブルグループの組み合わせにコントラクトが指定されていない場合に使用するデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ、オープンネットワーク、またはクローズドネットワークに基づいて、デフォルトポリシーを設定できます。

（注） すべてのネットワーク インフラストラクチャ デバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny]に変更することをお勧めします。そのようにしない場合、すべてのネットワーク接続が失われる可能性があります。

リスト ビュー

[Group-Based Access Control] ウィンドウの右上にある [List] アイコンをクリックして、[List] ビューを起動します。

- [Source View]：送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。
- [Destination View]：宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、「請負業者」送信元スケーラブルグループの一部であるユーザーが使用できる宛先グループを確認するには、[Source] ビューを使用します。「財務サーバー」宛先スケーラブルグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

ポリシー適用統計データをポリシーリストテーブルで表示することもできます。選択した期間内のポリシーの許可と拒否の総数が表示されます。

ポリシー適用統計は、グループベースのポリシーおよびテレメトリデータ言語（TDL）サブスクリプション用にプロビジョニングされたネットワークデバイスから収集されます。これらの設定は、通常、ファブリックの一部であるネットワークデバイスに関して自動的にプロビジョニングされます。非ファブリック ネットワーク デバイスに関しては手動設定を実行できます。

ポリシー適用統計データを使用する場合は、次の点に注意してください。

- ポリシー適用統計データは、グループベースポリシー分析パッケージが展開されている場合にのみ使用できます。
- テレメトリ サブスクリプションは、ファブリック ネットワーク デバイスと非ファブリック ネットワーク デバイスの両方に関する基本プロビジョニングの一部として追加されます。新しいネットワークデバイスが DNAC に追加され、サイトに割り当てられると、TrustSec 適用コマンドがプッシュされます。
- Software-Defined Access（SDA）は、ファブリックに追加されたネットワークデバイスに TrustSec 適用を追加します。TrustSec テレメトリデータは、ネットワークデバイスでこの適用が有効になっている場合にのみ収集されます。有効になっていない場合は、ポリシーモニターリングに使用されるテレメトリ サブスクリプションが TrustSec の TDL データの収集に使用されます。
- Cisco IOS XE 16.12 以降では、TDL ストリーミングデータがサポートされています。
- ネットワークデバイスで NETCONF を有効にする必要があります。
- 非ファブリック ネットワーク デバイスについては、次の設定を手動で追加する必要があります。

  ```
  cts role-based enforcement vlan-list <VLAN of the endpoints>
  ```

- Cisco DNA Center 2.2.2 にアップグレードすると、[Provision] > [Network Devices] > [Inventory] ウィンドウに次のメッセージが表示される場合があります。

  IOS-XE デバイスがネットワークで検出されました。これには、保証データの新しいテレメトリ サブスクリプションを有効にし、既存のサブスクリプションの一部をパフォーマンスのために最適化する必要があります。netconf を有効にし、これらのデバイスのインベントリクレデンシャルで netconf ポートを設定する必要があることに注意してください。また、これらのデバイスは、グループベースのポリシー モニターリング テレメトリの新しいサブスクリプションを受信することに注意してください。これらのサブスクリプションをプロビジョニングするためのアクションを実行しますか?

  [Apply Fix] をクリックして、サイトが割り当てられているすべてのネットワークデバイスに設定をプッシュします。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco Identity Services Engine（Cisco ISE）に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

マトリクス ビュー

[Group-Based Access Control] ウィンドウの右上にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューはコアポリシービューであり、すべてのスケーラブルグループに関するすべてのポリシーの概要を提供します（明示的またはデフォルトを問わない）。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセス コントロール ポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元スケーラブルグループがリストされます。

• 宛先軸：水平軸にはすべての宛先スケーラブルグループがリストされます。

特定の送信元スケーラブルグループと宛先スケーラブルグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。次の色は、各セルに適用されるポリシーを示しています。

• [Permit]：緑色

• [Deny]：赤色

• [Custom]：金色

• [Default]：灰色

マトリックスの上部に表示される [Permit]、[Deny]、[Custom]、または [Default] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

セルをクリックすると、[Create Plicy] または [Edit Policy] スライドインペインが開き、選択したセルのポリシーを作成または編集できます。[Create Policy] スライドインペインには、送信元と宛先のスケーラブルグループが読み取り専用フィールドとして表示されます。ポリシーのステータスとアクセス契約を更新できます。

ポリシーマトリックスのカスタムビューを作成して、関心のあるポリシーだけに絞り込むことができます。これを実行するには、[View] ドロップダウンリストをクリックし、[Create View] を選択します。カスタムビューを作成するときに、カスタムビューに含めるスケーラブルグループのサブセットを指定できます。必要に応じて、カスタムビューを保存し、後で編集することができます。[View] ドロップダウンリストをクリックし、[Manage Views] を選択して、カスタムビューを作成、編集、複製、または削除します。[Default View] には、すべての送信元および宛先スケーラブルグループが表示されます。

カーソルでマトリックスコンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任意の場所に移動して配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。この領域をドラッグして、マトリックスをスクロールできます。

（注） ミニマップはデフォルトで閉じられています。[Expand] アイコンをクリックして、ミニマップを展開して表示します。

セルを選択すると、[Matrix] ビューによってそのセルと対応する行（送信元スケーラブルグループ）およびカラム（宛先スケーラブルグループ）が強調表示されます。選択したセルの座標（送信元スケーラブルグループおよび宛先スケーラブルグループ）がマトリックスコンテンツ領域の近くに表示されます。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

[Filter] オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリックスのサブセットを表示できます。フィルタを作成して、関心のあるポリシーだけに絞り込むことができます。フィルタを作成するには、含める送信元および宛先グループを選択します。

Cisco DNA Center と Cisco ISE を統合します。Cisco ISE は、Cisco DNA Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティグループ アクセス コントロール リスト（SGACL）、およびイーグレスポリシーの [TrustSec Workcenter] ユーザーインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の一部を定義します。
2. 特定した分類のスケーラブルグループを作成します。
3. 制御するネットワークトラフィックのタイプのアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバーや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザーのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックのフローを許可する方法を定義します。

スケーラブルグループの作成

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者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**[Policy]** > **[Group-Based Access Control]** > **[Scalable Groups]** の順に選択します。

ステップ 2 [Create Scalable Group] をクリックします。
[Create Scalable Group] スライドインペインが表示されます。

ステップ 3 [Create Scalable Group] スライドインペインで、スケーラブルグループの名前と説明（オプション）を入力します。

（注） [Name] フィールドでサポートされる文字は次のとおりです：

- 英数字
- アンダースコア (_)

スケーラブルグループ名は英字で開始する必要があります。

Cisco DNA Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のスケーラブルグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ～ 65519 です。

ステップ 4 このスケーラブルグループに関連付ける**仮想ネットワーク**をドロップダウンリストから選択します。デフォルトでは、デフォルトの仮想ネットワーク（DEFAULT_VN）が選択されています。

ステップ 5 スケーラブルグループを Cisco Application Centric Infrastructure（ACI）に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 **[Save]** をクリックします。

[Scalable Groups] ウィンドウには、スケーラブルグループ名、タグ値、割り当てられた仮想ネットワーク、および関連付けられたポリシーが表示されます。このウィンドウでは、スケーラブルグループのサンプルを表示することもできます。それらのスケーラブルグループを使用または削除できます。

スケーラブルグループは、[Scalable Groups] ウィンドウから編集または削除できます。スケーラブルグループの詳細を表示するには、[Scalable Group Name] のリンクをクリックします。スケーラブルグループの詳細を更新するには、[View Scalable Group] ウィンドウで [Edit] をクリックします。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ネットワークデバイスへの変更に関する通知を送信するように要求します。

スケーラブルグループの [Policies] 列のリンクをクリックすると、そのスケーラブルグループとそれが属するポリシーを使用するアクセス制御ルールが表示されます。スケーラブルグループが任意のアクセスポリシーで使用されている場合は、それを削除することはできません。

Cisco ISE との同期が完了していない場合は、スケーラブルグループの横にオレンジ色の三角形のアイコンが表示されます。

Cisco ISE は、 内部エンドポイントグループ（IEPG）を同期し、Cisco ISE に関連付けられている読み取り専用スケーラブルグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。これらのスケーラブルグループは、[Created In] 列の値が ACI である [Scalable Groups] ウィンドウに表示されます。ACI から学習したスケーラブルグループを編集または削除することはできませんが、ポリシーで使用することはできます。

[Associated Contracts] 列には、ACI から学習したスケーラブルグループに関連付けられている ACI 学習契約が表示されます。[Associated Contracts] 列に表示されるリンクをクリックすると、関連付けられた契約に関する詳細が表示されます。

IEPG が ACI で更新されると、対応するスケーラブルグループ設定が Cisco ISE で更新されます。Cisco ISE でスケーラブルグループが作成されると、新しい EEPG が ACI に作成されます。

（注） 名前が「ANY」またはタグ値が 0xFFFF/65535 のスケーラブルグループを作成することはできません。スケーラブルグループ ANY/65535 は、Cisco DNA Center デフォルトポリシーに使用される予約済みの内部スケーラブルグループです。

Cisco DNA Center でスケーラブルグループを Cisco ISE と同期する場合、次のようになります。

- スケーラブルグループが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- スケーラブルグループが Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco DNA Center と Cisco ISE の両方でスケーラブルグループ名が同じだが、説明と ACI データが異なっている場合は、 Cisco DNA Center が Cisco ISE で指定されたデータを使用して更新されます。
- Cisco DNA Center と Cisco ISE でスケーラブルグループ名が同じだが、タグ値が異なる場合は、Cisco ISE で指定されたタグ値を持つ新しいスケーラブルグループが Cisco DNA Center に作成されます。Cisco DNA Center にすでにあるスケーラブルグループの名前は、サフィックス _DNAC で更新されます。
- タグ値が同じだが、スケーラブルグループ名が異なる場合は、Cisco DNA Center のスケーラブルグループ名が Cisco ISE で指定された名前で更新されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。Access contracts define the actions（permit or deny）performed when the traffic matches a network application, protocol, and port.

（注） Cisco ISE のセキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco DNA Center のアクセス契約と呼ばれます。

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者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**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、契約の名前と説明を入力します。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

  トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1つの契約に複数のルールを作成するには、[Plus]記号をクリックし、[Action]列と[Application]列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用してドラッグして、ルールの順序を変更します。

[Logging]トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期化テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 **[Save]** をクリックします。

[Access Contracts] リストウィンドウで、契約の表示、作成、複製、更新、および削除ができます。

また、[Access Contracts] ウィンドウでサンプル契約を表示することもできます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約（Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log）は削除できません。

[Access Contracts] ウィンドウの [Contract Name] リンクをクリックして、契約の詳細を表示します。契約の詳細を編集するには、[View Contract] ウィンドウで [Edit] をクリックします。

Cisco ISE との同期が完了していない場合は、契約の横にオレンジ色の三角形のアイコンが表示されます。

ACI から学習した契約は [Access Contracts] ウィンドウに表示され、[Created In] 列の値が [ACI] になります。ACI から学習した契約を編集したり削除したりすることはできませんが、ACI から学習したスケーラブルグループの使用中にポリシーで使用することはできます。マトリックスビューからポリシーを作成または更新する場合に、ACI から学習したスケーラブルグループを接続先グループとして選択すると、関連する契約が [Preferred Contracts] タブに表示されます。[All Contracts] タブですべての契約を確認できます。

[Rules Count] 列で、各契約で使用されているルールの数を確認できます。

契約を使用するポリシーを表示するには、契約の [Policies] 列のリンクをクリックします。

ポリシーで使用されている場合、契約を削除することはできません。契約を削除する前に、そのポリシーから契約を削除する必要があります。

スケーラブルグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新したポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Cisco DNA Center に表示されるポリシー情報と一致しない可能性があります。この状況を解決するには、ネットワークデバイスに、更新したポリシーを展開する必要があります。

既存の契約を複製し、必要な詳細を編集して新しい契約を作成することができます。契約を複製すると、既存の契約に含まれるすべての情報がコピーされ、コピーした契約は、既存の契約名の末尾に文字列 `Copy` が付加された名前になります。

[Filter] オプションを使用して、探している契約を検索できます。

Cisco DNA Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- コントラクトがに存在Cisco ISEし、にCisco DNA Center存在しない場合は、にCisco DNA Center作成されます。
- Cisco DNA CenterとCisco ISEの契約名が同じであるが、説明とトラフィックルールの内容が異なっている場合、Cisco DNA CenterはCisco ISEで指定されたデータを使用して更新されます。
- 契約名とルールが同じですが、説明が異なっている場合Cisco DNA Centerは、でCisco ISE指定された説明を使用して更新されます。
- Cisco ISEの Text SGACL コマンドラインは、非解析コンテンツとして移行されます。これらの契約は編集できますが、Cisco DNA Centerでは解析または構文チェックは実行されません。Cisco DNA Center で加えた変更は、同様に Cisco ISE にも反映されます。
- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Cisco DNA Center のデフォルトポリシーとして移行されます。

グループベースのアクセス コントロール ポリシーの作成

スケーラブルグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセス コントロール ポリシーを作成する際には、以前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1 つの送信元

グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。「Finance Servers」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先と複数の送信元グループを使用してアクセス コントロール ポリシーを作成できます。

グループベースのアクセス コントロール ポリシーの作成

ステップ 1 [Policy List] または [Matrix]ビューで、[Create Policies] をクリックします。

ステップ 2 [Source To Destination(s)] をクリックして、単一の送信元と複数の宛先グループを含むアクセス コントロール ポリシーを作成します。

a) 選択する送信元スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックして、新しいスケーラブルグループを作成します。詳細については、「スケーラブルグループの作成 （272 ページ）」を参照してください。

b) [Next] をクリックします。

c) 選択した送信元スケーラブルグループにマッピングする宛先スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。詳細については、「アクセス契約の作成 （274 ページ）」を参照してください。

必要に応じて、契約の詳細を表示および編集できます。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) **[Save]** をクリックします。

ステップ 3 [Destination to Source(s)] をクリックして、1つの宛先と複数の送信元グループを含むアクセス コントロール ポリシーを作成します。

a) 選択する宛先スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックします。

b) **[次へ (Next)]** をクリックします。

c) 選択した宛先スケーラブルグループにマッピングする送信元スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックします。

必要に応じて、契約の詳細を表示および編集できます。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) **[Save]** をクリックします。

（注） [Scalable Group] リストエリアの右上隅にある [Toggle]ボタンを使用して、[List]ビューと [Drag and Drop]ビューを切り替えることができます。[Drag and Drop] ビューを使用すると、アクセス コントロール ポリシーの作成時に、スケーラブルグループを [Source] フィールドと [Destination] フィールドにドラッグアンドドロップすることができます。ただし、[Drag and Drop]ビューには、最初の 50 のスケーラブルグループのみが表示されます。スケーラブルグループの数が少ない場合（最大 50）は、[Drag and Drop] ビューを使用できます。スケーラブルグループが 50 を超える場合は、[List] ビューを使用してすべてのグループを表示します。

Cisco DNA Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、 Cisco DNA Center は Cisco ISE で指定された契約で更新されます。
- ポリシーモード情報（有効、無効、またはモニター）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは Cisco ISE ではデフォルトで有効になっていません）。Cisco DNA Center では、単一のポリシーに対して複数のアクセス契約を使用することはサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Cisco DNA Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションがあります（デフォルトポリシーを使用する場合）。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

シスコのグループベースポリシー分析

ここでは、シスコのグループベースポリシー分析について詳しく説明します。

グループベースポリシー分析で提供される情報を使用することで、資産間の通信を可視化してグループベースポリシーを作成したり、新しいアクセスコントロールの導入による影響を評価したり、ポリシーで許可する必要があるプロトコルを正確に特定したりできます。

シスコのグループベースポリシー分析では、ネットワーク上の資産のグループとそれらの通信に関する次のような情報が集約されます。

- 相互に通信しているグループ
- 通信の種類
- 特定の資産が属するグループ

インストール

Cisco DNA Center のライセンスの種類は次のとおりです。

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage と Cisco DNA Premier には、グループベースポリシー分析パッケージが含まれています。このパッケージは、次のアーカイブ（.tar.gz ファイル）で構成されています。

- バックエンド
- ユーザー インターフェイス
- サマライザパイプライン
- 集約の定義

シスコのグループベースポリシー分析はCisco DNA Centerの一部ですが、デフォルトではインストールされません。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]** > **[Installed Apps]** の順に選択します。[Policy Applications] で [Group-Based Policy Analytics] まで下にスクロールします。[Install] をクリックしてアプリケーションをインストールします。

ハードウェアとソフトウェアの互換性

プラットフォーム サポート

シスコのグループベースポリシー分析は、次のハードウェア プラットフォームでサポートされています。

- 44 コアのシングルノードクラスタと 3 ノードクラスタ
- 56 コアのシングルノードクラスタと 3 ノードクラスタ
- 112 コアのシングルノードクラスタと 3 ノードクラスタ

これらのプラットフォームは、ここで説明するパフォーマンスと拡張性の要件を満たしている必要があります。

サポートされているハードウェアの詳細については、「Cisco UCS M4 appliances」または「Cisco UCS M5 appliances」を参照してください。

次の表に、Cisco DNA Center およびシスコのグループベースポリシー分析でサポートされるパフォーマンスメトリックをコアプラットフォームごとに示します。NetFlow メトリックは、シスコのグループベースポリシー分析で導入されています。

表 *41* : パフォーマンスメトリック

メトリック	44 コア、3 ノード	56 コア	112 コア
デバイス （NAD）	5000 スイッチが 1000、ルータが 1000、またはその両方の組み合わせ、AP が 4000	8000 スイッチが 2000、ルータが 2000、またはその両方の組み合わせ、AP が 6000	18,000 スイッチが 5000、ルータが 5000、またはその両方の組み合わせ、AP が 12,000
Clients （エンドポイント）	25,000 ワイヤレスが 20,000、有線が 5,000	40,000 ワイヤレスが 30,000、有線が 10,000	100,000 ワイヤレスが 60,000、有線が 40,000
NetFlow/秒	30,000	48,000	120,000

デバイス サポート

シスコのグループベースポリシー分析を使用するには、NetFlow を有効にする必要があります。次の表に、さまざまなネットワークデバイスで NetFlow を有効にする方法を示します。

表 *42 :* デバイス サポート

ネットワーク デバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
ルータ	Cisco 1000 シリーズ サービス統合型ルータ（ISR1K）	対応	対応	対応	対応
	Cisco 4000 シリーズ サービス統合型ルータ（ISR4K）	対応	対応	対応	対応
	Cisco 1000v シリーズ クラウド サービス ルータ（CSR 1000v）	対応	対応	対応	対応
	Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR1K）	対応	対応	対応	対応

ネットワークデバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
スイッチ	Cisco Catalyst 9200 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9300 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9400 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9500 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 9600 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 2k シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3560 シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3650 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 3850 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 4k シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 6500 シリーズ スイッチ	非対応	対応	対応	対応
	Cisco Catalyst 6800 シリーズ スイッチ	非対応	対応	対応	対応

ネットワークデバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレートエディタツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
ワイヤレス コントローラ	Cisco 3504 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 5520 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 8540 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco Catalyst 9800 ベースのコントローラ	対応	対応	対応	対応

Cisco ISE

Cisco ISE 2.4 パッチ 7 以降、2.6 パッチ 1 以降、および 2.7 がサポートされています。

Cisco StealthWatch

Cisco Stealthwatch 7.x 以降がサポートされています。

ブラウザのサポート

シスコのグループベースポリシー分析は、次の Web ブラウザを備えた 64 ビットの Windows、Macintosh、および Linux システムと互換性があります。

- Google Chrome：バージョン 73.0 以降
- Mozilla Firefox：バージョン 65.0 以降

コネクタについて

シスコのグループベースポリシー分析は、次のソース（コネクタとも呼ばれます）からテレメトリを収集します。コネクタを設定するには、シスコのグループベースのポリシー分析の初期設定 ワークフローに従うか、**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** > **[Settings]** > **[Configuration]** の順に選択します。

グループデータコネクタ

グループデータコネクタは、資産が分類されるグループに関する情報を収集します。グループデータコネクタには Cisco ISE と Cisco Stealthwatch があります。

- **Cisco ISE**

  Cisco ISE は、アイデンティティおよびアクセス コントロール ポリシーを管理する次世代のプラットフォームとして、企業のコンプライアンス遵守、インフラストラクチャ セキュリティの強化、サービスオペレーションの効率化を実現します。Cisco ISE は、仮想マシンまたは物理マシン、あるいはその両方の組み合わせにインストールされます。Cisco ISE を構成するサービスに Cisco Platform Exchange Grid（pxGrid）があります。これは、SessionDirectory、スケーラブルグループ、およびその他の情報を共有するためのパブリッシャおよびサブスクライバとして機能するモジュールです。PxGrid は、クエリインターフェイスを使用し、一括ダウンロードをサポートしています。ネットワークのユーザーの認証、許可、アカウンティングが行われ、セッションディレクトリが維持されます。ユーザーイベントは、SessionDirectory サービスに登録されているコネクタにパブリッシュされます。スケーラブルグループ通知などの他のサービスにも登録できます。

  ネットワークに入ってきたパケットは、認証で取得したユーザーアイデンティティとデバイスの情報を使用して分類されます。このパケット分類は、パケットがネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータパス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、スケーラブルグループタグ（SGT）と呼ばれることもあります。ネットワークデバイスで SGT に応じてトラフィックをフィルタ処理できるようにすることにより、Cisco ISE でアクセス コントロール ポリシーを適用できるようになります。

  さらに、Cisco ISE は、ネットワークに接続されているエンドポイントの情報も収集します。これには、デバイスのタイプ、OS、OS のバージョン、IP アドレスなどの属性が含まれます。これらは ISE プロファイルと呼ばれます。

  Cisco ISE コネクタは、シスコのグループベースポリシー分析に使用するスケーラブルグループタグ（SGT）の定義とプロファイルを Cisco ISE から提供します。

- **Cisco StealthWatch**

  Cisco Stealthwatch は、高度な脅威検出、脅威への迅速な対応、およびネットワークトラフィックのセキュリティ分析を可能にするネットワークベースの異常検出システムです。Cisco Stealthwatch コネクタは、Cisco Stealthwatch で設定されているホストグループを取得します。ホストグループは基本的に、場所、機能、トポロジなどの類似の属性を持つ複数のホスト IP アドレスまたは IP アドレス範囲の仮想コンテナです。

通信コネクタ

通信コネクタは、グループベースのポリシーの決定に役立つグループ間のトラフィックに関する情報を収集します。これは、Cisco DNA Center で管理しているネットワークデバイスからの NetFlow を使用して実行されます。Cisco DNA Center では、NetFlow がネイティブで収集および集約されます。

シスコのグループベースのポリシー分析の初期設定

このワークフローでは、Cisco ISE、Cisco Stealthwatch、NetFlow などの特定のソースからネットワークアクティビティやエンドポイントに関連するテレメトリデータを収集するために必要なデータコネクタを設定できます。このタスクは、初めてデータコネクタを設定するときに便利です。

始める前に

Cisco DNA Center にシスコのグループベースポリシー分析がインストールされている必要があります。

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**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。[Create policies with more confidence] ウィンドウが表示されます。

ステップ 2 [Get Started] をクリックします。
[Configure your data connectors] ウィンドウが表示されます。

ステップ 3 [Let's Do it] をクリックします。

[Configure Group Data Connectors] ウィンドウが表示されます。

Cisco DNA Center にインストールされている Cisco ISE のバージョンがシスコのグループベースポリシー分析を実行するために必要なバージョンよりも前のバージョンの場合は、次のエラーメッセージが表示されます。

ステップ 4 設定するコネクタの下部にある [Configure] をクリックします。
新しいウィンドウが開き、Cisco DNA Center の [Settings] ウィンドウにリダイレクトされます。ここで必要なコネクタを設定できます。Cisco ISE コネクタを設定する必要があります。Cisco Stealthwatch コネクタの設定は任意です

ステップ 5 [Settings] ウィンドウを閉じます。[Configure Group Data connectors] ウィンドウで、正常に設定されたコネクタの [Configure] オプションの横に緑色のドットが表示されます。

ステップ 6 [Next] をクリックします。

[Configure Communication Connectors] ウィンドウが表示されます。

ステップ 7 次のいずれかのオプションを使用して、通信コネクタ（NetFlow）を設定します。

- Cisco DNA Center のデバイスインターフェイスで NetFlow を手動でプロビジョニングします。
- [Template Editor] をクリックし、Cisco DNA Center の**テンプレートエディタツール**を使用して NetFlow を設定します。

- [Telemetry in Network Settings] をクリックし、ネットワーク設定のテレメトリのセクションで NetFlow を設定します。

ステップ 8 [Next] をクリックします。
[Summary] ウィンドウにコネクタの設定の詳細情報が表示されます。

ステップ 9 グループとエンドポイントの検出を開始するには、[Done] をクリックします。

グループとエンドポイントの確認

ここでは、各種グループ間のトラフィックを可視化するさまざまな方法について説明します。

複数のグループから複数のグループ

[Overview] ウィンドウの [Scalable Groups] ボックスに表示されている数をクリックすると、[Explore Scalable Groups] ウィンドウが表示されます。このウィンドウでは、スケーラブルグループについてのすべてのグループ間通信の概要を確認できます。デフォルトでは、過去 24 時間の時間範囲のデータが表示されます。これは、過去 14 日間に設定された [Overview] ウィンドウの時間範囲とは異なることに注意してください。チャートには、一意のフローが最も多い送信元スケーラブルグループなどについて、特定の期間における上位 25 の送信元スケーラブルグループとその対応するやり取りが表示されます。

 アイコンをクリックするとチャートビューが表示され、  をクリックするとテーブルビューが表示されます。

テーブルビューで、特定の行の [See destinations] リンクをクリックすると、選択した送信元スケーラブルグループに対応するすべての宛先スケーラブルグループが表示されたウィンドウが開き、各宛先スケーラブルグループの一意のフローの数が表示されます。

送信元グループをクリックすると、**単一のグループから複数のグループ**のウィンドウが表示されます。

リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

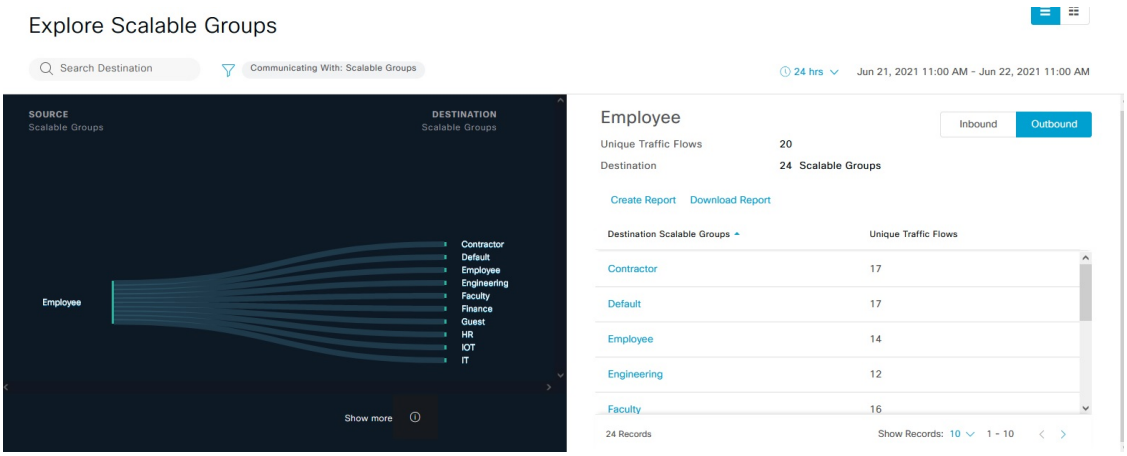
[Overview] ウィンドウの [ISE Profiles] ボックスに表示されている数をクリックすると、[Explore ISE Profiles] ウィンドウが表示されます。このウィンドウでは、送信元が ISE プロファイルで宛先がスケーラブルグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをスケーラブルグループにする必要があります。

[Overview] ウィンドウの [Stealthwatch Host Groups] ボックスに表示されている数をクリックすると、[Explore Stealthwatch Host Groups] ウィンドウが表示されます。このウィンドウでは、送信元が Stealthwatch ホストグループで宛先がスケーラブルグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをスケーラブルグループにする必要があります。

単一のグループから複数のグループ

単一のグループから複数のグループ：アウトバウンド

このウィンドウには、単一の送信元グループと複数の宛先グループの間のアクティビティが表示されます。送信元と宛先の少なくとも一方がスケーラブルグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。



アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

[Outbound] をクリックすると、選択したスケーラブルグループから開始された接続が表示されます。[Inbound] をクリックすると、このスケーラブルグループに対して別のグループから開始された接続が表示されます。

任意の列をクリックして、昇順または降順で並べ替えることができます。

グループをクリックすると、選択したグループを宛先とする**単一のグループから単一のグループ**のウィンドウが表示されます。送信元グループは変わりません。

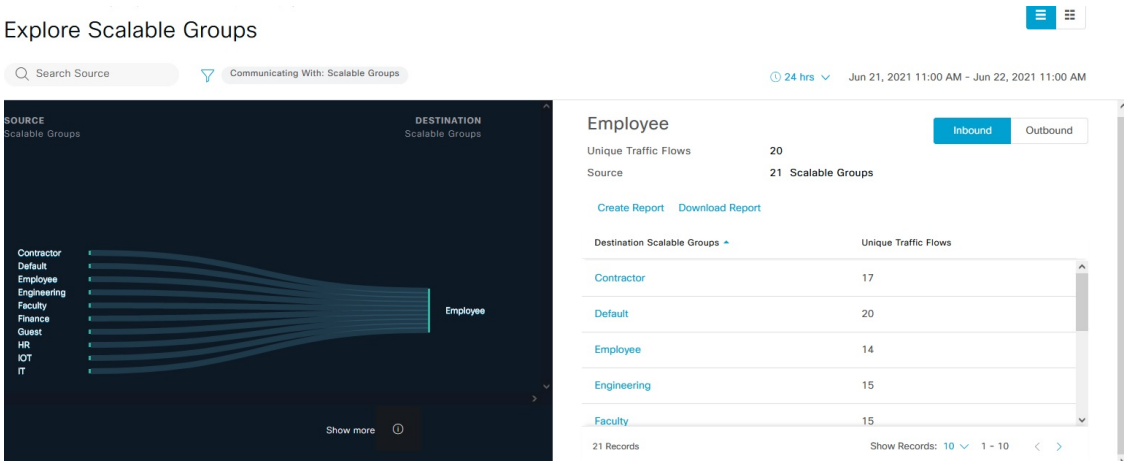
リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

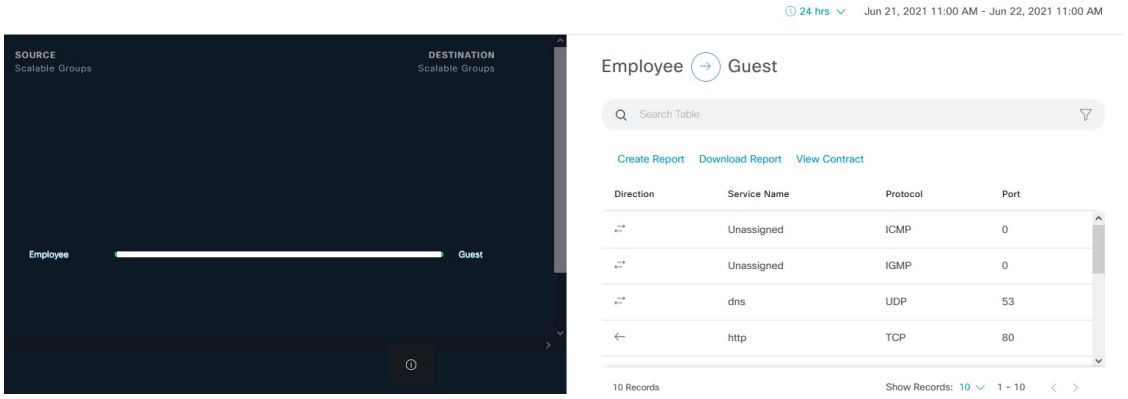
単一のグループから複数のグループ：インバウンド

[Inbound] をクリックすると、選択したスケーラブルグループを宛先としていずれかのグループから開始されたすべての接続が表示されます。



単一のグループから単一のグループ

このウィンドウには、単一の送信元グループと単一の宛先グループの間のアクティビティが表示されます。送信元グループと宛先グループの少なくとも一方がスケーラブルグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。



リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。

送信元グループと宛先グループの間に表示されている方向矢印をクリックすると、このビューの送信元グループと宛先グループが入れ替わります。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。トラフィックフローに使用されるポートとプロトコルを確認することもできます。契約の詳細については、「アクセス契約」を参照してください。

 アイコンをクリックするとチャートビューが表示され、  をクリックするとテーブルビューが表示されます。

日時セレクタを使用して日付と時刻を設定できます。

アクセス契約

アクセス契約は [Analytics] ワークフローで直接作成および変更できるようになりました。

View Contract

[View Contract] ウィンドウを起動するには、[Explore Scalable Groups] ウィンドウで [View Contract] をクリックします。[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。

この表には [Policies] ウィンドウからもアクセスできます。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Policy]** > **[Group-Based Access Control]** > **[Policies]** の順に選択します。

ポリシーマトリックスビューで、契約を作成または変更するセルをクリックします。[Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

現在、送信元グループと宛先グループの間に契約が割り当てられていない場合、データは表示されません。[Change Contract] または [Create Access Contract] オプションを使用して、契約を作成または変更することができます。

[Action] 列の [View traffic] をクリックして、そのルールに一致するフローのリストを表示します。

アクセス契約の作成

[Contract Content] ウィンドウを起動するには、[Policy Details] ペインで [Create Access Contract] をクリックします。トラフィックフィルタルールを作成するには、次の手順を実行します。

1. [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
2. From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、プラスのアイコンをクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルのアイコンを使用して、ルールをドラッグして順序を変更します。

[All Unique Traffic Flows] ペインの [Add to Contract] オプションを使用して契約にエントリを追加することができます。

新しく作成または編集した契約を保存する際は、次のオプションがあります。

- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

契約の変更

[Change Contract] ウィンドウを起動するには、[Policy Details] ペインで [Change Contract] をクリックします。使用可能なすべての契約が表示されます。必要な契約を選択し、[Change] をクリックすると、その契約をポリシーに追加できます。

契約の編集

[Edit] オプションは、契約がすでにポリシーに追加されている場合にのみ表示されます。契約の詳細を編集するには、契約の名前の後に表示される [Edit] をクリックします。

契約を更新したら、[Save] をクリックします。次のオプションを使用できます。

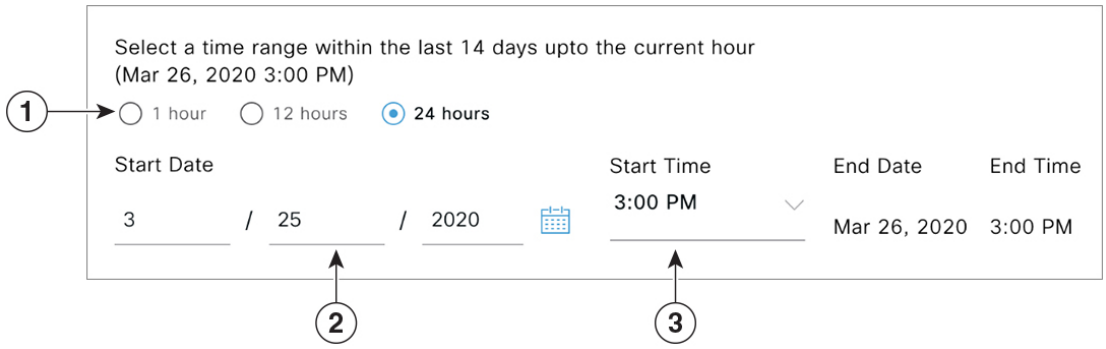
- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

適切なオプションを選択した後に、名前と説明を入力し（1 つ目または 3 つ目のオプションを選択した場合）、[Confirm] をクリックします。

日時セレクタ

接続の概要を表示する期間を選択できます。過去 14 日から現在の 1 時間までの時間範囲を選択できます。

図 *6* : 日時セレクタ



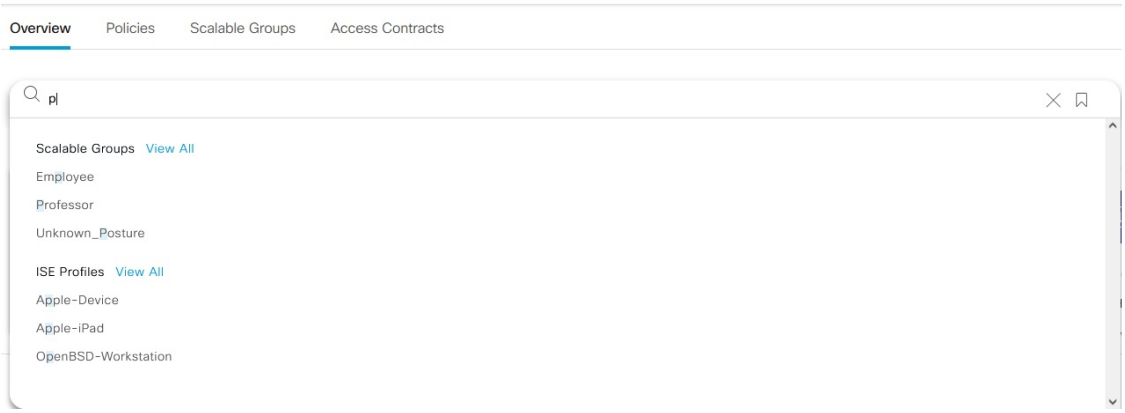
1. 次のいずれかのオプションを選択します。[End Time] は自動的に調整されます。
2. 月、日、年を手動で入力するかカレンダーアイコンを使用して [Start Date] を指定します。
3. [Start Time] をドロップダウンメニューから選択します。

検索の使用

[Overview] ウィンドウには、スケーラブルグループ、ISE プロファイル、Stealthwatch ホストグループ、IP アドレス、または MAC アドレスのデータ全体を検索するための [Search] フィールドが用意されています。

検索フィールドへの文字入力を開始すると、スケーラブルグループ、ISE プロファイル、および Stealthwatch ホストグループの自動検索が実行され、グループタイプごとに最大 3 件の結果が表示されます。IP アドレスの場合、関連文字は整数とピリオドです。MAC アドレスの場合、関連文字は 16 進数とコロンです。

図 *7* : *[Search]* ウィンドウ



（注）
- [Search Results] ウィンドウは、[View All] リンクをクリックするまで開きません。
- 読み取り専用ユーザーは、IPアドレスやMACアドレスは検索できません。詳細については、「ロールベース アクセス コントロール」を参照してください。

[Focus] ドロップダウンリストから、検索条件を変更するために必要なオプションを選択します。

フィルタのアイコン（  ）は高度なフィルタ処理に使用され、MAC アドレスまたは IP アドレスを検索する場合にのみ使用できます。  アイコンをクリックすると、各列の列名の上に検索フィールドが表示されます。

列ごとの検索条件は、最大 3 つまで入力できます。列ごとの条件を複数入力する場合は、OR 演算または AND 演算を指定できます。このように作成したクエリでは、複数の列を対象に AND 演算が実行されます。

 アイコンをクリックして [Save Current Search] オプションを使用すると、現在表示されている検索を保存できます。

保存した検索を削除するには、  アイコンをクリックします。保存した検索の名前にカーソルを合わせ、  アイコンをクリックします。[Delete Saved Filter] ダイアログボックスで [Yes] をクリックすると、フィルタが完全に削除されます。

ロールベース アクセス コントロール

シスコのグループベースポリシー分析は、ロールベース アクセス コントロールをサポートしています。読み取り/書き込みユーザーと読み取り専用ユーザーが区別されます。ただし、シスコのグループベースポリシー分析のリリース 1.0 は可視化を主としたもので、システムに変更は加えられないため、読み取り専用ユーザーに対する制限は限られたものになります。

- 読み取り専用ユーザーは検索クエリを保存できません。
- 読み取り専用ユーザーは シスコのグループベースのポリシー分析の初期設定 ウィンドウで変更を行うことはできません。
- データのエクスポートはHTTPS POST操作であるため、読み取り専用ユーザーはデータをエクスポートできません。
- 読み取り専用ユーザーはグループによる検索のみを実行でき、HTTPS POST操作を伴う他の検索機能は実行できません。

IP ベースのアクセス コントロール ポリシー

IP ベースのアクセス コントロール ポリシーは、アクセス コントロール リスト（ACL）と同じ方法でシスコ デバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセス コントロール ポリシーにはプロトコル タイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィック フローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセス コントロール ポリシーを使用して、セキュリティ、モニターリング、ルート選択、ネットワーク アドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセス コントロール ポリシーには、次の 2 つの主要コンポーネントがあります。

- [IP Network Groups]：IP ネットワーク グループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワーク グループに含めることができる IP サブネットは 1 つだけです。
- [Access Contract]：アクセスコントラクトは、IP ベースのアクセス コントロール ポリシーとグループベースのアクセス コントロール ポリシーの両方で使用される共通の構成要素です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセス コントロール ポリシー設定のワークフロー

始める前に

- 新しい IP ベースのアクセス コントロール ポリシーを作成中に、**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** ウィンドウでグループを追加する場合、Cisco ISE は必須ではありません。
- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
  - ネットワークサーバー（AAA、DHCP、DNS サーバーなど）：グローバル ネットワーク サーバーの設定 （204 ページ） を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのログイン情報：グローバル デバイス クレデンシャルについて （188 ページ）を参照。
  - IP アドレスプール：IP アドレス プールを設定する （197 ページ）を参照。
  - SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなどのワイヤレス設定：グローバル ワイヤレス設定の構成 （156 ページ）を参照。
  - デバイスのプロビジョニング：プロビジョニング （363 ページ）を参照。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「IP ネットワーク グループの作成 （295 ページ）」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IPベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション（許可または拒否）を指定します。詳細については、「IPベースのアクセス コントロール契約の作成 （295 ページ）」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、IPベースのアクセス コントロール ポリシーの作成 （297ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

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**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP サーバー（DHCP Server）]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS サーバー（DNS Server）]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

IP ネットワーク グループの作成

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**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[グループの追加（Add Group）]** をクリックします。

ステップ 3 **[名前（Name）]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 **[説明（Description）]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 **[IP アドレスまたは IP/CIDR（IP Address or IP/CIDR）]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

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**[Policy]** > **[IP Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[IP ネットワーク グループ（IP Network Groups）]** テーブルで、編集または削除するグループ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 次のいずれか 1 つのタスクを実行します。

- グループを変更するには、**[編集（Edit）]**をクリックします。フィールドの定義については、IP ネットワーク グループの作成 （295 ページ） を参照してください。必要な変更を行って、[Save] をクリックします。
- グループを削除するには、**[削除（Delete）]** をクリックし、次に **[はい（Yes）]** をクリックして確定します。

IP ベースのアクセス コントロール契約の作成

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**[Policy]** > **[IP Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 [コントラクトの追加（Add Contract）] をクリックします。

ステップ 3 契約の名前と説明を入力します。

ステップ 4 **[暗黙的アクション（Implicit Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 5 テーブルの **[アクション（Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 6 **[ポート/プロトコル（Port/Protocol）]** ドロップダウン リストから、ポートまたはプロトコルを選択します。

a) Cisco DNA Centerに必要なポートまたはプロトコルがない場合は、**[ポート/プロトコルの追加（Add Port/Protocol）]** をクリックして、自分で作成します。
b) **[名前（Name）]** フィールドで、ポートまたはプロトコルの名前を入力します。
c) [Protocol] ドロップダウンリストから、[UDP]、[TDP]、または [TCP/UDP] を選択します。
d) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。
e) Cisco DNA Centerで定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、**[競合を無視する（Ignore Conflict）]** チェックボックスをオンにします。
f) **[保存（Save）]** をクリックします。

ステップ 7 （任意） 契約にさらにルールを含めるには、**[追加（Add）]** をクリックして、手順 5 および 6 を繰り返します。

ステップ 8 [Save] をクリックします。

IP ベースのアクセス コントロール ポリシー契約の編集または削除

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセス コントロール ポリシー（IP Based Access Control Policies）]** ウィンドウのポリシーの状態が **[変更（MODIFIED）]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開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**[Policy]** > **[IP Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[編集（Edit）]をクリックして変更を行い、[保存（Save）] をクリックします。フィールドの定義については、IP ベースのアクセス コントロール契約の作成 （295 ページ）を参照してください。

  （注） ポリシーで使用されている契約を変更した場合は、**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[Deploy] をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、[削除（Delete）] をクリックします。

IP ベースのアクセス コントロール ポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセス コントロール ポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、Cisco WLC が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。
- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す [変更済み（Modified）] というステータスでフラグが付けられます。

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**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 [ポリシーの追加（Add Policy）] をクリックします。

ステップ 3 次のフィールドに入力します。

フィールド	説明
Policy Name	ポリシーの名前。
Description	ポリシーを表す単語またはフレーズ。
SSID	SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセス ポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。 （注） SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。 ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。
Site Scope	サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲 （301 ページ）を参照してください。

フィールド	説明
Source	契約の影響を受けるトラフィックの送信元。[Source] ドロップダウンリストから、IP ネットワークグループを選択します。使用したい IP ネットワークがない場合は、[+ グループの追加（+Group）] をクリックして作成します。
Contract	ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加（Add Contract）] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可（permit）]（すべてのトラフィックを許可）または [拒否（deny）]（すべてのトラフィックを拒否）を選択することもできます。
Destination	契約の影響を受けるトラフィックの宛先。[宛先（Destination）] ドロップダウン リストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+ IP ネットワーク グループの作成（+Create IP Network Group）] をクリックして作成します。
Direction	送信元と宛先間のトラフィック フローの関係を設定します。送信元から宛先へのトラフィック フローの契約を有効にするには、[一方向（One-Way）] を選択します。両方向（送信元から宛先へ、および宛先から送信元へ）でのトラフィック フローの契約を有効にするには、[双方向（Bi-directional）] を選択します。

ステップ 4 （任意） IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成（Create IP Network Group）] をクリックします。

ステップ 5 （任意） 別のルールを追加するには、プラス記号をクリックします。

（注） ルールを削除するには、[x] をクリックします。

ステップ 6 （任意） ルールの順序を変更するには、変更したい順序でルールをドラッグ アンド ドロップします。

ステップ 7 [Deploy] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの [ステータス（Status）] は、[展開済み（DEPLOYED）] として表示されます。[ポリシー名（Policy Name）] の横にあるワイヤレス アイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセス コントロール ポリシーの編集または削除

必要な場合は、IP ベースのアクセス コントロール ポリシーを変更または削除できます。

（注） ポリシーを編集すると、[IPベースのアクセスコントロールポリシー（IP-Based Access Control Policies）] ウィンドウのポリシーの状態が [変更（MODIFIED）] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開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**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 編集または削除するポリシーの横にあるチェック ボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集（Edit）]をクリックします。完了したら、[Save]をクリックします。フィールドの定義については、IP ベースのアクセス コントロール ポリシーの作成 （297 ページ）を参照してください。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

ステップ 3 ポリシーを変更した場合は、ポリシー名の横にあるチェック ボックスをオンにして [展開（Deploy）] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセス コントロール ポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開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**[Policy]** > **[IP Based Access Control]** > **[IP Based Access Control Policies]** の順に選択します。

ステップ 2 展開するポリシーを探します。

ステップ 3 ポリシーの横にあるチェック ボックスをオンにします。

ステップ 4 [Deploy] をクリックします。
ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ 5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、**[今すぐ実行（Run Now）]** ラジオ ボタンをクリックし、**[適用（Apply）]** をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシー

Quality of Service（QoS）とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoS を設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高い Quality of Experience（QoE）の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Cisco DNA Center のアプリケーション ポリシーを使用してネットワークに設定できます。アプリケーション ポリシーは、次の基本的なパラメータで構成されています。

- [Application Sets]：同様のネットワークトラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design（CVD）に基づいて 3 つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせてより詳細に調整できます。
- [Site Scope]：アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。

Cisco DNA Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Cisco DNA Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。

（注） Cisco DNA Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーション ポリシーでの CVD ベースの設定

アプリケーション ポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design（CVD）に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテ

ストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition』（http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694）で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- シスコ検証済みデザイン（CVD）
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

サイトの範囲

サイト範囲は、アプリケーションポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレスデバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレス デバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルの RF 干渉、輻輳、ネットワーク デバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメントにセグメントごとのポリシーを適用できるすることで、優先順位の高いトラフィックが受ける、ワイヤレス ネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連のグループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーション セットを分類します。

ビジネス関連グループ（ビジネス関連、デフォルト、ビジネスと無関係）は、基本的に 3 種類のトラフィック（高優先順位、ニュートラル、低優先順位）にマッピングされます。

- **ビジネス関連（Business Relevant）**：（高優先トラフィック）このグループのアプリケーションは組織の目的に直接関与し、音声、ビデオ、ストリーミング、コラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズ リソース アプリケーション、電子メール、ファイル転送、コンテンツ配布など、さまざまな種類があります。ビジネス関連として指定されているアプリケーションは、Internet

Engineering Task Force（IETF）RFC 4594 の規定に従い、業界推奨のベスト プラクティスに従って処理されます。

- **デフォルト（Default）**：（平均的優先度のトラフィック）このグループは、ビジネスに関連している場合もあればしていない場合もあるアプリケーションを対象としています。たとえば一般的な HTTP または HTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィック フローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **ビジネスと無関係（Business Irrelevant）**：（低優先トラフィック）このグループは、組織の目的達成に寄与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテイメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーション セットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、（デフォルトでは）YouTubeはビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミング ビデオ アプリケーション セットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた（特定の a から b へのトラフィック フローが作成された）ときにトラフィックが特定の方法で処理されるように、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーション トラフィックの送信元。たとえば、クライアント/サーバー アーキテクチャでは、トラフィック フローは主にサーバーからクライアントの方向であるため、アプリケーション サーバーがプロデューサと見なされます。ピアツーピア アプリケーションの場合は、リモート ピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーション トラフィックの受信者。コンシューマに該当するのは、クライアント/サーバー アーキテクチャの場合はクライアント エンドポイント、ピアツーピア アプリケーションの場合はローカル デバイスなどです。コンシューマはエンドポイント デバイスであることがありますが、場合によっては、そのようなデバイスの特定のユーザーであることもあります（通常、IPアドレスまたは特定のサブネットによって識別

される）。また、あるアプリケーションが別のアプリケーション トラフィック フローのコンシューマになる場合もあります。

このような関係を設定することにより、このシナリオに一致するトラフィックに特定のサービス レベルを設定することが可能になります。

マーキング、キューイング、ドロッピングの処理

Cisco DNA Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロッピングをベースとしています。Cisco DNA Center は、デフォルト カテゴリのすべてのアプリケーションをデフォルトの転送アプリケーション クラスに割り当て、無関係なビジネス カテゴリのすべてのアプリケーションをスカベンジャ アプリケーション クラスに割り当てます。関連するビジネス カテゴリのアプリケーションについては、Cisco DNA Center はアプリケーションのタイプに基づいてトラフィック クラスをアプリケーションに割り当てます。次の表に、アプリケーション クラスとそれぞれの処理を示します。

表 *43* : マーキング、キューイング、ドロッピングの処理

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
該当する	VoIP[3]	Expedited Forwarding（EF）	プライオリティキューイング（PQ）	VoIP テレフォニー（ベアラのみ）トラフィック。たとえば、Cisco IP 電話。
	ブロードキャストビデオ	クラス セレクタ（CS）5	PQ	ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミング メディア フロー（Cisco IP Video Surveillance や Cisco Enterprise TV など）。（非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローを意味します。）
	リアルタイムインタラクティブ	CS4	PQ	非弾性の高解像度インタラクティブ ビデオ アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco TelePresence など）。
	マルチメディア会議	相対的優先転送（AF）41	帯域幅（BW）キューと Differentiated Services Code Point（DSCP）Weighted Random Early Detect（WRED）	デスクトップソフトウェアのマルチメディア コラボレーションアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco Jabber や Cisco WebEx など）。
	マルチメディア ストリーミング	AF31	BW キューと DSCP WRED	ビデオオンデマンド（VoD）ストリーミング ビデオフローおよび仮想デスクトップアプリケーション。たとえば、Cisco Digital Media System。
	ネットワーク制御	CS6	BW キューのみ[4]	EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズネットワークの信頼性の高い運用のために必要とされるネットワーク コントロール プレーン トラフィック。
	シグナリング	CS3	BW キューと DSCP	IP 音声およびビデオ テレフォニー インフラストラクチャのコントロールプレーン トラフィック。
	Operations, Administration, and Management（OAM）	CS2	BW キューと DSCP[5]	SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック
		AF21		

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
	トランザクションデータ（低遅延データ）		BW キューと DSCP WRED	エンタープライズ リソース プランニング（ERP）、顧客関係管理（CRM）、およびその他のデータベース アプリケーションなどのインタラクティブ（フォアグラウンド）データ アプリケーション。
	バルクデータ（高スループットデータ）	AF11	BW キューと DSCP WRED	電子メール、File Transfer Protocol（FTP）、バックアップ アプリケーションなどの非インタラクティブ（バックグラウンド）データ アプリケーション。
デフォルト	デフォルトの転送（ベストエフォート）	DF	デフォルト キューと RED	デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービス クラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。
非関連	スカベンジャー	CS1	最小 BW キュー（ディファレンシャル）と DSCP	非ビジネス関連のトラフィック フロー、およびビジネス関連でないグループに割り当てられているアプリケーション（エンターテイメント向けのデータやメディア アプリケーションなど）。たとえば、YouTube、Netflix、iTunes、Xbox Live。

[3] VoIP シグナリング トラフィックは、コール シグナリング クラスに割り当てられます。
[4] ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。
[5] OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービス プロバイダのプロファイル

サービス プロバイダ（SP）プロファイルは、特定の WAN プロバイダのサービス クラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーション ポリシーがデバイスに展開されると、各 SP プロファイルには、各 SP クラスを DSCP 値と帯域幅割り当てのパーセンテージにマップする特定のサービス レベル契約（SLA）が割り当てられます。

アプリケーション ポリシーを設定するときに SP プロファイルの DSCP 値と 帯域幅割り当てのパーセンテージをカスタマイズできます。

SPプロファイルを作成したら、そのプロファイルをWANインターフェイスで設定する必要があります。

表 *44 : 4* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
デフォルト	0	—	—	31

表 *45 : 5* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
クラス 3 データ	AF11	—	—	1
デフォルト	ベスト エフォート	—	—	30

表 *46 : 6* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 1 データ	AF31	—	—	10
クラス 3 データ	AF11	—	—	1
ビデオ	AF41	—	—	34
音声	EF	はい	10	—
デフォルト	0	—	—	30

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 2 データ	AF21	—	—	25

表 *47 : 8* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
ネットワーク-コントロール管理	CS6	—	—	5
ストリーミング ビデオ	AF31	—	—	10
コール シグナリング	CS3	—	—	4
スカベンジャー	CS1	—	—	1
インタラクティブ ビデオ	AF41	—	—	30
音声	EF	はい	10	—
デフォルト	0	—	—	25
重要なデータ	AF21	—	—	25

キューイング プロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。

（注） キューイングプロファイルは、サービスプロバイダプロファイルに接続されているWAN側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Cisco DNA Center は、より低いインターフェイス速度でインターフェイスを取り扱います。

（注） Cisco DNA Centerは、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチ ポートが管理上ダウンしている場合、Cisco DNA Center は速度を検出できません。この場合、Cisco DNA Centerは、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーション ポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーション ポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーション ポリシーのキューイング ポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

キューイング ポリシーに関する次の追加の注意事項および制約事項に注意してください。

- LANキューイングプロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイングプロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィック クラス キューイングをカスタマイズしても、シスコのサービス プロバイダ スイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Cisco DNA Center を使用することなく実施します。

表 *48 :* デフォルト *CVD LAN* キューイング ポリシー

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[6]
ビジネス関連の音声	10%
ビジネス関連のブロードキャストビデオ	10%
ビジネス関連のリアルタイム インタラクティブ	13%
ビジネス関連のマルチメディア会議	10%

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[6]
ビジネス関連のマルチメディア ストリーミング	10%
ビジネス関連のネットワーク制御	3%
ビジネス関連のシグナリング	2%
ビジネス関連の OAM	2%
ビジネス関連のトランザクションデータ	10%
ビジネス関連のバルクデータ	4%
ビジネス関連のスカベンジャ	1%
ビジネス関連のベストエフォート	25%

[6] 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブ トラフィック クラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト（ACL）および ACE を格納するためのメモリ（TCAM と呼ばれる）が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Cisco DNA Center は次の順序で TCAM スペースを割り当てます。

1. [Rank]：カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号（ただし既存のデフォルトNBARアプリケーションは除く）。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。

（注）
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
- NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。

2. [Traffic Class]：優先順位は次の順序に基づいています。シグナリング、バルクデータ、ネットワーク制御、Operations Administration Management（Ops Admin Mgmt）、トランザクショ

ンデータ、スカベンジャ、マルチメディアストリーミング、マルチメディア会議、リアルタイム インタラクティブ、ブロードキャストビデオ、VoIP テレフォニー。

3. [Popularity]：CVD の基準に基づいて割り当てられた番号（1 ～ 10）。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。

（注）
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
- デフォルト NBAR アプリケーションには、CVD の基準に基づいてポピュラリティ番号（1 ～ 10）が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません（ランクのみ変更されます）。

4. [Alphabetization]：2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを指定したポリシーを定義する場合を想定しましょう。

- カスタム アプリケーション custom_realtime。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション custom_salesforce。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- corba-iiop という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 9 が付与されています。
- gss-http という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルト NBAR アプリケーションにはランクはありませんが、トラフィック クラスと（CVD に基づいて）デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

アプリケーションの設定順	理由
1. カスタム アプリケーション custom_realtime	カスタム アプリケーションには最も高い優先順位が付与されます。custom_salesforce アプリケーションと custom_realtime アプリケーションのランクおよびポピュラリティが同じであるとすると、これらのアプリケーションはアルファベット順にソートされ、custom_realtime が custom_salesforce より前になります。
2. カスタム アプリケーション custom_salesforce	

アプリケーションの設定順	理由
3. お気に入りのアプリケーション gss-http	これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Cisco DNA Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は、Ops Admin Mgmt トラフィック クラスであるため、先に処理され、その後にトランザクションデータ トラフィック クラスの corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。
4. お気に入りのアプリケーション corba-iiop	
5. 他のすべてのデフォルト NBAR アプリケーション	他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

（注） ポリシーを保存または展開した後に、名前を変更することはできません。

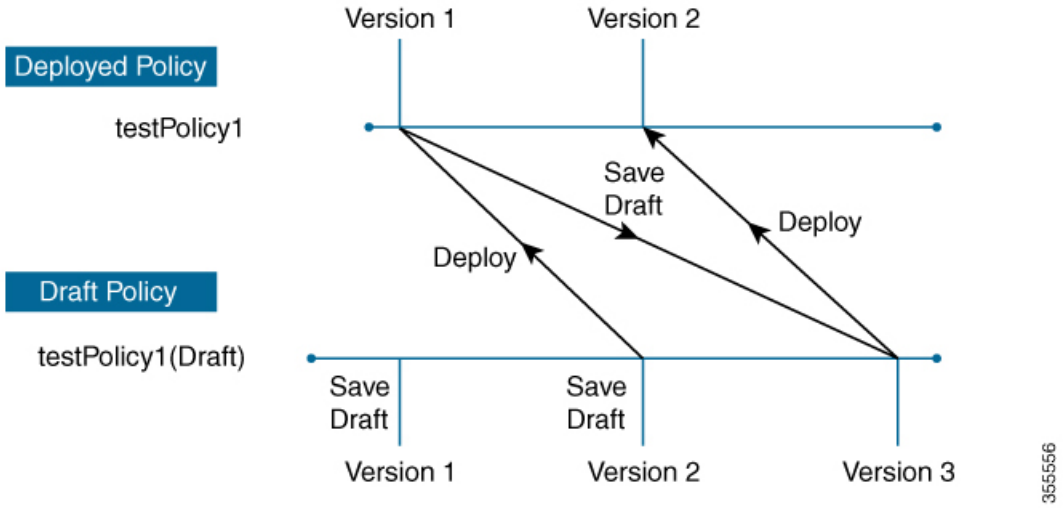
ドラフトポリシーと展開したポリシーは相互に関連付けられますが、それぞれ独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Cisco DNA Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Cisco DNA Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、次の図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフトポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 *8*: 展開したポリシーとドラフト ポリシーのバージョン管理



ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフト ポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシー バージョンの履歴表示と以前のバージョンへのロール バックについては、ポリシーのバージョン管理 （313 ページ）を参照してください。

ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用される CLI を生成できます。

プレビュー操作では、ポリシーのCLIコマンドが生成され、デバイスの実行コンフィギュレーションのCLIコマンドと比較され、デバイスでポリシーを設定するのに必要な残りのCLIだけが返されます。

プレビュー出力の確認後、範囲内の全デバイスにポリシーを展開するか、ポリシーの変更を続行することができます。

ポリシーの事前チェック

アプリケーションポリシーを作成するとき、ポリシーを展開する前に、サイト範囲のデバイスでサポートされるかどうかを確認できます。事前チェック機能では、デバイス タイプ、モデル、ライン カード、およびソフトウェア イメージが作成したアプリケーション ポリシーをサポートするかどうかチェックします。これらのコンポーネントのいずれかがサポートさCisco DNA Centerれていない場合、はデバイスの障害を報告します。Cisco DNA Centerまた、障害を修正する方法についても説明します。これらの対応で障害が修正されない場合、サイト範囲からデバイスを削除できます。

アプリケーション ポリシーをそのまま展開すると、事前チェック プロセス中に障害が報告されたデバイスでポリシー展開が失敗します。失敗を回避するには、サイト範囲からデバイスを削除するか、デバイス コンポーネントをアプリケーション ポリシーがサポートするレベルに更新します。サポート対象デバイスのリストについては、Cisco DNA Center のサポート対象デバイスドキュメントを参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。

（注） スケジュール イベントが発生すると、ポリシーは、さまざまなポリシー コンポーネント（アプリケーション、アプリケーションセット、およびキューイング プロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットは Cisco DNA Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーションセットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。

（注） ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーション セット メンバー、LAN キューイング プロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Cisco DNA Centerは、デバイスの元のCisco Modular QoS CLIポリシー設定をデタッチしますが、それらはデバイス上に残ります。Cisco DNA Centerは、デバイスの元のNBAR設定をCisco DNA Centerに保存します。このアクションにより、必要に応じてオリジナルのモジュラー式QoS CLIポリシーとNBAR設定を後でデバイスに復元することが可能になります。

（注） このようにモジュラー式QoS CLIポリシーはデバイスから削除されませんが、ユーザーがこれらのポリシーを削除すると、元のポリシー復元するCisco DNA Centerの機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Cisco DNA Centerは、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーション ポリシーを展開する前に存在していたモジュラー式QoS CLIポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤ スイッチング（MLS）設定などのキューイング ポリシーは復元されません。代わりに、デバイスは、Cisco DNA Centerによって最後に適用されたMLS設定を維持します。

元のポリシー設定をデバイスに復元すると、Cisco DNA Centerに保存されているポリシーが削除されます。

この機能には、次のような追加のガイドラインと制限事項があるので、注意してください。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Cisco DNA Centerは、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Cisco DNA Centerは、ポリシーを自動的に削除したり、デバイスのQoS設定を元の(事前Cisco DNA Center)設定に復元したりしません。

陳腐化したアプリケーション ポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーション ポリシーを再展開する必要があります。

アプリケーション ポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- SPプロファイルの割り当て、WANサブ回線のレート、WANまたはLANマーキングなどのインターフェイスの変更。
- キューイング プロファイルの変更。

- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識（CBAR）ステータスの変更。

アプリケーション ポリシーのガイドラインと制限事項

- Cisco DNA Center Cisco DNA Center は、ワイヤレスコントローラ（WLC）上で同じ SSID 名を使用して複数のワイヤレス LAN（WLAN）を学習することはできません。WLC には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Cisco DNA Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

  WLC ごとに重複する SSID 名を意図的に持つことも、Cisco DNA Center を使用して重複する SSID 名を持つ WLC を誤って追加してしまうこともあります。いずれの場合も、WLC ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

  - [Learn Config]：Cisco DNA Center は WLC ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。（[設定の学習（Learn Config）] は、通常はブラウンフィールド シナリオで使用されます）。
  - [Application Policy]：Cisco DNA Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストレーン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
  - [Multiscale Network]：MULTISCALE ネットワークでは、複数のデバイスの複数の重複する SSID 名が原因で問題が発生することもあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、[設定の学習（Learn Config）] を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Cisco DNA Center が非ファブリック SSID 名を持つデバイスに対して操作を実行しようとする場合に競合が生じることがあります。
  - [IPACL Policy]：Cisco DNA Center は、IPACL ポリシーの展開時に、重複する SSID のいずれか 1 つにのみランダムにポリシーを適用します。また、Flex Connect が関係するシナリオも影響を受けます。

- Cisco DNA Center では、デバイス設定に対するアウト オブ バンド（OOB）の変更は推奨されません。OOB に変更を加えると、Cisco DNA Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Cisco DNA Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。

- QoS trust 機能は変更できません。
- ワイヤレスコントローラではカスタムアプリケーションはサポートされていません。したがって、ワイヤレス アプリケーション ポリシーの作成時はカスタムアプリケーションは選択されません。
- 設計から SSID を削除してワイヤレスコントローラを再プロビジョニングする前に、対応するワイヤレス アプリケーション ポリシーを必ず削除してください。
- eWLC のワイヤレスアプリケーションは、学習された設定からプロビジョニングされた SSID ではサポートされません。

（注） Cisco DNA Center では、AireOS および eWLC プラットフォームの FlexConnect ローカルスイッチングモードはサポートされていません。

アプリケーション ポリシーの管理

ここでは、アプリケーション ポリシーの管理の方法に関する情報について説明します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件を満たしていることを確認してください。

- Cisco DNA Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートします。お使いのネットワーク内でデバイスとソフトウェアバージョンがサポートされているかどうかを確認するには、*Cisco DNA Center* のサポート対象デバイス を参照してください。
- ISR-G2、ASR 1000、ワイヤレス LAN コントローラなど、シスコのネットワーク デバイスに AVC（Application Visibility and Control）機能のライセンスがインストールされていることを確認します。詳細については、「*NBAR2 (Next Generation NBAR) Protocol Pack FAQ*」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、IOS XE バージョン 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS 設定のスイッチを IOS XE バージョン 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Cisco DNA Center で特定するには、インターフェイス タイプ（WAN）および（必要に応じて）副回線レートとサービス プロバイダのサービス クラス モデルを指定する必要があります。詳細については、サービス プロバイダ プロファイルの WAN インターフェイスへの割り当て （331 ページ）を参照してください。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳

細については、デバイスのロールの変更（インベントリ） （84 ページ）を参照してください。

アプリケーション ポリシーの作成

ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。例えば、ネットワーク応答時間を最短化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスのロールの変更（インベントリ） （84 ページ）を参照してください。
- サイトへのデバイスの追加詳細については、「デバイスをサイトに追加する （80 ページ）」を参照してください。
- SP 向けのトラフィック用に対してこのポリシーを SP プロファイルで設定する場合は、SP プロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後に SP プロファイルに戻り、SLA 属性をカスタマイズして SP プロファイルを WAN インターフェイスに割り当てます。詳細については、サービス プロバイダ プロファイルの設定 （203 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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [アプリケーション ポリシー名（Application Policy Name）] フィールドに、ポリシーの名前を入力します。

ステップ 4 [有線（Wired）] または [ワイヤレス（Wireless）] ラジオ ボタンのいずれかを選択します。

ステップ 5 ワイヤレスネットワークの場合は、[SSID] ドロップダウンリストからプロビジョニングされた SSID を選択します。

ステップ 6 [サイトの範囲（Site Scope）] をクリックし、展開するポリシーの横にあるチェック ボックスをオンにします。

（注） 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じ SSID で別のポリシーに割り当て済みのサイトを選択することができません。

ステップ 7 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。

a) [サイトの範囲（Site Scope）] ペインで、興味のあるサイトの横にある ⚙ をクリックします。

選択した範囲内のデバイスのリストが表示されます。

b) 除外するデバイスを見つけ、関連する [ポリシーの除外（Policy Exclusions）] 列にあるトグル ボタンをクリックします。

c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。

d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

e) [< Back to Devices in *Site-Name*] をクリックします。

f) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 8 WAN デバイスでは、特定のインターフェイスを設定できます。

a) [Site Scope] ペインで、目的のサイトの横にある ⚙ をクリックします。

b) サイトのデバイスのリストで、目的のデバイスの横にある [SP Profile Settings] 列の [Configure] をクリックします。

（注） このオプションは、ルータの場合にのみ使用可能です。

c) [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

d) [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- 物理インターフェイス：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- トンネルインターフェイス：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

e) [サービス プロバイダ プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン リストから SP プロファイルを選択します。

f) （任意） 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

g) （任意） 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ～ f を繰り返します。

h) **[Save]** をクリックします。

i) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 9 [サイトの範囲（Site Scope）] ペインで、[OK] をクリックします。

ステップ 10 （任意） Cisco Validated Design（CVD）キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

a) [キューイング プロファイル（Queuing Profiles）] をクリックします。
b) 左ペインのリストから、キューイング プロファイルを選択します。
c) [Select] をクリックします。

ステップ 11 （任意） このポリシーが SP 向けトラフィックである場合は、SP プロファイルの SLA 属性をカスタマイズします。

a) [SP プロファイル（SP Profile）] をクリックします。
b) SP プロファイルを選択します。
c) SLA 属性をカスタマイズします（[DSCP]、[SP 帯域幅（%）（SP Bandwidth %）]、および [キューイング帯域幅（%）（Queuing Bandwidth %）]）。

ステップ 12 （任意） ネットワークで使用されるアプリケーション セットのビジネスとの関連性を設定します。

Cisco DNA Center には、ビジネス関連性グループに事前設定されたアプリケーション セットが付属しています。あるビジネス関連性グループから別のグループにアプリケーションセットをドラッグアンドドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。

ステップ 13 （任意） コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

a) アプリケーション グループを展開します。
b) 目的のアプリケーションの横にある歯車アイコン ⚙ をクリックします。
c) [トラフィックの方向（Traffic Direction）] エリアで、[単方向（Unidirectional）] または [双方向（Bi-directional）] ラジオ ボタンを選択します。
d) 既存のコンシューマを選択するには、[コンシューマ（Consumer）] ドロップダウン リストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加（+ Add Consumer）] をクリックして、[コンシューマ名（Consumer Name）]、[IP/サブネット（IP/Subnet）]、[プロトコル（Protocol）]、および [ポート/範囲（Port/Range）] を定義します。
e) [OK] をクリックします。

ステップ 14 ホスト トラッキングを設定します。[ホスト トラッキング（Host Tracking）] トグル ボタンをクリックして、ホスト トラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Cisco DNA Center では、コラボレーション エンドポイント（テレプレゼンスユニットやシスコ電話など）が接続されているスイッチに、ACL のエントリを自動的に適用します。

ACE は、コラボレーション エンドポイントによって生成された音声およびビデオトラフィックを照合し、音声およびビデオトラフィックが正しくマークされるようにします。

ホストトラッキングがオンの場合、Cisco DNA Center はサイトの範囲内でコラボレーション エンドポイントの接続をトラッキングし、コラボレーション エンドポイントがネットワークに接続されるか、1 つ

のインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホストトラッキングが終了すると、Cisco DNA Center は、コラボレーション エンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、コラボレーションエンドポイントで正しく設定されるように、ACL のポリシーを再展開する必要があります。

ステップ 15 （任意） デバイスに送信される CLI コマンドをプレビューします。詳細については、「アプリケーション ポリシーのプレビュー （326 ページ）」を参照してください。

ステップ 16 （任意） ポリシーを展開するデバイスを事前にチェックします。詳細については、「アプリケーション ポリシーの事前チェック （327 ページ）」を参照してください。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （311 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに展開するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （313 ページ）を参照してください。

  （注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーションポリシー情報の表示

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを名前で並べ替えたり、名前、ステータス、キューイング プロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、それぞれに関する次の情報が表示されます。

- [Policy Name]：ポリシーの名前。

- [Version]：ポリシーの反復。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、ポリシーのドラフト （311 ページ）およびポリシーのバージョン管理（313 ページ）を参照してください。
- [Policy Status]：ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9000 デバイスに適用されたポリシーがポートチャネルの更新（作成/変更/削除）によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- [Deployment Status]：最新の展開の状態（デバイスごと）。次の概要を示します。
  - 正常にプロビジョニングされたデバイス
  - プロビジョニングに失敗したデバイス
  - 展開が終了したためにプロビジョニングされなかったデバイス。

  最新の導入の状態をクリックすると、[ポリシーの展開（Policy Deployment）] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。デバイスごとに、次の情報が表示されます。
  - デバイスの詳細（名前、サイト、タイプ、ロール、および IP アドレス）
  - 成功した導入のステータス。ステータスの横にある歯車のアイコンをクリックすると、[Effective Marking Policy] ウィンドウが開き、[Business Relevant] および [Business Irrelevant] アプリケーションと、それらが最終的に渡されるトラフィッククラスキューが表示されます。TCAM リソースまたは古いNBAR プロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
  - 障害ステータスには、障害の理由が示されます。
- [Scope]：ポリシーに割り当てられているサイト（デバイスではなく）の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。
- [LAN Queuing Profile]：ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーション ポリシーの編集

アプリケーション ポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 対応するポリシーの横にあるラジオ ボタンをクリックします。

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

ステップ 5 必要に応じて、アプリケーション ポリシーを変更します。

ステップ 6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、アプリケーション ポリシーの作成 （317 ページ）を参照してください。

ステップ 7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ 8 [Select] をクリックします。

ステップ 9 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （311 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。詳細については、ポリシーのスケジューリング （313 ページ）を参照してください。

  （注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを作成、編集、または複製します。

ステップ 3 [ドラフトの保存（Save Draft）] をクリックします。

詳細については、ポリシーのドラフト （311 ページ）を参照してください。

アプリケーション ポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再展開する必要があります。

（注） IOS バージョン 16.x 以降を搭載した Cisco Catalyst 3850、Catalyst 3650、および Catalyst 9000 デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

カスタムアプリケーションの作成後、デバイスに関してCBARが有効になっている場合、そのデバイスでカスタムアプリケーションが自動的に設定されます。デバイスにアプリケーションポリシーを展開する前に、最新のアプリケーションレジストリへの同期の完了を待つ必要があります。**Provision** > **Services** > **Service Catalog** > **Application Visibility** で同期ステータスを確認することができます。

デバイスに関してCBARが有効になっている場合は、カスタムアプリケーションがCBARを介して設定されるため、アプリケーションポリシーの展開時には属性セットおよびマップだけがデバイスで設定されます。

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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[導入（Deploy）] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のいずれかの適切なアクションを選択します。

- デバイスからポリシーを削除する（推奨）
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスをブラウンフィールド設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（RunNow）]ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

ポリシー導入のキャンセル

[導入（Deploy）] をクリックすると、Cisco DNA Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いが見つかった場合は、ポリシーの展開をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に40台のデバイスが設定されます。デバイスが 40 台以下の場合にポリシーの展開をキャンセルしても、デバイスの最初のバッチへの展開がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシーの展開をキャンセルできます。

[中止（Abort）] をクリックすると、Cisco DNA Center によって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止（Policy Aborted）] に変更されます。Cisco DNA Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態（設定中、成功、または失敗）が反映されます。

ポリシー導入中に [中止（Abort）] をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーション ポリシーの削除

不要になったアプリケーション ポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレスポリシー プロファイルの関連付けが削除されます。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 削除するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 削除するポリシーの横にあるラジオ ボタンを選択します。

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

ステップ 5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[Cancel] をクリックします。

ステップ 7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[Application Policies] ページで、ポリシーの削除ステータスを確認できます。ステータスに [deletion failed] と表示された場合は、次の手順を実行します。

a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。

b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーション ポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーで必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 複製するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 複製するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[複製（Clone）] を選択します。

ステップ 5 必要に応じてアプリケーションポリシーを設定します。アプリケーションポリシーの設定については、アプリケーション ポリシーの作成 （317 ページ）を参照してください。

ステップ 6 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （311 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （313 ページ）を参照してください。

  （注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーション ポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Cisco DNA Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

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

ステップ 5 [Undeploy Policy] ウィンドウで、[Restore devices to original configurations] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

[Application Policies] ページで、ポリシーの復元ステータスを確認できます。ステータスに [restoration failed] と表示された場合は、次の手順を実行します。

a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーション ポリシーをリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD 設定の詳細については、アプリケーション ポリシー （300 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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

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

ステップ 5 [シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

ステップ 7 次のいずれか 1 つのタスクを実行します。

- ポリシーのドラフトを保存するには、[ドラフトの保存（Save Draft）] をクリックします。
- ポリシーを展開するには、[展開（Deploy）] をクリックします。

アプリケーション ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用する CLI を生成して設定をプレビューできます。

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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （317 ページ）またはアプリケーション ポリシーの編集 （321 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 ポリシーを展開する前に、[プレビュー（Preview）] をクリックします。

範囲内のデバイスのリストが表示されます。

ステップ 4 対象のデバイスの横にある [生成（Generate）] をクリックします。

Cisco DNA Center により、ポリシーの CLI が生成されます。

ステップ 5 [表示（View）] をクリックして CLI を表示するか、CLI をクリップボードにコピーします。

アプリケーション ポリシーの事前チェック

アプリケーションポリシーを展開する前に、サイト範囲内のデバイスがサポート対象であるかどうかをチェックできます。事前チェック プロセスには、デバイスのモデル、ライン カード、およびソフトウェア イメージの検証が含まれます。

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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （317 ページ）またはアプリケーション ポリシーの編集 （321 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 [事前チェック（Pre-check）] をクリックします。

Cisco DNA Center は、デバイスをチェックして、問題があれば [事前チェック結果（Pre-Check Result）] 列に内容を報告します。[Errors] タブには、このポリシーをサポートしていないデバイスが表示されます。[Warnings] タブには、デバイスにこのポリシーを展開することを選択した場合に、サポートされていない制限や機能が表示されます。[Warnings] タブに一覧表示されているデバイスのポリシーを展開することもできます。問題を解決するには、Cisco DNA Center のサポート対象デバイスに記載されている仕様にデバイスを準拠させます。

アプリケーション ポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号（反復）と、バージョンが保存された日付と時刻が含まれています。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[履歴（History）] を選択します。

ステップ 4 [ポリシー履歴（Policy History）] ダイアログボックスでは、次のことを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異（Difference）] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック（Rollback）] をクリックします。

ポリシーの以前のバージョンにロール バック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で 5 バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも 2 つのポリシーバージョンを作成しておく必要があります。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。

選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン（最も大きい番号）が一覧の最上部に表示され、最も古いバージョン（最も小さい番号）が最下部に表示されます。

ステップ 4 （任意） 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。

ステップ 5 ロールバックする先のポリシー バージョンを決定した場合、そのポリシー バージョンに対して [Rollback] をクリックします。

（注） 選択したサイトの範囲がポリシー バージョン間で変更された場合、ロールバックは選択されている現在（最新）のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。

ステップ 6 [OK] をクリックして、ロールバック手順を確定します。

ロールバック先のバージョンが最新バージョンになります。

キューイング プロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイング プロファイルの作成

Cisco DNA Center では、デフォルトの CVD キューイング プロファイル（CVD_QUEUING_PROFILE）を提供します。このキューイングプロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成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**[Policy]** > **[Application QoS]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [Add Profile] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダを使用して各トラフィック クラスに帯域幅を設定します。プラス記号（+）またはマイナス（-）記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーション クラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1 つのアプリケーション クラスに帯域幅を追加すると、別のアプリケーション クラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーション クラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーション クラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 （高度なユーザー向け）Cisco DNA Center が各トラフィック クラスで使用する DSCP コード ポイントをカスタマイズするには、[表示（Show）] ドロップダウン リストで、[DSCP値（DSCP Values）] を選択し、フィールドに特定の数値を入力して、各アプリケーション クラスの値を設定します。

SP のクラウド内で必要な DSCP コード ポイントをカスタマイズするには、SP のプロファイルを設定します。

ステップ 6 [Save] をクリックします。

キューイング プロファイルの編集または削除

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**[Policy]** > **[Application]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [キューイング プロファイル（Queuing Profile）] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存（Save）] をクリックします。フィールドの詳細については、キューイング プロファイルの作成 （329 ページ）を参照してください。
- プロファイルを削除するには、[削除（Delete）] をクリックします。

アプリケーション ポリシーによって参照されている場合は、キューイング プロファイルを削除できません。

WAN インターフェイスのアプリケーション ポリシーの管理

次のセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダ プロファイルの SLA 属性をカスタマイズ

自身のクラス モデルによって SP プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせて SP プロファイルの SLA 属性をカスタマイズすることができます。SP プロファイルのデフォルトの SLA 属性の詳細については、サービス プロバイダのプロファイル （305 ページ）を参照してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

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**[Policy]** > **[Application]** > **[Application Policies]** の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

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

ステップ 5 [SPプロファイル（SP Profiles）] をクリックし、SP プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更できます。

- [DSCP]：Differentiated Services Code Point（DSCP）値。有効値は 0 ～ 63 です。
  - Expedited Forwarding（EF）
  - クラスセレクタ（CS）：CS1、CS2、CS3、CS4、CS5、CS6
  - 相対的優先転送：AF11、AF21、AF41
  - [Default Forwarding (DF)]

  これらの DSCP 値の詳細については、マーキング、キューイング、ドロッピングの処理 （303 ページ）を参照してください。
- [SP Bandwidth %]：特定のサービスクラスに割り当てられた帯域幅の割合。
- [Queuing Bandwidth %]：各トラフィッククラスに割り当てられた帯域幅の割合。次のうちいずれかの変更を行うことができます。

- キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
- SP 帯域幅から自動的にキューイング帯域幅を計算するには、鍵アイコンをクリックしてキューイング帯域幅の設定をロックし、次に [OK] をクリックして確認します。デフォルトでは、Cisco DNA Center は、SP クラスのすべてのトラフィック クラスのキューイング帯域幅の合計がそのクラスの SP 帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に配信します。

ステップ 7 [OK] をクリックします。

サービス プロバイダ プロファイルの WAN インターフェイスへの割り当て

アプリケーション ポリシーがすでに作成済みで、SP プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスに Subline Rate の設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時に SP プロファイルを WAN インターフェイスに割り当てることができます。詳細については、「アプリケーション ポリシーの作成 （317 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**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

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

ステップ 5 [Site Scope] ペインで、対象のサイトの横にある歯車アイコンをクリックします。

ステップ 6 対象のデバイスの [SPプロファイル設定（SP Profile Settings）] 列にある [設定（Configure）] をクリックします。

ステップ 7 [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

ステップ 8 [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- **物理インターフェイス**：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- **トンネルインターフェイス**：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

ステップ 9 [サービス プロバイダー プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン フィールドをクリックし、SP プロファイルを選択します。

ステップ 10 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

ステップ 11 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ～ 10 を繰り返します。

ステップ 12 **[Save]** をクリックします。

ステップ 13 [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 14 [OK] をクリックします。

ステップ 15 [Deploy] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

ステップ 16 次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオ ボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

トラフィック コピー ポリシー

Cisco DNA Center を使用して、2 つのエンティティ間の IP トラフィック フローがモニターリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定できます。

Cisco DNA Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。

（注） トラフィック コピー ポリシーにはスケーラブル グループまたは IP ネットワーク グループのいずれかを含めることができるため、このガイド全体を通して、グループという用語を使用する場合は他に指定がなければスケーラブル グループおよび IP ネットワーク グループの両方を指します。

送信元、宛先、およびトラフィックのコピー先

Cisco DNA Center トラフィックのモニターリングプロセスを簡素化します。物理ネットワークトポロジを知っている必要はありません。必要なのは、トラフィック フローの送信元および宛先とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元（Source）]：モニターするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザー、またはアプリケーションに接続することがあります。送信元グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイーサネット、10 ギガビット イーサネット、またはポート チャネル インターフェイスのみです。
- [宛先（Destination）]：モニターするトラフィックが流れる IP サブネットです。IP サブネットはサーバー、リモート ピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先（Traffic Copy Destination）]：ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケットキャプチャ ツールまたはネットワーク分析ツールになります。

（注） 宛先では、スイッチ プローブ デバイスなどのネットワーク アナライザやその他のリモート モニターリング（RMON）プローブを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイス タイプは、イーサネット、ファストイーサネット、ギガビット イーサネット、または 10 ギガビット イーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されます。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。

（注） 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

トラフィック コピー ポリシーの注意事項と制限事項

トラフィック コピー ポリシー機能には次の制約事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Cisco DNA Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータス メッセージを表示しません。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。
- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィック コピー ポリシー設定のワークフロー

始める前に

- モニター対象にする、トラフィック コピー ポリシーで使用されている送信元スケーラブル グループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「IP ネットワーク グループの作成 （295 ページ）」を参照してください。

ステップ 1 トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、トラフィック コピーの宛先の作成 （335 ページ）を参照してください。

ステップ 2 トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、トラフィック コピー契約の作成 （335 ページ）を参照してください。

ステップ 3 トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、トラフィック コピー ポリシーの作成 （336 ページ）を参照してください。

トラフィック コピーの宛先の作成

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[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [Save] をクリックします。

トラフィック コピーの宛先の編集または削除

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[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 編集または削除する宛先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 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 宛先を削除するには、**[削除（Delete）]** をクリックします。

トラフィック コピー契約の作成

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[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 ダイアログボックスに、契約の名前と説明を入力します。

ステップ 4 **[コピー先（Copy Destination）]** ドロップダウン リストから、コピー先を選択します。

（注） コピー先は、1 つのトラフィック コピー契約に対し 1 つだけ指定できます。

選択可能なコピー先がない場合は、1 つ作成できます。詳細については、トラフィック コピーの宛先の作成 （335 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

トラフィック コピー契約の編集または削除

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[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 編集または削除する契約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 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 契約を削除するには、[削除（Delete）] をクリックします。

トラフィック コピー ポリシーの作成

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

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

ステップ 4 [説明（Description）] フィールドにポリシーを表す単語またはフレーズを入力します。

ステップ 5 [契約（Contract）] フィールドで、[契約の追加（Add Contract）] をクリックします。

ステップ 6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存（Save）] をクリックします。

ステップ 7 [使用可能なグループ（Available Groups）] エリアから、[送信元（Source）]エリアにグループをドラッグ アンド ドロップします。

ステップ 8 [使用可能なグループ（Available Groups）]エリアから、[宛先（Destination）]エリアにグループをドラッグ アンド ドロップします。

ステップ 9 [Save] をクリックします。

トラフィックコピーポリシーの編集または削除

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

ステップ 2 編集または削除したいポリシーの横のチェック ボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。

- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

第 15 章

Cisco AI エンドポイント分析

Cisco AI エンドポイント分析の概要

可視性は、エンドポイントを保護するための最初のステップです。Cisco AI エンドポイント分析は、エンドポイントと Internet of Things（IoT）デバイスの識別とプロファイリングに役立つエンドポイント可視性ソリューションです。Cisco AI エンドポイント分析エンジンを使用すると、さまざまなソースからネットワーク経由で受信したテレメトリ情報を使用して、エンドポイントにラベルを割り当てることができます。

Cisco AI エンドポイント分析で使用できるプロファイリングラベルは、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプです。これは多要素分類と呼ばれます。

Cisco AI エンドポイント分析は、潜在的に危険なエンドポイントやデバイスを特定して対処することを可能にする信頼スコアなどの機能により、ネットワークにおける繊細な可視化と処置を実現します。Cisco AI エンドポイント分析の GUI から Cisco ISE を介して ANC ポリシーを適用することにより、潜在的なリスクを管理することもできます。Cisco AI エンドポイント分析でエンドポイントのランダムおよび変更 MAC アドレスの問題をモニターして回避し、MAC アドレスの代わりに「DUID」と呼ばれる一意の属性を使用してエンドポイントを正確に識別することができます。

Cisco AI エンドポイント分析は、さまざまなソースからエンドポイントテレメトリを収集するのに役立ちます。主要なソースは、Network-Based Application Recognition（NBAR）メカニズムです。NBAR メカニズムは、Cisco Catalyst 9000 シリーズ スイッチ（アクセスデバイス）に組み込まれていて、ディープ パケット インスペクション（DPI）を実行します。Cisco AI エンド

ポイント分析は、Cisco DNA トラフィック テレメトリ アプライアンスからテレメトリを受信することもできます。

Cisco ISE、自己登録型ポータル、ServiceNow のような構成管理データベース（CMDB）ソフトウェアなど、さまざまなソースからエンドポイントコンテキスト情報を収集できます。

Cisco AI エンドポイント分析を使用すると、さまざまなネットワークデバイスからのデータインフローが可能になり、エンドポイントをより高い精度で容易に識別してプロファイリングし、異常に対処する機能が拡張されます。Cisco AI エンドポイント分析では、さまざまなエンドポイント情報を集約し、そのデータを使用してエンドポイントをプロファイリングできます。エンドポイントのプロファイリング後、AI と機械学習アルゴリズムを使用して、さまざまな方法を直感的に活用することで不明なエンドポイントの数を減らすこともできます。

Cisco AI エンドポイント分析の主な機能

- **Cisco AI エンドポイント分析ダッシュボード**

  Cisco AI エンドポイント分析ダッシュボードでは、ネットワークに接続されているエンドポイントの全体像を確認できます。既知のエンドポイント、不明なエンドポイント、プロファイリングされたエンドポイント、プロファイリングされていないエンドポイントの数を表示できます。インテリジェントなプロファイリング提案を表示して、エンドポイントのプロファイリングと管理をどのように強化できるかを確認することもできます。

- **機械学習機能を使用したネット内の不明なエンドポイントの削減**

  Cisco AI エンドポイント分析では、エンドポイントのグループ化で学習した情報に基づいてプロファイリング提案が提供されます。このような提案を使用して、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

- **システムルールおよびカスタム プロファイリング ルールによるエンドポイントの管理**

  ネットワークに接続されたエンドポイントを確実にプロファイリングおよび管理するには、シスコが提供するシステムルールと自分で設計したカスタムルールを使用します。

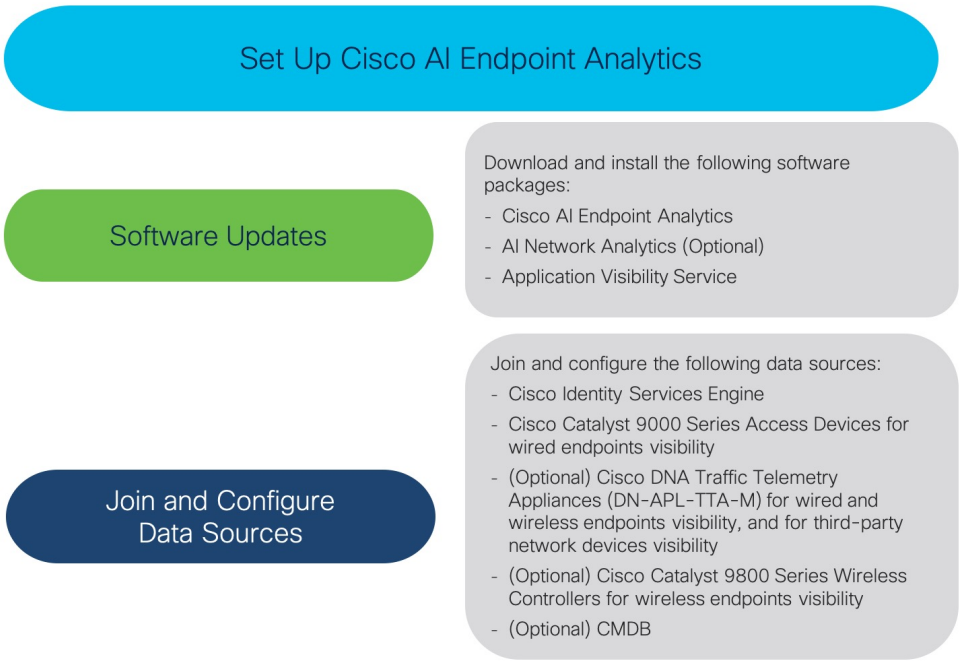
- **Cisco AI エンドポイント分析によるエンドポイントの登録**

  Cisco AI エンドポイント分析を使用して、エンドポイントをオンボードおよびプロファイリングできます。この登録プロセスでエンドポイント属性データが収集されて、エンドポイントのプロファイリングに使用されます。

- **外部ソースを使用したエンドポイントの登録**

  構成管理データベース（CMDB）などエンドポイントデータの外部ソースの中には、Cisco AI エンドポイント分析に接続できるものがあります。これにより、ネットワーク内のエンドポイントを簡単に登録、管理、およびプロファイリングできます。

Cisco DNA Center での Cisco AI エンドポイント分析のセットアップ



ソフトウェア アップデートのインストール

次の手順で説明するように、Cisco AI エンドポイント分析を使用するためのソフトウェアアップデートを Cisco DNA Center にインストールします。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[System]** > **[Software Updates]** の順に選択します。

ステップ 3 表示される [Updates] タブで、[Cisco AI Endpoint Analytics]、[AI Network Analytics]、および [Application Visibility Service] が [Application Updates] セクションにリストされているかどうかを確認してください。これらのアプリケーション更新のいずれかが表示されている場合は、[Install All] ボタンをクリックします。

- Cisco DNA Center でエンドポイント プロファイリング ソリューションにアクセスするには、[Cisco AI Network Analytics] 更新をインストールします。
- 機械学習と AI の機能を使用してインテリジェントなプロファイリング提案を受け取るには、[AI Network Analytics] 更新をインストールします。

- NBAR およびコントローラベースのアプリケーション認識（CBAR）の技術を使用してエンドポイント プロファイリングを通知するには、[Application Visibility Service] 更新をインストールします。

ステップ 4 これらの更新のいずれも [Updates] タブにリストされていない場合は、[Installed Apps] タブをクリックして、更新がすでにインストールされ、使用可能であるかどうかを確認してください。[Installed Apps] タブでは、ソフトウェアインストールが正常に完了しているかどうかも確認できます。

データ ソースの接続と有効化

（注） Cisco AI エンドポイント分析が使用するデータ ソースが、Cisco DNA Center にすでに接続されている可能性があります。データ ソースが接続されている場合は、次の手順を参照して、Cisco AI エンドポイント分析でデータ ソースを使用できることを確認します。

Cisco AI エンドポイント分析が結果を提供できるようにするには、Cisco ISE または Catalyst 9000 シリーズ アクセスデバイスを Cisco DNA Center に追加する必要があります。

1. **Cisco ISE を Cisco DNA Center に接続します。**

   『*Cisco DNA Center Appliance Installation Guide*』の「Complete First-Time Setup」にある「Integrate Cisco ISE with Cisco DNA Center」セクションを参照してください。

   次の Cisco ISE リリースが Cisco AI エンドポイント分析をサポートしています。

   - 2.4 パッチ 11 以降
   - 2.6 パッチ 5 以降
   - 2.7 パッチ 1 以降
   - 3.0 以降のリリース

   Cisco ISE 管理ポータルで、次の手順を実行します。

   1. **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
   2. [Endpoint Analytics Settings] エリアで、次のチェックボックスをオンにします。
      - [Publish Endpoint Attributes to AI Endpoint Analytics]
      - [Consume Endpoint Profiles from AI Endpoint Analytics]

   Cisco ISE が 802.1X または MAB 認証方式でエンドポイントを認証すると、収集されたエンドポイント属性が Cisco AI エンドポイント分析で使用可能になります。

2. **有線エンドポイントが表示されるように、Cisco 9000 シリーズ アクセス デバイスを Cisco DNA Center に接続します。**

   『*Cisco DNA Center User Guide*』の「Discover Your Network」を参照してください。

Cisco AI エンドポイント分析の機能を有効にするには、Cisco 9000 シリーズ アクセスデバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードします。

必要なアクセスデバイスの CBAR を有効にするには、Cisco DNA Center で [Menu] アイコン（☰）をクリックします。

1. **[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
2. データが必要な Cisco Catalyst 9000 アクセスデバイスを選択します。[Site Devices] セクションのデバイス名の横にあるチェックボックスをオンにします。
3. [Enable CBAR] をクリックします。

3. **（任意）ワイヤレスエンドポイントを可視化するには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Center に接続します。**

次の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ モデルが、Cisco AI Endpoint Analytics の非ファブリックモードでサポートされています。

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 （405 ページ） でCisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定およびプロビジョニングするには、Cisco DNA Centerを参照してください。

4. **（任意）有線およびワイヤレスエンドポイントを可視化し、サードパーティのネットワークデバイスを可視化するには、Cisco DNA トラフィック テレメトリ アプライアンスを Cisco DNA Center に接続します。**

Cisco DNA トラフィック テレメトリ アプライアンス（DN-APL-TTA-M）は、ミラーリングされたネットワークトラフィックからテレメトリを生成してエンドポイントを分析できるようにします。このアプライアンスでは、Network-Based Application Recognition（NBAR）ベースでプロトコルを検査し、エンドポイント属性を抽出できます。

テレメトリアプライアンスで収集されたエンドポイント属性を Cisco AI エンドポイント分析で受信するには、Cisco ISE と Cisco DNA Center を統合する必要があります。

Cisco DNA Center でのアプライアンスのインストール、接続の構成、およびアプライアンスの管理については、『Cisco DNA Traffic Telemetry Appliances』を参照してください。

Cisco DNA トラフィック テレメトリ アプライアンスに接続されたアクセススイッチのスイッチドポートアナライザ（SPAN）受信ポートで CBAR を有効にするには、次のコマンドを使用します。

```
ip nbar protocol-discovery
```

テレメトリアプライアンスに接続されているすべてのエンドポイントが Cisco AI エンドポイント分析に表示されるわけではありません。Cisco DNA アシュアランス で管理される

ネットワーク アクセス デバイス（NAD）にも接続されているエンドポイントのみが、Cisco AI エンドポイント分析に表示されます。

5. **（任意）Cisco DNA Center で ServiceNow を有効にします。**

   ServiceNow を Cisco DNA Center に接続した後に、Cisco DNA Center の [Menu] アイコン（☰）をクリックし、**[Platform]** > **[Manage]** > **[Bundles]** を選択します。

   バンドル [Endpoint Attribute Retrieval with ITSM (ServiceNow)] の [Status] が [New] の場合は、バンドルの [Enable] をクリックします。

6. **（任意）Cisco DNA Center で Cisco AI 分析を有効にします。**

   AI ベースのエンドポイントグループ化、カスタム プロファイリング ルール自動化、およびエンドポイントラベルに関する提案を受け取るには、また、ネットワーク内のスプーフィングされている可能性のあるデバイスを検出するには、[Cisco AI Analytics] ウィンドウで、必要な設定を有効にする必要があります。

   これらの AI ベースの提案を受け取るには、AI ネットワーク分析ソフトウェアをインストールする必要があります。

   1. Cisco DNA Center のメインメニューから、**[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]** の順に選択します。
   2. 有効にする次の各サービスのトグルボタンをクリックします。

      - **AI エンドポイント分析**：AI ネットワーク分析は、機械学習を利用してネットワークのインテリジェンスを推進し、ネットワークパフォーマンスを効果的に改善して問題解決を加速できるようにします。AI ネットワーク分析は、ネットワークの動作を分析し、ネットワーク環境に適応することで、ノイズや誤検出を大幅に削減します。
      - **エンドポイント スマートグループ化**：エンドポイントスマート グループ化は、AI と機械学習を使用して、AI ベースのエンドポイントグループ化、自動化されたカスタムプロファイリングルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らします。
      - **AI スプーフィング検出**：AI スプーフィング検出は、動作モデルに基づいてスプーフィングされているエンドポイントを識別します。モデルは現在、デバイスから収集されたフロー情報を使用して構築されています。[Send data to help Cisco improve the model] トグルボタンを有効にすることにより、シスコによるデータ収集を可能にすることもできます。これにより、シスコによって動作モデルがさらに強化されます。

エンドポイント テレメトリ ソース

Cisco AI エンドポイント分析は、次の方法でテレメトリデータを受信します。

- **ディープ パケット インスペクション**

ディープ パケット インスペクションは、Cisco Catalyst 9000 シリーズ アクセス デバイスによって実行される高度なパケット分析方法です。これらのアクセスデバイスは、NBAR を実行します。NBAR は、アプリケーション トラフィックを検査し、プロトコル分析を実行して、精度の高いエンドポイントを検出および識別し、プロファイリングします。

ディープ パケット インスペクションのプロファイリングは、ネットワークへのエンドポイントトラフィックから収集されたさまざまな属性に基づいています。これらの属性は、パケットヘッダーレイヤ 4 ～ 7 から複数のプロトコルにわたって収集されます。

- **構成管理データベース接続**

  Cisco AI エンドポイント分析は、エンドポイント プロファイリングの精度を高めるために、構成管理データベース（CMDB）接続からエンドポイントデータを受信します。ServiceNow との接続により、CMDB から Cisco AI エンドポイント分析への情報を受信できます。

- **機械学習機能**

  プロファイリング用に収集されたデータは、匿名化されて、Cisco Cloud でデバイスデータレイクとして機能する場所に送信されます。ここでは、機械学習アルゴリズムで使用可能なデータを分析し、必要に応じて評価して適用できるプロファイリングルールを作成します。エンドポイント プロファイリングと管理を簡素化かつ効率化できるように、Cisco AI エンドポイント分析によってスマート プロファイリング ルールが提案されます。既存のルールも評価され、この継続学習に基づいて改善提案が提供されます。

[Cisco AI Endpoint Analytics Overview] ウィンドウ

Cisco DNA Center のメインメニューから **[Policy]** > **[AI Endpoint Analytics]** の順に選択します。

[Overview] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Missing Profiles] の 2 つのグループに分かれて表示されます。Cisco AI エンドポイント分析は、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元の 4 つの要因に基づいてエンドポイントをプロファイリングします。エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Missing Profiles] グループにプロファイリングされます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

- 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
- 以前に受け入れられていたルールの変更提案。
- 不要になったプロファイリングルールの確認。

詳細については、プロファイリングルール提案の変更（357ページ）を参照してください。

- **プロファイルラベルが欠落したエンドポイント**

  このダッシュレットには、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。表示される数は一部重複しています。たとえば、エンドポイントに OS タイプとハードウェアモデルの両方の情報がない場合、そのエンドポイントは両方のラベルの数に含まれます。

  特定のプロファイルラベルが欠落しているエンドポイントを確認するには、このダッシュレットのラベルをクリックします。[Endpoint Inventory] ウィンドウには、エンドポイントのリストが表示されます。このリストは、選択したプロファイルラベルが不明であるエンドポイントが表示されるようにフィルタ処理されます。

Endpoint Inventory

[Endpoint Inventory] タブで、データソースを介して Cisco AI エンドポイント分析に接続されているエンドポイント。このタブには、[Focus] ドロップダウンリストを使用して選択できる 2 つのビューがあります。

- [All Endpoints]：これは [Endpoint Inventory] タブのデフォルトビューです。このビューには、接続されているすべてのエンドポイントのプロファイリング情報が表示されます。

  [All Endpoints] ビューには、**エンドポイントタイプ**、**OS タイプ**、**ランダム MAC かどうか**、**信頼スコア**などのプロファイリング情報が表示されます。表示するエンドポイントのプロファイリング情報を選択するには、テーブルの右上隅にある垂直省略記号アイコンをクリックします。次のプロファイリング情報セットのいずれかを選択し、[Apply] をクリックします。

  - [All]：使用可能なすべてのプロファイリング情報が表示されます。このセットは編集できません。
  - [General]：これを選択すると、エンドポイントの全体図を確認できるプロファイリング情報が表示されます。これは、デフォルトで表示される列のセットです。このセットは編集できません。
  - [Detailed]：これを選択すると、エンドポイントを深く洞察できるプロファイリング情報が表示されます。このセットは編集できません。
  - [Custom]：これは編集可能な唯一のセットです。[Endpoint Inventory] ウィンドウに表示するプロファイリング情報をオンまたはオフにします。

必要な [View Known Profiles] ボタンをクリックして、[All Endpoints] ビューに表示されるエンドポイントのリストをフィルタ処理することもできます。**エンドポイントタイプ**、**ハードウェア製造元**、**ハードウェアモデル**、および **OS タイプ**でエンドポイントのリストをフィルタ処理できます。

- [Trust Score]：このビューでは、エンドポイント インベントリ リストがフィルタ処理され、信頼スコアが割り当てられているエンドポイントだけが表示されます。

  [Trust Score] ビューには、エンドポイントの全体的な信頼スコアを示すさまざまな要因の列が表示されます。信頼スコアは、動作異常が検出されたエンドポイントを特定するために役立ちます。これにより、エンドポイントの詳細情報を調べて、必要な修復アクションを実行することができます。低い信頼スコアを管理するためにエンドポイントに ANC ポリシーを適用する場合、[Trust Score] ビューには、適用された ANC ポリシーの名前とポリシーが適用された日時も表示されます。エンドポイントの信頼スコアを参照してください。

要件に基づいて一連のエンドポイントを簡単にフィルタ処理できます。エンドポイントを登録したり、登録済みのエンドポイントを編集、削除、およびプロファイリングしたりできます。単一または複数のエンドポイントを選択するには、MAC アドレスの横にあるチェックボックスをオンにします。これにより、選択したエンドポイントに対して、[Actions] ドロップダウンリストから特定のアクションを実行することができます。

エンドポイントのプロファイリングの完全な詳細を表示するには、エンドポイントの [MAC Address] をクリックします。表示されるスライドインダイアログボックスには、ユーザーの詳細、エンドポイントの詳細、およびエンドポイントの属性の詳細が含まれます。

[Details] タブには、Cisco DNA Center リリース 2.2.2 以降の次の新しいフィールドが Cisco ISE から受信した詳細とともに表示されます。

- [Authentication Status]：このフィールドには、エンドポイントが Cisco ISE で認証された場合は [Started]、そうでない場合は [Disconnected] と表示されます。
- [Authorization Profile]：Cisco ISE のエンドポイントに設定されている認証ポリシーがここに表示されます。
- [Scalable Group Tag]：Cisco ISE のエンドポイントに設定されたスケーラブルグループタグがここに表示されます。

これらの属性の詳細については、使用する Cisco ISE リリースの Cisco ISE 管理者ガイド [英語] を参照してください。

Cisco DNA Center リリース 2.2.2 以降では、エンドポイントの詳細を示すスライドイン ダイアログボックスに [Trust Score] タブがあります。このタブには、エンドポイントの信頼スコアを示すさまざまな要因の詳細が表示されます。エンドポイントの信頼スコアを参照してください。

Cisco DNA Center リリース 2.2.3 以降では、[Details] タブに [Previous MAC Addresses] エリアがあり、MAC ランダム化機能が有効になっているエンドポイントで使用された MAC アドレスが表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコアを参照してください。

Cisco AI エンドポイント分析データのエクスポート

このウィンドウからエンドポイントとエンドポイントの詳細のリストをエクスポートするには、[Export] をクリックします。[Endpoint Inventory] ウィンドウでフィルタを適用すると、フィルタ処理されたエンドポイントのみがエクスポート用に処理されます。すべてのエンドポイントの詳細をエクスポートするには、フィルタが適用されていないことを確認して、[Export] をクリックします。

[Export] をクリックすると、[Reports] ウィンドウで新しいタブが開きます。[Generated Reports] ウィンドウには、開始されたエクスポートのリストが表示され、リストの一番上に最新のエクスポート要求が表示されます。[Endpoint Inventory] ウィンドウから生成されたレポートの [Template Category] 列に [AI Endpoint Analytics] が含まれています。レポートの生成には数分かかります。レポートのダウンロード準備ができると、[Last Run] 列の値が [Not Initiated] から、その横にダウンロードアイコンがあるタイムスタンプに変わります。タイムスタンプは、エクスポートリストが生成された時刻を示します。ダウンロードアイコンをクリックして、エンドポイントのリストの CSV ファイルをシステムにダウンロードします。

次の手順で、[Reports] ウィンドウから Cisco AI エンドポイント分析データをエクスポートすることもできます。

（注） エンドポイントの AI エンドポイント分析データの最初のエクスポートは [Endpoint Inventory] ウィンドウから実行する必要があります。その後、[Reports] ウィンドウから直接 AI エンドポイント分析レポートを生成できます。

1. メインメニューから [Reports] を選択します。
2. [Report Templates] をクリックし、メニューから [AI Endpoint Analytics] を選択します。
3. [Generate a New Report] ダイアログボックスで [Let's Do It] をクリックします。
4. [Select Report Template] ウィンドウでは、[Endpoint Profiling] テンプレートがデフォルトで適用されています。[Next] をクリックします。
5. [Setup Report Scope] ウィンドウで、[Report Name] フィールドに値を入力します。[Endpoint Inventory] ウィンドウからエクスポートするエンドポイントのリストに適用するフィルタを定義します。すべてのエンドポイントの詳細をエクスポートするには、[Scope]エリアで値を選択しないでください。[Next] をクリックします。
6. [Select File Type] ウィンドウの [Client Details] エリアで、選択したパラメータを確認できます。関連するフィールドの横にあるチェックボックスをオンまたはオフにして、エクスポートする情報を編集します。[Next] をクリックします。
7. [Schedule Report] ウィンドウで、[Run Now]、[Run Later] （[One-Time] または [Run Recurring]）のオプションボタンをクリックします。[Run Later] の [One-Time] および [Run Recurring] オプションには、エクスポートの時間を定義するスケジューリングフィールドが表示されます。[Next] をクリックします。

8. [Delivery and Notification] ウィンドウでは、[Email Report] チェックボックスをオンにしないでください。[Next] をクリックします。
9. [Summary] ウィンドウで、このワークフローで選択したすべての設定を確認します。設定を編集するには、対応する [Edit] オプションをクリックします。[Next] をクリックします。
10. ワークフローの最後のウィンドウで、レポートが生成されていることが通知されます。生成されたレポートのリストを表示するには、このウィンドウの [View Reports] リンクをクリックします。レポートが生成され、このウィンドウに表示されるまでに数分かかります。

エンドポイントのフィルタ処理

フィルタオプションを使用すると、一連のエンドポイントを表示してアクションを実行できます。これらのエンドポイントは、プロファイリングデータ、プライマリ プロファイリング ラベル、既知のプロファイル、および正常性ステータスに基づいてフィルタ処理できます。

エンドポイントをフィルタ処理するには、次の手順を実行します。

1. [Endpoint Inventory] ウィンドウで、[Filter] をクリックします。
2. 次の各ドロップダウンリストから、値を選択します。
   - **Mac Address**
   - **エンドポイント タイプ**
   - **ハードウェア モデル**
   - **ハードウェア製造元**
   - **OS Type**
   - **登録ステータス（Registration status）**
3. [Apply] をクリックします。

また、4つのプライマリ プロファイリング ラベルで表示されるプロファイリング済みのエンドポイントをフィルタ処理することもできます。[View Known Profiles] セクションで 1 つ以上のラベルをクリックします。

エンドポイントの正常性ステータスは 5 分ごとに更新されます。次の [In Network] オプションのいずれかをクリックして、正常性ステータスに基づいてエンドポイントをフィルタ処理できます。

- [All]：正常性ステータスに関係なく、ネットワーク内のすべてのエンドポイントが表示されます。
- [Active]：ネットワークでアクティブなエンドポイントのみが表示されます。
- [Inactive]：ネットワークでアクティブでなくなったエンドポイントのみが表示されます。

属性用語集

属性用語集は、Cisco ISE プローブデータから使用可能なすべてのプロファイリング属性のリストです。

すべてのプロファイリング属性を表示するには、次の手順を実行します。

1. [Endpoint Inventory] ウィンドウで、エンドポイントの MAC アドレスをクリックします。
2. 右側に表示される新しい領域で、[View Attribute Glossary] をクリックします。

[Attribute Glossary] ウィンドウに、属性ごとに次の情報が表示されます。

- **キープロファイリング属性**
- **説明**
- **関連付けられたプロファイルラベル**
- **[Source]**
- **Dictionary**
- **ディスカバリの方法**

用語集では、すべてのプロファイリング属性の詳細ビューが表示されます。プロファイリング属性がプロファイルラベルの作成に頻繁に使用される場合は、そのラベルが [Associated Profile Labels] 列に一覧表示されます。

また、ルールの論理条件の作成中に、[Choose Attribute Condition] ウィンドウに属性用語集を表示することもできます。詳細については、「カスタムルールの作成」を参照してください。

エンドポイントの登録

新しいエンドポイントをオンボードおよびプロファイリングするには、そのエンドポイントを Cisco AI エンドポイント分析に登録します。エンドポイントのプロファイリング情報は、分類のための信頼できる情報源です。また、[Register Endpoint] オプションを使用して、登録済みのエンドポイントの新しいプロファイル情報を更新することもできます。

ステップ 1 **[Actions]** > **[Register Endpoints]** の順に選択します。

ステップ 2 [Single] または [Bulk] のいずれかのオプションボタンをクリックして、単一のエンドポイントまたは複数のエンドポイントを登録するかどうかを選択します。

オプション	手順
シングル	[MAC Address]、[Endpoint Type]、[Hardware Model]、および [Hardware Manufacturer] にエンドポイントの値を入力します。
バルク（**Bulk**）	1. [Download .csv Template] オプションをクリックして、.csvテンプレートをダウンロードします。

オプション	手順
	2. ダウンロードした .csv ファイルに、登録する必要がある各エンドポイントの詳細を入力します。具体的には、MACアドレス、エンドポイントタイプ、ハードウェアモデル、およびハードウェア製造元です。このファイルを保存します。 3. [Choose a File] オプションを使用して .csv ファイルをアップロードします。 [Bulk] オプションを使用すると、一度に最大 500 個のエンドポイントを登録できます。

ステップ 3 [Next] をクリックします。

ステップ 4 [Review Endpoint] ウィンドウでエンドポイントの詳細を確認します。変更が必要な場合は、エンドポイントの詳細を編集することもできます。

（注） 既存のエンドポイントの登録中は、エンドポイントのプロファイルラベルの変更が紫色で反映され、編集できます。

ステップ 5 [Next] をクリックして、登録プロセスを続行します。

ステップ 6 [登録（Register）] をクリックします。

登録済みのエンドポイントの編集

登録済みのエンドポイントのプロファイリング情報は、[Endpoint Inventory] ウィンドウから更新できます。

ステップ 1 編集するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Edit Endpoint] をクリックします。

ステップ 4 [Endpoint Type]、[Hardware Model]、[Hardware Manufacturer] に詳細を入力します。

ステップ 5 [Save] をクリックします。

登録済みのエンドポイントの削除

登録済みのエンドポイントがネットワークの一部ではなくなった場合は、Cisco AI エンドポイント分析から削除できます。

ステップ 1 削除するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Delete Endpoint] をクリックします。

次のメッセージが表示されます。

「Do you really want to delete the selected endpoint(s)?」

ステップ 4 [Yes] をクリックして、Cisco AI エンドポイント分析からエンドポイントを完全に削除します。

プロファイリングルール

Cisco AI エンドポイント分析のプロファイリングルールを使用すると、共通の属性を組み合わせてエンドポイントをグループ化できます。これらの属性により、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元でエンドポイントを識別できます。プロファイリングルールを使用すると、多くのエンドポイントを簡単に管理できます。

Cisco AI エンドポイント分析は、DPI、メディアプロトコル、医療業界のプロトコルなどを介してネットワークデバイスからプロファイリングデータを受信します。Cisco ISE からのプロファイリングデータは、pxGrid を介して通信されます。これらのプロファイリング属性をデバイスディクショナリで使用してプロファイルルールを作成できます。

プロファイリングルールは、Cisco AI エンドポイント分析の [Profiling Rules] タブで確認できます。このタブの下に表示されるテーブルで、[Rule Name] エントリをクリックすると、割り当てられたプロファイルと使用される属性が表示されます。

Cisco AI エンドポイント分析でエンドポイントをプロファイリングするために使用されるプロファイリングルールは次のとおりです。

- システムルール
- シスコの規則
- Cisco AI ルール

ルールの優先順位付け

Cisco AI エンドポイント分析のプロファイリングルールには優先順位があります。プロファイリングルールの実行は、このルールの優先順位に従って、精度の高いエンドポイントをプロファイリングします。

Cisco AI エンドポイント分析ではユーザー入力がプライマリであるため、プロファイリングルールの優先順位は次のようになります。

- 管理者が作成した静的プロファイル（たとえば、[Register Endpoints] オプションを使用して追加したプロファイル）。
- 管理者が作成したカスタムルール。
- デフォルトで使用可能なシスコ提供のシステムルール。

- 機械学習対応のスマートグループ化ワークフローによって自動生成されたルール。

ルールに設定された優先順位を表示するには、[Profiling Rules] ウィンドウで [Rule priorityitization] をクリックします。

登録済みのエンドポイントは、さまざまなプロファイリングラベルの複数の Cisco AI エンドポイント分析ルールによってプロファイリングできます。次の表に、2 つのエンドポイントに対するプロファイリングルールの設計を示します。

エンドポイント 1	エンドポイント 2
システムルールによってプロファイリングされたハードウェアモデル	システムルールによってプロファイリングされたハードウェアモデル
Cisco AI ルールによってプロファイリングされた OS タイプ	カスタムルールによってプロファイリングされたハードウェアモデル
カスタムルールによってプロファイリングされたハードウェア製造元	Cisco AI ルールによってプロファイリングされたハードウェアモデル

エンドポイント 2 のルール優先順位では、カスタムルールが他のルールよりも優先されます。エンドポイント 2 のハードウェアモデルラベルは、カスタムルールによってプロファイリングされます。

エンドポイント 1 の場合、ルールごとに異なるプロファイルラベルが定義され、それに応じて各ラベルがプロファイリングされます。

プロファイリングルールのフィルタ処理

ステップ 1 [Profiling Rules] ウィンドウで、[Filter] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

ステップ 3 対応するドロップダウンリストからエンドポイント属性の値を選択して、一連のエンドポイントをフィルタ処理します。

ステップ 4 [Apply] をクリックします。

更新されたプロファイリングルールの表示

ステップ 1 [Endpoint Inventory] ウィンドウに移動します。

ステップ 2 エンドポイントの MAC アドレスの横にあるチェックボックスをクリックして、エンドポイントのプロファイリングの詳細を表示します。

ステップ 3 プロファイルラベルの横にある情報アイコンをクリックし、ルール名をクリックして、割り当てられたプロファイルと属性の詳細を表示します。

システムルール

Cisco AI エンドポイント分析には、エンドポイントをプロファイリングするためのシステムルールと呼ばれる事前定義済みのルールが用意されています。Cisco AI エンドポイント分析を導入すると、特定のルールを設定することなく、エンドポイントのゼロデイ可視性を実現できます。

新しくオンボーディングされたエンドポイントは、デフォルトでシステムルールを使用してプロファイリングされます。

ネットワークデバイスは、Cisco DNA Center の **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで管理されます。

これらのネットワークデバイスは、システムルールによってプロファイリングされ、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウには表示されません。ただし、カスタムルールでプロファイリングされたエンドポイントは、カスタムルールがネットワークデバイスを [Device Type] として作成されるため表示できます。

シスコの規則

システムルールのほかに、エンドポイント属性を組み合わせて、エンドポイントをプロファイリングするためのカスタムルールを作成することもできます。カスタムルールは、Cisco AI エンドポイント分析の他のエンドポイント プロファイリング ルールよりも優先されます。

プロファイリングルールの論理と条件

[Endpoint Inventory] ウィンドウでカスタム プロファイリング ルールを作成できます。カスタム プロファイリング ルールを作成するには、エンドポイントの属性と値に基づいて論理条件を作成する必要があります。これらの属性は、ネットワークプローブデータから収集され、[Attribute Glossary] ウィンドウで使用できる分類属性とは異なります。

値は、エンドポイントグループを一意に識別するユーザー入力です。次の演算子を使用して、属性と値から正規表現が作成されます。

演算子	説明
次の文字列を含む	属性は、選択した値を持ちます。
イコール	属性は、選択した値に厳密にマッピングされます。
一致する	属性は、選択した値の正規表現パターンと一致する必要があります。
Starts With	属性は、選択した値で始まる必要があります。

（注） Contains、Equals、および Starts With は、大文字と小文字を区別する演算子です。大文字と小文字を区別しない値の場合は、Matches 演算子を使用します。

論理（[AND] および [OR]）によってこれらの条件をさらに組み合わせて、ネストされたルールを作成できます。

論理条件の作成と編集

論理条件を作成するには、次の手順に従います。

ステップ 1 [Choose Attribute Conditions] ウィンドウで、更新する [Attribute] の横にあるチェックボックスをオンにします。

ステップ 2 [Operator] ドロップダウンリストからオプションを選択します。

ステップ 3 [Value] フィールドに値を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 表示される [Add Logic to Conditions] ウィンドウで、条件間の [AND] ロジックまたは [OR] ロジックをドラッグアンドドロップして、カスタムルールの条件の論理シーケンスを作成します。

（注） 条件の横にある垂直省略記号を使用して、[Add Logical Conditions] ウィンドウで属性条件を追加または編集することもできます。

ステップ 6 [Next] をクリックします。

カスタムルールの作成

ステップ 1 [Endpoint Inventory] ウィンドウで、プロファイリングするエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Profile with Custom Rules] を選択します。

ステップ 3 表示される [Name Rule and Type] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、[Profile Label] ドロップダウンリストからラベルを選択します。

[Profile Label] ドロップダウンリストから選択した内容に応じて、対応するフィールドが表示され、その名前は動的に更新されます。たとえば、[Endpoint Type] を選択すると、[Endpoint Type] フィールドが表示されます。

ステップ 4 表示される新しいフィールドに値を入力します。情報の入力を開始すると、一致するオプションが表示されます。要件に一致するオプションがあれば、そのオプションを選択します。なければ、タイプ名全体を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される [Choose Attribute Conditions] ウィンドウで、論理条件を作成します。

詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 7 [Review Rule] ウィンドウで、このカスタムルールでプロファイリングされるエンドポイントのリストを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Profiles] をクリックします。

カスタムルールの編集

ステップ 1 [Profiling Rules] ウィンドウで、編集する管理ルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Edit] を選択します。

ステップ 3 表示される [Edit] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、ルールの作成時に選択した [Profile Label] に基づいてプロファイルの詳細を選択または入力します。

ステップ 4 [Logic and Conditions] セクションで、垂直省略記号をクリックし、[Edit] を選択して、プロファイリングルールの論理と条件を更新します。詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 5 **[次へ (Next)]** をクリックします。

ステップ 6 **[適用 (Apply)]** をクリックします。
既存のルールが新しいプロファイリングの詳細で更新されると、そのルールでプロファイリングされたエンドポイントが新しいプロファイリングの詳細で更新されます。

カスタムルールの削除

ステップ 1 [Profiling Rules] ウィンドウで、削除するルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Delete] を選択します。

次のメッセージが表示されます。

「Do you really want to delete the selected Rule(s)?」

ステップ 3 [Yes] をクリックして、Cisco AI エンドポイント分析からルールを完全に削除します。

カスタムルールが削除されると、このルールでプロファイリングされたエンドポイントがシステムルールで更新されます。

Cisco AI ルールまたはスマートグループ化

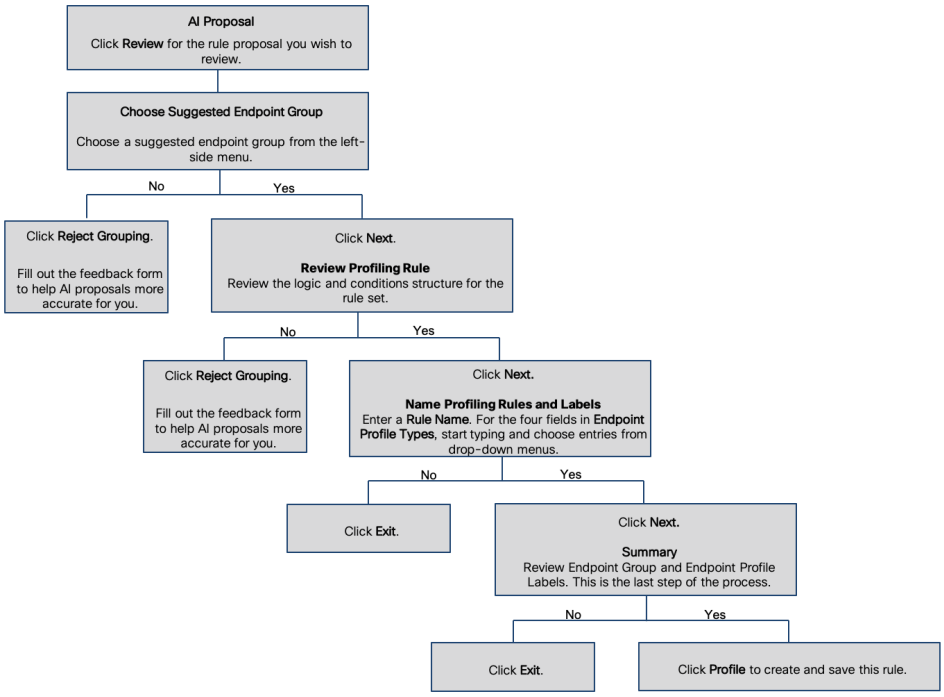
Cisco AI エンドポイント分析は、ML クラウドを使用して、ネットワーク上の不明なエンドポイントを動的にグループ化します。また、不明なエンドポイントのグループにカスタムラベル

を割り当てることもできます。クラスタを確認し、示されたプロファイリング提案を承認または拒否できます。

プロファイリング提案を承認すると、選択したエンドポイントをプロファイリングして、今後ネットワークに参加する同様のエンドポイントをプロファイリングするためのプロファイリングルールが自動的に作成されます。

プロファイリングルール提案の変更

[Endpoint Analytics] ホームページの [AI Proposal] ダッシュレットには、スマートグループ化によって生成されたエンドポイントクラスタに基づいてルール提案が表示されます。AI 提案を表示するには、対応する提案タイプの横にある [Review] をクリックし、次の決定表に従って進みます。



プロファイリングルールのインポート

カスタムプロファイリングルールと Cisco AI ルールを移行するには、.json ファイルをインポートします。

ステップ 1 [Profiling Rule] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Import Profiling Rules] を選択します。

ステップ 3 [Choose a file] をクリックし、システムの .json ファイルを参照します。

ステップ 4 [OK] をクリックします。

プロファイリングルールのエクスポート

Cisco AI エンドポイント分析からカスタムルールおよび Cisco AI プロファイリングルールをエクスポートしてバックアップできます。[Export Profiling Rules] オプションは、使用可能なすべてのカスタムルールと Cisco AI プロファイリングルールをエクスポートします。ルールを選択してエクスポートすることはできません。

ステップ 1 [Profiling Rules] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Export Profiling Rules] を選択します。

ステップ 3 [Yes] をクリックして、すべてのカスタムルールと ML プロファイリングルールをエクスポートします。終了するには、[No] をクリックします。

（注） 同じファイルを Cisco AI エンドポイント分析に再度インポートできます。

階層

Cisco AI エンドポイント分析階層は、エンドポイントタイプに基づいてエンドポイントの論理グループを作成するのに役立ちます。エンドポイントのカテゴリとサブカテゴリを作成すると、エンドポイントの可視性に焦点が当てられ、許可プロセスが簡素化されます。

デフォルトの [All Endpoints] 親カテゴリからカテゴリを作成できます。エンドポイントの総数、エンドポイントタイプ、サブカテゴリなどのカテゴリの詳細が [Hierarchy] ウィンドウの個々のボックス内に表示されます。

カテゴリを作成、編集、および削除して、階層を並べ替えることができます。

カテゴリとサブカテゴリの作成

ステップ 1 [Hierarchy] ウィンドウで、親カテゴリの水平省略記号をクリックします。

ステップ 2 [Create Category] をクリックします。

ステップ 3 カテゴリ名を入力します。

ステップ 4 Enter キーを押します。

次のタスク

カテゴリを作成したら、[Endpoint Type] ウィンドウからエンドポイントタイプをドラッグアンドドロップするか、カテゴリを編集してエンドポイントを追加できます。

カテゴリまたはサブカテゴリの編集

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 表示される [Edit] ウィンドウで、[Category Name] に値を入力します。

ステップ 4 カテゴリを再割り当てする場合は、ドロップダウンメニューから [Parent Category] を入力します。

ステップ 5 [Endpoint Type] タブをクリックします。

ステップ 6 [Actions] をクリックし、[Add Endpoint Type] を選択します。

ステップ 7 [Search Dropdown] リストからエンドポイントタイプを選択します。

ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

[Endpoint Type] ウィンドウで、[All]、[Available]、および [Assigned] でエンドポイントタイプをフィルタ処理できます。

カテゴリからのエンドポイントタイプの削除

ステップ 1 [Hierarchy] ウィンドウで、削除するカテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。

ステップ 4 削除するエンドポイントタイプの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] をクリックし、[Remove From Category] を選択します。

次のメッセージが表示されます。

「Are you sure you want to delete this category?」

ステップ 6 カテゴリからエンドポイントを削除するには、[Yes] をクリックします。終了するには、[No] をクリックします。

カテゴリからのエンドポイントタイプの再割り当て

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。

ステップ 4 再割り当てするエンドポイントタイプの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] をクリックし、[Re-assign to existing category] または [Re-assign to a new category] を選択します。

オプション	手順
既存のカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから既存のカテゴリを選択します。 2. **[保存（Save）]** をクリックします。
新しいカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから [New Category] を選択します。 2. [Parent Category] ドロップダウンリストから親カテゴリを選択します。 3. [New Category] フィールドにカテゴリ名を入力します。 4. [Save（保存）] をクリックします。

カテゴリの削除

始める前に

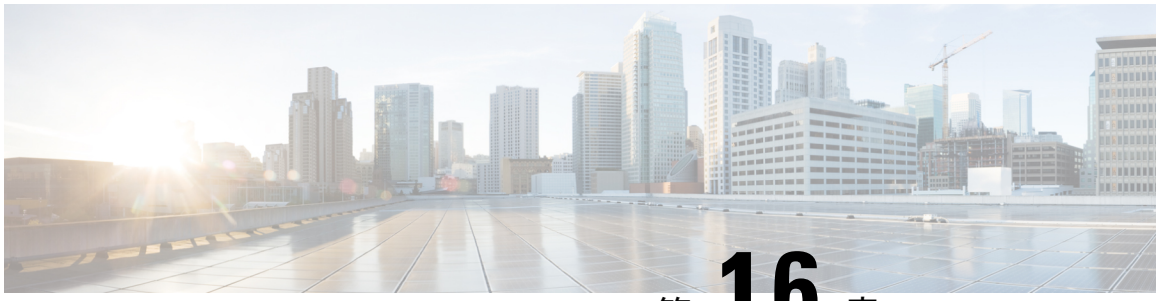
親カテゴリを削除する前に、そのサブカテゴリを確認します。サブカテゴリを別の既存のカテゴリまたは新しいカテゴリに再割り当てできます。そうしないと、すべてのサブカテゴリが親カテゴリとともに削除されます。カテゴリの削除中にサブカテゴリを再割り当てすることもできます。

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [削除（Delete）] をクリックします。

サブカテゴリが割り当てられているカテゴリを削除する場合には、[Reassign Relationships] ダイアログボックスが表示されます。次のオプションのいずれかを選択します。

オプション	条件	手順
既存のカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	1. [Category] ドロップダウンリストからカテゴリを選択します。 2. [Reassign] をクリックします。 親カテゴリが削除され、選択したカテゴリにサブカテゴリが再割り当てされます。
新しいカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	1. [Parent Category] ドロップダウンリストからカテゴリを選択します。 2. [New Category] フィールドにカテゴリ名を入力します。 3. [Reassign] をクリックします。 親カテゴリが削除され、新しいカテゴリにサブカテゴリが再割り当てされます。
カテゴリからの削除	親カテゴリとともにサブカテゴリを削除します。	[Reassign] をクリックします。 親カテゴリとそのサブカテゴリが削除されます。



第 16 章

ネットワークのプロビジョニング

プロビジョニング

Cisco DNA Center でネットワークのポリシーを設定した後に、デバイスをプロビジョニングできます。この段階で、デバイスにオンボードし、デバイス間にポリシーを導入します。

プロビジョニングデバイスには、次の側面が含まれます。

- プラグ アンド プレイでのデバイスのオンボーディングと、デバイスのインベントリへの追加。
- 必要な設定とポリシーのインベントリ内デバイスへの展開。
- デバイスのサイトへの追加。
- ファブリックサイトの作成とデバイスのファブリックへの追加。

Cisco DNA Center プロビジョニングでは IBNS 2.0 のみをサポートしています。これにより AAA 設定が変更され、関連するすべての認証コマンドがクラスベースのポリシー言語（CPL）制御ポリシーの対応するコマンドに変換されます。CPL 変換では、変換 CLI **authentication display [legacy|new-style]** が無効になるため、現在の設定をバックアップしておくことを推奨します。また、IBNS 2.0 に合わせた AAA 設定の更新をサポートするように変更管理期間を設定してください。

プラグ アンド プレイ プロビジョニングを使用したオンボードデバイス

プラグ アンド プレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワーク デバイスを自動的かつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグ アンド プレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Cisco DNA Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。
- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Cisco DNA Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、次の操作を実行します。

- メインの Cisco DNA Center の設定で、[System] > [Settings] > [Smart Account] を使って、Cisco スマートアカウントのクレデンシャルを設定します。
- [System] > [Settings] > [Device EULA Acceptance] を使用して、メインの Cisco DNA Center の設定でシスコ エンド ユーザー ライセンス契約（EULA）に同意します。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide for Cisco DNA Center』で、デバイスのクリーンアップとリセットの詳細を参照してください。

ここでは、プラグアンドプレイプロビジョニングの一般的な使用例とワークフローについて説明します。

計画されたプロビジョニング

管理者は、次のように新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

1. 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（124ページ）』を参照してください。
2. 必要に応じて、デバイスに適用する「[Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day 0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成（209ページ）を参照してください。
3. 展開するデバイスのタイプについて、ネットワーク プロファイルを定義します。「ネットワーク プロファイルの作成（176 ページ）」を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLIおよびSNMP）を定義します。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。「デバイス クレデンシャルについて（185 ページ）」を参照してください。
5. 必要に応じて、プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェア イメージのインポート（104 ページ）を参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集（372 ページ）またはデバイスの一括追加（374 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング。

計画前に新しいネットワーク デバイスをネットワークに追加すると、このネットワーク デバイスは要求のないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、コントローラ ディスカバリの前提条件（366 ページ）で説明されているいずれかの検出方法を使用して自動的に追加することもできます。管理者は、次の方法でデバイスをプロビジョニングできます。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示（370 ページ）」を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング（377 ページ）」を参照してください。

Cisco スマート アカウントの同期およびプロビジョニング

ネットワーク デバイスは、シスコのプラグ アンド プレイ接続クラウド サービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Cisco DNA Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。「バーチャル アカウント プロファイルの登録または編集 （375 ページ）」を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。スマート アカウントからのデバイスの追加 （376 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （370 ページ）」を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （377 ページ）」を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

コントローラ ディスカバリの前提条件

プラグ アンド プレイによってデバイスのオンボーディングが自動化されます。デバイスは、Cisco DNA Centerコントローラを検出して接続できるようにする必要があります。デバイスは、次のいずれかの方法でコントローラを自動的に検出できるようにする必要があります。

- DHCP：DHCP コントローラ ディスカバリ （366 ページ）を参照してください。
- DNS：DNS コントローラ ディスカバリ （368 ページ）を参照してください。
- Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラ ディスカバリ （368 ページ）を参照してください。

DHCP コントローラ ディスカバリ

シスコのネットワークデバイスは初回起動時にスタートアップ設定を使用しない場合、DHCP オプション 43 を使用して Cisco DNA Center コントローラの検出を試行します。

DHCP による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。このオプションにより、Cisco DNA Center コントローラの IP アドレスを持つネットワークデバイスが通知されます。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。デバイスの Cisco Plug and Play IOS エージェントは、応答から Cisco DNA Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool         <-- Name of DHCP pool
```

```
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;"    <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）
- I*xxx.xxx.xxx.xxx*;：Cisco DNA Center コントローラの IP アドレスまたはホスト名（大文字の i の後）。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Cisco DNA Center コントローラへの接続に使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- K4;：デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- T*trustpoolBundleURL*：デフォルト（Cisco DNA Centerコントローラ）以外の別の場所から trustpool バンドルを取得する場合は、このオプション パラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Tftp://10.30.30.10/ios.p7b」と指定します。

  trustpool セキュリティを使用していて、T パラメータを指定しない場合、デバイスは Cisco DNA Center コントローラから trustpool バンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラ ディスカバリ （368 ページ）を参照してください。

Cisco DNA Center システム証明書に FQDN のみの SAN フィールドがある場合、PnP を開始する前に、シードデバイスの DHCP プールを編集して、FQDN、B2 ー B1、dns-server、および domain-name を含むオプション 43 文字列を含める必要があります。

DHCP プールが Cisco スイッチまたはルータに依存している場合の設定例は次のとおりです。

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS コントローラ ディスカバリ

DHCP ディスカバリが Cisco DNA Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コントローラの完全修飾ドメイン名（FQDN）を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワークデバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Cisco DNA Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラ ディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウド サービスによって、デバイスが Cisco DNA Center コントローラの IP アドレスを検出できます。ネットワークデバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connec に接続するときに、最初に Cisco trustpool バンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワークデバイスを展開する方法についての概要を説明します。

始める前に

シスコの各種ネットワークデバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Cisco DNA Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace（CCW）を介してプラグアンドプレイ ネットワークデバイスを注文した場合、Cisco スマートアカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワークデバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマート アカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。『バーチャル アカウント プロファイルの登録または編集 （375 ページ）』を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワークデバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグ アンド プレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。『プラグアンドプレイ対応デバイスのプロビジョニング （377 ページ）』を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワークデバイスがインストールされ、電源が投入されます。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Cisco DNA Center コントローラを検出し、Cisco DNA Center でプラグ アンド プレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。

（注） デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバのローカル NTP サーバ アドレスにマップします。

プラグアンドプレイ導入ガイド

プラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Cisco DNA Center

コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。

- シスコのルータトランク/アクセスポートの構成：一般的なブランチネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の導入モデルはプラグアンドプレイでサポートされます。
  - ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセス ポートとして設定できます。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。
- 非 VLAN 1 構成：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

この手順では、プラグアンドプレイデバイスを表示する方法、デバイスでアクションを実行する方法、および新しいデバイスを追加する方法について説明します。

ステップ 1 Cisco DNA Center GUI で、**[Menu]** アイコン（☰）をクリックして、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックして、デバイスリストを更新します。

ステップ 3 デバイスの名前をクリックします。

デバイスの詳細を示すウィンドウが表示されます。

ステップ 4 [Details]、[History]、[Configuration]、または [Stack] タブをクリックして、デバイスに関するさまざまな種類の情報を表示します。一部のタブには、クリックして詳細を表示できる追加のリンクがあります。

[スタック（Stack）] タブは、スイッチ スタック デバイスの場合にのみ表示されます。

ステップ 5 デバイスで特定のタスクを実行するには、ダイアログ ボックスの上部にある次のアクションをクリックします。使用可能なアクションは、デバイスの状態によって異なります。

- [Refresh]：デバイス状態情報を更新します。
- [Claim]：デバイスを要求しプロビジョニングします。プラグアンドプレイ対応デバイスのプロビジョニング （377 ページ） を参照してください。
- [Edit]：デバイスを編集します。デバイスの追加または編集 （372 ページ） を参照してください。
- [Reset]：デバイスがエラー状態になっている場合に、デバイスをリセットします。デバイスのリセット （389 ページ） を参照してください。
- [Delete]：デバイスを削除します。デバイスの削除 （388 ページ）を参照してください。

ステップ 6 複数のデバイスに対してアクションを実行するには、テーブルビューで各デバイスの横にあるチェックボックスをオンにし、[Actions] ドロップダウンメニューからアクションを選択します。

ステップ 7 [Add Device] をクリックして、新しいデバイスを追加します。

異なる方法でデバイスを追加する用法の詳細については、デバイスの追加または編集 （372 ページ）、デバイスの一括追加 （374 ページ）、またはスマート アカウントからのデバイスの追加 （376 ページ） を参照してください。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。一部の列はソートに対応しています。ソートに対応している場合、列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

（注） デフォルトの列表示設定では一部の列が非表示になっています。これは、列の見出しの右端にある 3 つの点（ ⋮ ）をクリックするとカスタマイズできます。

表 *49* : デバイス情報

カラム	説明
#	行番号。
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタックアイコンはスイッチスタックを示します。
Serial Number	デバイスのシリアル番号。

カラム	説明
Product ID	デバイスの製品 ID。
IP Address	デバイスの IP アドレス。
Source	デバイスエントリの送信元： • [User]：ユーザーが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
状態	• [Unclaimed]：デバイスはプロビジョニングされていません。 • [Planned]：デバイスはすでに要求されていますが、まだサーバーと接続していません。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。
Onboarding State	デバイスのオンボーディング状態。デバイスの履歴に移動するには、経過表示バーをクリックします。
Site	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグ アンド プレイに接続した日時。
Smart Account	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Account	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
Created	デバイスがプラグ アンド プレイに追加された日時。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストからデバイスを追加または編集する方法について説明します。代わりに、[編集（Edit）] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 *50 : [*デバイス（*Device*）*]* フィールド

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
Product ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名
Enable SUDI Authorization	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブル スイッチにのみ適用されます。

始める前に

デバイスにログイン情報が必要な場合は、グローバルデバイスログイン情報が **[Design]** > **[Network Settings]** > **[Device Credentials]** ページで設定されていることを確認します。詳細については、グローバル CLI クレデンシャルの設定 （188 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、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 次のようにデバイスを追加または編集します。

- デバイスを追加するには、[Add Devices] をクリックし、[Single Device] をクリックします。
- デバイスを編集するには、編集する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 テーブルの上部にあるメニューバーから [アクション（Actions）] > [編集（Edit）] をクリックします。**[デバイスの編集（Edit Device）]** ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （377 ページ）、を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。

ステップ 1 Cisco DNA Center GUI で、**[Menu]** アイコン（☰）をクリックして、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Bulk Devices] をクリックします。

ステップ 4 [Download File Template] をクリックしてファイルテンプレートをダウンロードします。

さまざまなデバイスの必須のフィールドとオプションのフィールドについては、ファイルテンプレートを参照してください。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。デバイスタイプによっては、特定のフィールドが必須になることに注意してください。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
- **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 7 **[デバイスのインポート（Import Devices）]** をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかの操作を実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （377 ページ）、を参照してください。

バーチャル アカウント プロファイルの登録または編集

この手順により、Cisco DNA Center コントローラを、リダイレクション サービス向けの Cisco スマート アカウントに、Cisco Plug and Play Connect のデフォルトのコントローラとして登録できます。また、これによって Cisco Plug and Play Connect クラウド ポータルから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

表 *51* : バーチャルアカウント フィールド

フィールド	説明
スマートアカウントの選択	Cisco スマート アカウント名
バーチャルアカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
デフォルト コントローラ プロファイルとして使用	Cisco DNA Center コントローラを Cisco プラグアンドプレイ接続のクラウド ポータルにデフォルト コントローラとして登録するには、このボックスにチェックを付けます。
コントローラ IP または FQDN	この Cisco DNA Center コントローラの IP アドレスまたは完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名

始める前に

メインの Cisco DNA Center の設定で、**[System]** > **[Settings]** > **[Smart Account]** を使って、Cisco スマートアカウントのクレデンシャルを設定します。

ステップ 1 Cisco DNA CenterGUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[システム（System）]** > **[設定（Settings）]** > **[PnP 接続（PnP Connect）]**の順に選択します。

ステップ 2 テーブル内のバーチャルアカウントを表示します。

このテーブルには、登録されている Plug and Play Connect のバーチャル アカウント プロファイルがすべて一覧表示されます。

ステップ 3 次のように、バーチャル アカウント プロファイルを追加または編集します。

- バーチャルアカウントを登録するには、[Register] をクリックします。[Register Virtual Account] ダイアログが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集したいプロファイル名の横にあるラジオボタンをクリックし、テーブルの上にあるメニュー バーの [Edit Profile] をクリックします。[edit virtual account] ダイアログが表示されます。

ステップ 4 上述の [Virtual Account Fields] テーブルを参照して、必要に応じてフィールドを設定します。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- 新しいバーチャルアカウントプロファイルを登録する場合は、[登録（Register）]をクリックします。
- バーチャル アカウント プロファイルを編集する場合は、[変更（Change）] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。詳細については、スマート アカウントからのデバイスの追加 （376 ページ）を参照してください。

スマート アカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

バーチャル アカウント テーブルには、プロファイルごとに情報が表示されます。

表 *52 :* バーチャル アカウント情報

カラム	説明
バーチャル アカウント	バーチャルアカウント名
スマート アカウント	バーチャルアカウントが関連付けられているスマートアカウント
同期ステータス	直近の同期プロセスのステータス
同期の結果	最後の同期プロセスの結果

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。『バーチャル アカウント プロファイルの登録または編集 （375 ページ）』を参照してください。**[Add Devices]** > **[Smart Account Devices]** ダイアログの **[PnP Connect]** リンクをクリックすると、[PnP Connect] 設定ページに直接移動できます。

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]** > **[Plug and Play]** を選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Smart Account Devices] をクリックします。

ステップ 4 Cisco.com ID を入力する必要がある場合（Cisco.com ID は「Not Associated（関連付けなし）」として表示されます）、次の手順を実行します。

a) [Add] リンクをクリックします。
b) Cisco.com ユーザ名とパスワードを入力します。
c) ログイン情報を Cisco DNA Center で永続的に保存する場合は [Save For Later] をクリックします。ログイン情報を 1 回のみ使用する場合は、このチェックボックスをオフのままにします。
d) [Submit] をクリックします。`

ステップ 5 デバイスを追加する Plug and Play Connect バーチャル アカウント プロファイルの名前の横にあるラジオ ボタンをクリックします。

PnP Connect バーチャル アカウント プロファイルを登録する必要がある場合は、[PnP Connect] リンクをクリックします。Cisco.com のログイン情報を追加する必要がある場合は、[Cisco.com ID] の横にある [Add] リンクをクリックします。Cisco ID を変更する場合は、[Not me?] リンクをクリックします。

ステップ 6 [同期（Sync）] をクリックして、このバーチャル アカウントの Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイに、デバイス インベントリを同期させます。

追加されたデバイスは、SmartAccount に設定されたソースとともに [プラグアンドプレイデバイス（Plug and Play Devices）] テーブルに表示されます。

次のタスク

新しく同期されたデバイスを要求します。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （377 ページ）、を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスのプロビジョニングまたは要求では、イメージとオンボーディングの設定をデバイスに展開するか、ワイヤレスデバイスのネットワークプロファイルを展開して、それをインベントリに追加してプロビジョニングします。デバイスの初起動を要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスをプロビジョニングするためのワークフローは、デバイスのタイプによって次のように異なります。

- スイッチとルータの参照資料： スイッチまたはルータ デバイスのプロビジョニング （377 ページ）
- ワイヤレス LAN コントローラ、アクセスポイント、センサの参照資料： ワイヤレスまたはセンサー デバイスのプロビジョニング （383 ページ）

スイッチまたはルータ デバイスのプロビジョニング

デバイスを要求すると、それをサイトに割り当て、イメージをインストールし、サイト設定とオンボーディング構成を展開してインベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスが要求される場合、Cisco DNA Center からのシステム構成 CLI コマンドの一部はまずデバイスにプッシュされてから、定義した [Onboarding Configuration (Day-0)] テンプレートにプッシュされます。[Onboarding Configuration] テンプレートに同じ CLI コマンドがある場合、これらは最後に適用されるため、システム設定が上書きされます。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報（CLI および SNMP）
- SSH v2 および SCP サーバの有効化
- HTTP および HTTPS サーバの無効化
- スイッチでは、vtp モードの透過が有効になっています

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください。

この手順では、[Plug and Play Devices] リストからデバイスを要求する方法について説明します。代わりに、[要求（Claim）] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「コントローラ ディスカバリの前提条件（366 ページ）」を参照してください。
- 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（124 ページ）』を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。「デバイス クレデンシャルについて（185 ページ）」を参照してください。
- （オプション）イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。『ソフトウェア イメージのインポート（104 ページ）』を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これは ソフトウェアイメージのプロビジョニング（109ページ）で説明されています。プラグアンドプレイプロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- 必要に応じて、デバイスに適用する「[Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。『デバイス設定の変更を自動化するテンプレートの作成（209 ページ）』を参照してください。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用できます。これにより、Cisco DNA Center は、特に複数の IP または VRF のシナリオにおいて、その IP アドレスをデバイスの管理 IP アドレスとして使用できます。

- デバイスのネットワークプロファイルを定義します。『ネットワークプロファイルの作成（176 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、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[Actions] > [Claim] をクリックします。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスクレデンシャルの定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスクレデンシャルを定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （オプション）必要に応じて、最初のカラムのデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ 7 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 （オプション）次のように、デバイステーブルに対するグローバルな変更を行います。

a) テーブルに表示されるカラムを変更するには、テーブル見出しの右端にある 3 つの点をクリックし、目的のカラムを選択します。[Apply] をクリックして、変更内容を保存します。
b) [Clear Images] をクリックして、デバイス用に設定されたデフォルトイメージをクリアします。イメージをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
c) [Clear Templates] をクリックして、デバイス用に設定されたデフォルトテンプレートをクリアします。テンプレートをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
d) デバイスに設定されているライセンスレベルをクリアするには、[Clear License Level] をクリックします。ライセンスレベルをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
e) デバイスの横にある [Actions] カラムの 3 つの点をクリックし、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択することで、あるデバイスのイメージまたはテンプレートを他のデバイスに適用できます。スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

ステップ 9 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （オプション）必要に応じて [Device Name] フィールドでデバイスのホスト名を変更します。
c) （オプション）[イメージ（Image）] ドロップダウン リストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
d) （オプション）[テンプレート（Template）] ドロップダウン リストで、デバイスに適用する [オンボーディングの設定（onboarding configuration）] テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

   選択したテンプレートの横にある [Preview] をクリックすると、テンプレートが表示されます。

e) （オプション）スタックの番号を付け直す場合は、[Select a Cabling Scheme] ドロップダウンリストで、スタックのケーブル配線スキームを選択します。

   この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線スキームに従って接続されている場合にのみ表示されます。

図 *9 :* ケーブル配線スキーム

f) （オプション）スタックの番号を付け直す場合は、[Select a Top of Stack serial Number] ドロップダウンリストで、スタックスイッチの先頭のシリアル番号を選択します。

この項目は、スタック構成をサポートしているスイッチが図のように接続されている場合にのみ表示されます。

g) （任意）[Select a License Level] ドロップダウンリストで、スタックのライセンスレベルを選択します。

この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

h) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 10 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 11 **[Next]** をクリックします。

[Provision Templates] ウィンドウが表示されます。ここでは、テンプレートに定義されたパラメータの値を指定できます。

ステップ 12 設定するデバイスの名前をクリックし、次の手順を実行します。

a) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。赤のアスタリスクは、必須フィールドを示します。

b) 選択したデバイスの起動設定に実行中の設定をコピーしたい場合、[Copy running config to startup config] チェックボックスをオンにします。

c) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。

ステップ 13 すべてのデバイスのパラメータ値を一括で指定するには、次の手順を実行します。

a) [**エクスポート (Export)**] をクリックして、CSV テンプレートファイルを保存します。

b) 各パラメータの値をファイルに追加して、ファイルを保存します。
c) [Import] をクリックします。
d) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップするか、**[click to select]** と表示されている場所をクリックしてファイルを選択します。
e) [Import] をクリックします。

ステップ 14 **[Next]** をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 15 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。「テンプレートのプロビジョニング」手順に戻ってパラメータ値やテンプレートを変更したり、[Design]エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] オプションボタンをクリックし、[OK] をクリックします。

ステップ 16 Day-0 Config 列のリンクをクリックして、デバイス、その設定、設定プレビューエラーの詳細を確認することができます。

ステップ 17 [要求（Claim）] 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 18 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デバイスのプロビジョニング （390 ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイ プロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

ワイヤレスまたはセンサー デバイスのプロビジョニング

デバイスに設定を割り当て、それをインベントリに追加してワイヤレスデバイスを要求すると、プロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください。

この手順では、[プラグアンドプレイデバイス（Plug And Play Devices）] リストからデバイスを要求する方法について説明します。代わりに、[要求（Claim）] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「コントローラ ディスカバリの前提条件 （366 ページ）」を参照してください。
- 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 （124 ページ）』を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。デバイス クレデンシャルについて （185 ページ）を参照してください。
- ワイヤレス アクセス ポイント デバイスをプロビジョニングするには、ワイヤレス アクセス ポイントを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。これは、Mobility Express アクセスポイントでは必要ありません。
- センサー デバイスをプロビジョニングするには、センサーが Cisco DNA Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Cisco DNA Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Cisco DNA Center の仮想 IP アドレスです。

- ワイヤレス アクセス ポイント デバイスのワイヤレス無線周波数プロファイルを定義します（Mobility Express アクセスポイントを除く）。「ワイヤレス無線周波数プロファイルの作成 （168 ページ）」を参照してください。
- Mobility Express アクセスポイントの場合は、IP アドレスプールと管理インターフェイスを定義します。『IP アドレス プールを設定する （197 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、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレスデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス表の上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスクレデンシャルの定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスクレデンシャルを定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 （任意） 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP（アクセスポイント）または ME（Mobility Express）を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、ワイヤレス LAN コントローラやセンサーデバイスには表示されません。

ステップ 7 [サイトの選択（Select a Site）] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。アクセスポイントデバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 9 （任意） テーブルに表示される列を変更するには、テーブル見出しの右端にある 3 つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。

b) （任意） [デバイス名（Device Name）] フィールドで、必要に応じてデバイス名を変更します。

c) アクセスポイントデバイスの場合、[Radio Frequency Profile] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。

d) ワイヤレス LAN コントローラの場合、次のフィールドに値を入力します。[Management IP]、[Subnet Mask]、[Gateway]、[IP Interface Name]、また任意で [VLAN ID]。

e) Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。

f) ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサーデバイスプロファイル（バックホール）を選択します。

（注） ソフトウェアリリース 1.3.1.2 よりも古い Cisco Aironet 1800s アクティブセンサの場合は、センサデバイスプロファイル **`CiscoProvisioningSSID`** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

g) 変更した場合は、[保存（Save）] をクリックします。それ以外の場合は、[キャンセル（Cancel）] をクリックしてリストに戻り、他のデバイスを設定します。

h) **[アクション（Actions）]** 列の **[他のデバイスに...を適用（Apply … to Other Devices）]** をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスに**[割り当て（Assign）]** をクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 12 **[Next]** をクリックします。
[概要（Summary）] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 13 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[割り当ての設定（Assign Configuration）] 手順に戻って設定を変更したり、[設計（Design）] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] オプションボタンをクリックし、[OK] をクリックします。デバイスを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 14 [要求（Claim）] 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 15 **[はい（Yes）]** をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デ

バイスのプロビジョニング （390 ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイ プロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

Cisco DNA トラフィック テレメトリ アプライアンス のプロビジョニング

この手順では、[Plug And Play Devices] リストから Cisco DNA トラフィック テレメトリ アプライアンス を要求する方法について説明します。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド[英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。
- 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 （124 ページ）』を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。「デバイス クレデンシャルについて （185 ページ）」を参照してください。

（注） SNMPv3 の制限事項：

- 認証用の SHA とプライバシー用の AES128 がサポートされています。
- MD5 はサポートされていません。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージがアップロードされていて、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェア イメージのインポート （104 ページ）を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ展開プロセスは、後でデバイスイメージの更新時に使用される展開プロセスとは異なります。詳細については、ソフトウェア イメージのプロビジョニング （109 ページ）を参照してください。プロビジョニング中、プラグアンドプレイではデバイスの事前チェック、自動フラッシュクリーンアップ、または事後チェックは実行されません。デバイスは工場出荷時の初期状態である必要があります。

- デバイスのネットワークプロファイルを定義します。『Cisco DNA トラフィック テレメトリ アプライアンス のネットワークプロファイルの作成』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、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] または [Find] オプションを使用して、Cisco DNA トラフィック テレメトリ アプライアンス を見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[Actions] > [Claim] をクリックします。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスログイン情報の定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスログイン情報を定義する必要があります。これらの必須タスクは、要求プロセスの前提条件です。これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ 7 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意） [Device Name] フィールドで、必要に応じてデバイスのホスト名を変更します。
c) （任意） [Image] ドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

d) 何らかの変更を行った場合は、[Save] をクリックします。変更していない場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 9 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] をクリックします。すべてのデバイスを設定するまで、設定手順を繰り返します。

ステップ 10 **[Next]** をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 11 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要のあるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。プロビジョニングエラーを回避するには、デバイスを要求する前に問題を解決する必要があります。場合によっては、[Design] 領域に再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりする必要があります。問題を解決したら、このタブに戻り、[Retrying getting Day-0 configuration preview for failed device(s)] オプションボタンをクリックします。次に [OK] をクリックします。

ステップ 12 Day-0 Config 列のリンクをクリックして、デバイス、その設定、設定プレビューエラーの詳細を確認することができます。

ステップ 13 [要求（Claim）] 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 14 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認できます。詳細については、デバイスのプロビジョニング（390ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[Plug and Play Devices] リストからデバイスを削除する方法を示します。代わりに、[削除（Delete）] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。

（注） デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。

ステップ 1 Cisco DNA Center GUI で、**[Menu]** アイコン（☰）をクリックして、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 削除する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[アクション（Actions）] > [削除（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 5 [Yes] クリックして、このデバイスを削除することを確認します。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、**[Ddelete]** を使用します。

（注） デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップ コンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、[Plug and Play Devices] リストからデバイスをリセットする方法を示します。代わりに、[Reset] をクリックしてデバイスの詳細ウィンドウからリセットすることもできます。

ステップ 1 Cisco DNA Center GUI で、**[Menu]** アイコン（☰）をクリックして、**[Provision]** > **[プラグアンドプレイ（Plug and Play）]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions（アクション）] > [Reset（リセット）]** 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 5 次のいずれかのオプションを選択します。

- [Reset and keep current claim parameters]：現在の請求パラメータが維持され、デバイスは [Planned] 状態になります。
- [Reset and remove all claim parameters]：現在の請求パラメータを削除し、デバイスが [Unclaimed] 状態になります。

ステップ 6 [Reset] をクリックします。

デバイスのプロビジョニング

次のセクションでは、さまざまなシスコデバイスをプロビジョニングする方法について説明します。

ワイヤレスデバイスと国コードについて

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り当てられています（ヨーロッパの場合はEなど）が、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます（フランスの場合はFR、スペインの場合はESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

Cisco DNA Center は、割り当てられたサイトに応じて、国コードを使用してコントローラをプロビジョニングします。コントローラの場合は、複数のサイトに割り当てることができます。そのため、複数の国コードを割り当てることができます。Cisco DNA Center は、プロビジョニング中に、サイトをサイトの国コードとともにコントローラに割り当てます。たとえば、インドと米国の両方のサイトを管理するコントローラには、IN と US の国コードが割り当てられます。

アクセスポイントは、プロビジョニングされると、フロアに割り当てられます。アクセスポイントが ROW AP の場合、Cisco DNA Center は、サイトの国コードを取得して AP に割り当てます。同じフロア上の追加の AP には、同じ国コードが割り当てられます。

国コード情報は、コントローラとアクセスポイントのデバイス 360 ページに表示されます。

サポートされている国コードの製品ごとの完全なリストについては、https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html を参照してください。

Cisco AireOS コントローラのプロビジョニング

始める前に

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次のグローバル ネットワーク設定を定義したことを確認します。
  - AAA、DHCP、および DNS などのネットワーク サーバー。

    詳細については、グローバル ネットワーク サーバーの設定 （204 ページ）を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。

    詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、およびグローバル HTTPS クレデンシャルの設定 （193 ページ）を参照してください。
  - IP アドレス プール

    詳細については、「IP アドレス プールを設定する （197 ページ）」を参照してください。
  - SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。

    詳細については、「グローバル ワイヤレス設定の構成 （156 ページ）」を参照してください。
- インベントリに シスコ ワイヤレス コントローラがあることを確認します。ない場合は、[Discovery] 機能を使用してコントローラを検出します。
- サイトに シスコ ワイヤレス コントローラ が追加されたことを確認してください。詳細については、デバイスをサイトに追加する （80 ページ）を参照してください。
- デバイスで既存の VLAN を再利用することはできません。デバイスにすでに存在する同じ VLAN を Cisco DNA Center がプッシュすると、プロビジョニングは失敗します。

Cisco DNA Center によって管理されている ワイヤレスコントローラ の設定に手動で変更を加えることはできません。Cisco DNA Center GUI からすべての設定を実行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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [DEVICE TYPE] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な ワイヤレスコントローラ のリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 6 [Choose a site] をクリックして ワイヤレスコントローラ にサイトを割り当てます。

ステップ 7 [Add Sites] ウィンドウで、ワイヤレスコントローラを関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 8 [Apply] をクリックします。

ステップ 9 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 10 ワイヤレスコントローラのロールを選択します（[Active Main WLC] または [Guest Anchor WLC]）。

ステップ 11 [Select Primary Managed AP Locations] をクリックして、ワイヤレスコントローラ の管理 AP の場所を選択します。

ステップ 12 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、親サイトの下にある子は自動的に選択されます。

（注） 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレスコントローラ で管理できるのは 1 つのサイトのみです。

ステップ 13 **[Save]** をクリックします。

ステップ 14 [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレスコントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレスコントローラ プロビジョニングにのみ適用できます。

[インターフェイスと VLAN の設定（Configure Interface and VLAN） **]** ウィンドウが表示されます。

ステップ 15 **[** インターフェイス名（Interface Name） **]** ドロップダウン リストからインターフェイス名を選択します。

ステップ 16 [VLAN ID] フィールドに、VLAN の値を入力します。

ステップ 17 [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。

ステップ 18 [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。

ステップ 19 [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 20 [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。

ステップ 21 [OK] をクリックします。

ステップ 22 （オプション）ゲスト アンカー ワイヤレスコントローラ の場合、[Assign Guest SSIDs to DMZ site] で [VLAN ID] を変更して、VLAN ID 設定を変更します。

ステップ 23 [Mobility Group] で [Configure] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

[Configure Mobility Group] サイドパネルが表示されます。

ステップ 24 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択します。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 25 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 26 [Mobility Peers] で [Add] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

ステップ 27 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 28 **[Save]** をクリックします。

ステップ 29 モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 30 [Next] をクリックします。

[Model Configuration] ウィンドウが表示されます。

ステップ 31 [Devices] ペインで、[Find] フィールドにモデル設定設計の名前を入力して検索するか、デバイスを展開してモデル設定設計を選択します。

選択したモデル設定設計が右側のペインに表示されます。

ステップ 32 プロビジョニングするモデル設定設計の [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。

この手順では、すべての設定を編集することはできません。

ステップ 33 必要な変更を加えて、[Apply] をクリックします。

ステップ 34 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 35 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 36 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 37 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**
- **Managed Sites**
- **Interfaces**
- **Advanced Configuration**
- **モビリティ グループの設定**
- **モデル設定**

ステップ 38 [Deploy] をクリックして、コントローラをプロビジョニングします。

ステップ 39 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] メッセージで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] メッセージが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activity]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

    （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 40 セカンダリコントローラをプロビジョニングします。

ステップ 41 展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design]をクリックしてサイトのプロファイルを変更し、もう一度 ワイヤレスコントローラ をプロビジョニングします。

ステップ 42 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 43 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 44 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 45 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 46 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 47 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

Cisco DNA Center からのシスコ ワイヤレス コントローラの高可用性の設定

シスコ ワイヤレス コントローラ高可用性（HA）を Cisco DNA Center から設定できます。現在、ワイヤレスコントローラ HA の形成および中断の両方がサポートされています。スイッチオーバーオプションはサポートされていません。

ハイ アベイラビリティ用 Cisco ワイヤレス コントローラ設定の前提条件

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが [Managed] 状態になっている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

シスコ ワイヤレス コントローラ HA の設定

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]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとして設定するコントローラ名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 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、シスコ ワイヤレス コントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

ステップ 6 [Configure HA] をクリックします。
HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリ ワイヤレス コントローラが設定されます。成功したら、セカンダリ ワイヤレス コントローラが設定されます。設定が完了したら、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 7 HA 設定を確認するには、**[Devices]** > **[Inventory]** ページで、HA デバイスとして設定したデバイスをクリックします。

ステップ 8 [Wireless Info] タブをクリックします。

[Redundancy Summary] には、[Sync Status] が [In Progress] として表示されます。Cisco DNA Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレス コントローラ（ワイヤレスコントローラ 2）は、Cisco DNA Center から削除されます。このフローは、ワイヤレスコントローラでの正常な HA 設定を示しています。

高可用性プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレス コントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。設定は、アクティブからスタンバイに同期されます。
2. [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
   - SSO が有効になっています
   - ワイヤレス コントローラがアクティブ状態になっています

- ワイヤレス コントローラがホット スタンバイ状態になっています

3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブ コントローラを指します。スタンバイ ワイヤレス コントローラのユーザー インターフェイス、Telnet、および SSH は機能しません。コンソールとサービス ポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

シスコ ワイヤレス コントローラ HA を設定するには、Cisco DNA Center で次のコマンドを送信します。

Cisco DNA Center で次のコマンドを ワイヤレスコントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center で次のコマンドを ワイヤレスコントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレスコントローラ から HA 設定を検証するには、次のコマンドを入力します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

Cisco DNA Center からの高可用性設定済みブラウンフィールドデバイスの無効化

Cisco DNA Center の高可用性無効化機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と Cisco AireOS コントローラでサポートされています。

始める前に

高可用性ブラウンフィールドデバイスが Cisco DNA Center の外部で設定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]** > **[Device]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 無効にする高可用性機能を持つワイヤレスコントローラの名前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 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

[High Availability] ページには、Cisco DNA Center の外部から設定された、選択されたワイヤレスコントローラの**冗長性の概要**が表示されます。

ステップ 4 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

選択されたワイヤレスコントローラの高可用性が正常に無効になったことを示す成功メッセージが画面の下部に表示されます。

シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、ディスカバリ機能を使用して AP を検出します。詳細については、ネットワークの検出 （19 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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

（注） 名前を入力してサイトを検索するか、[Global] を展開してサイトを選択することがします。選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

デバイスファミリや到達可能性ステータスなどのさまざまな基準に基づいてデバイスをフィルタ処理するには、[Filter] をクリックして、必要な選択を行い、[Apply] をクリックします。

ステップ 2 プロビジョニングする AP 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 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 4 [Assign Site] ステップで、次のパラメータを設定します。

a) [Choose a floor] をクリックし、サイトに AP を割り当てます。
b) [Choose a Floor] スライドインペインで、AP が存在するフロアを選択し、[Save] をクリックします。
c) [Next] をクリックします。

ステップ 5 [Configuration] ステップで、次のパラメータを設定します。

a) [Advanced Configuration] をクリックして、アンテナスロットの無線アンテナプロファイルを設定します。

（注） 高度な設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア リリース 17.6 以降を搭載した Cisco Catalyst 9130AXE ユニファイド アクセス ポイントでサポートされています。

b) [Slot 1] および [Slot 2] ドロップダウンリストから、AP 無線スロット 1 およびスロット 2 のビーム選択値を設定します。
c) [保存（**Save**）] をクリックします。
d) [RF Profile] ドロップダウンリストで、デフォルト設定をそのままにするか、リストから別の値を選択します。オプションは、**高**、**標準**、**低**です。

デフォルトの RF プロファイルは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタムプロファイルです。

e) [Mesh Role] ドロップダウンリストで、[Root] または [Mesh] を選択します。
f) [Next] をクリックします。

ステップ 6 [Summary] ステップでデバイスの詳細を確認し、[Deploy] をクリックして AP をプロビジョニングします。

[Provision Device] スライドインペインが表示されます。

ステップ 7 [Provision Device] スライドインペインで、次の手順を実行します。

- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- 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 8 AP グループの作成または変更が進行中であることを示すメッセージに続き、プロビジョニング後に AP がリブートすることを示すメッセージが表示されます。[OK] をクリックします。

展開が正常に完了した場合、[Inventory] ウィンドウの [Last Sync Status] 列に「SUCCESS」と表示されます。

FlexConnect モードの AP への ICMP ping の有効化

到達不能状態にある FlexConnect モードの AP への Internet Control Message Protocol（ICMP）ping を有効にすることができます。Cisco DNA Center は、ICMP を使用して、到達不能状態にある FlexConnect AP への ping を 5 分ごとに実行することで到達可能性を強化してから、[Inventory] ウィンドウの到達可能性ステータスを更新します。

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

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにして ICMP ping を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

「ICMP Ping status updated successfully」という成功メッセージが表示されます。

Cisco DNA Center は、シスコ ワイヤレス コントローラとの関連付けは解除されているが到達可能な FlexConnect AP への ping を開始します。到達可能性ステータスは [Inventory] ウィンドウで確認できます。

ステップ 4 到達可能性ステータスを確認するには、**[Provision]** > **[Inventory]** を選択します。

ステップ 5 デバイスが ICMP ping によって到達可能である場合、[Reachabilty] 列に [Ping Reachable] と表示されます。

Cisco AireOS Mobility Express AP の Day 0 ワークフロー

始める前に

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、1 つ以上の 802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント（AP）と、ネットワーク内のその他の AP を管理する内蔵ソフトウェアベースの ワイヤレスコントローラ で構成されます。ワイヤレスコントローラ として機能している AP をプライマリ AP といい、このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP を下位 AP といいます。

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、およびグローバル SNMPv3 クレデンシャルの設定 （191 ページ）を参照してください。
- WLAN、インターフェイス、RF プロファイルを作成します。
- DHCP サーバーにオプション #43 とオプション #60 を設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。これを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。
- インベントリに Mobility Express AP があることを確認してください。ない場合は、ディスカバリ機能を使用して検出します。詳細については、CDP を使用したネットワークの検出 （25 ページ）、IP アドレス範囲を使用したネットワークの検出 （32 ページ）、およびインベントリについて （51 ページ）を参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

ステップ 1 Cisco Mobility Express は DHCP サーバーに接続し、Cisco DNA Center プラグアンドプレイサーバーに接続します。

ステップ 2 DHCP サーバーは、オプション #43 を使用して IP アドレスを割り当てます。オプション #43 は、 Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。

ステップ 3 Mobility Express AP は PnP エージェントを開始し、PnP サーバーに接続します。

（注） ネットワーク内に一連の Mobility Express AP がある場合、内部プロトコルを通過します。プロトコルは 1 つの Mobility Express AP を選択します。これは、シスコ ワイヤレス コントローラで、PnP サーバーに到達するためのプライマリ AP として設定されます。

ステップ 4 [Provision] > [Devices] > [Plug and Play] タブで未要求 AP を検索します。 > >

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onbording Status] が [Initialized] になるまで待機する必要があります。

ステップ 5 この AP を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 6 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 7 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 10 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 11 **[Save]** をクリックします。

ステップ 12 **[Next]** をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 13 [Summary] ページで [Claim] をクリックします。

Mobility Express AP が要求されると、設定された IP アドレスが Mobility Express AP に割り当てられます。

ステップ 14 要求されたデバイス（AP）と ワイヤレスコントローラ は、**[Provision]** > **[Device Inventory]** > **[Inventory]** ページで確認できるようになりました。

ステップ 15 また、CSV ファイルからデバイスを一括して追加することもできます。

詳細については、「デバイスの一括追加 （374 ページ）」を参照してください。

CSV を使用して Mobility Express AP を一括インポートすると、すべての Mobility Express AP が **[Device]** > **[Plug and Play]** ページに表示されます。VRRP プロトコルに基づいて、インポートされた Mobility Express AP のうち 1 台だけがプライマリ AP になって要求に応じ、残りは下位 AP になります。プライマリ AP

を要求した後、下位 AP を要求する必要はありません。Cisco DNA Center は、[Plug and Play] ページから下位 AP をクリアしません。これらの下位 AP は、**[Devices]** > **[Plug and Play]**ページから手動で削除する必要があります。

ステップ 16 シスコ ワイヤレス コントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （391 ページ） を参照してください。

ステップ 17 AP をプロビジョニングするには、#unique_194 を参照してください。

Cisco AireOS コントローラのためのブラウンフィールドのサポート

始める前に

Cisco DNA Center を使用すると、シスコ ワイヤレス コントローラなどのブラウンフィールド デバイスをネットワークに追加してプロビジョニングできます。ブラウンフィールドとは、既存サイトの以前から存在しているインフラストラクチャに属しているデバイスのことです。

この手順では、Cisco DNA Center を使用して、ブラウンフィールド Cisco AireOS コントローラをプロビジョニングする方法を示します。

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。詳細については、ネットワークの検出 （19 ページ）およびインベントリについて （51 ページ）を参照してください。
- ワイヤレスコントローラ は到達可能で、 [インベントリ（Inventory）] ウィンドウで管理状態でなければなりません。詳細については、インベントリについて （51 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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタの場合、デバイスの名前を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 3 プロビジョニングする ワイヤレスコントローラ デバイス名の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 5 [Assign Site] ステップで、サイトをコントローラに関連付けます。

a) [Choose a site] をクリックして、コントローラにサイトを割り当てます。
b) [Choose a site] スライドインペインで、ワイヤレスコントローラ を関連付けるサイトを選択し、[Save] をクリックします。
c) [Next] をクリックします。

ステップ 6 [Resolve Conflict] ステップに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。

ステップ 7 [Next]をクリックします。

ステップ 8 [Design Object] ウィンドウに、学習したすべての設定が一覧表示されます。

a) 左ペインで [Network] をクリックします。

右側のペインに、デバイス設定学習の一部として学習されたネットワーク設定と、次の情報が表示されます。

- [AAA サーバー（AAA Server）] の詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。
- [DHCP Server] の詳細。
- AAA サーバーの共有秘密を入力します。

b) 左ペインで [ワイヤレス（Wireless）] をクリックします。

右側のペインには、企業 SSID、ゲスト SSID、アンテナ無線プロファイル、およびワイヤレスインターフェイスの詳細が一覧表示されます。

事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

c) 左ペインで [破棄された設定（Discarded Config）] をクリックします。

右ペインに、Cisco DNA Center 上で競合する設定、または既に存在する設定が一覧表示されます。破棄された設定エントリは、次のように分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイス設定

d) [Next]をクリックします。

[ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

e) **[Save]** をクリックします。

「ブラウンフィールド設定に成功しました（`Brownfield Configuration is Successful`）」というメッセージが表示されます。

ステップ 9 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 10 [Network Profiles] ウィンドウで、次の項目を設定します。

a) [Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

b) [サイトをプロファイルに追加（Add Sites to Profile）] ウィンドウでドロップダウンリストからサイトを選択して、[保存（Save）] をクリックします。

ステップ 11 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

a) [Filter] をクリックして、プロビジョニングするデバイスを見つけます。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

b) プロビジョニングするコントローラ デバイス名の隣にあるチェック ボックスをオンにします。
c) [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。
d) [サイトの割り当て（Assign Site）] ウィンドウで詳細を確認して、[次へ（Next）] をクリックします。

[Configurations] ステップが表示されます。

e) [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。
f) [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。
g) [Next] をクリックします。

ステップ 12 次の情報が表示される [Summary] ステップを確認します。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **Interfaces**

ステップ 13 [展開（Deploy）] をクリックします。

ステップ 14 [Provision Devices] スライドインペインで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

（注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。

- [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から N 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレスコントローラ。
- Catalyst 9800-80 ワイヤレスコントローラ。
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS、および Hyper-V）に展開可能、Cisco DNA Center で管理可能。
- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ。
- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを一覧表示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレスコントローラ	最大 6000 アクセスポイントと 64,000 クライアントをサポートします。 最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。 最大 100-GE のアップリンクおよびシームレスなソフトウェアアップデートを搭載したモジュール型ワイヤレスコントローラ。
Cisco Catalyst 9800-40 ワイヤレスコントローラ	シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。 最大 2000 アクセスポイントと 32,000 クライアントをサポートします。 最大 40 Gbps のスループットをサポートし、1 ラックユニットスペースを使用します。 4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ	Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、プライベートクラウドまたはパブリッククラウドに Infrastructure as a Service（IaaS）として導入できます。 Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、ハイアベイラビリティとセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。 Cisco Catalyst 9800-CL クラウド ワイヤレスコントローラの仮想フォームファクタは、ESXi、KVM、Cisco ENCS、および Hyper-V ハイパーバイザをサポートするプライベートクラウド向けです。
Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレス インフラストラクチャを一貫したポリシーと管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリックモードでのみアクセスポイント（AP）をサポートします。
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。 • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ（9800-L-C RJ45） • Cisco Catalyst 9800-L ファイバ シリーズ ワイヤレス コントローラ（9800-L-F SFP）

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を一覧表示します。

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[7] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

[7] ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。（A required disk image was missing）」という警告が表示され、「VM の展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。（Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.）」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1）ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする（ESXI 6.5 クライアントバージョン 1.29.0 はテスト済みで必須）。2）OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Cisco DNA Center でサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）のバージョンを示します。

（注） Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS 3.11.x からは Cisco Enterprise NFVIS 3.12.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 4.1.x へのアップグレードはサポートされていません。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム デバイス プラットフォーム	注記
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Cisco DNA Center は、次の NFVIS アップグレードパスをサポートします。NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2。 Cisco Enterprise NFVIS 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 3.12.1 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.12.1 から Cisco Enterprise NFVIS 3.12.2 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.2 から 3.12.2 へのアップグレードはサポートされていません。 Cisco Enterprise NFVIS 3.12.2 は、Cisco DNA Center でサポートされています。
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. ソフトウェアイメージのアップグレードに関する詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート（412 ページ） を参照してください。

3. Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。

   Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System Settings]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

4. Cisco Identity Services Engine と Cisco DNA Center を連動させます。統合後、関連する設定やデータとともに Cisco DNA Center が検出されたデバイスは、Cisco ISEにプッシュされます。

5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

   詳細については、CDP を使用したネットワークの検出 （25 ページ）またはIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

   ワイヤレス管理 IP アドレスを手動で追加する必要があります。

   [Discovery] ウィンドウで Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択して、デバイスのループバック インターフェイスの IP アドレスを指定します。

6. 検出されたデバイスが [Device Inventory] ページに [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （51 ページ）およびインベントリに関する情報の表示 （53 ページ）を参照してください。

   デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアシュアランス接続を確認するには、次のコマンドを使用します。

   - **#show crypto pki trustpoints | sec DNAC-CA**

     ```
     Trustpoint DNAC-CA
         Subject Name:
         cn=kube-ca
               Serial Number (hex): 00E***************
         Certificate configured.
     ```

   - **#show crypto pki trustpoints | sec sdn-network**

     ```
     Trustpoint sdn-network-infra-iwan:
         Subject Name:
         cn=sdn-network-infra-ca
             Serial Number (hex): 378***************
         Certificate configured.
     ```

   - **#show telemetry ietf subscription all**

     ```
     Telemetry subscription brief

       ID               Type        State       Filter type
       ---------------------------------------------------
       1011             Configured  Valid       tdl-uri
       1012             Configured  Valid       tdl-uri
       1013             Configured  Valid       tdl-uri
     ```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. 認証サーバーとポリシーサーバーの設定時に TACACS サーバーを設定します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザー名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロード （127 ページ）を参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

10. AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

    詳細については、「AP の追加、配置、および削除 （135 ページ）」を参照してください。

11. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

    詳細については、グローバルネットワーク設定の管理 （184 ページ）、グローバル ネットワーク サーバーの設定 （204 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

    詳細については、「ワイヤレス無線周波数プロファイルの作成 （168 ページ）」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

Cisco DNA Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

IP アドレスプールを作成するには、IP アドレス プールを設定する （197 ページ）を参照してください。

プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「LAN アンダーレイのプロビジョニング」を参照してください。

14. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Centerは地理的な場所全体でさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）を参照してください。

15. バックホールの設定を行います。詳細については、

16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Policy] ウィンドウで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワーク （478 ページ）および仮想ネットワークの作成を参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成 （276 ページ）」を参照してください。

17. 高可用性を設定します。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する （413 ページ）」を参照してください。

18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （429 ページ）」を参照してください。

19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

    詳細については、アプリケーション ポリシーの作成 （317 ページ）、アプリケーション ポリシーの展開 （323 ページ）、およびアプリケーション ポリシーの編集 （321 ページ）を参照してください。

（注） アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラデバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

  詳細については、CDP を使用したネットワークの検出 （25 ページ）またはIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

  詳細については、インベントリについて （51 ページ）およびインベントリに関する情報の表示 （53 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**[Design]** > **[Image Repository]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアイメージをインポートします。

詳細については、「ソフトウェア イメージのインポート （104 ページ）」を参照してください。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て （105 ページ）」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「ゴールデン ソフトウェア イメージの指定 （107 ページ）」を参照してください。

ステップ 5 ソフトウェアイメージのプロビジョニング

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

ステップ 6 [Inventory] ウィンドウで、イメージをアップグレードする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニング （109 ページ）を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性（HA）を設定するには、次の前提条件を満たす必要があります。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスが同じソフトウェアバージョンを実行していて、プライマリ Catalyst 9800 シリーズ ワイヤレス コントローラ上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH回線設定、NETCONF-YANG設定などの事前設定は、Catalyst 9800 シリーズ ワイヤレス コントローラアプライアンスで完了します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Cisco DNA Center から正常に実行されます。
- デバイスは到達可能で、[Managed] 状態になっています。

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]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレスコントローラのリストを取得します。

ステップ 4 [Inventory] ウィンドウで目的の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 名をクリックし、プライマリコントローラとして設定します。

ステップ 5 [High Availability] タブをクリックします

デフォルトで選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドはグレー表示されます。

ステップ 6 [Select Primary Interface] および [Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 7 [Select Secondary C9800] ドロップダウン リストから、HA ペアを作成するセカンダリコントローラを選択します。

ステップ 8 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

（注） 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Catalyst 9800 シリーズ ワイヤレス コントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 9 [Netmask] フィールドに、ネットマスクアドレスを入力します。

ステップ 10 [Configure HA] をクリックします。

HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HA が有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 11 HA が開始されたら、[High Availability] タブの [Redundancy Summary] に、[Sync Status] が [HA Pairing is in Progress]として表示されます。HA ペアリングが成功したことを Cisco DNA Center が検出すると、[Sync Status] が [Complete] になります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ（Catalyst 9800 シリーズ ワイヤレス コントローラ 2）が Cisco DNA Center から削除され

ます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラ での正常な HA 設定を示しています。

ステップ 12 手動でコントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 13 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 14 プロセスが完了した後に発生するアクションのリストを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン（SSO）を使用して設定されます。デバイスは、ロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートするために再起動します。設定はアクティブからスタンバイへと同期されます。
- [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
  - SSO は有効
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 がアクティブ状態である
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 2 がスタンバイ状態である

ハイ アベイラビリティについて

高可用性（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Cisco DNA Center を介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリに高可用性を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリに高可用性を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip
1.1.1.2
```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリに HA を設定するには、次のコマンドを使用します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレス コントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリに HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
  ```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラから高可用性設定を検証します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。
- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラデバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。

- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- ハイアベイラビリティ設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性

N+1 高可用性の概要

Cisco DNA Center は、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 プラットフォームで N+1 高可用性（HA）をサポートします。

HA-SKU を使用した N+1 HA は、Cisco 2504、5500、7500、および 8500 シリーズのスタンドアロン ワイヤレス コントローラおよび WiSM2 コントローラでサポートされています。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンター間のコントローラに冗長性をもたらします。

N+1 HA では、単一のシスコ ワイヤレス コントローラを複数のプライマリコントローラのバックアップコントローラとして使用できます。これらのワイヤレスコントローラは互いに独立していて、インターフェイスの設定や IP アドレスを共有しません。

Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリコントローラの設定をサポートします。

N+1 HA は AP レベルごとに設定され、設定はグローバルレベルではなく AP に直接プッシュされます。

AP フォールバックオプションが有効の場合、プライマリ ワイヤレスコントローラ が動作を再開すると、AP はバックアップ ワイヤレスコントローラ からプライマリ ワイヤレスコントローラ に自動的にフォールバックします。

（注） プライマリコントローラとセカンダリコントローラは、同じデバイスタイプである必要があります。たとえば、プライマリデバイスが Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、セカンダリデバイスも Cisco Catalyst 9800 シリーズ ワイヤレス コントローラである必要があります。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

このリリースでは、N+1 HA 設定に次の制限があります。

- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。

- 耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチ オーバー（AP SSO）機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points（CAPWAP）ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Cisco DNA Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

  詳細については、CDP を使用したネットワークの検出 （25 ページ）またはIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

- ワイヤレスコントローラが到達可能で、[Managed] 状態である必要があります。

  詳細については、インベントリについて （51 ページ）およびインベントリに関する情報の表示 （53 ページ）を参照してください。

- デバイス間のネットワーク接続を確認します。プライマリコントローラがダウンした場合、AP が N+1 の設定に従ってセカンダリコントローラに参加できるようにする必要があります。

- 2 つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング A とビルディング B のような 2 つのビルディングを作成し、ビルディング A をコントローラ 1 のプライマリ管理場所かつコントローラ 2 のセカンダリ管理場所に設定し、ビルディング B をコントローラ 2 のプライマリ管理場所としてのみ設定できます。

  詳細については、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

  詳細については、「AP の追加、配置、および削除 （135 ページ）」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）とゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）を参照してください。

Cisco DNA Center からの N+1 高可用性の設定

この手順では、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 コントローラで N+1 高可用性（HA）を設定する方法を示します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 4 プライマリコントローラのプライマリ管理 AP 場所を割り当てるには、[Choose a site] をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。

ステップ 6 [Next] をクリックします。

[Configuration] ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。

ステップ 7 [Select Primary Managed AP Locations] をクリックして、プライマリコントローラの管理対象 AP のロケーションを追加または更新できます。

ステップ 8 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 9 インターフェイスと VLAN の詳細を設定します。

ステップ 10 [Configure Interface and VLAN] 領域で、IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 11 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 12 [Summary] ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイス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。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。

ステップ 13 次に、セカンダリコントローラをプロビジョニングします。

ステップ 14 [Inventory] ウィンドウで目的のコントローラの隣にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。

ステップ 15 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 16 セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。

セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。

ステップ 17 [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 18 **[Next]** をクリックします。

[Configuration] ウィンドウが表示され、セカンダリデバイスのプライマリ管理対象 AP の場所とセカンダリ管理対象 AP の場所が表示されます。

ステップ 19 [Select Secondary Managed AP Locations] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。

ステップ 20 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 21 セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。

ステップ 22 [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 23 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 24 [Summary] ウィンドウで、セカンダリコントローラの管理対象 AP の場所やその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイス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。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。

ステップ 25 プライマリコントローラおよびセカンダリコントローラの管理対象場所を確認するには、**[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。

ステップ 26 [Device details] ウィンドウで、[Managed ap locations] タブをクリックして、プライマリおよびセカンダリの管理対象場所の詳細を表示します。

ステップ 27 プライマリコントローラの AP をプロビジョニングします。

ステップ 28 **[Network Devices]** > **[Inventory]** ウィンドウで、プロビジョニングする AP の横にあるチェックボックスをオンにします。

ステップ 29 [Action] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

ステップ 30 [Assign Site] ウィンドウで、[Choose a Floor] をクリックして、プライマリの管理対象場所からフロアを選択します。

ステップ 31 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 32 デフォルトでは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタム RF プロファイルが、[RF Profile] ドロップダウンリストで選択されています。

[RF Profile] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。

ステップ 33 **[Next]** をクリックします。

ステップ 34 [Summary] ウィンドウで、詳細を確認します。

ステップ 35 [Deploy] をクリックして、プライマリ AP をプロビジョニングします。

ステップ 36 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後にAPがリブートします。続行しますか?（After provisioning AP(s) will reboot. Do you want to continue?）」というメッセージが表示されます。

ステップ 37 [OK] をクリックします。

展開が成功すると、[Device Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

モビリティ設定の概要

Cisco DNA Center のモビリティ設定では、一連の シスコ ワイヤレス コントローラ をモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なる ワイヤレスコントローラ に割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Cisco DNA Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定には、次の注意事項および制限事項があります。

- [Provision] ページでは、モビリティを設定するために複数のコントローラを選択することはできません。
- グループ名をデフォルトにしてモビリティグループを作成することはできません。これにより、モビリティおよび RF グループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOS コントローラでモビリティグループを設定しているときに仮想 IP アドレスが変更された場合は、ワイヤレスコントローラ を手動で再起動する必要があります。
- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に 1 つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレスコントローラ に IP アドレス 192.0.2.1 がない場合、Cisco DNA Center は仮想 IP アドレス 192.0.2.1 をすべての ワイヤレスコントローラ にプッシュします。

- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[Mobility Configuration] ページでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレスコントローラをゲストアンカーとしてプロビジョニングする場合は、それがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコ ワイヤレス コントローラ でモビリティを設定するために使用できるワークフローを示します。

- モビリティ設定は、[Provision] ページの [Configuration] ウィンドウで使用できます。
- モビリティを設定するには、モビリティグループ名、RF グループ名、およびモビリティピアを使用して ワイヤレスコントローラ をプロビジョニングする必要があります。
- ワイヤレスコントローラ のプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレスコントローラ を再同期して、最新のトンネルステータスを取得します。

モビリティ設定の使用例

次の使用例では、コントローラ間のモビリティの設定手順について説明します。

使用例 1

シスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、およびワイヤレスコントローラ 3 は、モビリティグループ名（デフォルト）を使用して Cisco DNA Center に新たに追加されていて、まだプロビジョニングされていません。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレスコントローラ 2 および ワイヤレスコントローラ 3 をピアとして追加することによって、ワイヤレスコントローラ 1 をプロビジョニングします。
2. ワイヤレスコントローラ 2 をプロビジョニングします。

   [Provision] ウィンドウでは、ワイヤレスコントローラ 2 のモビリティ設定がグループ名とピアとともに自動的に入力されます。
3. ワイヤレスコントローラ 3 をプロビジョニングします。
4. すべての ワイヤレスコントローラ をプロビジョニング後、ワイヤレスコントローラ を再同期して、最新のトンネルステータスを受信します。

使用例 2

異なるモビリティグループ名を持つシスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、および ワイヤレスコントローラ 3はすでに Cisco DNA Center に追加され、プロビジョニングされています。

1. モビリティグループ名、RF グループ名を設定してワイヤレスコントローラ 1 をプロビジョニングし、ピアとしてワイヤレスコントローラ 2 およびワイヤレスコントローラ 3 を追加します。
2. モビリティ設定は、ワイヤレスコントローラ 2、ワイヤレスコントローラ 3 などの他のピア間で自動的に複製されます。
   - ワイヤレスコントローラ 1 のプロビジョニングが成功すると、ワイヤレスコントローラ 2 と ワイヤレスコントローラ 3 がピアとして ワイヤレスコントローラ 1 に追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 3 は、ワイヤレスコントローラ 2 のピアとして追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 は、ワイヤレスコントローラ 3 のピアとして追加されます。

モビリティグループの設定

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 **[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 3 モビリティを設定する Catalyst 9800 シリーズ ワイヤレス コントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision WLC Mobility]** の順に選択します。

[Configure Mobility Group] サイドパネルが表示されます。

詳細については、「モビリティ設定の概要 （421 ページ）」を参照してください。

ステップ 5 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択できます。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 6 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 7 モビリティの暗号化設定を有効または無効にするには、[DTLS High Cipher Only] ボタンをクリックします。

暗号方式の設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.5 以降に適用されます。変更を有効にするには、デバイスを手動で再起動する必要があります。

ステップ 8 DTLS（Data Datagram Transport Layer Security）暗号方式の設定を変更した後にデバイスを手動で再起動して、プロビジョニング後に変更を有効にするには、[Restart for DTLS Ciphers to take effect] ボタンをクリックします。

ステップ 9 DTLS データ暗号化を有効にするには、[Data Link Encryption] ボタンをクリックします。

ステップ 10 [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。

ステップ 11 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、 Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 12 **[Save]** をクリックします。

ステップ 13 モビリティグループ名と RF グループ名をリセットするには、次のいずれかの方法を実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

DTLS 暗号スイートについて

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。

リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ、および Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ プラットフォームでは複数の DTLS（Data Datagram Transport Layer Security）暗号スイートを設定できます。

複数の DTLS 暗号スイートの設定

DTLS 暗号スイートは、グローバルレベルまたはサイトレベルで設定できます。

始める前に

- **[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]** ページでデバイス可制御性機能が有効になっていることを確認します。
- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

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**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 同じ DTLS 暗号スイート設定ですべてのサイトを設定するには、左側のツリーメニューで [Global] を選択します。

DTLS暗号スイートをサイトレベルで設定するには、左側のツリーメニューでサイトを選択します。DTLS暗号スイートの設定は、その特定のサイトで使用可能なコントローラにプッシュされます。

ステップ 3 暗号スイートをデバイスの可制御性の一部として設定するには、[Skip DTLS Ciphersuite Config] チェックボックスをオフにします。

ステップ 4 デフォルト暗号スイートまたはカスタム暗号スイートを設定します。

デフォルトでは、**デフォルト**暗号スイートが選択されています。

[Default Ciphersuite] ボックスにはデフォルト暗号スイートのリストが示され、これらの暗号スイートが、デバイスでデフォルトとして設定されています。これらのデフォルト暗号スイートの優先順位は変更できません。

ステップ 5 カスタム暗号スイートを設定するには、[Custom] ボタンをクリックします。

カスタム暗号スイートは、優先順位に従ってデフォルト暗号スイートを上書きします。

ステップ 6 [Version] ドロップダウンリストから、DTLS のバージョンを選択します。

Cisco DNA Center は、DTLS のバージョンに基づいて、使用可能な暗号スイートを表示します。

ステップ 7 暗号スイートを適用しない場合は、その暗号スイートの横にある青色のボタンをクリックします。

ステップ 8 暗号スイートの優先順位を変更するには、各暗号スイートをクリックしたままドラッグします。

ステップ 9 [**保存**（**Save**）] をクリックします。

「DTLS Ciphersuite Config Saved successfully」というメッセージが表示されます。

ステップ 10 暗号スイートの設定を適用するには、デバイスをプロビジョニングする必要があります。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （429 ページ）を参照してください。

N+1 ローリング AP アップグレードについて

Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの N+1 高可用性設定では、ローリング AP アップグレード機能がサポートされます。この機能は、ワイヤレス LAN ネットワーク内の Cisco AireOS コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP のソフトウェアイメージをアップグレードするのに便利です。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードすることができます。

プライマリコントローラは、無線リソース管理ネイバー AP マップを使用して、候補の AP を識別します。アップグレードプロセスは、イメージが候補の AP に事前ダウンロードされている間に、ソフトウェアイメージをプライマリコントローラにダウンロードすることから始まります。候補の AP がアップグレードされて再起動されると、これらの AP は、セカンダリコントローラに段階的に参加します。すべての AP がセカンダリコントローラに参加した後、プライマリコントローラは再起動します。これらの AP は、再起動された後、段階的にプライマリコントローラに再度参加します。

次に、ローリング AP アップグレードを設定するための前提条件を示します。

- 2 つの ワイヤレスコントローラ（1 つはプライマリコントローラ、もう 1 つはセカンダリとして）の N+1 ハイアベイラビリティ設定。
- プライマリコントローラと N+1 コントローラの設定は同じで、ネットワーク内の同じ場所を管理します。
- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。

  ゴールデンイメージは、ネットワークデバイスの標準化されたイメージであり、Cisco DNA Center は Cisco.com からイメージを自動的にダウンロードします。イメージの標準化は、デバイスのセキュリティと、デバイスのパフォーマンスの最適化に役立ちます。
- N+1 コントローラはに到達可能であり、Cisco DNA Center で [Managed] 状態になっています。
- 両方のコントローラが同じモビリティグループの一部であり、プライマリコントローラと N+1 コントローラの間にモビリティトンネルが確立されます。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。

ローリング AP アップグレードを設定するワークフロー

この手順では、Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでローリング AP アップグレードを設定する方法を示します。

（注） N+1 ローリング AP アップグレードは、ファブリックおよび非ファブリックの展開でサポートされています。

ステップ 1 Cisco DNA Center をインストールします。

詳細については、Cisco Digital Network Architecture Center 設置ガイド [英語] を参照してください。

ステップ 2 Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

ステップ 3 ディスカバリ機能を使用して ワイヤレスコントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

詳細については、CDP を使用したネットワークの検出 （25 ページ）またはIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

ステップ 4 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

詳細については、インベントリについて （51 ページ）およびインベントリに関する情報の表示 （53 ページ）を参照してください。

デバイスが [Managed] になるまで待機する必要があります。

ステップ 5 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロード （127 ページ）を参照してください。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

ステップ 6 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「AP の追加、配置、および削除 （135 ページ）」を参照してください。

ステップ 7 プライマリ管理対象 AP の場所、およびローリング AP アップグレードが有効になっていて、モビリティグループがセカンダリコントローラをピアとして設定されている状態で、プライマリコントローラをプロビジョニングします。

これを行うには、**[Provision]** > **[Devices]** > **[Inventory]** の順に選択し、プライマリコントローラ名の横にあるチェックボックスをオンにします。

ステップ 8 モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。

詳細については、「モビリティ設定の概要 （421 ページ）」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することによって、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、Cisco AireOS コントローラのプロビジョニング （391 ページ）および Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （429 ページ）を参照してください。

ステップ 10 プライマリコントローラに関連付けられている AP をプロビジョニングします。

詳細については、「#unique_194」を参照してください。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

詳細については、「ソフトウェア イメージのインポート （104 ページ）」を参照してください。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て （105 ページ）」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、ゴールデン ソフトウェア イメージの指定 （107 ページ）を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、**[Provision]** > **[Devices]** > **[Software Images]** の順に選択します。
- イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 **[Provision]** > **[Devices]** > **[Software Images]** ページで、プライマリコントローラの横にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニング （109 ページ）を参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニターするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ページには、次の情報が表示されます。

- [Distribution Operation]：イメージ配信プロセスに関する情報が表示されます。イメージは Cisco DNA Center からプライマリデバイスにコピーされます。配信プロセスが完了すると、アクティブ化操作が開始されます。
- [Activate Operation]：アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation]：ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに参加している AP の数など、ローリング AP アップグレードの概要が表示されます。

  [View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニングを行う前に、Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー（408 ページ） の手順を完了したことを確認します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名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 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 4 [Assign Site] ウィンドウで、[Assign Site] をクリックしてサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 **[Next]** をクリックします。

[Configuration] ウィンドウが表示されます。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのブラウンフィールドサポート

Cisco DNA Center を使用すると、シスコ ワイヤレス コントローラや Cisco Catalyst 9800 シリーズ ワイヤレス コントローラなどのブラウンフィールドデバイスをネットワークに追加してプロビジョニングできます。ブラウンフィールドとは、既存サイトの以前から存在しているインフラストラクチャに属しているデバイスのことです。

ここでは、Cisco DNA Center によるブラウンフィールドの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニングについて説明します。

始める前に

- インベントリに Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ があることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。詳細については、ディスカバリについて（19 ページ）を参照してください。

- Catalyst 9800 シリーズ ワイヤレス コントローラ が到達可能で、[Inventory] ウィンドウで [Managed] 状態であることを確認します。詳細については、インベントリについて （51 ページ）を参照してください。
- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。新しいネットワーク階層を作成できるほか、Cisco Prime Infrastructure に既存のネットワーク階層がある場合はその階層を Cisco DNA Center にインポートすることもできます。

  既存のネットワーク階層のインポートとアップロードの詳細については、既存のサイト階層をアップロード （127 ページ）を参照してください。

  新しいネットワーク階層の作成については、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、ビルディングへのフロアの追加 （132 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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。このウィンドウには、ネットワークで使用できる検出済みのすべてのデバイスが一覧表示されます。

ステップ 2 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ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 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 4 [Assign Site] ステップで、次のパラメータを設定します。

a) [Choose a site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ にサイトを割り当てます。

b) [Choose a site] ウィンドウで、Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けるサイトを選択し、[Save] をクリックします。

c) **[次へ (Next)]** をクリックします。

ステップ 5 [Resolve Conflict] ステップに Cisco DNA Center および Catalyst 9800 シリーズ ワイヤレス コントローラで使用可能な構成が表示されます。解決する必要がある、競合する構成は、赤いボックスで強調表示されています。

[Choose this config in Cisco DNA Center] セクションに Cisco DNA Center で使用可能な構成が表示され、[Choose this config in Device] セクションに Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスで使用可能な構成が表示されます。

a) Cisco DNA Center の構成を保持するには、[Choose this config] セクションで対応する赤色のボックスをクリックして、保持する構成を選択します。これにより、デバイス設定が上書きされます。

たとえば、Cisco DNA Center が SSID の認証タイプとして Open を使用していて、デバイスが認証タイプとして wpa2_enterprise を使用している場合、保持する構成を決定できます。Cisco DNA Center の構成を保持するには、[Choose this config] で [Open] を選択します。Cisco DNA Center の構成を保持すると、デバイスの構成が上書きされます。

デバイスの構成を保持するには、[Choose this config in Device] セクションで対応する赤色のボックスをクリックして、保持する構成を選択します。デバイスの構成を保持すると、Cisco DNA Center の構成が上書きされることに注意してください。

b) [Warning] ダイアログボックスで [OK] をクリックします。

c) **[次へ (Next)]** をクリックします。

[Design Object] ウィンドウに、デバイスで学習された構成が一覧表示されます。

ステップ 6 [Design Object] ステップで次の項目を設定します。

a) 左ペインで [Network] をクリックします。右側のペインに、デバイス構成学習プロセスの一部として学習されたネットワーク構成と、次の情報が表示されます。

- [AAA サーバー（AAA Server）] の詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。
- [HCP Server] には、デバイスで使用可能なすべての DHCP サーバーに関する詳細が表示されます。
- [NTP Server] には、デバイスで使用可能なすべての NTP サーバーに関する詳細が表示されます。
- AAA サーバーの共有秘密を入力します。

b) 左ペインで [ワイヤレス（Wireless）] をクリックします。デバイスに存在するエンタープライズ SSID、ゲスト SSID、ワイヤレスインターフェイス、アンテナ無線プロファイル、および RF プロファイルが表示されます。

事前共有キー（PSK）を使用する SSID の場合、[事前共有キー] を指定する必要があります。

c) 左ペインで [Ignored Config] をクリックします。

Cisco DNA Center の競合する構成と既存の構成が表示されます。破棄される構成エントリは次のカテゴリに分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイスの設定

d) [Next]をクリックします。

ステップ 7 [Network Profile] ステップに AP と WLAN の組み合わせに基づいて作成されたネットワークプロファイルまたはサイトプロファイルが一覧表示されるので、それらを確認し、[Save] をクリックします。

「ブラウンフィールド設定に成功しました（`Brownfield Configuration is Successful`）」というメッセージが表示されます。

ステップ 8 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Design]** > **[Network Profiles]** の順に選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 9 [Network Profiles] ウィンドウで、次の項目を設定します。

a) [Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

b) [Add Sites To Profile] スライドインペインで、サイトの横にあるチェックボックスをオンにして、このプロファイルを関連付けます。

c) [**保存（Save）**] をクリックします。

ステップ 10 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 11 [Filter] をクリックして、プロビジョニングするデバイスを見つけます。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 12 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

ステップ 13 [Actions] ドロップダウンリストから、**[Provision]** > > **[Provision Device]** の順に選択します。

ステップ 14 [Assign Site] ステップで詳細を確認して、[Next] をクリックします。

ステップ 15 [Configuration] ステップで、次の項目を設定します。

a) [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

b) [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

c) [Next] をクリックします。

ステップ 16 次の情報が表示される [Summary] ステップを確認します。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **ローリング AP アップグレード**
- **インターフェイス**

ステップ 17 [展開（Deploy）] をクリックして、デバイスをプロビジョニングします。

a) デバイスを今すぐ展開するか、または展開を後の時間でスケジュールするかどうかを求められます。

デバイスを今すぐ展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

将来の日付と時刻でデバイスの展開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、展開する日時を定義します。

ステップ 18 AP をプロビジョニングします。

詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （398 ページ）を参照してください。

Cisco Embedded Wireless Controller on Catalyst Access Points 対応 Day 0 ワークフロー

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（EWC AP）は、次世代の Wi-Fi ソリューションであり、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に Cisco Catalyst 9100 シリーズアクセスポイントを統合し、進化および成長し続ける組織にそのクラスで最高のワイヤレスエクスペリエンスをもたらします。

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。

  詳細については、ネットワーク階層のサイトの作成（125 ページ）、建物の追加（130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。

  詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、およびグローバル SNMPv3 クレデンシャルの設定 （191 ページ）を参照してください。

- SSID、ワイヤレスインターフェイス、および無線周波数プロファイルを作成します。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）、ゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）、ワイヤレスインターフェイスの作成 （168 ページ）、およびワイヤレス無線周波数プロファイルの作成（168 ページ）を参照してください。

（注） Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ では、Flex ベースの SSID の作成のみがサポートされています。

- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が接続されているスイッチでオプション #43 を使用して DHCP サーバーを設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。これを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。

- インベントリに Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ があることを確認します。ない場合は、ディスカバリ機能を使用して検出します。詳細については、CDP を使用したネットワークの検出 （25 ページ）、IP アドレス範囲を使用したネットワークの検出 （32 ページ）、およびインベントリについて （51 ページ）を参照してください。

- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、次のような複数のフォームファクタで使用できます。

- Catalyst 9115AX アクセスポイント上の Cisco 組み込みワイヤレスコントローラ
- Catalyst 9117AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9120AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9130AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ

ステップ 1 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が DHCP サーバーと通信します。

DHCP サーバーは、応答で、オプション #43 とともに IP アドレスを提供します。オプション #43 には、Cisco プラグアンドプレイサーバーの IP アドレスが含まれています。

ステップ 2 オプション #43 に基づいて、 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ はプラグアンドプレイ エージェントをオンにし、Cisco DNA Center プラグアンドプレイサーバーに接続します。

（注） ネットワーク内に Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ のセットがある場合、それらは内部プロトコルを通過します。プロトコルは、PnP サーバーに到達するために シスコ ワイヤレス コントローラ 上でプライマリ AP として設定されている 1 つの Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を選択します。

ステップ 3 [Provision] > [Devices] > [Plug and Play] タブで未要求 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を検索します。 > >

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onboarding State] 列の下でオンボーディングステータスが [Initialized] になるまで待つ必要があります。

ステップ 4 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 6 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 9 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**

- **[Subnet Mask]**
- **[Gateway]**

ステップ 10 **[Save]** をクリックします。

ステップ 11 **[Next]** をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 12 [Summary] ページで [Claim] をクリックします。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が要求されると、設定された IP アドレスが Cisco Embedded Wireless Controller に割り当てられます。

ステップ 13 要求されたデバイス（内部 AP を備えた Cisco Embedded Wireless Controller）は、[Provision] > [Devices] > [Inventory] ウィンドウの下で使用可能になりました。 > >

ステップ 14 AP をプロビジョニングするには、#unique_194 を参照してください。

ステップ 15 追加の Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （391 ページ） を参照してください。

ステップ 16 CSV ファイルからデバイスを一括インポートするには、デバイスの一括追加 （374 ページ） を参照してください。

ステップ 17 デバイスを手動で追加するには、「デバイスの追加または編集」を参照してください。

Cisco DNA Center を使用した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの Cisco AireOS コントローラの移行

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。
- ディスカバリ機能を実行して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態になっていることを確認します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。NETCONF は、ネットワークの設定をインストール、操作、削除するためのメカニズムです。
- Cisco AireOS コントローラを検出して、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態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（≡）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Cisco AireOS コントローラ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 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 5 [Add Sites] ウィンドウで、Cisco AireOS コントローラと関連付けるサイト名の横にあるチェックボックスをオンにします。

ステップ 6 [**保存（Save**）] をクリックします。

ステップ 7 [Action] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択して、Cisco AireOS コントローラデバイスから構成を学習します。

ステップ 8 [Assign Site] ウィンドウで、[Next] をクリックします。

ステップ 9 [Resolve Conflict] ウィンドウに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。[Next]をクリックします。

ステップ 10 [Design Object] ウィンドウで、[Next] をクリックします。

ステップ 11 左側のペインで [Network] をクリックします。

右側のペインに、デバイス構成学習プロセスの一部として学習されたネットワーク構成と、次の情報が表示されます。

- AAA サーバーの詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。パスワードは暗号化されており、Cisco DNA Center はパスワードを学習できないため、AAA サーバーの共有秘密を入力します。
- HCP サーバー。デバイスで使用可能なすべての DHCP サーバーに関する詳細が表示されます。
- NTP サーバー。デバイスで使用可能なすべての NTP サーバーに関する詳細が表示されます。

ステップ 12 [Next] をクリックします。

ステップ 13 左ペインで [Wireless] をクリックします。

[Wireless] ウィンドウに、デバイスに存在するエンタープライズ SSID、ゲスト SSID、ワイヤレスインターフェイス、および RF プロファイルが一覧表示されます。

ステップ 14 事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

ステップ 15 左ペインで、[Discarded Config] をクリックします。

Cisco DNA Center の競合する設定と既存の設定が表示されます。破棄される構成エントリは次のカテゴリに分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイスの設定

ステップ 16 [Next]をクリックします。

ステップ 17 [ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

ステップ 18 **[Save]** をクリックします。

成功メッセージが表示されます。

ステップ 19 **[Design]** > **[Network Settings]** > **[Wireless]** の順に選択して、Cisco DNA Center が Cisco AireOS コントローラから学習した SSID とインターフェイス設定を表示します。

ステップ 20 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 21 [ネットワーク プロファイル（Network Profile）] ページで [サイトの割り当て（Assign Site）] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 22 [Add Sites to Profile] ウィンドウでドロップダウンリストからサイトを選択して、[Save] をクリックします。

ステップ 23 [プロビジョニング（Provision）] タブをクリックします。

ステップ 24 プロビジョニングする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 25 [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

ステップ 26 [Choose a site] をクリックして Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ にサイトを割り当てます。

ステップ 27 [Choose a site] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラを関連付けます。

ステップ 28 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 29 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 30 プライマリ コントローラの管理 AP の場所を設定するには、[Select Primary Managed AP Locations] をクリックします。

ステップ 31 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その親サイトの下にある子は自動的に選択されます。

ステップ 32 **[Save]** をクリックします。

ステップ 33 **[Next]** をクリックします。

ステップ 34 [Summary] ウィンドウには、Cisco AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにプッシュされる設定が表示されます。

次の詳細情報を確認します。

- デバイスの詳細
- ネットワークの設定
- SSID
- 管理サイト
- インターフェイス
- 詳細設定

ステップ 35 [Deploy] をクリックして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをプロビジョニングします。

- デバイス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。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。

ステップ 36 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 37 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 38 手動で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 39 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 40 AP をプロビジョニングします。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイスロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ
ファブリックエッジ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP： • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i アクセスポイント

デバイスロール	プラットフォーム
	• Cisco Aironet 1815w アクセスポイント • Cisco Aironet 1815m アクセスポイント • Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセス ポイント • Cisco Aironet 4800 シリーズ アクセス ポイント Cisco 802.11ac Wave 1 AP • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセス ポイント • Cisco Aironet 3700 シリーズ アクセス ポイント

事前設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、スイッチが **aaa new-model** ですでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

3. Cisco Identity Services Engine と Cisco DNA Center を連動させます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。

4. Cisco Catalyst 9000 シリーズスイッチおよびエッジスイッチを検出します。

   Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。

   エッジスイッチを検出するために NETCONF を有効にする必要はありません。

   詳細については、CDP を使用したネットワークの検出 （25 ページ）およびIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

   [Preferred Management IP] を [Use Loopback] に変更します。

5. デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （51 ページ）およびインベントリに関する情報の表示 （53 ページ）を参照してください。

   デバイスが**管理対象**状態になっていることを確認します。

6. ネットワークの地理的な場所を表すネットワーク階層を設計します。サイト、ビルディング、フロアを作成すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロード （127 ページ）を参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130ページ）、およびビルディングへのフロアの追加 （132ページ）を参照してください。

7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

   ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。APは、ファブリックネットワークにデバイスを追加した後にオンボードされます。

   詳細については、「AP の追加、配置、および削除 （135 ページ）」を参照してください。

8. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。

詳細については、グローバルネットワーク設定の管理 （184 ページ）、グローバル ネットワーク サーバーの設定 （204 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

9. CLI、SNMP、HTTP などのデバイスのログイン情報を設定します。

   詳細については、グローバルデバイス クレデンシャルについて （188 ページ）、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、グローバル HTTPS クレデンシャルの設定 （193 ページ）を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

    IP アドレスプールを設定するには、IP アドレス プールを設定する （197 ページ）を参照してください。

    プロビジョニングするビルディングの IP アドレスプールを予約するには、「LAN アンダーレイのプロビジョニング」を参照してください。

11. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義すると、Cisco DNA Center はあらゆる場所にあるさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず、[Wireless] ページで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （156 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）を参照してください。

12. バックホールの設定を行います。詳細については、

13. [Policy] ページで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワーク （478 ページ）および仮想ネットワークの作成を参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加します。詳細については、「グループベースのアクセス コントロール ポリシーの作成 （276 ページ）」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズスイッチとエッジノードスイッチをプロビジョニングします。

    - ファブリックドメインを作成します。
    - CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。

- Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
- ファブリックドメイン内のオンボード AP。

デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー（439 ページ）の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスをプロビジョニングする方法について説明します。

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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチ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 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ステップで、次の項目を設定します。

a) [Choose a site] をクリックします。
b) [Choose a site] スライドインペインで、サイトの横にあるチェックボックスをオンにして、デバイスを関連付けます。
c) **[Save]** をクリックします。
d) [Apply] をクリックします。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。

ステップ 5 **[Devices]** > **[Inventory]** ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
b) **[Next]** をクリックします。
c) [Summary] ステップで設定を確認し、[Deploy] をクリックします。
d) [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。

- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。
- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

    （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 6 エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、[Provision] を選択します。
b) **[Next]** をクリックします。
c) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 7 ファブリックサイトにデバイスを追加するには、Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[Fabric Sites]** の順に選択します。

ステップ 8 ファブリックサイトを作成します。詳細については、「ファブリックサイトの追加（468ページ）」を参照してください。

ステップ 9 IP トランジットネットワークを追加します。

ステップ 10 デバイスを追加して、ファブリックサイトに仮想ネットワークを関連付けます。

ステップ 11 Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。

a) デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。
b) エッジノードをクリックして、[Add to Fabric] を選択します。
c) **[Save]** をクリックします。

ステップ 12 デバイス上で組み込みのワイヤレスを有効にするには、[Edge]、[CP+Border+Edge] または [CP+Border] として追加されたデバイスをクリックし、[Embedded Wireless] をクリックします。

a) ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合は、Cisco DNA Center に「機能を有効にするには、9800-SW イメージが必要です[OK] をクリックして、9800-SW イメージを手動でインポートしてください。（9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually）」という警告メッセージが表示されます。

b) [OK] をクリックして、イメージを手動でインストールします。

c) [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。

d) [Import] をクリックします。

インポートの進捗状況が表示されます。

e) [Activate image on device] をクリックします。

「デバイスでイメージが有効化されると、デバイスがリブートします。デバイスをリブートしてもよろしいですか。（Activate image on device will reboot the device. Are you sure you want to reboot the device?）」という警告メッセージが表示されます。

f) [Yes] をクリックします。

デバイスパッケージのアップグレードが完了すると、デバイスがリブートし、オンラインになります。

g) 表示されるダイアログボックスに、コントローラで管理されている AP の場所が表示されます。ここからサイトの変更、削除、または再割り当てができます。

h) **[Next]** をクリックします。

ステップ 13 [Summary] ステップで詳細を確認し、[Save] をクリックします。

ステップ 14 [Modify Fabric] ステップで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックサイトで AP をオンボードします。

ステップ 15 Cisco DNA Center GUI で、[Provision] タブをクリックします。

ステップ 16 **[Fabric]** タブをクリックします。

ファブリックサイトのリストが表示されます。

ステップ 17 作成したファブリックサイトを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。

ステップ 18 ファブリックサイト内のデバイスに適用される認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される事前定義済みの設定です。認証テンプレートを選択したら、[Save] をクリックします。

ステップ 19 [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。

ステップ 20 [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。

ステップ 21 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。

ステップ 22 [Update] をクリックして設定を保存します。

AP は、指定したプールから IP アドレスを取得します。このプールは、AP VLAN に関連付けられていて、いずれかの検出方法を通じてシスコ ワイヤレス コントローラに登録されます。

ステップ 23 ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。

ステップ 24 [Inventory] > [Resync] を実行して手動で再同期をトリガーし、組み込みのワイヤレス用の Cisco DNA Center で AP を確認します。
検出された AP が [Provision] ページの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。

ステップ 25 AP をプロビジョニングします。

詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （398 ページ）を参照してください。

ステップ 26 アプリケーションポリシーを設定および展開します。詳細については、アプリケーション ポリシーの作成（317 ページ）、アプリケーションポリシーの展開（323 ページ）、およびアプリケーションポリシーの編集 （321 ページ）を参照してください。

アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。

2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは動作しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス

ファブリックインアボックスに関する情報

Cisco Catalyst 9000 シリーズ スイッチには、Cisco DNA Center を使用して設定できる、単一のスイッチでファブリックエッジ、コントロールプレーン、ボーダー、および組み込みのワイヤレス機能をホストする機能があります。

この機能を使用すると、小規模サイトの場所での設定が簡素化され、Cisco SD-Access の導入コストが削減されます。

Cisco Catalyst 9000 シリーズスイッチに CP+ ボーダー + エッジノードを追加する方法については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （429 ページ）を参照してください。

拡張性に関する情報

次の表に、デバイスの拡張性に関する情報を示します。

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズ スイッチ	Cisco Catalyst 9500 シリーズ スイッチ	Cisco Catalyst 9500-H シリーズ スイッチ
仮想ネットワーク	256	256	256	256
ローカルエンドポイント/ホスト	4 K	4 K	4 K	4 K
SGT/DGT テーブル	8K	8K	8K	8K
SGACL（セキュリティ ACE）	5K	18K	18K	18K

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアバージョンのさまざまな シスコ ワイヤレス コントローラ で実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Cisco DNA Center Cisco DNA Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしての Cisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

このリリースのコントローラデバイスで IRCM を設定する際の制限事項を次に示します。

- フォーリンコントローラとしてのCisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- 複数のアンカーコントローラの設定、および 1 つのフォーリン コントローラ シナリオの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。
- ゲストアンカーノードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。
- モビリティトンネルは暗号化されません。

ゲスト アンカーの設定とプロビジョニング

ゲスト アンカー シスコ ワイヤレス コントローラ を設定するには、次の手順に従います。

（注） ゲストアンカーの構成は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラではサポートされていません。

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成（125ページ）、建物の追加（130ページ）、およびビルディングへのフロアの追加（132ページ）を参照してください。

ステップ 2 AAA、DHCP、DNS サーバーなどのネットワーク サーバーを設定します。詳細については、グローバル ネットワーク サーバーの設定 （204 ページ）およびCisco ISE またはその他の AAA サーバーの追加 （204 ページ）を参照してください。

ステップ 3 Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）」を参照してください。

ステップ 4 Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して ワイヤレスコントローラ を検出し、そのデバイスが **[Devices]** > **[Inventory]** ウィンドウに [Managed] 状態で表示されていることを確認します。詳細については、「ディスカバリについて （19 ページ）」を参照してください。

ステップ 5 アクティブなメイン ワイヤレスコントローラ として外部 ワイヤレスコントローラ をプロビジョニングします。「Cisco AireOS コントローラのプロビジョニング （391 ページ）」を参照してください。

ステップ 6 ゲスト アンカーとして ワイヤレスコントローラ のロールを選択し、ゲスト アンカー コントローラをプロビジョニングします。詳細については、「Cisco AireOS コントローラのプロビジョニング （391 ページ）」を参照してください。

ステップ 7 CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャルを設定します。詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、

グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、およびグローバル HTTPS クレデンシャルの設定 （193 ページ）を参照してください。

IRCM：Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

  詳細については、CDP を使用したネットワークの検出 （25 ページ）またはIP アドレス範囲を使用したネットワークの検出 （32 ページ）を参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

  新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （125 ページ）、建物の追加 （130 ページ）、およびビルディングへのフロアの追加 （132 ページ）を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「AP の追加、配置、および削除（135 ページ）」を参照してください。

- AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

  詳細については、グローバルネットワーク設定の管理 （184 ページ）、グローバル ネットワーク サーバーの設定 （204 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

- ゲスト ワイヤレス ネットワークの SSID を作成します。

  詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成 （162 ページ）」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じに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**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ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 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 10 アクティブなメイン ワイヤレスコントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 11 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [IP Address]：インターフェイス IP アドレスを入力します。
- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。

ステップ 12 **[Next]** をクリックします。

ステップ 13 [Summary] ウィンドウで、設定の詳細を確認します。

ステップ 14 [Deploy] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。

ステップ 15 **[Devices]** > **[Inventory]** ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 16 手順 3 ～ 8 を繰り返します。

ステップ 17 Cisco AireOS コントローラのロールを [Guest Anchor] として選択します。

ステップ 18 ゲストアンカー ワイヤレスコントローラ の場合は、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 19 手順 11 ～ 14 を繰り返します。

Meraki デバイスのプロビジョニング

この手順では、Meraki ダッシュボードによって管理されている Cisco Meraki デバイスに SSID をプロビジョニングする方法について説明します。

始める前に

- Meraki ダッシュボードを Cisco DNA Center と統合します。Meraki ダッシュボードの統合（75 ページ）を参照してください。
- SSID を作成します。エンタープライズ ワイヤレス ネットワーク用 SSID の作成（156 ページ）を参照してください。

（注） Meraki ダッシュボードは、次の種類の SSID をサポートしています。

- [Open]：この SSID は、Meraki ダッシュボードの [Open] に対応しています。
- [WPA2 Personal]：この SSID は、Meraki ダッシュボードの [preshared key with WAP2] に対応しています。
- [WPA2 Enterprise]：この SSID は、Cisco Meraki ダッシュボードの Meraki 認証またはマイ Radius サーバーを使用した WAP-2 暗号化に対応しています。Cisco DNA Center におけるビルディングレベルのクライアントおよびエンドポイントの認証用に AAA サーバーまたは Cisco ISE サーバーを定義している場合は、その設定が Cisco Meraki ダッシュボードの [my Radius server] にプロビジョニングされます。それ以外の場合は、Meraki デバイスによる認証に [Meraki Radius] が使用されます。

すべての SSID に対して、インターフェイス名を選択できます。Cisco DNA Center で [Management] インターフェイスを選択した場合、VLAN ID は 0 です。つまり、Cisco Meraki ダッシュボードではサポートされないため、Cisco Meraki ダッシュボードでは VLAN タギングは無効になります。Cisco DNA Center で SSID のカスタムインターフェイスを作成すると、Cisco Meraki ダッシュボードで、カスタムインターフェイス名と VLAN ID を使用して AP タグが作成されます。

- ネットワークプロファイルを作成し、SSID がプロビジョニングされるサイトに割り当てます。

（注） Cisco DNA Center のネットワーク階層 [Sites] > [Buildings]は、Meraki ダッシュボードの [Organization] > [Network] に対応しています。ワークフローの [Add Sites to Profile] ウィンドウで、[Buildings] を選択することをお勧めします。

（注） Cisco DNA Center Meraki ネットワークを作成して、SSID をネットワークにプロビジョニングします。Meraki ダッシュボードは、Meraki ネットワーク構成を Meraki デバイスに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]**。

[Network Devices] > **[Inventory]** ウィンドウが表示され、検出されたすべてのデバイスが示されます。

ステップ 2 Meraki ダッシュボードを表示するには、左側のペインで [Global] サイトを展開し、ビルディングを選択します。

選択したビルディングで使用可能なすべての Meraki ダッシュボードが表示されます。

ステップ 3 プロビジョニングする Meraki ダッシュボードの横にあるチェックボックスをオンにします。

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

[Assign Site] ウィンドウが表示され、Meraki ダッシュボードと関連付けられたビルディングを確認できます。

ステップ 5 関連付けられたビルディングを変更するには、[Choose a site] をクリックします。

ステップ 6 [Choose a site] ウィンドウで、ビルディングを選択して [Save] をクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。管理ビルディングは、プライマリロケーションで表示できます。

ステップ 8 Meraki ダッシュボードのセカンダリ管理ロケーションを選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 9 [Managed AP Location] ウィンドウで、ビルディング名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 **[Save]** をクリックします。

ステップ 11 **[Next]** をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**

（注） Meraki 展開では、各ネットワークで最大 15 の SSID がサポートされています。

- **管理サイト**

ステップ 12 [展開（Deploy）] をクリックします。

ステップ 13 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。
- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

    （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイスインベントリ（Device Inventory）] ウィンドウの [プロビジョニングステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。

ルーティングおよび NFV プロファイルのプロビジョニング

始める前に

ルーティングと NFV プロファイルをプロビジョニングする前に、次のグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS などのネットワーク サーバー。詳細については、グローバル ネットワーク サーバーの設定 （204 ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、グローバル CLI クレデンシャルの設定 （188 ページ）、グローバル SNMPv2c クレデンシャルの設定 （189 ページ）、グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、およびグローバル HTTPS クレデンシャルの設定 （193 ページ）を参照してください。
- IP アドレス プール詳細については、「IP アドレス プールを設定する （197 ページ）」を参照してください。
- SP プロファイル。詳細については、「サービス プロバイダ プロファイルの設定 （203 ページ）」を参照してください。

（注） Cisco Firepower Threat Defense Virtual を NFV プロビジョニングフローを通じてプロビジョニングする場合、デフォルトのクレデンシャルユーザー名が保持され、パスワードはネットワーク設定でサイトに割り当てられたクレデンシャルプロファイルの設定に基づいて更新されます。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。

[Network Devices] > [Inventory] ウィンドウが表示されます。このウィンドウには、すべての検出済みデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [Routers] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能なデバイスのリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 サイトで [Assign] をクリックすると、[Assign Device to Site] ウィンドウが表示されます。[Choose a Site] をクリックします。

ステップ 6 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

NFVIS デバイスをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。[O] をクリックして WAN の IP アドレスを入力します。[+Edit Services] ウィンドウで詳細を確認します。**[Next]** をクリックします。

（注） vEdge 関連サービスをプロビジョニングする前に、[System Settings] ページで vManage 設定を構成する必要があります。詳細については、『Cisco DNA Center Administrator Guide』の「Configure vManage Properties」を参照してください。

- [ENCS Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Custom Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ルータをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。
  - 回線インターフェイスとしてギガビットイーサネットを選択した場合は [O] をクリックし、静的 IP アドレスを選択した場合は WAN IP アドレスを入力します。[DHCP] を選択した場合は、DHCP サーバーの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている場合は、[Do Not Change] を選択して、ドロップダウンリストからプライマリ WAN として設定されているインターフェイスを選択します。
  - 回線インターフェイスとしてセルラーを選択した場合は、[O] をクリックして、[IP Negotiated] を選択し、ドロップダウンリストから [Interface Name] を選択して [Access Point Name (APN)] を入力します。サービスプロバイダに応じて、[PAP] チェックボックスまたは [CHAP] チェックボックスをオンにします。
  - 複数のサービスプロバイダを利用している場合は、バックアップ WAN インターフェイスの [IP SLA Address] を入力します。

  仮想ルータをプロビジョニングしている場合、このウィンドウは表示されません。
- [Router LAN Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

  [Interface(s)] ドロップダウンリストから 1 つの L3 インターフェイスまたは 1 つまたは複数の L2 インターフェイスを選択できるようになりました。
- [Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ステップ 7 [展開（Deploy）] をクリックします。

ステップ 8 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。
- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

- 将来の日付と時刻でデバイスの展開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、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。

ファイアウォール プロファイルのプロビジョニング

この手順では、Firepower Management Center（FMC）によって管理される Firepower Threat Defense（FTD）デバイスをプロビジョニングする方法について説明します。

始める前に

- FMC と Cisco DNA Center を統合します。Firepower Management Center の統合 （77 ページ）を参照してください。
- ネットワーク階層内でサイトを作成します。ネットワーク階層のサイトの作成（125 ページ）を参照してください。

- ファイアウォールのネットワークプロファイルを作成し、FTDデバイスがプロビジョニングされるサイトに割り当てます。ファイアウォール用のネットワークプロファイルの作成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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 プロビジョニングする FTD デバイスの横にあるチェックボックスをオンにして、[Site] 列の下にある [Assign] をクリックします。

ステップ 3 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 4 [Choose a Site] ウィンドウで、階層からサイトを選択して [Save] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Now] をクリックしてデバイスをサイトにすぐに割り当てるか、[Later] をクリックして特定の時間にスケジュールします。

ステップ 7 [**Assign**] をクリックします。

（注） **[Activities]** > **[Tasks]** で、サイトへのデバイスの割り当てのステータスを確認できます。

ステップ 8 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Provision Firewall Profile] ウィンドウが表示されます。

ステップ 9 [Confirm Profile] ページで詳細を確認し、[Next] をクリックします。

ステップ 10 [Firewall Type] ページで詳細を確認し、[Next] をクリックします。

[FTD Configuration] ページが表示されます。

ステップ 11 ルーテッドモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

ステップ 12 トランスペアレントモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択します。
b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択します。
c) [Bridge Virtual Interface] エリアを展開し、次の手順を実行します。
   - [Bridge Group Number]：ブリッジグループ番号を入力します。有効な値は 1 ー 250 です。
   - [IP]：FTD デバイスの IP アドレスを入力します。
   - [Subnet Mask]：サブネットマスクを入力します。

ステップ 13 **[Next]** をクリックします。

[概要（Summary）] ページが表示されます。このページには、デバイスの仕様の概要が表示されます。

ステップ 14 [Summary] ページで詳細を確認し、[Deploy] をクリックします。

[Provision Firewall device(s)] ダイアログボックスが表示されます。

ステップ 15 [Now]、[Later]、または [Generate configuration preview] オプションボタンをクリックします。

- [Now]：プロビジョニングがすぐに開始されます。
- [Later]：特定の時間にプロビジョニングがスケジュールされます。
- [Generate configuration preview]：選択したデバイスに展開するために後で使用できるプレビューを作成します。

ステップ 16 [Apply] をクリックします。

（注） **[Activities]** > **[Tasks]** で、ファイアウォールデバイスのステータスを確認できます。[Provision Firewall device(s)] ダイアログボックスで [Generate configuration preview] を選択した場合は、**[Activities]** > **[Work Items]** でステータスを表示できます

LAN アンダーレイのプロビジョニング

LAN 自動化を使用して、LAN アンダーレイをプロビジョニングします。

始める前に

- ネットワーク階層を設定します。（デバイスをサイトに追加する（80ページ）を参照）。
- 以下のグローバルネットワーク設定が定義済みであることを確認します。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー（グローバル ネットワーク サーバーの設定（204 ページ）を参照）。

- CLI、SNMP、HTTP、HTTPS などのデバイスのクレデンシャル(グローバル CLI クレデンシャルの設定 （188ページ）、グローバル SNMPv2c クレデンシャルの設定 （189ページ）、グローバル SNMPv3 クレデンシャルの設定 （191 ページ）、グローバル HTTPS クレデンシャルの設定 （193 ページ）を参照)。
- IP アドレスプール（IP アドレス プールを設定する （197 ページ） を参照）。

- インベントリに少なくとも 1 つのデバイスがあることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して検出します。

（注） 検出されたサイトがユーザー名「cisco」の CLI ログイン情報を使用して設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように設定されたスイッチで次の操作が実行されていることを確認します。
  - Day-0 設定はスイッチで実行されます。
  - 40G Quad Small Form-Factor Pluggable（QSFP）トランシーバはスーパバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパバイザ上の 1 ～ 8 のポートには、10G または 1G Small Form-Factor Pluggable（SFP）トランシーバは挿入されません。デュアル スーパーバイザ エンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。

    Catalyst 9400 シリーズ スーパーバイザの詳細については、『Cisco Catalyst 9400 Series Supervisor Installation Note』を参照してください。

ステップ 1 プロビジョニングするサイト用に IP アドレスプールを予約します。

（注） LAN 自動化 IP アドレスプールのサイズは、25 ビットのネットマスク以上である必要があります。

a) Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
b) [Network Hierarchy] ペインで、サイトを選択します。
c) [Reserve] をクリックし、[Reserve IP Pool] ウィンドウで次のフィールドに値を入力して、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。
   - [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
   - [Type]：IP アドレスプールのタイプ。LAN 自動化の場合は、**LAN** を選択します。
   - [IP Address Space]：[IPv4] または [IPv6] をオンにしてアドレスプールを作成します。デュアルスタックプールを作成するには、[IPv4] と [IPv6] の両方のチェックボックスをオンにします。

- [Global IP Pool]：IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。

  （注） LAN 自動化では、IPv4 サブネットのみが使用されます。

- [Prefix length / Number of IP Addresses]：グローバル IP アドレスプールのすべてまたは一部を予約するために使用する IP サブネットとマスクアドレス、または予約する IP アドレスの数。
- [Gateway]：ゲートウェイ IP アドレス。
- [DHCP Server(s)]：DHCP サーバーの IP アドレス。
- [DNS Server(s)]：DNS サーバーの IP アドレス。

d) [Reserve] をクリックします。

ステップ 2 デバイスを検出してプロビジョニングします。

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

すべての検出されたデバイスが表示されます。

b) [Actions] > [Provision] > [LAN Automation] の順にクリックします。

c) [LAN Automation] ウィンドウで、次のフィールドに値を入力します。

- Primary Site：このサイトからプライマリデバイスを選択します。
- Peer Site：このサイトがピアデバイスの選択に使用されます。このサイトは、プライマリサイトとは異なる場合がありますので注意してください。
- Primary Device：Cisco DNA Center が新しいデバイスを検出しプロビジョニングする起点として使用するプライマリデバイスを選択します。
- Peer Device：ピアデバイスを選択します。
- SELECTED PORTS OF PRIMARY DEVICE：新規デバイスの検出とプロビジョニングに使用するポート。[Modify Selections] をクリックしてポート番号を入力します。
- Discovered Device Site：新たに検出されたすべてのデバイスがこのサイトに割り当てられます。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
- Main IP Pool：LAN 自動化用に予約された IP アドレスプール（ステップ 1 を参照）。
- Link Overlapping IP Pool：他のサイトと共有される IP アドレスプール。アンダーレイでポイントツーポイントリンクに対する /31 IP アドレスを設定するために使用されます。

  リンク重複 IP プールには、親サイトから継承されるサブプールか他のサイトで定義されているサブプールを指定できます。

  リンク重複 IP プールを使用すると、マルチサイト展開で /31 IP アドレスの重複が可能になります。異なるサイトのホストにおいて、/31 リンクで IP アドレスを再利用できます。

  リンク重複 IP プールを定義した場合、[Main IP Pool] フィールドで定義されたアドレスが管理 IP（ループバックアドレスや VLAN アドレスなど）に使用されます。

- ISIS Domain Password: LAN 自動化が開始するときにユーザーが指定する IS-IS パスワード。パスワードがすでにシードデバイスに存在する場合は、再使用され、上書きされることはありません。ユーザーが指定するパスワードが入力され、既存の IS-IS パスワードがデバイスにない場合、ドメインパスワードが使用されます。プライマリとセカンダリシードの両方がドメインパスワードをもつ場合、それらが一致することを確認してください。
- Enable Multicast：このチェックボックスをオンにすると、アンダーレイ ネイティブ マルチキャストが有効になります。LAN 自動化によって、シードデバイスを RP とし、検出されたデバイスをサブスクライバとするマルチキャストツリーが作成されます。
- Device Name Prefix：プロビジョニングしているデバイスの名前プレフィックス。Cisco DNA Center で各デバイスをプロビジョニングするときに、ここで指定されたテキストでデバイスにプレフィックスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして **Access** を入力した場合、各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3 のように名前が付けられます。
- Choose a File：[Browse] をクリックして、ホスト名マップファイルを選択します。選択した CSV ファイルに記述されているシリアル番号とホスト名のマッピングを使用して、検出されたデバイスに対してユーザーが指定した名前が設定されます。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。

  CSV ファイルの例を次に示します。

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

d) [Start] をクリックします。

Cisco DNA Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Cisco DNA Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 3 プロビジョニングしているデバイスの進行状況をモニターして確認します。

a) **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順にクリックします。

[LAN Automation Status] ウィンドウに、デバイスのプロビジョニングの進捗状況が表示されます。

（注） 新しいデバイスのプロビジョニングには数分かかる場合があります。

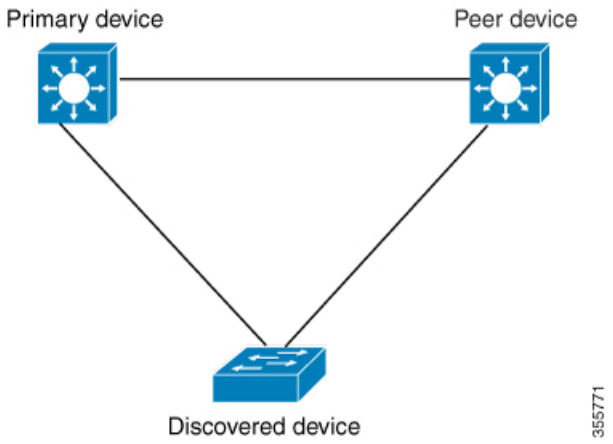
b) すべてのデバイスが検出されてインベントリに追加され、管理状態になったら、[LAN Automation Status] ウィンドウで [Stop] をクリックします。

LAN 自動化プロセスが完了し、新規デバイスがインベントリに追加されます。

LAN 自動化のピアデバイスの使用事例

デュアル ホームのスイッチのプロビジョニング

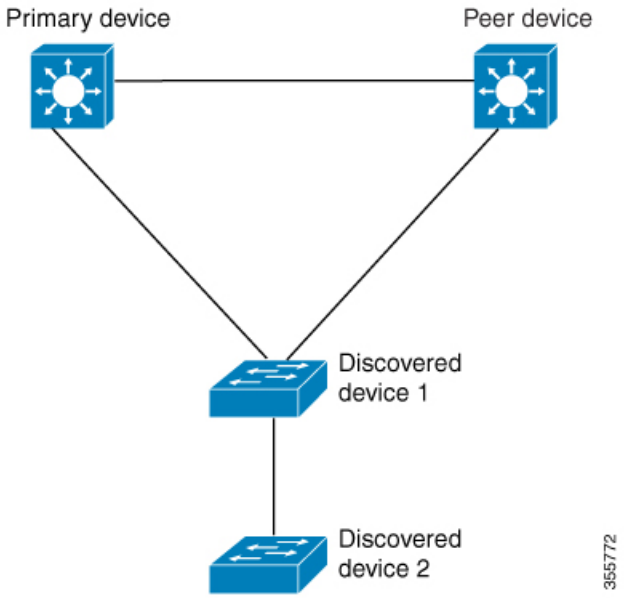
デュアル ホームのスイッチのプロビジョニングのために、常にピア デバイスを選択する必要があります。



Cisco DNA Center プライマリ デバイスで DHCP サーバーを設定します。Cisco DNA Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2 つのレイヤー 3 ポイントツーポイント接続を設定します。1 つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう 1 つの接続は検出されたデバイスとピア デバイスの間で確立されます。

（注） LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Cisco DNA Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Cisco DNA Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から 検出されたデバイス *2* に接続するためにルートする

検出されたデバイス *3*という名前のデバイスが以下の検出されたデバイス *2*に直接接続されるシナリオを考えてください。検出されたデバイス *2* と 検出されたデバイス *3*の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリ デバイスから 2 段階以上離れているためです。

LAN 自動化の状態を確認

実行中の LAN 自動化ジョブのステータスを確認できます。

始める前に

LAN 自動化ジョブを作成し、開始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**[Provision]** > **[Inventory]** の順に選択します。

すべての検出されたデバイスが表示されます。

ステップ 2 **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順に選択します。
[LAN Automation Status] ウィンドウに、実行中と完了のすべての LAN 自動化ジョブのステータスが表示されます。

プロビジョニング後のデバイスの削除

- 既にファブリック ドメインに追加されているデバイスを削除する場合、ファブリック ドメインからそのデバイスを削除し、次に**[プロビジョニング（Provision）]**メニューから削除します。
- **[インベントリ（Inventory）]**ウィンドウからデバイスを削除することはできません。代わりに、**[プロビジョニング（Provision）]**メニューからプロビジョニングしたデバイス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（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

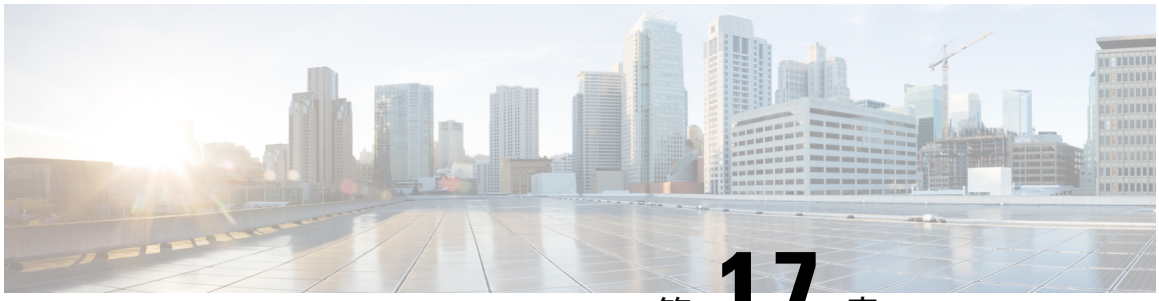
ステップ 2 検出され、プロビジョニングされたすべてのデバイスが表示される**[インベントリ（Inventory）]**タブをクリックします。

ステップ 3 削除するデバイスの横にあるチェックボックスをオンにします。

（注） APは、接続していたコントローラが削除された場合にのみ削除されます。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[デバイスの削除（Delete Device）]** を選択します。

ステップ 5 確認プロンプトで、[OK] をクリックします。



第 17 章

ファブリックネットワークのプロビジョニング

ファブリックネットワークについて

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Cisco DNA Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリックサイト

ファブリックサイトは、コントロールプレーン、ボーダー、エッジ、ワイヤレスコントローラ、ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計することができます。

ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス
- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

Software-Defined Access ファブリックネットワークは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。ファブリックサイトの全体的な集約は、多数のエンドポイントに対応し、モジュール方式で（または水平方向に）拡張します。複数のファブリックサイトは、トランジットサイトを使用して相互接続されます。

トランジットサイト

トランジットサイトとは、2つ以上のファブリックサイトを相互に接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続するサイトです。トランジットネットワークには 2 つのタイプがあります。

- IP トランジット：通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。
- SDA トランジット：LISP/VxLAN のカプセル化を使用して 2 つのファブリックサイトを接続します。SDA トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SDA トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループタグを使用して維持されます。

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される事前プロビジョニングチェックのセットです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになりました。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- 接続チェック：エッジノードからマップサーバーへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック（ブラウンフィールドチェック）：SD-Access を介してプッシュされる設定と競合する設定がデバイスにあり、それが後でエラーになる可能性がないかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：サポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco Controller）を使用してデバイスが実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスにループバック インターフェイスが設定されている必要があります。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。
- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。

サポートされているソフトウェアバージョンの詳細については、「Cisco SD-Access Hardware and Software Compatibility Matrix」を参照してください。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。問題を修正し、デバイスのプロビジョニング ワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザーインテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレスデバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

  有線デバイスの設定変更によって SNMP トラップがトリガーされ、それによってコンプライアンスチェックがトリガーされます。Cisco DNA Center サーバーが SNMP サーバーとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Cisco DNA Center 上の仮想ネットワークのユーザーインテントの現在の状態に準拠するように、必要な VRF がデバイスに設定されているかどうかを確認します。

- ファブリックロール：デバイスの設定が Cisco DNA Center のファブリックロールのユーザーインテントに準拠しているかどうかを確認します。
- セグメント：セグメントの VLAN 設定と SVI 設定を確認します。
- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、新しいファブリックサイトを作成できます。つまり、サイトのテレメトリ設定を構成するときには、[Monitor wired clients] を有効にしておく必要があります。

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

ステップ 2 [Fabric Sites] タブで、[Add fabric site] をクリックします。

または、最初の 2 つの手順の代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** を選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let's Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 （オプション）ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、表示されたネットワーク階層からファブリックサイトを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウでファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 8 [作成（Create）] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」というメッセージが表示されます。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）

- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大6つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

1. Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
2. [Inventory] ウィンドウに、検出されたデバイスが表示されます。
3. ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
4. ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
5. 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで**[Inventory]** > **[Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 3 デバイスをクリックします。スライドインペインには、次の [Fabric] オプションが表示されます。

オプション	説明
エッジ	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
Border	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスを一体型ファブリックとして設定するには、[Control Plane]、[Border]、および [Edge] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane] と [Border] の両方を選択します。

ステップ 4 [Add] をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、ファブリックへのデバイスの追加（469ページ）で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

ボーダーノードとしてデバイスを追加するには、次の手順を実行します。

ステップ1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ2 ボーダーノードを追加するファブリックサイトを選択します。
インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ3 デバイスをクリックします。

ステップ4 表示されるスライドインウィンドウで、[Border] トグルボタンをクリックします。

ステップ5 表示されたウィンドウで、[Layer 3 Handoff] タブをクリックします。

ステップ6 [Enable Layer-3 Handoff] チェックボックスを選択します。

ステップ7 デバイスの [ローカル自律番号（Local Autonomous Number）] を入力します。

ローカル自律番号がデバイスですでに設定されている場合は、その番号が表示され、このフィールドは無効になります。デバイスですでに設定されているローカル自律番号を変更することはできません。

ステップ8 [Select 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。

IP プールは IP トランジットネットワークを追加する場合にのみ選択します。

ステップ9 ボーダーデバイスで有効になっているトランジットネットワークを選択します。

a) ボーダーで SDA トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した SDA トランジットドメインを選択します。

[Add] をクリックします。

b) ボーダーで IP トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した IP トランジットドメインを選択します。

[Add] をクリックします。

表示されるウィンドウで、次の手順を実行します。

1. デザイン階層から IP プールを選択します。選択したプールは、ボーダーノードと IP ピア間で IP ルーティングを自動化するために使用されます。
2. [インターフェイスの追加（Add Interface）] をクリックして、次の画面でインターフェイスの詳細を入力します。

3. ドロップダウン リストから [外部インターフェイス（External Interface）] を選択します。
4. [Interface Description] で、インターフェイスのカスタム説明を入力します。
5. [リモートAS番号（Remote AS Number）] を入力します。
6. リストで [仮想ネットワーク（Virtual Network）] をチェックします。この仮想ネットワークは、ボーダーによってリモートピアにアドバタイズされます。1 つ、複数、またはすべての仮想ネットワークを選択できます。
7. **[Save]** をクリックします。

ステップ 10 デフォルトでは、ボーダーは外部ボーダーとして指定され、外部ルートをインポートせずに、すべての不明なトラフィックへのゲートウェイとして機能します。ボーダーを内部ボーダーとして設定すると、既知のトラフィックへのゲートウェイとして、特定の外部ルートをインポートするように設定できます。ボーダーには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。

- ボーダーを外部ボーダーとして指定し、不明なネットワークへの接続を提供するには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにします。
- ボーダーを内部ボーダーとして指定し、特定のネットワークアドレスのゲートウェイとして動作させるには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにしないでください。
- このボーダーノードを内部および外部ボーダーとして指定するには、[Default to all Virtual Networks] チェックボックスをオンにします。これは、エッジノードから送信されたすべての既知のトラフィックおよび不明なトラフィックへのゲートウェイとして機能します。（[Do not Import External Routes] チェックボックスはオンにしないでください）。

ステップ 11 （オプション）ファブリックネットワークに非ファブリックネットワークを接続している場合、または従来のネットワークから SDA ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] タブをクリックします。仮想ネットワークのリストと、各仮想ネットワークの IP プールの数が表示されます。

a) ハンドオフする仮想ネットワークをクリックします。

仮想ネットワークを選択すると、仮想ネットワークに存在する IP アドレスプールのリストが表示されます。非ファブリックデバイスを接続できるインターフェイスのリストも表示されます。

b) [External Interface] を選択してください。

Cisco DNA Center リリース 2.1.2.6 では、レイヤ 2 ハンドオフを実行できる複数のインターフェイスを選択できます。

c) [Interface Description] に説明を入力します。
d) ファブリックを拡張する必要がある [External VLAN] 番号を入力します。

Cisco DNA Center 2.1.2.6 より前のリリースでは、仮想ネットワークは 1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークを処理することはできません。

Cisco DNA Center リリース 2.1.2.6 以降のリリースでは、仮想ネットワークは単一のインターフェイスまたは複数のインターフェイスでハンドオフできます。セグメントのレイヤ 2 ハンドオフを 2 つの異なるデバイスで実行することもできます。いずれの場合も、ネットワークにループが形成されていないことを確認します。

e) **[Save]** をクリックします。

ステップ 12 [Add] をクリックします。

LISP Pub/Sub の設定

最初のコントロールプレーンをファブリックに追加する場合にのみ、ファブリックサイトで LISP Pub/Sub を設定できます。

始める前に

ファブリックデバイスが Cisco IOS XE リリース 17.6.1 以降で動作す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、[SD ACCESS] で **[Provision]** > **[Fabric Sites]** の順に選択します。

ステップ 2 [Fabric Sites] タブで、LISP Pub/Sub を設定するサイトをクリックします。

[SITE] ウィンドウに、サイト要素の概要が表示されます。

ステップ 3 コントロールプレーンとして設定するデバイスをクリックします。

ステップ 4 表示されるスライドインペインで、[Control Plane] トグルボタンをクリックして、このプレーンを設定します。

ステップ 5 [Configure Control Plane] ウィンドウで、[LISP PubSub] ルート配布プロトコルを選択し、[Add] をクリックします。

ステップ 6 [展開（Deploy）] をクリックします。

ステップ 7 [Modify Fabric] ウィンドウで、操作をスケジュールし、[Apply] をクリックします。

ファブリックサイトの LISP Pub/Sub の設定を確認するには、[SITE SUMMARY] ウィンドウで LISP Pub/Sub のステータスを確認します。

IP のトランジット ネットワークの作成

新しい IP トランジット ネットワークを追加するには、次の手順に従います。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[SD ACCESS] で **[Provision]** > **[Transits & Peer Networks]** の順に選択します。

ステップ 2 [Transits and Peer Networks] ウィンドウで、[Add Transit] をクリックします。

ステップ 3 [Transit/Peer Network] スライドインウィンドウで、トランジットネットワークの名前を入力します。

ステップ 4 ネットワークのトランジットの名前を入力します。

ステップ 5 [IP-Based Transit/Peer Network Type] を選択します。
ルーティング プロトコルが BGP にデフォルトとして設定されます。

ステップ 6 トランジットネットワークの自律システム番号（ASN）を入力します。

ステップ 7 [Save] をクリックします。

SDA トランジット ネットワークの作成

新しい SDA トランジット ネットワークを追加するには、次の手順に従います。

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

ステップ 2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。

ステップ 3 ドロップダウンメニューで [Transit/Peer Network] をクリックします。

ステップ 4 ネットワークのトランジットの名前を入力します。

ステップ 5 トランジット タイプとして [SD-Access] を選択します。

ステップ 6 このトランジット ネットワークの**トランジット コントロール プレーンのサイト**を入力します。少なくとも 1 つのトランジット マップ サーバーを選択します。

ステップ 7 このトランジット ネットワークの**トランジット コントロール プレーン**を入力します。

ステップ 8 2 番目のマップサーバーを追加するには、手順 7 と手順 8 を繰り返します。

ステップ 9 **[Save]** をクリックします。

次のタスク

SDA トランジットの作成後、ファブリック サイトに移動し、SDA トランジットを接続するサイトに接続します。**[Provision]** > **[Fabric]** > **[Fabric Site]** の順に移動します。作成したファブリック サイトを選択します。**[Fabric Site]** > **[Border]** > **[Edit Border]** > **[Transit]** の順にクリックします。ドロップダウンリストでSDA トランジットサイトをポイントし、[Add] をクリックします。

ホスト オンボーディングの設定

[Host Onboarding] タブでは、ファブリック ドメインにアクセスできる各種デバイスまたはホストの設定を指定することができます。

[Host Onboarding] タブには次のサブタブがあります。

- [Authentication Template] タブ：ファブリック用の認証テンプレートを選択します。認証テンプレートは、Cisco ISE から取得される一連の定義済みの設定です。認証テンプレートを選択したら、[Save] をクリックします。
- [Virtual Networks] タブ：IP アドレスプールを仮想ネットワーク（デフォルト、ゲスト、またはユーザー定義）に関連付け、[Update] をクリックします。表示される IP アドレス プールは、サイト固有のプールのみです。
- [Wireless SSIDs] タブ：ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択してアドレス プールを割り当て、[保存（Save）] をクリックできます。
- [Port Assignment] タブ：ファブリックドメインに接続するデバイスのタイプに応じて、各ポートに固有の設定を適用します。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

  次の制約事項に注意してください。

  - Cisco SD-Access 展開環境では、AP、拡張ノード、ユーザーデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）、および単一サーバーのみがサポートされます。
  - 内部スイッチまたは仮想スイッチを備えたサーバーはサポートされていません。
  - その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

認証テンプレートの選択

ファブリックサイト内のすべてのデバイスに適用される認証テンプレートを選択できます。

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 [Fabric Sites] ウィンドウで、ファブリックサイトを選択します。

ステップ 3 [Host Onboarding] タブをクリックします。

ステップ 4 [Authentication] タブで、サイトの認証テンプレートを選択します。

- **クローズ認証（Closed Authentication）**：認証前のすべてのトラフィック（DHCP、DNS、ARP を含む）は廃棄されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- **認証なし**
- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。

選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

サイトレベルの認証を変更する前に、マクロまたは自動設定を使用して AP がオンボーディングされ、かつまだ定期的な再同期が行われていないファブリックデバイスがあれば再同期する必要があります。

ステップ 5 （オプション）選択した認証方式の設定を編集するには、[Edit] をクリックします。

スライドインウィンドウに、選択した認証方式のパラメータが表示されます：[First Authentication Order]、[802.1x to MAB Fallback]、[Wake on LAN]、[Number of hosts]。

（注） [Number of hosts] は、ポートに接続できるデータホストの数を指定します。[Single] の場合、ポートでは 1 つのデータクライアントのみを保持できます。[Unlimited] の場合、ポートで複数のデータクライアントと 1 つの音声クライアントを保持できます。

必要な変更を行って、**[保存（Save）]** をクリックします。

編集ウィンドウが閉じます。保存された変更は、認証テンプレートが編集されているサイトにのみ適用されます。

ステップ 6 [展開（Deploy）] をクリックします。
ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックサイトの各アクセスデバイスを設定できます。デバイスの各ポートのネットワーク動作設定を指定できます。

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 2 表示された [Fabric Sites] ウィンドウで、ファブリックサイトをクリックします。

ステップ 3 [Host Onboarding] タブで、[Port Assignment] タブをクリックします。

ステップ 4 左側のペインに表示されるファブリックデバイスのリストから、設定するデバイスを選択します。
デバイスで使用可能なポートが右側のペインに表示されます。

ステップ 5 デバイスのポートを選択し、[Assign] をクリックします。

ステップ 6 [Port Assignment] スライドインウィンドウの [Connected Device Type] ドロップダウンリストで、コネクテッドデバイスのタイプを次のオプションから選択します。

オプション	説明
トランク	ポートをトランクポートとして設定します。
[Access Point(AP)]	アクセスポイントに接続するポートを設定します。
[User Devices (IP phone, computer, laptop)]	ホストデバイスに接続するポートを設定します。

a) トランクポートを接続するには、[Trunk] を選択し、このポートの [Description] を入力します。

b) アクセスポイントを接続するには、[Access Point(AP)] を選択し、次の手順を実行します。

1. [VLAN Name / IP Address Pool (Data)] ドロップダウンリストから VLAN と IP アドレスを選択します。
2. [Authentication] ドロップダウンリストから認証タイプを選択します。
3. コネクテッドデバイスに関する [Description] を入力します。

c) ホストデバイスを接続するには、[User Devices (IP phone, computer, laptop)] を選択し、次の手順を実行します。

1. [VLAN Name / IP Address Pool (Data)] ドロップダウンリストからデータの IP アドレスプールを選択します。
2. プロビジョニングされているグループである [Scalable Groups] を選択します。

   スケーラブルグループは、[No Authentication] プロファイルでのみサポートされます。
3. [VLAN Name / IP Address Pool (Voice)] ドロップダウンリストから音声の IP アドレスプールを選択します。
4. [Authentication] ドロップダウンリストから認証テンプレートを選択します。
5. コネクテッドデバイスに関する [Description] を入力します。

d) [更新（Update）] をクリックします。

ステップ 7 すべてのポートの割り当てが完了したら、[Deploy] をクリックします。

ファブリックネットワークのワイヤレス SSID の設定

ステップ 1 [Wireless SSID] セクションで、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

ステップ 2 [Choose Pool] をクリックし、SSID の IP プール予約を選択します。

ステップ 3 [Assign SGT] ドロップダウンリストから、SSID のスケーラブルなグループを選択します。

ステップ 4 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

仮想ネットワーク

仮想ネットワークは、共通物理ネットワークインフラストラクチャ内でトラフィックをセグメント化するために使用されるオーバーレイです。これは「マクロセグメンテーション」とも呼ばれます。レイヤ 2 仮想ネットワークはスイッチドトラフィックをセグメント化し、レイヤ 3 仮想ネットワークはルーテッドトラフィックをセグメント化します。Cisco SD-Access ファブリックに接続されている各エンドポイントは、静的エッジポート設定または Identity Service Engine からの動的ポリシーに基づいて、特定の仮想ネットワークに割り当てられます。仮想ネットワークのエンドポイントは、マイクロセグメンテーションポリシーによって明示的にブロックされていないかぎり、相互に通信できます。異なる仮想ネットワークにまたがるエンドポイントは、デフォルトでは、相互に通信できません。仮想ネットワーク間トラフィックの場合は、接続ポリシーを Cisco SD-Access ファブリックの外部（フュージョンデバイス上など）で実装する必要があります。

仮想ネットワークの一般的な使用例は、社内エンドポイントとビルディング管理システムの両方を含むオフィスビルです。社内エンドポイントは、照明、暖房、換気、空調などのビルディングシステムとは別にセグメント化する必要があります。この場合、ネットワーク管理者は、2 つ以上の仮想ネットワークを使用して社内エンドポイントとビルディングシステムをマクロセグメント化することにより、ビルディングシステムと社内エンドポイントの間の不正アクセスをブロックすることができます。

レイヤ 3 仮想ネットワークは、複数のファブリックサイトやネットワークドメイン（ワイヤレス LAN、キャンパス LAN、および WAN）にまたがる場合があります。レイヤ 2 仮想ネットワークは、単一のファブリックサイト内に存在します。

レイヤ 3 仮想ネットワークの作成

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]** > **[Create Layer 3 Virtual Network]** の順に選択します。

または、[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択して [Layer 3 VNs] タブに移動し、[Create Layer 3 VN] をクリックすることもできます。

ステップ 2 [Add Virtual Network] ワークフローウィンドウで、[Let's Do it] をクリックします。

ステップ 3 [Create Layer 3 Virtual Networks] ウィンドウで、作成するレイヤ 3 仮想ネットワークの数を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 レイヤ 3 仮想ネットワークの名前を入力し、[Next] をクリックします。

ステップ 6 レイヤ 3 仮想ネットワークをファブリックサイトおよびファブリックゾーンに関連付けるには、ドロップダウンリストからレイヤ3仮想ネットワークを選択し、対応するドロップダウンリストからファブリッ

クサイトを選択します。仮想ネットワークは複数のファブリックサイトに割り当てることができます。作成したすべてのレイヤ 3 仮想ネットワークについて、この関連付けを繰り返します。

または、[By Fabric Site] タブで、ファブリックサイトに複数の仮想ネットワークを割り当てることができます。

ステップ 7 [Next] をクリックします。

ステップ 8 この仮想ネットワークが複数のファブリックサイトに関連付けられている場合のトラフィックの出口動作を設定します。

a) デフォルトでは、[Local Exit] が選択されています。これにより、関連付けられている各ファブリックサイトのローカルボーダーを通過してトラフィックが出るようになります。

b) 仮想ネットワークを位置指定し、指定された境界でトラフィックが出られるようにするには、[Remote Exit] を選択します。

関連付けられているファブリックサイトのリストから、この仮想ネットワークにおけるすべてのトラフィックに関して出口として機能するボーダーを持つサイトを選択します。関連付けられている他のファブリックサイトは、この仮想ネットワークを継承します。

ステップ 9 [Next] をクリックします。

ステップ 10 仮想ネットワークを設定する前に、[Summary] ウィンドウで仮想ネットワークの設定を確認します。

ステップ 11 仮想ネットワークのコンテキストを作成するには、[Create] をクリックします。

ステップ 12 選択したサイトに仮想ネットワークを割り当てるには、[Deploy] をクリックします。

ステップ 13 仮想ネットワークの作成を確認するには、[View All Virtual Networks] をクリックします。

ステップ 14 [Virtual Networks] ウィンドウに、ファブリックに含まれるすべてのレイヤ 3 仮想ネットワークの詳細情報が表示されます。

レイヤ 2 仮想ネットワークの作成

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]** > **[Create Layer 2 Virtual Network]** の順に選択します。

または、[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択して [Layer 2 VNs] タブに移動し、[Create Layer 2 VN] をクリックすることもできます。

ステップ 2 [Create L2 Virtual Network] ウィンドウで、[Let's Do it] をクリックします。

ステップ 3 ファブリックに接続する VLAN の数を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 [Configure VLANs] ウィンドウで、次の手順を実行します。

a) 各 VLAN の **VLAN 名**とオプションの **VLAN ID** を入力します。

b) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。
レイヤ 2 仮想ネットワークではフラッディングがデフォルトで有効になっています。

c) [Next] をクリックします。

ステップ 6 [Select your CPs for each L2VN] ウィンドウで、作成した各レイヤ 2 仮想ネットワークのファブリックサイトとレイヤ 3 仮想ネットワークを選択します。

レイヤ 2 仮想ネットワークが複数のファブリックサイトに展開されている場合、Cisco DNA Center は、共通プールを使用してサブネットを拡張します。

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、レイヤ 2 仮想ネットワークの設定を確認します。[作成（Create）] をクリックします。

ステップ 9 レイヤ 2 仮想ネットワークのプロビジョニングを確認するために、[Submit] をクリックします。

レイヤ 2 仮想ネットワークがプロビジョニングされると、成功メッセージが表示されます。

ステップ 10 レイヤ 2 仮想ネットワークの作成を確認するには、[Virtual Network Overview] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブには、ファブリックに含まれるすべてのレイヤ 2 仮想ネットワークの詳細情報が表示されます。

ファブリックサイトへのレイヤ 3 仮想ネットワークの追加

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[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブで、目的のレイヤ 3 仮想ネットワークについて、**[Actions (…)]** > **[Add to fabric site]** の順にクリックします。

ステップ 4 [Select Fabric Site] スライドインウィンドウで、サイトを選択し、[Select] をクリックします。

この仮想ネットワークを別のファブリックサイトに追加するには、次の手順を実行します。

レイヤ 3 仮想ネットワークへのゲートウェイの追加

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[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブで、目的のレイヤ 3 仮想ネットワークについて、**[Actions (…)]** > **[Add gateways]** の順にクリックします。

[Add Pools to an L3VN] ウィンドウに、選択したレイヤ 3 仮想ネットワークが割り当てられているすべてのサイトが表示されます。

ステップ 4 [Add Pools to an L3VN] ウィンドウの左側のペインで、ゲートウェイを作成するレイヤ 3 仮想ネットワークを選択し、次の手順を実行します。

a) ドロップダウンリストから [IP Pool] を選択します。

（注） ファブリックサイトと同じサイトレベルで予約されている IP プールからのみ選択できます。ネットワーク設定を設計するときに、IP プールの予約できます。

b) [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] を選択します。

c) [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。

VLAN ID については、次の点に注意してください。

- VLAN ID 1、1002 ー 1005、2046、および 4095 は予約済みで、使用できません。
- カスタム VLAN ID を指定しない場合は、Cisco DNA Center が 1021 ー 2020 の範囲の VLAN ID を生成します。

d) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。

e) [Scalable Group] ドロップダウンリストからグループを選択します。

f) レイヤ 2 フラッディングを有効にするには、[Flooding] トグルボタンをクリックします。

（注） レイヤ 2 フラッディングにはアンダーレイマルチキャストが必要であり、これは LAN 自動化中に設定されます。LAN 自動化でアンダーレイをプロビジョニングしない場合は、アンダーレイマルチキャストを手動で設定します。

g) この IP プールをクリティカル IP アドレスプールに含めるには、[Critical VLAN] トグルボタンをクリックします。

クリティカルプールは、認証サーバーを使用できない場合に、クローズド認証プロファイルに使用されます。認証サーバーがない場合、クリティカルプールにクリティカル VLAN が割り当てられ、未認証のすべてのホストがそのクリティカル VLAN に配置されます。

h) この IP プールをワイヤレス IP アドレスプールとして有効にするには、[Wireless] トグルボタンをクリックします。

i) IP ダイレクトブロードキャスト機能を有効にするには、[Directed Broadcast] トグルボタンをクリックします。

（注）
- IP ダイレクトブロードキャストを有効にする前に、レイヤ 2 フラッディングを有効にしてください。
- ルータおよび Nexus 7000 シリーズ スイッチは、IP ダイレクトブロードキャストをサポートしていません。
- IP ダイレクトブロードキャストを有効にする前に、アンダーレイマルチキャストが有効になっていることを確認してください。

j) IP プールをさらに関連付けるには、アイコンをクリックして上記の手順を繰り返します。
k) [Next] をクリックします。

ステップ 5 [Summary] ウィンドウで、エンドポイントの接続設定を確認します。

ステップ 6 [Provisions in progress] ウィンドウで、[Submit] をクリックします。

ステップ 7 成功メッセージが表示された後にゲートウェイの作成を確認するには、[Virtual Network overview] をクリックします。

ステップ 8 [Virtual Networks] ウィンドウ の [Segments] の下にある [Layer 2 VNs] タブに、すべてのレイヤ 2 仮想ネットワークとその詳細情報が表示されます。

ファブリックゾーンの設定

ファブリックサイト（親サイト）は、ネットワークを簡単に管理できるように、より小さなサブネットによるファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、コントロールプレーンとボーダーのために親サイトに接続します。Cisco DNA Center の以前のリリースから移行した場合は、既存のファブリックサイトにファブリックゾーンを作成することができます。このファブリックゾーンは、親サイトのすべてのプロパティを継承します。

はじめる前に

- ネットワーク階層がグローバルサイトの下に作成されていることを確認します。
- 階層の最下位に位置していない親サイトを選択します。

次に、ファブリックゾーンを設定するためのワークフローの概要を示します。

1. 次のいずれかの方法でファブリックゾーンを作成します。
   - [Create a Fabric Site and Fabric Zones] ワークフローを使用して、ファブリックサイトとそのゾーンを作成します。詳細については、ファブリックサイトおよびそのファブリックゾーンの作成 （483 ページ）を参照してください。
   - 既存のファブリックサイトを編集して、ファブリックゾーンを追加します。詳細については、既存のファブリックサイトでのファブリックゾーンの作成 （484 ページ）を参照してください。

2. ファブリックゾーンにエッジノードと拡張ノードを追加します。詳細については、ファブリックへのデバイスの追加 （469 ページ）を参照してください。
3. ファブリックゾーンにレイヤ 3 仮想ネットワークとセグメントを割り当てます。ファブリックゾーンで使用できるのは親サイトの仮想ネットワークとセグメントのみであることに注意してください。詳細については、「ファブリックゾーンへの仮想ネットワークの追加 （484 ページ）」を参照してください。

（注） ファブリックゾーンに追加されたセグメントは、親サイトでは更新できません。

親サイトのファブリックゾーンのエッジノードおよび拡張ノードは編集できません。

ファブリックゾーンのエッジノードは、親サイトのコントロールプレーンまたはボーダーとして設定できます。

ファブリックサイトおよびそのファブリックゾーンの作成

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 2 [Fabric Sites] タブで、[Add Fabric Site] をクリックします。

または、最初の 2 つの手順を実行する代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** の順に選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let’s Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、表示されたネットワーク階層からファブリックサイトを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 8 [作成（Create）] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。「**Success!**Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

既存のファブリックサイトでのファブリックゾーンの作成

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

ステップ 2 [Fabric Sites] タブで、ファブリックサイトを選択します。

[Site] ウィンドウで、**[More Actions]** > **[Edit Fabric Zone]** をクリックします。

ステップ 3 [Designate fabric zones] ウィンドウで、ファブリックゾーンとして追加するエリア、ビルディング、またはフロアを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 6 [作成（Create）] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。「**Success!**Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

次のタスク

- 新しく作成したファブリックゾーンにエッジデバイスと拡張ノードデバイスだけを追加します。

  ファブリックゾーンに割り当てられたデバイスを親サイトに割り当てることはできません。ただし、ファブリックゾーンに割り当てられたエッジデバイスを親サイトのコントロールプレーンまたはボーダーとして設定することは引き続き可能です。

- ファブリックゾーンに IP プールと仮想ネットワークを割り当てます。

ファブリックゾーンへの仮想ネットワークの追加

始める前に

ファブリックゾーンが作成されていることを確認します。

ファブリックゾーンに追加できるのは親サイトの仮想ネットワークだけであることに注意してください。

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[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択します。

ステップ 5 [Layer 3] タブで、[Add Layer 3 VN] をクリックします。

ステップ 6 [Add Virtual Network] スライドインペインで、ファブリックゾーンに追加する仮想ネットワークを選択します。[更新（Update）] をクリックします。

ファブリックゾーンへのレイヤ 2 仮想ネットワークの追加

始める前に

ファブリックゾーンに追加されたゲートウェイは親サイトで更新できないことに注意してください。

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[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウで、**レイヤ 2 仮想ネットワーク**の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 2 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択します。

ステップ 5 [Layer 2] タブで、[Add Layer 2/ Gateways] をクリックします。

ステップ 6 [Select L2VNs/Gateway] スライドインペインで、ゲートウェイを設定するファブリックゾーンのレイヤ 3 仮想ネットワークを選択します。

ステップ 7 [Next] をクリックします。

ステップ 8 [L2VNs/Gateway(s)] ドロップダウンリストから、目的のゲートウェイを選択します。

ステップ 9 [Add] をクリックします。

拡張ノードデバイスの設定

拡張ノードはレイヤ 2 スイッチモードで動作するデバイスで、ファブリックテクノロジーをネイティブにはサポートしていません。拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。拡張ノードでの [Port Assignment] は、[Host Onboarding] ウィンドウで実行できます。

（注） 拡張ノードは、ユーザー インターフェイスベースのプロビジョニング ワークフローではオンボードできません。拡張ノードをオンボードするには、デバイス設定を工場出荷時の初期状態にリセットし、デバイスの電源をオンにした後に、SD-Access 自動化ワークフローを使用する必要があります。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

ポリシー拡張ノードは、仮想ネットワーク内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードのポート割り当て時に、[Group] を選択できます。

Cisco IOS XE 17.1.1s 以降のリリースのソフトウェアを実行している Cisco Catalyst 産業用イーサネット（IE）3400、IE 3400 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチは、ポリシー拡張ノードデバイスです。

Cisco デジタル ビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco 産業用イーサネット 4000、4010、5000 シリーズスイッチは、ポリシー拡張ノードデバイスではありません。ポート割り当て時の [Cisco TrustSec] と [Group] の選択はサポートされていません。

拡張ノードの設定手順

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズスイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

ポリシー拡張ノードをサポートするエッジノードでサポートされているソフトウェアの最小バージョンは Cisco IOS XE 17.1.1 s です。

（注） ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズスイッチは、拡張ノードデバイスをサポートしていません。

以下に、拡張ノードでサポートされている最小ソフトウェアバージョンを示します。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ：15.2(7)E0s（LAN ベースライセンスが有効になっている）

  IP サービスライセンスがある場合は、Switch Database Management（SDM）テンプレートを `dual-ipv4-and-ipv6 default` に手動で変更する必要があります。

- Cisco Catalyst IE 3400、3400 Heavy Duty（X-coded および D-coded）シリーズ スイッチ：IOS XE 17.1.1s
- Cisco Catalyst IE 3300 シリーズ スイッチ：IOS XE 16.12.1s
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：15.2(7)E0s

ポリシー拡張ノードを設定する前に、次のことを確認してください。

- ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE 17.1.1 s です。
- ポリシー拡張ノードとそれをサポートするエッジノードの両方で、Network Advantage と DNA Advantage のライセンスレベルが有効になっている必要があります。

ステップ 1 拡張ノードのネットワーク範囲を設定します。IP アドレスプールを設定する （197 ページ） を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP クレデンシャルが設定されていることを確認します。

ステップ 2 拡張 IP アドレスプールを INFRA_VN に割り当てます。レイヤ 3 仮想ネットワークへのゲートウェイの追加 （480 ページ） を参照してください。[Pool Type] で [Extended] を選択します。

Cisco DNA Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

（注） オプション 43 の詳細については、DHCP コントローラ ディスカバリ （366 ページ） を参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。リングまたはデイジーチェーン内の後続の拡張ノードに関して、それが接続している、前の拡張ノードでポートチャネルを作成します。

（注） この手順は、ファブリックのグローバル認証モードが [Open]、[Low Impact]、または [Closed] の場合にのみ完了してください。ファブリックサイトが [No Authentication] モードに設定されている場合、ポートチャネルは、プラグアンドプレイ プロビジョニングを使用した拡張ノードのオンボーディング中に自動的に作成されます。

ポートチャネルを作成するには、次の手順を実行します。

a) [Provision] > [Fabric Sites] > [Fabric Infrastructure] に移動し、ファブリックエッジノード（または接続に応じて拡張ノード）を選択します。タイトルにデバイス名の付いたウィンドウがスライド表示されます。

b) [Port Channel] タブで、[Create Port Channel] をクリックします。

c) 次のすべてのフィールドに入力します。

- [Connected Device Type] ロップダウンリストから [Extended Node] を選択します。
- [Port Aggregation Protocol (PAgP)] を選択します。

  Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAgP をサポートしています。

- Cisco IOS XE 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [On] を選択します。
- 拡張ノードのオンボーディングでは Link Aggregation Control Protocol（LACP）は機能しないことに注意してください。
- ポートチャネルとしてバンドルするポートを選択します。

d) [Done] をクリックします。

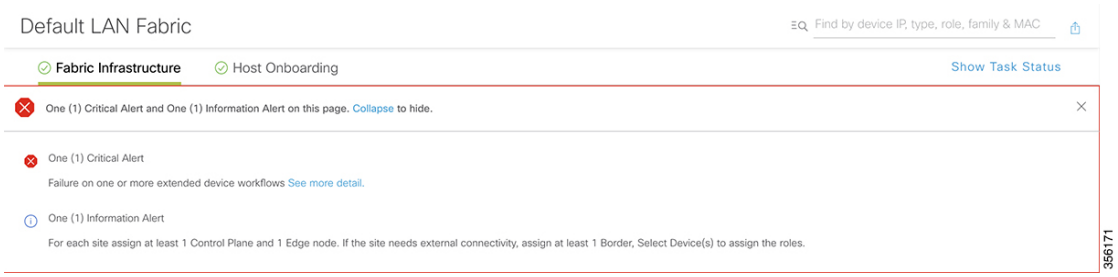
これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

Cisco DNA Center Cisco DNA Center では、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。次に、拡張ノードデバイスがファブリックに追加されます。これで、拡張ノードデバイスがオンボードされ、管理できるようになりました。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ（X）とともに表示されます。

拡張ノードの設定中にワークフローでエラーが発生した場合は、[Topology] ウィンドウにバナーでエラー通知が表示されます。



[See more details] をクリックしてエラーを確認します。

[Task Monitor] ウィンドウがスライド表示され、拡張ノード設定タスクのステータスが表示されます。

[See Details] をクリックして、エラーの原因および考えられるソリューションを確認します。

ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバーなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポート チャネルの作成

認証がクローズド認証の場合にのみ、次の手順を実行します。他の認証モードでは、次の手順が自動化されていることに注意してください。

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]** > **[Fabric]** の順に選択します。

ステップ 2 表示されたウィンドウで、ファブリックをクリックします。

ステップ 3 [Fabric Sites] ペインで、サイトを選択します。

ステップ 4 [Fabric Infrastructure] タブをクリックすると、すべてのファブリックデバイスが表示されます。

ステップ 5 ファブリックエッジノードをクリックします。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 6 [Port Channel] タブで、[Create Port Channel] をクリックします。

ステップ 7 表示されたポートの一覧から、バンドルするポートを選択します。

ステップ 8 [Connected Device Type] ドロップダウンから、接続済みのデバイスのタイプを選択します。

a) ファブリックエッジノードと拡張ノードの間にポートチャネルを作成する場合は、[Extended Node] を選択します。

b) ファブリックエッジノードとサーバーの間にポートチャネルを作成する場合は、[Server] を選択します。

ステップ 9 プロトコルとして [PAGP] を選択します。

ステップ 10 [Done] をクリックします。

作成した新しいポートチャネルがウィンドウに表示されます。

ステップ 11 [Provision] > [Fabric] > [Host Onboarding] ページに移動します。作成されたポートチャネルを選択します。

ステップ 12 [更新（Update）] をクリックします。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも 1 つのメンバーインターフェイスが存在す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]** > **[Fabric]** の順に選択します。

ステップ 2 表示されたウィンドウで、ファブリックをクリックします。

ステップ 3 [Fabric Sites] ペインで、サイトを選択します。

ステップ 4 [Fabric Infrastructure] タブをクリックすると、すべてのファブリックデバイスが表示されます。

ステップ 5 ファブリックエッジノードをクリックします。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 6 [Port Channel] タブを選択します。

ステップ 7 表示されるポートチャネルのリストから、更新するポートチャネルを選択します。

結果のウィンドウに、選択したポートチャネルのすべてのインターフェイスとステータスが表示されます。

ステップ 8 ポートチャネルで必要な更新を実行します。

ポートチャネルにインターフェイスを追加したり、ポートチャネルの既存のインターフェイスを削除したりできます。

ステップ 9 [Done] をクリックします。

ポートチャネルの削除

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

ステップ 2 表示された [Fabric Sites] ウィンドウで、ファブリックサイトをクリックします。

ステップ 3 [Fabric Infrastructure] タブで、ポートチャネルを削除するデバイスをクリックします。

ステップ 4 スライドインウィンドウで、[Port Channel] タブをクリックします。

開いた [Port Channel] ビューには、既存のポートチャネルがすべて表示されます。

ステップ 5 ポートチャネルを選択し、[Delete] をクリックします。

ステップ 6 プロンプトで [Yes] をクリックします。

マルチキャスト概要

マルチキャスト トラフィックは、次のような異なる方法で転送されます。

- ランデブー ポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。
- 最短パス ツリー（SPT）経由。PIM Source Specific Multicast（SSM）では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジ ルータで送信元が認識されると SPT に切り替わります。

『IP マルチキャスト ルーティング テクノロジーの概要（IP Multicast Technology Overview）』を参照してください。

マルチキャストの設定

Cisco DNA Center には、仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローが用意されています。このワークフローでは、ネットワークでのマルチキャスト実装（ネイティブマルチキャストまたはヘッドエンドレプリケーション）を選択することもできます。

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]**。
すべてのプロビジョニングされたファブリックドメインがウィンドウに表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。ファブリックに設定されているすべてのサイトが表示されます。マルチキャストを設定するサイトを選択します。

ステップ 3 [Fabric Sites] ペインで、選択したサイトの横にある歯車アイコンをクリックします。

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

マルチキャスト構成のワークフローの最初のウィンドウが表示されます。

ステップ 5 [Enabling Multicast] ウィンドウで、ネットワークのマルチキャスト実装方式（[Native Multicast] または [Head-end replication]）を選択し、[Next] をクリックします。

ステップ 6 [Virtual Networks] ウィンドウで、マルチキャストを設定する仮想ネットワークを選択します。[Next] をクリックします。

ステップ 7 [Multicast pool mapping] ウィンドウで、[IP Pools] 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。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。[Next] をクリックします。

ステップ 8 [Select multicast type] ウィンドウで、実装するマルチキャストのタイプを選択し、[Next] をクリックします。

- **SSM**（送信元特定マルチキャスト）
- **ASM**（任意の固有のマルチキャスト）

ステップ 9 次の手順を実行します。

a) [SSM] を選択した場合は、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。

1. 225.0.0.0 ～ 239.255.255.255 の IP グループ範囲を選択します。
2. IP グループの [Wildcard Mask] を入力します。
3. [Next] をクリックします。

b) [ASM] を選択した場合は、ランデブーポイント（RP）のタイプを選択します。

- **内部 RP**
- **外部 RP**

[次へ (Next)] をクリックします。

ステップ 10 ランデブーポイントを設定するには、次の手順を実行します。

内部ランデブーポイントを設定する場合は、次のようにします。

a) 内部ランデブーポイントとして設定する必要があるデバイスを選択します。選択した 2 番目のランデブーポイントは、冗長ランデブーポイントになります。**[次へ (Next)]** をクリックします。
b) 一覧表示されている各仮想ネットワークに内部ランデブーポイントを割り当てます。[Next] をクリックします。

外部ランデブーポイントを設定する場合は、次のようにします。

a) [Setup your External RP] ウィンドウで、外部ランデブーポイントの IPv4 または IPv6 アドレスを入力します。

（オプション）2 番目の IPv4 または IPv6 アドレスのセットを入力できます。

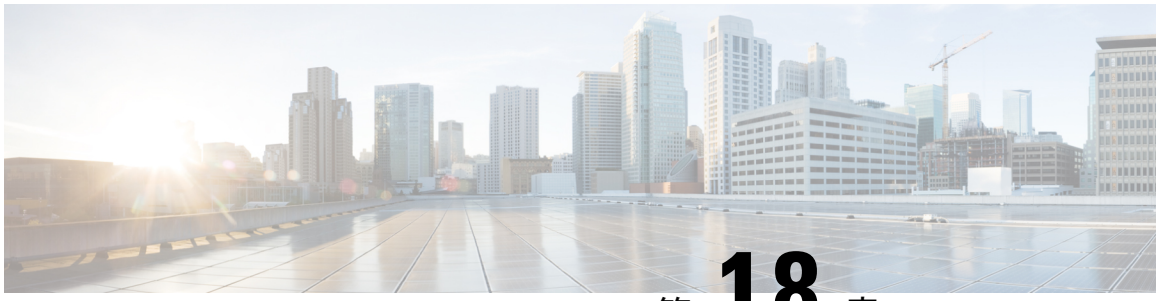
[Next] をクリックします。

b) [Select which RP IP Address(es) to utilize] ウィンドウで、各仮想ネットワークの IP アドレスを選択します。

[Next] をクリックします。

ステップ 11 構成を送信する前に、[Summary] ウィンドウに表示されているマルチキャスト設定を確認し、必要に応じて変更します。

[Finish] をクリックして、マルチキャストの設定を完了します。



第 18 章

サービスのプロビジョニング

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。

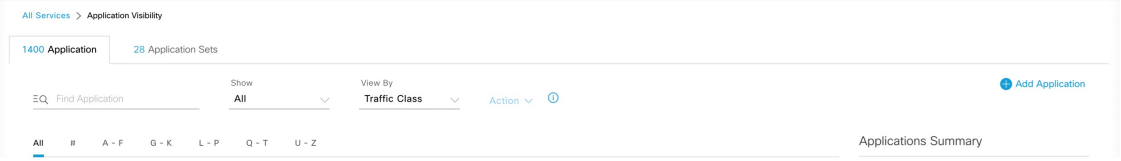
- [Application Policy]：キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。
- [Application Registry]：アプリケーションとアプリケーションセットを表示、管理、および作成できます。
- [Application Visibility Service]：Network-Based Application Recognition（NBAR）および CBAR の技術を使用してアプリケーションを分類できます。

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。

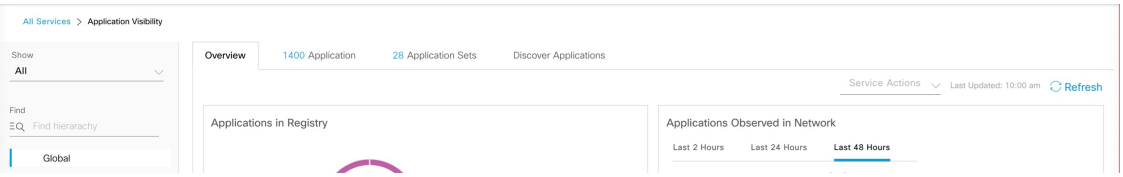
パッケージは必要に応じて任意にインストールできます。

（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：継続的なモニター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 *53 : [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	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。 • [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 Cisco DNA 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
ネットワークで確認されたアプリケーション	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。 （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。
アクティブな認識方法によるデバイス	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。 • CBAR 対応デバイス：ルータとスイッチ • 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 • IP/ポートベースのデバイス：スイッチ • 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
CBAR 準備状況ステータス	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。 • [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 • [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

グラフ	説明
Service Health and CBAR Health	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。 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。 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。 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。
CBAR 正常性の問題と修復	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。 • エラー（P1） • 警告（P2） • その他 （P3） [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。

[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 *54 : [Day-N Application Visibility]* ビュー：*[Site Devices Table]*

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。

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。
アプリケーションポリシー	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）が一方向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（309 ページ）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 NBAR アプリケーションを選択した場合、選択した NBAR 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 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。

フィールド	説明
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。
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 （502 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（503 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（504 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 （500 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 Click the **APplication Sets** tab.

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 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。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 （65 ページ）」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。

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（513 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 （514 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 （514 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。

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]** > **[App Hosting for Switches]** 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 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

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 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。

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 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設定の編集

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構成が必要な場合は、アプリケーション構成を編集できます。

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 アプリケーションを編集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、[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 （517 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 （517 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 （514 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 （521 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 （61 ページ）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 （135 ページ）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 （514 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 （552 ページ）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

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。

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 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 （124 ページ）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 （197 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、**[Provision]** > **[Site to Site VPN]** の順に選択します。

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 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] をクリックして VPN を作成します。

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、**[Provision]** > **[Site to Site VPN]** の順に選択します。

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、**[Provision]** > **[Site to Site VPN]** の順に選択します。

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]** 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]** 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を生成します。

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 [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 次のいずれかを実行し、[Next] をクリックします。

- 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。
- 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 11 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 12 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 13 [構成] をクリックします。

画面には、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 14 [View Provisioning Status] をクリックします。

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（526 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。

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 *55 : 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

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 Cisco DNA 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。
- 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 （527 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 （528 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 （528 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

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 （530 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 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 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、[Next] 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. 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] を選択します。
3. [**保存（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、[Next] をクリックします。

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) [Next] をクリックし、[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。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。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。

d) [Next] をクリックします。

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 [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] ウィンドウで詳細を確認し、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* からのみモニタできます。

ネットワークデバイスでの Cisco Umbrella の無効化

ステップ 1 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 （530 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 （530 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 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 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 [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 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウで、[Deploy] をクリックします。

ステップ 8 [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 9 [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 （530 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 （530 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。

第 19 章

ネットワークデバイスのコンプライアンス監査

コンプライアンスの概要

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性があるネットワークのインテントの逸脱や**帯域外**の変更を特定するのに役立ちます。

ネットワーク管理者は、Cisco DNA Center でソフトウェアイメージ、PSIRT、ネットワークプロファイルなどコンプライアンスのさまざまな側面のコンプライアンス要件を満たさないデバイスを簡単に特定できます。

コンプライアンスチェックは、自動化することも、オンデマンドで実行することもできます。

- 自動コンプライアンスチェック：Cisco DNA Center でデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリやSWIMなどさまざまなサービスからのトラップと通知をリッスンして、データを評価します。
- 手動コンプライアンスチェック：Cisco DNA Center でユーザーが手動でコンプライアンスをトリガーできるようにします。
- スケジュールされたコンプライアンスチェック：スケジュールされたコンプライアンスジョブは、毎週実行されるコンプライアンスチェック（毎週土曜日の午後 11 時に実行）です。

手動コンプライアンスの実行

Cisco DNA Center では、コンプライアンスチェックを手動でトリガーできます。

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]** > **[Inventory]** の順に選択します。

ステップ 2 一括してコンプライアンスチェックを行う場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

ステップ 3 デバイスごとにコンプライアンスチェックを行う場合は、次の手順を実行します。

a) コンプライアンスチェックを実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

c) または、[Compliance] 列（使用可能な場合）をクリックし、[Run Compliance] をクリックします。

ステップ 4 デバイスの最新のコンプライアンスステータスを表示するには、次の手順を実行します。

a) デバイスとインベントリを選択します。デバイス情報の再同期 （87 ページ）を参照してください。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

（注）
- 到達不能のデバイスやサポートされていないデバイスに対してコンプライアンスの実行をトリガーすることはできません。
- デバイスに対してコンプライアンスを手動で実行しない場合、コンプライアンスチェックはコンプライアンスのタイプに応じて一定期間後に実行されるように自動的にスケジュールされます。

コンプライアンスサマリーの表示

インベントリページには、デバイスごとにコンプライアンスの集約ステータスが表示されます。

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]** > **[Inventory]** の順に選択します。

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックすると、コンプライアンス サマリー ウィンドウが開きます。このウィンドウには、選択したデバイスに適用可能な次のコンプライアンスチェックが表示されます。

- スタートアップ設定と実行中の設定
- ソフトウェア イメージ

- 重大なセキュリティの脆弱性
- ネットワークプロファイル
- ファブリック
- アプリケーションの可視性

（注）
- [Network Profile]、[Fabric]、および [Application Visibility] はオプションであり、デバイスが必要なデータでプロビジョニングされている場合にのみ表示されます。
- コンプライアンスデバッグの場合、カスタマーセットアップから次の情報を収集します。
  1. コンプライアンスサマリーのスクリーンショットと、不一致を並べて表示したスクリーンショット。
  2. デバッグログには **spf-service-manager-service** が含まれている必要があります。システム設定の [Debugging Logs] ウィンドウで、**spf-service-manager-service** の [Service] ドロップダウンリストを有効にし、**spf-service-manager-service** で **com.cisco.dnac.compliance** の [Logger Name] を設定する必要があります。

コンプライアンスのタイプ

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
スタートアップ設定と実行中の設定	このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。デバイスのスタートアップ設定と実行中の設定が同期していない場合は、コンプライアンスがトリガーされ、アウトオブバンド変更の詳細レポートが表示されます。スタートアップ設定と実行中の設定の比較に関するコンプライアンスは、アウトオブバンド変更の 5 分以内にトリガーされます。	• [Noncompliant]：スタートアップ設定と実行中の設定は同じではありません。詳細ビューには、スタートアップと実行中との違いか、または実行中と以前の実行中との違いが表示されます。 • [Compliant]：スタートアップ設定と実行中の設定は同じです。 • [NA (Not Applicable)]：このコンプライアンスタイプのデバイス（AireOS など）はサポートされていません。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
ソフトウェアイメージ	このコンプライアンスチェックは、Cisco DNA Center のタグ付きのゴールデンイメージがデバイスで実行されているかどうかをネットワーク管理者が確認するために役立ちます。これにより、デバイスのゴールデンイメージと実行中のイメージとの違いがわかります。ソフトウェアイメージに変更があると、遅延なくすぐにコンプライアンスチェックがトリガーされます。	• [Noncompliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行していません。 • [Compliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行しています。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージを使用できません。
重大なセキュリティ（PSIRT）	このコンプライアンスチェックでは、ネットワークデバイスが重大なセキュリティの脆弱性なしで実行されているかどうかを確認できます。	• [Noncompliant]：デバイスに重要なアドバイザリがあります。詳細レポートには、その他のさまざまな情報が表示されます。 • [Compliant]：デバイスに重大な脆弱性はありません。 • [NA (Not Applicable)]：Cisco DNA Center でネットワーク管理者がセキュリティ アドバイザリ スキャンを実行していないか、デバイスがサポートされていません。
ネットワークプロファイル	Cisco DNA Center では、ネットワークプロファイルでインテント設定を定義して、そのインテントをデバイスにプッシュできます。アウトオブバンド変更またはその他の変更のために任意の時点で違反が検出された場合、このチェックにより、それが識別されて、評価され、フラグが立てられます。違反は、コンプライアンス サマリー ウィンドウの [Network Profiles] でユーザーに対して表示されます。 （注） ネットワーク プロファイル コンプライアンスは、ルータおよびワイヤレス LAN コントローラに適用されます。	• [Noncompliant]：デバイスでプロファイルのインテント設定が実行されていません。 • [Compliant]：ネットワークプロファイルがデバイスに適用されており、同時に、Cisco DNA Center にプッシュされたデバイス設定がデバイスでアクティブに実行されています。 • [Error]：根本的なエラーのため、コンプライアンスがステータスを計算できませんでした。詳細については、エラーログを参照してください。
ファブリック（SDA） この機能はベータ版です。	ファブリック コンプライアンスは、ファブリック インテント違反（ファブリック関連の設定のアウトオブバンド変更など）の識別に役立ちます。	• [Noncompliant]：デバイスでインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
アプリケーションの可視性	Cisco DNA Center では、アプリケーション可視性インテントを作成して、CBAR および NBAR を介してデバイスにプロビジョニングできます。デバイスにインテント違反がある場合、このチェックにより、違反が識別されて、評価され、[Application Visibility] に準拠または非準拠として表示されます。自動コンプライアンスチェックは、5 時間ごとに実行されるようにスケジュールされます。	• [Noncompliant]：デバイスで CBAR/NBAR 設定が実行されていません。 • [Compliant]：デバイスで CBAR/NBAR のインテント設定が実行されています。

N-1/N-2 からのアップグレード後のコンプライアンス動作

- N-1/N-2 からのアップグレードが正常に完了すると、該当するすべてのデバイス（システムでコンプライアンスが実行されたことがないデバイス）のコンプライアンスチェックがトリガーされます。
- コンプライアンスは、[Startup vs Running] タイプを除き、インベントリ上のデバイスのステータスを計算して表示します。
- アップグレード後、[Startup vs Running] タイルに [NA] が「Configuration data is not available」というテキストとともに表示されます。
- アップグレードが正常に完了してから 1 日後に、1 回限りのスケジューラが実行され、デバイスで構成データを使用できるようになります。[Startup vs Running] タイルに、正しいステータス（[Compliant]/[Non-Compliant]）と詳細データが表示され始めます。
- トラップを受信すると、設定アーカイブサービスが構成データを収集し、コンプライアンスチェックが再度実行されます。

（注） アップグレードセットアップでは、[Flex Profile] インターフェイスのコンプライアンスの不一致は無視してください。インターフェイス名の場合、[1] が [management] にマッピングされます。

第 20 章

構築と展開のワークフロー

AP 更新ワークフロー

ここでは、Cisco DNA Center のワークフローを使用して古いアクセスポイントを新しいアクセスポイントに置き換える方法を説明します。

AP 更新ワークフローの概要

AP 更新機能では、Cisco DNA Center のワークフローを使用して古い AP モデルを新しい AP モデルに置き換えることができます。

AP 更新ワークフローでは、Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP をサポートしています。

AP 更新ワークフローでサポートされる AP は次のとおりです。

- Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
- Cisco Aironet 1810W シリーズ アクセス ポイント
- Cisco Aironet 1815i アクセスポイント
- Cisco Aironet 1815w アクセス ポイント
- Cisco Aironet 1815m アクセスポイント
- Cisco Aironet 1830 シリーズ アクセス ポイント
- Cisco Aironet 1850 シリーズ アクセス ポイント

- Cisco Aironet 1800 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Catalyst 9115 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9117 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9120 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9130 シリーズ Wi-Fi 6 アクセスポイント

AP 更新ワークフロー

この手順では、Cisco DNA Center で古い AP を新しい AP に置き換える方法を示します。

始める前に

- 古い AP がプロビジョニング済みで、到達不能な状態になっている必要があります。
- 新しい AP が シスコ ワイヤレス コントローラに接続されて Cisco DNA Center のインベントリに登録され、到達可能な状態になっている必要があります。
- 古い AP と新しい AP が同じワイヤレスコントローラに関連付けられている必要があります。

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**[Workflows]** > **[Access Point Refresh]** の順に選択します。

使用可能なワークフローのライブラリが表示されます。これらのワークフローを使用することで、特定のタスクを手順に従って実行できます。

ステップ 2 [Let's Do it] 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。

[Get Started] 画面が表示されます。

ステップ 3 [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 Network Sites] 画面で、AP を更新するフロアまで移動し、[Next] をクリックします。

右側のペインに、選択したビルディング、フロア、およびそのフロアにプロビジョニングされている AP の合計数が表示されます。

すでにプロビジョニングされた状態の AP を置き換えることができます。

ステップ 5 [Select Access Points] 画面で、交換するデバイス名の横にあるチェックボックスをオンにし、[Next] をクリックします。

ステップ 6 [Select procedure for providing New Access Points] 画面で、新しい AP の詳細を指定する方法を選択します。[Add New Access Point detail via CSV file] または [Add New Access Point detail via GUI] のいずれかを選択できます。

- 新しいデバイス名とシリアル番号を含むカンマ区切り値（CSV）ファイルをアップロードする場合は、[Add New Access Point detail via CSV file] オプションボタンをクリックします。
  - これを行うには、[Download Selected Devices List] テンプレートをクリックし、新しい AP のデバイス名とシリアル番号を追加します。ダウンロードした CSV テンプレートファイルには、古い AP の詳細が含まれています。新しい AP のデバイス名とシリアル番号を追加した後、CSV ファイルをインポートするか、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します。
  - CSV ファイルをインポートするには、[Choose file] をクリックし、CSV の場所を参照して [Open] をクリックします。

    Cisco DNA Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。[View Details] をクリックすると、エラーメッセージの詳細が表示されます。

- GUI を使用して新しい AP の詳細を追加する場合は、[Add New Access Point detail via GUI] オプションボタンをクリックし、[Next] をクリックします。

  [Assign New Access Points] 画面が表示され、古い AP のそれぞれに対して新しい AP を割り当てることができます。

  - [Old Devices] 領域に、古い AP の IP アドレス、古い AP の名前、サイトの詳細、プラットフォーム、AP シリーズの情報などの詳細が表示されます。[New Devices] 領域で、新しいデバイスに関する詳細を入力します。
  - [Choose Serial Number] ドロップダウンリストから、新しい AP のシリアル番号を選択します。

    新しい AP がすでにワイヤレスコントローラに関連付けられ、インベントリに登録されている場合、その AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Managed] として表示されます。

    新しい AP が PnP で Cisco DNA Center に接続されている場合、その AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Unclaimed] として表示されます。

    新しい AP のシリアル番号がインベントリに登録されていない場合、そのシリアル番号は [Serial Number] ドロップダウンリストに表示されません。インベントリに登録されていない新しいシリアル番号を追加するには、[Choose Serial Number] ドロップダウンリストでシリアル番号を入力して [+] をクリックします。

（注） Cisco DNA Center で検証チェックが実行され、エラーがある場合は表示されます。続行する前に、これらのエラーを修正する必要があります。

新しい AP をプロビジョニングする前に、次の依存関係を解決する必要があります。

- cisco.com のログイン情報を入力してデバイスの EULA に同意します。
- シスコ ワイヤレス コントローラ ソフトウェア イメージ バージョンを更新します。この検証によって AP の更新が中止されることはありません。
- [AP Connected SwitchPort]：この検証メッセージによって AP の更新が中止されることはありません。

ステップ 7 [Next] をクリックします。

古い AP から新しい AP にコピーされた構成が、[Configuration Copied from Old Access Point to New] 画面に表示されます。

ステップ 8 [Next] をクリックします。

ステップ 9 [Submit Access Point Refresh Task] 画面で、[Provision] をクリックして AP 更新タスクを開始します。

ステップ 10 [Track Replacement Status] 画面で AP 交換ステータスをモニターできます。

- AP 交換ステータスの詳細を確認するには、[View Details] をクリックします。
  - AP の交換に成功した場合、[Replacement Status] ウィンドウの [Replacement Status] に [REPLACED] と表示されます。
  - AP の交換に失敗した場合、[Replacement Status] に [Error] と表示されます。
  - 交換エントリを削除するには、[Actions] 列で青色の 3 つのドットをクリックし、[Delete] をクリックします。[Warning] ダイアログボックスで、[Yes] をクリックします。
  - プロビジョニングの概要を CSV ファイルにダウンロードしてローカルに保存するには、[Export] をクリックします。
  - プロビジョニング ステータス レポートをダウンロードするには、[Download Report] をクリックします。

    （注） 新しい AP がインベントリでまだ検出されず、対応する AP 更新エントリが新しいデバイスの接続を待機している場合、または PnP 要求プロセスが進行中の場合は、シスコ ワイヤレス コントローラを再同期する必要があります。

ステップ 11 [Next] をクリックして、概要画面で詳細を確認します。

ステップ 12 交換が正常に完了すると、Cisco DNA アシュアランス で古い AP と新しい AP についての AP 更新イベントが生成されます。

AP 更新イベントは、[AP View 360] ウィンドウの [Event Viewer] で確認できます。

[Network Hierarchy] ウィンドウの対応するフロアマップで、新しい AP が自動的に更新されます。

ユーザー定義ネットワークの設定ワークフロー

ここでは、Cisco DNA Center でワークフローを使用して Cisco ユーザー定義のネットワークサービスを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の概要

プリンタ、スピーカー、Apple TV、Google Chromecast、リングドアベル、スマート電球など、ネットワーク上のホームデバイス、コンシューマデバイス、IoT デバイスは、デバイスの検出と使用が簡単になるように、Apple Bonjour などの Simple Service Discovery Protocol（SSDP）、マルチキャスト DNS（mDNS）、ユニバーサル プラグ アンド プレイ（UPnP）に依存しています。

Cisco ユーザー定義のネットワークサービスは、寮の部屋、教室、講堂などの共有環境において、クライアントデバイスのセキュアでリモートのオンボーディングを提供します。ユーザー定義のネットワークサービスを使用すると、SSDP（Apple Bonjour など）、mDNS プロトコル（AirPlay、AirPrint、画面ミラーリング、印刷など）、UPnP プロトコルのセキュアな使用が可能になり、共有環境におけるやり取りや共有を登録されたデバイスのみと行えるようになります。

ユーザー定義のネットワークサービスは、次のソリューションを提供します。

- クライアントデバイスの簡単でセキュアなオンボーディング。
- 特定のユーザーに属するクライアントデバイスの自動セグメンテーション。
- 他のユーザーを招待してデバイスを共有する機能。

サポートされる Cisco DNA Center、Cisco Identity Services Engine、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のソフトウェアバージョンとアクセスポイントは次のとおりです。

- Cisco DNA Center リリース 1.3.1.2 以降
- Cisco Identity Services Engine リリース 2.7 以降
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.1.x
- Cisco 802.11ac Wave 2 AP：
    - Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
    - Cisco Aironet 1810W シリーズ アクセス ポイント
    - Cisco Aironet 1815i アクセスポイント
    - Cisco Aironet 1815w アクセスポイント

- Cisco Aironet 1815m アクセスポイント
- Cisco 1830 Aironet シリーズ アクセスポイント
- Cisco Aironet 1850 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント

- Cisco 802.11ac Wave 1 AP
  - Cisco Aironet 1700 シリーズ アクセス ポイント
  - Cisco Aironet 2700 シリーズ アクセス ポイント
  - Cisco Aironet 3700 シリーズ アクセス ポイント

ユーザー定義のネットワークサービスを設定するための前提条件

Cisco ユーザー定義のネットワークサービスを設定する前に、次の前提条件を満たしている必要があります。

- AP が シスコ ワイヤレス コントローラ に参加していることを確認します。
- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の シスコ ワイヤレス コントローラと AP を検出します。
- AAA サーバー クライアント エンドポイントを Cisco Identity Services Engine にマッピングします。
- 認証トークンを Cisco DNA Center に追加します。
- 非ファブリック エンタープライズ SSID またはゲストワイヤレス SSID を任意のセキュリティで作成し、ネットワークプロファイルにマッピングします。
- SSID をプロビジョニングします。

ユーザー定義のネットワークサービスの設定

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 **[Workflows]** > **[Configure Cisco User Defined Network]** ウィンドウから設定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は、このほかに **[Provision]** > **[Services]** > **[Cisco User Defined Network]** ウィンドウからも設定できます。

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**[Workflows]** > **[Configure Cisco User Defined Network]** の順に選択します。

ステップ 2 [Let's Do It] をクリックします。

[Let's start with configuring the Service] 画面が表示されます。Cisco DNA Center を Cisco DNA Center Cloud に接続するために、Cisco DNA Center Cloud ポータルを使用して認証トークンを生成する必要があります。

ステップ 3 [Configure Cloud Service] をクリックします。

Cisco DNA Center Cloud アプリケーションが新しいタブで開きます。

ステップ 4 cisco.com アカウントの ID とパスワードを使用して Cisco DNA Center Cloud にログインします。

- 左側のメニューで [Authentication Token] タブをクリックします。

  [Authentication Token] ウィンドウが表示されます。

- [Authentication Token] ウィンドウで、[Generate New Token] をクリックします。

  認証トークンが生成されます。

- [Copy Token] をクリックして、認証トークンをコピーします。

ステップ 5 Cisco DNA Center の [Let's start with configuring the Service] 画面に戻ります。

ステップ 6 [Next] をクリックして、コピーした認証トークンを検証します。

ステップ 7 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 8 [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。

- [Select Sites] ドロップダウンリストからサイトを選択します。
- [Disable User Defined Network Service] チェックボックスをオンにすると、ワークフローが有効になっているすべてのサイトで無効になります。

ステップ 9 [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。

- [SSID(s)] ドロップダウンリストから、ユーザー定義のネットワークサービスを有効にする SSID を選択します。
- 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] をオンにします。
- 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。

- 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 10 [Next] をクリックします。

ステップ 11 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。
- ネットワークでのサービスのプロビジョニングを後で行う場合は、[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 12 次の詳細を確認し、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。

- **認証トークン**
- **選択したサイトと SSID**
- **スケジューリング**

ステップ 13 [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 14 [View Provisioning Status] をクリックします。

スイッチでのアプリケーション ホスティングの有効化

次の手順は、ThousandEyes Enterprise Agent、iPerf などの Docker アプリケーションを特定のサイトの選択したスイッチで有効にするために役立ちます。

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（513 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 （514 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 （514 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 App]** > **[Hosting for Switches]** の順に選択します。アプリケーションを選択し、画面下部の [Install] をクリックします。

ステップ 2 **[Workflows]** > **[Enable Apps on Switches]** > **[Let's Do it]** の順に選択してワークフローを起動することもできます。

ワークフローが起動されます。

（注） ページの上部にある青色の進捗状況バーにカーソルを合わせると、そこに一覧表示される前の手順に戻ることができます。

ステップ 3 [Select Site] ウィンドウで、アプリケーションを有効にするビルディングに移動します。

ステップ 4 [Next] をクリックします。

ステップ 5 [Select App] ウィンドウでアプリケーションを選択します。

ステップ 6 [Next] をクリックします。

（注） [+ New App] リンクにアクセスして、Cisco DNA Center に存在しないアプリケーションを追加できます。

ステップ 7 [Select Switches] ウィンドウで、アプリケーションを有効にするデバイスを選択します。

（注） [Select Switches] ダイアログボックスで指定したテンプレートに詳細を入力することにより、デバイスを一括でインポートまたはエクスポートできます。

ステップ 8 [Next] をクリックします。

ステップ 9 [Configuration App] ウィンドウで、以降の設定を実行します。

- **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 resources as asked by the app] または [Allocate all resources available on a device] チェックボックスをオンにします。
- [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 10 [Summary]ページで、選択したスイッチにアプリケーションをインストールする前に詳細を確認します。

ステップ 11 [Next] をクリックします。

[Provisioning Task] ウィンドウに、スイッチでのアプリケーションの展開を追跡するタスク名が表示されます。

ステップ 12 自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 13 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。

ステップ 14 [View Details] 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と障害を確認します。

ステップ 15 [Next] をクリックします。

アプリケーションが正常に有効化されました。

タスクの結果の概要と成功/失敗の回数が表示されます。

ステップ 16 [Manage App] をクリックします。ここで、アプリケーションのライフサイクル動作を管理して、N 日目のタスクを実行することができます。

IoT サービスの有効化ワークフロー

ここでは、Cisco DNA Center のワークフローを使用して、Cisco Catalyst 9100 シリーズ アクセス ポイントで Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法について説明します。

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

この手順では、選択した Catalyst 9100 シリーズ アクセス ポイントで、Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効に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**[Workflows]**。

使用可能なワークフローのライブラリが表示されます。これらのワークフローを使用することで、特定のタスクを手順に従って実行できます。

ステップ 2 [Enable IOT Services] をクリックします。

ステップ 3 [Let's Do It] をクリックして、インストールワークフローを開始します。

ステップ 4 [Select Site] ウィンドウで、IoT サービスを有効にするフロアまで移動します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Select the Application] ウィンドウで、ネットワークで IoT を有効にするための SES-imagotag ESL Connector アプリケーションを選択し、[Next] をクリックします。

（注） Cisco DNA Center に存在しないアプリケーションを追加するには、「アプリケーションの追加」を参照してください。

[Select Access Points] ウィンドウには、特定のフロアで使用可能なすべての AP が表示されます。

ステップ 7 [Select Access Points] ウィンドウで、IoT コネクタアプリケーションをインストールするデバイスの [Device Name] の横にあるチェックボックスをオンにします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、選択した AP にアプリケーションをインストールする前に詳細を確認し、[Next] をクリックします。

[Provisioning Task] ウィンドウが表示され、AP への任意のアプリケーションの展開を追跡するために作成されたタスク名が表示されます。

ステップ 10 自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 11 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。

ステップ 12 [View Details] 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。

ステップ 13 [Next] をクリックします。

タスク完了[Done! Task Completed] ウィンドウが表示されます。

ステップ 14 [Manage IoT Application] をクリックして、Day-N タスクを実行します。

IoT アプリケーションの管理

この手順では、IoT アプリケーションを管理する方法を示します。

始める前に

Cisco Catalyst 9000 シリーズ アクセス ポイントで IoT サービスを有効にしておく必要があります。

ステップ 1 IoT サービスを有効にした後、[Done! Task Completed] ウィンドウで [Manage IoT Application] をクリックします。

ステップ 2 [Hostname] の横にあるチェックボックスをオンにして、次のタスクを実行します。

- アプリケーションを起動するには、[Actions] ドロップダウンリストから [Start App] を選択します。
- アプリケーションを停止するには、[Actions] ドロップダウンリストから [Stop App] を選択します。
- アプリケーション設定を編集するには、[Actions] ドロップダウンリストから [Edit App Config] を選択します。
- アプリケーションをアップグレードするには、[Actions] ドロップダウンリストから [Upgrade App] を選択します。
- 選択した AP からアプリケーションをアンインストールするには、[Actions] ドロップダウンリストから [Uninstall App] を選択します。

ステップ 3 AP 名をクリックすると、次の詳細が表示されます。

- [AP Name]
- AP Status
- IP アドレス
- 状態

ステップ 4 [Tech Support logs] をクリックして、アプリケーション ホスティング ログを収集します。

Cisco DNA Center からの AP 設定について

[Configure Access Points] ワークフローを使用すると、Cisco DNA Center で AP レベルと無線レベルのパラメータを設定および展開できます。

次の AP レベルパラメータを設定できます。

- AP の位置
- AP 管理ステータス
- AP モード
- AP LED ステータス
- AP フェールオーバー優先度
- ハイ アベイラビリティ

次の無線レベルパラメータを設定できます。

- 無線管理ステータス
- 無線出力の設定
- 無線チャンネルの設定

AP ワークフローの設定

この手順では、Cisco DNA Center で AP および無線パラメータを設定する方法を示します。

始める前に

AP がサイトに割り当てら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**[Workflows]** > **[Configure Access Points]** の順に選択します。

ステップ 2 [Let's Do it] 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。

[Get Started] 画面が表示されます。

ステップ 3 [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 from the hierarchy] 画面で、AP 関連の設定を適用するサイトに移動します。

右側のペインに、選択したフロア、およびそのフロアで使用可能な AP の数が表示されます。

ステップ 5 [Next] をクリックします。

[Select Access Points] 画面に、選択したサイトで使用可能なすべての AP が一覧表示されます。

ステップ 6 [Select Access Points] 画面で、AP のチェックボックスをオンにして、AP 名を一括編集します。

ステップ 7 [Next] をクリックします。

[Modify AP Name] 画面には、前の画面で選択した AP のリストが表示されます。

ステップ 8 [Modify AP Name] 画面で、次のいずれかの方法を使用して AP の新しい名前を入力します。

- [Create a New Naming Convention]：このオプションボタンをクリックして、命名規則に基づいて名前を入力し、[Apply Pattern] をクリックします。[Access Points] テーブルには、入力した命名パターンに基づいて新しい AP 名が表示されます。
- [Upload a CSV file]：このオプションボタンをクリックして、サンプル CSV テンプレートファイルをダウンロードし、そのファイルに AP 名を追加します。次に、CSV ファイルをドラッグしてドロップエリアにドロップすることにより、または [Choose a file] をクリックし、CSV ファイルを参照して選択することにより、ファイルをアップロードします。

ステップ 9 [Next] をクリックします。

ステップ 10 [Configure AP Parameters] 画面で、次の AP パラメータを設定できます。

- [Location]：このチェックボックスをオンにして、ロケーションの詳細を入力します。
- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP LED Status]：AP LED ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP Mode]：このチェックボックスをオンにして、[Select AP Mode] ドロップダウンリストから AP モードを選択します。有効なモードは、[Local/Flex]、[Monitor]、[Bridge]、および [Flex+Bridge] です。
- [AP Failover Priority]：このチェックボックスをオンにして、[AP Failover Priority] ドロップダウンリストから AP のフェールオーバー優先順位を選択します。有効なオプションは次のとおりです。
  - [Low]：アクセスポイントに優先度レベル 1 を割り当てます。これは最も低い優先度レベルです。これはデフォルト値です。
  - [Medium]：アクセスポイントに優先度レベル 2 を割り当てます。

- [High]：アクセスポイントに優先度レベル 3 を割り当てます。
- [Critical]：アクセスポイントに優先度レベル 4 を割り当てます。これは最も高い優先度レベルです。

- [Controller Configuration]：このチェックボックスをオンにして、アクセスポイントのプライマリ、セカンダリ、およびターシャリコントローラの名前と IP アドレスを設定します。

ステップ 11 [Next] をクリックします。

ステップ 12 [Configure 802.11 a/n/ac/ax Parameters] 画面で、次の 802.11 a/n/ac/ax パラメータを設定します。

- [Admin Status] チェックボックスをオンにして、[Disable] ボタンをクリックして管理ステータスを無効にします。
- [Power Assignment] チェックボックスをオンにして、[Custom] ボタンをクリックして [Select Custom Power] ドロップダウンリストからカスタム電力を選択します。
- [Channel Assignment] チェックボックスをオンにして、[Custom] ボタンをクリックして [Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width] チェックボックスをオンにして、[Select Channel Width] ドロップダウンリストからいずれかのチャネル帯域幅オプションを選択します。
  - **20 MHz**
  - **40 MHz**
  - **80 MHz**
  - **160 MHz**
- [Antenna Name] チェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。
- アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、特定の空間領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ー 40 です。
- [Azimuth] チェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。
- [Elevation] チェックボックスをオンにして、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。
- [Next] をクリックします。

ステップ 13 [Configure 802.11 b/g/n Parameters] 画面で、次の 802.11 b/g/n パラメータを設定します。

- [Admin Status] チェックボックスをオンにして、[Disable] ボタンをクリックして管理ステータスを無効にします。

- [Power Assignment] チェックボックスをオンにして、[Custom] ボタンをクリックして [Select Custom Power] ドロップダウンリストからカスタム電力を選択します。
- [Channel Assignment] チェックボックスをオンにして、[Custom] ボタンをクリックして [Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Antenna Name] チェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。
- アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、特定の空間領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ー 40 です。
- [Azimuth] チェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。
- [Elevation] チェックボックスをオンにして、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。

ステップ 14 [Next] をクリックして、概要画面で詳細を確認します。[Summary] 画面で、次の AP 設定の詳細を確認し、該当するセクションで [Edit] をクリックして、変更を加えます。

- [Select Site from the hierarchy]
- [Select Access Points]
- [Modify AP Name]
- [Select AP Parameters]
- [Select 802.11 a/n/ac/ax Parameters]
- [Select 802.11 b/g/n/ax Parameters]

ステップ 15 [Next] をクリックします。

ステップ 16 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。

ステップ 17 すぐにプロビジョニングする場合は、[Now] オプションボタンをクリックして、[Next] をクリックします。後でプロビジョニングする場合は、[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。

ステップ 18 [Track Provision Status] 画面で、[AP Configuration Provision] ステータスを確認できます。

デバイスの交換ワークフロー

このワークフローでは、故障したデバイスを交換するための詳細な手順が示されます。

（注） [Inventory] ページから故障したデバイスを交換することもできます。詳細については、故障したデバイスの交換 （93 ページ）を参照してください。

始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

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]** > **[Replace Device]** の順に選択します。

ステップ 2 [Let's Do it] 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。

ステップ 3 [Choose Device Type] 画面で、交換する故障したデバイスのタイプを選択し、[Next] をクリックします。

ステップ 4 [Choose Site] 画面で、故障したデバイスがあるサイトを選択し、[Next] をクリックします。

ステップ 5 [Choose Faulty Device] 画面で、交換する故障したデバイスを 1 つ選択し、[Next] をクリックします。

ステップ 6 [Choose Faulty Device] 画面で故障したデバイスが見つからない場合は、次の手順を実行します。

a) [Add Faulty Device] をクリックします。
b) 故障したデバイスを選択し、[Next] をクリックします。
c) [Mark For Replacement] ウィンドウで、[Mark] をクリックします。
d) [Next] をクリックします。

ステップ 7 [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

ステップ 8 （任意） 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。

a) [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
b) [Add New Device] ウィンドウで、デバイスの**シリアル番号**を入力し、[Add New Device] をクリックします。

または

a) [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。

b) [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。

ステップ 9 [Next] をクリックします。

ステップ 10 [Schedule Replace] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時間でのデバイスの交換をスケジュールします。

交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時間でのデバイスの交換をスケジュールすることは可能です。

ステップ 11 [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。

ステップ 12 [Next] をクリックして [Summary] ページで詳細情報を確認します。

ステップ 13 [Summary] ページで、次の手順を実行します。

a) （任意） 前の手順で選択したデバイスタイプ、故障したデバイス、および交換用デバイスを変更する場合は、[Edit] をクリックします。

b) （任意） [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。

c) [置換（Replace）] をクリックします。

ステップ 14 [Click Monitor Replacement Status] をクリックして [Provision] ページの [Mark for Replacement] ビューに移動します。

ステップ 15 交換用デバイスの [Replace Status] をクリックすると、次のように RMA ワークフローの進捗状況が表示されます。

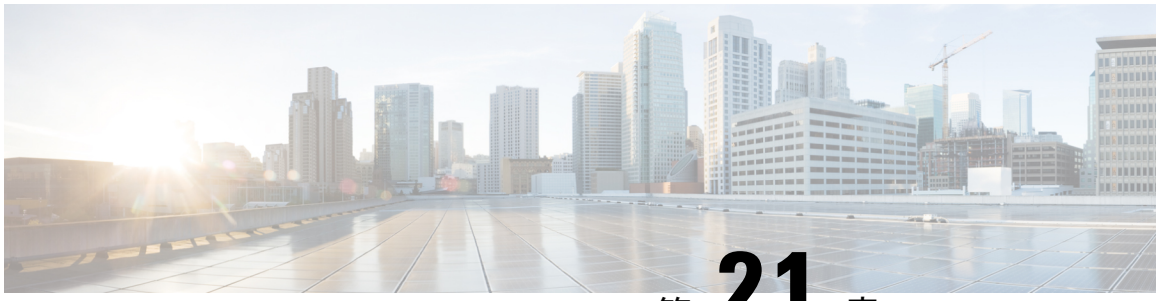
- （PnP）交換用デバイスを請求します。
- 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
- ライセンスを展開する。
- VLAN 構成をプロビジョニングします。
- スタートアップ構成をプロビジョニングします。
- 交換用デバイスをリロードします。
- 交換用デバイスの到達可能性を確認します。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- 交換用デバイスを同期します。
- 故障したデバイスを CSSM から削除します。
- 交換用デバイスを CSSM に追加します。
- PKI 証明書を失効化して作成します。
- Cisco ISE を更新します。
- 障害のあるデバイスを削除します。

ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

ステップ 16 エラーメッセージが表示された場合は、エラーリンクをクリックします。

ステップ 17 [Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

（注） [Main Inventory] ページには、障害のあるデバイスと交換した新しいデバイスの詳細が表示されます。



第 21 章

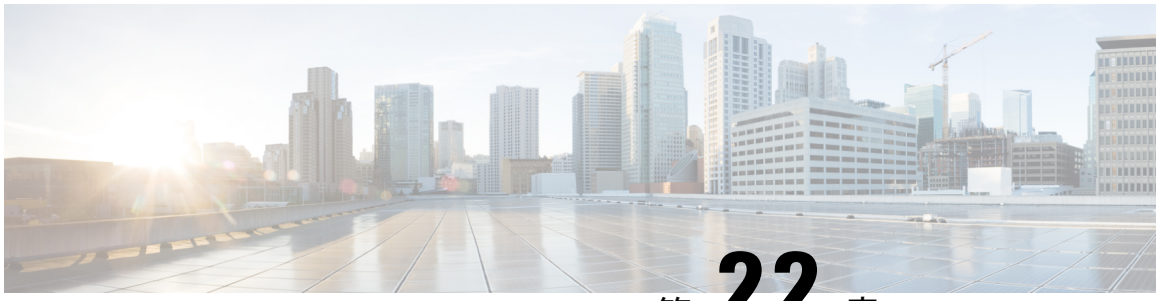
Cisco DNA アシュアランス

Cisco DNA アシュアランス

Cisco DNA アシュアランス は、Cisco DNA Center から入手可能なアプリケーションです。

ネットワークの正常性、クライアントの正常性、およびアプリケーションの正常性をモニターおよびトラブルシューティングする方法、および NetFlow の収集を有効にする方法など、アシュアランス アプリケーションの詳細については、Cisco DNA Assurance のユーザーガイドを参照してください。

Cisco DNA アシュアランス



第 22 章

データプラットフォームを使用した Cisco DNA Center のトラブルシューティング

データ プラットフォームについて

データ プラットフォームには、Cisco DNA Center アプリケーションのモニターとトラブルシューティングに役立つツールがあります。[Data Platform] には、ネットワークのパターン、トレンド、問題領域を特定するのに役立つ、さまざまな入力から合成されたデータが表示されます。たとえば、ネットワークに問題が発生した場合、パイプラインがエラー状態になっているかどうか、特定のエリアにおけるリアルタイム トラフィック フローが何かなど、問題に対する回答を迅速に得ることができます。データ プラットフォームの主なエリアは次のとおりです。

- [Analytics Ops Center]：データがコレクタとパイプラインを経由してどのように流れているかをグラフィカルに表示します。また、ネットワーク内のパターン、傾向、次のような問題領域を特定できる Grafana ダッシュ ボードも用意されています。分析 Ops センターを使用したトラブルシューティング （564 ページ）を参照してください。
- [Collectors]：さまざまなネットワークテレメトリとコンテキストデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。コレクタの設定情報の表示または更新 （566 ページ）を参照してください。
- [Store Settings]：アプリケーションのデータの保存期間を指定できます。データ保持設定の表示 （567 ページ）を参照してください。
- [Pipelines]：Cisco DNA Center アプリケーションが、ストリーミングデータを処理できるようにします。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル

化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。『パイプライン ステータスの表示 （567 ページ）』を参照してください。

分析 Ops センターを使用したトラブルシューティング

分析 Ops センターは、データがコレクタとパイプラインを経由してどのように流れているかに関するグラフィカル表示を提供します。また、ネットワーク内のパターン、傾向、次のような問題領域を特定するために役立つ Grafana ダッシュ ボードを提供します。

- アシュアランス の見つからないデータ。
- 不正確な正常性スコア。
- デバイスがインベントリではモニター対象として表示され、アシュアランスではモニター対象外として表示される。

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

ステップ 2 [Analytics Ops Center] をクリックします。
アプリケーションのリストが表示されます。

ステップ 3 メトリックを表示するアプリケーション名、たとえば、[Assurance] をクリックします。

アプリケーション内のすべての既存のコレクタとパイプラインのグラフィカル表示が現れます。また、各パイプラインに対応する CPU またはスループット値も提供されます。

各コンポーネントの現在のヘルス ステータスは、色によって示されます。

- 赤色：エラー
- 黄色：警告
- 灰色：通常動作

ステップ 4 パイプラインの履歴データを表示するには、[Timeline & Events] をクリックします。

時間間隔のデータを提供するタイムライン バーが表示されます。次のことも実行できます。

- スライダを移動して、特定の時間のデータを表示する
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- イベントをクリックして、その特定の時点での分析 Ops センターの可視化を表示する

ステップ 5 問題のトラブルシューティングに役立つ追加の詳細を表示し、エラーまたは警告の原因を特定するには、コレクタ名をクリックします。

スライドインペインに次のタブが表示されます。

- [Metrics]：直近 30 分間に収集された使用可能なメトリックの選択肢が提示されます。コンポーネントのステータス、開始時間と停止時間、およびエラーの例外を示す概要情報が表示されます。別の時間間隔を選択することもできます。
- [Grafana]：より詳細にデバッグするために各コンポーネントに関連付けられているダッシュボードが表示されます。

ステップ 6 データが特定のパイプラインを経由して流れているかどうかを表示するには、パイプラインストリームをクリックします。

スライドインペインが表示され、内部にグラフが表示されます。グラフは、アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示します。グラフの情報は、スライドインペインでドロップダウンリストから選択する時間間隔に基づきます。オプションは、[Last 30 Min]、[Last Hour]、[Last 2 Hours]、および [Last 6 Hours] です。デフォルトは、[Last 30 Min] です。

ステップ 7 パイプラインが通常レベルで流れていない場合は、カーソルをストリームに合わせると、遅延メトリックが表示されます。

ステップ 8 特定のパイプラインの詳細情報を表示するには、パイプライン名をクリックします。

適切な [Pipeline] ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

ステップ 9 [Analytics Ops Center] ページに表示されるメトリックを変更するには、[Key Metrics] をクリックして、最大 2 つのメトリックを選択し、[Apply] をクリックします。

デフォルトでは、Cisco DNA Center は CPU とスループットのメトリックを表示します。

ステップ 10 特定のフローのメトリックを表示するには、次を実行します。

a) [View Flow Details] をクリックします。
b) コンポーネントの左上隅にあるチルダ（～）をクリックして、3つの接続されたコンポーネント（コレクタ、パイプライン、ストア）を選択します。
c) [View Flow] をクリックします。
Cisco DNA Center は、その特定のフローに関連付けられたメトリックを表示します。

コレクタの設定情報の表示または更新

コレクタは、さまざまなネットワークテレメトリおよびコンテクスチュアルデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。

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

ステップ 2 [コレクタ（Collectors）] をクリックします。各コレクタの横にある色付きの点は、全体的なステータスを示しています。

ステップ 3 追加の詳細を表示するには、コレクタ名をクリックします。

適切な *[コレクタ（Collector）]* ページが表示されます。デフォルトでは、Cisco DNA Center に **[設定（Configuration）]** タブが表示され、現在の設定リストを確認できます。

ステップ 4 構成を表示、更新、または削除するには、特定の構成名をクリックします。

ステップ 5 新規の設定を追加するには、**[Configuration]** タブで **[+ Add]** をクリックします。

スライドインペインが表示されます。

ステップ 6 設定に必要な情報をスライドインペインに入力します。

ステップ 7 （任意） **[Anonymize]** チェックボックスをオンにすると、**[WIRELESSCOLLECTOR]** などの一部コレクタのデータを匿名化できます。

（注） [Anonymize] チェックボックスをオンにすると、**[Client Health]** ウィンドウに表示されるホスト名とユーザ ID は、復号化できない一方向ハッシュを用いてスクランブル処理されます。

重要 データを匿名化する場合は、**[ディスカバリ（Discovery）]** ツールを使用してデバイスを検出する前に、**[匿名化（Anonymize）]** チェックボックスをオンにしてください。デバイスを検出した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 8 [Save Configuration] をクリックします。

ステップ 9 設定されているインスタンスを表示するには、[インスタンス（Instances）] タブをクリックします。

ステップ 10 概要情報とメトリックを表示するには、リストからインスタンスを選択します。

ステップ 11 （任意） Cisco DNA Center を Cisco Connected Mobile Experience（CMX）と統合する場合は、CMX 側でデータの匿名化を選択できます。次の手順を実行します。

a) SSH クライアントを使用して、cmxadmin CLI ユーザとして Cisco CMX にログインします。

b) ルートユーザに変更します。

c) `/opt/cmx/etc/node.conf` に移動し、`[location]` の下に **`user_options`** を追加します。次に例を示します。

```
[location]
…
user_options=-Dhideusername=true
```

d) Cisco CMX CLI で、次のコマンドを入力します。

```
cmxctl agent restart
cmxctl location restart
```

データ保持設定の表示

アプリケーションのデータの保存期間を表示できます。

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

ステップ 2 [Store Settings] をクリックします。

ステップ 3 完了した履歴消去ジョブのリストを表示するには、[Data Purge Schedule] をクリックします。

[HISTORY] テーブルには、消去ジョブの名前、結果、時刻、その他のデータが表示されます。テーブル内のデータをソート、フィルタリング、エクスポートすることができます。

ステップ 4 現在のデータの保持または消去の設定を表示するには、[Data Retention & Purge Configuration] をクリックします。次の出力が表示されます。

- [Document Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのデータの設定。
- [Metric Graph Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのグラフィカルデータの設定。

パイプライン ステータスの表示

データ パイプラインによって、Cisco DNA Center アプリケーションは、ストリーミング データを処理できます。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。

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

ステップ 2 [Pipelines] をクリックします。

ステップ 3 アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示するには、パイプライン名をクリックします。

適切な [Pipeline] ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

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。