



Cisco DNA Center 1.3.3 SD-Access ワイヤレス設計および 導入ガイド

SD-Access.....	2
SD-Access ワイヤレス	3
SD-Access ワイヤレスアーキテクチャ	5
Cisco DNA Center を使用した SD-Access ワイヤレスのセットアップ.....	15
SD-Access の設計	32
SD-Access のポリシー	42
SD-Access オーバーレイのプロビジョニング	48
SD-Access ワイヤレス：内部の仕組み	85
SD-Access のワイヤレス統合の設計	89
SD-Access ワイヤレスゲストアクセス設計	99
SD-Access ワイヤレスでのマルチキャスト	100
SD-Access ワイヤレスのハイアベイラビリティ	104
付録：SD-Access ワイヤレス機能の詳細情報.....	108

改訂日：2020年3月13日

エグゼクティブサマリー

デジタル化は、あらゆる業界のビジネスを変革しています。その結果、すべての企業が IT 企業への転換を迫られています。調査によると、デジタルを使いこなす企業は収入を増やすだけでなく、平均で 29 % 以上も収益性を高めています（出典：Leading Digital）。この変革はきわめて重要で差し迫った事態です。というのも、企業の 40 % は淘汰される危険にさらされているからです（出典：Digital Vortex）。

Cisco Digital Network Architecture (Cisco DNA Center) は、以下の機能を提供する一連の設計原則に基づいて構築された、オープンなソフトウェア主導型アーキテクチャです。

- ビジネス革新の高速化を促進するインサイトとアクション
- ビジネスとユーザの期待に応えながら、コストと複雑さを低減する自動化とアシュアランス
- 組織の継続的な拡大や成長に伴うリスクを低減するセキュリティとコンプライアンス

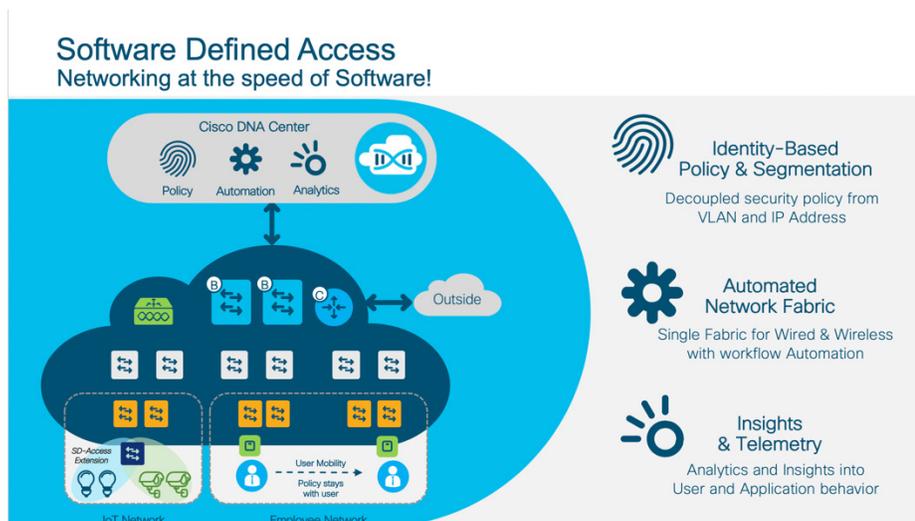
Cisco® Software-Defined Access (SD-Access) は Cisco DNA の重要な構成要素であり、シスコのお客様に、Cisco DNA の原則と利点を提供します。

SD-Access

SD-Access はシスコの次世代エンタープライズ ネットワーキング アクセス ソリューションであり、セキュリティ、セグメンテーション、および柔軟性の高いサービスロールアウトをファブリックベースのインフラストラクチャで統合できるように設計されています。優れた GUI エクスペリエンスが特長で、Cisco DNA Center アプリケーションによってネットワーク プロビジョニングを自動化します。構成、プロビジョニング、トラブルシューティングなどの日常的なタスクを自動化することで、ネットワークの適応時間を短縮し、問題解決を改善するとともに、セキュリティ侵害の影響を軽減します。これらの利点によって、ビジネスの CapEx および OpEx を大幅に節約できます。

図 1 は、SD-Access の利点をまとめたものです。

図 1. SD-Access の利点



このドキュメントでは、SD-Access のワイヤレス統合に重点を置いています。読者は SD-Access ファブリックの概念とこのネットワークアーキテクチャの主要コンポーネントに精通していることが想定されています。

SD-Access 機能の詳細については、SD-Access サイト (https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/software-defined-access/index.html) および『SD-Access 設計ガイド』(シスコ検証済みデザイン (CVD)) を参照してください。

SD-Access ワイヤレス

SD-Access ワイヤレスは、ファブリックおよび Cisco DNA Center による自動化の利点をすべて得ることを目的に、SD-Access アーキテクチャにワイヤレスアクセスを統合します。

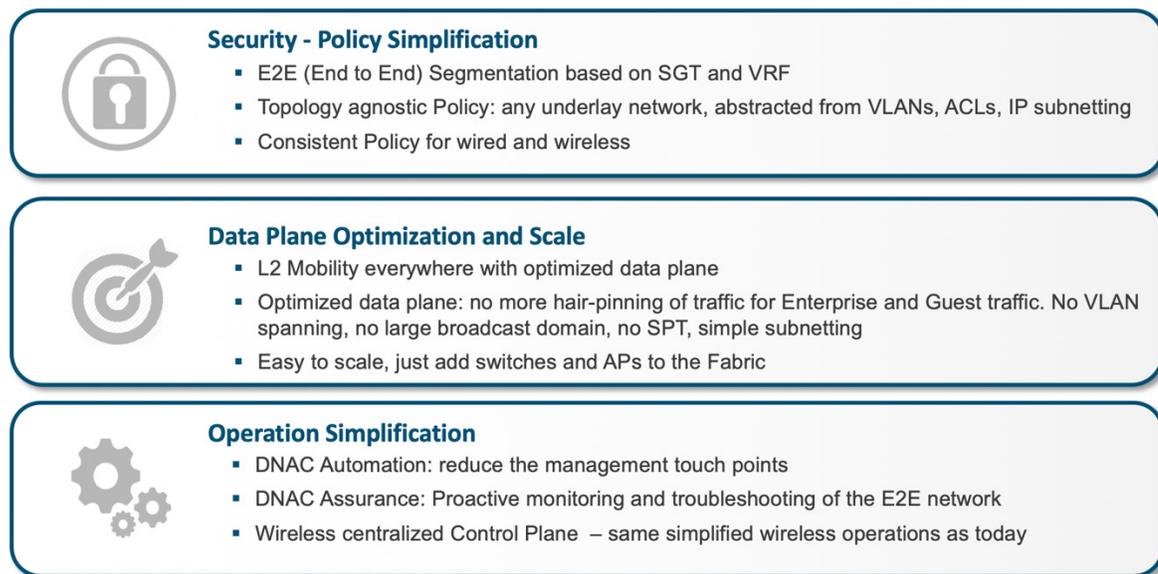
SD-Access ワイヤレスの利点には次のようなものがあります。

- **集中管理型ワイヤレス コントロールプレーン**：Cisco Unified Wireless Network 導入環境で提供されている革新的な RF 機能が、SD-Access ワイヤレスでも活用されます。IT 導入を簡素化させる無線リソース管理 (RRM)、クライアント オンボーディング、クライアントモビリティなどに関して、ワイヤレスの運用は Cisco Unified Wireless Network の場合と同じです。
- **分散型データプレーンの最適化**：データプレーンは、トラフィックの分散に通常伴う処理 (VLAN のスパンニング、サブネット化、大規模なブロードキャストドメインなど) なしに最適なパフォーマンスと拡張性を実現するために、エッジスイッチに分散されます。
- **場所を問わないシームレスなレイヤ 2 ローミング**：SD-Access ファブリックにより、クライアントは同じ IP アドレスを保持しながらキャンパス全体でシームレスにローミングできます。
- **ゲストおよびモビリティのトンネリングの簡素化**：アンカー ワイヤレス コントローラ (WLC) が不要になり、フォーリンコントローラをホッピングせずにゲストトラフィックをネットワークエッジ (DMZ) に直接送信できます。
- **ポリシーの簡素化**：SD-Access では、ポリシーとネットワークの構成体 (IP アドレスや VLAN) との間の依存関係が解消されるため、有線クライアントとワイヤレスクライアントのポリシーを定義および実装する方法がシンプルになります。
- **セグメンテーションの簡略化**：セグメンテーションはファブリック内をエンドツーエンドで伝達され、仮想ネットワーク ID (VNI) とスケーラブルグループタグ (SGT) に基づいて階層化されます。有線とワイヤレスの両方のユーザに同じセグメンテーションポリシーが適用されます。

次の事項を維持しながらこれらすべての利点を獲得できます。

- 将来に備えた Wi-Fi 6 アクセスポイント (AP)、802.11 Wave 1、802.11ac Wave 2 AP、Cisco 3504、5520、8540、C9800-40、C9800-80、C9800-CL、および EWC (Catalyst 9300、9400、9500 で実行されている 9800 ソフトウェア) を含む**最高クラスのワイヤレス**。
- 既存の AireOS WLC をサポートし、**投資を保護する**。SD-Access ワイヤレスは 802.11ac Wave 2 AP に最適化されていますが、Wave 1 AP もサポートしています。

図 2. SD-Access ワイヤレスの利点



SD-Access のワイヤレス統合

SD-Access ファブリックに基づく有線ネットワークを使用しているお客様には、ワイヤレスアクセスを統合するための2つのオプションがあります。

- SD-Access ワイヤレス アーキテクチャ
- Cisco Unified Wireless Network ワイヤレスオーバーザトップ (OTT)

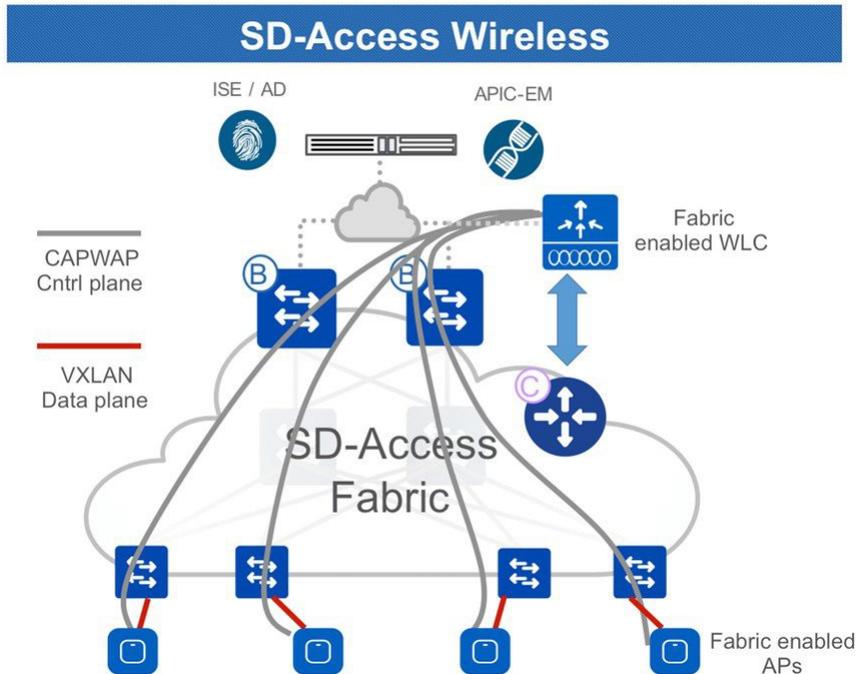
SD-Access ワイヤレスオプションは、ワイヤレスユーザとモノのためにファブリックの利点を最大限に活用しているため、最初に検討してみましょう。最初にアーキテクチャと主要なコンポーネントを紹介し、その後、Cisco DNA Center を使用して SD-Access ワイヤレスネットワークを設定する方法を説明します。

OTT は基本的に、ファブリック有線ネットワーク上で従来のワイヤレスを実行します。このオプションについては、設計上の考慮事項を含め後に本書で説明でされます。

SD-Access ワイヤレスアーキテクチャ

図 3 は、全体的な SD-Access ワイヤレスアーキテクチャを示しています。

図 3. SD-Access ワイヤレスアーキテクチャ

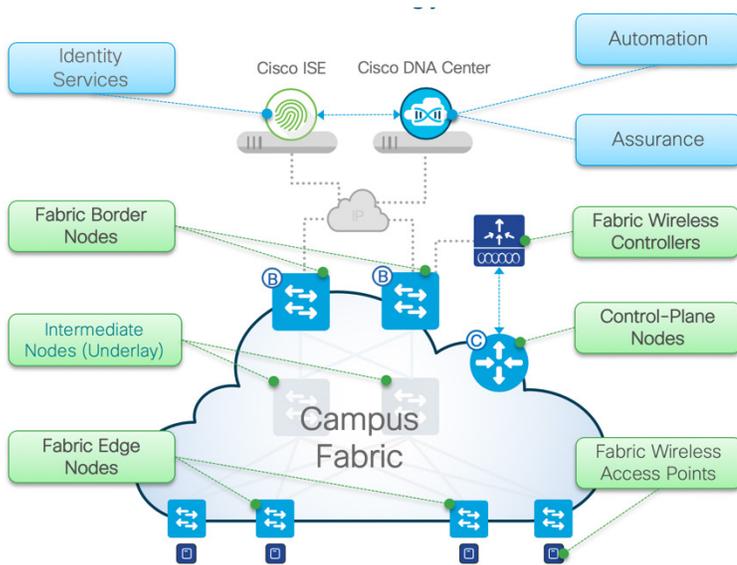


SD-Access ワイヤレスでは、コントロールプレーンが集中管理されます。つまり、Cisco Unified Wireless Network と同様に、AP と WLC の間で Control and Provisioning of Wireless Access Points (CAPWAP) トンネルが維持されます。主な違いは、SD-Access ワイヤレスではデータプレーンはファブリック対応 AP から直接 Virtual Extensible LAN (VXLAN) を使用して分散されることです。WLC と AP は、ファブリックに統合されて、AP は、「特別な」クライアントとしてファブリックオーバーレイ (エンドポイント ID スペース) ネットワークに接続されます。

SD-Access ワイヤレスアーキテクチャのコンポーネント

図 4 は、SD-Access ワイヤレスアーキテクチャの主要なコンポーネントを示しています。これらのコンポーネントの説明を以下に示します。

図 4. SD-Access ワイヤレスアーキテクチャのコンポーネント



- **Network Automation** - Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** - Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** - NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** - Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** - A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** - A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** - A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

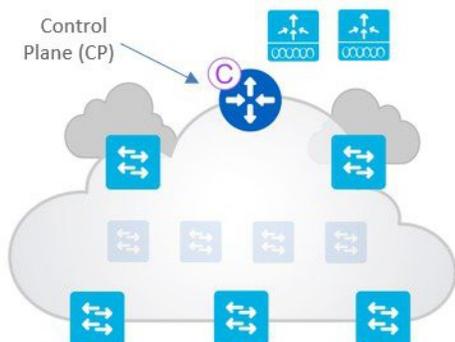
- **コントロールプレーン (CP) ノード** : エンドポイント ID とデバイス間の関係を管理するホストデータベース。
- **ファブリックボーダー (FB) ノード** : 外部レイヤ 3 ネットワークを SD-Access ファブリックに接続するファブリックデバイス (コアやディストリビューションスイッチなど)。
- **ファブリックエッジ (FE) ノード** : 有線エンドポイントを SD-Access ファブリックに接続するファブリックデバイス (アクセススイッチなど)。
- **ファブリック WLC** : ファブリック対応のワイヤレスコントローラ。
- **ファブリック AP** : ファブリック対応のアクセスポイント。
- **Cisco DNA Center** : エンタープライズ ネットワークの自動化およびアシュアランスを一元管理できるソリューション。Cisco DNA Center は、エンタープライズ ソフトウェア定義型ネットワーク (SDN) コントローラ、ポリシーエンジン (Cisco Identity Services Engine (ISE))、および分析エンジン (Cisco ネットワーク データ プラットフォーム (NDP)) を統合します。
- **ポリシーエンジン** : ユーザまたはデバイスをグループに動的にマッピングし、ポリシーを定義する外部 ID サービス (ISE など)。
- **アシュアランスエンジン** : ユーザまたはデバイスからアプリケーションへのフローを分析し、ファブリックス テータスをモニタするデータコレクタ (NDP)。

次のセクションでは、SD-Access ワイヤレスアーキテクチャの主なコンポーネントの役割と機能について説明します。

コントロールプレーン ノード

ファブリック コントロール プレーン ノードは LISP マップサーバリゾルバに基づいており、ファブリックエンドポイント ID データベースを実行してオーバーレイ到達可能性情報を提供します。

図 5. コントロールプレーン ノード



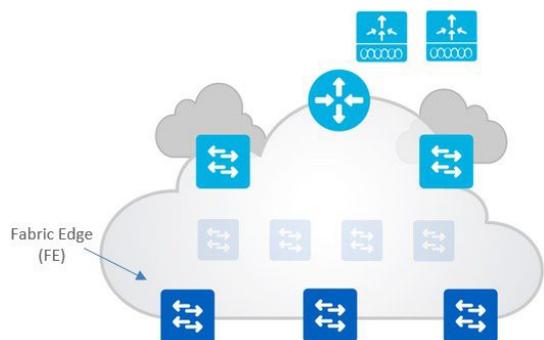
CP はホストデータベースであり、エンドポイント ID (EID) とその他の属性をエッジノードバインドまで追跡します。次の処理を実行します。

- 複数のタイプの EID ルックアップキー (IPv4/32、IPv6/128*、または MAC アドレス) をサポートします。
- エッジノード、有線ローカルエンドポイントのファブリック WLC とワイヤレスクライアントそれぞれからプレフィックス登録を受信します。
- リモートエッジノードからのルックアップ要求を解決し、エンドポイントを特定します。
- ファブリックエッジノード、ワイヤレスクライアント モビリティを設定したボーダーノードおよびルーティングロケータ (RLOC) 情報を更新します。

ファブリックエッジノード

ファブリックエッジは、ファブリックに接続されたユーザとデバイスの接続を行います。

図 6. ファブリックエッジノード



ファブリックエッジは次の処理を実行します。

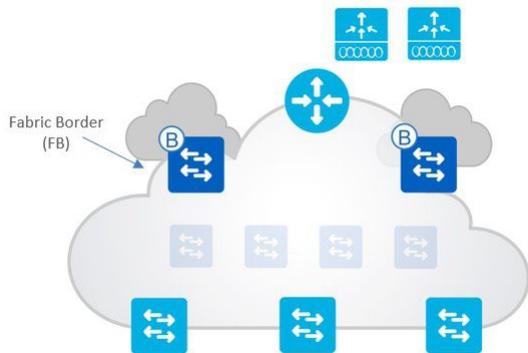
- 有線エンドポイントの識別と認証を行います。
- コントロールプレーンノードにワイヤレス IPv4 または IPv6 エンドポイント ID 情報を登録します。
- 接続されたエンドポイントにエニーキャストレイヤ 3 ゲートウェイを提供します。
- ワイヤレスクライアントに仮想ネットワーク (VN) サービスを提供します。

- AP をファブリックにオンボーディングし、AP に VXLAN トンネルを構成します。
- ゲストボーダーおよびゲスト コントロール プレーン ノードと通信するワイヤレスホストにゲスト機能を提供します。

ファブリックボーダーノード

ファブリックに出入りするすべてのトラフィックは、ファブリックボーダーノードを経由します。

図 7. ファブリックボーダーノード



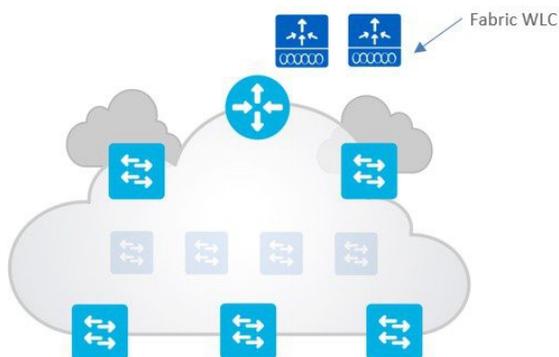
- ファブリックボーダーノードには、ボーダーノードとデフォルトボーダーノードの 2 種類があります。どちらのタイプも、ファブリックオーバーレイに出入りするすべてのデータトラフィック、および VN やグループベースのポリシー適用（ファブリック外のトラフィックに対して）に対して、基本的なルーティング エントリ ポイントと出口ポイントを提供します。
- ファブリックボーダーを使用して、「既知の」IP またはマスキュートをマップシステムに追加します。既知のルートとは、ファブリックエッジノード（リモート WLC、共有サービス、データセンター、ブランチ、プライベートクラウドなど）にアドバタイズする任意の IP またはマスクのことです。
- デフォルトボーダーは、ラストリゾートゲートウェイとして「不明」ルート（インターネットやパブリッククラウドなど）に使用されます。
- ボーダーは、ファブリックドメインと非ファブリックドメインがエンドポイントの到達可能性とポリシー情報を交換する場所です。
- ボーダーは、ドメイン間でコンテキスト（Virtual Route Forwarding (VRF) および SGT）の変換を行います。

ファブリック対応 WLC

- ファブリック対応 WLC は LISP コントロールプレーンに統合されます。

ワイヤレス機能については、コントロールプレーンは WLC で集中管理されます。

図 8. ファブリック対応 WLC



- WLC は、AP イメージまたは設定、RRM、クライアントセッション管理およびローミング、その他すべての無線コントロールプレーン機能を引き続き提供します。
- ファブリック統合について
 - ワイヤレスについては、EID としてクライアント MAC アドレスが使用されます。
 - SGT および VNI を使用したクライアント MAC アドレスの登録のために、コントロールプレーンノードのホストトラッキング データベースと通信します。
 - VN 情報は、ファブリックエッジ上の VLAN にマッピングされます。
 - WLC はホストトラッキング データベースをワイヤレスクライアントのローミング情報で更新します。
- **ファブリック対応 WLC は AP と同じサイトに物理的に配置する必要があります**（初期リリースでは、WLC から WAN 経由で AP を展開することはサポートされていません）。

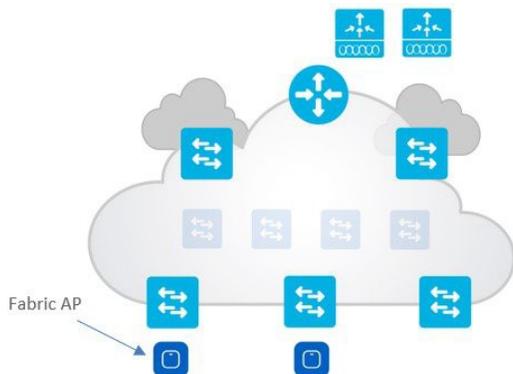


(注) WLC と AP の遅延は 20 ミリ秒以内である必要があります。これは通常、同じ物理サイトに配置されていることを意味します。

ファブリック AP

ファブリック AP では、ワイヤレスエッジに SD-Access データプレーンを拡張します。

図 9. ファブリック AP



- ファブリック AP はローカルモード AP であり、ファブリックエッジスイッチに**直接接続**する必要があります。
- CAPWAP コントロールプレーンは、トランスポートとしてファブリックを使用して WLC に移動します。
- ファブリックは、サービスセット識別子 (SSID) ごとに有効になります。
 - ファブリック対応 SSID の場合、AP は 802.11 トラフィックを 802.3 に変換し、クライアントの VNI および SGT 情報をエンコードする VXLAN にカプセル化します。
 - AP は、WLC によってプログラムされた転送テーブルに基づいてクライアントトラフィックを転送します。通常、VXLAN トンネルの宛先は最初のホップのスイッチになります。
 - ファブリック SSID 上のワイヤレスユーザの SGT および VRF ベースポリシーは、有線の場合と同様に、ファブリックエッジで適用されます。
- ファブリック対応 SSID の場合、カプセル化として VXLAN を利用し、AP にユーザデータプレーンが分散されます。
- AP は、SSID ポリシー、Application Visibility and Control (AVC)、Quality of Service (QoS) などのすべてのワイヤレス固有の機能を適用します。



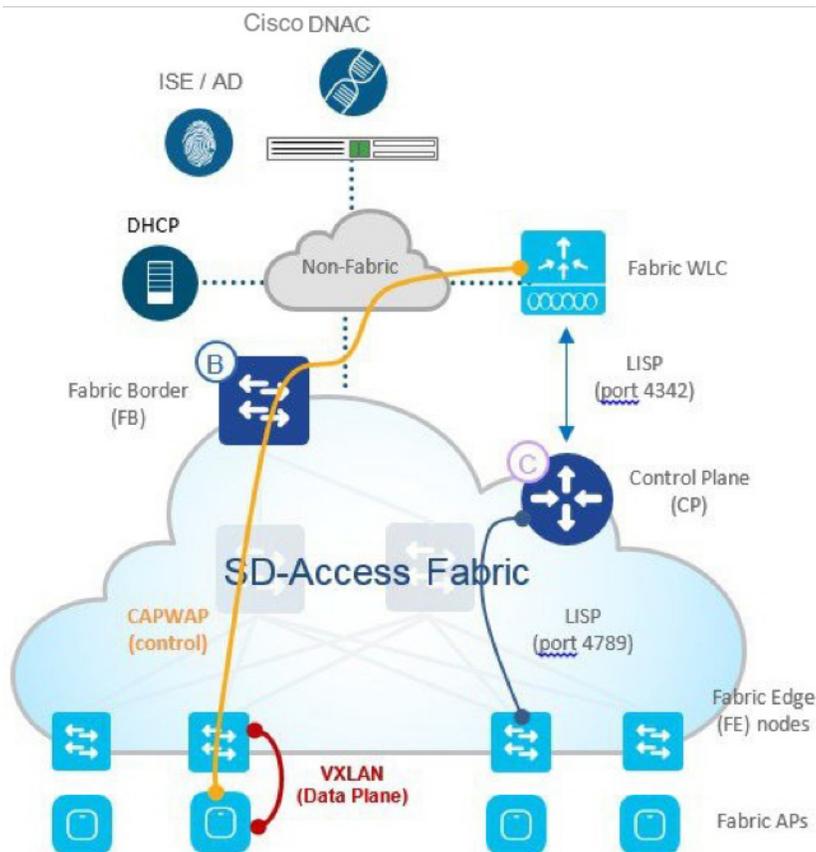
(注) AP 上の機能サポートについては、WLC リリースノートを参照してください。

AP は、サポートされているファブリック拡張ノードのいずれかにオプションで接続できます。サポートされているスイッチモデルについては、発注ガイド (<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739242.html>) を参照してください。

SD-Access ワイヤレスプロトコルと通信インターフェイス

図 10 は、SD-Access ワイヤレスで使用されるプロトコルとインターフェイスを示しています。

図 10. 異なるコンポーネント間の通信



- WLC と AP 間：コントロールプレーン WLC と AP 間の通信は、既存のモードと同様に CAPWAP を通じて行われます。
- AP とスイッチ間：データトラフィックは VXLAN トンネルカプセル化を使用して AP からエッジスイッチにスイッチングされます。UDP ポートは標準の 4789 です。
- WLC とコントロールプレーンノード間：WLC は、コントローラの TCP ポート 4342 上で実行されているコントロールプレーンと通信します。
- Cisco DNA Center と WLC 間：最初のリリースでは、Cisco DNA Center は SSH/Telnet を介してコマンドライン インターフェイス (CLI) を使用し、WLC を設定します。
- Catalyst 9800 プラットフォームでは、Cisco DNA Center は netconf-yang モデルを使用してデバイスの設定をプッシュおよびプロビジョニングします。netconf-yang の有効化については、以降の項で説明します。netconf は TCP ポート 830 を使用します。
- EWC (Catalyst 9300、9400 および 9500 で実行されている 9800 ソフトウェア) では、コントロールプレーンは Catalyst スイッチにあります。9800 ソフトウェアにコントロールプレーンと通信する LISP エージェントが存在します。
- スイッチとコントロールプレーンノード間：ファブリック対応スイッチは、TCP ポート 4789 のコントロールプレーンノードと通信します。

SD-Access ワイヤレスプラットフォームのサポート

SD-Access ワイヤレスアーキテクチャは次の WLC および AP でサポートされます。

Cisco 3504、5520、8540 シリーズ ワイヤレスコントローラ

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ (9800-40、9800-80、9800-L、9800-CL)

C9300、C9400、C9500 シリーズ スイッチの Cisco Catalyst 9800 組み込み型ワイヤレス

Wi-Fi 6 アクセスポイント : Cisco Catalyst 9115AX および Cisco Catalyst 9117AX

Wi-Fi 6 アクセスポイント : Cisco Catalyst 9120AX シリーズ

Wi-Fi 6 アクセスポイント : Cisco Catalyst 9130AX シリーズ

802.11 Wave 2 アクセスポイント : Cisco Aironet 1800、2800、3800 シリーズ

802.11 Wave 1 アクセスポイント : Cisco Aironet 1700、2700、3700 シリーズ

802.11 Wave 2 屋外アクセスポイント : Cisco Aironet 1540、1560

802.11 Wave 2 アクセスポイント : Cisco Aironet 4800 アクセスポイント

サポートされるデバイスとソフトウェアの最新情報については、SD-Access 互換性マトリックス

(<https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html>) を参照してください。

SD-Access ワイヤレスネットワーク展開

この項では、SD-Access ワイヤレスネットワークに WLC と AP を展開する際の重要な考慮事項について説明します。次の図を参照してください。

アクセスポイントは次のように展開する必要があります。

- ファブリックエッジ (または拡張ノードスイッチ) に直接接続されている
- ファブリックオーバーレイの一部である
- グローバルルーティングテーブルにマップされている INFRA_VN に属す
- ローカルモードで WLC に接続する

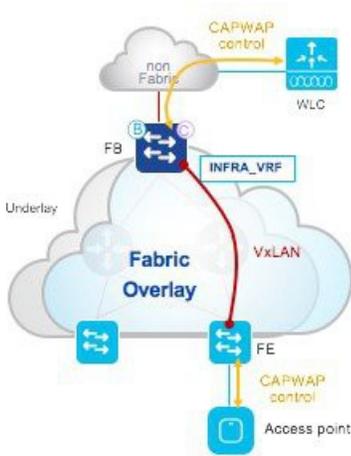
WLC は次のように展開する必要があります。

- ファブリックの外部に接続されている (必要に応じてボーダーに直接接続)
- グローバルルーティングテーブル内に存在する
- VRF 間リークは AP が WLC に接続する際に不要である
- 1つのコントロールプレーンノード (冗長性のために2つ) としか通信しないため、1つの WLC は1つのファブリックドメイン (FD) にしか属せない



- (注) ファブリック コントロール プレーン プロトコルに耐障害性を持たせるには、**各ファブリックノードのグローバルルーティングテーブルに WLC への特定のルートが存在することが重要です**。WLC の IP アドレスへのルートは、ボーダーでアンダーレイ内部ゲートウェイプロトコル (IGP) に再配布されるか、各ノードで静的に設定する必要があります。WLC は SD-Access 内の RLOC と見なされるため、LISP RLOC 到達可能性チェックの一環として、アンダーレイ上に WLC への特定のルートが必要です。つまり、WLC はデフォルト ルート経由で到達できません。

図 12. AP と WLC の展開



AP と WLC 間の通信

ネットワーク展開の観点からは、アクセスポイントはオーバーレイネットワークに接続され、WLC は従来の IP ネットワークの SD-Access ファブリックの外にあります。



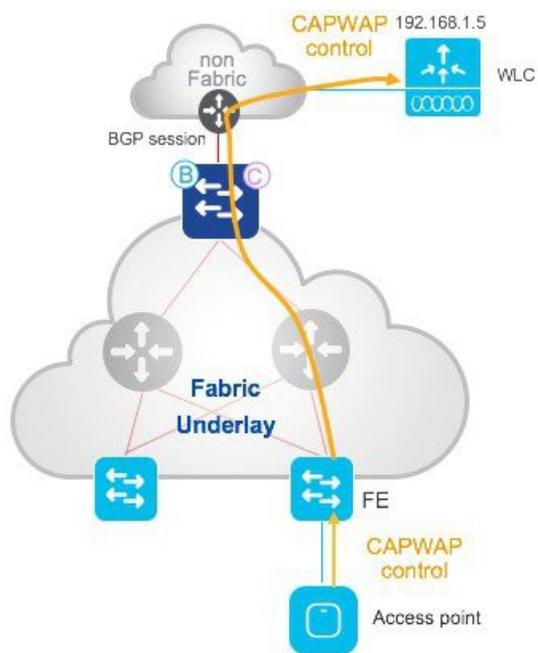
- (注) WLC が物理的にサイトに設置され、WAN を経由しないようにします。ファブリック AP はローカルモードにし、AP と WLC の間の遅延は 20 ミリ秒未満にする必要があります。

WLC サブネットは、アンダーレイにアダプタイズされるので、ネットワーク内のファブリックノード (ファブリックエッジおよびコントロールプレーン) はネイティブルーティングを実行して WLC に到達できます。オーバーレイの AP サブネットは外部ネットワークにアダプタイズされ、WLC はオーバーレイ経由で AP に到達できます。

ここで、CAPWAP トラフィックがファブリック対応 SSID の AP と WLC 間でどのように流れるかを少し詳しく見ていきましょう。これは、AP 接続操作専用のコントロールプレーントラフィックと他のすべてのコントロールプレーントラフィックです (クライアント データ プレーントラフィックは AP から VXLAN を使用してスイッチに配信されるため、WLC には送信されません)。

AP から WLC への南北方向の CAPWAP トラフィックを図 13 に示します。

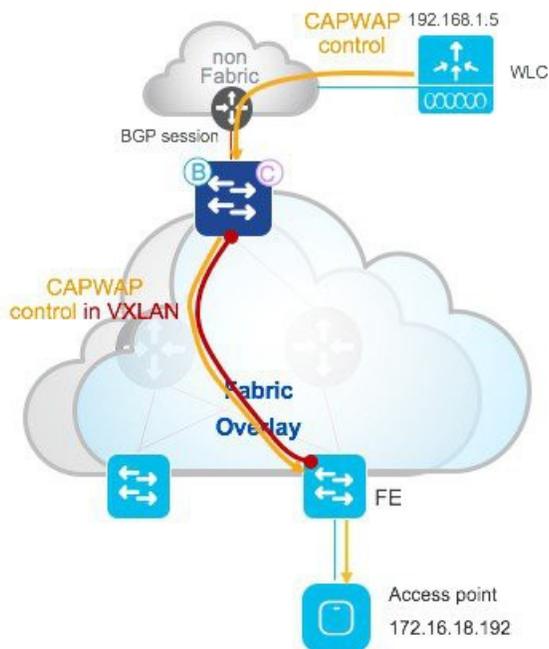
図 13. AP から WLC への南北方向の CAPWAP トラフィック



- ボーダー（内部または外部）は、アンダーレイ内の WLC ルートを（選択した IGP を使用して）再配布します。
- FE がグローバルルーティングテーブルでルートを学習します。
- FE が AP から CAPWAP パケットを受信すると、FE は RIB で一致を検出し、パケットは VXLAN カプセル化なしで転送されます。
- AP から WLC への CAPWAP トラフィックがアンダーレイで移動します。

WLC から AP への北南方向の CAPWAP トラフィックを図 14 に示します。

図 14. WLC から AP への北南方向の CAPWAP トラフィック



- AP サブネットは、オーバーレイの一部として、コントロールプレーンに登録されています。
- ボーダーは、AP のローカル EID スペースをコントロールプレーンからグローバル ルーティング テーブルにエクスポートし、AP ルートを LISP マップキャッシュエントリにインポートします。
- ボーダーは外部ドメインにローカル AP EID スペースをアドバタイズします。
- ボーダーは、WLC から CAPWAP パケットを受信すると、LISP ルックアップが行われ、トラフィックは VXLAN カプセル化を使用して FE に送信されます。
- WLC から AP への CAPWAP トラフィックがオーバーレイで移動します。



(注) AP から WLC までの CAPWAP トラフィックパスについて説明してきました。AP から発信された他のタイプのトラフィックにも同じパスが適用され、DHCP、DNS などのグローバル ルーティング テーブルで既知の宛先に送信されます。

Cisco DNA Center を使用した SD-Access ワイヤレスのセットアップ

この項では、Cisco DNA Center を使用して SD-Access でワイヤレス機能を設定するためのステップバイステップガイドを提供します。Cisco DNA Center では、SD-Access ソリューションの自動化、ポリシー、およびアシュアランスを一元管理できます。

SD-Access ワイヤレスをセットアップするための前提条件の 1 つとして、Cisco DNA Center がインストールされている必要があります。ワイヤレス LAN コントローラ (WLC) は、Cisco DNA Center でサポートされているイメージとともにインストールする必要があります。

以降の項のワークフローとスクリーンショットは、Cisco DNA Center 1.3.3 のものです。

Identity Service Engine (ISE) をインストールし、少なくともプライマリ PAN、PSN、MNT のペルソナを準備する必要があります。必要な規模をサポートする分散モデルに対応するには、後述の ISE 導入ガイドを参照してください。Identity Service Engine (ISE) では、PxGRID および ERS API サービスが実行されている必要があります。

SDA の互換性のあるソフトウェアに関する推奨事項の詳細については、下記の互換性マトリックスガイドを参照してください。

[SD-Access 互換性ガイド](#)

Cisco DNA Center のインストールおよびアップグレードプロセスについては、次のリンクの手順に従ってください。

[Cisco DNA Center インストールガイド](#)

Cisco ワイヤレス LAN コントローラ (WLC) をインストールして設定し、初期設定を完了します。Aire-OS または Catalyst 9800 プラットフォームについては、以下の手順を参照してください。

[Cisco Aire-OS 8540 導入ガイド](#)

[Cisco Aire-OS 5520 導入ガイド](#)

[Cisco Catalyst 9800 導入ガイド](#)

[Identity Services Engine \(ISE\) のインストールガイド](#)

9800 組み込みワイヤレス LAN コントローラ (EWC)

Catalyst 9k スイッチに組み込みワイヤレスコントローラをインストールするための前提条件の 1 つとして、netconf が有効になっている必要があります。Cisco DNA Center はデバイスで netconf を有効にします。netconf は、Cisco DNA Center がデバイスに設定をプロビジョニングするために使用する方法の 1 つです。

以下の項では、Cisco DNA Center を使用して netconf を有効にしない場合に、Catalyst 9k スイッチで netconf を手動で有効にするために必要な手順について説明します。Cisco DNA Center でデバイスに netconf をプロビジョニングするには、ディスカバリプロセス中にログイン情報の 1 つとして netconf が選択されていることを確認します。ワイヤレスパッケージをインストールするには、Catalyst スイッチをインストールモードで実行する必要があります。ワイヤレスパッケージのバージョンは、スイッチングプラットフォームで実行されている Cisco IOS-XE のバージョンと同じである必要があります。

Catalyst 9k スイッチが 16.11.1c で実行されている場合、9800-SW パッケージは同じバージョン (16.11.1) である必要があります。ワイヤレスパッケージを適切にインストールするには、スイッチで DNA-Advantage ライセンスがアクティブになっている必要があります。これは show version コマンドで確認できます。アクティブでない場合は、通常のライセンスコマンドを使用して評価版をアクティブ化できます。

Catalyst 9k ファミリのワイヤレスパッケージのソフトウェアは、Cisco.com のスイッチング製品ファミリにあります。

イメージは特別リリースとしても掲載されており、SDA 互換性マトリックスを介して特別リリースの参照でイメージを取得できます。



Cisco Catalyst 9800 Embedded Wireless on C9300, C9400, C9500 Series Switch	IOS XE 16.12.2t , IOS XE 16.12.1s, IOS XE 16.11.1c	IOS XE 17.1.1s IOS XE 16.12.2t , IOS XE 16.12.1s, IOS XE 16.11.1c
--	---	---

EWC は現在、SD-Access 展開でのみサポートされています。Cisco DNA Center は、Catalyst 9k スイッチでのワイヤレスパッケージのプロビジョニングとインストールに使用されます。

ステップ 1 DNA-Advantage ライセンスが有効になっていることを確認します。

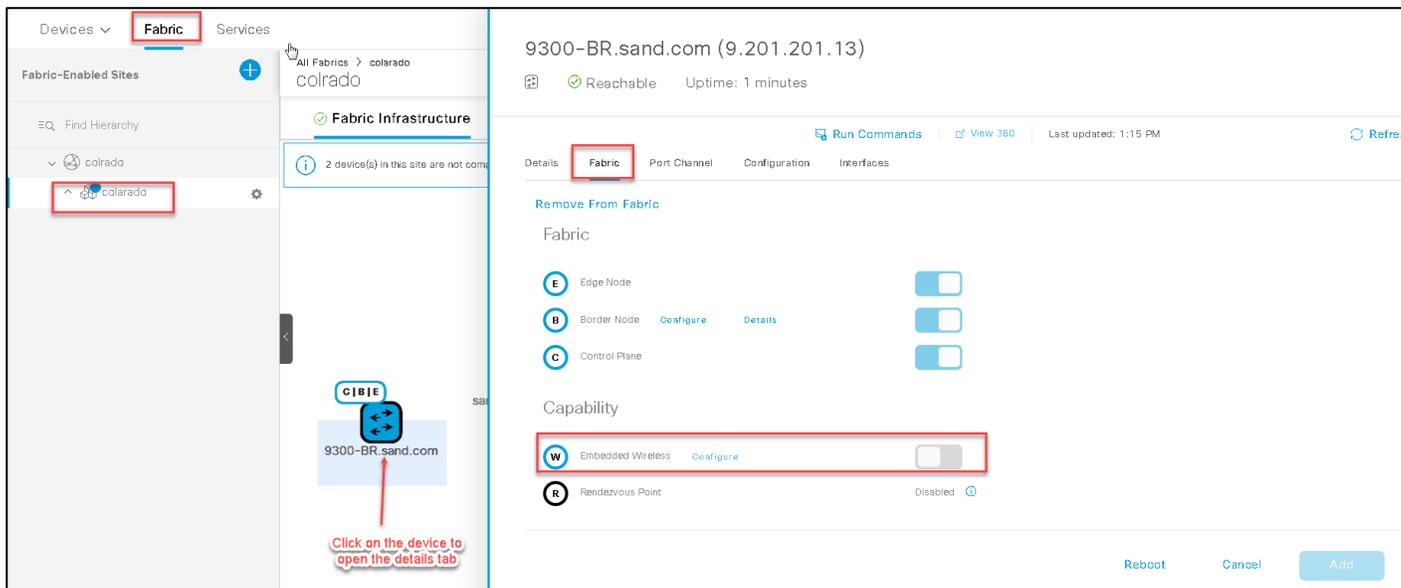
```
Switch#show version | b Technology
Technology Package License Information:
-----
Technology-package           Technology-package
Current           Type           Next reboot
-----
network-advantage      Permanent      network-advantage
dna-advantage      Subscription      dna-advantage
```

ステップ 2 Catalyst スイッチで netconf を手動で有効にします。

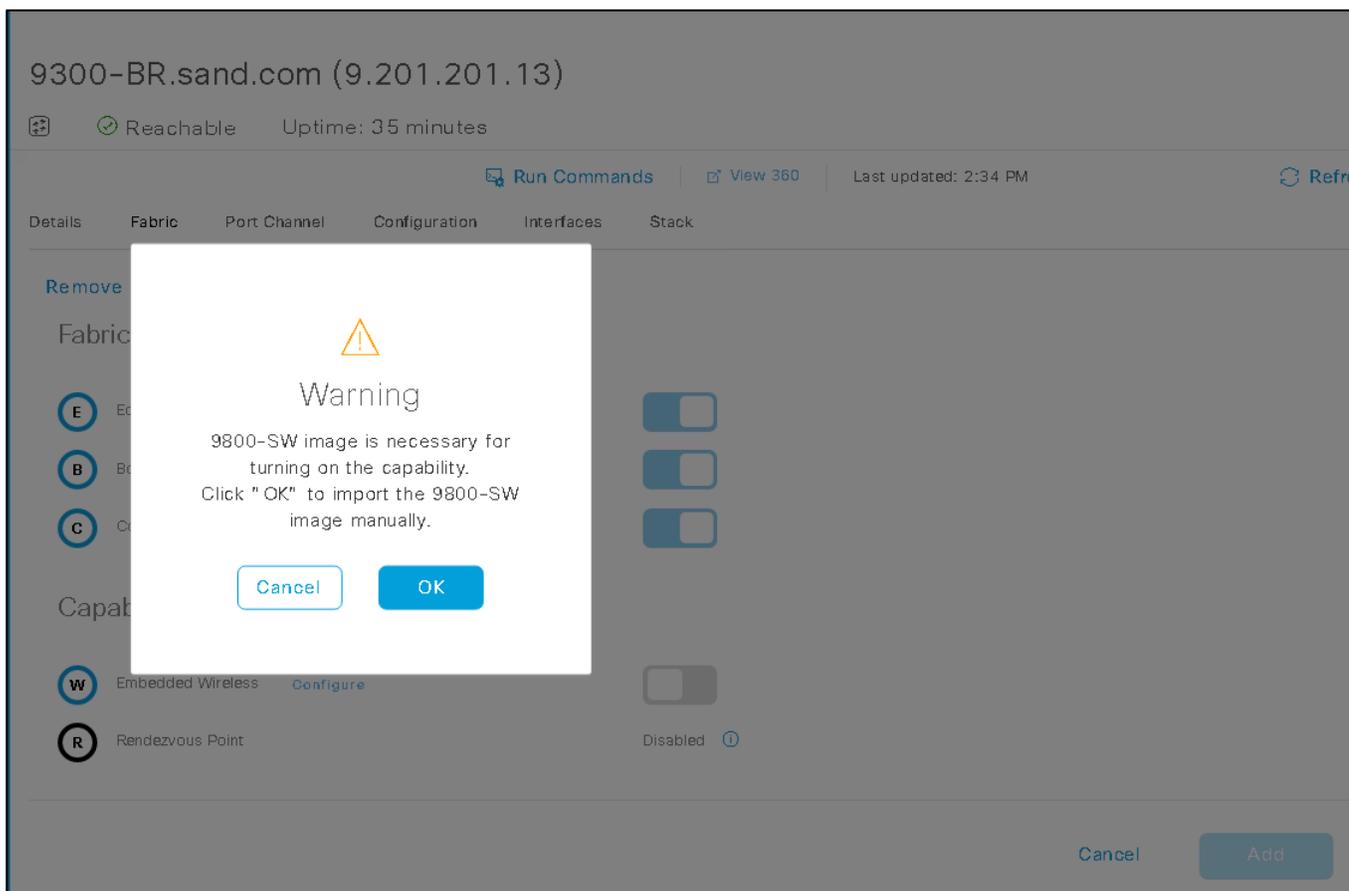
```
Switch# netconf-yang -> NETCONF/YANG をグローバルに有効にします。初期化に最大 90 秒かかることがあります。
Switch# aaa new-model
Switch# authorization exec default local -> NETCONF-SSH 接続と edit-config 操作に必要

Switch#show netconf-yang status
netconf-yang: enabled -> netconf ステータス
netconf-yang ssh port: 830-> Cisco DNA Center がデバイスに接続するためのポート
netconf-yang candidate-datastore: disabled
```

ステップ 3 デバイスが検出されてファブリックに追加されたら、Catalyst 9k スイッチで 9800-SW を有効にする必要があります。ワイヤレスコントローラ機能を有効にするには、デバイスをクリックしてデバイスの詳細ページを開きます。詳細ページで、管理者はデバイスでサポートされている機能を確認できます。サポートされている機能の 1 つに [Embedded Wireless] があります。スライダーを移動してオプションを有効にします。



ステップ4 組み込みワイヤレス機能を追加したら、次のプロセスでは、Cisco DNA Center の SWIM モジュールを使用してデバイスに 9800-SW イメージをインポートします。[OK] をクリックして SWIM プロセスを実行します。



ステップ5 イメージの場所を指定します。アクティブ化オプションを有効にして [Import] をクリックします。

9300-BR.sand.com

1 Download Image 2 Manage Scope 3 Advanced 4 Summary

Select an image from computer

Choose File C9800-SW-ios...2.01.SPA.bin

OR

Enter image URL

Activate image after import

Import

Cancel Back Next

9300-BR.sand.com

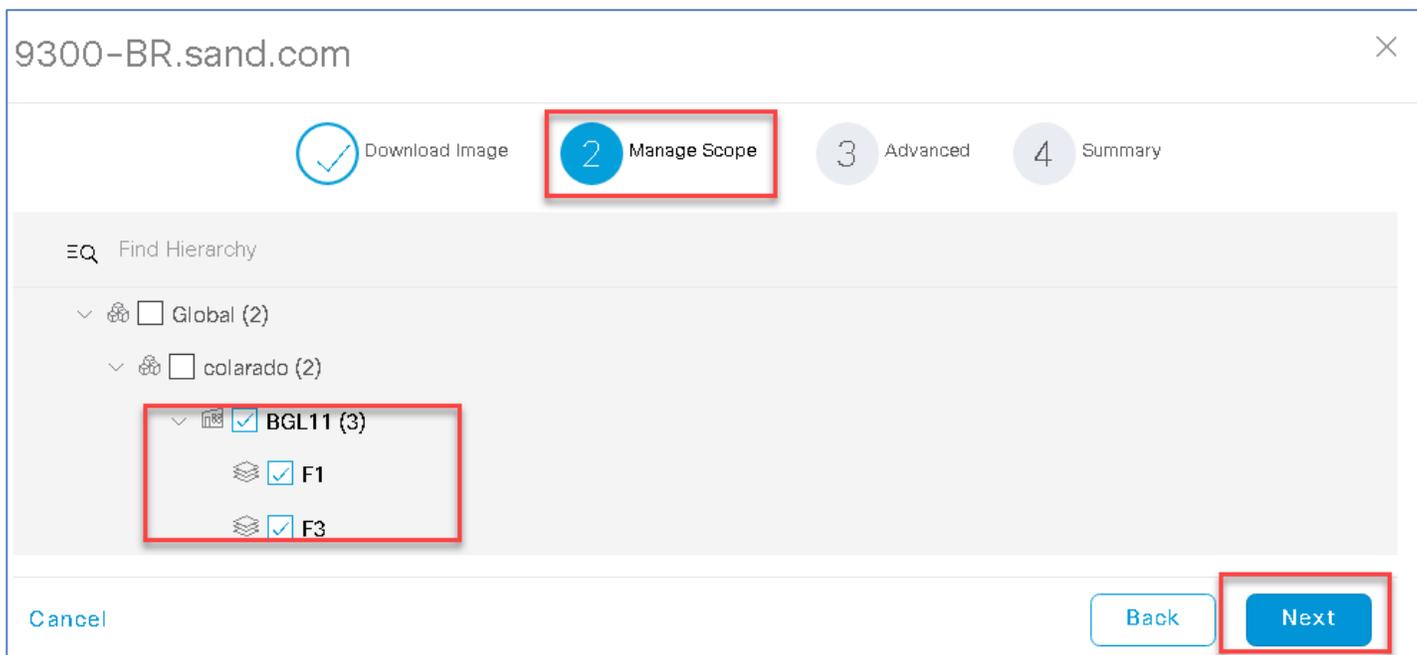
1 Download Image 2 Manage Scope 3 Advanced 4 Summary

Image imported successfully

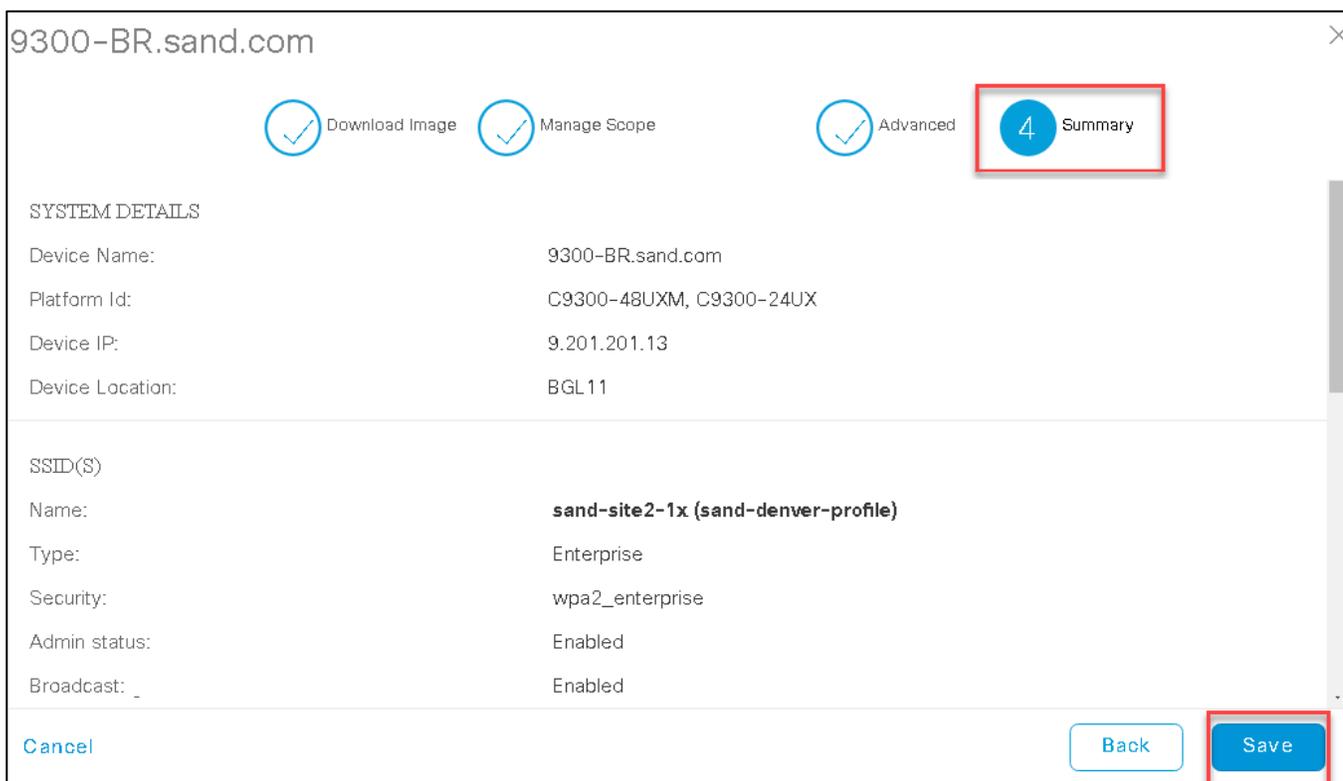
C9800 Image activated successfully

Cancel Back Next

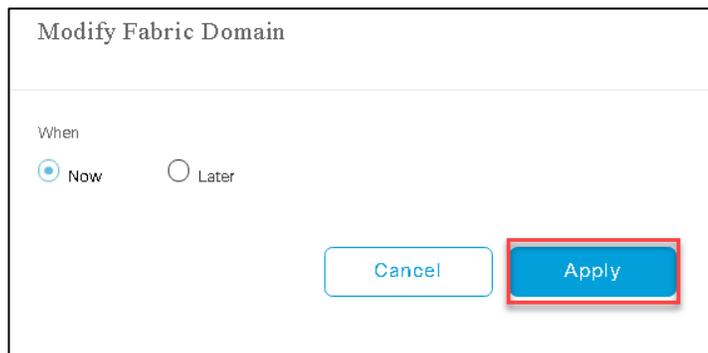
ステップ6 イメージがデバイスにインポートされてアクティブになったら、デバイスによって管理されるサイトを選択します。



ステップ7 Cisco DNA Center に、デバイスにプロビジョニングされた SSID 設定などの設定の概要が表示されます。



ステップ 8 組み込みワイヤレスを追加したら、ファブリック設定を保存します。



Modify Fabric Domain

When

Now Later

Cancel Apply

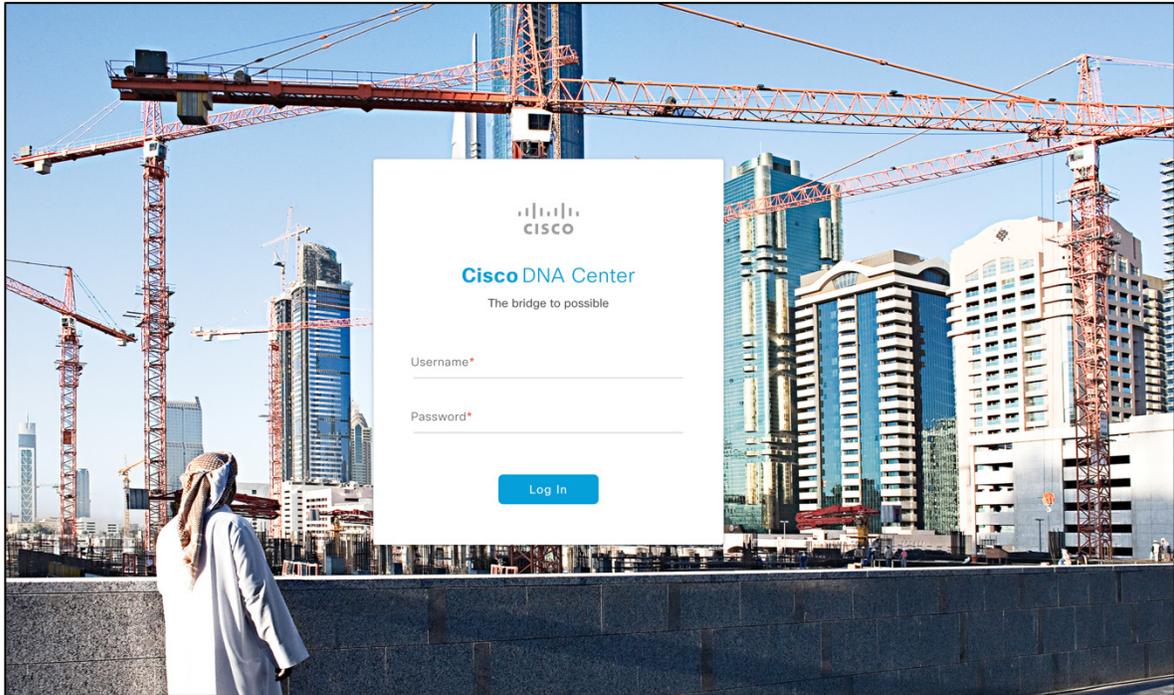
ファブリック対応 AP とファブリックエッジとしての Catalyst 4500E

SD-Access ファブリックがファブリックエッジ (FE) としての Catalyst 4500E で構成され、AP が直接接続されている場合は、特別な考慮が必要です。ファブリック対応ワイヤレス (FEW) を使用すると、シスコのアクセスポイントはそれぞれのファブリックエッジへの VxLAN トンネルを作成します。Catalyst 4500E で VxLAN トンネルをサポートするには、スイッチをインストールモードで起動する必要があります。スイッチ上のドーターカードは、アクセストンネルからの VxLAN ヘッダーのカプセル化を解除します。

Catalyst 4500E でサポートされている推奨リリース、スーパーバイザモジュール、およびラインカードについては、SDA 互換性ガイドを参照してください。

もう 1 つの重要な考慮事項は、アクセスポイント (AP) をサポートされているラインカードに直接接続できる一方で、アップストリームを残りのファブリックに接続するためにスーパーバイザモジュールのポートを使用する必要があります。

ドーターカードがプラットフォームで有効になっているかどうかを確認するには、show module CLI を使用してください。



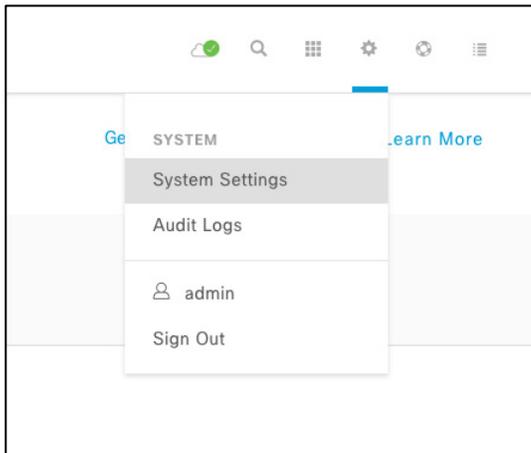
ステップ2 ログイン後、Cisco DNA Center ランディングページが表示されます。

A screenshot of the Cisco DNA Center dashboard. The top navigation bar includes "Cisco DNA Center" and menu items: DESIGN, POLICY, PROVISION, ASSURANCE, PLATFORM. The main content area starts with a "Welcome, admin" message and a "Get Started" button. Below this is an "Assurance Summary" section with three cards: "Health" (Healthy as of Jan 28, 2020 11:35 AM) showing percentages for Network Devices, Wireless Clients, and Wired Clients; "Critical Issues" (Last 24 Hours) showing 0 P1 and 0 P2 issues; and "Network Snapshot" showing "Network Devices" (As of Jan 28, 2020 11:46 AM) with 0 Unclaimed and "Application Policies" (As of Jan 28, 2020 11:46 AM) with 0 Successful Deploys.

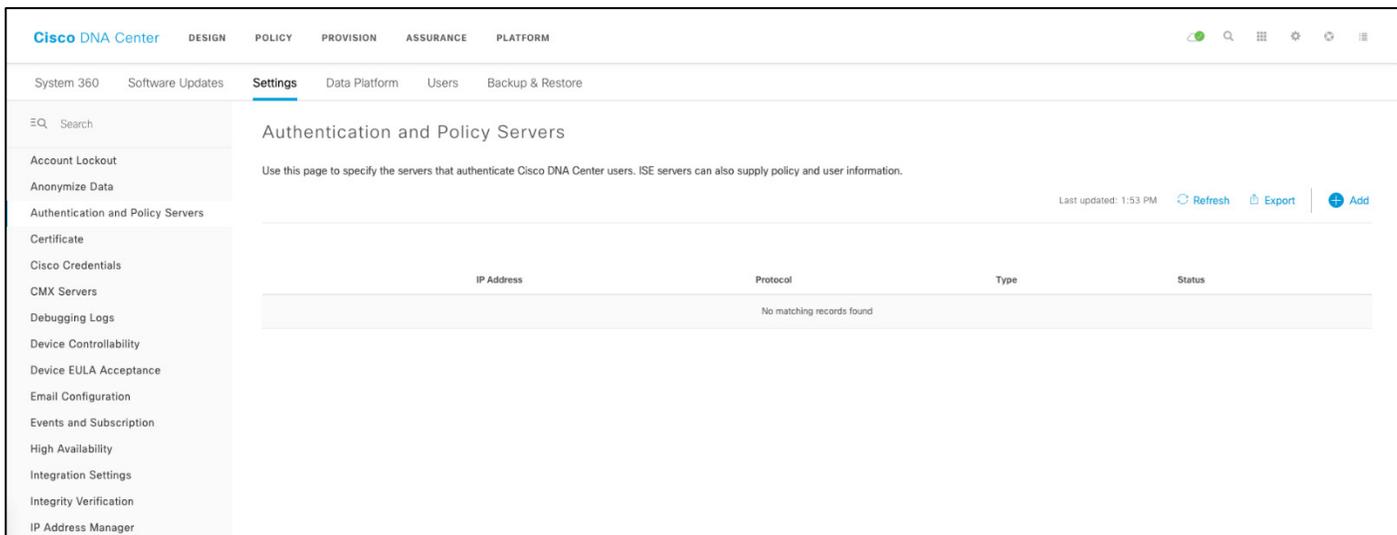
Cisco DNA Center への ISE の追加

SGT のダウンロードおよび新しいポリシーの作成には、Cisco DNA Center が安全に ISE と通信する必要があります。ISE サーバと Cisco DNA Center は pxGrid と REST API サービスを使用して情報を交換します。

Cisco DNA Center に ISE を追加するのは非常に簡単です。Cisco DNA Center で、ホームページの右上隅にある「歯車」シンボルをクリックして [System Settings] に移動します。



[System Settings] ページで、[Authentication and Policy Servers] をクリックし、[Add] をクリックして新しいサーバを追加します。



ISE 情報を入力します（忘れずに [Cisco ISE server] スイッチを切り替えます）。

Add AAA/ISE server

Server IP Address*
10.195.180.131

Shared Secret*
.....

Cisco ISE server
 On

Username*
admin

Password*
.....

FQDN*
prabhjit-ise.cisco.com

Subscriber Name*
dnac-133

SSH Key
|

Virtual IP Address(es)

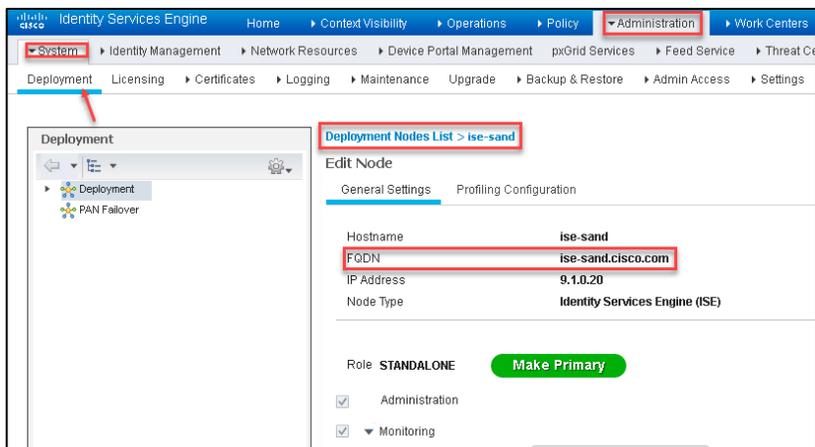
View Advanced Settings

Cancel Apply

共有秘密は、ネットワークデバイス（スイッチおよび WLC）で使用されるパスフレーズを定義するもので、ネットワーク アクセス デバイス（NAD）の作成時に ISE で設定されます。Cisco DNA Center により、ネットワークデバイス上の RADIUS サーバ設定と ISE サーバ上の NAD 設定が自動化されます。ユーザ名とパスワードは、ISE クラスターの管理者ログイン情報です。ISE の FQDN（ホスト名 + ドメイン名）を入力します。

(注) 管理者ログイン情報が Web GUI と SSH アクセスで同じであることを確認します。

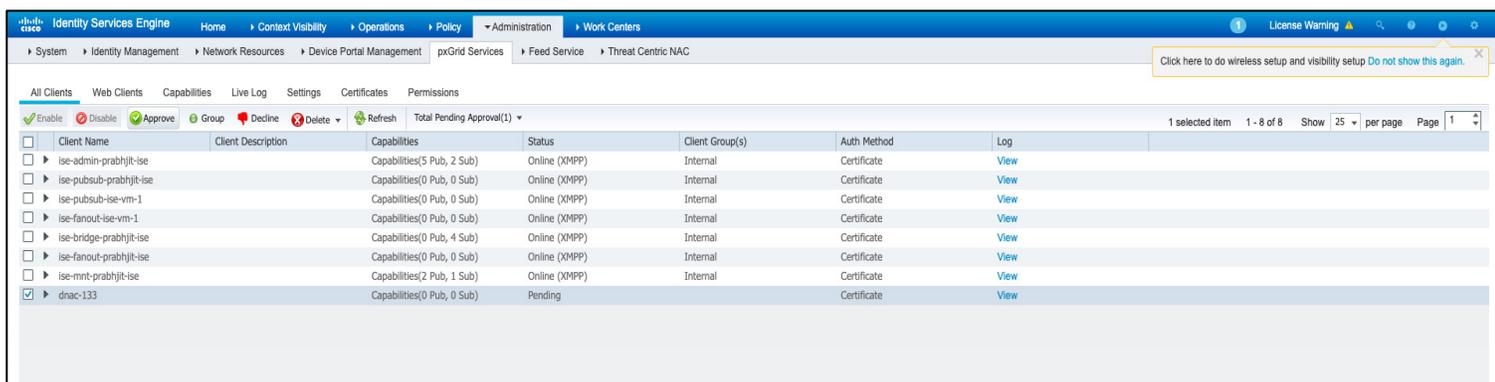
今日の時点では、Cisco DNA Center は DNS を使って FQDN を検証しませんが、この名前は ISE サーバの実名と一致する必要があります。サブスクリバの名前を追加することを忘れないでください。これは、pxGrid ログイン情報を確立するために重要です（この名前は、ISE 上の既存のユーザ名と一致する必要はありません）。



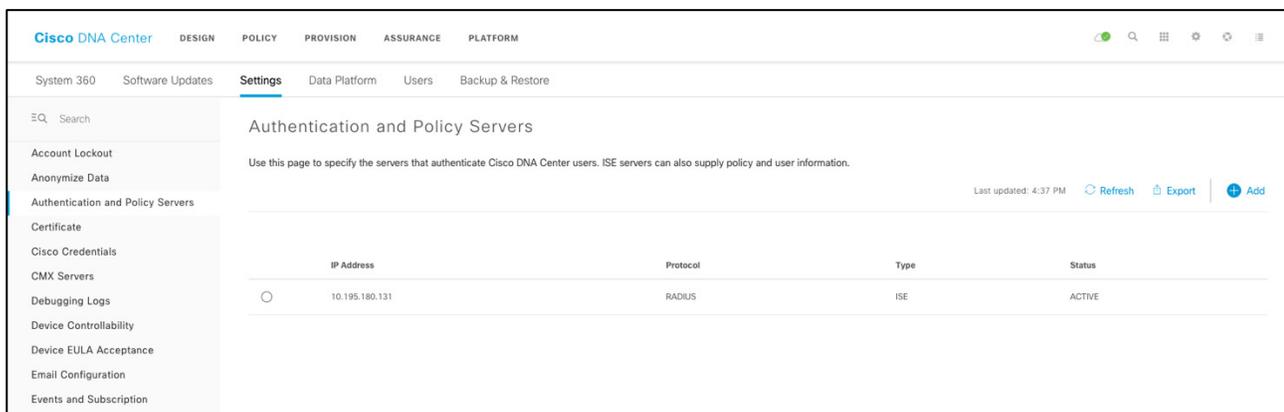
ISE クラスターの FQDN 名を取得するには、プライマリ PAN の Web GUI にログインし、次のリンクに移動します。

[Administration] > [System] > [Deployment] > クラスターのホスト名

ISE に移動し、[Administration]、[pxGrid Services] の順に移動して、サブスクリバ名 dnac-133 を承認することで Cisco DNAC の pxGrid 接続を承認します。



Cisco DNAC で ISE のステータスを確認します。

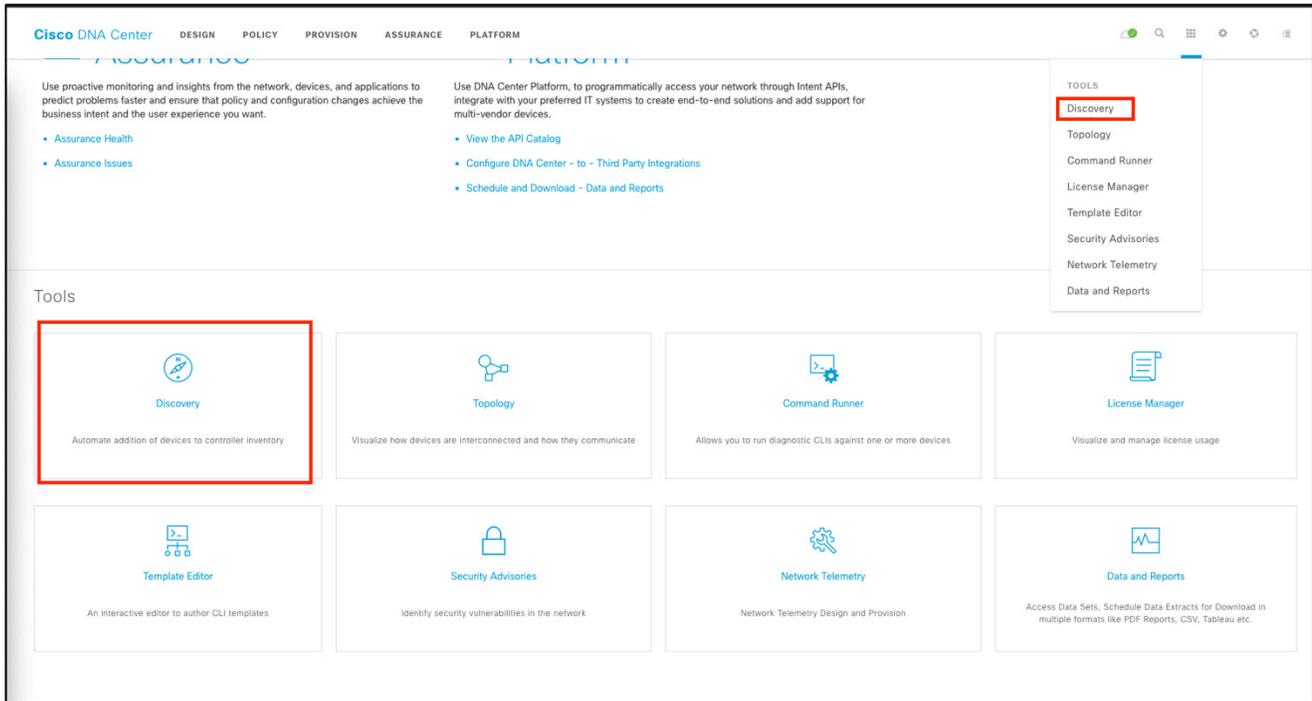


SD-Access WLC ディスカバリ

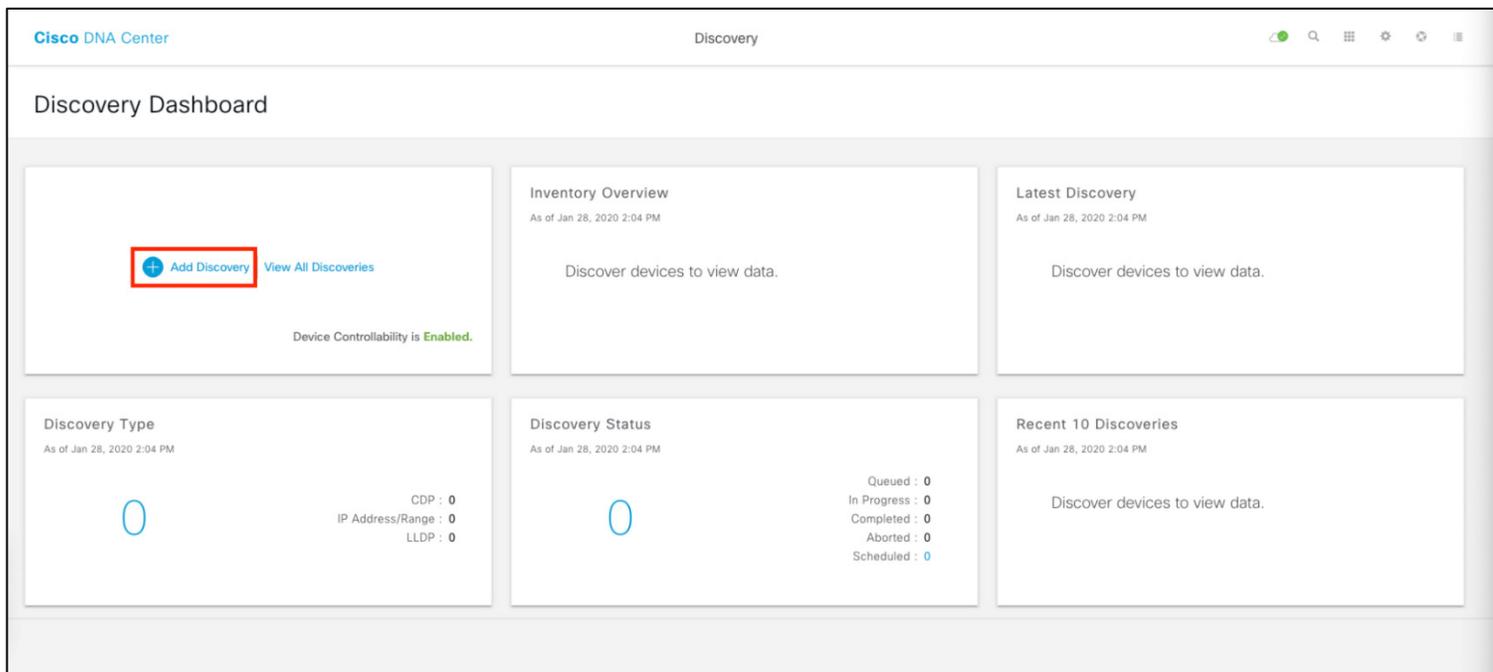
Cisco DNA Center のディスカバリツールは、Cisco Discovery Protocol または IP アドレス範囲で既存のアンダーレイデバイスを検索する場合に使用します。ここでの前提条件は、有線ネットワークがすでに検出されていることです。

手順

ステップ 1 Cisco DNAC のホームページで、[Tools] > [Discovery] まで下にスクロールするか、右上にある [Discovery] を選択してデバイスを検出し、Cisco DNA Center のプロセスを開始します。



検出されたデバイスの概要を確認できる [Discovery Dashboard] が表示されます。[Add Discovery] をクリックして新しい検出を開始します。

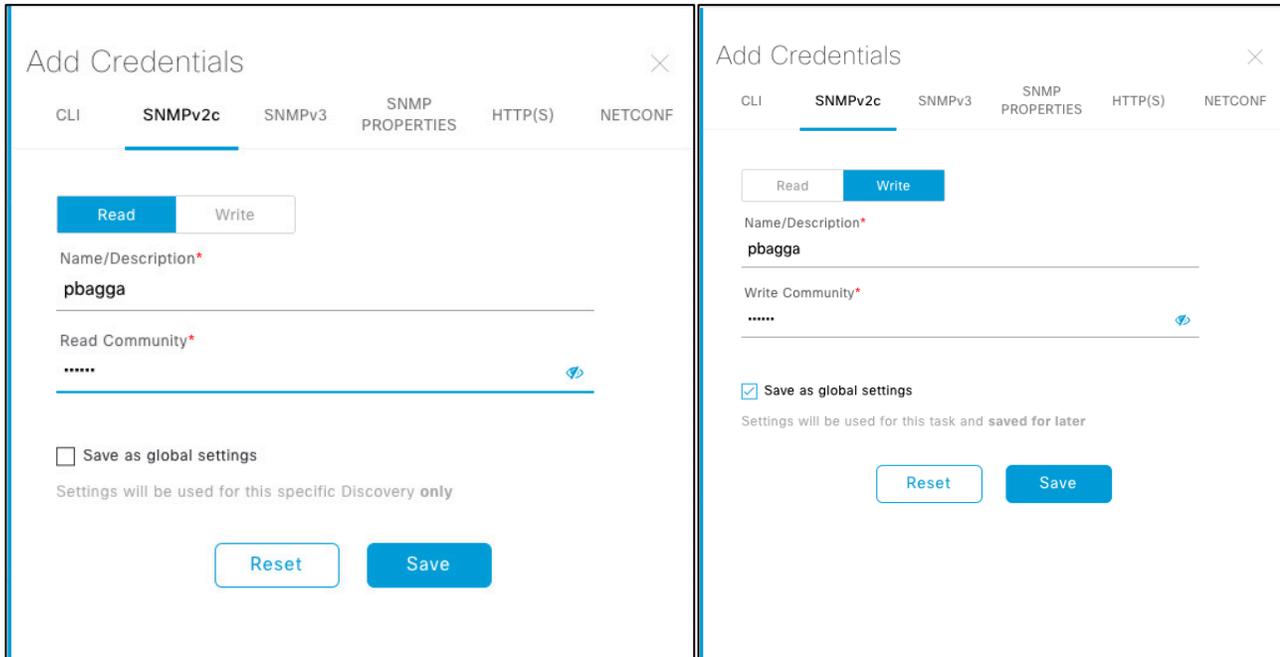


ステップ2 検出名を入力し、検出タイプとして [Range] を選択し、ネットワークの WLC の管理 IP アドレスを範囲の開始および終了として入力します。

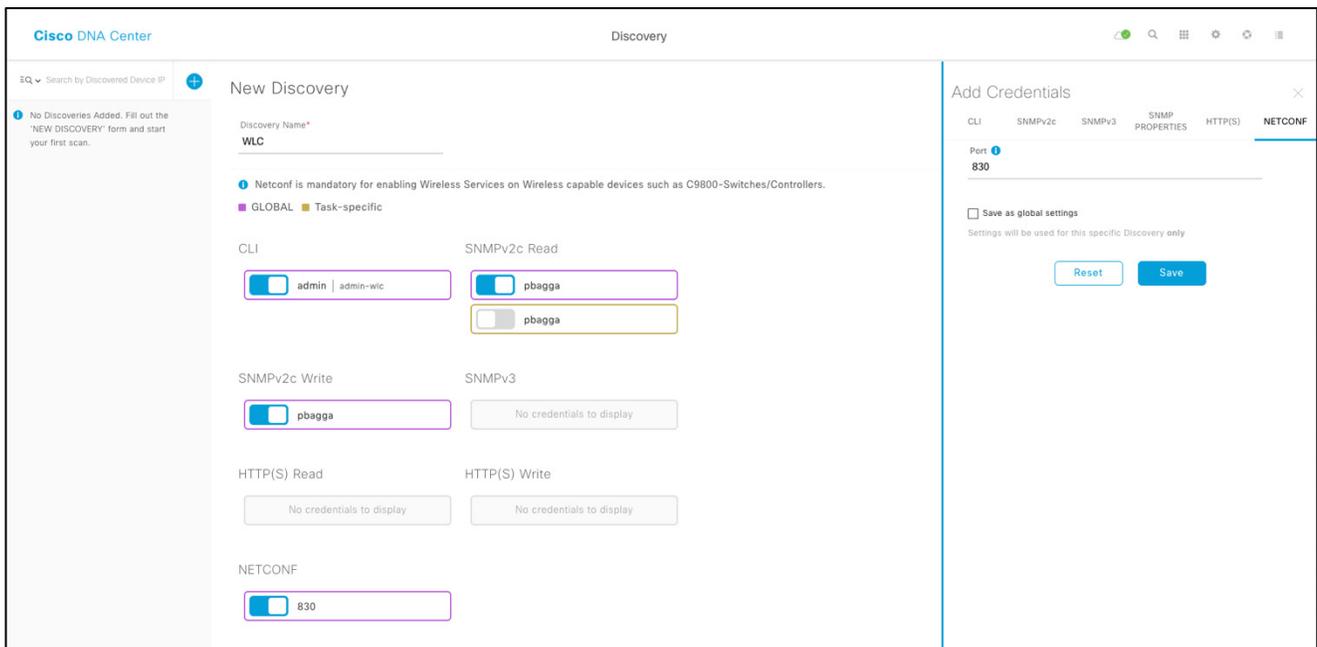
The screenshot shows the 'New Discovery' configuration page in Cisco DNA Center. The 'Discovery Name' is 'WLC'. The 'Discovery Type' is 'IP Address/Range'. The 'From' IP is '192.168.1.10' and the 'To' IP is '192.168.1.10'. The 'Preferred Management IP Address' is 'None'. The 'Credentials' section shows that CLI and SNMPv2c Read credentials are not displayed. A 'Reset' button and a 'Discover' button are at the bottom right.

ステップ3 [Add Credentials] をクリックして、WLC にアクセスするためのログイン情報を追加します。デバイスの Simple Network Management Protocol (SNMP) ログイン情報 (読み取りおよび書き込み) を次のように入力します。

The screenshot shows the 'New Discovery' configuration page with the 'Add Credentials' dialog open. The dialog has tabs for 'CLI', 'SNMPv2c', 'SNMPv3', 'SNMP PROPERTIES', 'HTTP(S)', and 'NETCONF'. The 'SNMPv2c' tab is selected. The 'Name/Description' is 'admin-wlc', the 'Username' is 'admin', and the 'Password' is masked. The 'Enable Password' checkbox is checked. The 'Save as global settings' checkbox is also checked. 'Reset' and 'Save' buttons are at the bottom of the dialog.



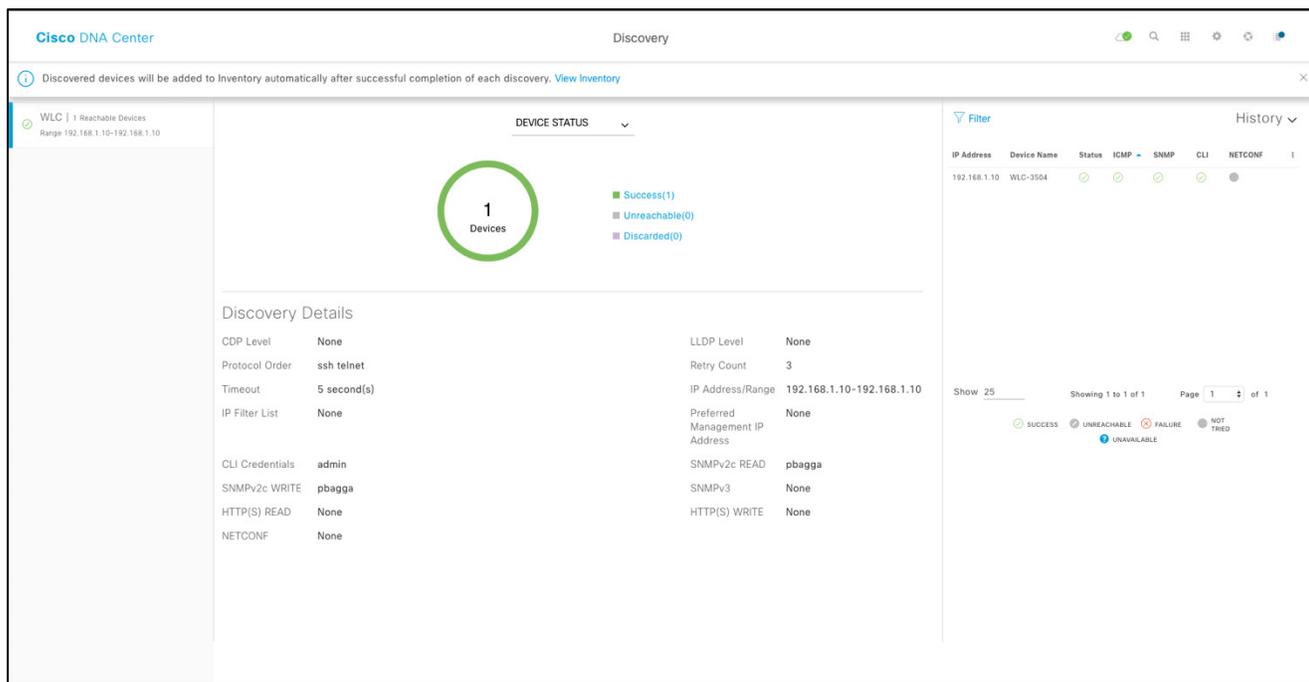
検出中にログイン情報に対して指定されたすべてのオプションを有効にすると、検出された WLC で Cisco DNA Center によってその設定が行われます。Cisco DNA Center は Telnet/SSH 経由でデバイスにログインし、デバイスで SNMP と netconf を有効にします。SNMP の読み取りおよび書き込みはアシュアランスに使用され、netconf はワイヤレス LAN コントローラ (WLC) に設定をプロビジョニングする方法の 1 つとして使用されます。プラットフォームで SSH を有効にする方法については、ワイヤレス LAN コントローラのコンフィギュレーションガイドを参照してください。



ステップ 4 [Credentials] セクションを折りたたんで、[Advanced] セクションを展開します。クリックして [Telnet] や [SSH] を選択します。SSH は、AIRE-OS ベースのワイヤレス LAN コントローラ (WLC) ではデフォルトで有効になっています。Catalyst 9800 ワイヤレス LAN コントローラ (WLC) で SSH を有効にするには、[コンフィギュレーション ガイド](#)を参照してください。

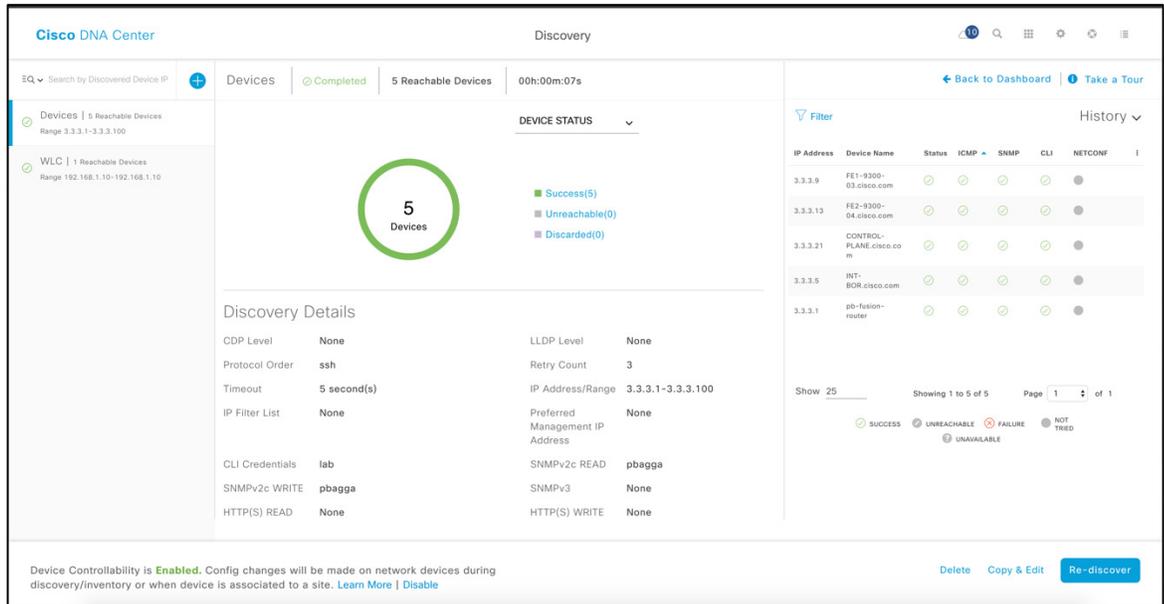


右下隅にある [Discover] をクリックします。ディスカバリが開始すると、ページにディスカバリ設定と詳細が表示されます。



同様に、ファブリックに含める他のデバイスをネットワーク内で検出します。有線デバイスが検出され、その名前が画面の右側に順次表示されます。

(注) ここでも、他のファブリックの有線デバイス (ボーダーノードとエッジノード) がすでに検出されていることが前提とされています。スイッチには Cisco Discovery Protocol ディスカバリを使用することをお勧めします。



(注) デバイスディスカバリが完了すると、検出されたデバイスがすべて Cisco DNA Center のデバイスインベントリに表示されます。

インベントリ アプリケーション

手順

ステップ 1: デバイスのディスカバリ後、デバイス インベントリ アプリケーションを開いてそのデバイスを表示するには、上部で [Provision] > [Inventory] の順にクリックします。

ステップ 2: [Provision] の [Inventory] ページで、すべてのデバイスの [Reachability Status] が [Reachable] に、[Last Inventory Collection Status] が [Managed] になっている必要があります。

(注) 前述のディスカバリ手順を省略した場合は、デバイスが [Managed] と表示されていることを確認します。そうならない場合は、次に進む前に修正する必要があります。

The screenshot shows the Cisco DNA Center interface in the 'PROVISION' tab. The main content area displays a table of network devices under the 'Inventory' focus. The table has the following columns: Device Name, IP Address, Support Type, Device Family, Site, Reachability, Last Sync Status, Last Updated, Serial Number, and Device Series. There are six devices listed, all of which are 'Reachable' and 'Managed'.

Device Name	IP Address	Support Type	Device Family	Site	Reachability	Last Sync Status	Last Updated	Serial Number	Device Series
CONTROL-PLANE.cisco.com	3.3.3.21	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW2243E0UD	Cisco Catalyst 9300 Series
FE1-9300-03.cisco.com	3.3.3.9	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW2248AHLW	Cisco Catalyst 9300 Series
FE2-9300-04.cisco.com	3.3.3.13	Supported	Switches and Hubs	Assign	Reachable	Managed	an hour ago	FCW2248DHHS	Cisco Catalyst 9300 Series
INT-BOR.cisco.com	3.3.3.5	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW1934C1D8	Cisco Catalyst 3850 Series
pb-fusion-router	3.3.3.1	Supported	Switches and Hubs	Assign	Reachable	Managed	3 hours ago	FDO1735Q0FR	Cisco Catalyst 3650 Series
WLC-3504	192.168.1.10	Supported	Wireless Controller	Assign	Reachable	Managed	4 hours ago	FCW2221M0JT	Cisco 3500 Series Wireless

SD-Access の設計

Cisco DNA Center Design の使用開始

Cisco DNA Center には強力な設計アプリケーションが備わっており、あらゆる規模のお客様が、物理サイトおよび共通リソースを簡単に定義できます。これは、直感的に使用できる階層形式で実装されており、デバイスのプロビジョニング時に複数の場所で同じリソースを再定義する必要がありません。

手順

ステップ 1 次の例のような [Design] ページを使用して、ネットワークのサイトとサイト階層を作成します。

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Network Hierarchy Network Settings Image Repository Network Profiles Authentication Template

EQ Find Hierarchy

Global No sites found.

+ Add Site Import

Add Area

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Area Name*
San Jose

Parent
Global

Cancel Add

Or

Import Sites

EQ Find Buildings

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Network Hierarchy Network Settings Image Repository Network Profiles Authentication Template

EQ Find Hierarchy

Global San Jose

+ Add Site Import

Add Building

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Building Name*
Building 22

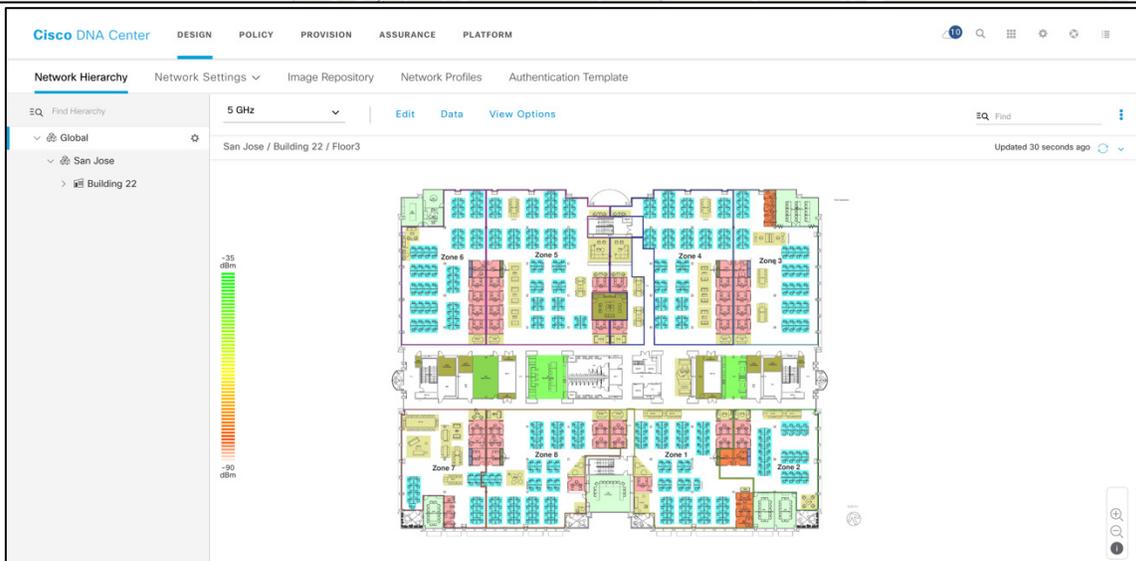
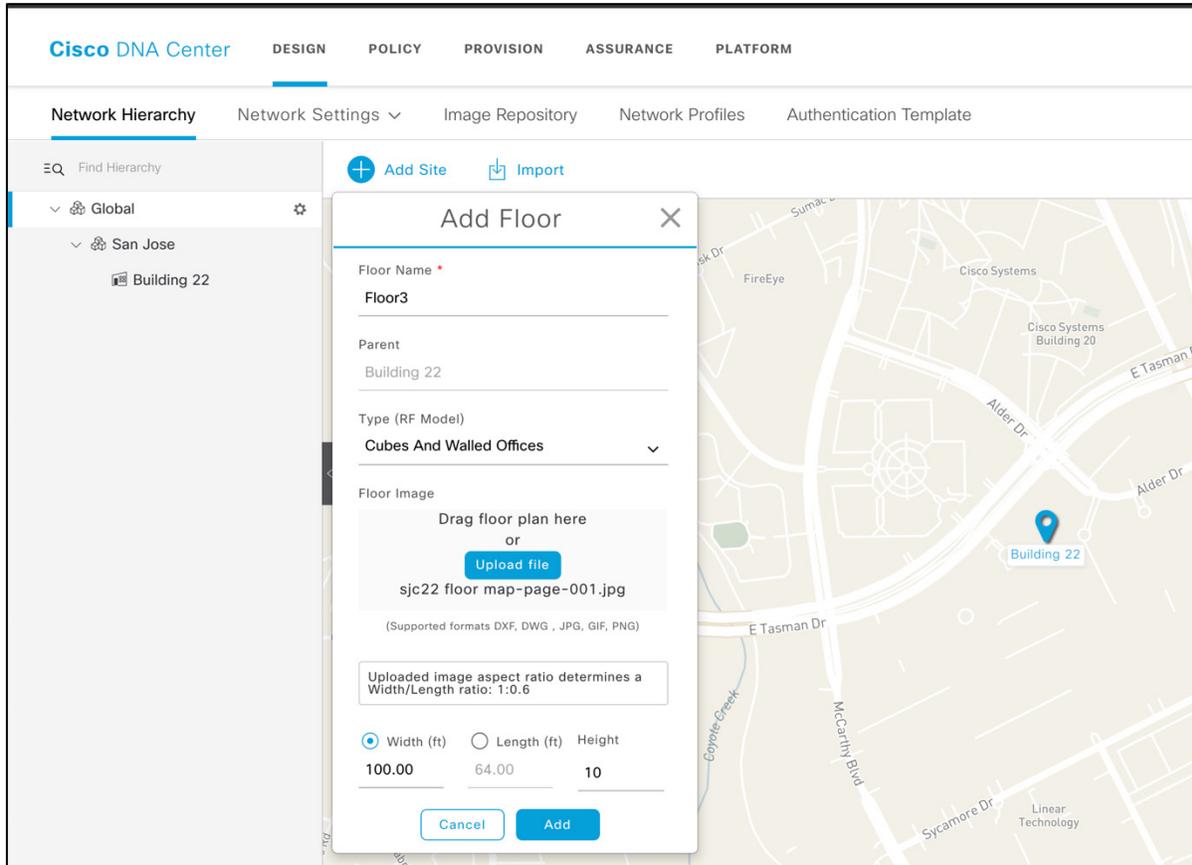
Parent
San Jose | Global/

Address
Alder Drive, Milpitas, California 95035,

Latitude* **37.4124503** Longitude* **-121.9168115**

Cancel Add

EQ Find Buildings



ネットワーク設定 (Network settings)

Cisco DNA Center では、[Design] の [Network Settings] アプリケーションに共通のリソースと設定を保存できます。これにより、企業に属する情報が保管できるため、Cisco DNA Center 全体で再利用できます。DHCP、DNS サーバおよびデバイスログイン情報はここで定義されている必要があります。

IP プールの作成

AP とクライアントサブネット両方の IP プールを、DHCP サーバのネットワーク アドレッシング スキームに従って手動で設定します。また、DHCP オプション 43 を AP IP プールの DHCP サーバに定義し、AP を WLC に登録します。このガイドでは、IP アドレスマネージャ (Infoblox) の統合を活用しないため、Cisco DNA Center ではこの手順は自動化されません。

手順

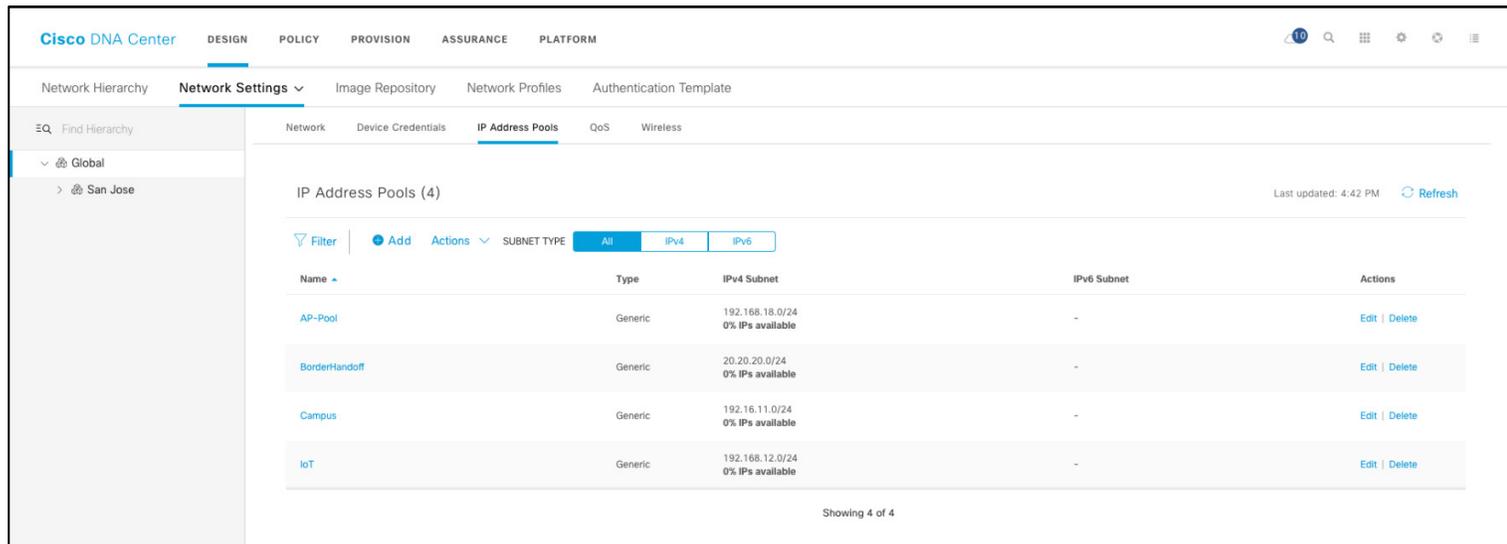
メニューを使用し、[Design] > [Network Settings] の順に移動し、[IP Address Pools] を選択します。[Add] をクリックして、ダイアログボックスを開き新しい IP プールを作成します。

The screenshot displays the Cisco DNA Center interface. The top navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. The 'Network Settings' menu is expanded, showing 'IP Address Pools' as the selected option. The main area shows a map of a campus with 'Building 22' highlighted. The 'Add IP Pool' dialog box is open, showing the following configuration details:

- IP Pool Name: Campus-14
- Type: Generic
- IP Address Space: IP v4 (selected), IP v6 (unselected)
- IP Subnet: 192.168.11.0
- CIDR Prefix: /24 (255.255.255.0)
- Gateway IP Address: 192.168.11.1
- DHCP Server(s): 10.5.130.2
- DNS Server(s): 171.70.168.183

The dialog box also includes a search field for DNS servers with the value '171.70.168.183' entered.

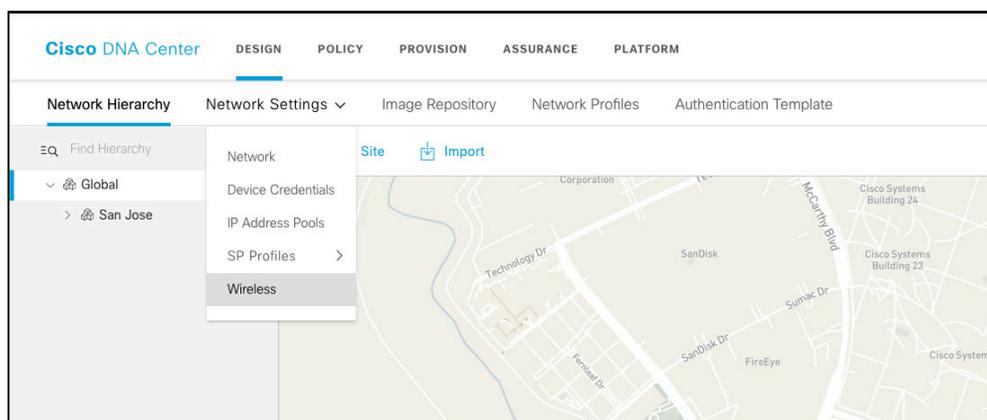
完了したら、Cisco DNA Center のクライアントおよび AP 用の [IP Address Pools] タブは次のページのようにになります。



ワイヤレス SSID の作成

手順

ステップ 1 [Network Settings] の [Wireless] タブをクリックします。



SSID の作成は 2 段階のプロセスです。ネットワークのタイプを選択し、セキュリティタイプを割り当て、まずワイヤレスネットワークを作成し、次にワイヤレスプロファイルを作成または割り当てます。新しいプロファイルを作成する場合は、この SSID をブロードキャストするサイトを追加します。ワークフローを実行するには、次の手順を参照してください。

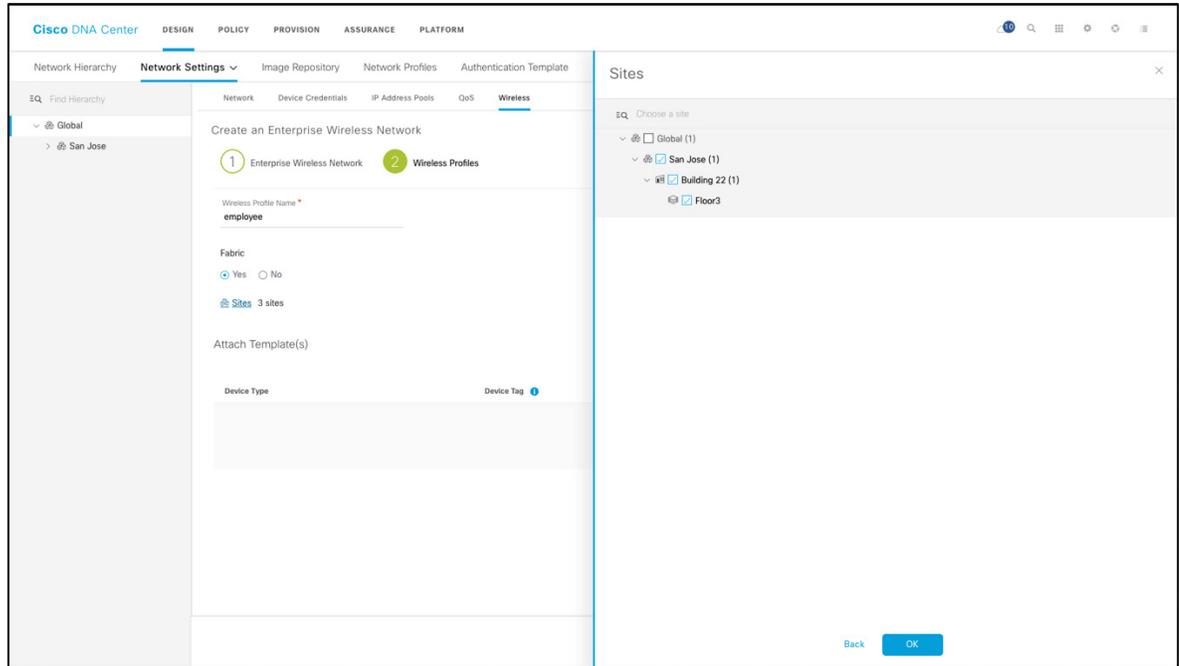
ステップ 2 エンタープライズワイヤレス SSID (この例では「Internal03」) で [Add] をクリックし、[Level of Security] として [WPA2 Personal] とセキュアなパスフレーズを選択します。Fast Transition (802.11r) は、SSID の作成のフェーズで設定できます。

(注) このガイドのすべての例では、SSID、プロファイル、プールなどの名前は参考用です。ユーザーは自分自身で任意の名前を指定できます。

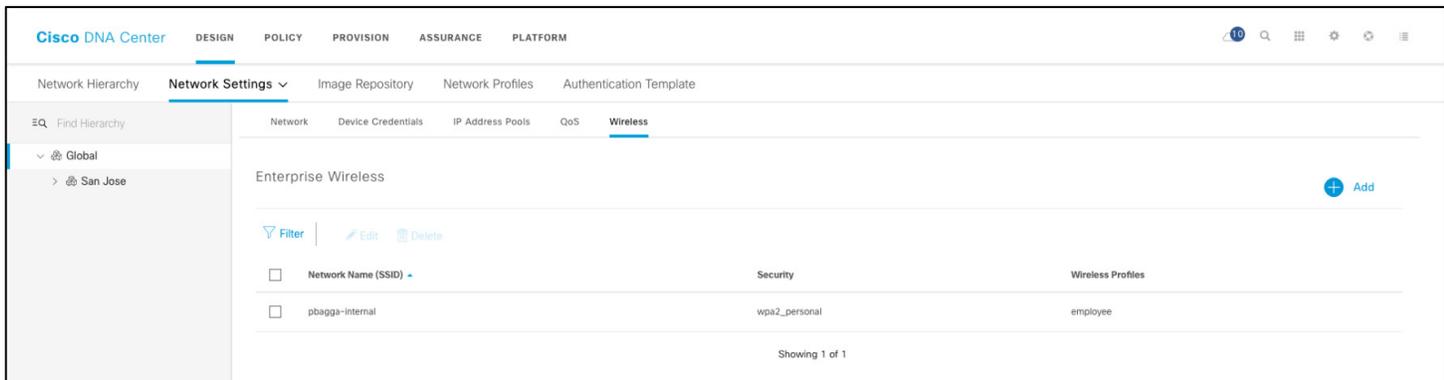
ステップ 3

[Next] をクリックします。まだ設定されていない場合、Cisco DNA Center ではワイヤレスプロファイルを作成して SSID に関連付けるように求められます。この場合のワイヤレスプロファイルの名前は「employee」です。すでにプロファイルがある場合は、既存のプロファイルのいずれかを選択できます。ネットワークプロファイルは、SSID、ファブリックまたは非ファブリックのタイプ、およびブロードキャストされるサイトを定義します。[Finish] をクリックしてワイヤレスプロファイルを作成します。

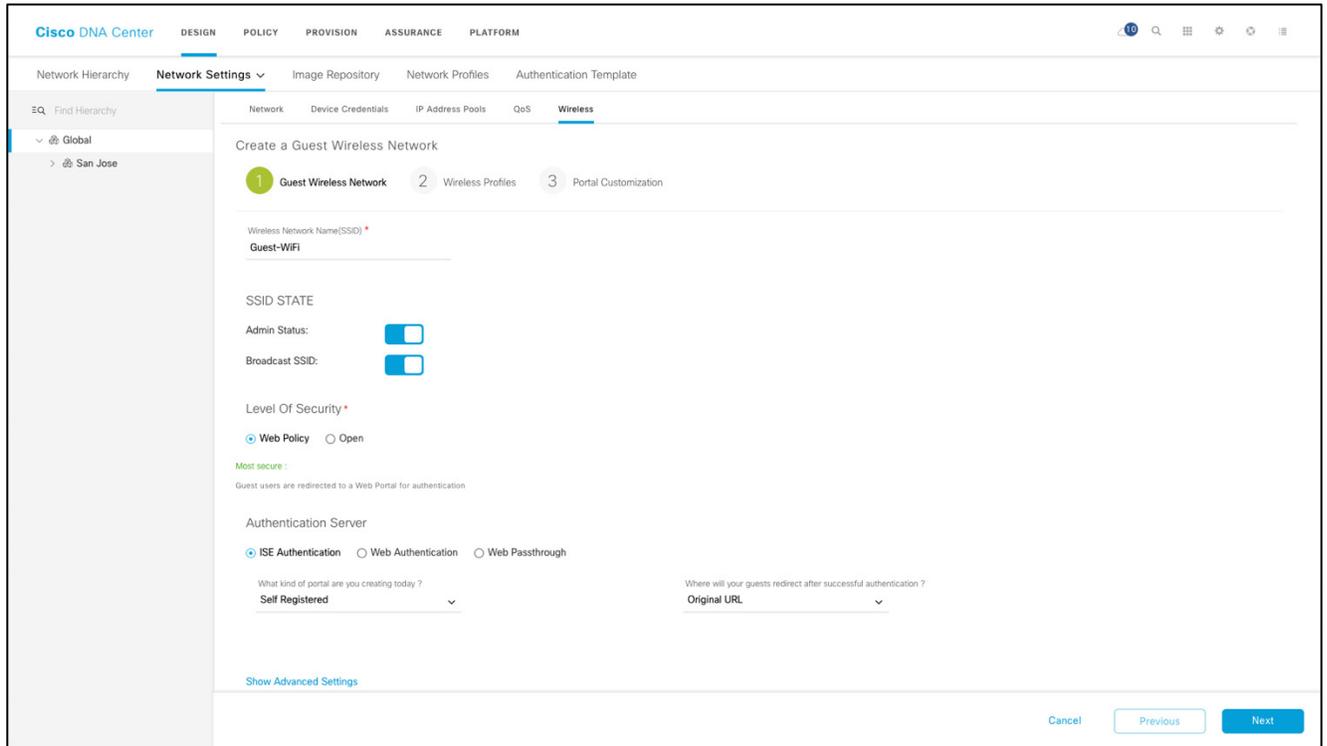
[Wireless Profile] で、プロファイルが SD-Access ファブリック用かどうかを指定し、このプロファイルの SSID がブロードキャストされる場所を追加します。下記の例では、SSID pbagga-internal がサイト Sanjose にマップされています。子サイト (Floor-1) は設定を継承します。サイトの最初の文字を入力し、表示されるかを確認します。



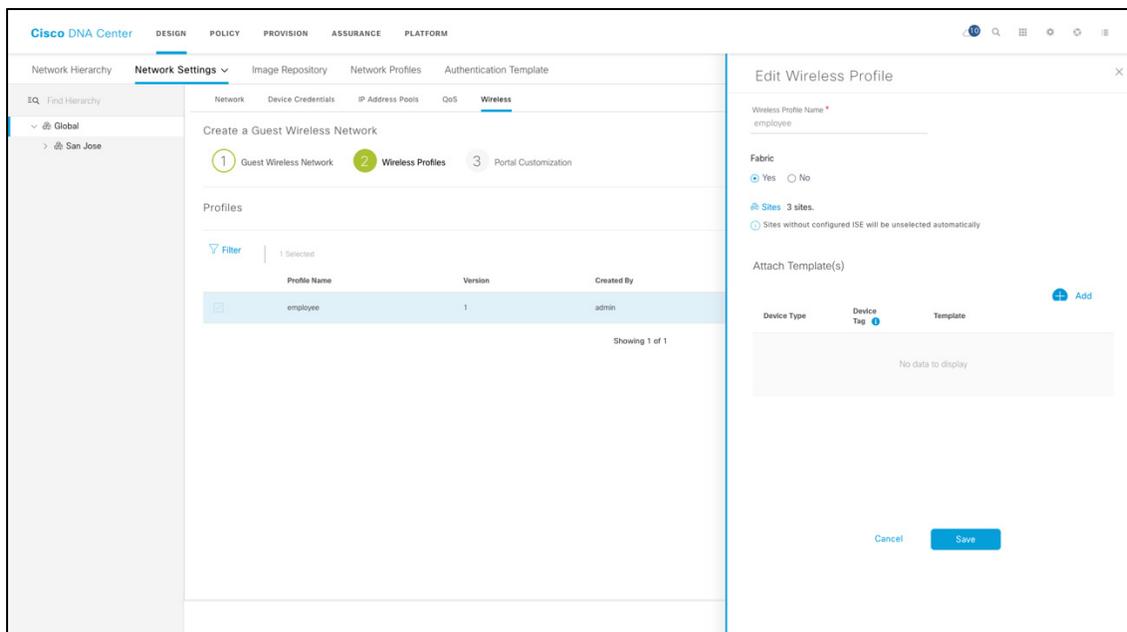
ステップ 4 プロファイルを設定したら、[Save] をクリックし、SSID のメインページに戻ります。



ステップ5 これで、ゲスト SSID を作成できます。[Guest Wireless] にある [Add] アイコンをクリックし、ゲスト SSID を追加します。

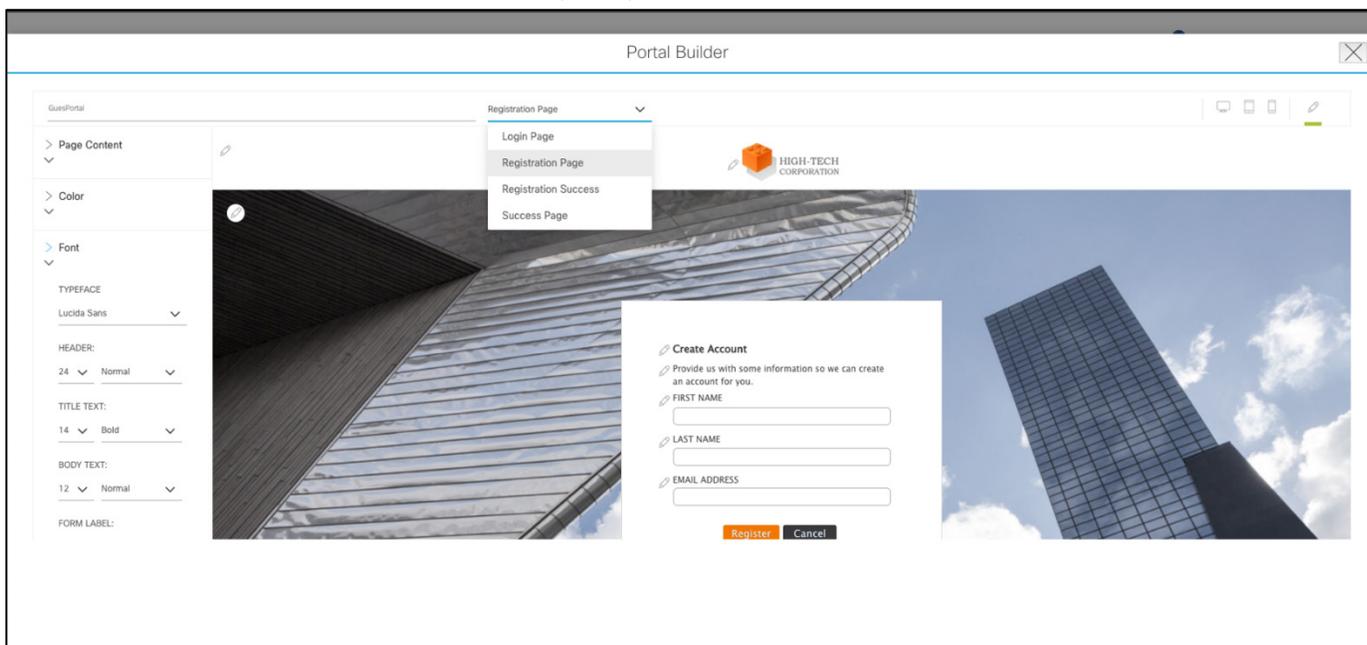


ステップ6 非ゲスト SSID の場合と同様に、SSID をネットワークプロファイルに追加します。



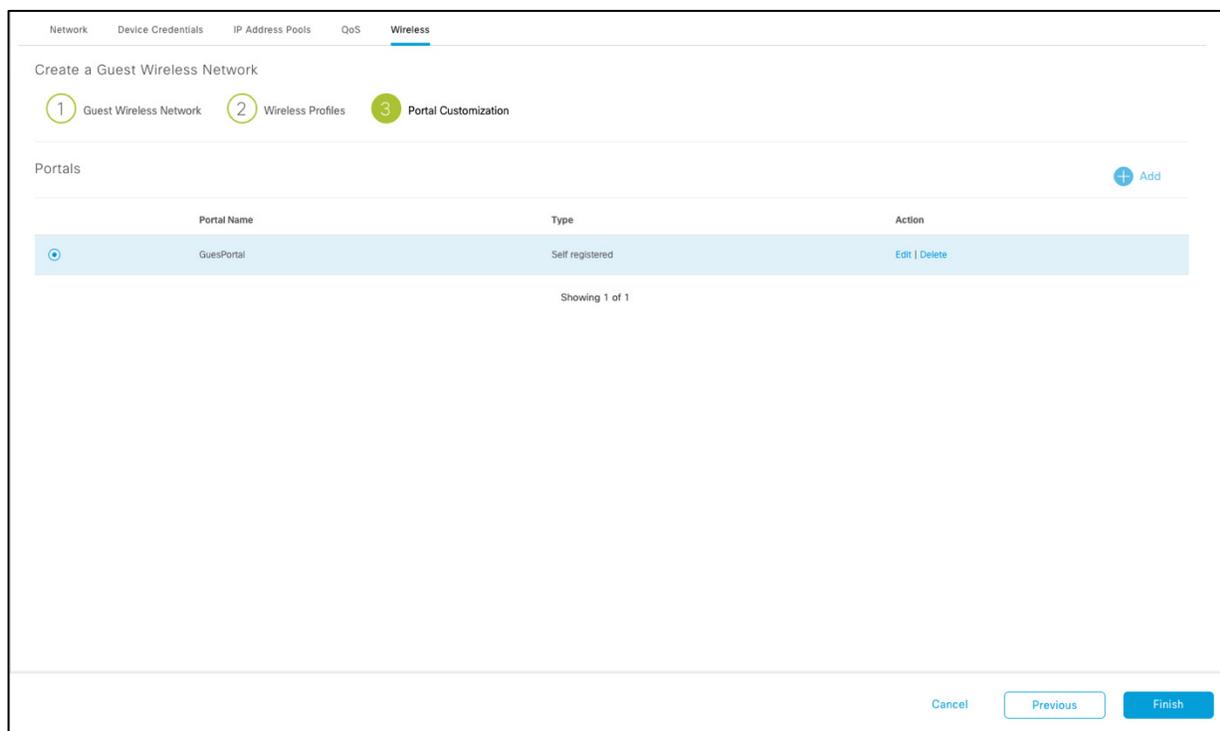
ステップ 7

Cisco DNA Center は、ポータルおよびプロフィール設定用に ISE とのバックエンド統合を提供します。以下のスクリーンショットには、ポータルのカスタマイズに使用できるオプションがあります。ISE を使用した中央 Web 認証 (CWA) がサポートされています。



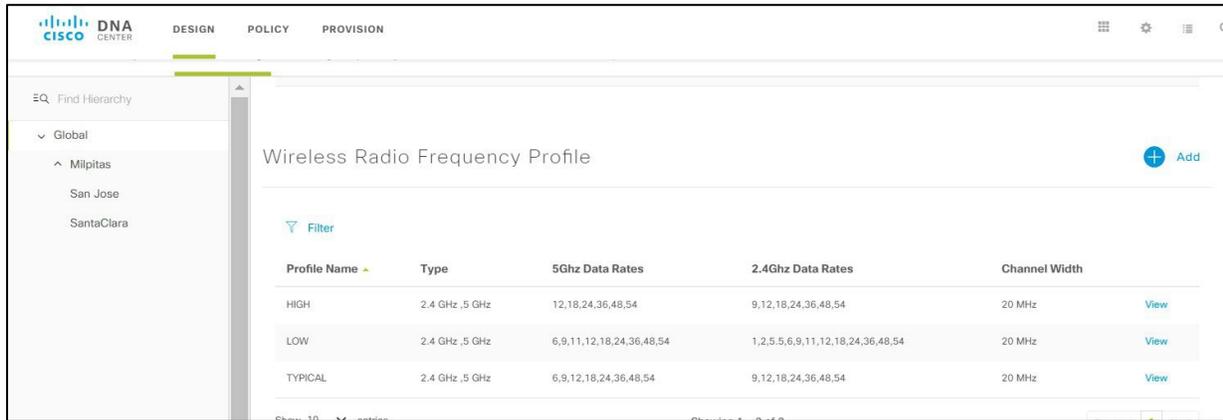
ステップ 8

[Finish] をクリックして、ゲスト SSID 設計フェーズを完了します。



ステップ 9

必要に応じて、カスタマイズされた RF プロファイルを設定できます。設計フェーズのプロファイルは、プロビジョニングフェーズで適用されます (このガイドで後述)。ワイヤレスページを下にスクロールし、使用可能なワイヤレス無線周波数プロファイルを表示します。



新しいプロファイルを作成するには、[Add New] をクリックします。次のページが表示されます。

PROFILE NAME*
demo

PROFILE TYPE

^ 2.4 GHz On

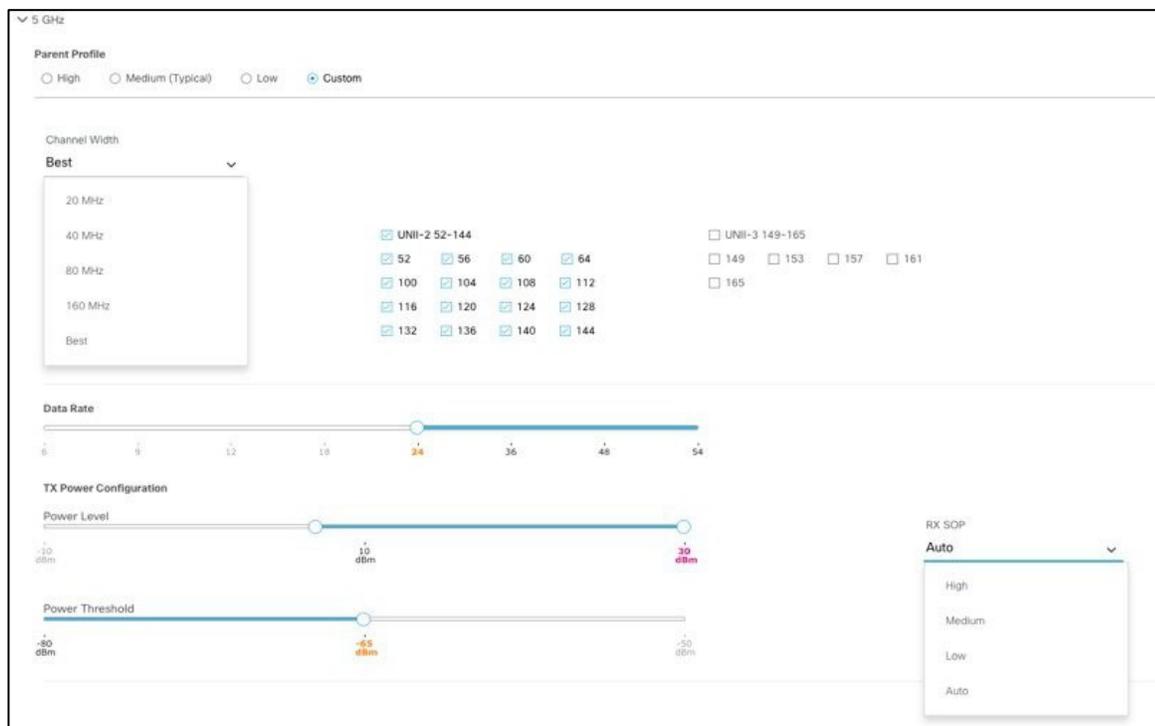
Parent Profile
 High Medium (Typical) Low Custom

^ 5 GHz On

Parent Profile
 High Medium (Typical) Low Custom

Cancel Save

2.4 または 5 GHz バンドの親プロファイルに対して、カスタマイズパラメータ（動的帯域幅選択、DCA チャンネルの柔軟性と HD RF 設定）を選択します。



SD-Access のポリシー

SD-Access では、ネットワークポリシーは、Cisco TrustSec® に基づくグループベースポリシーです。仮想ネットワーク (VN) (VRF に相当) とスケーラブルグループタグ (SGTS) は、階層的なネットワークポリシーとセグメンテーションを提供するために使用されます。マクロレベルでは、VN を使用して、コントロールプレーンとデータプレーンの観点からユーザグループを完全に分離できます。これはステートフル セグメンテーションで、通常 VRF 間のトラフィックを許可するためにファイアウォールを通過します。VN では、SGT を使用して、セキュリティグループ アクセス コントロール リスト (SGACL) に基づいて、ユーザ間でステートレスポリシーを定義し、マイクロセグメンテーションを実装できます。SD-Access の利点は、これが有線とワイヤレスの両方のユーザに当てはまるということです。

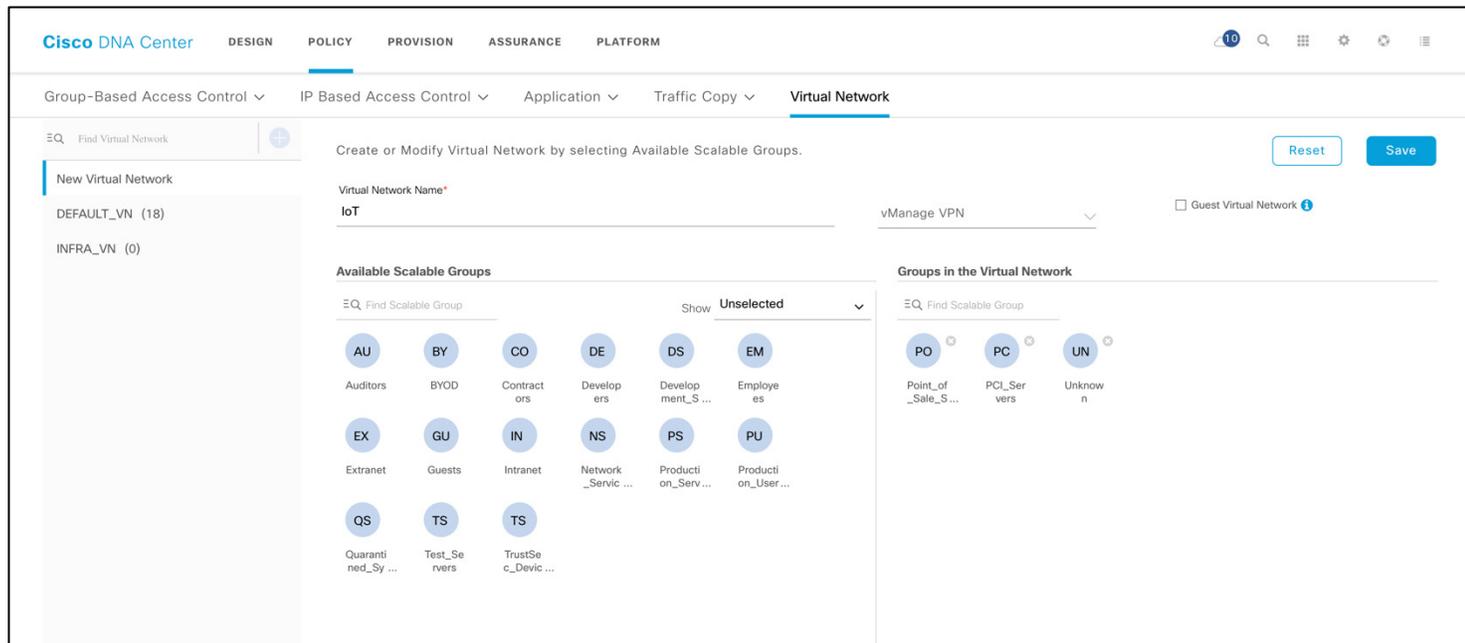
以降では、ファブリック内の 2 つのグループ間にポリシーを作成し、コントラクトを割り当てます。2 つのユーザグループ「employees」と「pci_servers」の間で HTTP アクセスを許可するコントラクト「demo_access」が作成されます。

SGT をユーザに割り当てるには、Identity Services Engine (ISE) ガイドでセグメンテーションについて参照してください。

[ISE セグメンテーションガイド](#)

手順

ステップ 1 [Policy] > [Virtual Network] ページで、[+] アイコンをクリックして新しい VN を作成します。名前を選択して VN にスケーラブルグループを割り当てます。この手順は任意です。

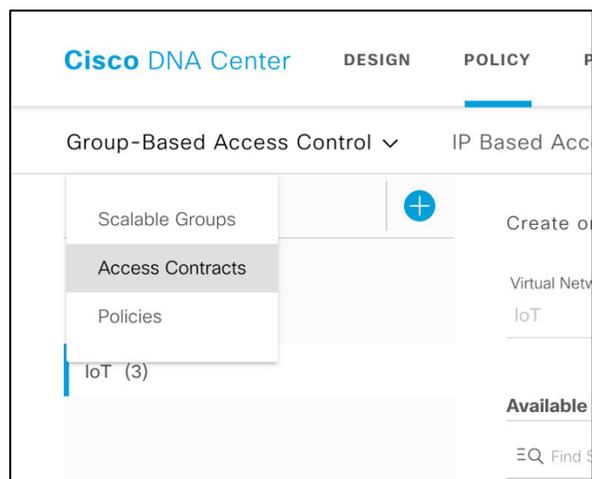


(注) この時点で VN にグループ (SGT) を追加する理由は、オンボーディングセクションで明確になります。SSID またはポートに SGT を静的に割り当てる場合は、プールの関連付けを使用して行い、この時点で VN に含まれている SGT から選択できる SGT を選択します。

ステップ 2 [Save] をクリックして VN を作成します。

正常に作成されると、画面の右下隅にメッセージがポップアップ表示されます。

ステップ 3 次に、[Policy] > [Group-Based Access Control] > [Access Contracts] の順にクリックして、コントラクトを追加します。コントラクトとは、スケーラブルグループ間で許可されるトラフィックを定義する場所です。



ウィンドウの右上隅にある [Add Contract] アイコンをクリックして、次のようにコントラクトエディタを開きます。この例では、特定のポートまたはプロトコル（この場合は HTTP）の許可アクションを使って「demo_access」を作成しました。暗黙の拒否アクションに注意してください。これをデフォルトの許可アクションに変更できます。[Save] をクリックして、コントラクトを作成します。

The screenshot shows the Cisco DNA Center interface with a notification banner at the top stating: "Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations". Below the navigation tabs (DESIGN, POLICY, PROVISION, ASSURANCE, PLATFORM), the 'POLICY' tab is active. Underneath, there are dropdown menus for 'Group-Based Access Control', 'IP Based Access Control', 'Application', 'Traffic Copy', and 'Virtual Network'. The main content area displays 'Access Contracts (8)' with a 'Refresh' button and a '+ Create Access Contract' button. A table lists the existing contracts:

Name	Description	Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0
AllowWeb	Sample contract to allow access to Web	2	No	1
Deny IP	Deny IP SGACL		No	3
Deny_IP_Log	Deny IP with logging		No	0
DenyRemoteServices	Sample contract to block Remote Access and telnet services	4	No	0

The screenshot shows the 'Create Access Contract' dialog box. The 'Name' field is filled with 'demo_access'. Below the table 'CONTRACT CONTENT (1)', the configuration is as follows:

#	Action	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Permit	http	TCP	Destination	80	<input type="checkbox"/>	+ X

At the bottom, the 'Default Action' is set to 'Permit' and the 'Logging' toggle is turned off. 'Cancel' and 'Save' buttons are located at the bottom right.

新しいコントラクトが作成されますが、まだ展開されていません。展開するには、新しいコントラクトのチェックボックスをクリックし、[Deploy] をクリックします。

This screenshot shows the Cisco DNA Center interface with a notification at the top: "Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations". Below the notification, the "Group-Based Access Control" section is active. The "Access Contracts (9)" table is displayed with the following data:

Name	Description	Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0
demo_access	Sample contract to allow access to Web	2	No	1
demo_access		1	No	0

This screenshot shows the same interface as above, but the "demo_access" contract is now selected, indicated by a blue checkmark in the first column. The "Actions" menu is open, and "Deploy" is selected. A "1 Selected" indicator is visible above the table.

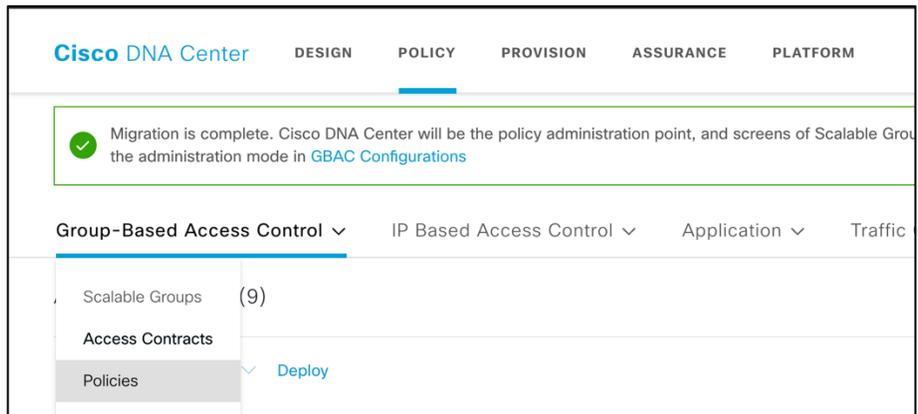
This screenshot shows the final state where the "demo_access" contract has been successfully deployed. The "Deployed" column now shows "Yes" for the "demo_access" contract, and the "Policies" column shows "0".

Name	Description	Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	Yes	0
AllowWeb	Sample contract to allow access to Web	2	Yes	1
demo_access		1	Yes	0

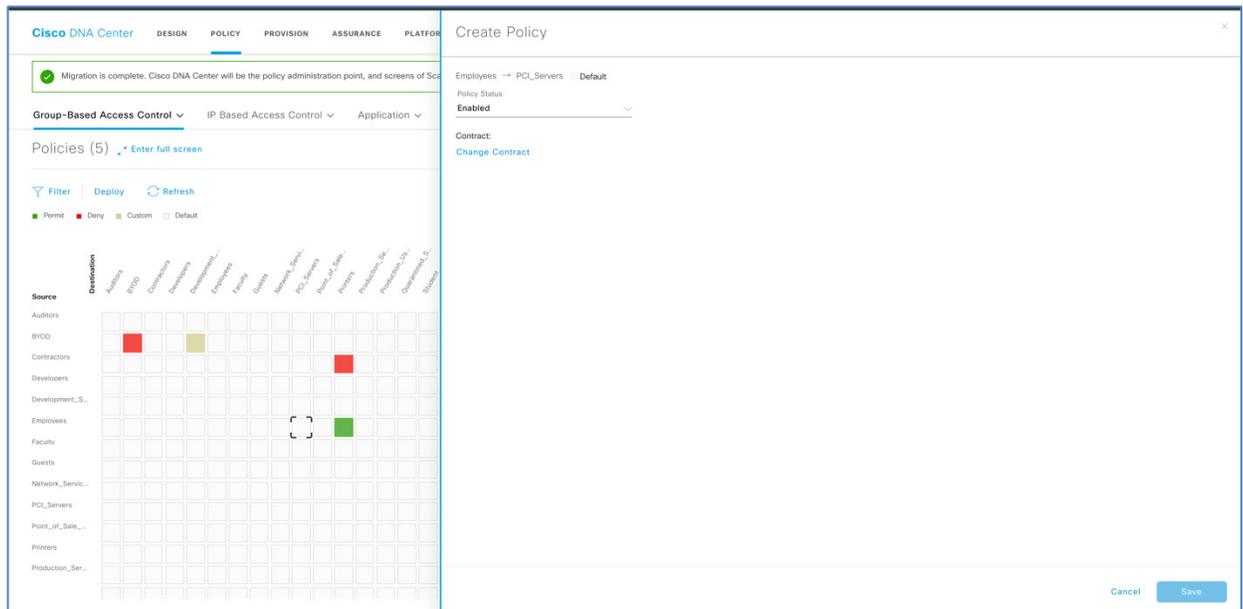
(注)

スクリーンショットは参考用です。コントラクトに自由に名前を付け、任意の許可アクションを割り当てできます。

ステップ 4 最後に、コントラクト（ステップ 3 で作成）を使用してグループベース アクセス ポリシーを作成し、スケーラブルグループをひも付けます。[Policy] > [Group-Based Access Control] > [Policies] に移動します。



ステップ 5 [Policy] に、送信元と宛先のスケーラブルグループを含むマトリックスが表示されます。スケーラブルグループの任意の組み合わせ（[Employees] > [PCI_Servers] など）をクリックします。



右側のペインで [Change Contract] をクリックし、前の手順で作成した「demo_access」コントラクトを選択します。これは、Employee と PCI_Servers 間のポリシーです。

< Edit Policy ×

Change Contract + Create Contract

Filter

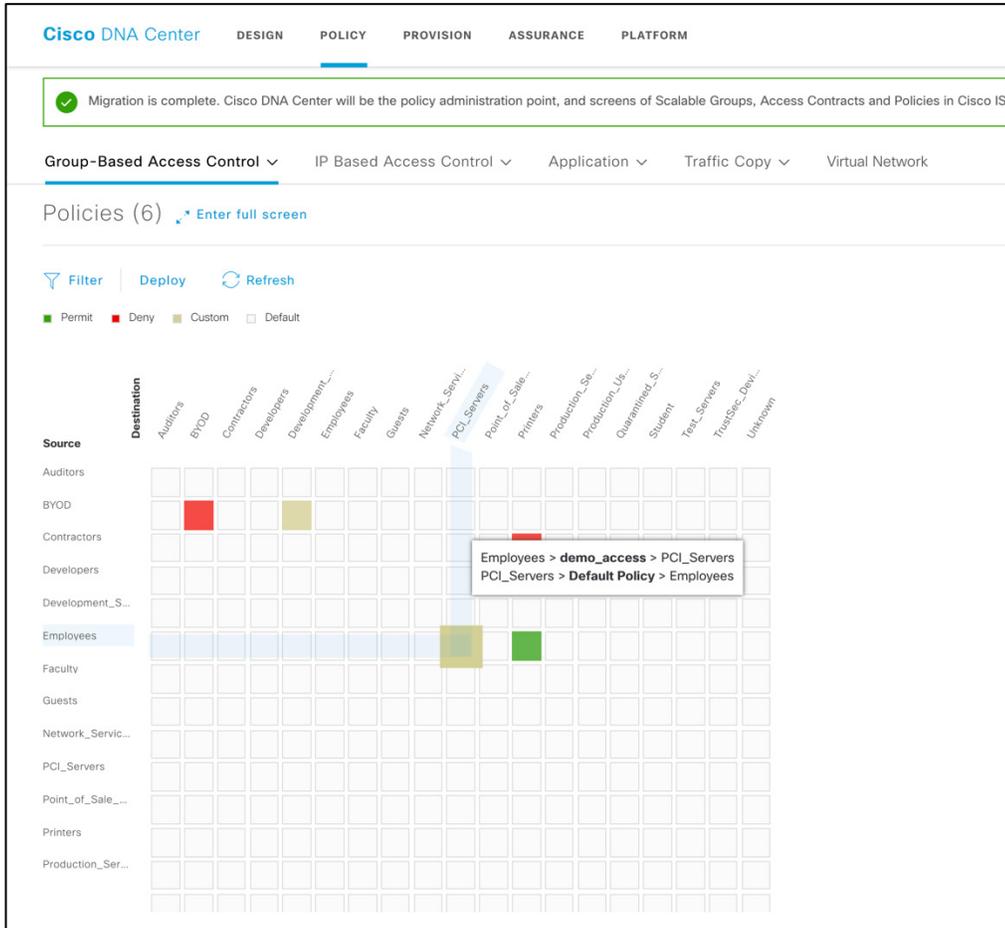
Name	Description	Policies Referencing
<input checked="" type="radio"/> demo_access		0
<input type="radio"/> Deny IP	Deny IP SGACL	3
<input type="radio"/> Deny_IP_Log	Deny IP with logging	0
<input type="radio"/> dfsfsd	dfsndfsdnf	0
<input type="radio"/> Permit IP	Permit IP SGACL	1
<input type="radio"/> Permit_IP_Log	Permit IP with logging	0
<input type="radio"/> AllowWeb	Sample contract to allow access to Web	1
<input type="radio"/> AllowDHCPDNS	Sample contract to allow DHCP and DNS	0
<input type="radio"/> DenyRemoteServices	Sample contract to block Remote Access and telnet services	0

Show 10 entries Showing 1 - 9 of 9 Previous 1 Next

Cancel Change

[Change] と [Save] をクリックして、このポリシーが適用されることを確認します。

ポリシーのマトリックページで、スケーラブルグループアクセスリストポリシーが作成されたことを確認します。



(注) 上のスクリーンショットは説明のみを目的としたものです。選択したスケーラブルグループに応じてポリシーを作成してください。

SD-Access オーバーレイのプロビジョニング

[Provision] セクションでは、ネットワークの設定を実際にデバイスにプッシュします。

デバイス (WLC) のプロビジョニング

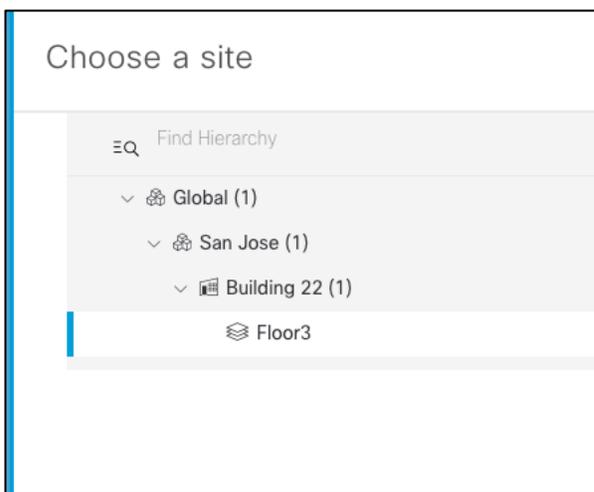
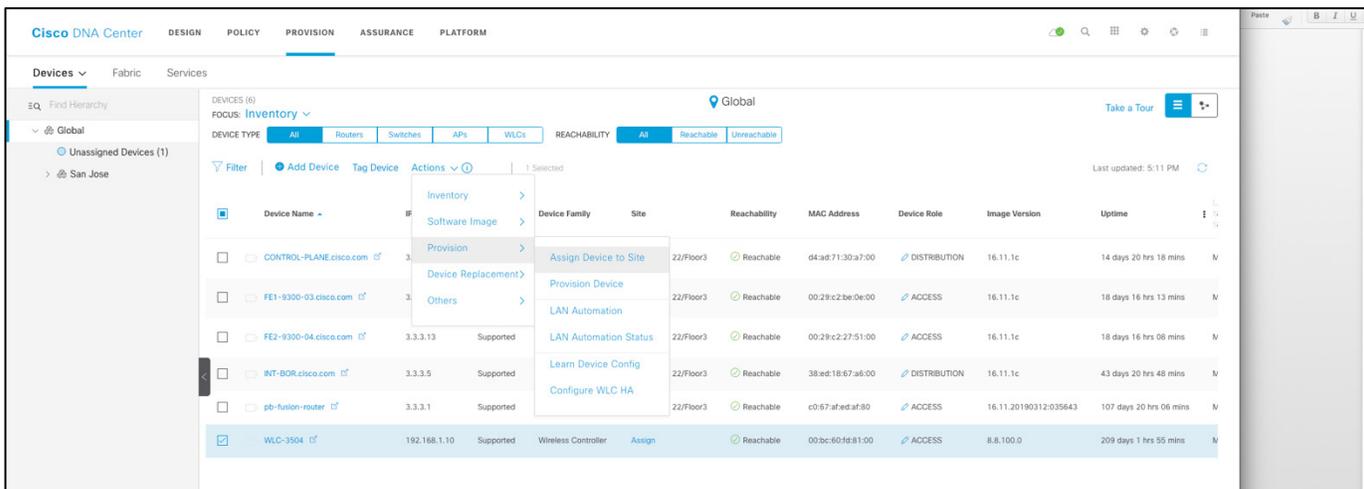
手順

ステップ 1 トップメニューから [Provision] タブを選択します。

WLC を選択し、設計フェーズで作成済みのサイトに関連付けて、プロビジョニングプロセスを開始します。

ステップ 2 1 回クリックして WLC を選択します。WLC を選択したら、[Actions] メニューをプルダウンして [Assign Device to Site] を選択し、WLC が物理的に設置されている場所に割り当てます。この手順は、物理的に配置されているサイトに対応する規制ドメインに WLC を割り当てる上で重要です。このサイトは、建物またはフロア、つまり座標を持つサイトである必要があります。

(注) 上のスクリーンショットは説明のみを目的としたものです。ご自身の WLC を選択してください。



(注) ステートフル スイッチオーバー ハイ アベイラビリティ (SSO HA) を設定する場合、2 番目の WLC は、この時点で同じサイトに追加する必要があります。次に、同じ [Device Inventory] ページから、プライマリとして設定する WLC をクリックし、[High Availability] タブに移動します。ここでは、プライマリとセカンダリの両方のコントローラの管理および冗長性管理情報を入力し、[OK] をクリックします。コントローラが再起動され、しばらくした後、インベントリ内の WLC が 1 つのみ表示されるようになります。今後、単一の WLC であるかのようにプロビジョニングを続行することができます。

WLC-3504 (192.168.1.10) ×

📶 Reachable Uptime: 209 days 1 hours 55 minutes

[Run Commands](#) | [View 360](#) | Last updated: 5:13 PM [Refresh](#)

Details | Interfaces | Wireless Info | Mobility

Device Name	WLC-3504	Location	Global/San Jose/Building 22/Floor3
Device Type	Wireless Controller	Reachability	Reachable
IP Address	192.168.1.10	Uptime	209 days 1 hours 55 minutes
Last Sync Status	Managed	Role	ACCESS
MAC Address	00:bc:60:fd:81:00		

INVENTORY

Serial Number	FCW2221M0JT	Resync Interval	6 hours
Last synced	3 hours ago	Series	Cisco 3500 Series Wireless LAN Controller
Platform	AIR-CT3504-K9		

SOFTWARE IMAGES

Software Image	Cisco Controller	Software Version	8.8.100.0
Image Series	-	Update Status	This image needs to be golden

PROVISION

Provision Status	Not Provisioned	Last Provisioned	-
Credential Status	Not Provisioned		

ステップ 3 WLC をサイトに追加したら、その WLC を選択して [Provision] をクリックします。

Cisco DNA Center DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices Fabric Services

Find Hierarchy

Global

Unassigned Devices

San Jose

DEVICES (8)
FOCUS: Inventory

DEVICE TYPE: All Routers Switches APs WLCs REACHABILITY: All Reachable Unreachable

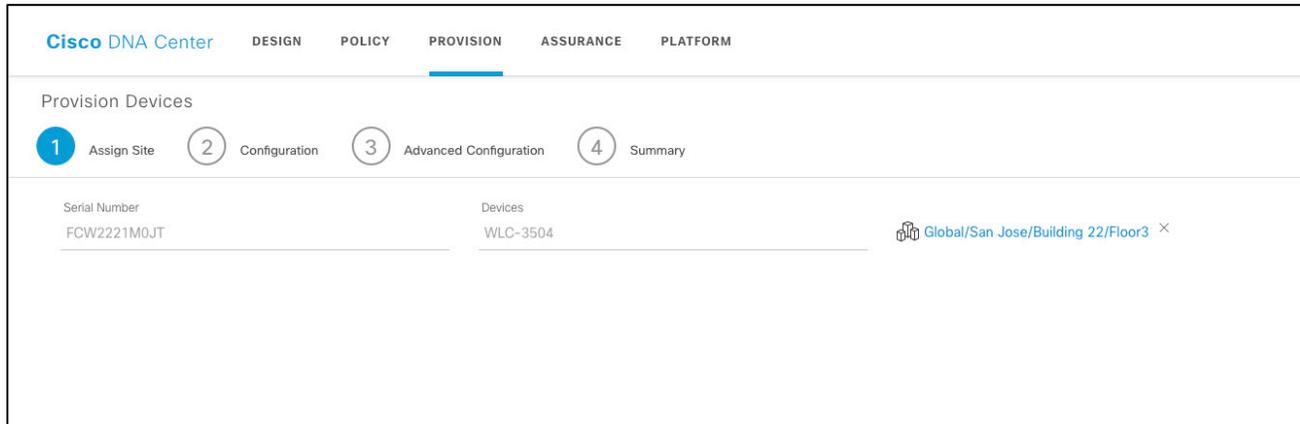
Filter Add Device Tag Device Actions 1 Selected

Device Name	Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime
CONTROL-PLANE.cisco.com	3	22/Floor3	Reachable	d4:ad:71:30:a7:00	DISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins
FE1-9300-03.cisco.com	3	22/Floor3	Reachable	00:29:c2:be:0e:00	ACCESS	16.11.1c	18 days 16 hrs 13 mins
FE2-9300-04.cisco.com	3.3.3.13 Supported	22/Floor3	Reachable	00:29:c2:27:51:00	ACCESS	16.11.1c	18 days 16 hrs 08 mins
INT-BDR.cisco.com	3.3.3.5 Supported	22/Floor3	Reachable	38:ed:18:67:a6:00	DISTRIBUTION	16.11.1c	43 days 20 hrs 48 mins
pb-fusion-router	3.3.3.1 Supported	22/Floor3	Reachable	c0:67:af:ed:af:80	ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins
WLC-3504	192.168.1.10 Supported	Wireless Controller .../Building 22/Floor3	Reachable	00:bc:60:fd:81:00	ACCESS	8.8.100.0	209 days 1 hrs 55 mins

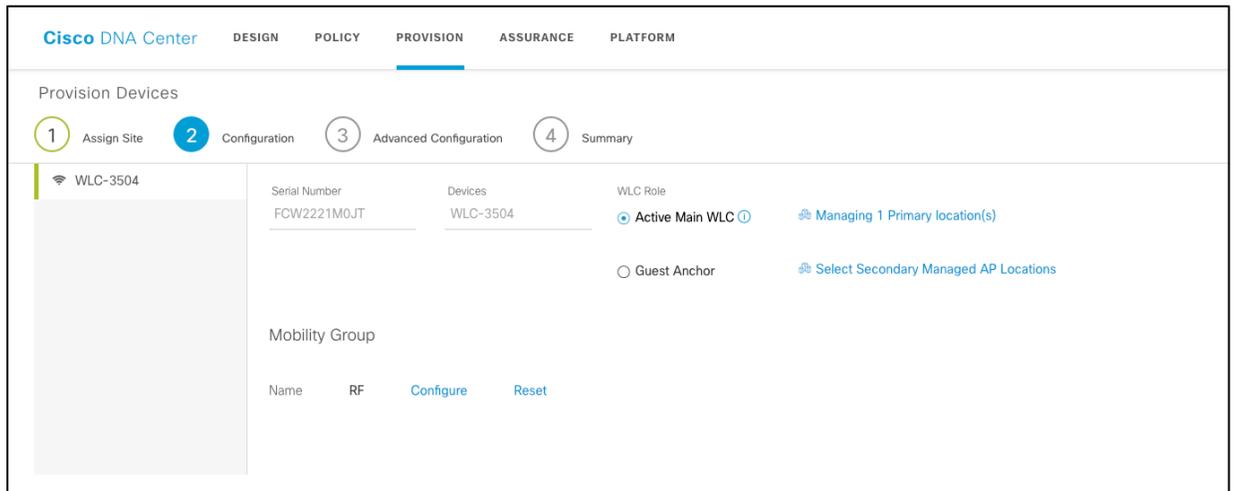
Inventory
Software Image
Provision
Device Replacement
Others

Assign Device to Site
Provision Device
LAN Automation
LAN Automation Status
Learn Device Config
Configure WLC HA

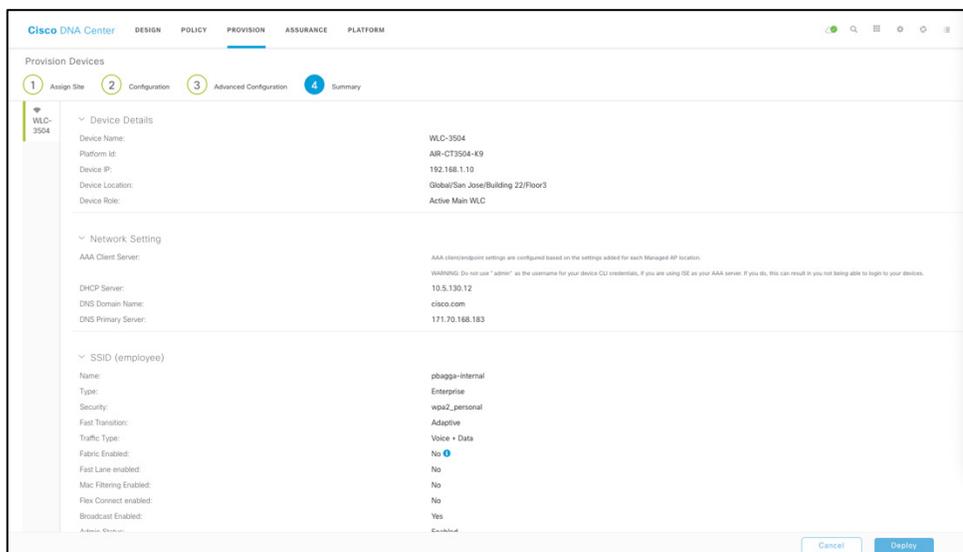
ステップ 4 WLC を配置する場所を選択します。Syslog/SNMP や NTP などのネットワークプロファイルで定義された設定が WLC にプッシュされます。



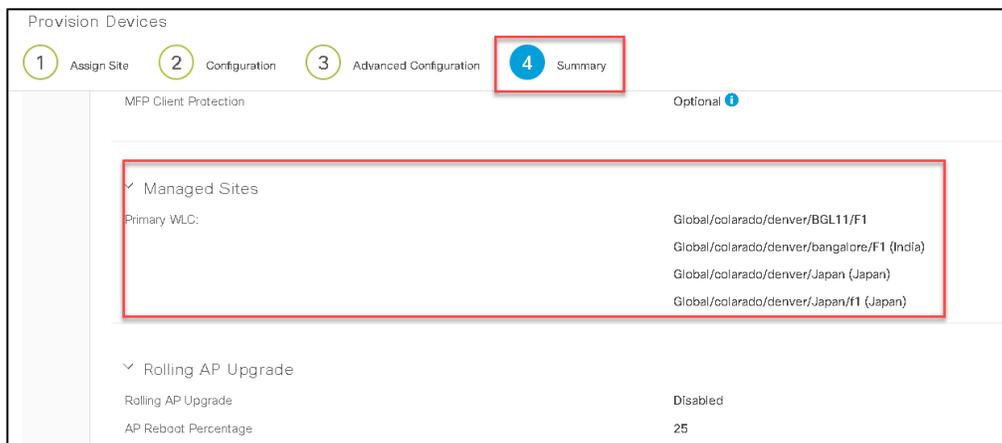
ステップ 5 この WLC で管理される AP ロケーションを選択します。存在する場合、AP が導入されるフロアを選択することが重要です。[Next] をクリックします。



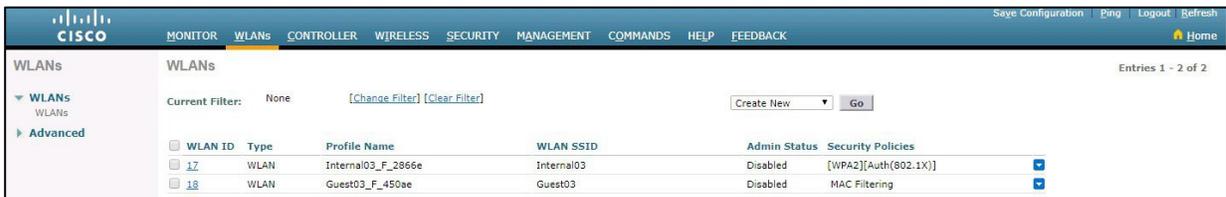
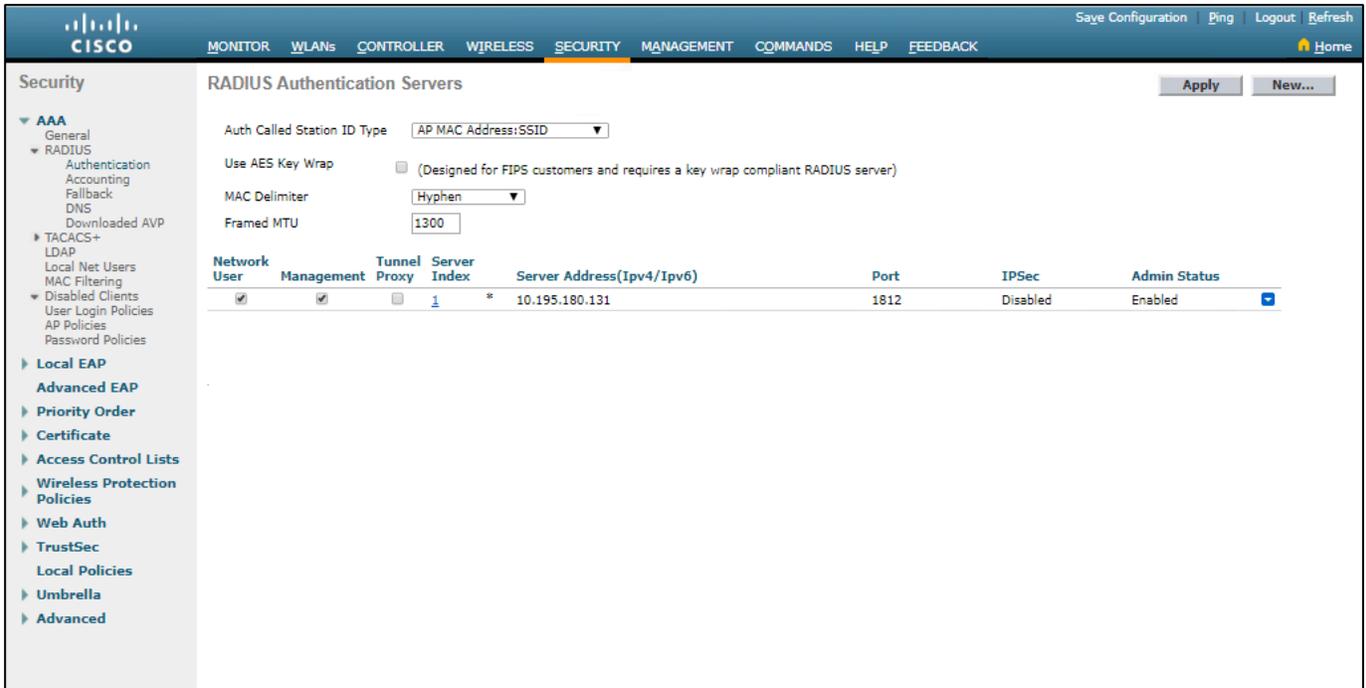
ステップ 6 Cisco DNA Center から WLC プロビジョニングの一環としてプッシュされる設定（システム詳細や、認証、許可、およびアカウントिंग（AAA）、DHCP、DNS サーバ、SSID および管理サイトのグローバル設定）を確認します。[Deploy] をクリックします。



(注) WLC の国コードは、アクセスポイントがマッピングされている地域に基づいて選択されます。たとえば、WLC がインドと米国の地域にマッピングされたアクセスポイントを管理している場合、DNAC によってプッシュされる国コードは「US、IN」です。国コードは建物にマッピングされ、その下のフロアは国コードを建物から継承します。Cisco DNA Center によって WLC にプッシュされる国コードについては、次のスクリーンショットを参照してください。



ステップ 6 Cisco DNA Center を使用してプッシュされる設定 (RADIUS サーバが認証やアカウントングで使用する設定など) は、WLC で表示できます。2 つの WLAN が作成されていて、ID は 17 より大きく、ステータスは無効に設定されていて、各サイトに 1 つ WLAN が関連付けられています。ホストオンボーディングを設定して SSID にプールを割り当てるまで、WLAN は無効状態になります。



Cisco Catalyst 9800 WLC のスクリーンショット :

```

-9800-1#sh wlan summary
Number of WLANs: 3
ID  Profile Name                SSID                Status Security
-----
17  sand-site2_Sanjos_F_c2d2d249 sand-site2-1x      DOWN  [WPA2][802.1x][AES]
18  sand-mac-s_Global_F_183f26d4 sand-mac-site2     DOWN  [open]
19  sand-nonfa_Sanjos_NF_584c9d37 sand-nonfabric     DOWN  [WPA2][802.1x][AES]

```

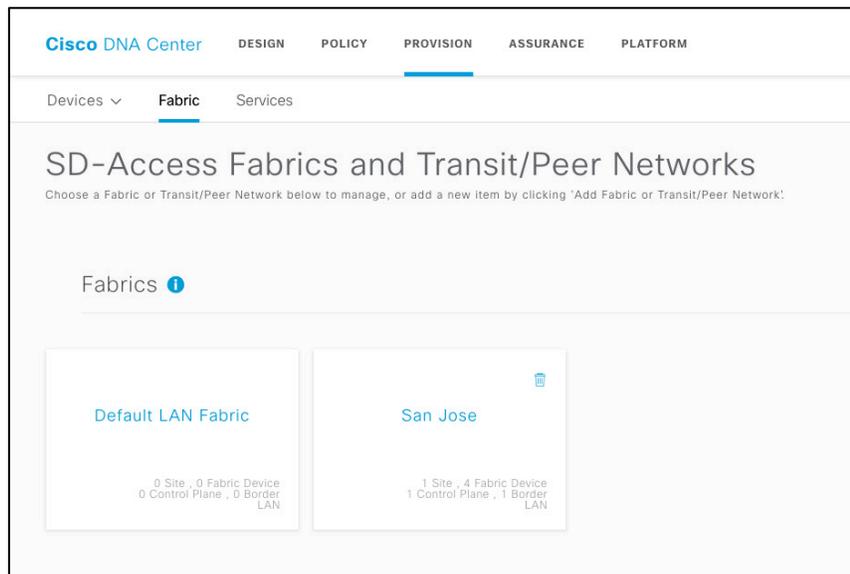
(注) 上のスクリーンショットは説明のみを目的としたものです。ご自身のネットワークに関連する設定 (IP アドレスと名前) が WLC で表示されるのを確認できます。

これで、Cisco DNA Center はサイト内のどこにデバイスがあるのかを認識するので、ファブリック プロビジョニングを開始できます。

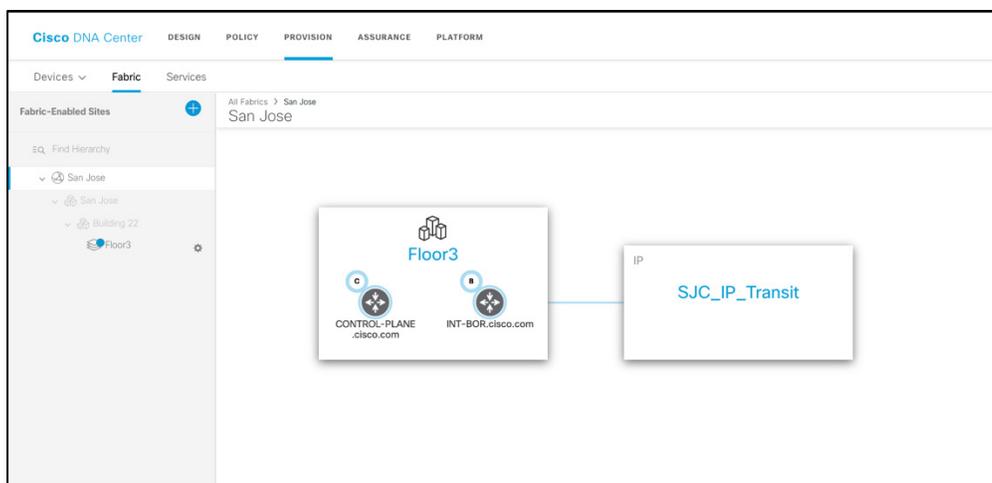
ファブリックの作成

手順

- ステップ 1** メニューから [Fabric] を選択します。SD-Access ファブリックを作成、管理するための新しいページが表示されます。
- ステップ 2** 新しいファブリックを作成するか、[Default LAN Fabric] をクリックします。次の例では、San Jose という新しいファブリックを作成しました。



San Jose ファブリックで、[Floor 3] をクリックします。



- ステップ 3** [Select Devices] をクリックし、ノードをファブリックに追加します。デバイスをファブリックに追加するには、WLC-3504 をクリックし、[Wireless] オプションボタンを選択して WLC をファブリックに追加します。[Add] をクリックします。

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Devices Fabric Services

Fabric-Enabled Sites + All Fabrics > Floor3 San Jose

EQ Find Hierarchy

San Jose
San Jose
Building 22
Floor3

EQ Find by device IP, type, role, family & MAC

Fabric Infrastructure Host Onboarding Show Task Status

1 Authentication on Extended Node and Critical VLAN features are not yet enabled. Do you want to enable those features? Enable Authentication on Extended Node and Critical VLAN.

Collapse All Custom View Mar 12, 2020 5:33 PM

WLC-3504

Cancel Save

WLC-3504 (192.168.1.10)

Reachable Uptime: 209 days 5 hours 7 minutes

Run Commands View 360 Last updated: 5:34 PM Refresh

Details Fabric Port Channel Interfaces Wireless Info Mobility

Remove From Fabric

Fabric

Wireless

Cancel Add

WLC-3504 (192.168.1.10)

Reachable Uptime: 209 days 5 hours 7 minutes

Run Commands View 360 Last updated: 5:34 PM Refresh

Details Fabric Port Channel Interfaces Wireless Info Mobility

Remove From Fabric

Fabric

Wireless

Cancel Add

[Save] と [Apply] をクリックして設定を WLC にプッシュし、WLC をファブリックに含めます。

WLC-3504

Cancel Save

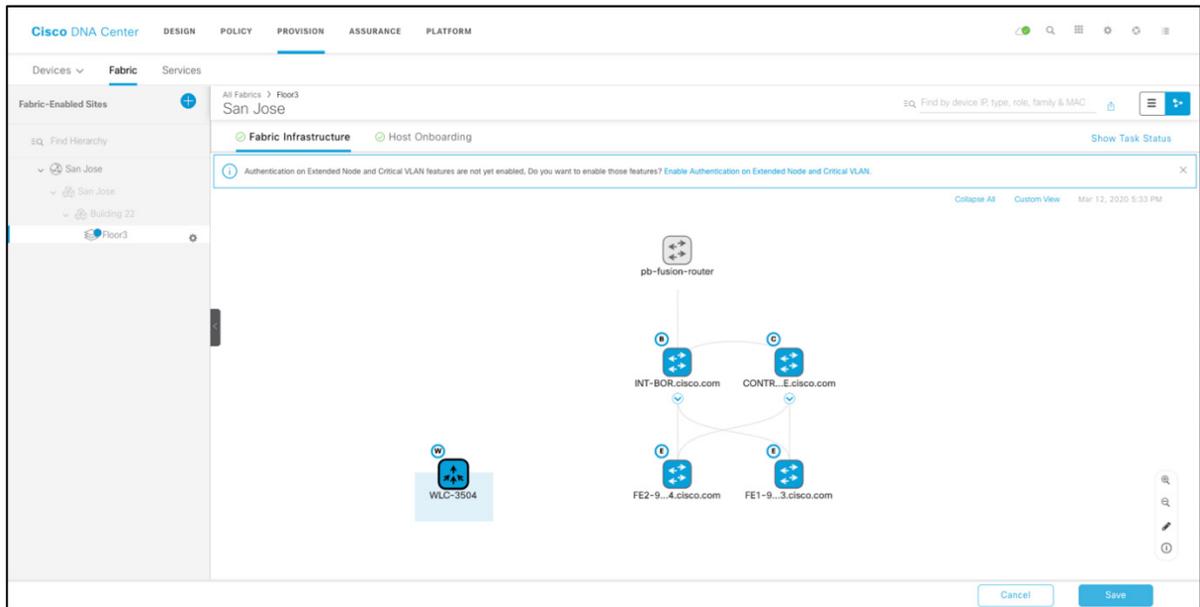
Modify Fabric Domain

When

Now Later

Cancel Apply

ステップ 4 次の例のようにデバイスがファブリックに追加されると、色がグレーから青に変化します。



(注) 上のスクリーンショットは説明のみを目的としたものです。ファブリックには複数のノードを設定できます。

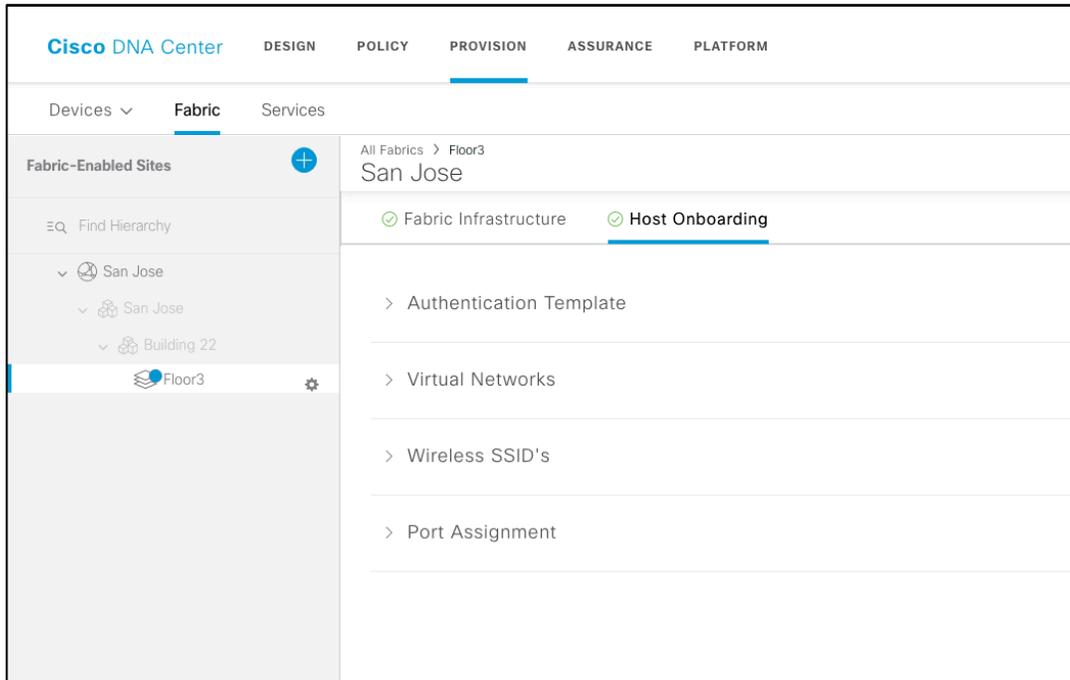
AP およびホストオンボーディング

このガイドでは、ファブリック有線ネットワークがすでにプロビジョニングされていることが前提となっているため、WLCを追加した後は、APとワイヤレスクライアントをオンボーディングする必要があります。そのため、IPアドレスプールを追加し、ファブリック内での通信にAPとワイヤレスホストを有効にする必要があります。SD-AccessにIPプールを設定すると、Cisco DNA Centerはすぐに各エッジノードに接続し、ホストが通信できるように適切なスイッチ仮想インターフェイス (SVI) を作成します。

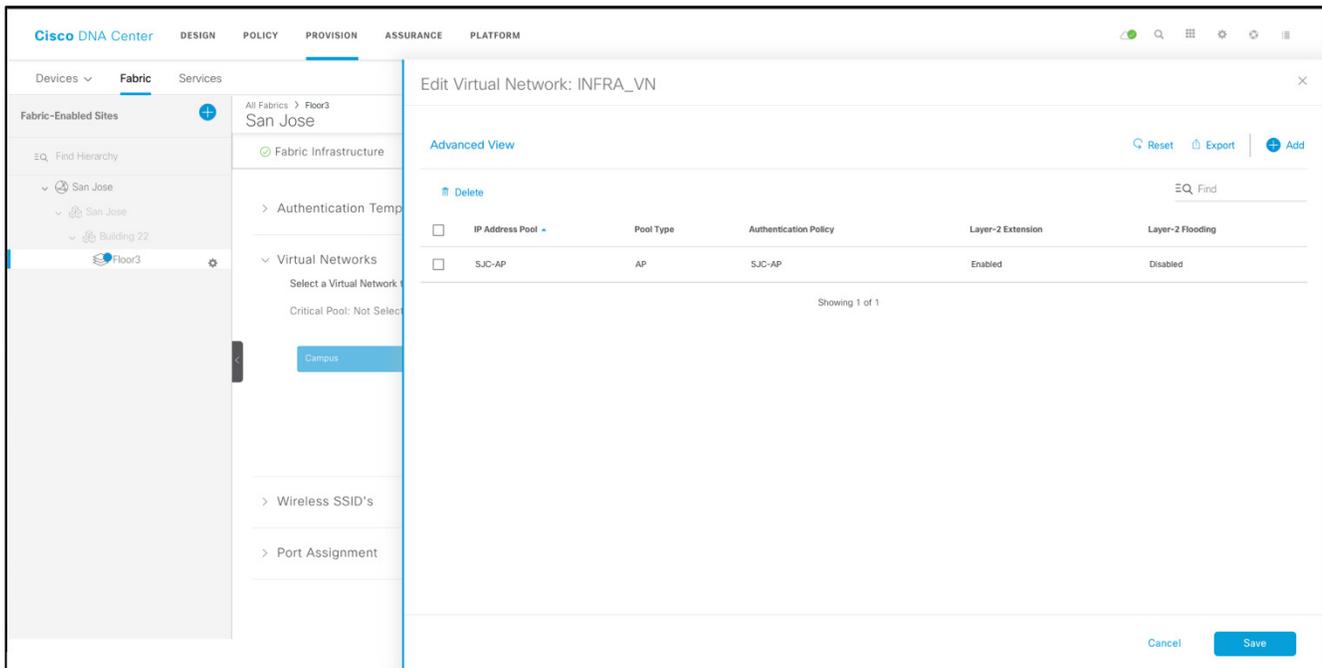
また、エニーキャストゲートウェイがすべてのエッジノードに適用されます。ホストが追加のプロビジョニングを行わずに、どのエッジノードにもローミングが簡単にできるため、これはSD-Accessの不可欠な要素です。

手順

ステップ 1 この画面の上部の [Host Onboarding] をクリックして、APおよびクライアントデバイスのIPプールの有効化を開始します。



ステップ 2 [Virtual Networks] で [INFRA VN] をクリックすると、アドレスプールが設定済みのウィンドウが開きます。AP のアドレス プールを選択します。この VN に対して AP プロビジョニングとレイヤ 2 拡張機能がすでにオンになっていることに注意してください。どちらも AP をオンボードするために必要です。[Save] をクリックします。



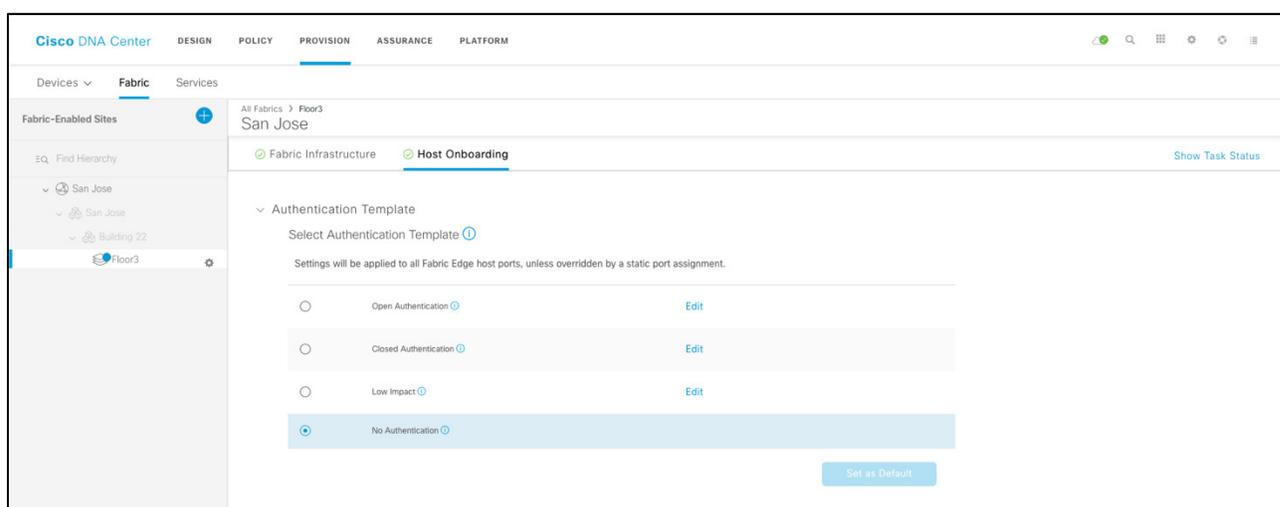
レイヤ 2 拡張機能の設定により、レイヤ 2 LISP を有効にし、レイヤ 2 VNID をこのプールに関連付けることで、イーサネットフレームをファブリック上にエンドツーエンドで伝送できます。これにより、レイヤ 2 ストレッチ済みサブネットサービスのシミュレートが可能になります。

[AP Provision Pool] を選択すると、すべてのエッジノードスイッチに設定マクロが自動的にプッシュされます。そのため、AP が直接接続されている場合、スイッチは Cisco Discovery Protocol を介して AP であることを認識し、そのポートにマクロが自動的に適用され、プールに関連付けられた適切な VLAN に物理ポートが割り当てられます。

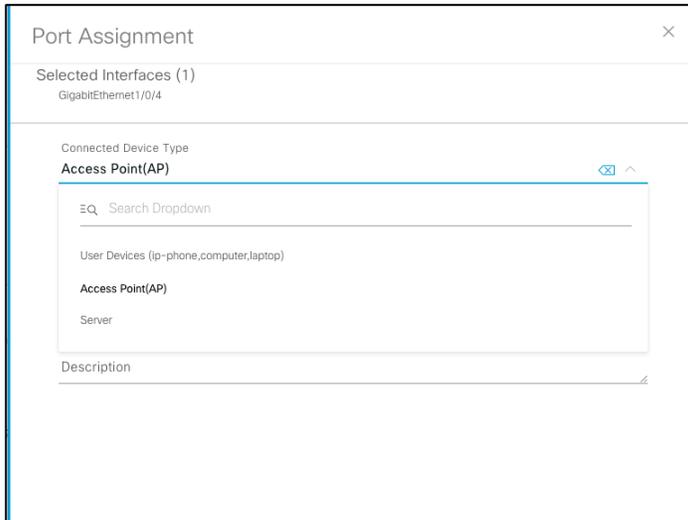
ポートに対して [No Authentication] テンプレートを選択した**場合にのみ**、AP オンボーディングの FE で CDP マクロがプッシュされます。

Cisco DNA Center 1.2.x では、ファブリックエッジ (FE) に接続されたデバイスを AP として識別するためにマクロが使用されていました。マクロがデバイスをシスコのアクセスポイントとして検出すると、関連する設定がそのポートにプロビジョニングされます。

Cisco DNA Center 1.3.x では、デバイスをシスコのアクセスポイントとして識別するために Autoconf が使用されるため、ポートに適切な設定がプロビジョニングされます。次の例は、[No Authentication] モードに設定されたポートを示しています。アクセスポイントは、クローズド認証ポートに接続できます。クローズド認証モードでアクセスポイントをオンボードする方法の詳細については、次の項で説明します。Autoconf は、デバイス分類子を使用して、ポートに接続されているエンドデバイスを識別します。



[Port Assignment] セクションで、AP に接続されているポートを選択し、[Connected Device Type] として [Access Point (AP)] を選択します。



この時点では、AP は適切な VLAN またはサブネットに割り当てられ、指定されたプールから IP アドレスを取得し、標準のメカニズム（プラグアンドプレイ、DHCP オプション 43、DNS など）のいずれかを使用して WLC を検出します。その後、AP が WLC に接続されます。

クローズド認証による AP オンボーディング

この項では、ユーザがクローズド認証モードを理解していることを前提としています。DNAC 1.3.3 の SD-Access ファブリックは、dot1x の優先順位が最も高く、次にマシン認証バイパス（MAB）が続く、クローズド認証モードをサポートします。すぐに使用できるアクセスポイントでは、dot1x サブリカントが有効になっておらず、ファブリックエッジで認証するためのログイン情報がプロビジョニングされていません。クローズド認証で AP をオンボードするために使用される主な機能の 1 つに、Identity Services Engine（ISE）のプロファイリング機能があります。

このプロファイリング機能により、ISE はエンドポイントの ID を識別し、プロファイリング後に適切な認証プロファイルを割り当てることができます。

プロファイリングの詳細については、コミュニティページのガイドを参照してください。

[ISE Profiling Design Guide](#)

Cisco DNA Center により、ファブリックデバイスのプロファイリング設定が自動化されます。ファブリックデバイスにプッシュされるプロファイリング設定の例を次に示します。

```

device-sensor filter-list cdp list iseCDP
tlv name device-name
tlv name capabilities-type
tlv name version-type
tlv name platform-type
!
device-sensor filter-list dhcp list iseDHCP
option name host-name
option name parameter-request-list
option name class-identifier
!
device-sensor filter-list lldp list iseLLDP
tlv name system-name
tlv name system-description
tlv name system-capabilities
device-sensor filter-spec dhcp include list iseDHCP
device-sensor filter-spec lldp include list iseLLDP
device-sensor filter-spec cdp include list iseCDP
device-sensor notify all-changes

```

Cisco DNA Center により、ファブリックエッジ上のテンプレートが自動化されます。このテンプレートは、Identity Services Engine でアクセスポイントがプロファイリングされた後、属性として返される必要があります。

```

template ApAutzTemplate
switchport access vlan 2045
switchport mode access
access-session interface-template sticky timer 10
!

```

クロード認証の AP オンボーディングフローについて説明します。

ステップ 1：AP がクロード認証用に設定されたファブリックエッジのポートに接続します。AP は dot1x メッセージに回答できず、ファブリックエッジは MAB にフォールバックします。

MAB を使用したアクセスポイントの初期認証：

The screenshot shows the Cisco ISE Administration console. The 'Policy Elements' tab is active, displaying a table with columns for Status, Rule Name, and Conditions. A rule named 'wired_MAB' is highlighted in yellow. The conditions for this rule are 'Normalised Radius: RadiusFlowType EQUALS WiredMAB'. There are also buttons for 'PermitAccess' and 'Auto create security group'.

May 03, 2020 12:37:21.973 PM	●	🔒	0	ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	✓	🔒		ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	✓	🔒		ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:28.569 PM	✓	🔒		78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	✓	🔒		78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	✓	🔒			78.72.5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	✓	🔒		78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM	✓	🔒			78.72.5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	✓	🔒		78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A		Default >> MAB	Default >> wired_MAB	PermitAccess

ステップ 2 : MAB を使用してポートが承認されたら、Identity Services Engine はエンドポイントをプロファイリングし、アクセスポイントとして分類します。

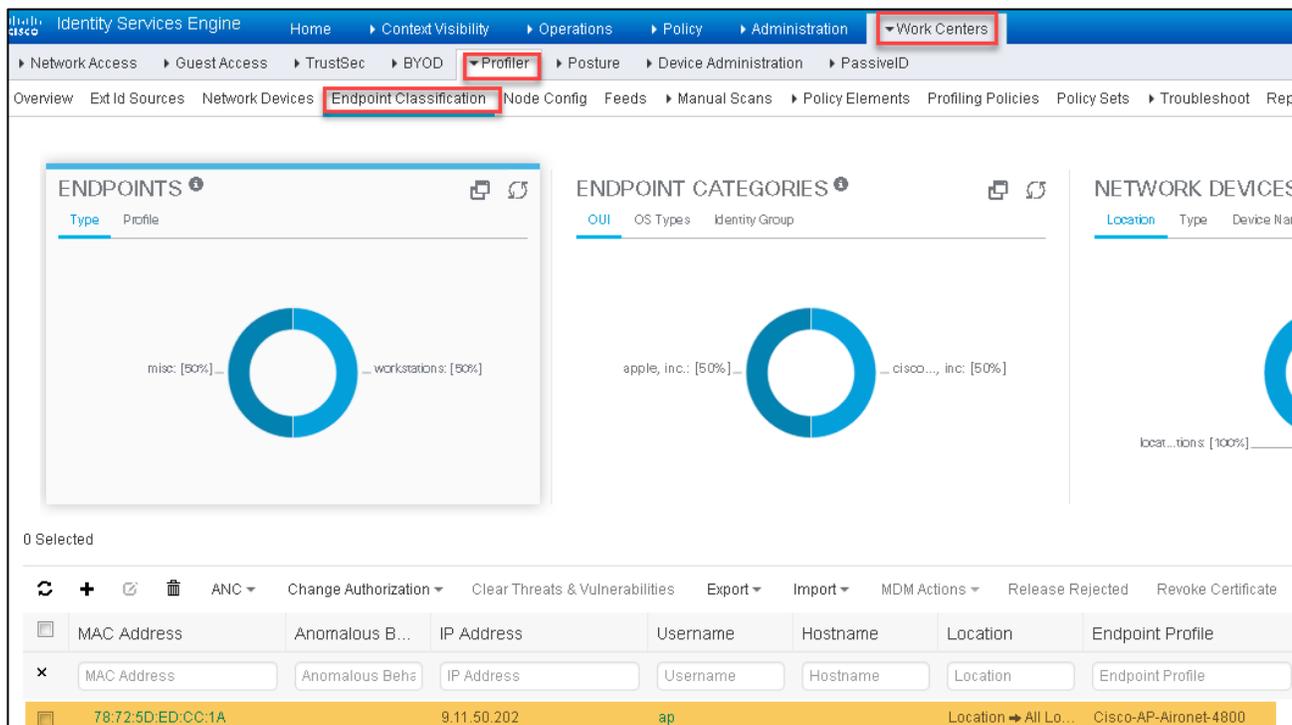
ISE はファブリックエッジへの COA を開始します。ファブリックエッジが認証プロセスを再開します。

これらの手順は、以下の ISE ポリシーログで強調表示されています。ファブリックエッジは、RADIUS アカウンティングパケットを使用してプロファイリング情報を Identity Services Engine に送信します。

ISE のポリシーセット :



ISE のプロファイリング情報 :



ファブリックエッジによって Identity Services Engine (ISE) に送信されるプロファイリングデータ :

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Profiler > Endpoint Classification. The specific endpoint being viewed is 78:72:5D:ED:CC:1A. The interface shows the following details:

- MAC Address: 78:72:5D:ED:CC:1A
- Username: ap
- Endpoint Profile: Cisco-AP-Aironet-4800
- Current IP Address: 9.11.50.202
- Location: Location → All Locations

The 'Attributes' tab is selected, showing the following data:

General Attributes	
Description	
Static Assignment	false
Endpoint Policy	Cisco-AP-Aironet-4800
Static Group Assignment	false
Identity Group Assignment	Profiled

Other Attributes	
OUI	Cisco Systems, Inc
cdpCachePlatform	cisco AIR-AP4800-A-K9
cdpCacheVersion	Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/techsupport/14-2015 by Cisco Systems, Inc.
lldpSystemDescription	Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/techsupport/86-2019 by Cisco Systems, Inc. Compiled Sun Dec 15 03:23:03 PST 2019 by vipendya

アクセスポイントの認証プロファイル :

Authorization Profiles > Ap_template_return_1

Authorization Profile

* Name: Ap_template_return_1

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

MACSec Policy

NEAT

Interface Template: ApAutzTemplate

Web Authentication (Local Web Auth)

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=ApAutzTemplate

ISE COA および後続の再認証 :

May 03, 2020 12:37:21.973 PM			0	ap1234	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM				ap1234	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM				ap1234	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:28.569 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.444 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A		Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.052 PM				78.72.5D.ED.CC:1A	78.72.5D.ED.CC:1A		Default >> MAB	Default >> wired_MAB	PermitAccess

ステップ 3 : MAB を使用して再認証した AP が、オプション 43 を使用して Cisco Wireless LAN Controller (WLC) に接続します。WLC には、アクセスポイントで dot1x サプリカントを有効にするための関連設定があります。アクセスポイントで dot1x 設定を有効にする方法の詳細については、次の URL を参照してください。WLC の設定を有効にするには、WLC にログインするか、Cisco DNA Center のテンプレートを使用します。

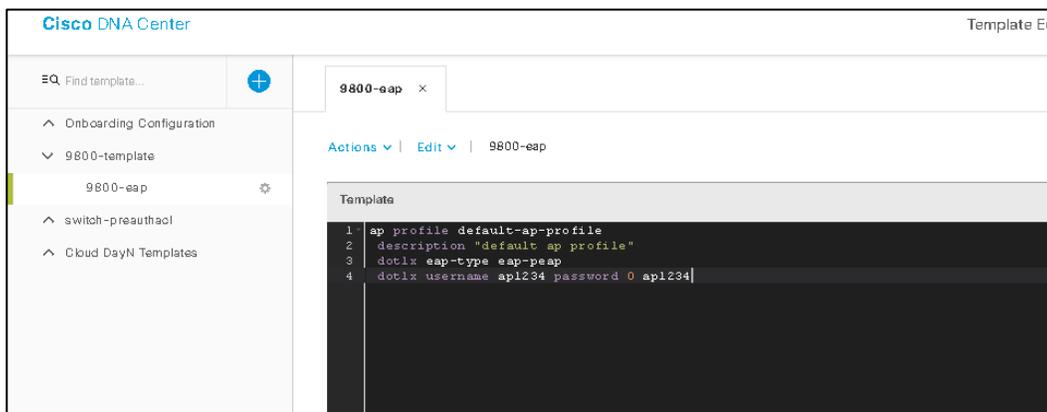
AIRE-OS ベースのワイヤレス LAN コントローラにおける dot1x の有効化 :

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_802_1x_cap_supPLICANT_on_cos_ap.html

Catalyst 9800 ワイヤレス LAN コントローラにおける dot1x の有効化 :

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-1x-support.html

Catalyst 9800 ワイヤレス LAN コントローラのサンプルテンプレートのスクリーンショットを次に示します。このテンプレートは説明を目的としたものです。必要に応じてテンプレートを書き換え、変更してください。



ステップ 4 : アクセスポイントがリセットされ、dot1x サブリカントが有効になり、ISE で認証されます。承認の一環として、ISE はファブリックエッジのテンプレート「ApAutzTemplate」を返し、適切なテンプレートをポートに割り当てます。

dot1x サブリカントが有効になった AP のリセットと ISE での認証 :

May 03, 2020 12:37:21.973 PM			0	ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1	
May 03, 2020 12:37:21.957 PM				ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1	
May 03, 2020 12:37:21.908 PM				ap1234	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling		
May 03, 2020 12:35:28.569 PM					78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM					78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM						78.72.5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM					78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM						78.72.5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM					78.72.5D:ED:CC:1A	78.72.5D:ED:CC:1A		Default >> wired_MAB		PermitAccess

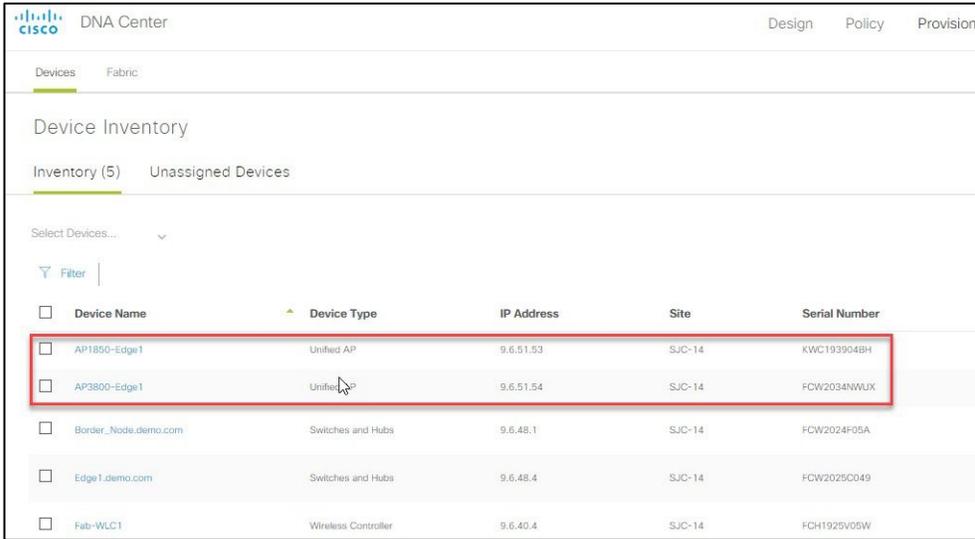
(注) プロファイリングを必要な精度で行うには、Identity Services Engine でプロファイラフィードを最新に更新する必要があります。EAP-FAST または PEAP の場合、アクセスポイントで使用するログイン情報を Identity Services Engine (ISE) で設定する必要があります。EAP-TLS の場合、AP に証明書をプッシュする必要があります。アクセスポイントに証明書をプッシュする方法については、ステップ 3 の URL を参照してください。

AP のプロビジョニング

これで AP は IP アドレスを取得し、WLC の管理 IP アドレスを学習したため、AP は、WLC に接続されます。もちろん、これは AP と WLC の間に IP 接続があることを前提としています（これは本書の対象から外れ、WLC が接続されている場所に依存し、通常はファブリックの外にあります）。AP は、WLC に登録されると、Cisco DNA Center の [Inventory] ページに表示されます。

手順

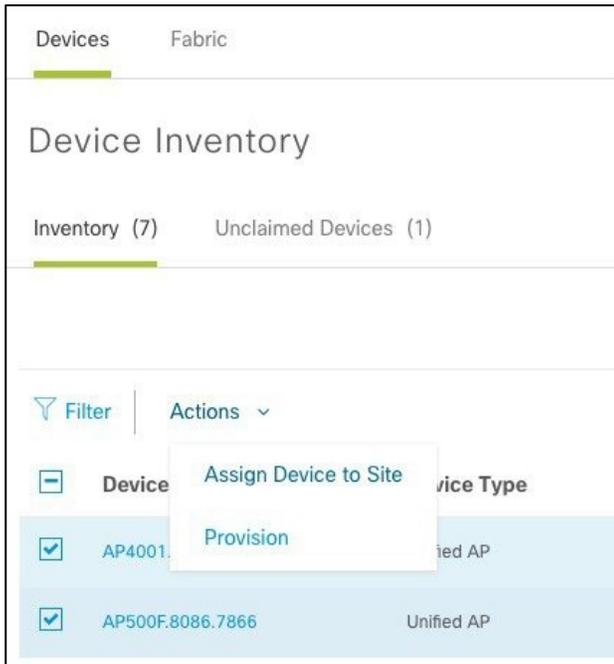
ステップ 1 [Provision] > [Devices] > [Inventory] に戻ると、ファブリック対応のワイヤレスコントローラに参加している AP が表示されます。



Device Name	Device Type	IP Address	Site	Serial Number
AP1850-Edge1	Unified AP	9.6.51.53	SJC-14	KWC193904BH
AP3800-Edge1	Unified AP	9.6.51.54	SJC-14	FCW2034NWUX
Border_Node.demo.com	Switches and Hubs	9.6.48.1	SJC-14	FCW2024F05A
Edge1.demo.com	Switches and Hubs	9.6.48.4	SJC-14	FCW2025C049
Fab-WLC1	Wireless Controller	9.6.40.4	SJC-14	FCH1925V05W

(注) 上のスクリーンショットは説明のみを目的としたものです。ご使用の設定では、別の 802.11ac Wave 2 アクセスポイントモデルの場合があります。

ステップ 2 次の例のように、[Device] 一覧から 1 つ以上の AP を選択し、[Assign Device to Site] を選択します。

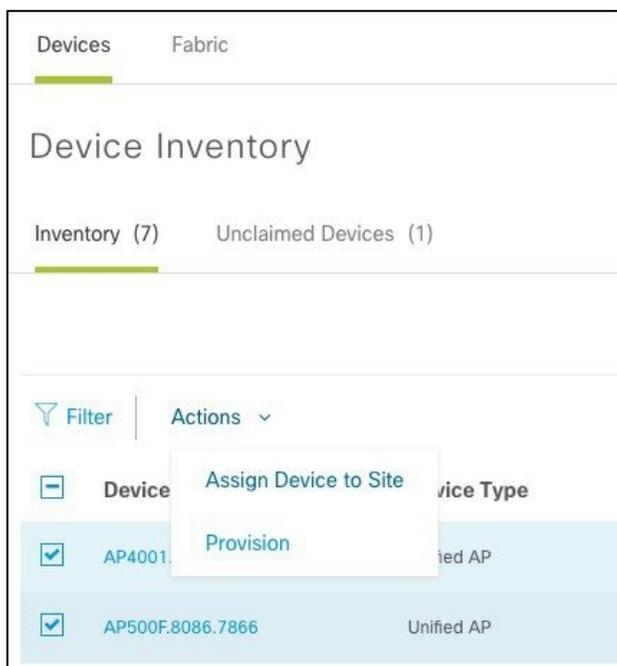


Device	Device Type
AP4001	Unified AP
AP500F.8086.7866	Unified AP

APが配置されるフロアを選択し、[Assign] をクリックします。APが登録されているWLCが、そのフロアを管理するためにプロビジョニングされていることを確認します。フロアが後に追加された場合は、戻って、WLCをもう一度プロビジョニングし、特定のフロアを追加できます。



ステップ 3 次の例のように、[Device] 一覧から 1 つ以上の AP を選択してプロビジョニングします。今回は、[Actions] メニューから [Provision] を選択します。



フロアを選択するか、または、すでに選択されている場合、[Next] をクリックします。

(注) サイトをすべてのデバイスにマッピングするには、[Apply to All] を選択します。

ステップ 4 AP の RF プロファイルとして [High]、[Typical]、[Low] のいずれかを選択するか、または以前に定義されたカスタマイズされたものを選択します。下記の例では、[Typical] を選択して [Next] をクリックしています。

Serial Number	Device Name	RF Profile
FDW2130B3L2	AP4001.7A70.6004	TYPICAL
FDW2130B3KR	AP500F.8086.7866	TYPICAL

Apply to All

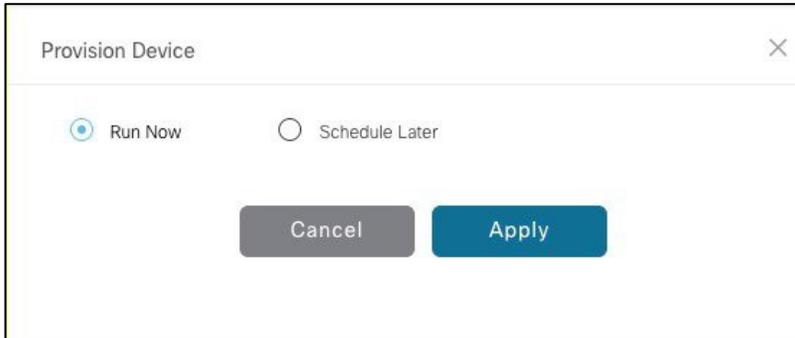
ステップ 5 [Deploy] をクリックすると、AP プロビジョニングの一環として、設定は次のように AP にプッシュされます。AP は再起動し、WLC に再度参加します。

Device Details

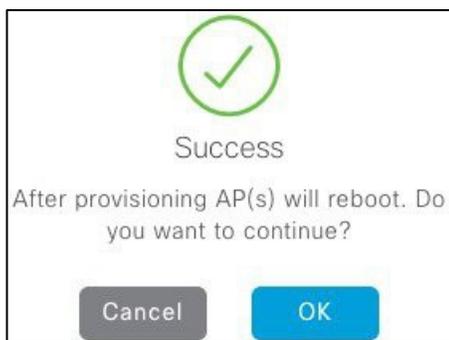
Device Name:	AP4001.7A70.6004
Serial Number:	FDW2130B3L2
Mac Address:	70:70:8b:20:29:00
Device Location:	Floor-1
RF Profile:	TYPICAL
Radio Type:	2.4GHz/5GHz
Channel Width:	20 MHz
2.4GHz/5GHz Data Rates:	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

Cancel Deploy

ポップアップ表示されるウィンドウで [Run Now] をクリックします。



AP が再起動されることを警告するメッセージが表示されます。OK をクリックします。



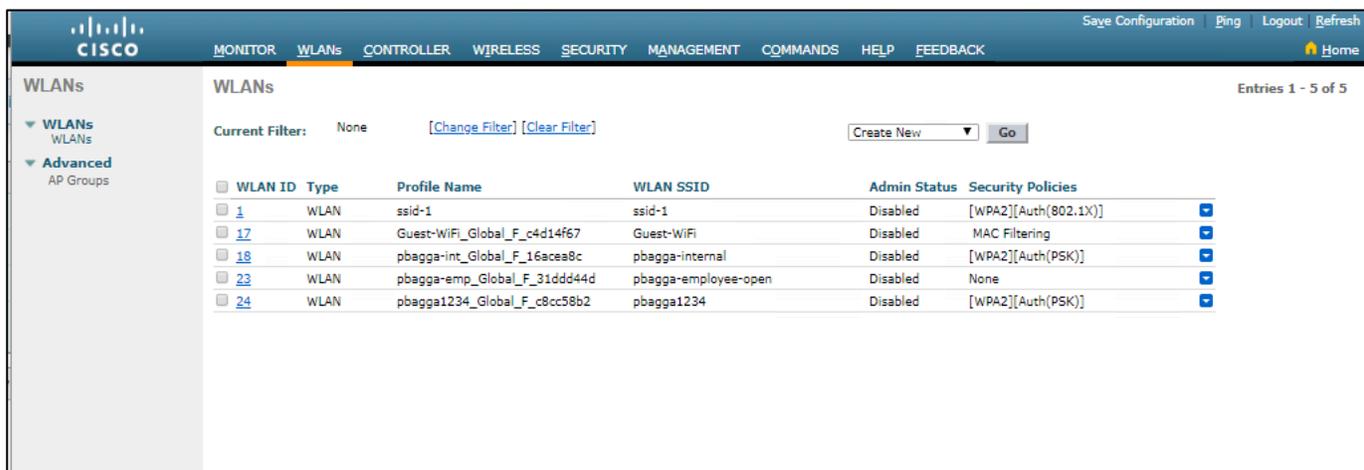
ステップ 6 AP の [Provision Status] が [Success] と表示されます。

<input type="checkbox"/>	Device Name	Device Type	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
<input type="checkbox"/>	AP4001.7A70.6004	Unified AP	172.16.3.131	...loor-1/Diegem	FDW2130B3L2	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success
<input type="checkbox"/>	AP500F8066.7866	Unified AP	172.16.3.130	...loor-1/Diegem	FDW2130B3KR	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success

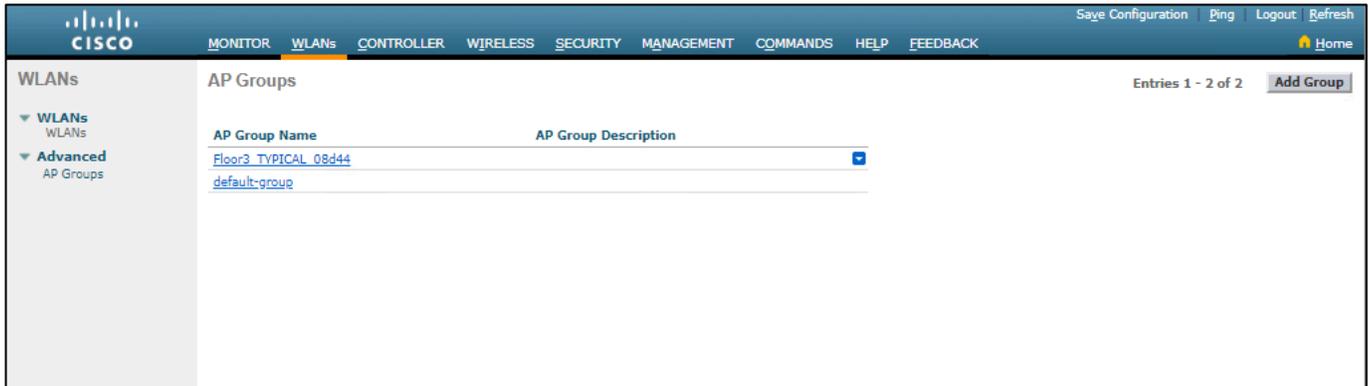
(注) 上のスクリーンショットは説明のみを目的としたものです。AP 導入の詳細については、ご使用の設定では異なる場合があります。

ステップ 7 AP プロビジョニングの一環として、一部の設定は WLC にプッシュされます。

AP グループは、マッピング先のサイト（前述の手順 3）の名前を付けて作成されます。



下記の例では、AP と WLAN はこの AP グループに含まれています。



Catalyst 9800 WLC の場合は、アクセスポイントに 3 つのタグが割り当てられます。

サイトタグ：サイトタグには、CAPWAP タイマー、AP ユーザ名、パスワードなどの AP 接続プロファイルの特性が含まれています。

RF タグ：RF タグには、割り当てられた RF プロファイルの特性が含まれています。

ポリシータグ：ポリシータグには、WLAN およびポリシープロファイルのマッピングが含まれています。

タグの使用方法の詳細については、Catalyst 9800 の設定モデルを説明する次の URL を参照してください。

[Understand Catalyst 9800 Wireless Controllers Configuration Model](#)

アクセスポイントに割り当てられたタグ :

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode
sand-4800-site2	AIR-AP4800-A-K9	3	✓	9.11.50.202	7872.5dee.53c0	Local

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Edit AP

Location* Global/colorado/den

Base Radio MAC 7872.5dee.53c0

Ethernet MAC 7872.5ded.cc1a

Admin Status ENABLED

AP Mode Local

Operation Status Registered

Fabric Status Enabled

LED State ENABLED

LED Brightness Level 8

CleanAir NSI Key

RLOC IP 9.201.201.14

Control Plane Name default-control-plane

Tags

Policy PT_denve_BGL11_F

Site default-site-tag

RF TYPICAL

ポリシータグの詳細 :

Configuration > Tags & Profiles > Tags

Policy Tag Name

default-policy-tag

PT_denve_BGL11_F1_45efe

Edit Policy Tag

Changes may result in loss of connectivity for some clients that are associated to APs with t

Name* PT_denve_BGL11_F

Description PolicyTagName PT_1

WLAN-POLICY Maps: 3

WLAN Profile	Policy Profile
sand-mac-s_Global_F_4256d671	sand-mac-s_Global_F_4256d671
sand-site2_Sanjos_F_7a13809e	sand-site2_Sanjos_F_7a13809e
sand-nonfa_Sanjos_NF_5aec7152	sand-nonfa_Sanjos_NF_5aec7152

RF タグの詳細 :

Configuration > Tags & Profiles > Tags

Policy Site **RF** AP

+ Add -X Delete

RF Tag Name
<input checked="" type="checkbox"/> TYPICAL
<input type="checkbox"/> default-rf-tag

1 10 items per page

Edit RF Tag

Name* TYPICAL

Description Enter Description

5 GHz Band RF Profile	Typical_Client_Densi
2.4 GHz Band RF Profile	Typical_Client_Densi

サイトタグの詳細 :

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add -X Delete

Site Tag Name
<input checked="" type="checkbox"/> default-site-tag

1 10 items per page

Edit Site Tag

Name* default-site-tag

Description default site tag

AP Join Profile default-ap-profile

Control Plane Name

Enable Local Site

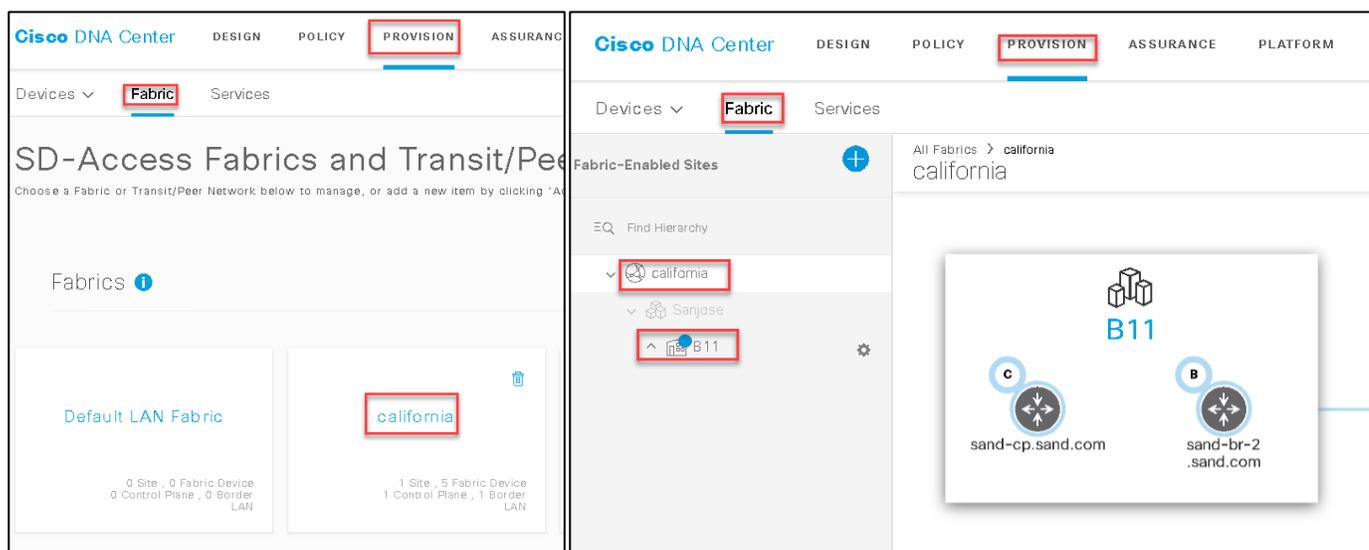
オンボーディングクライアント

次に、クライアントがワイヤレスネットワークに参加できるように、ワイヤレスクライアントと SSID に IP プールを割り当てる必要があります。

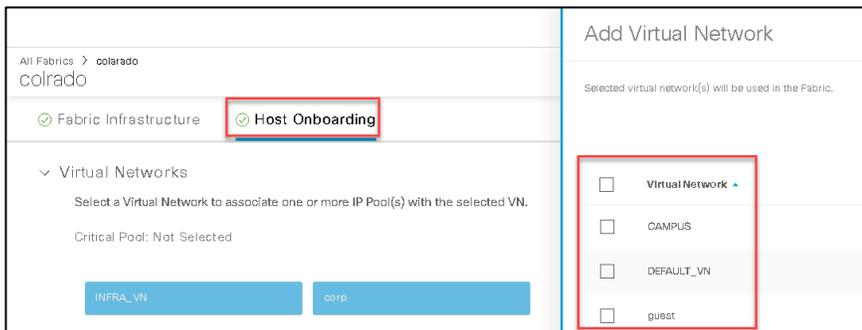
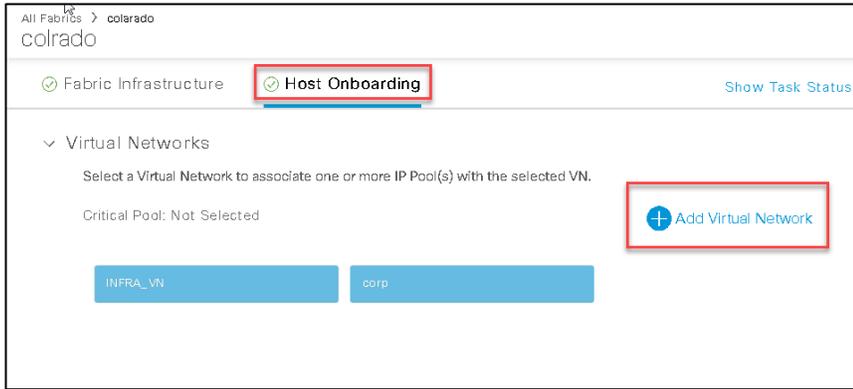
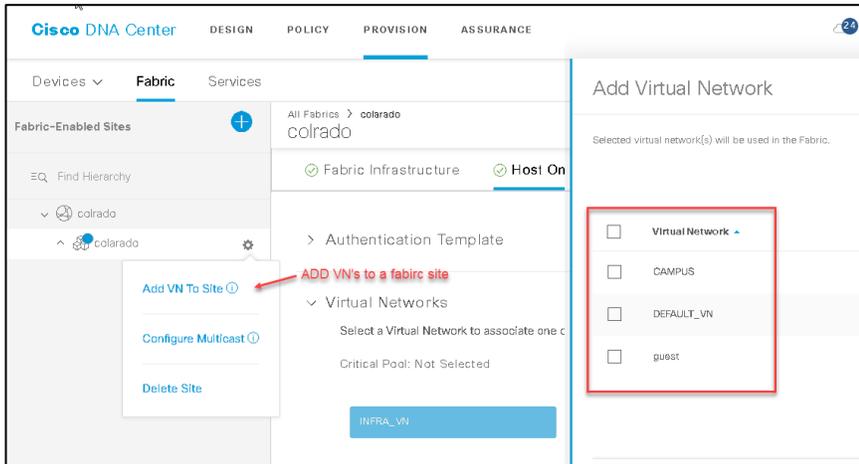
手順

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Fabric] の順に移動します。

この例では、「California」という名前でファブリックを編集します。ファブリックにはすでにコントロールプレーンとボーダーが設定されていると想定します。この項では、ワイヤレス LAN コントローラをファブリックに追加し、ワイヤレスクライアントでホストのオンボーディングを有効にする方法について説明します。

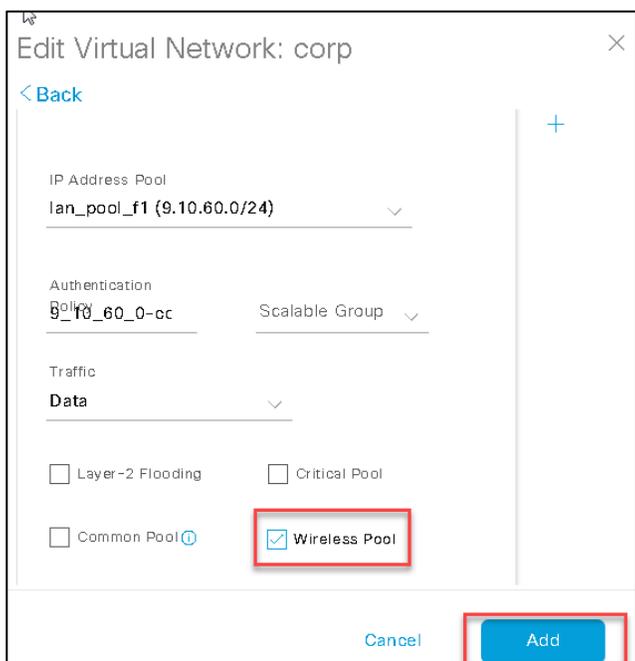
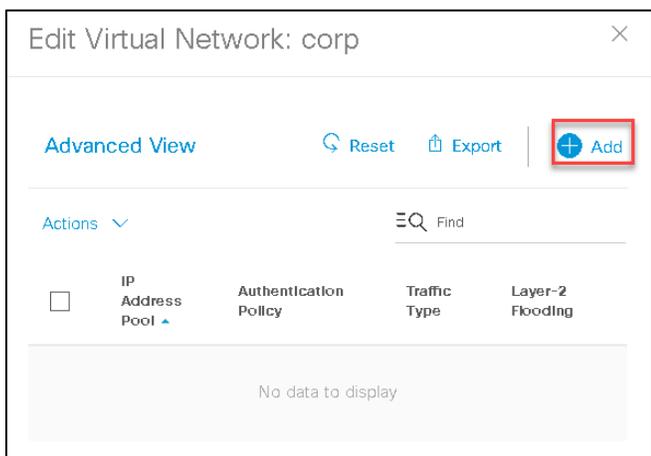


ステップ 2 Cisco DNAC 1.3.3 では、新しい VN を作成した場合、ファブリックに手動で追加する必要があります。1.3.3 に移行する場合、以前のバージョンに存在していたすべての VN がホストのオンボーディングページで使用可能になります。ホストのオンボーディングページで VN を使用できない場合は、サイトの横にある「歯車」アイコンをクリックして、ファブリックに VN を追加します。または、ホストのオンボーディングページから VN を追加します。追加する新しい VN にファブリックボーダーから設定されたハンドオフがあることを確認します。



ステップ 3 仮想ネットワークをサイトに追加したら、ファブリック内のクライアントが使用する VN に IP プールを関連付ける必要があります。VN (次の例では corp) をクリックし、使用可能なアドレスプールからワイヤレスクライアントのアドレスプールを選択します。

重要：ワイヤレスクライアントがプールを使用する必要がある場合は、オプション [Wireless Pool] を有効にします。

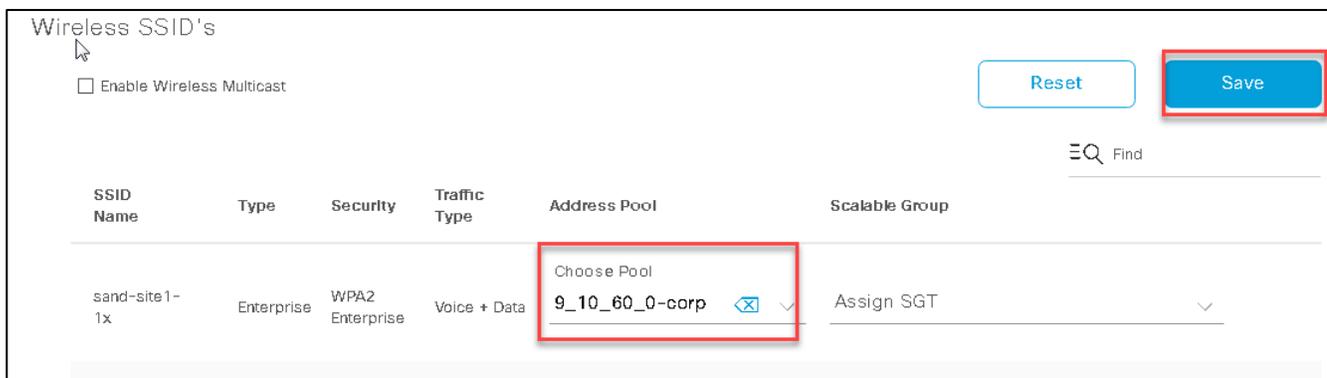


[Add] をクリックして、プールを VN に関連付けます。トラフィックタイプのオプション ([Data] または [Voice + Data]) は、有線クライアントにのみ関連します。ワイヤレスクライアントに対する対応設定は、SSID レベルで実行されます。

Cisco DNA Center 1.3 以降のデフォルトでは、管理者はプールをワイヤレス LAN コントローラ (WLC) にプッシュするために [Wireless Pool] オプションを有効にする必要があります。これは、Cisco WLC にプロビジョニングされたレイヤ 2 VNID を最適化するための措置です。[Wireless Pool] オプションが有効になっていないプールは、それぞれのレイヤ 2 VNID で WLC にプロビジョニングされません。

(注) クライアント認可の一環として VNID オーバーライドを使用する場合は、オーバーライドプールで [Wireless Pool] オプションが有効になっていることを確認してください。

ステップ 4 以前に設定したプールに、SSID を関連付けます (必要に応じて、この SSID に参加するすべてのクライアントに割り当てられるように SGT を関連付けることもできます)。



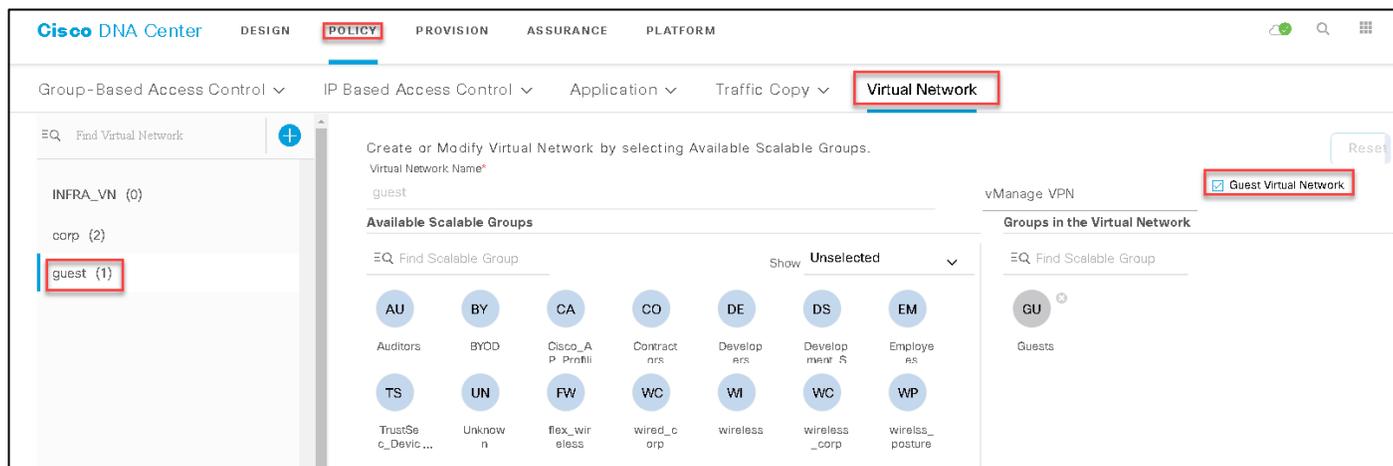
オンボーディングゲストクライアント

ゲスト SSID において、2つの実装方法を選択できます（後に、ゲスト設計の項でさまざまな使用可能な設計の詳細について説明します）。

1. ゲストトラフィックに同じエンタープライズゲスト CP ノードを使用します。ゲスト SSID はファブリックの専用ゲスト VN に関連付けられ、ファブリック セグメンテーション（VNI、SGT）を利用してゲストトラフィックを隔離します。
2. ゲストトラフィック専用のゲストコントロールプレーンとボーダーを使用します。

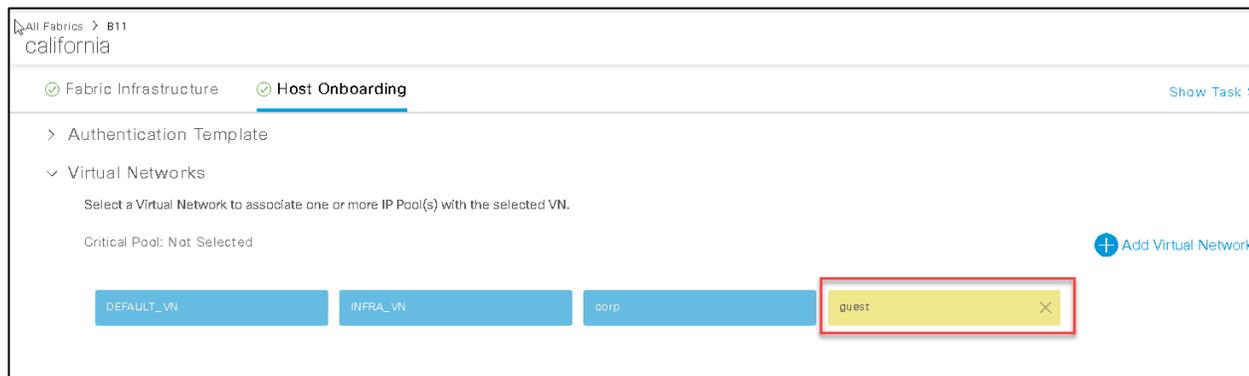
両方のケースにおいて、SSID を設定する前に、VN をゲストが有効であるとマークする必要があります。これにより、これが適切に設定される必要がある「特別な」VNであることを Cisco DNA Center に通知することになります。

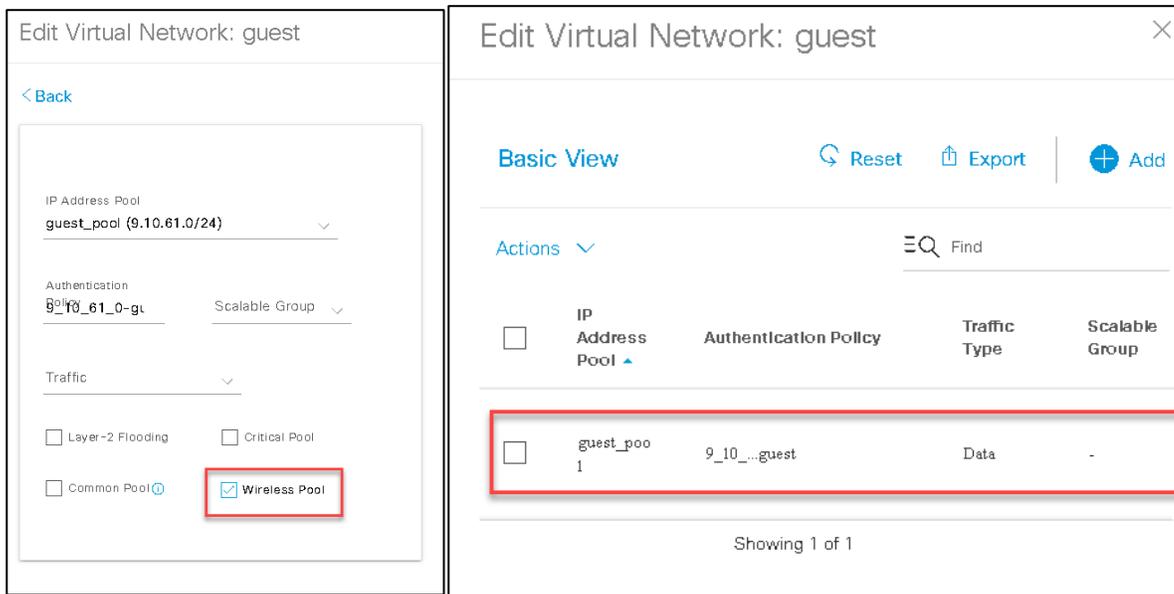
[Policy] > [Virtual Networks] の順に移動し、新しい VN を作成します。以下に示すように、[Guest Virtual Network] チェックボックスをオンにし、この仮想ネットワークに属するスケーラブルグループを追加します。



VN をサイトに追加するには、クライアント オンボーディングの項のステップ 2 を参照してください。

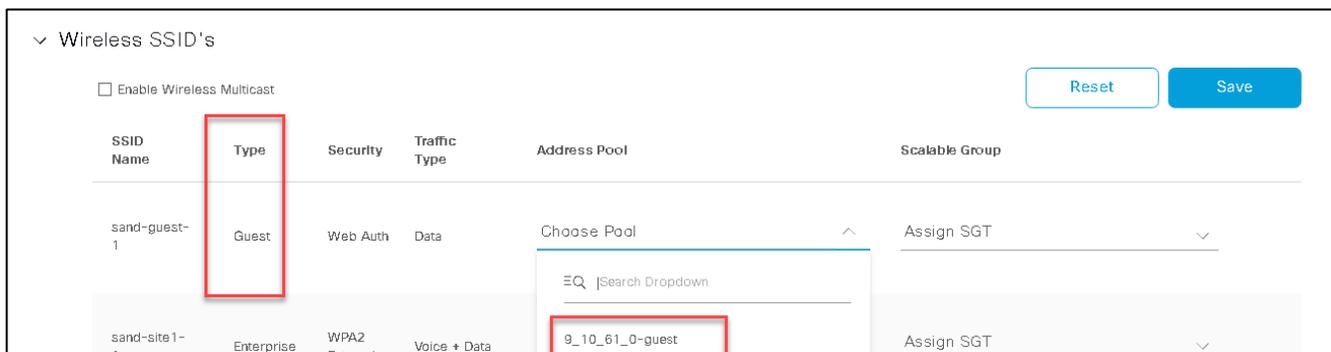
これで、オンボーディングセッションで SSID を設定できます。一般的なコントロールプレーンノードについては、手順は、他の SSID の設定と同様です。ゲストクライアントに使用している VN をクリックし、使用可能なアドレスプールからワイヤレスクライアントのアドレスプールを選択します。[Update] をクリックします。次の例を参照してください。





DNAC 1.3 以降では、[Wireless SSID's] サブセクションでこの IP プールをワイヤレス SSID に関連付けるには、[Wireless Pool] チェックボックスをクリックする必要があります。

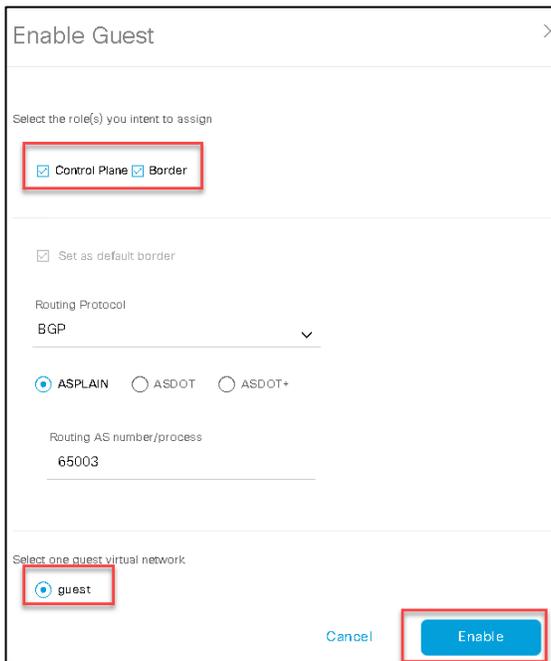
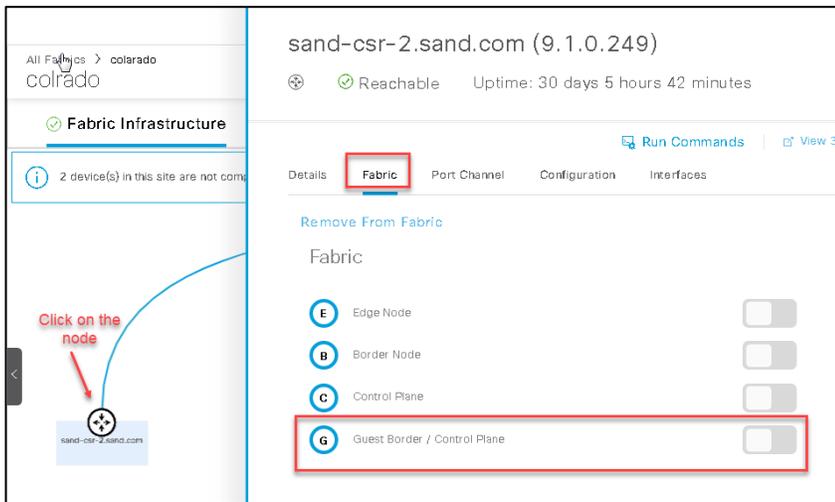
次に、通常のエンタープライズ SSID に対してステップ 4 で行ったように、ゲスト SSID をプールに関連付けて [Save] をクリックします。



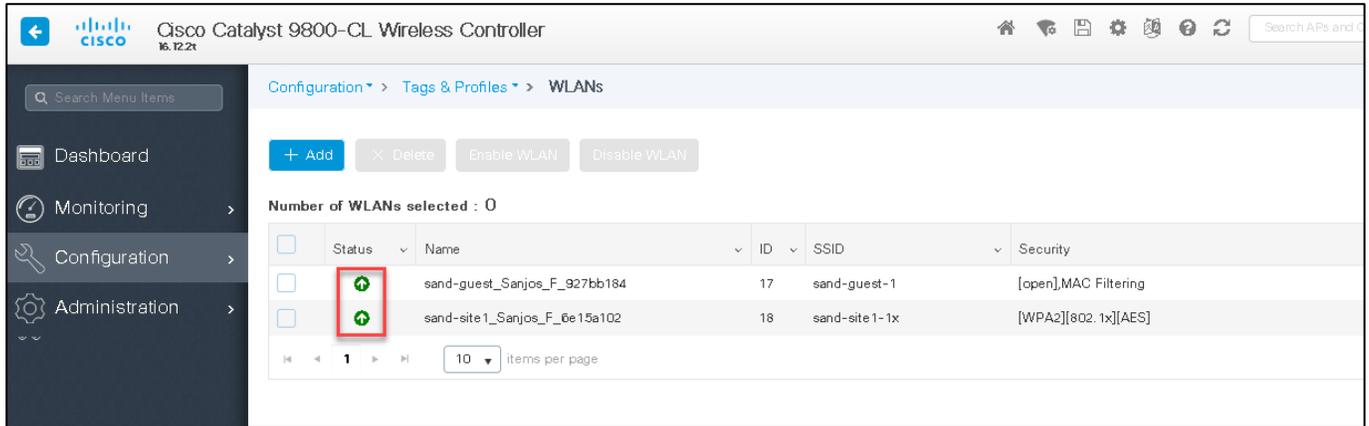
ゲストトラフィック専用のボーダーとコントロールプレーンを使用する場合は、ゲストコントロールプレーンとボーダーをファブリックに追加する必要があります。デバイスアイコンをクリックしてデバイスの詳細ページを開きます。

下記のウィンドウがポップアップ表示され、ボーダーとコントロールプレーンの両方の機能を選択できます。また、ゲストが有効であるとマークした VN がここに表示されます。内部的に Cisco DNA Center はファブリック設定を処理してゲスト SSID をプールに関連付け、そのプールをゲストコントロールプレーンおよびボーダーにマッピングします。

注目すべき重要なポイントは、ゲストボーダーおよびコントロールプレーンを同じデバイスに配置することが推奨される点です。ゲストボーダーからのハンドオフは手動プロセスで、管理者は外部ドメインへのハンドオーバーを行うための任意のプロトコルを設定できます。



ステップ 5 ステップ 4 で SSID をプールに関連付けした場合は、WLC で、SSID の [Admin Status] が [Enabled] になっていることが確認できます。



(注) 上の WLC のスクリーンショットは説明のみを目的としたものです。WLAN 名とセキュリティは、ご使用の設定では異なる場合があります。

ステップ 6 これで、クライアントはファブリック対応のワイヤレス SSID に接続可能です。WLC に移動し、接続されたクライアントの詳細を確認できます。

[Monitoring] > [Wireless] > [Clients] に移動します。



クライアントファブリックステータスとSGTタグが、認証ルールに基づいてISEからWLCにプッシュされていることを確認できます。

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Total Client(s) in the Network: 2
Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID
<input checked="" type="checkbox"/> 1c36.bb00.17d4	9.10.60.204	fe80::6d87:cd22:da30:4472	sand-3800-site1	sand-site1
<input type="checkbox"/> 1c36.bb0e.09b4	9.10.61.200	N/A	sand-3800-site1	sand-guest

1 10 items per page

Click on the client mac to open the details

Client

360 View General QoS Statistics ATF Statistics Mobility

Client Properties AP Properties Security Information Client St

VLAN default

Multicast VLAN 0

Server IP 9.1.0.20

11v DMS Capable No

QoS Map Capable No

FlexConnect Data Switching N/A

HexConnect Authentication N/A

FlexConnect Central Association N/A

Control plane name default-control-plane

antenna 0 9 s ago -36 dBm

antenna 1 9 s ago -36 dBm

EoGRE No/Simple client

Type 55 17

Data 11

Fabric

Fabric Status	Enabled
RLOC	9.254.254.70
VNID	8210
SGT	16

Assisted Roaming Neighbor List

マルチキャストの設定

ワイヤレスでマルチキャストを有効にするには、最初に有線ネットワークでマルチキャストを設定する必要があります。次の手順で説明されているように、Cisco DNA Center により、両方の設定が非常に簡単になります。

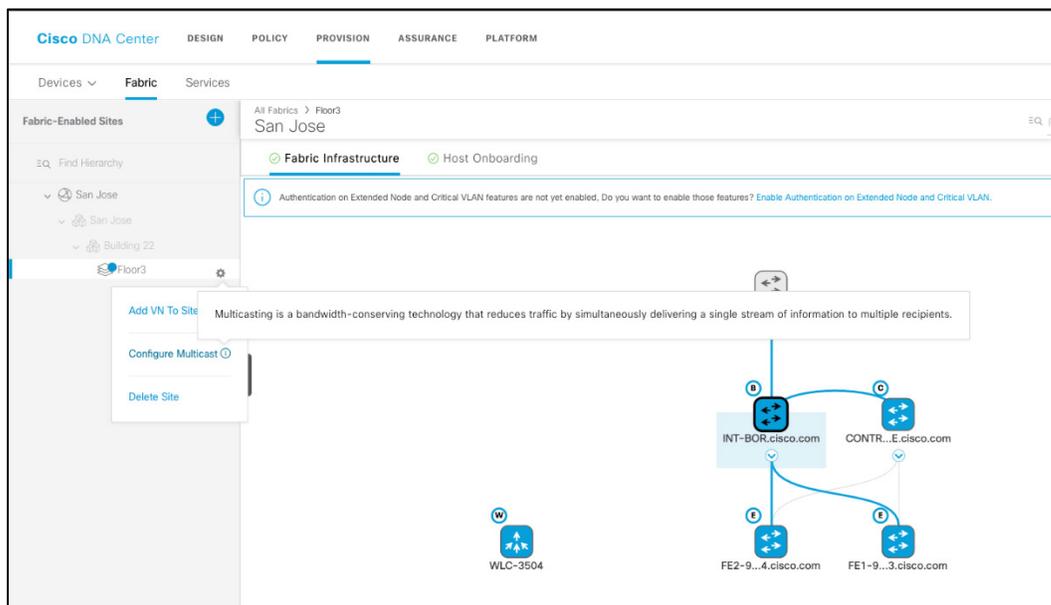


(注) ワイヤレスマルチキャストは慎重に検討する必要があります。

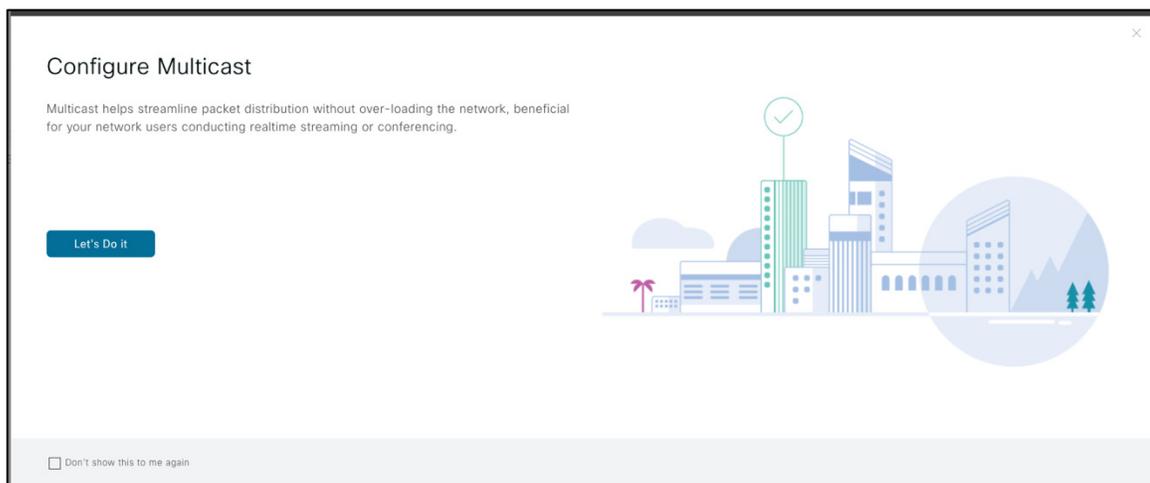
マルチキャスト IP トラフィックが AP に到達すると、これらのパケットはブロードキャストレイヤ 2 フレームとして無線で送信されます。これは、基本的にトラフィックが最高の必須データレート（接続されたすべてのクライアントに到達できるように）で送信されることを意味し、伝送フレームが認識されないため、電波でコリジョンが発生し、フレームが損失します。これは、電波を介したマルチキャストトラフィックの達成可能なスループットに影響を与えます。Wi-Fi 経由でマルチキャストトラフィックのパフォーマンスと信頼性を向上させるために、シスコは AP でマルチキャストフレームをユニキャストフレームに変換する VideoStream 機能を開発し、前述の問題を解決しました。VideoStream（マルチキャスト ツー ユニキャスト機能とも呼ばれる）は、Cisco DNA Center 1.3 以降のテンプレートを使用してサポートされます。

手順

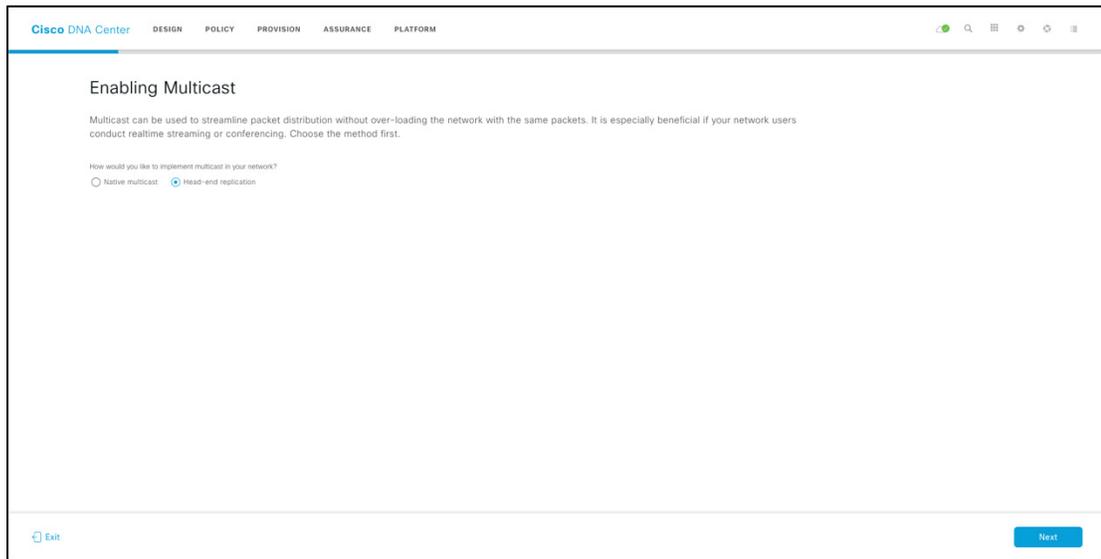
ステップ 1 [Fabric] > [San Jose] > [Floor 3] でサイトの歯車メニューをクリックし、[Configure Multicast] をクリックします。これをクリックすると、ファブリックでマルチキャストを有効にする手順のワークフローが表示されます。



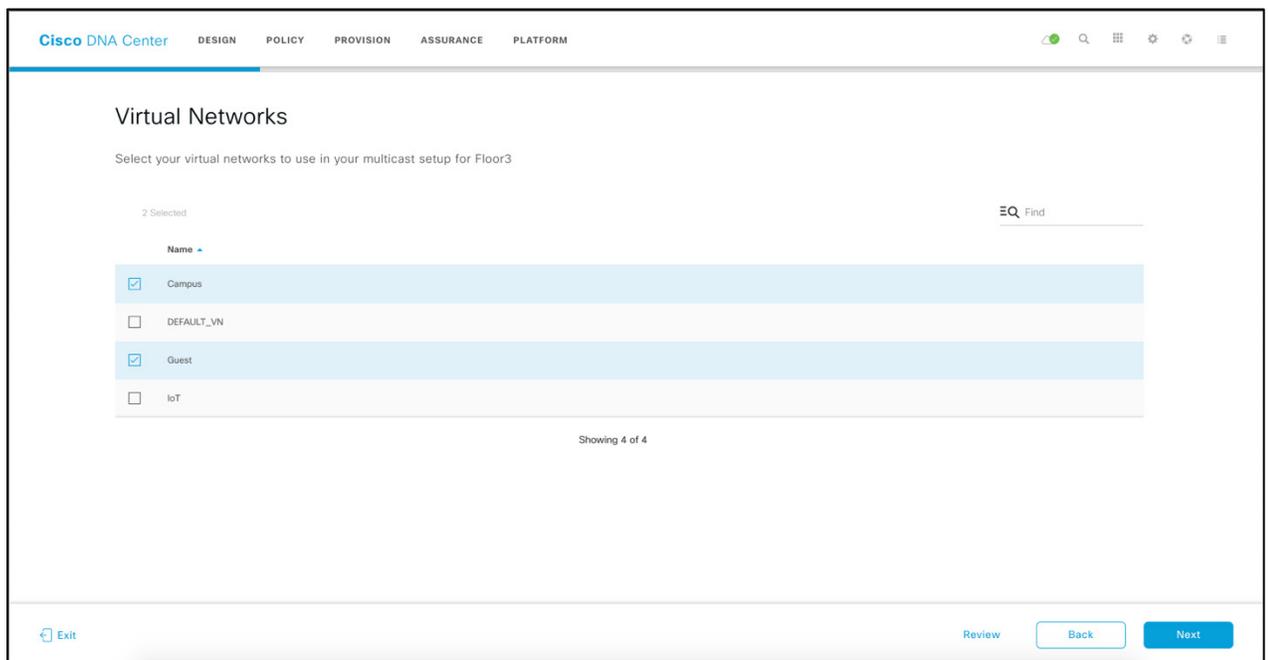
ステップ 2 [Enable Multicast] ワークフローで、[Let's do it] をクリックしてマルチキャストを設定します。



ステップ 3 [Native Multicast] または [Headend Multicast] を選択し、[Next] をクリックします。



ステップ 4 Floor3 のマルチキャスト設定で使用する仮想ネットワークを選択し、[Next] をクリックします。



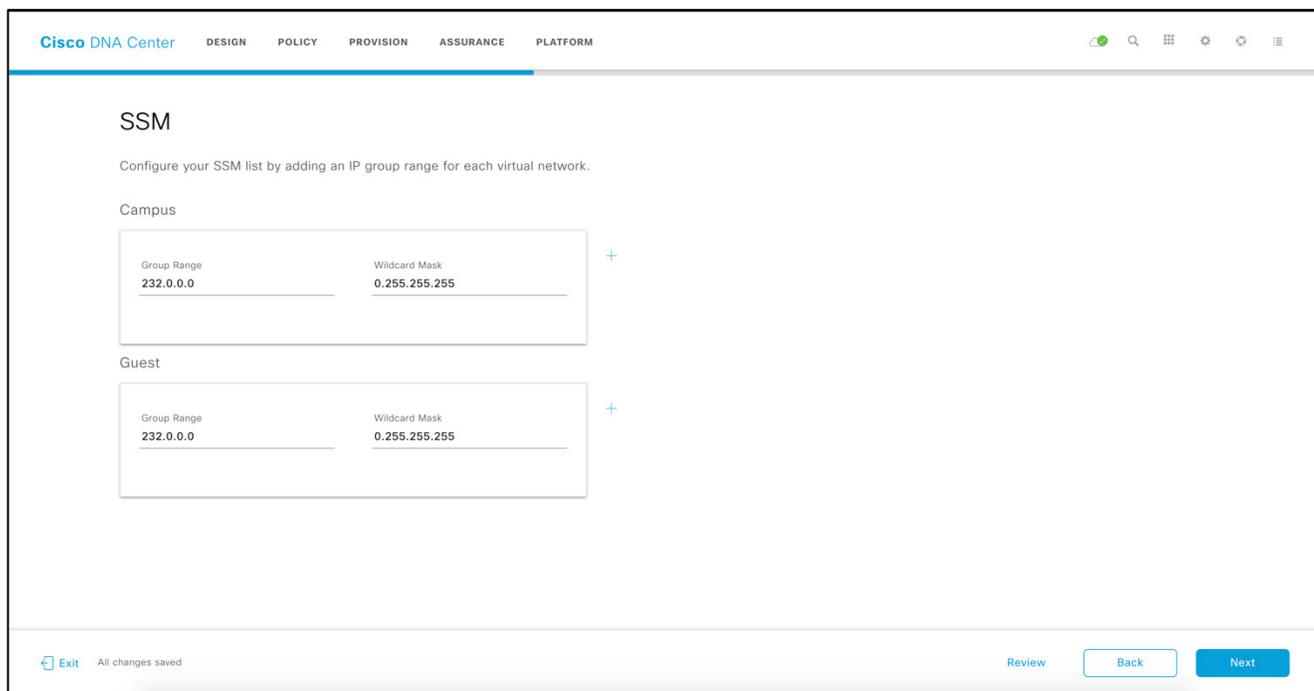
ステップ 5 [Multicast Pool mapping] ページで、マルチキャストトラフィックの送信に使用する IP プールを選択します。マルチキャストを有効にするには、すべてのファブリックノードで VN ごとに IP アドレスが必要になります。[Next] をクリックして次のセクションに進みます。

The screenshot shows the 'Multicast Pool mapping' configuration page in Cisco DNA Center. The page title is 'Multicast Pool mapping'. Below the title, there is a note: 'Every Fabric node requires an IP Address per VN to enable multicast.' The configuration is organized into two sections: 'Campus' and 'Guest'. Under 'Campus', the 'IP Pools*' dropdown menu is set to 'Campus-Multicast-SJC (1.1.1.0)'. Under 'Guest', the 'IP Pools*' dropdown menu is open, showing a search bar and two options: 'Campus-Multicast-SJC (1.1.1.0)' and 'Guest-Multicast-SJC (2.2.2.0)'. At the bottom of the page, there is an 'Exit' button with the text 'All changes saved', and navigation buttons for 'Review', 'Back', and 'Next'.

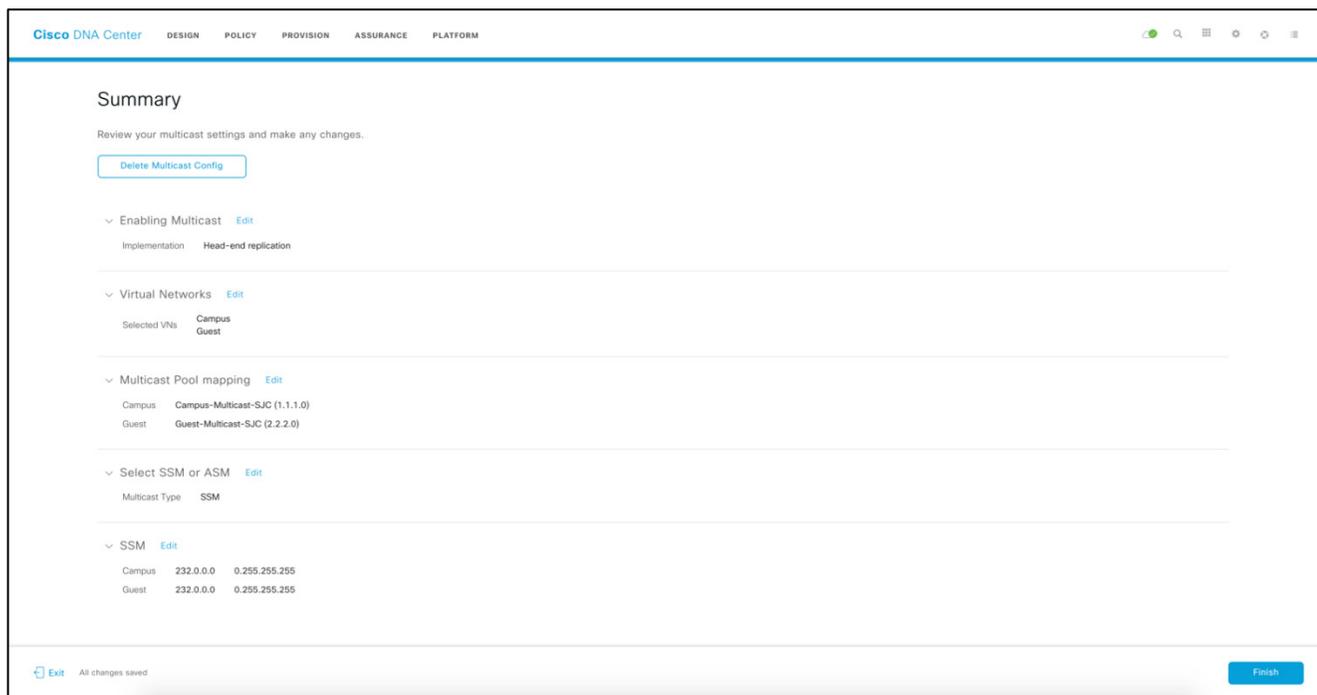
ステップ 6 [SSM] または [ASM] を選択します。

The screenshot shows the 'Select SSM or ASM' configuration page in Cisco DNA Center. The page title is 'Select SSM or ASM'. Below the title, there is a descriptive paragraph: 'The Source Specific Multicast (SSM) feature is an extension of IP multicast where traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.' Below this, another paragraph states: 'Multicast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network users conduct realtime streaming or conferencing. Choose the method first.' There are two radio button options: 'SSM' (which is selected) and 'ASM'. At the bottom of the page, there is an 'Exit' button and navigation buttons for 'Review', 'Back', and 'Next'.

ステップ 7 SSM の場合はマルチキャスト IP 範囲を選択します。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。



ステップ 8 すべてのマルチキャスト設定を確認し、[Finish] をクリックしてマルチキャストを展開します。



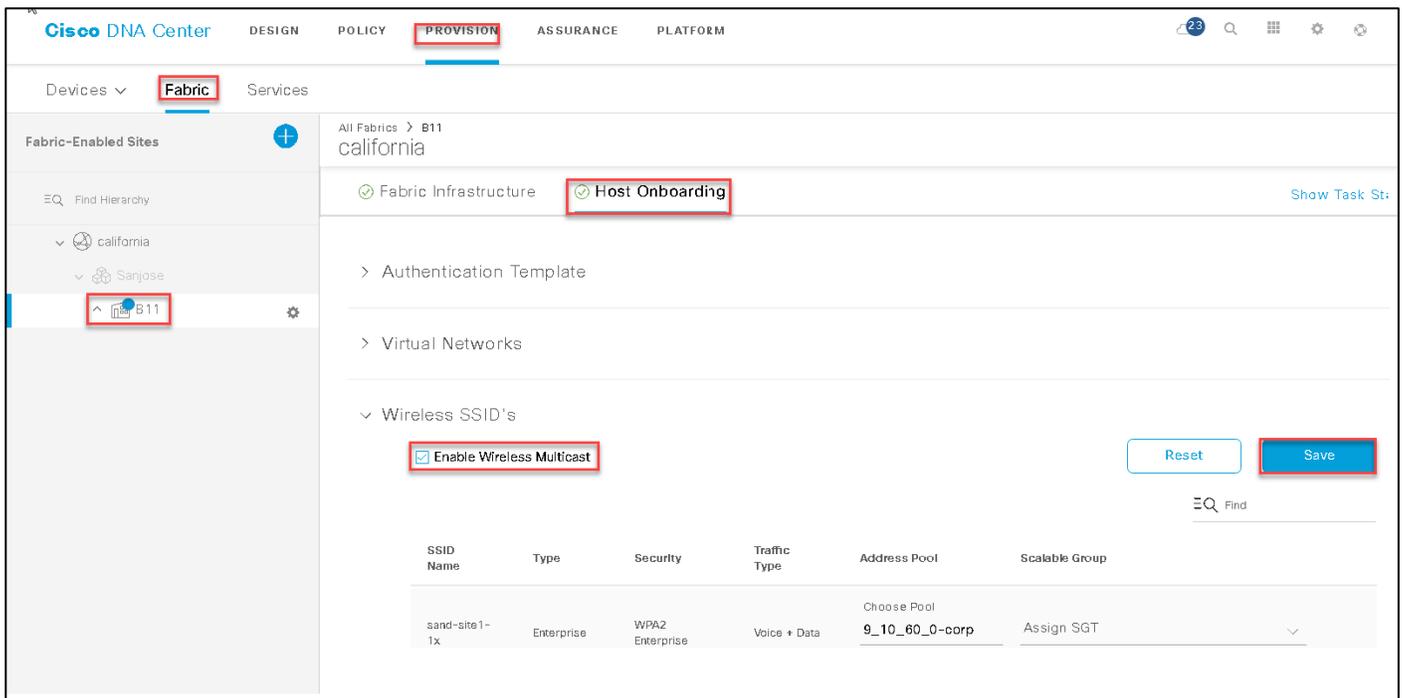
これで、マルチキャスト設定ワークフローが完了します。



ステップ 9 有線ファブリック インフラストラクチャにマルチキャストを展開した後、マルチキャストを SD-Access ワイヤレス インフラストラクチャで有効にする必要があります。ワイヤレスでマルチキャストを有効にするオプションは、ホストのオンボーディングページの SSID 設定にあります。

Cisco DNA Center のホームページから次のように移動します。

[Provision] > [Fabric] > ファブリックサイト > [Host Onboarding] > [Wireless SSID's]

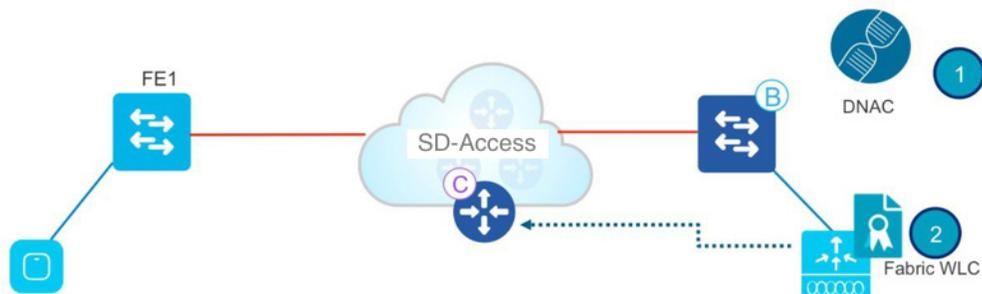


SD-Access ワイヤレス : 内部の仕組み

この項では、SD-Access ワイヤレスの基本的な動作について説明し、Cisco DNA Center の「舞台裏」で何が起きているのかを明確に理解できるようにします。このフローでは、設計フェーズを完了し、実装およびプロビジョニングフェーズのみに焦点を当てていることを前提としています。

ファブリックに WLC を追加

図 15. ファブリックに WLC を追加

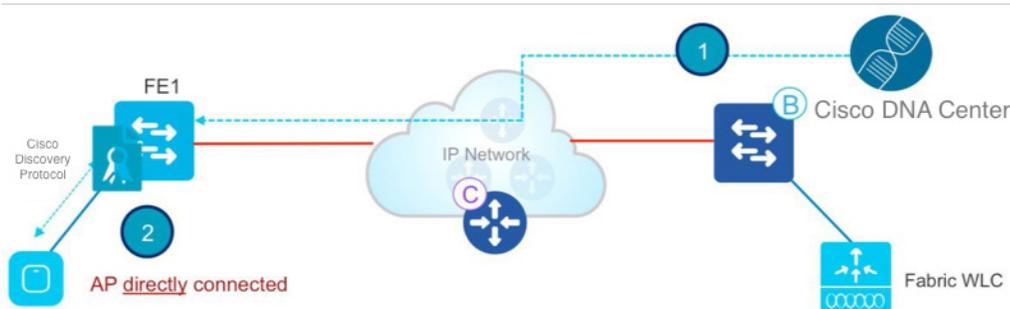


Cisco DNA Center では、最初にファブリックドメインに WLC をプロビジョニングしてから追加します。

1. ファブリック設定が WLC にプッシュされます。WLC はファブリックを認識します。最も重要なことは、ファブリック コントロールプレーンへのセキュアな接続を確立するために、WLC でログイン情報を設定することです。
2. WLC は SD-Access ワイヤレスへの参加が可能になります。

AP 参加フロー

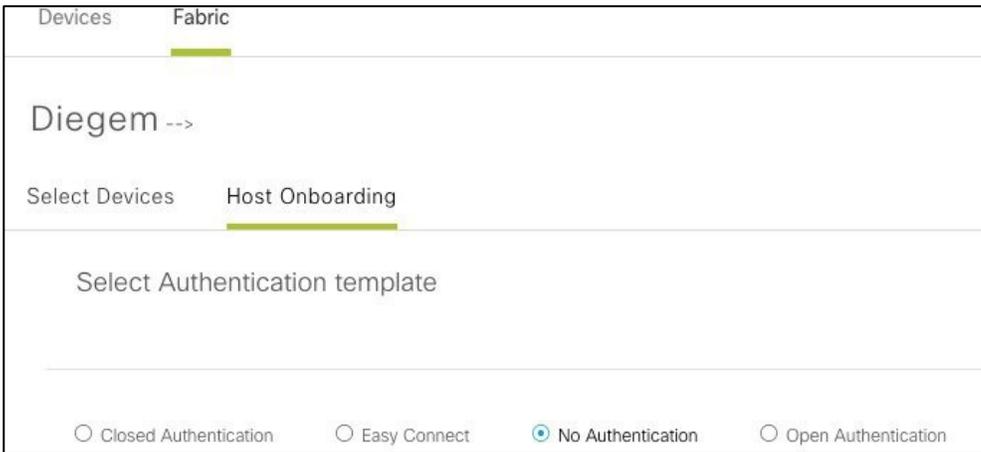
図 16. AP の接続と検出



1. 管理者ユーザは、Cisco DNA Center 内のプールを INFRA_VN 内の AP 専用（これはプール定義内の [AP Provisioning] ボックスをチェックすることを意味します）に設定します。Cisco DNA Center は、AP VLAN と関連テンプレートをファブリックエッジに事前プロビジョニングします。Cisco DNA Center 1.3 以降では Autoconf を使用し、リリース 1.2 ではマクロを使用します。
2. AP は電源に接続されオンになります。FE のデバイス分類子は Cisco Discovery Protocol を介して AP であることを検出し、テンプレート設定を適用してスイッチポートを正しい VLAN に割り当てます。
3. AP は DHCP 経由で IP アドレスを取得します。AP は、ファブリックに有線接続された「特別な」ホストです。

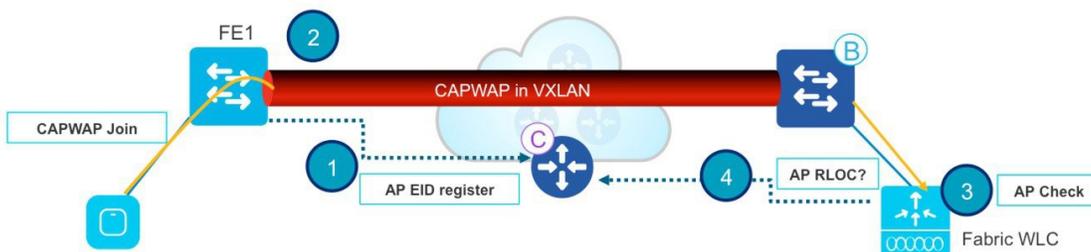


(注) Cisco DNA Center 1.3 の時点では、デバイスをアクセスポイントとして識別するために Autoconf が使用されます。Autoconf は、ポートが [No Authentication] モードに設定されている場合にのみ機能します。スイッチポートテンプレートはホストオンボーディングの設定時に選択します。次のスクリーンショットを参照してください。



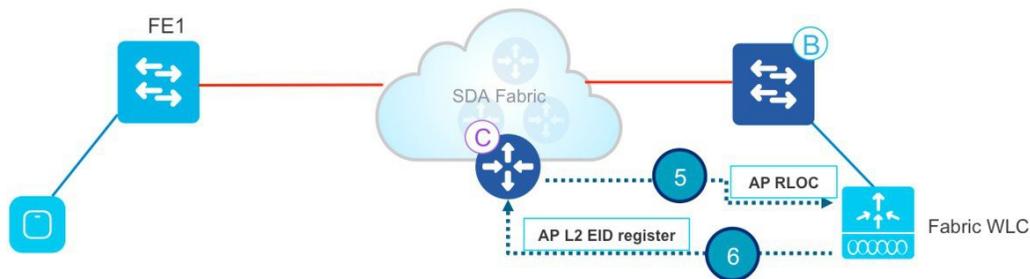
その他の認証テンプレートを選択すると、管理者ユーザは、右の IP プールを AP のスイッチポートに静的にマッピングする必要があります。AP はクローズド認証ポートでもサポートされます。ワークフローと手順は AP オンボーディングの項で定義されています。

図 17. AP オンボーディング



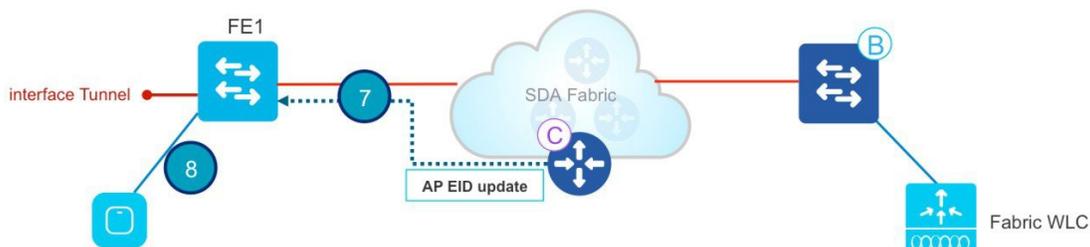
1. ファブリックエッジでは、コントロールプレーンノードで AP の IP アドレスが登録されます。これで、AP ロケーションはファブリックで認識されるようになりました。
2. AP は従来の方法 (DHCP オプション 43、DNS、プラグアンドプレイ) を使用して WLC について学習し、WLC に接続します。ファブリック AP はローカルモード AP として参加します。
3. WLC は AP がファブリック対応 (つまり、Wave 2 または Wave 1 AP) かどうかを確認します。
4. AP モデルがサポートされている場合、WLC は CP に AP がファブリックに接続されているかどうかを問い合わせます。

図 18. RLOC および EID 情報の交換



5. CP は RLOC 情報で WLC に応答します。つまり、AP はファブリックに接続されており、WLC の AP 詳細情報がファブリック対応として表示されるようになります。
6. WLC は、ホストトラッキングデータベースに AP のレイヤ 2 LISP 登録を行います（これにより、AP は「特別な」セキュアクライアントとして登録されます）。これは WLC から FE への重要なメタデータ情報の転送に使用されます。

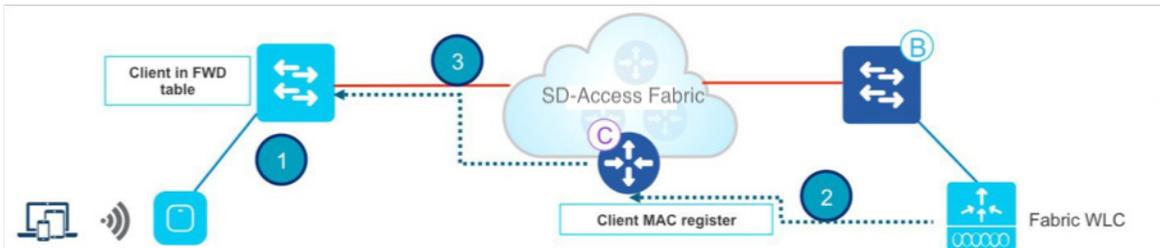
図 19. AP の VXLAN トンネルの作成



7. WLC によるこのプロキシ登録に応答して、CP はファブリックエッジに通知して、WLC から受信したメタデータを渡します（AP であることを示し、AP の IP アドレスを提供するフラグ）。
8. ファブリックエッジは情報を処理し、このクライアントが AP であることを認識して、指定された IP アドレスへの VXLAN トンネルインターフェイスを作成します（最適化：スイッチ側はクライアント接続を待機している状態）。

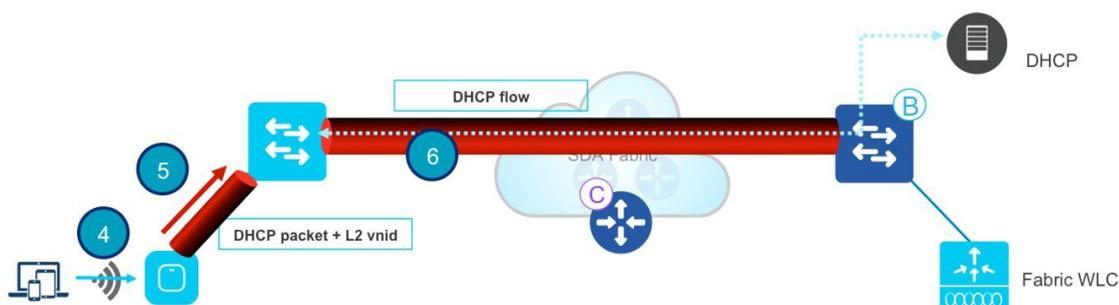
クライアント オンボーディング フロー

図 20. 認証およびポリシーの取得



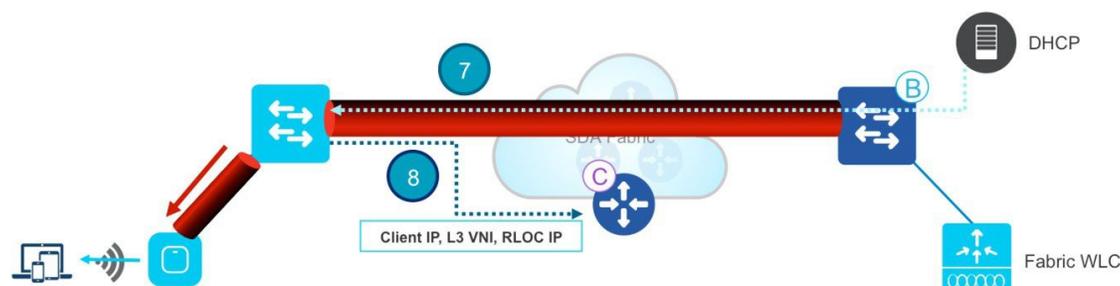
1. クライアントはファブリック対応 WLAN に対して認証されます。WLC は ISE からクライアント SGT を取得し (WLAN が 802.1X 認証用に設定されていることを前提とします)、AP をクライアントのレイヤ 2 VNID および SGT で更新します。WLC は、(AP への接続プロセス中に保存された) 自身の内部記録から AP の RLOC を認識しています。
2. WLC プロキシはクライアントのレイヤ 2 情報を CP に登録します。これは LISP 変更メッセージであり、クライアント SGT などの追加情報を渡します。
3. CP は FE に通知し、FE はクライアントの MAC アドレスをレイヤ 2 転送テーブルに追加し、SGT に基づいて ISE からポリシーを取得します。

図 21. DHCP フロー



4. クライアントが DHCP 要求を開始します。
5. AP はレイヤ 2 VNI 情報を使用して、その要求を VXLAN にカプセル化します。
6. ファブリックエッジはレイヤ 2 VNID を VLAN と VLAN インターフェイスにマッピングし、エニーキャスト IP を DHCP リレーとして使用して、オーバーレイの DHCP を転送します (有線ファブリッククライアントの場合と同様)。

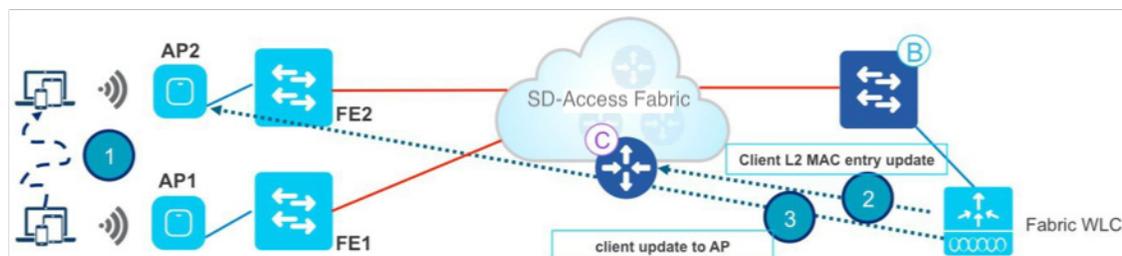
図 22. オンボーディングプロセスの完了



7. クライアントは DHCP から IP アドレスを受信します。
8. DHCP スヌーピング (スタティックの場合 ARP またはこの両方) は、ファブリックエッジによるホストトラッキングデータベースへのクライアント登録をトリガーします。これで、クライアント オンボーディング プロセスは完了します。

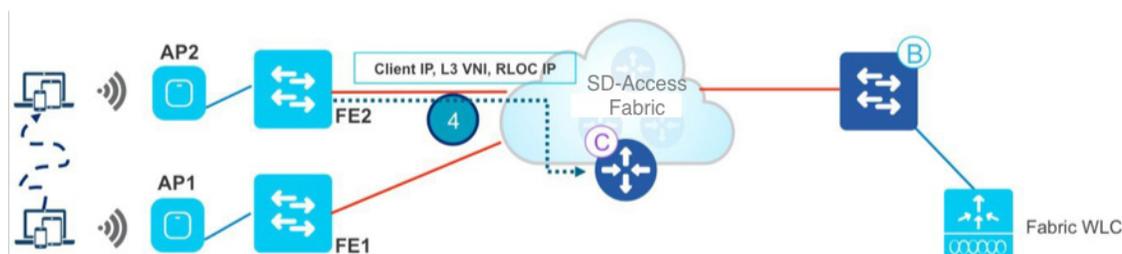
クライアント ローミング フロー

図 23. クライアント情報の更新



1. クライアントは FE2 の AP2 にローミングします (スイッチ間ローミング)。AP2 は WLC に通知します。
2. WLC は、クライアント情報 (SGT、RLOC IP アドレス) を使用して AP 上の転送テーブルを更新します。
3. WLC は、FE2 の新しい RLOC を使用して CP でレイヤ 2 MAC エントリを更新します。

図 24. コントロールプレーン通知



4. CP は次のように通知します。
 - ファブリックエッジ FE2 (「ローミング先」のスイッチ) に、VXLAN トンネルを参照する転送テーブルにクライアント MAC を追加するように通知します。
 - ファブリックエッジ FE1 (「ローミング元」のスイッチ) に、ワイヤレスクライアントのクリーンアップを実行するように通知します。
 - ファブリックボーダーに、このクライアントの内部 RLOC を更新するように通知します。
5. FE はトラフィックの受信時に、CP でレイヤ 3 エントリ (IP アドレス) を更新します。

FE2 に同じ VLAN インターフェイス (エニーキャストゲートウェイ) があるため、ローミングはレイヤ 2 です。

SD-Access のワイヤレス統合の設計

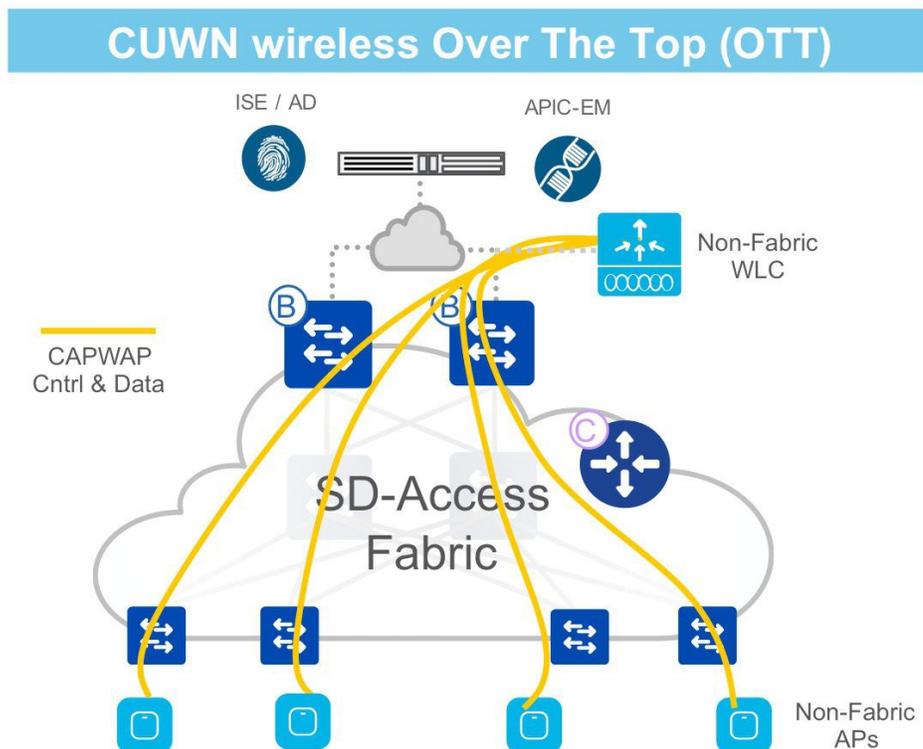
前述のとおり、SD-Access ファブリックでワイヤレスを展開するには、次の 2 つの方法があります。

- Cisco Unified Wireless Network ワイヤレス OTT : SD-Access ファブリックは IP 転送ネットワークであり、ワイヤレスはピュアなオーバーレイです。
- SD-Access ワイヤレス : ワイヤレスが SD-Access に統合され、ファブリックのすべての利点を活用できます。

Cisco Unified Wireless Network ワイヤレス OTT

この場合は、従来のワイヤレスが SD-Access ファブリック上で実行されます。このモードは、有線ネットワーク上で SD-Access を最初に実装し、次にワイヤレス統合を計画しているお客様向けの移行手順として重要です。

図 25. Cisco Unified Wireless Network ワイヤレス OTT



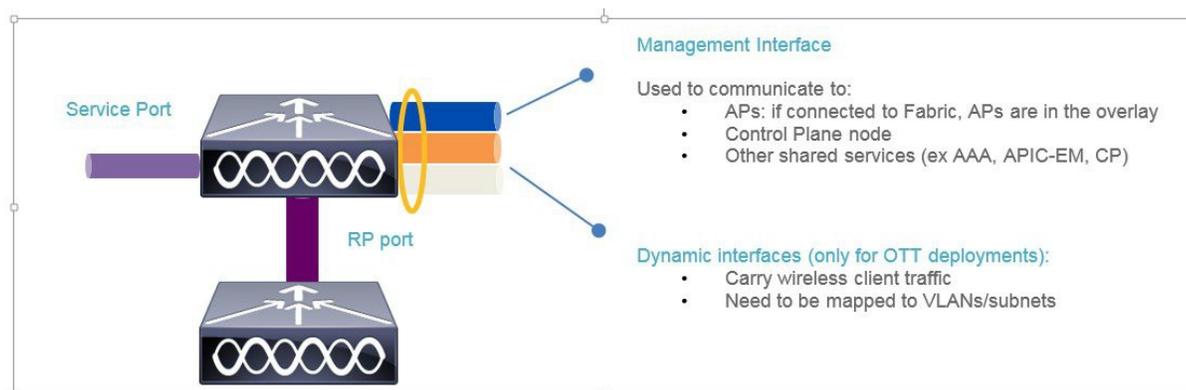
- CAPWAP を使用する従来型の Cisco Unified Wireless Network アーキテクチャがコントロールプレーンとデータプレーンで使用され、WLC で終端します（中央モード）。
- SD-Access ファブリックは AP と WLC 間の有線インフラストラクチャ内の伝送路にすぎません。
- CUWN ワイヤレス OTT は完全な SD-Access へ移行するためのステップです。

2 種類の展開のさまざまな設計上の考慮事項を検討する前に、WLC のどのインターフェイスが使用されるのか、また異なる展開でどのように使用されるのかを明確にしましょう。

WLC インターフェイス

どちらの SD-Access 統合モードでも、SD-Access ワイヤレスと OTT に適用される WLC インターフェイスについて考慮します。

図 26. WLC インターフェイス



- WLC は、ファブリックネットワーク外のアンダーレイネットワーク（グローバルルーティングテーブル）に接続されます。
- ファブリックネットワークに接続されている AP は、オーバーレイネットワークにあるとみなされます。つまり、ファブリックエッジのポートはすべてファブリック対応ということになります。オーバーレイにポートを接続し、アンダーレイに他のポートを接続することはできません。
- 管理インターフェイスは、WLC と AP との CAPWAP コントロールチャネルと、AAA、Cisco DNA Center などの共有サービスとの通信に通常使用されています。
- SD-Access ワイヤレスを使用して展開した場合、管理インターフェイスはコントロールプレーンノードとの統合にも使用されます。
- 冗長ポート（RP）はアクティブおよびスタンバイ HA ペア間の高可用性（HA）通信に使用され、ボックス障害またはネットワーク障害時にシームレスでステートフルなスイッチオーバーを提供します。
- ダイナミック インターフェイスは、ワイヤレスがオーバーザトップで導入されている、つまりファブリック インフラストラクチャが、集中型処理のために WLC に返送される CAPWAP コントロールおよびデータチャネルの伝送路にすぎない場合のみ使用されます。
- サービスポートは、通常どおり、アウトオブバンド管理に使用されます。

Cisco Unified Wireless Network ワイヤレス OTT ネットワーク設計

まず最初に、Cisco Unified Wireless Network ワイヤレス OTT とは何でしょうか。このモードでは、AP と WLC 間の従来の CAPWAP トンネルがファブリックネットワークへのオーバーレイとして実行されます。つまり、ファブリックは CAPWAP のトランスポートとなります。Cisco Unified Wireless Network ワイヤレス OTT を導入する理由は主に 2 つあります。

1. OTT ソリューションは移行のステップとなる場合があります。お客様はまず有線インフラストラクチャを SD-Access ファブリックに移行し、ワイヤレスネットワークを「そのまま」の状態に維持する必要があります。つまり、現在ワイヤレスが動作する方法は変えません。これは、有線およびワイヤレス インフラストラクチャを管理するさまざまな IT オペレーションチーム、有線ネットワークのアップグレードを最初に決定するさまざまな購入サイクルが原因となっている可能性があります。または単に IT チームがワイヤレス部分を統合する前にまず有線側のファブリックを熟知したいと思っていることが原因である可能性もあります。
2. また、ワイヤレス OTT を導入するための別の理由として、お客様はワイヤレスのファブリックに移行したくない、またはできない可能性があります。これは、所有している大半の AP が SD-Access でサポートされていない古い AP (802.11n 以前) であるか、SD-Access ワイヤレス (8.5 以上) を実行するために必要な新しい WLC ソフトウェアの証明書を必要としている可能性があります。または、単にお客様がワイヤレスの「そのまま」の状態を維持し、変更を加えたくない可能性もあります。

各コンポーネントの最も重要な設計考慮事項を考えてみましょう。

WLC

図 27. WLC 接続

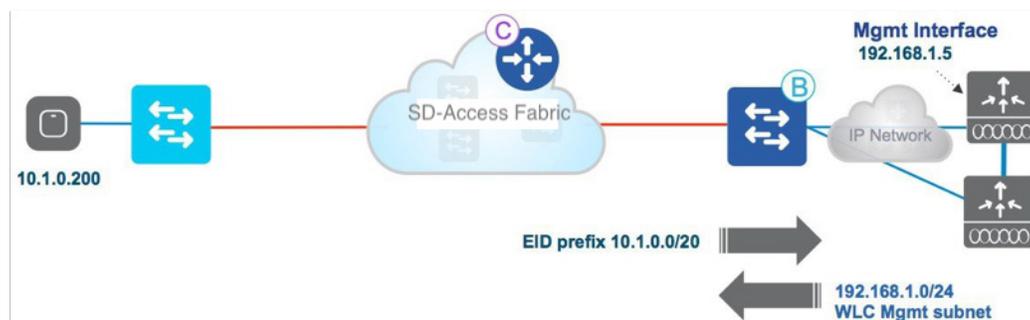


図 27 に示すように、ファブリックの外側に WLC (または冗長性のために複数の WLC) を接続することを推奨します。WLC は、Cisco SD-Access ソリューションのボーダーノードに接続することもできます。そのための設定は、ボーダーノードで手動で行う必要があります。通常、WLC はネットワークの中央 (データセンターまたは共有サービス) に接続されているため、WLC はアクセススイッチであることの多いファブリックエッジノードには接続されていないのが現実的です。

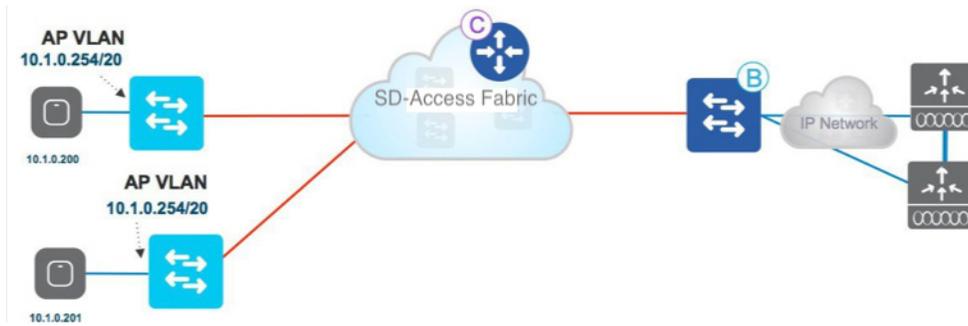
WLC はファブリックの外側に位置するため、ボーダーノードは管理インターフェイスサブネット (この例では 192.168.1.0/24) と AP の IP プール (この例では 10.1.0.0/16) 間の到達可能性を提供し、CAPWAP トンネルが形成され、AP は WLC に登録できます。Cisco DNA Center 1.3 では、AP は、グローバルルーティングテーブルにマップされている INFRA_VRF にあるため、ルートリークは必要ありません。



注意 シスコは、SDA ファブリックネットワークでは Cisco Unified Wireless Network Centralized モードと SD-Access ワイヤレスのみをサポートしています。Cisco FlexConnect® モードは、将来のリリースでサポートされます。

アクセスポイント

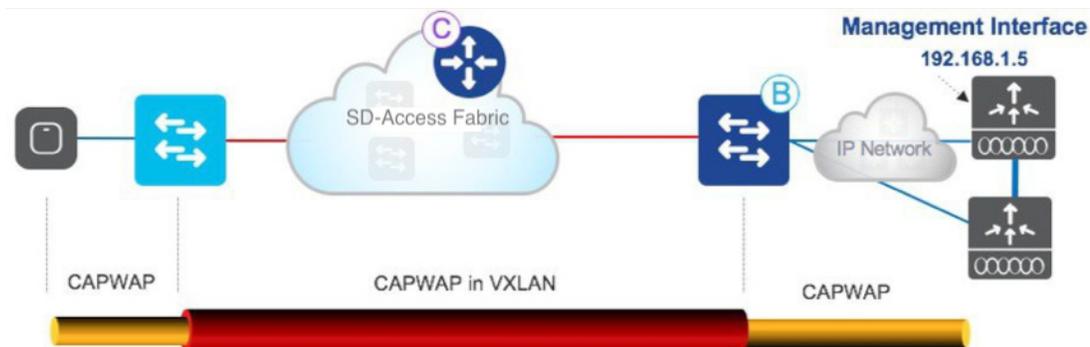
図 28. AP VLAN



アクセスポイントは単にファブリック インフラストラクチャの有線ホストであるため、ファブリックエッジスイッチのオーバーレイスペースに接続され、EID スペース内の特定のプールが割り当てられます。ファブリックの利点の1つは、すべての AP を1つの大きなサブネットに割り当てることができることです。これは、キャンパス全体で同じで、サブネットの設計を単純化し、オンボーディングの操作を簡素化します。

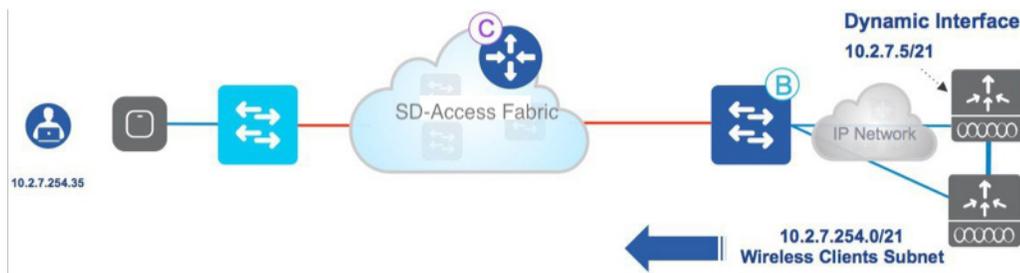
AP は有線クライアントのようなものなので、接続されているファブリックエッジスイッチによってファブリック コントロールプレーン ノードに登録されるため、ファブリック内でその位置がわかり、AP に到達します。この時点で、CAPWAP トンネルは、ファブリックを介して AP から WLC に形成されます (図 29 を参照)。

図 29. AP から WLC への CAPWAP トンネル



ワイヤレス LAN

図 30. ワイヤレス LAN 接続



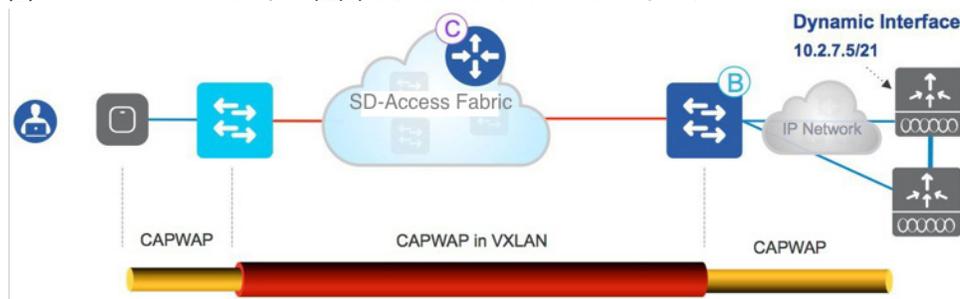
先ほど説明した、ワイヤレスが「そのまま」の状態で作動するというのは、WLC のワイヤレス SSID がダイナミック インターフェイスの形式で WLC の VLAN またはサブネットにマッピングされ、ワイヤレストラフィックが WLC の有線ネットワークに入り、そこでルーティングされるということです。

ボーダーノードは、ワイヤレスクライアントサブネットをファブリックにアダプタイズするため、ファブリックホストとワイヤレスクライアント間に接続を確立できるようになります。

クライアントトラフィックフロー

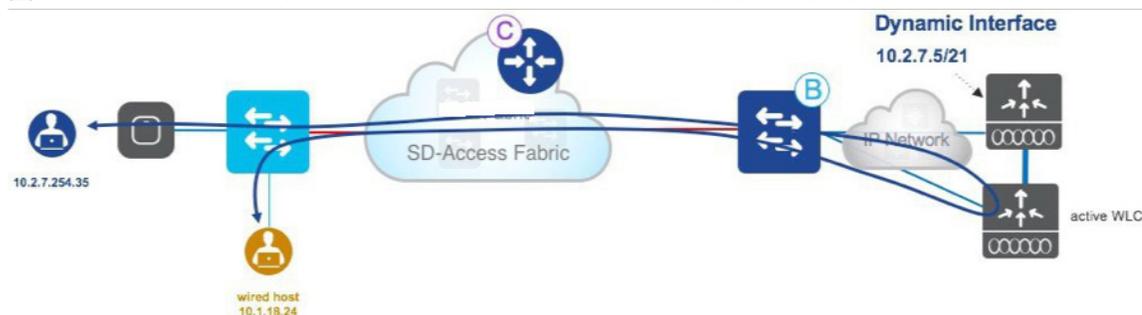
ワイヤレスクライアントがトラフィックを送信すると、CAPWAPトンネルがAPからWLCに構築されます。CAPWAPトラフィックは、APからファブリックエッジスイッチに到達し、VXLANにカプセル化して、ボーダーに転送します。外側のVXLANヘッダーは削除され、基礎となるCAPWAPパケットはWLCに転送されます。

図 31. CAPWAP トンネル経由のクライアントトラフィックフロー



Cisco Unified Wireless Network と同様に、クライアントは WLC によって認証およびオンボーディングされ、ワイヤレスクライアントトラフィックはファブリックの外部に送信されます。図 32 は、ワイヤレスクライアントとローカルのファブリック有線ホスト間の通信トラフィックフローを示しています。

図 32. ワイヤレスクライアントとローカルのファブリック有線ホスト間のトラフィックフロー



ワイヤレストラフィックは、WLC に至るまで送信され、WLC ダイナミック インターフェイス VLAN でブリッジされ、ボーダー経由でファブリッククライアントにルーティングされます。今日、この方法で通常の有線ネットワークは機能し、ワイヤレスでも同様です。ファブリックの場合は、ファブリックホストがファブリック外部の既知の宛先に通信します。

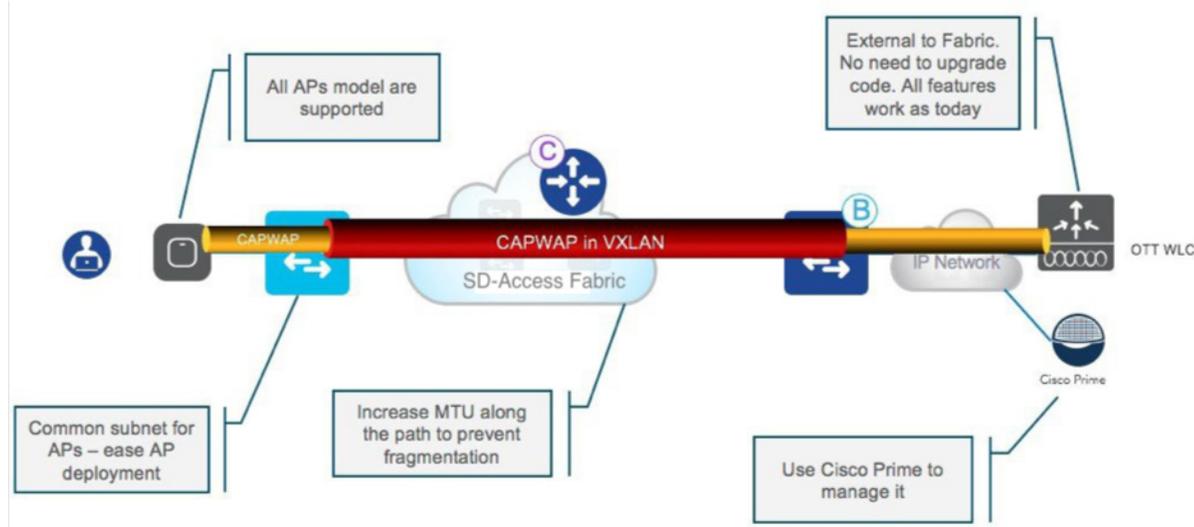
オーバーレイとしてのワイヤレス (OTT) : 設計考慮事項

OTT モードの重要な設計上の考慮事項のいくつかを要約します。

- すべての AP と WLC モードがサポートされます。ワイヤレスはファブリックに統合されていないため、ハードウェアおよびソフトウェアモデルに関する要件はありません。
- WLC はファブリックの外部に接続され、任意のコードバージョンをサポートしています。

- 二重 (VXLAN で CAPWAP) カプセル化によるパケットのフラグメント化を防ぐために、パスに沿った最大伝送ユニット (MTU) を増やすことをお勧めします。これは、パス内のすべてのスイッチがシスコ製品であり、ジャンボフレームをサポートする場合は、自動的に行われます。
- FCS では、OTT としてサポートされる唯一のモードは一元化されています。
- FCS では Cisco Prime を使用し、OTT ワイヤレス ネットワークを管理します。

図 33. OTT モードの設計上の考慮事項



SD-Access ワイヤレスネットワーク設計

SD-Access ファブリックのすべての利点を得るためには、統合された設計、したがって SD-Access ワイヤレスソリューションを選択する必要があります。アーキテクチャの見解から、統合は、次の 3 つの主な利点をもたらします。

- シンプルな管理およびコントロールプレーン：Cisco DNA Center は、ファブリックを起動し、数回クリックするだけでワイヤレス統合を設定するのに必要な自動化を提供します。集中管理型ワイヤレス コントロール プレーン (CAPWAP ベース) は、今日の Cisco Unified Wireless Network コントローラと同じ機能を提供します。
- 最適化されたデータプレーン：データプレーンは、通常生じる問題なしで分散されます。ファブリックのおかげで、複数のアクセススイッチにまたがる VLAN がなくなり、サブネット化が簡単になります。
- 統合されたポリシーとエンドツーエンドのセグメンテーション：ポリシーは補足的なものではなく、アーキテクチャ全体で一元的に統合されています。VXLAN ヘッダーは、VRF (VNID) と SGT の両方の情報を伝送し、エンドツーエンドの階層的なセグメンテーションを提供します。

図 34 は、統合設計の利点をまとめたものです。

図 34. 統合設計の利点

- **集中管理型ワイヤレス コントロールプレーン** : Cisco Unified Wireless Network 導入環境で提供されている革新的な RF 機能が、SD-Access ワイヤレスでも活用されます。IT 導入を簡素化させる無線リソース管理 (RRM) 、クライアント オンボーディング、クライアントモビリティなどに関して、ワイヤレスの運用は Cisco Unified Wireless Network の場合と同じです。
- **分散型データプレーンの最適化** : データプレーンは、トラフィックの分散に通常伴う処理 (VLAN のスパンニング、サブネット化、大規模なブロードキャストドメインなど) なしに最適なパフォーマンスと拡張性を実現するために、エッジスイッチに分散されます。
- **場所を問わないシームレスなレイヤ 2 ローミング** : SD-Access ファブリックにより、クライアントは同じ IP アドレスを保持しながらキャンパス全体でシームレスにローミングできます。
- **ゲストおよびモビリティのトンネリングの簡素化** : アンカー ワイヤレス コントローラ (WLC) が不要になり、フォーリンコントローラをホッピングせずにゲストトラフィックをネットワークエッジ (DMZ) に直接送信できます。
- **ポリシーの簡素化** : SD-Access では、ポリシーとネットワークの構成体 (IP アドレスや VLAN) との間の依存関係が解消されるため、有線クライアントとワイヤレスクライアントのポリシーを定義および実装する方法がシンプルになります。
- **セグメンテーションの簡略化** : セグメンテーションはファブリック内をエンドツーエンドで伝達され、仮想ネットワーク ID (VNI) とスケラブルグループタグ (SGT) に基づいて階層化されます。有線とワイヤレスの両方のユーザに同じセグメンテーションポリシーが適用されます。

ワイヤレス統合ソリューションの設計要素を簡単に分析します。

コントローラ

図 35. ファブリックに外部接続する WLC

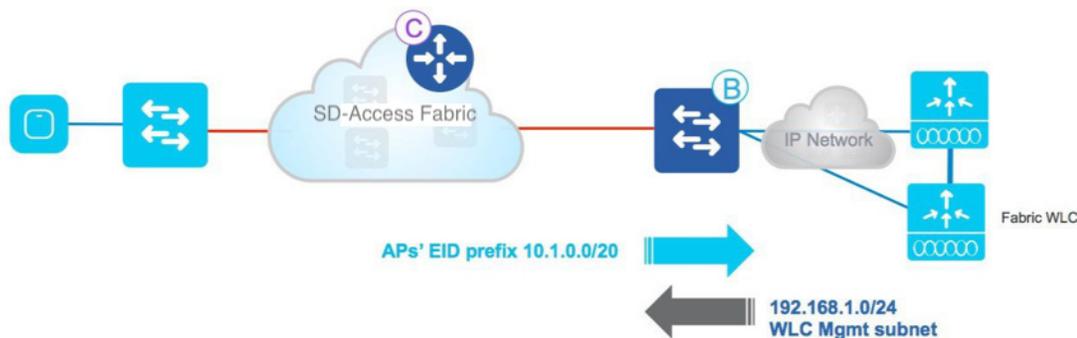


図 35 に示すように、外部からファブリックに WLC (または冗長性のために複数の WLC) を接続することを推奨します。

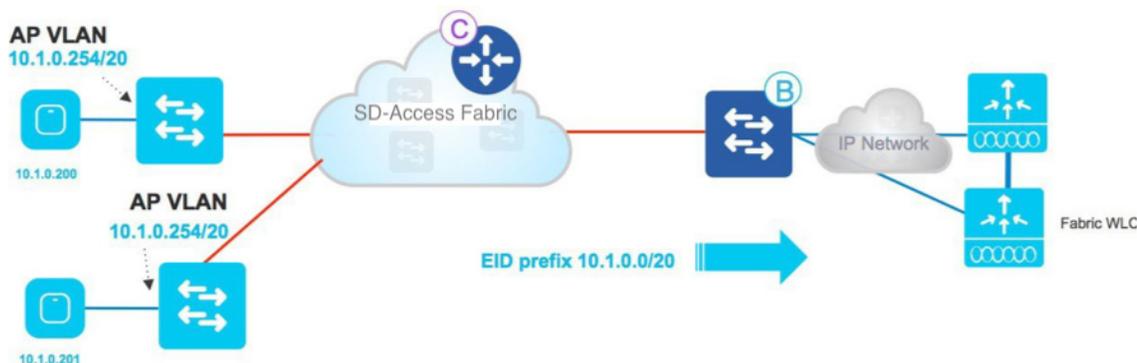
通常、WLC はネットワークの中央 (データセンターまたは共有サービス) に接続されているため、WLC はアクセススイッチであることの多いファブリックエッジノードには接続されていないのが現実的です。

WLC はファブリックの外側に位置するため、ボーダーノードは管理インターフェイスサブネット (この例では 192.168.1.0/24) と AP の IP プール (この例では 10.1.0.0/16) 間の到達可能性を提供し、CAPWAP トンネルが形成され、AP は WLC に登録できます。AP は、グローバルルーティングテーブルにマップされている INFRA_VRF にあるため、ルートリークは必要ありません。

また、WLC はアクセスポイントと同じ場所に配置する必要があります。この要件は Cisco Unified Wireless Network のローカルモード AP の場合と同じです。AP と WLC の間の最大遅延は 20 ミリ秒未満にする必要があります、これは通常、WLC を AP から WAN を介して配置できないことを意味します。

アクセスポイント

図 36. SD-Access ワイヤレスにおけるアクセスポイント

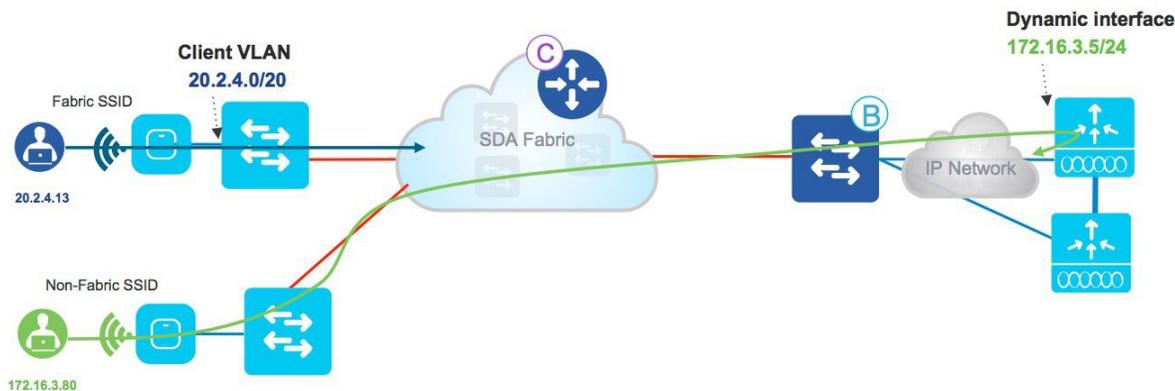


SD-Access ワイヤレスでは、AP をファブリックエッジノードに直接接続する必要があります。アクセスポイントはファブリック インフラストラクチャの「特別な」有線ホストであるため、ファブリックエッジスイッチのオーバーレイスペースに接続され、EID スペース内の特定のプールが割り当てられます。ファブリックの利点の1つは、すべての AP を1つの大きなサブネットに割り当てることができることです。これは、キャンパス全体で同じで、サブネットの設計を単純化し、オンボーディングの操作を簡素化します。

AP は有線クライアントのようなものなので、接続されているファブリックエッジスイッチによってファブリック コントロールプレーン ノードに登録されるため、ファブリック内でその位置がわかり、AP に到達します。AP は、OTT 設計について説明した際と同じ方法で、コントロールプレーンの機能のために WLC への CAPWAP トンネルを形成します。

ワイヤレス LAN

図 37. SD-Access ワイヤレスにおけるワイヤレス LAN



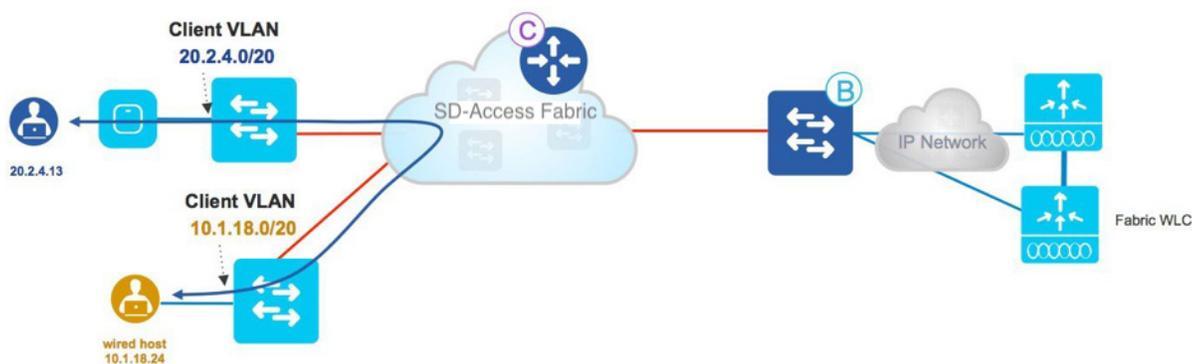
ファブリック機能は WLAN 単位で有効になります。ファブリック対応の WLAN の場合、クライアントトラフィックは分散され、中央コントローラには送られません。AP の VXLAN にカプセル化されて最初のホップのスイッチに送信されます。

一元化された CAPWAP WLAN は、共通のファブリック対応 WLC を使用して、同一または異なる AP 上のファブリック対応の WLAN と共存できます。これは「混合モード」と呼ばれ、Cisco DNA Center 1.1 で、既存のファブリックまたは Cisco Unified Wireless Network ワイヤレス構成を持たない WLC 展開をサポートしているため、新しい展開の場合にのみ使用できます。

クライアントフロー

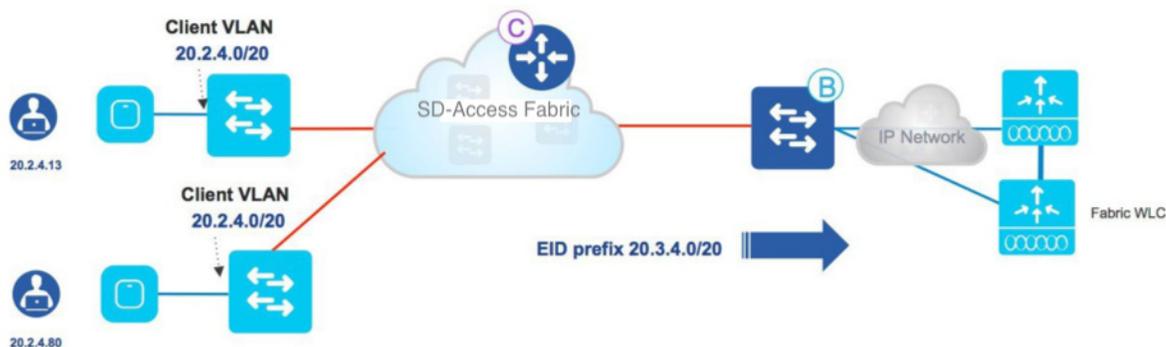
ファブリック対応 SSID の場合、ワイヤレスクライアントトラフィックはスイッチで分散されるため、中央コントローラへのヘアピニングはありません。有線クライアントへの通信は、ファブリックを通じて直接行われ、最適化されます。

図 38. SD-Access ワイヤレスにおけるクライアントフロー



クライアントサブネットはファブリックエッジスイッチに分散され、WLC で動的インターフェイスとクライアントサブネットを定義する必要はありません。クライアントサブネットは、すべてのファブリックエッジスイッチでエニーキャストゲートウェイを使用して定義され、VLAN にマッピングされます。これは、ワイヤレスクライアントがどこに接続しても、サブネットのために同じゲートウェイと話すことができることを意味します。つまり、クライアントはどこにでも元の IP アドレスを保持できます。言い方を換えれば、ファブリックのすべてのワイヤレスローミングはレイヤ 2 のローミングということもできます。

図 39. SD-Access ワイヤレスにおけるクライアントサブネット



SD-Access ワイヤレスゲストアクセス設計

ゲスト設計を検討する場合、ファブリックとの統合により3つの異なるソリューションが提供されます。

- ゲストアンカーコントローラを活用する OTT ソリューション
- 専用のゲスト仮想ネットワーク
- 専用のゲストファブリックドメイン

Cisco Unified Wireless Network ゲストアンカーを活用する OTT ソリューション

図 40. ゲストアンカーコントローラを活用する OTT ソリューション

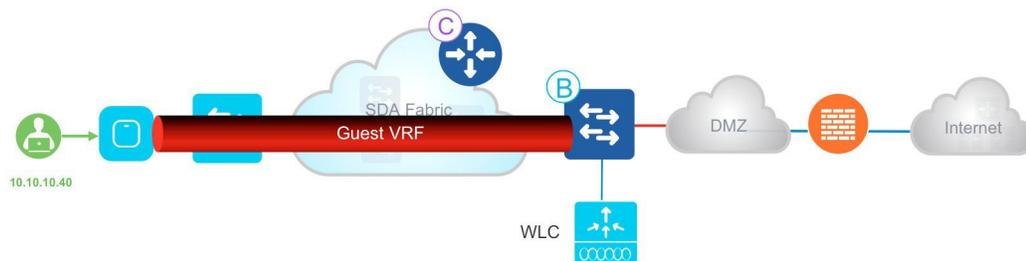


ゲスト無線ネットワークを OTT として展開することにより、ゲストアンカーコントローラへの投資を引き続き活用できます。ゲスト用の WLAN は、DMZ のゲストアンカーコントローラに固定されるように設定され、トラフィックはファブリックへのオーバーレイになります。この実績のある Cisco Unified Wireless Network ソリューションはお客様の投資を保護し、特にブラウンフィールド（既存環境）への導入に最適です。もちろん、このソリューションには、Cisco Unified Wireless Network ソリューションから継承された制限があります。

- ゲストトンネル数は 71 に制限されています。
- 有線ゲストに対応する別のソリューションがあり、アンカー WLC とは異なる方法で管理されます。

ゲスト専用 VN

図 41. 専用のゲスト VN



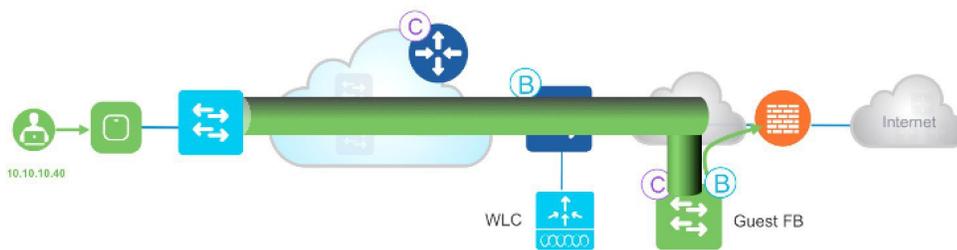
この設計では、ゲストネットワークは SD-Access ファブリック内のもう 1 つの VN であるため、ゲストデータプレーンを別のエンタープライズトラフィックから分離するために、エンドツーエンドのファブリック セグメンテーション (VNI と SGT を必要に応じて異なるゲストロールに使用) を活用します。ゲスト VN を作成し、IP プールを定義し、SSID をゲスト用の 1 つ以上のプールに関連付けることによって、Cisco DNA Center によって設定されます。このアプローチが前述のソリューションと比べて優れている主な点の 1 つは、これが有線と無線のゲストユーザにとって一貫したソリューションとポリシーであることです。

個別のファブリックドメインとしてのゲスト

データプレーントラフィックだけでなく、コントロールプレーンのためにゲストネットワークを完全に隔離する必要がある場合、Cisco DNA Center では専用のゲストコントロールプレーンとボーダー (基本的に専用のファブリックドメインである) を設定して、ゲストユーザを管理できます。

このソリューションでは、トラフィックは VXLAN の AP でファブリックエッジスイッチにカプセル化されていますが、FE は別のボーダーノードを使用するように設定されています。このボーダーノードは DMZ に存在でき、ゲストアンカーソリューションと同様の完全なトラフィック分離を提供します。ゲストユーザは専用 CP (ボーダーと同じ場所に配置される場合もされない場合もある) に登録され、DMZ 内でユーザに IP アドレスが割り当てられます。

図 42. ゲストコントロールプレーンおよびボーダー



前述の VN ソリューションと同様に、この設計は有線と無線のゲストに対してポリシーの一貫性を提供します。ゲストコントロールプレーンとボーダーの選択は、ソリューションの拡張性によって異なります。

ゲストボーダーからのハンドオフは手動プロセスで、管理者は DMZ 内の外部ノードへのハンドオーバーを行うためのスタティックルートを含む適切なプロトコルを選択できます。

SD-Access ワイヤレスでのマルチキャスト

SD-Access ワイヤレスでのマルチキャストについて知っておくべき重要な点を次にいくつか示します。

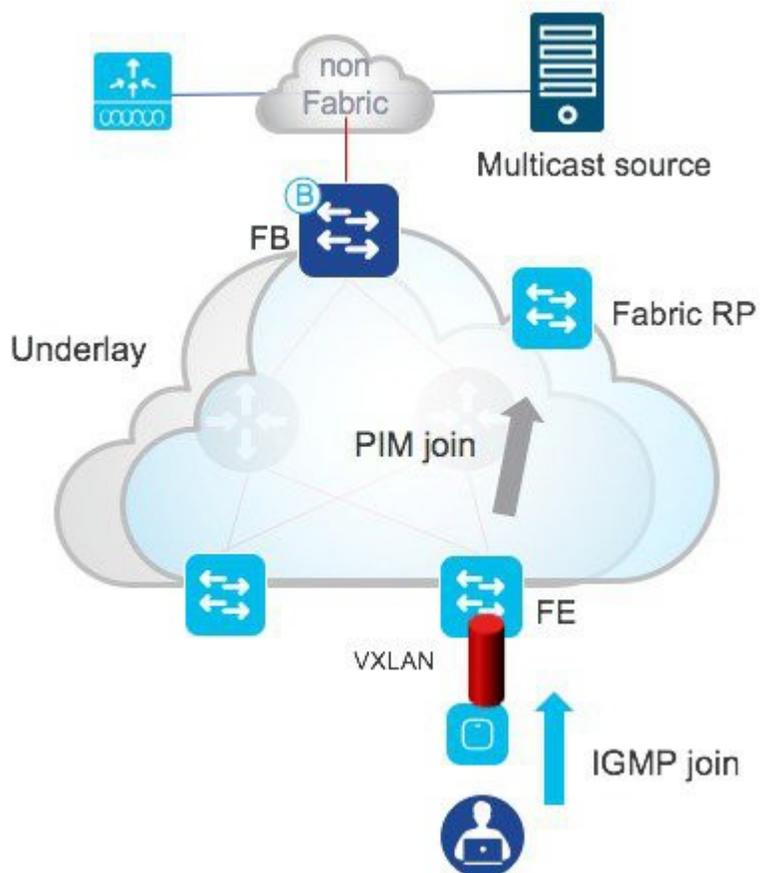
- マルチキャストトラフィックは、有線クライアントとワイヤレスクライアントの両方に対して、オーバーレイの EID スペースに転送されます。
- ワイヤレスでマルチキャストを有効にするには、WLC でグローバル マルチキャスト モードと Internet Group Management Protocol (IGMP) スヌーピングをグローバルに有効にする必要があります。

- Cisco DNA Center 1.3 では、ファブリック内のマルチキャストトラフィック転送で、ヘッドエンドレプリケーションとネイティブ転送の2つの方法が使用されます。これらの方法では、アンダーレイでのマルチキャストトラフィックの転送方法が異なります。ヘッドエンドレプリケーションでは、アンダーレイネットワークをマルチキャスト対応にする必要はありません。ファブリックへ送信されるマルチキャストトラフィックが複数のユニキャスト VXLAN トンネル（一部のマルチキャストレシーバが接続されているファブリックエッジノードごとに1つ）に複製されるため、この方法は最適ではありません。ネイティブマルチキャストの場合、アンダーレイをマルチキャスト対応にする必要があります。オーバーレイのマルチキャストトラフィックはアンダーレイマルチキャストで転送されるため、この方法は効率的です。パケットの複製は、関係するレシーバの場所に基づいてネットワークによって実行されます。

ここでは、マルチキャストのしくみについて説明します。

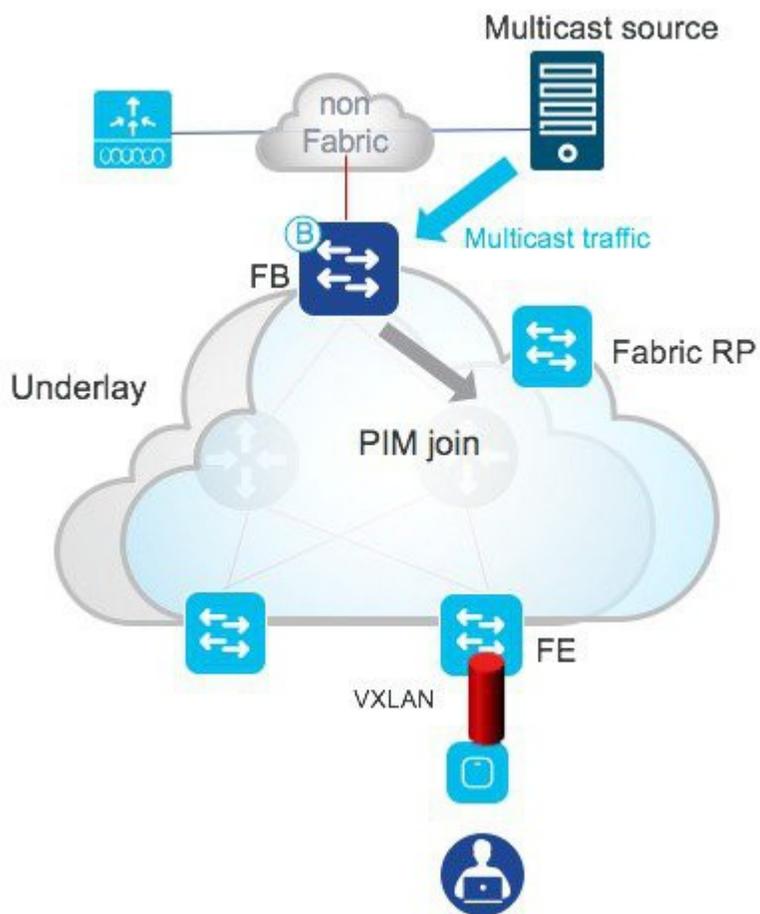
- マルチキャストクライアント（レシーバ）はオーバーレイにあります。マルチキャスト送信元はファブリックの外側にもオーバーレイ内にもあります（図 43 では送信元はファブリックの外側に表示されています）。
- オーバーレイで PIM スパースモード（PIM-SM）または PIM 送信元特定マルチキャスト（PIM-SSM）を実行する必要があります（VRF ごとに有効にする必要があります）。
- クライアントは特定のマルチキャストグループに対して IGMP Join を送信します。
- AP はそれを VXLAN にカプセル化し、アップストリームスイッチに送信します。
- ファブリックエッジノードはそれを受信し、ファブリック ランデブー ポイント（RP）に対して PIM Join を実行します（PIM-SM が使用されていると仮定します）。
- RP はエンドポイント IP スペースの一部としてオーバーレイに存在する必要があります。
- 図 43 に、上記の手順を示します。

図 43. SD-Access ワイヤレスでのマルチキャスト



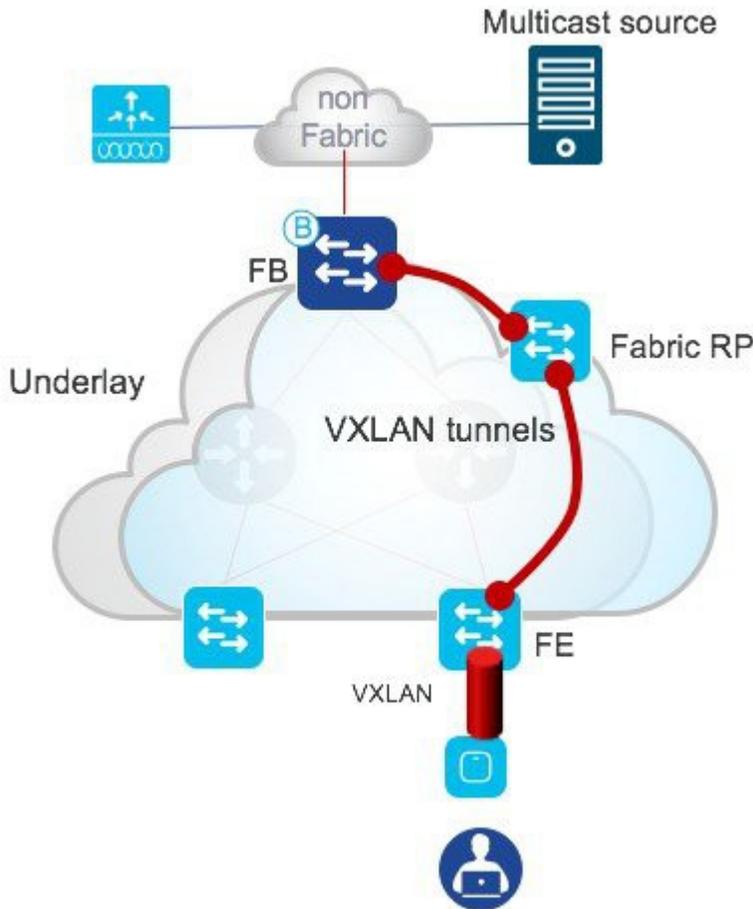
- この例では、マルチキャスト送信元は、ファブリックの外にあるため、そのセグメントの代表ルータであるファブリックボーダーに向けてインターフェイス上でマルチキャストトラフィックを送信します。
- FB はトラフィックを受信し、RP に対して PIM Join を実行します (PIM-SM が使用されていると仮定します)。
- これで、RP には、そのマルチキャストグループの送信元と受信側情報が入るようになりました。

図 44. SD-Access ワイヤレスでのマルチキャスト
(北から南)



- これで、RP には、特定のマルチキャスト グループの送信元と受信側情報が入るようになりました。
- FB は VXLAN トンネルを介してマルチキャスト送信元のトラフィックを RP に送信し、RP はそのトラフィックを別の VXLAN トンネルを介して FE に転送します。
- FE は VXLAN パケットを受信し、カプセル化解除してポリシーを適用し、VXLAN トンネルを介して再び AP に転送します。
- AP は、VXLAN ヘッダーを削除し、電波に元の IP マルチキャストパケットを送信します。

図 45. SD-Access ワイヤレスでのマルチキャスト



- 最初のマルチキャストパケットが FE に配信されると、最短パスフェールオーバー (SPT) が発生し、トラフィックは FB と FE 間で直接転送されます。
- FE は、受信した最初のマルチキャストパケットに基づいて FB がマルチキャスト送信元を所有していることを認識し、そのマルチキャストグループの FB に直接 PIM Join を送信します。
- これで FB は特定のマルチキャストグループを要求したクライアントを持つ FE を認識するようになりました。
- ヘッドエンド レプリケーションまたはネイティブマルチキャストを実行し、VXLAN はマルチキャストトラフィックをカプセル化し、それを関係する FE に転送します。
- マルチキャストトラフィックがオーバーレイに送信されます。
- FE は VXLAN パケットを受信し、カプセル化解除してポリシーを適用し、再び AP に転送します。
- AP は、VXLAN ヘッダーを削除し、電波に元の IP マルチキャストパケットを送信します。

SD-Access ワイヤレスのハイアベイラビリティ

SD-Access ワイヤレスソリューションの最も重要なコンポーネントは、WLC およびコントロールプレーンノードです。有線ファブリッククライアントと比較して、コントロールプレーンはワイヤレスでさらに重要な役割を果たします。クライアントロケーション情報を更新する役割を果たすため、クライアントローミングにおいて重要です。

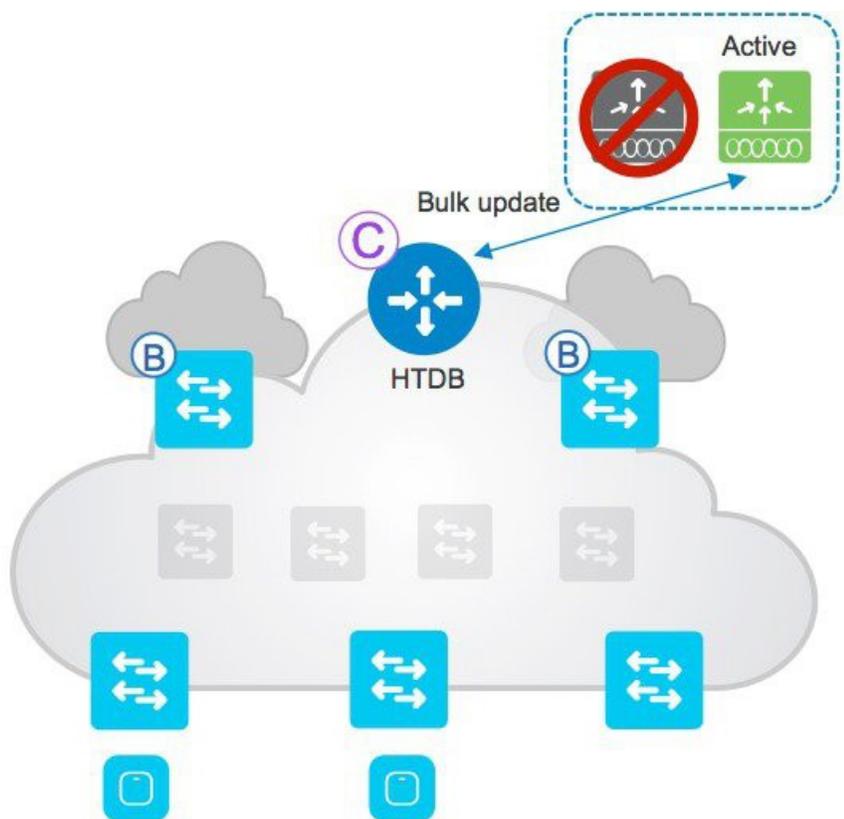
WLC と CP はどちらもハイアベイラビリティをサポートします。

コントローラの冗長性

コントローラのハイアベイラビリティでは、ファブリック対応コントローラに対する N+1 と SSO の両方の使用がサポートされています。

SSO を使用したステートフル冗長性

図 46. ステートフル スイッチオーバー

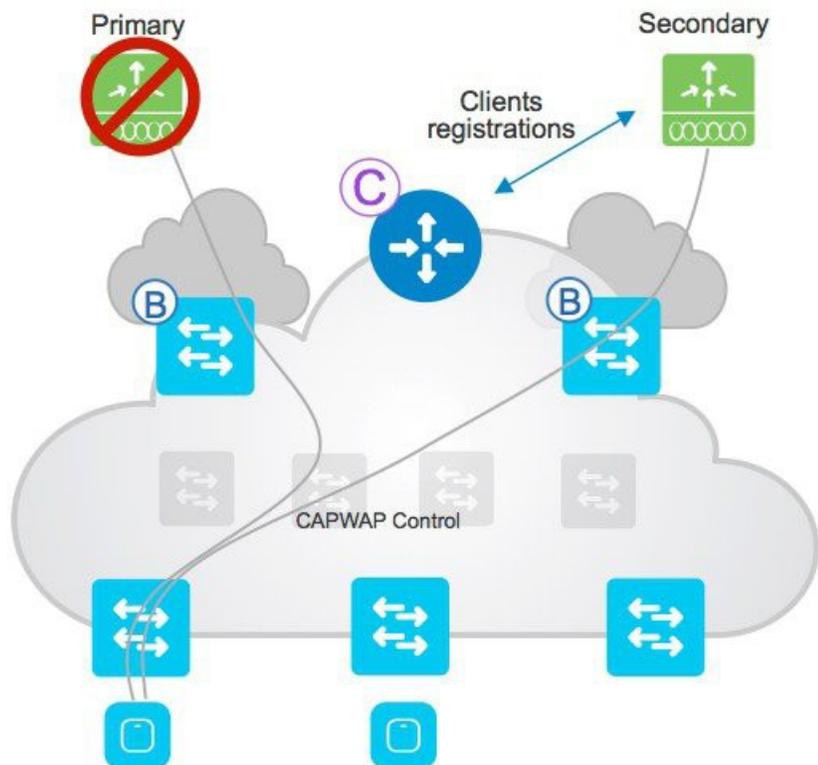


- WLC SSO ペアをファブリックは1つのノードと見なします。
- アクティブ WLC のみが CP ノードと通信します。
- ファブリック設定と CP 状態はアクティブ WLC とスタンバイ WLC の間で同期されます。
- 障害時は、新しいアクティブ WLC がファブリッククライアントをホストトラッキングデータベースノードに一括更新します (LISP 更新)。
- AP とクライアントは接続を維持します。

設計の項で説明したように、FCS では WLC がファブリックの外部に接続されているため、SSO ペアの接続に関する通常の考慮事項が適用されます。つまり、2つのコントローラ間の帯域幅および遅延要件は Cisco Unified Wireless Network アーキテクチャと同様です。

N+1 を使用したステートレス冗長性

図 47. N+1 冗長



ステートフル HA を必要としない場合は、N+1 の冗長性がサポートされます。N+1 の冗長性は Cisco DNA Center 1.3 まで自動化されていません。この機能のサポートについては、Cisco DNA Center のロードマップを参照してください。重要な考慮事項は次のとおりです。

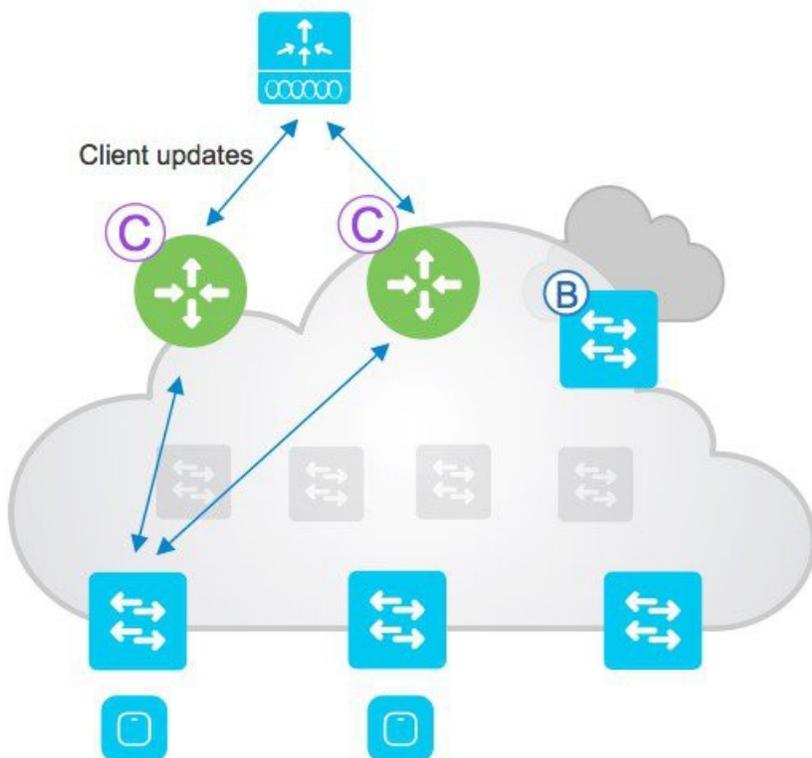
- AP はプライマリとセカンダリを使用して設定されます。
- AP と接続しているクライアントはプライマリに登録されます。
- プライマリの障害時、AP は接続を解除し、セカンダリに参加します。
- クライアントも接続を解除し、セカンダリに参加します。
- セカンダリはホスト トラッキング データベースに新規のクライアント登録を行います。



(注) N+1 の冗長性は Cisco DNA Center 1.3 まで自動化されていません。この機能のサポートについては、Cisco DNA Center のロードマップを参照してください。

コントロールプレーンの冗長性

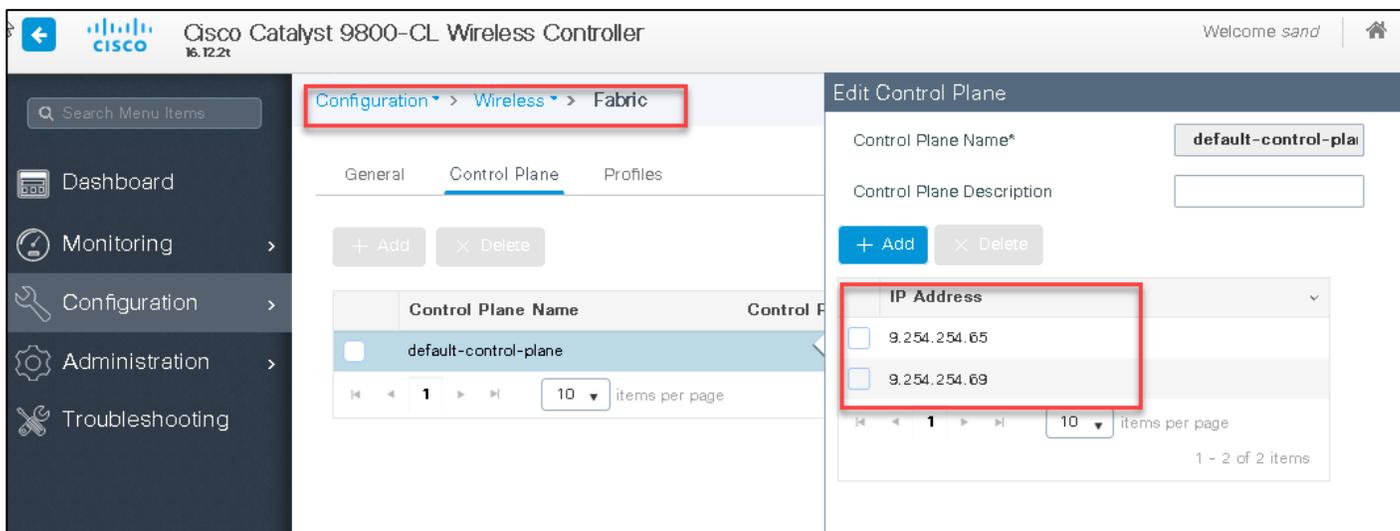
図 48. コントロールプレーンの冗長性



- コントロールプレーンノードの冗長性は、アクティブ/アクティブ設定でサポートされています。WLC（およびファブリックエッジ）は2つのCPノードで設定され、両方に情報を同期させます。
- 1つのCPノードで障害が発生した場合、すべてのクライアント情報はもう1つのCPノードで使用できます。WLCの設定（Aire-OSの参考用スクリーンショット）を次に示します。



Catalyst 9800 WLC の参考用スクリーンショット：



付録 : SD-Access ワイヤレス機能の詳細情報

次の表に、SD-Access ワイヤレスアーキテクチャでサポートされている主要な機能の一部を示します。

表 1 : SD-Access ワイヤレスアーキテクチャでサポートされている主要な機能

オープン/スタティック Wired Equivalent Privacy (WEP)	サポート対象
事前共有キーによるワイヤレス保護アクセス (WPA-PSK)	サポート対象
802.1X (WPA/WPA2)	サポート対象
MAC フィルタリング	サポート対象
ローカル拡張可能認証プロトコル (EAP)	サポート対象
AAA Override	サポート対象
内部/外部 Web 認証	サポート対象
事前認証アクセスコントロールリスト (ACL)	サポート対象
クライアントの IPv4 ACL	サポート対象 (SGT を優先し、推奨)
Application Visibility and Control (AVC)	サポート対象*
ローカルプロファイリング	サポート対象
RADIUS プロファイル	サポート対象
QoS プロファイル	サポート対象
ユーザ単位の帯域幅コントラクト	サポート対象
ワイヤレス侵入防御システム (wIPS)	サポート対象
Cisco Connected Mobile Experiences (CMX) 統合	サポート対象
NetFlow エクスポート	サポート対象
HA SSO	サポート対象

*Wave 2 AP のみ

ここで、ファブリックネットワークでの動作を理解するために、いくつかの機能について説明します。

AAA Override

ISE は SD-Access ワイヤレス SSID のファブリック インターフェイス名、ACL、QoS、SGT などのパラメータをオーバーライドできます。

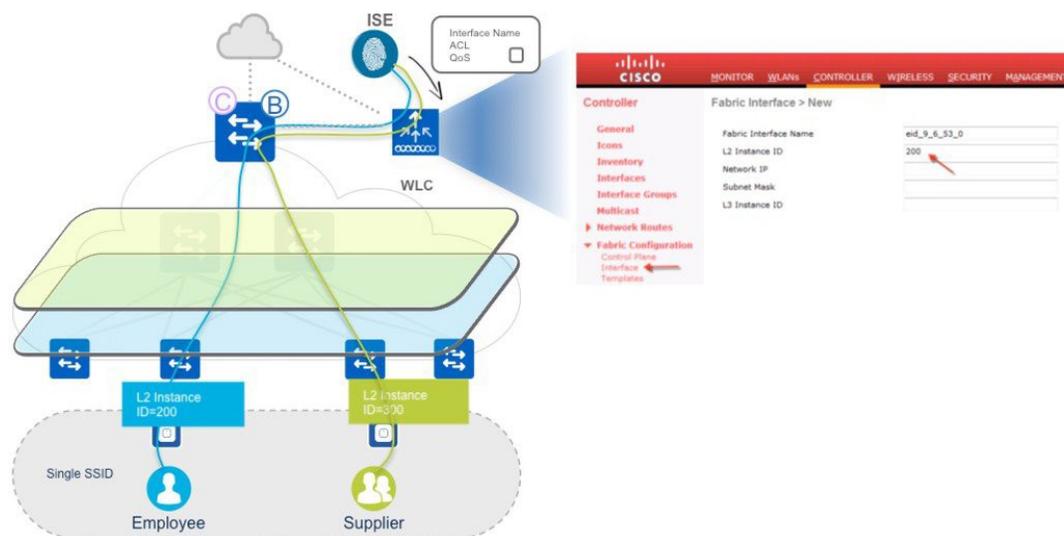
ファブリック インターフェイス名のオーバーライド

クライアントの認証と役割に基づいて、同じ SSID を異なるプールまたはサブネットにマッピングする場合はどうすればよいでしょうか。Cisco Unified Wireless Network では、このために VLAN オーバーライドを使用して、VLAN ID (名前または番号) を AAA サーバから WLC に戻します。

ファブリックでは、VLAN にはローカルスイッチだけがあり、IP プールにマップされるのはレイヤ 2 VNID です。これは、サブネットまたはプールに関連付けられているネットワーク識別子で、ワイヤレスでは SSID に関連付けられています。レイヤ 2 VNID は、AP から VXLAN ヘッダーのスイッチに転送されます。レイヤ 2 VNID は最終的に、ファブリックエッジスイッチで VLAN に、それから SVI (エニーキャストゲートウェイ) に、その後、レイヤ 3 VNID (VRF) にローカルマッピングされます。

SD-Access ワイヤレスでは、さまざまなプールを区別するためにレイヤ 2 VNID を渡す必要があります。ISE または他の AAA は VNID を直接使用しないため、Cisco Audio-Video Protocol (AVP) の Aire-Interface-Name または Interface-Name を使用して、クライアント認証時に特定の名前を返します。クライアントのレイヤ 2 認証は常にコントローラで行われるため、ISE と通信してそのインターフェイス名の値を取得し、レイヤ 2 VNID にマッピングするのは WLC です。

図 49. AAA Override



ISE では、特定のグループ認証プロファイルを設定して、次のスクリーンショットに示すように特定のインターフェイス名を返す必要があるため、ユーザが認証すると ISE は RADIUS ACCEPT_ACCEPT メッセージの特定の属性を返します。

▼ Advanced Attributes Settings

Airespace:Airespace-Interface-Nar = eid_9_6_53_0

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-Interface-Name = eid_9_6_53_0

ファブリック インターフェイス名は、次のようなマッピングを使用してレイヤ 2 インスタンス ID にマッピングされます。重要：Cisco DNA Center を設定すると、このマッピングと設定はすべて自動的に行われます。

The screenshot shows the Cisco DNA Center interface for configuring a new Fabric Interface. The sidebar on the left has a red arrow pointing to the 'Interface' option under 'Fabric Configuration'. The main form has the following fields:

Fabric Interface Name	eid_9_6_53_0
L2 Instance ID	200
Network IP	
Subnet Mask	
L3 Instance ID	

レイヤ 2 インスタンス ID は AP に送信され、VXLAN ヘッダーに埋め込まれます。

ACL および QoS プロファイルの AAA オーバーライド

WLC のファブリック ACL は AP に適用されます。ローカル WLC ACL とファブリック ACL の主な違いは、ファブリック ACL は方向を関連付けられていないことです。ファブリック SSID では、Flex ACL が SSID に設定されます。同じ ACL がインGRESS とイーGRESS 両方に適用されます。

ACL の AAA オーバーライドの場合：

- オーバーライド ACL 名は AP のファブリック ACL (Flex ACL) である必要があります。
- ACL テンプレートは ACL の AP へのプッシュに使用できます。

Controller

General
Icons
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Fabric Configuration
Control Plane
Interface
Templates
Redundancy
Mobility Management
Ports

Fabric ACL Template > Edit

Fabric ACL Template Name ACL Template
Status Modified

ACL

Fabric ACL

ca-redirect-acl	<input type="button" value="v"/>
cwa-redirect-acl	<input type="button" value="v"/>
test	<input type="button" value="v"/>

WLANs

WLANs
Advanced
AP Groups

Ap Groups > Edit 'default-group'

General | **WLANs** | APs | 802.11u | Location | Ports/Module

AP Group Name default-group
AP Group Description
NAS-ID none
Enable Client Traffic QoS
Enable DHCPv4 QoS
QoS Service Vlan Id
Fabric Flex ACL ACL Template



(注) IP ACL はサポートされていますが、SD-Access でセキュリティポリシーを適用する推奨方法は SGT の使用です。

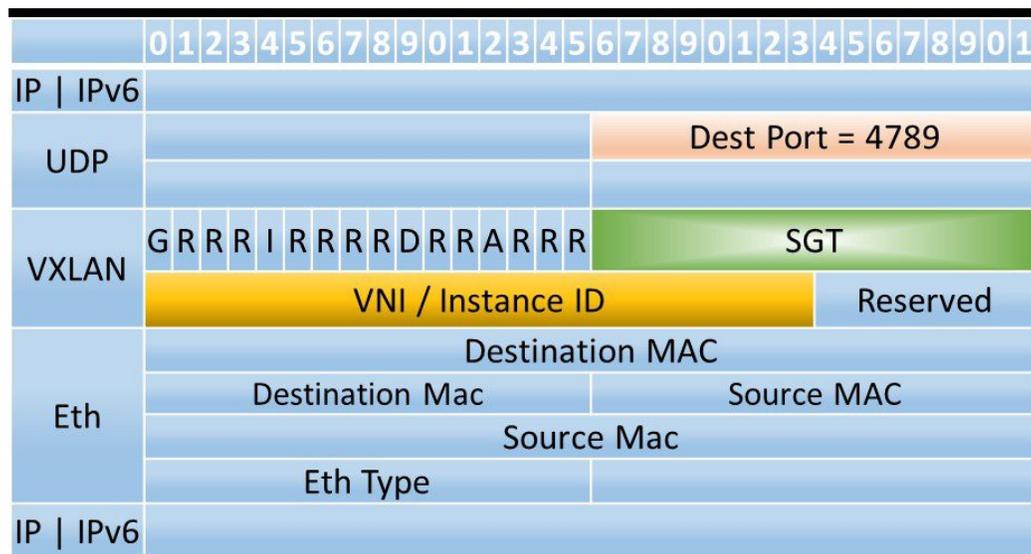
QoS プロファイル名のオーバーライドの場合：

- QoS プロファイル名は ISE からプッシュされます。
- アップストリームおよびダウンストリーム QoS が AP で適用されます。
- VXLAN トンネル QoS は内部ヘッダーから取得されます。

SGT を使用したグループベースのポリシー

WLC は、クライアントが接続した際に、ワイヤレスクライアントに使用する SGT を AP に送信します。AP は、ワイヤレスクライアントからアクセススイッチに VXLAN トンネル経由でデータパケットを転送するときに、VXLAN ヘッダーにこの SGT を追加します。この SGT はファブリックを介してエンドツーエンドに伝送されます。

図 50. VXLAN ヘッダーには SGT および VNI が含まれます



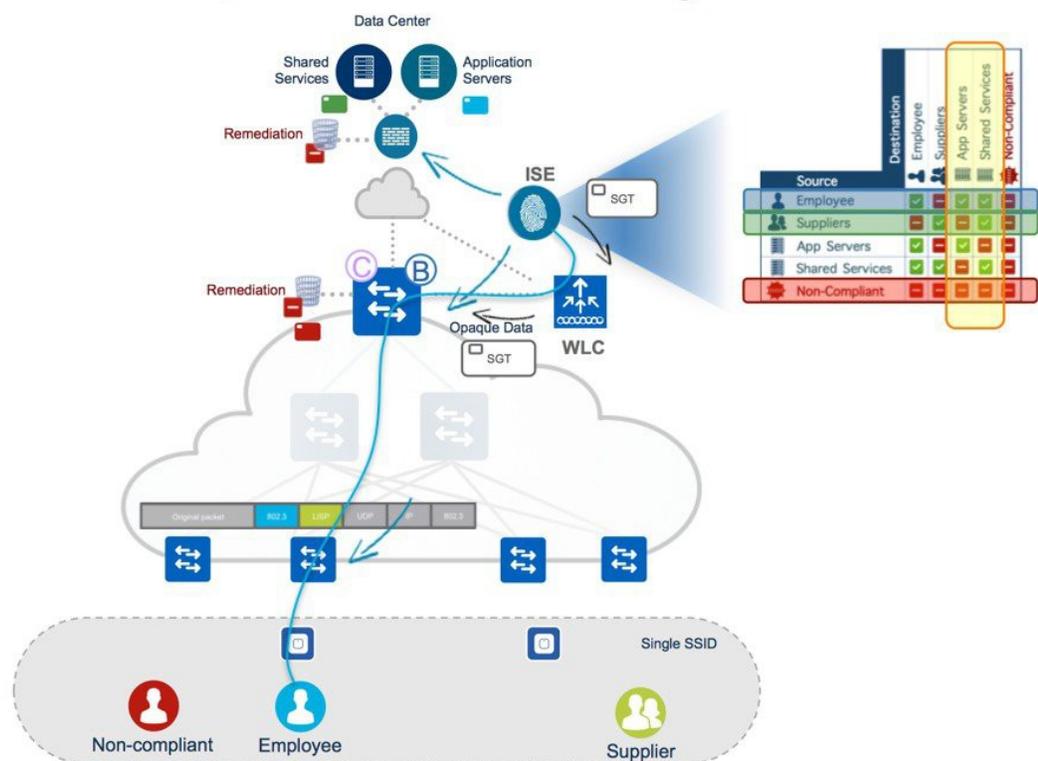
イーグレスアクセススイッチでは、SGT と DGT のペアで適用する SGACL を判断します。SGT はパケットに含まれており、DGT は宛先ホストの IP バインドに基づいて導かれます。

ワイヤレスクライアントのためにアクセススイッチに SGACL を適用する場合（アクセススイッチ（VXLAN トンネル送信元）のワイヤレスクライアントに向かうトラフィックに対する適用）、タグ（SGT と DGT）はスイッチで取得される必要があります。

次の手順は、グループベースポリシーのフローです。

- クライアントのレイヤ 2 認証が WLC で発生します。
- WLC はクライアント接続時に SGT を AP に送信します。
- WLC はクライアント登録時に CP を SGT で更新します。
- CP は FE を隠されたデータの SGT を使用して更新します。受信した SGT に基づいて、スイッチは ISE からポリシーをダウンロードします。
- AP はこの SGT を VXLAN ヘッダーに追加します。
- SGT は LISP ヘッダーのファブリックを介してエンドツーエンドで伝送されます。
- イーグレススイッチでは、SGT と DGT のペアによってパケットヘッダーの SGT に基づいて SGACL が判断されます。

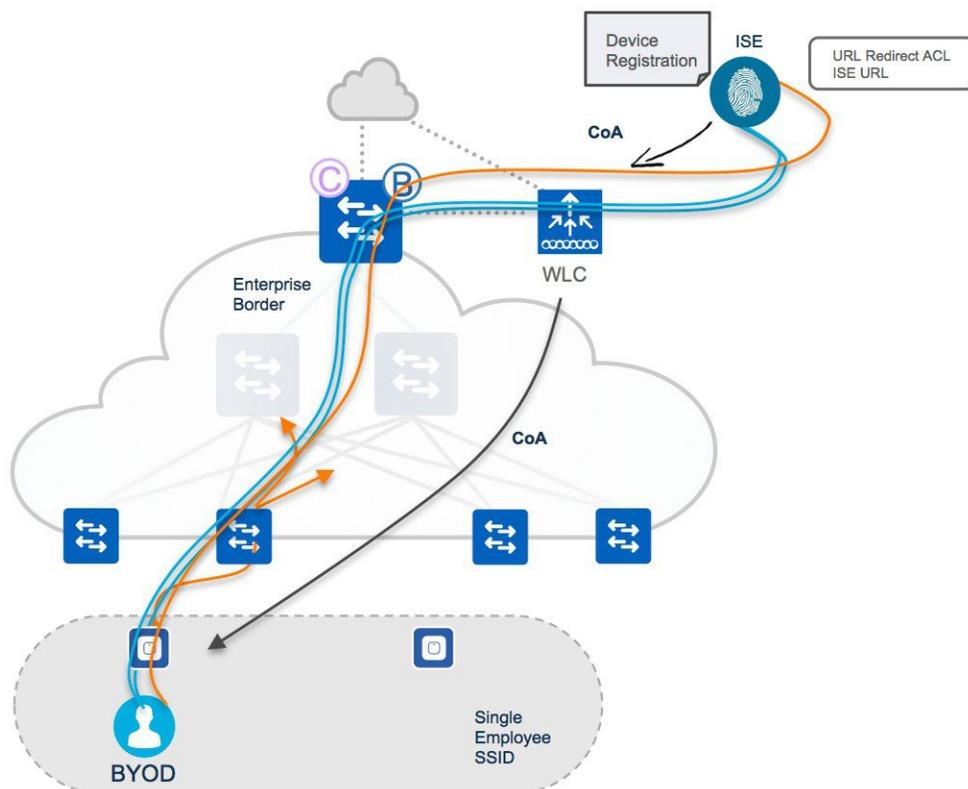
図 51. グループベースポリシーの SGT



CWA と BYOD の ISE

この項では、中央 Web 認証 (CWA) の基本的なフローについて説明します。これは、Cisco DNA Center の自動化でサポートされている唯一の種類の Web 認証です。

図 52. ISE を使用した CWA



1. レイヤ 2 認証が ISE サーバで発生します。MAC フィルタリングは、WLC で設定する必要があります。
2. クライアント認証フェーズ中に、URL リダイレクト ACL (Flex ACL タイプ) とリダイレクト URL が AP にプッシュされます。
3. クライアントトラフィックは、VXLAN トンネルでのデバイス登録とネイティブ サブリカント プロビジョニングのために ISE ポータルにリダイレクトされます。
4. 完了すると、ISE は認可変更 (CoA) を WLC に送信し、WLC は CoA を AP にプッシュします。
5. 次に、クライアントは EAP-TLS を使用して再認証します。デバイスは ISE サーバにとって既知となったため、認証が成功し、以降のデータトラフィックは AP から VXLAN さらにファブリックエッジにスイッチされます。

フローは次のとおりです。

1. レイヤ 2 認証が WLC で発生し、クライアントは WEBAUTH_REQD 状態に移行します。
2. HTTP リダイレクトが WLC で発生します。
3. Web 認証が内部 (WLC でホストされる Web ページ) または外部 (外部サーバでホストされる Web ページ) で発生します。
4. トラフィックは外部ローカル Web 認証の事前認証 ACL と一致すると、VXLAN トンネルでスイッチされます。内部 Web 認証の場合、トラフィックは CAPWAP を介して WLC に送信されます。
5. レイヤ 3 認証が完了すると、クライアントは RUN 状態になり、事前認証 ACL は削除されます。
6. ゲストデータトラフィックは FE から DMZ 内のゲストボーダーノードにスイッチされます。内部 Web 認証の場合、トラフィックは CAPWAP を介して WLC に送信されます。



(注) すべての設定は、WLC のユーザインターフェイスで直接実行する必要があります。

©2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2020 年 8 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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