# Cisco Catalyst Center を使用した Cisco SD-Access LISP の展開（CVD）

2025 年 5 月 5 日

# はじめに

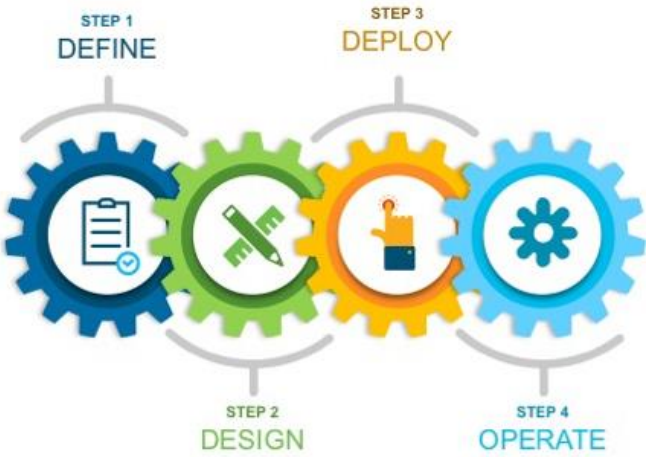
## このマニュアルについて

このガイドは、Cisco Catalyst Center を使用してシスコのソフトウェア定義型アクセス（Cisco SD-Access）ネットワークを設計、展開、および運用するための技術的なガイダンスを提供することを目的としています。

このドキュメントの対象読者には、Catalyst Center を使用してキャンパスネットワーク内に Cisco SD-Access ネットワークを実装する必要があるネットワーク設計エンジニアとネットワーク運用担当者が含まれます。

このガイドでは、Catalyst Center を使用して Day-0 と Day-*N* の運用で Cisco SD-Access ネットワークを設計および展開する方法と、Cisco SD-Access ネットワークの全体的な正常性を監視する方法に焦点を当てています。

**図 1.　　実装フロー**




このドキュメントの主なセクションは、次のとおりです。

- 「Cisco SD-Access ネットワークの定義」セクションでは、Cisco SD-Access ネットワークの主要なコンポーネントを含む Cisco SD-Access の概要と、Catalyst Center を使用して Cisco SD-Access の有線およびワイヤレスネットワークを展開する際の設計上の考慮事項について説明します。
- 「Cisco SD-Access ネットワークの設計」セクションでは、Catalyst Center と Cisco Identity Services Engine（Cisco ISE）の統合、サイト階層の作成、AAA、DNS、DHCP、NTP、SNMP、Syslog サーバーなどの、ネットワークの運用に必要なさまざまなネットワークサービスの設定、WLAN 展開用の SSID、VLAN、および RF プロファイルを持つ WLAN を含むワイヤレス設定の設定、ファブリックサイト、ファブリックゾーン、仮想ネットワーク、およびエニーキャストゲートウェイの有効化、ファブリックサイトでの関連付け、Cisco SD-Access と IP トランジットの設定について説明しています。
- 「Cisco SD-Access ネットワークの展開」セクションでは、ファブリックボーダーとコントロールプレーンノードとしてのファブリックサイトでのデバイスの検出およびプロビジョニング、Day-0 のデバイスのオンボーディングとファブリックエッジとしてのプロビジョニングのための LAN 自動化、Catalyst 9000 デバイスとスタンドアロン ワイヤレス コントローラの組み込みワイヤレスコントローラの設定、レイヤ 3 ハンドオフとレイヤ 2 ハンドオフの設定、マルチキャストの有効化について説明します。

  また、ボーダー設定とエニーキャストゲートウェイ設定でサポートされる属性と機能についても説明します。

- 「Cisco SD-Access ネットワークの運用」セクションでは、Cisco SD-Access ネットワークでの Day-N の運用について説明します。これには、アクセスポイント（AP）のオンボーディング、さまざまなタイプの拡張ノードとクライアント、ファブリック機能の修正と変更、RMA 手順で障害が発生したデバイスの交換、ファブリックサイトからのファブリックデバイスの削除、ファブリックサイトの切断が含まれます。
- 「Cisco SD-Access ネットワークと Cisco SD-Access アプリケーションの監視」セクションでは、Cisco Catalyst Assurance を使用して Cisco SD-Access ネットワーク展開を監視およびトラブルシューティングする方法について簡単に説明します。Cisco SD-Access システムヘルスツールは、Cisco SD-Access アプリケーションの正常性を監視するために使用されます。さらに、Cisco SD-Access 互換性マトリックスのチェックを使用して、サポートされていないデバイスやサポートされていないソフトウェアバージョンを実行しているデバイスの追加を防止します。

## Cisco SD-Access ネットワークの定義

このセクションでは、Cisco SD-Access アーキテクチャの概要と、Catalyst Center を介して有線およびワイヤレスのキャンパスネットワークを展開するための設計上の考慮事項について説明します。

# Cisco SD-Access ソリューション

### Cisco SD-Access とは

Cisco SD-Access は、従来のキャンパス設計の進化形であり、組織の目的（インテント）をそのまま反映できます。Cisco SD-Access は、有線およびワイヤレスのキャンパスネットワークを自動化する Catalyst Center で実行されるソフトウェアです。

Cisco SD-Access の不可欠な部分であるファブリックテクノロジーにより、有線およびワイヤレスのキャンパスネットワークと、プログラム可能なオーバーレイおよび簡単に導入可能な仮想ネットワーク（VN）を提供し、設計の意図を満たすように 1 つ以上の論理ネットワークをホストする物理ネットワークを可能にします。VN に加えて、キャンパスネットワークにおけるファブリックテクノロジーでは、通信の制御が強化され、ユーザーアイデンティティとグループメンバーシップに基づいたソフトウェア定義型セグメンテーションおよびポリシー適用が可能です。Catalyst Center を使用して、統合されたセキュリティとセグメンテーションを備えた VN の作成を自動化することで、運用コストを削減し、リスクを軽減します。ネットワークパフォーマンス、ネットワークインサイト、およびテレメトリは、Catalyst アシュアランスおよび分析機能を通じて提供されます。

### Cisco SD-Access が選ばれる理由

Cisco SD-Access は、次の主な理由により、従来のネットワーク展開よりも優れています。

- オーケストレーションと自動化によって実現された複雑さの軽減と運用の一貫性
- グループベースのポリシーを組み込んだ多層セグメンテーション
- 有線およびワイヤレスクライアントに提供されるダイナミック ポリシー モビリティ

Cisco SD-Access は、可視性、自動化、セキュリティ、簡素化を含む、インテントベースのネットワーキング基盤上に構築されています。Catalyst Center の自動化とオーケストレーションを使用すると、ネットワーク管理者は直感的なグラフィカル ユーザー インターフェイス（GUI）を介して企業環境全体での変更が可能です。

Cisco SD-Access は、仮想ルーティングおよび転送（VRF）テーブルとセキュリティグループタグ（SGT）を使用して、マクロセグメンテーション レベルとマイクロセグメンテーション レベルでネットワークを保護します。この多層セグメンテーションは、従来のネットワークでは最適ではありません。

多層セグメンテーションを組み込んだ、ユーザーまたはデバイスに関連付けられたセキュリティコンテキストはすべて、ネットワーク接続を認証している間に動的に割り当てられます。Cisco SD-Access は、有線とワイヤレスの接続に同じセキュリティポリシー機能を提供し、ユーザーまたはデバイスが接続タイプを変更しても安全なポリシーの一貫性を維持します。

Cisco SD-Access では、従来のネットワークのような IP ベースのセキュリティルールではなく、IP アドレスに依存しない SGT を使用した、グループベースの一元化されたセキュリティルールを使用します。ユーザーまたはデバ

イスがロケーション間を移動して IP アドレスを変更しても、グループメンバーシップはロケーションに依存しないネットワークアクセスであるため、セキュリティポリシーは同じままです。ネットワーク管理者は、多くのルールを作成したり、さまざまなデバイスで手動で更新したりする必要がないため、ネットワークのコンシューマにとってより動的で安定した環境が実現します。

## Cisco SD-Access ソリューション コンポーネント

Cisco SD-Access ソリューションでは、次の基本的な支柱を使用します。

- Catalyst Center
- Cisco Identity Services Engine（Cisco ISE）
- ファブリック接続をサポートする有線とワイヤレスのデバイスプラットフォーム

### Catalyst Center

Catalyst Center は、Cisco Digital Network Architecture（Cisco DNA）を強化するアプリケーションとサービスのコレクションを実行する集中型マネージャです。Catalyst Center は、ルータ、スイッチ、AP、ワイヤレス LAN コントローラを含むデジタル対応インフラストラクチャの基盤として構築されます。Catalyst Center ネットワークの自動化、分析、可視性、および管理は、Catalyst Center ソフトウェアを通じて実現されます。Cisco SD-Access はこのソフトウェアの一部であり、ポリシーの設計、プロビジョニング、および適用に使用され、インテリジェントな有線とワイヤレスのキャンパスネットワークの作成を支援します。

### Cisco ISE

Cisco ISE は、ネットワークにアクセスするユーザーとデバイスに対する管理上の可視性、制御、および一貫性を向上させる、セキュアなネットワーク アクセス プラットフォームです。Cisco ISE は、ネットワーク アクセス コントロール ポリシーを実装するための Cisco SD-Access の不可欠なコンポーネントです。Cisco ISE はポリシー導入を実行し、拡張可能なグループにユーザーとデバイスを動的にマッピングします。また、エンドツーエンドのセキュリティポリシーの適用も簡素化されます。Cisco ISE では、ユーザーとデバイスはシンプルで柔軟なインターフェイスに表示されます。Cisco ISE は、Cisco ISE でのエンドポイントイベント通知と、ポリシー設定の自動化のために、Cisco Platform Exchange Grid（pxGrid）と Representational State Transfer Application Programming Interfaces（REST API）を使用して Catalyst Center と統合されます。

Cisco SD-Access ソリューションは、エンドツーエンドのグループベースのポリシーをサポートすることにより、Cisco TrustSec マイクロセグメンテーションを SGT と統合します。SGT は、ファブリックカプセル化パケットのヘッダーで送信されるメタデータ値です。SGT は統合された REST API を介して Cisco ISE によって管理されますが、Catalyst Center はダッシュボードとして使用して、SGT を管理および作成し、ポリシーを定義します。グループおよびポリシーサービスは、Cisco ISE によって管理され、Catalyst Center のポリシー作成ワークフローによって調整されます。Cisco SD-Access ネットワークでは、Cisco ISE を Catalyst Center と統合することでポリシー管理が合理化され、ユーザーとデバイスをセキュリティグループに動的にマッピングできます。これにより、IP アクセスリストに依存した従来のネットワークポリシー導入に比べてより拡張性の高いソリューションを提供して、エンドツーエンドのセキュリティポリシー管理とセキュリティポリシー適用が容易になります。

**技術的なヒント：** Cisco SD-Access ソリューションがマクロセグメンテーションを使用している場合、Cisco ISE

は必須ではありません。

### ネットワーク インフラストラクチャ

Cisco SD-Access ソリューション インフラストラクチャには、ルータ、スイッチ、AP、およびワイヤレス LAN コントローラが含まれます。これらのデバイスでは、Catalyst Center はユーザーインターフェイス（UI）での選択に基づいて、さまざまなファブリックロールを展開します。

### Cisco SD-Access アーキテクチャの概要

Cisco SD-Access アーキテクチャは、ファブリックテクノロジーを使用してキャンパスネットワークをサポートします。これには、オーバーレイネットワークと呼ばれる VN の作成が含まれます。このネットワークは、アンダーレイネットワークと呼ばれる物理ネットワーク上で動作します。この設定により、デバイスを接続する代替トポロジを作成でき、ネットワークの柔軟性と機能性が向上します。このセクションでは、Cisco SD-Access の運用プレーンについて説明します。ファブリックアンダーレイとオーバーレイネットワークは、オーバーレイ内のデバイスにより、アクセスされる共有リソースセットである共有サービスを導入します。

### Cisco SD-Access の運用プレーン

Cisco SD-Access ソリューションを構成するこれらの主要テクノロジーは、それぞれが運用のさまざまなネットワークプレーンで異なるタスクを実行します。

- コントロールプレーン：

  Locator ID Separation Protocol（LISP）は、ファブリック内のインフラストラクチャ デバイス間のメッセージングおよび通信プロトコルとして使用されます。

- データプレーン：

  Virtual Extensible LAN（VXLAN）は、データパケットのカプセル化方式として使用されます。

- ポリシープレーン：

  Cisco TrustSec は、セキュリティとマイクロセグメンテーションに使用されます。

- 管理プレーン：

  Catalyst Center は、オーケストレーション、アシュアランス、可視性、および管理に使用されます。

#### コントロールプレーン（LISP）

多くのネットワークでは、エンドポイントに関連付けられた IP アドレスが、ネットワーク内のそのアイデンティティとその位置の両方を定義します。IP アドレスは、ネットワーク層の ID（だれのデバイスがネットワーク上にあるか）と、ネットワーク層ロケータ（どこのデバイスがネットワーク内にあるか、またはどのデバイスが接続されているか）の両方に使用されます。

LISP は、IP アドレッシングの新たなセマンティクスを提供するルーティングアーキテクチャです。ルーティングロケータ（RLOC）名前空間との関係で、エンドポイント識別子（EID）名前空間のマッピング関係を介してアイデンティティと場所を分離できます。

LISP コントロールプレーンのメッセージングプロトコルは、2 つの名前空間の間の通信と交換を行います。この関係は、EID-to-RLOC マッピングと呼ばれます。EID と RLOC を組み合わせることで、トラフィックの転送に必要なすべての情報が得られ、エンドポイントが（異なる RLOC の背後で関連付けられているまたはマッピングされている）ネットワークの別の場所で同じ IP アドレスを使用している場合でも対応できます。

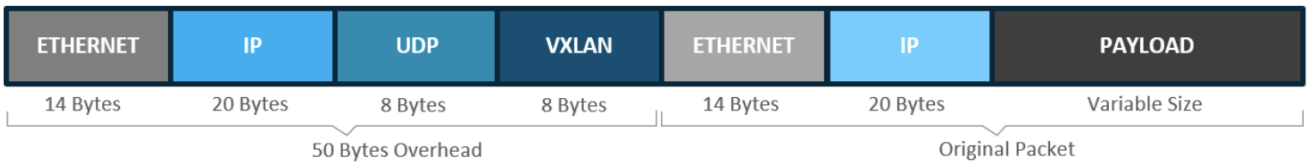
ファブリックデバイスは、コントロールプレーンノードにクエリを実行して、宛先アドレスに関連付けられたルーティングロケータを特定し（EID-to-RLOC マッピング）、その RLOC 情報をトラフィックの宛先として使用します。

**データプレーン（VXLAN）**

VXLAN は、データトラフィックの MAC-in-IP カプセル化方式です。エンドポイントから送信された元のフレームからの元のイーサネットヘッダーを保持します。これにより、元の通信の要件に応じて、レイヤ 2 とレイヤ 3 でオーバーレイを作成できます。たとえば、無線 LAN 通信では、レイヤ 2 のデータグラム情報（MAC アドレス）を使用してブリッジングの決定を行います。レイヤ 3 のフォワーディングロジックは直接必要ありません。

Cisco SD-Access では、VXLAN ネットワーク識別子（VNI）を使用して各オーバーレイネットワークを識別することで、ポリシーを決定するために使用できる代替の転送属性などの追加情報がファブリック VXLAN ヘッダーに配置されます。レイヤ 2 オーバーレイは VLAN から VNI への関連付け（レイヤ 2 VNI）で識別され、レイヤ 3 オーバーレイは VRF から VNI への関連付け（レイヤ 3 VNI）で識別されます。

VXLAN カプセル化は、ユーザー データグラム プロトコル（UDP）トランスポートを使用します。元のパケットをカプセル化するために使用される VXLAN および UDP ヘッダーとともに、ワイヤを介してパケットを転送するために外部 IP およびイーサネットヘッダーが必要です。図に示されているように、これらの追加ヘッダーにより、元のパケットに最低 50 バイトのオーバーヘッドが追加されます。




**Cisco TrustSec に基づいたポリシープレーン**

Cisco TrustSec は、ネットワーク内のユーザー、ホスト、およびネットワークデバイスを強力に識別する機能に基づいた、シスコネットワークデバイスのセキュリティを改善します。論理グループ権限を示すために SGT を使用します。SGT は、アクセスポリシーで使用されます。SGT は、シスコのスイッチ、ルータ、およびファイアウォールで認識され、トラフィックを適用するために使用されます。

Cisco TrustSec は、分類、伝達、および適用といったフェーズで構成されます。ユーザーとデバイスがネットワークに接続すると、ネットワークは、分類と呼ばれる特定のセキュリティグループを割り当てます。分類は、認証の結果に基づいて行うことも、SGT を IP、VLAN、またはポートプロファイルに関連付けることによって行うこともできます。ユーザートラフィックが分類されると、SGT は分類のポイントから適用アクションが適用される場所に送信されます。このプロセスは伝播と呼ばれます。

Cisco TrustSec で使用される SGT の伝播方法は次のとおりです。

- インラインタギング：

SGT は、イーサネットフレームに組み込まれます。イーサネットフレーム内に SGT を埋め込む機能には、特定のハードウェアサポートが必要です。

- SGT 交換プロトコル（SXP）：

  ハードウェアのサポートがないネットワークデバイスは、SXP を使用します。SXP は、IP アドレスマッピングと SGT をペアリングします。このペアリングにより、SGT 伝播がパス内の次のデバイスに対して続行されます。適用デバイスは、タグ情報に基づいてトラフィックを制御します。

シスコのファイアウォール、ルータ、またはスイッチを Cisco TrustSec の適用ポイントとすることができます。適用デバイスは送信元 SGT を取得し、それを宛先 SGT と比較して、トラフィックを許可するか拒否するかを決定します。

Cisco TrustSec の主要コンポーネントは、Cisco ISE です。Cisco ISE は、Cisco TrustSec のアイデンティティとセキュリティ グループ アクセス コントロール リスト（SGACL）を使用してスイッチをプロビジョニングします。

**Catalyst Center を用いた管理プレーン**

Catalyst Center は、ネットワークへのデバイス導入および設定の自動化を可能にして、運用の効率化に必要な速度と整合性を実現します。

自動化機能により、ファブリックデバイスのコントロールプレーン、データプレーン、およびポリシープレーンを、簡単かつシームレスに一貫して展開できます。インフラストラクチャ デバイスとエンドポイントの両方で、十分なアシュアランス、可視性、およびコンテキストが実現されます。

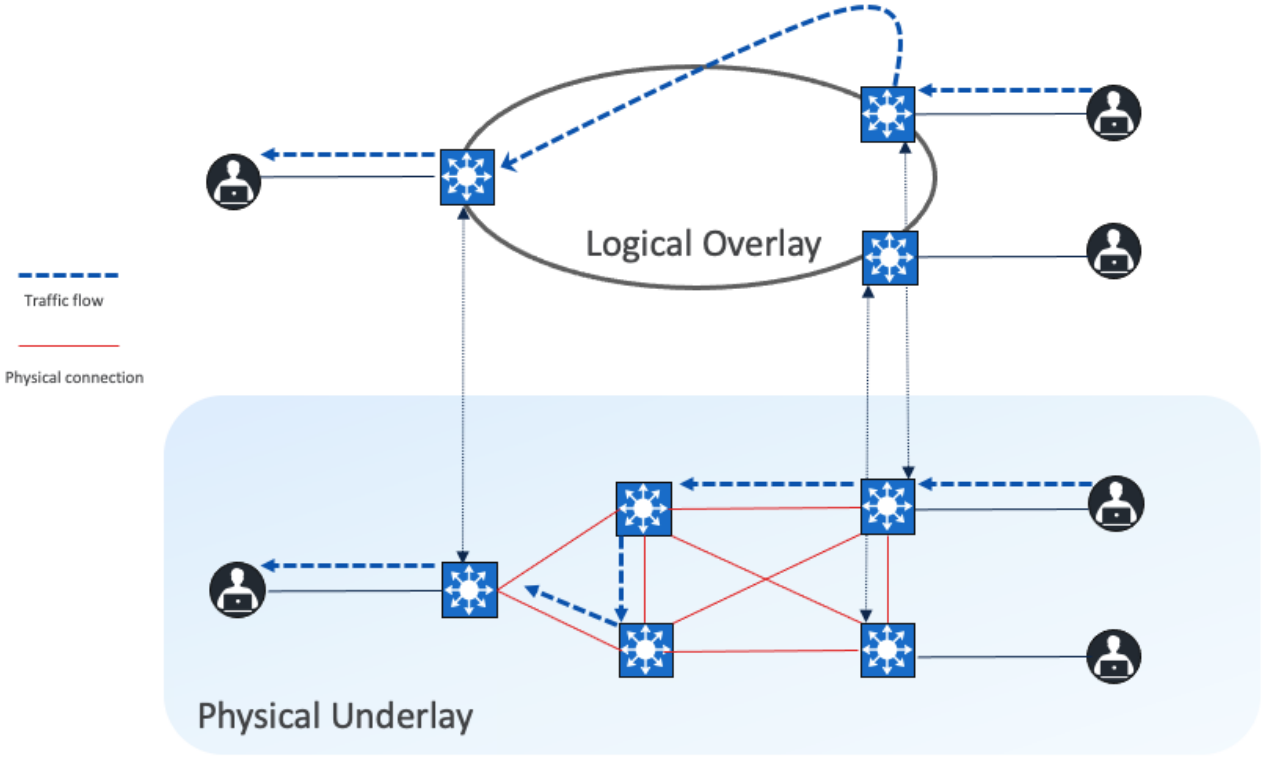
LISP と VXLAN を完全に理解して Cisco SD-Access のファブリックを展開する必要はありません。また、Cisco SD-Access によってエンドツーエンドで一貫性のある動作を実現するために、個々のネットワークコンポーネントおよび機能の設定方法を詳細に知る必要もありません。Catalyst Center は、有線とワイヤレスの Cisco SD-Access ネットワーク全体の設計、プロビジョニング、およびポリシー適用に使用される、一元化された直感的な管理システムです。ユーザーの意図を取得し、プログラムによってネットワークデバイスに適用されます。

## ファブリックアンダーレイ

アンダーレイネットワークは、Cisco SD-Access ネットワークの導入に使用される物理スイッチおよびルータによって定義されます。アンダーレイのすべてのネットワーク要素では、ルーティングプロトコルを使用して IP 接続を確立する必要があります。Cisco SD-Access のアンダーレイ実装では、ランダムなネットワークトポロジおよびプロトコルではなく、レイヤ 3 ルーテッドアクセス設計と呼ばれるキャンパスエッジスイッチを含む、構造化されたレイヤ 3 基盤を使用します。これにより、ネットワークのパフォーマンス、スケーラビリティ、復元力、および確定的なコンバージェンスが保証されます。

Cisco SD-Access では、アンダーレイスイッチ（エッジノード）でユーザーとエンドポイントの物理接続をサポートします。ただし、エンドユーザーのサブネットとエンドポイントは、アンダーレイネットワークの一部ではありません。これらは、自動化されたオーバーレイネットワークの一部です。

**図 2.　　オーバーレイとアンダーレイの関係**

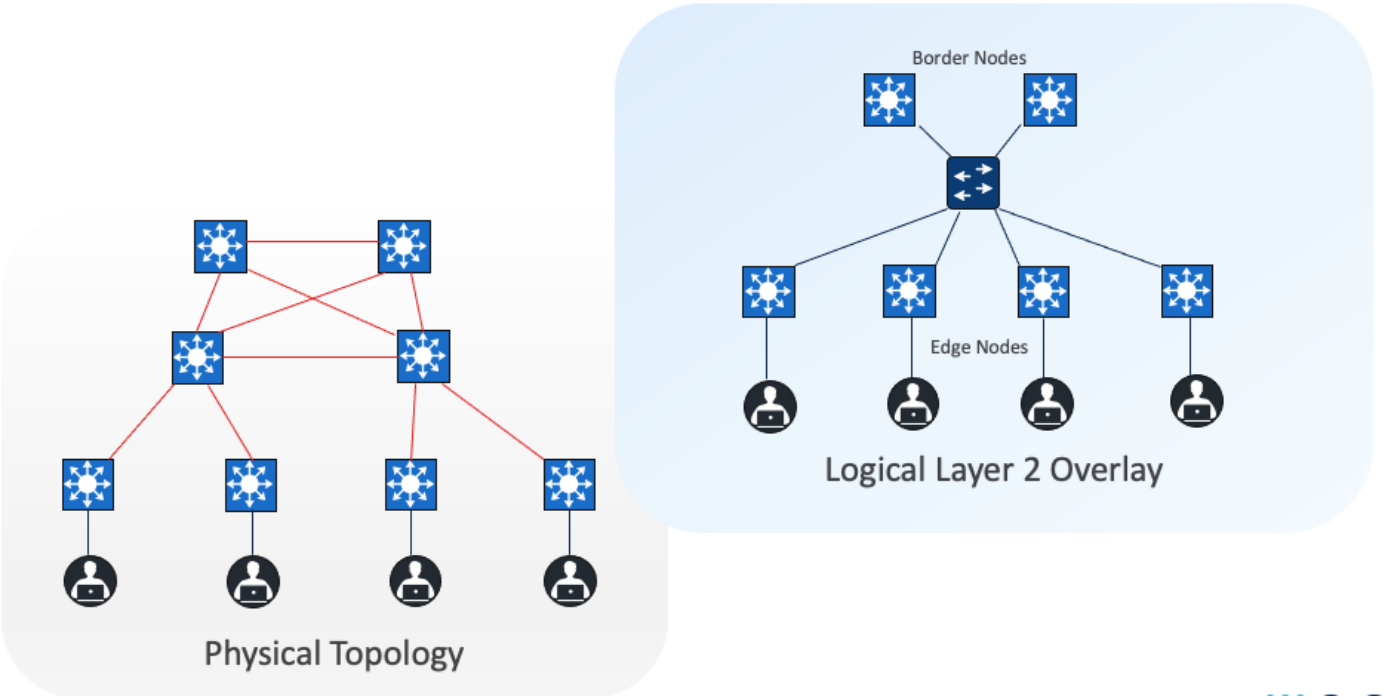



## ファブリックオーバーレイ

オーバーレイネットワークは、仮想化（VN）からアンダーレイネットワークの上位に作成されます。各 VN では、データプレーンによるトラフィック転送とコントロールプレーンによるシグナリングが行われ、ネットワークの分離と、アンダーレイネットワークからの独立性が維持されます。複数のオーバーレイネットワークを VN を介して同じアンダーレイネットワークで実行できます。Cisco SD-Access では、ユーザー定義のオーバーレイネットワークは、ルーティングテーブルの分離を提供する VRF インスタンスとしてプロビジョニングされます。

Cisco SD-Access では、LISP を介して提供されるサービスを通じてオーバーレイ全体でレイヤ 2 とレイヤ 3 の接続を拡張できます。レイヤ 2 オーバーレイサービスは、図に示すように、レイヤ 3 アンダーレイ上でサブネットを伝送することによって、LAN セグメントをエミュレートしてレイヤ 2 フレームを転送します。

**図 3.　　論理的に接続がスイッチされるレイヤ 2 オーバーレイ**




レイヤ 3 オーバーレイは、図に示すように、物理接続から IP ベースの接続を抽象化します。これにより、複数の IP ネットワークを各 VN の一部にすることができます。各レイヤ 3 オーバーレイ、そのルーティングテーブル、および関連するコントロールプレーンは、相互から完全に分離されます。

**図 4.　　論理的に接続がルーティングされるレイヤ 3 オーバーレイ**

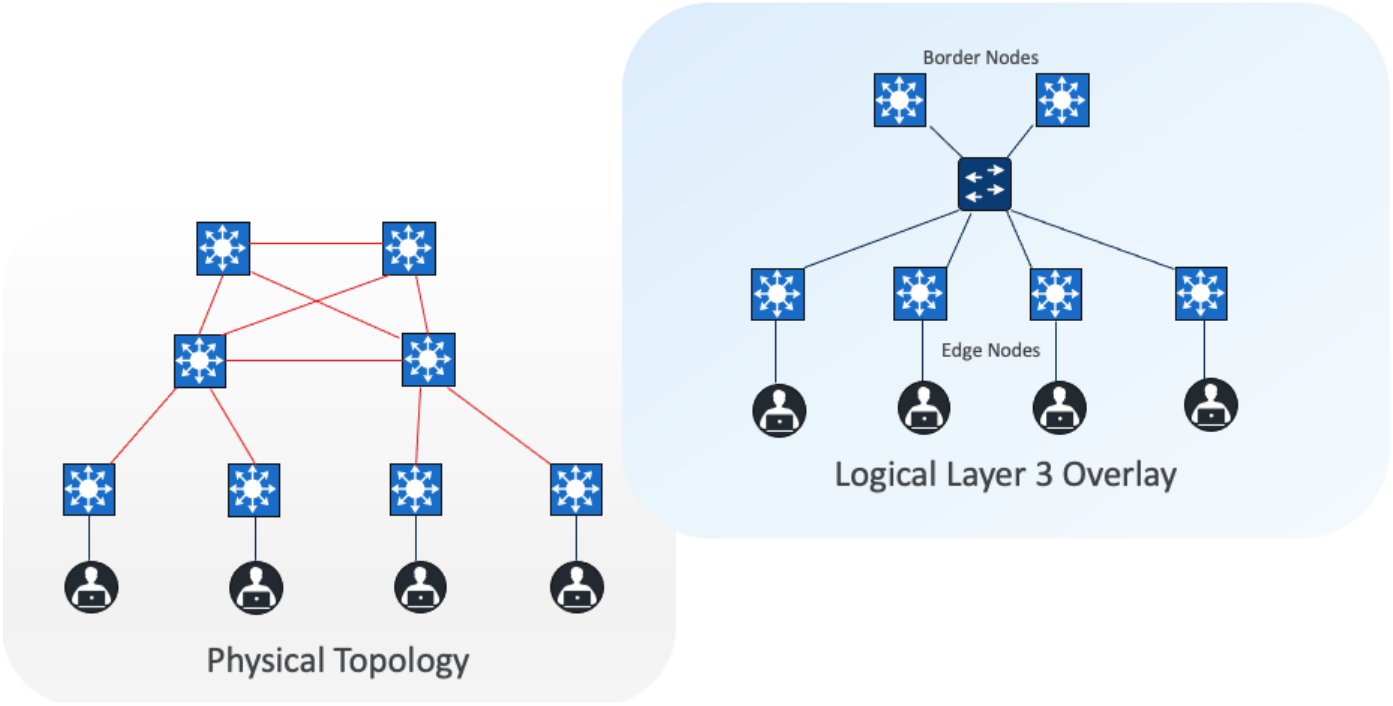
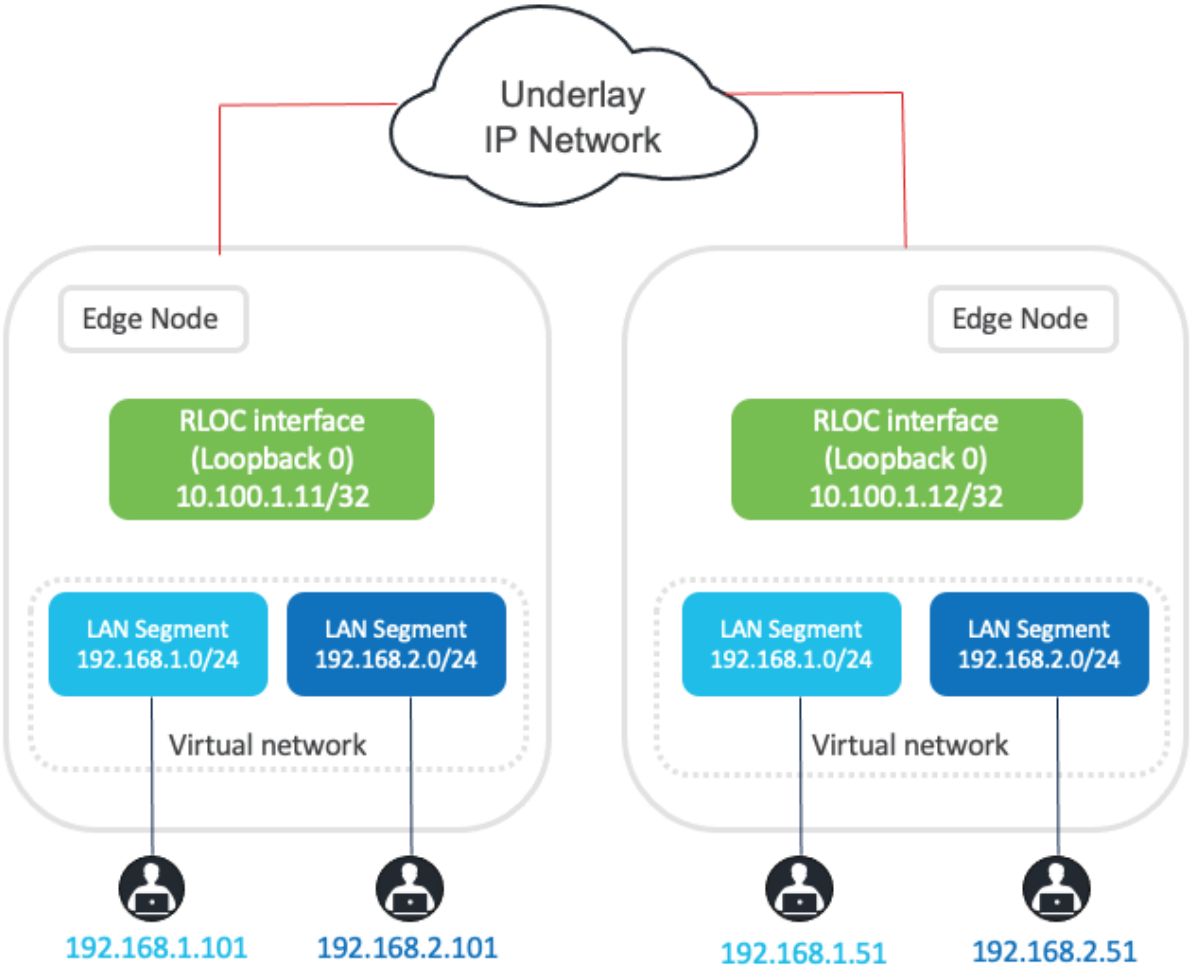



図 5 に、オーバーレイネットワークに含まれる 2 つのサブネットの例を示します。サブネットは、物理的に分離されたレイヤ 3 エッジノードデバイスに拡張できます。RLOC インターフェイスまたは Cisco SD-Access の Loopback0 インターフェイスは、同じ VN 内のエンドポイント間の接続を確立するために必要な唯一のアンダーレイルーティング可能アドレスです。

**図 5.　　サブネットストレッチの例**




**共有サービス**

すべてのネットワーク展開で、すべてのエンドポイントに必要な共通のリソースセットがあります。一般的な例は次のとおりです。

- アイデンティティサービス（例：AAA/RADIUS）
- ドメインネームサービス（DNS）
- Dynamic Host Configuration Protocol（DHCP）
- IP アドレス管理（IPAM）
- モニタリングツール（例：SNMP）
- データコレクタ（例：NetFlow、syslog）
- インターネットアクセス
- その他のインフラストラクチャ要素

これらの共通リソースは、多くの場合、共有サービスと呼ばれます。これらの共有サービスは、通常、Cisco SD-Access ファブリックの外部に存在します。ほとんどの場合、そのようなサービスはデータセンターに存在し、グローバル ルーティング テーブル（GRT）または別の専用 VRF の一部です。

Cisco SD-Access ファブリッククライアントは、オーバーレイ仮想ネットワークで動作します。共有サービスがグローバルルーティング空間の一部または別の VRF の一部である場合、ユーザー VRF と共有サービス間で VRF ルートリークの何らかの方法が必要です。これは、ピアデバイスまたはファイアウォールを使用して実現されます。

## Cisco SD-Access ネットワークの概要

### ファブリックサイト

ファブリックサイトは、ファブリックロールで動作しているデバイスの固有のセットと、それらのデバイスを接続するために使用される中間ノードで構成されます。ファブリックサイトには、必ずボーダーノードとコントロールプレーンノードがあり、多くの場合、ファブリックエッジノードがあります。ファブリックサイトには、関連付けられたファブリックワイヤレス LAN コントローラ（WLC）と Cisco ISE ポリシーサービスノード（PSN）を含めることもできます。

### ファブリックゾーン

ファブリックゾーンは、親ファブリックサイトの子セットです。ファブリックゾーンがない場合、すべての IP プールがすべてのファブリックエッジノードで設定され、すべてのファブリックエッジノードのすべてのサブネットにつながります。ゾーンにより、特定のファブリックエッジノードに特定のサブネットを持つことができる柔軟性が得られます。この設定により、より小さな場所に基づく単一のファブリックサイトでのファブリックエッジノードの大規模な展開を管理する方法が提供されます。たとえば、ファブリックサイトに 10 の建物を含めることができます。すべての建物にわたって、すべての IP プールを使用する必要がない場合があります。建物でファブリックゾーンを有効にすると、一部の IP プールが一部の建物でのみ使用できるようになります。

### トランジット

トランジットは、複数のファブリックサイトを接続したり、ファブリックサイトをデータセンターやインターネットなどの非ファブリックドメインに接続したりできます。トランジットは、ファブリックサイト間またはファブリックサイトと外部ドメイン間の接続のボーダーノード設定を Catalyst Center が自動化する方法を定義する Cisco SD-Access コンストラクトです。トランジットタイプは次のとおりです。

#### IP ベースのトランジット

IP ベースのトランジットを使用すると、パケットがファブリックサイトに出入りするときに、ファブリックボーダーノードによってファブリック VXLAN ヘッダーが追加または削除されます。VXLAN ヘッダーが削除されると、ファブリックサイト間の従来のルーティングおよびスイッチングプロトコルを使用してパケットが転送されます。IP ベースのトランジットは、データセンター、WAN、またはインターネットに通常接続されている、アップストリームのピアデバイスへの VRF-LITE 接続でプロビジョニングされます。IP トランジットは、VRF 認識ピアを使用した共有サービスへの接続にも使用できます。

#### Cisco SD-Access トランジット

Cisco SD-Access トランジットを使用した場合、パケットは、サイト間で VXLAN を使用してカプセル化されます。これは、ファブリックサイト間で VRF と SGT のポリシー構造をネイティブに伝送します。Cisco SD-Access トランジットを使用する際の主な考慮事項は次のとおりです。

- 接続は、ファブリックサイトのボーダー間のパス全体で推奨最大伝送ユニット（MTU）サイズ（9100 バイト）をサポートする必要があります。
- IP 到達可能性は、ファブリックサイト間に存在する必要があります。具体的には、すべてのファブリックサイトボーダーとトランジット コントロール プレーン ノードの間に既知のアンダーレイルートが必要です。デフォルトルートは、この目的には使用できません。

Cisco SD-Access トランジットは、異なるファブリックサイト間でのポリシー適用の拡張を必要とするお客様に推奨されます。

### VN

Cisco SD-Access は、VN を使用してオーバーレイ全体にレイヤ 3 およびレイヤ 2 接続を提供します。

レイヤ 3 オーバーレイは、独立したルーティングテーブルをエミュレートし、レイヤ 3 ネットワーク経由でレイヤ 3 フレームを転送します。このタイプのオーバーレイは、レイヤ 3 仮想ネットワーク（L3VN）と呼ばれます。L3VN は、従来のネットワークの仮想ルーティングおよび転送（VRF）テーブルに似ています。エンドポイント ID（IPV4/IPV6 アドレス）は L3VN 内でルーティングされます。

レイヤ 2 オーバーレイは、LAN セグメントをエミュレートして、レイヤ 2 ネットワーク経由でレイヤ 2 フレームをトランスポートします。このタイプのオーバーレイは、レイヤ 2 仮想ネットワーク（L2VN）と呼ばれます。L2VN は、従来のネットワークの VLAN に似ています。エンドポイント ID（MAC アドレス）は L2VN 内でスイッチングされます。

### エニーキャストゲートウェイ

エニーキャストゲートウェイは、Cisco SD-Access ネットワーク内の IP 対応エンドポイントにデフォルトゲートウェイを提供します。エニーキャストゲートウェイは、ファブリックサイト内のすべてのエッジノードで統一された、ハードコーディングされた MAC アドレスを持つスイッチ仮想インターフェイス（SVI）として示されます。これにより、サブネットを Cisco SD-Access ネットワーク全体に拡張できます。サブネットが拡張されているため、ホストはファブリックサイト内の任意の場所を移動しても、同じゲートウェイ IP アドレスおよび MAC アドレスを維持できます。

### SGT

SGT は、ネットワーク全体で送信元の権限を示すメタデータ値です。SGT を伝播するには、いくつかの方法があります。Cisco SD-Access ファブリック内では、SGT は VXLAN カプセル化パケットのヘッダーで伝播されます。Cisco SD-Access ファブリックの外部では、インラインタギング、SXP、スタティックバインディングなどを使用して SGT を維持できます。

Cisco ISE を通じて提供されるアイデンティティサービスにより、ファブリックに接続されているユーザーとデバイスを SGT に動的にマッピングできます。このアプローチにより、ネットワーク全体のセキュリティポリシーの管理と適用が簡素化され、IP アクセスリストに依存する従来のネットワークポリシーの実装と比較して、よりスケーラブルなソリューションが提供されます。

SGT の詳細：

- エンドポイントが SGT マッピングを認識しない
- SGT の範囲は 1 ～ 65533。SGT 0 は「不明」として使用される
- Catalyst Center と Cisco ISE の設定可能な SGT 値は 2 ～ 65519

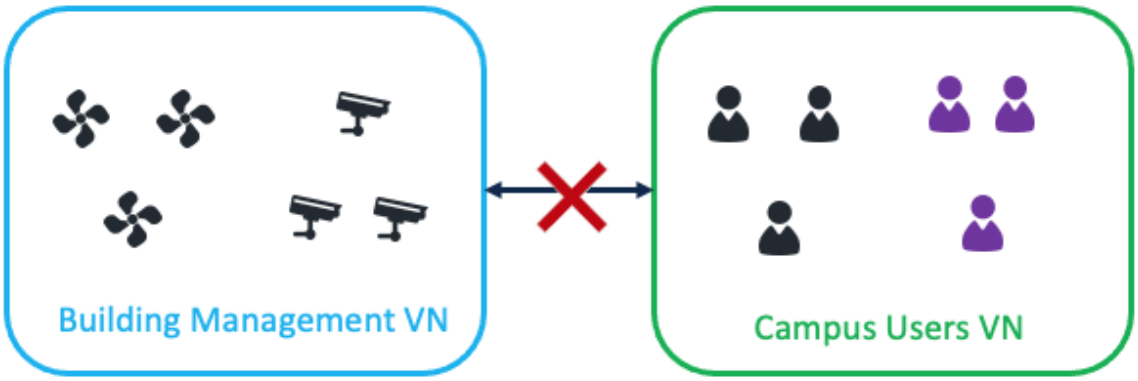
### セグメンテーション

Cisco SD-Access は、マクロセグメンテーションとマイクロセグメンテーションを作成します。

#### マクロセグメンテーション

第 1 レベルのセグメンテーションとしてのマクロセグメンテーションは VN を使用します。ユーザーとデバイスを別々の VN に配置して、それらの間で分離を行うことができます。異なる VN のエンドポイントは、相互に通信できません。

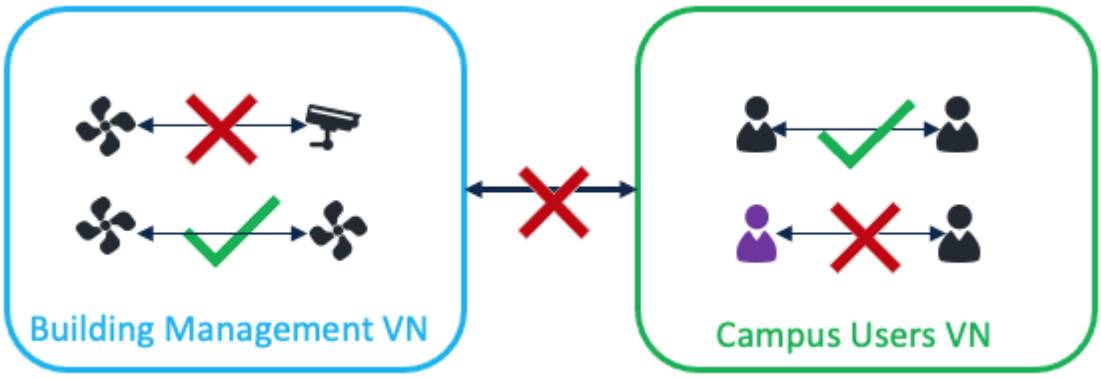
**図 6.　　例：「建物管理 VN」のエンドポイントは、「キャンパスユーザー VN」のエンドポイントと通信できない**




#### マイクロセグメンテーション

第 2 レベルのセグメンテーションとしてのマイクロセグメンテーションは、SGT を使用して実現されます。SGT は、VN 内のセグメント化に使用されます。SGT は、**デフォルトポリシー**の設定に応じて、特定の VN 内の通信を許可または拒否します。**デフォルトポリシー**の設定が許可の場合、同じ VN 内のユーザーとデバイスは相互に通信できます。SGT を使用すると、VN 内の通信を拒否できます。**デフォルトポリシー**の設定が拒否の場合、同じ VN 内のユーザーとデバイスは相互に通信できません。SGT を使用すると、VN 内の通信を許可できます。

**図 7.　　例：「建物管理 VN」と「キャンパスユーザー VN」のエンドポイントに異なる SGT が割り当てられている場合、トラフィックは SGT ポリシーに基づいて許可または拒否される**

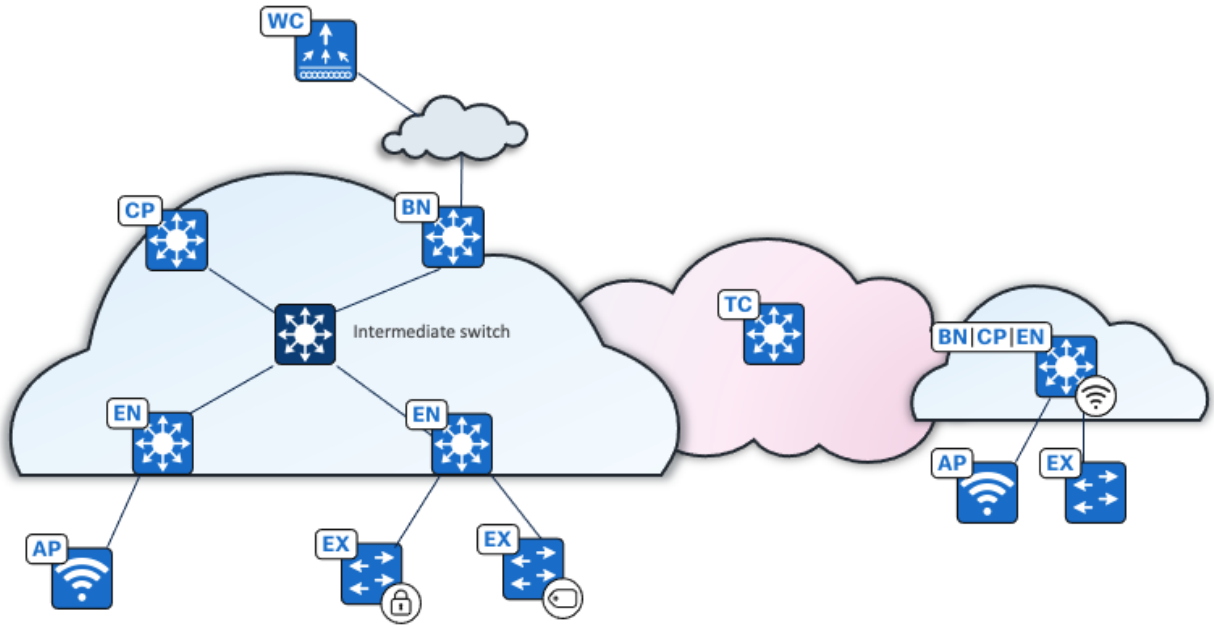


マイクロセグメンテーションでは、分類、伝達、および適用という主な概念によって定義された Cisco TrustSec ソリューションを使用しています。Catalyst Center は、セキュリティグループ、コントラクト、ポリシーなどのセキュリティポリシーを自動化し、Cisco ISE と同期します。分類、セキュリティグループの割り当て、およびポリシーダウンロードの処理は Cisco ISE の責任です。詳細については、「エンドツーエンド マイクロセグメンテーション」を参照してください。

### Cisco SD-Access ファブリックロール

ファブリックサイトが機能するには、少なくともファブリック コントロール プレーンとファブリックエッジが必要です。外部に接続する場合は、ファブリックボーダーも必要です。ネットワーク管理者は、ファブリックワイヤレス展開用のファブリック ワイヤレス コントローラとファブリック AP、ファブリックエッジへのレイヤ 2 アクセスを拡張するための拡張ノードなど、他のファブリックデバイスを追加できます。一部のファブリックロールは、単一のデバイスにコロケーションできます。

**図 8.　　ファブリックロール**




- コントロールプレーンノード 


  エッジ、ボーダーノード、ローカルエンドポイントを持つファブリック ワイヤレス コントローラからの登録を受信するマップサーバーです。また、コントロールプレーンノードは、エッジとボーダーからの要求を解決して宛先エンドポイントを見つけるマップリゾルバ（MR）でもあります。

- ボーダーノード 


  Cisco SD-Access ファブリックサイトと、ファブリック外部のネットワークとの間のゲートウェイです。ボーダーノードは、ファブリックサイトに出入りするためのゲートウェイとして機能し、ネットワーク仮想化

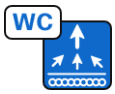
と、ネットワークの他の部分への SGT 伝播を処理します。レイヤ 3 ボーダーノードは、内部ボーダー、外部ボーダー、および内外ボーダーのタイプにすることができます。

- エッジノード 


  エンドポイントを Cisco SD-Access ファブリックに接続し、オプションでマイクロセグメンテーション ポリシーを適用するファブリックデバイスです。これらのデバイスは入力時にカプセル化を、出力時にはカプセル化解除を実行し、ファブリックネットワークに接続されたエンドポイント間でトラフィックを転送します。接続された有線およびワイヤレスエンドポイントにエニーキャストゲートウェイを提供し、認証と承認を担当します。

- アクセスポイント 

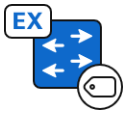

  ファブリック対応 SSID で設定されたファブリックワイヤレス LAN コントローラに関連付けられたファブリックモードです。ワイヤレスエンドポイントを Cisco SD-Access ファブリックに接続します。

- ワイヤレスコントローラ 


  ファブリック AP を Cisco SD-Access ファブリックに接続するコントローラです。ファブリック ワイヤレス コントローラは、ワイヤレスクライアントの MAC アドレスをファブリック コントロール プレーン ノードに登録します。

- 拡張ノード 


  ファブリックエッジノードへのレイヤ 2 ポート拡張です。必要に応じて、接続されたエンドポイントにマイクロセグメンテーション ポリシーを適用します。ファブリック AP を含むエンドポイントは、拡張ノードに直接接続できます。Catalyst Center でサポートされる拡張ノードタイプは次のとおりです。

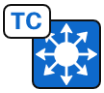
  - 拡張ノード：マイクロセグメンテーションはサポートされていません。
  - ポリシー拡張ノード 

：マイクロセグメンテーション アップリンクのサポートは、ポートチャネルとして設定されます。
  - サプリカントベースの拡張ノード 

：マイクロセグメンテーション アップリンク ポートのサポートは dot1x 認証です。

- 中間ノード  （アンダーレイ）

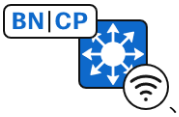
ファブリックデバイス間の相互接続に使用されるレイヤ 3 アンダーレイネットワークの一部です。これらは、デバイスの単一のレイヤに限定されません。中間ノードは、ファブリックロールではありません。

- トランジット コントロール プレーン ノード 


  Cisco SD-Access トランジットを使用する場合、トランジット コントロール プレーンは必須です。Cisco SD-Access トランジット全体へのサービス提供を除いて、サイトローカルのコントロールプレーンノードと同様に機能します。

  コントロールプレーンのコロケーションとのボーダー、コントロールプレーンとワイヤレスコントローラのコロケーションとのボーダー、コントローラプレーンとエッジのコロケーションとのボーダーなど、複数のファブリックロールを 1 つのデバイスにコロケーションできます。トランジット コントロール プレーン ノードは専用デバイスです。トランジット コントロール プレーンのコロケーションはサポートされていません。

- Catalyst 9000 デバイスの組み込みワイヤレスコントローラ（EWC）：

  ワイヤレスサブパッケージを使用する Catalyst 9000 デバイス（Catalyst 9000 の EWC）で有効です。これは、Catalyst 9000 デバイスが、コントロールプレーンのファブリックロール 

、エッジファブリックロール 

を持つボーダー、またはコントロールプレーンとエッジファブリックロールを持つボーダーを持つ、ファブリック内にある場合にサポートされます。

**注：** RLAN やアシュアランス モニタリング ツールなどの一部のワイヤレス機能は、Catalyst 9000 デバイスの EWC ではサポートされていません。ファブリックサイトでは、Catalyst 9000 デバイス上で最大 2 つの EWC を有効にできます。Catalyst 9000 デバイス上の EWC は、小規模なブランチでのみ推奨されます。Catalyst 9000 デバイス上の EWC は、ファブリック SSID のみをサポートします。

- ファブリックインアボックス（FiaB） 


  同じデバイス上でボーダーノード、コントロールプレーンノード、およびエッジノードのファブリックロールを組み合わせたものです。これは、単一のスイッチ、ハードウェアスタックを使用するスイッチ、または StackWise Virtual 展開にすることができます。同じスイッチを、ファブリック対応のワイヤレス設計の EWC として機能させることもできます。

### ファブリックロールのプラットフォームサポート

ASR 1000 シリーズ、ISR シリーズ、Catalyst 8000 シリーズ ルータなどの Cisco ルータプラットフォームは、主にボーダーおよびコントロール プレーン デバイスとしてサポートされます。Catalyst 9000 スイッチは、表 1 に示すように、ほとんどのファブリックロールをサポートします。

**表 1.** Cisco Catalyst 9000 シリーズ スイッチでサポートされているファブリックロール

| プラットフォームファミリ | エッジノード | コントロールプレーンノード | ボーダーノード | 拡張ノード | 組み込みワイヤレスコントローラ |
|---|---|---|---|---|---|
| Cisco Catalyst 9200 シリーズ | ✓ | — | — | ✓ | — |
| Cisco Catalyst 9300 シリーズ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cisco Catalyst 9400 シリーズ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cisco Catalyst 9500 シリーズ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cisco Catalyst 9600 シリーズ | — | ✓ | ✓ | — | — |

Cisco IE 3000 シリーズ、IE 4000 シリーズ、および IE 9000 シリーズ スイッチは、主に拡張ノードとして機能します。IE 9000 も、ファブリックエッジデバイスとしてサポートされています。

サポートされているプラットフォーム、サポートされているファブリックロール、推奨されるソフトウェアバージョンの詳細なリストについては、「Cisco SD-Access Compatibility Matrix」を参照してください。

## Cisco SD-Access の機能

### LISP パブリッシャ/サブスクライバ（LISP Pub/Sub）

前のセクションで説明したように、LISP プロトコルは、エンドポイント ID（EID）とそのルーティングロケータ（RLOC）を追跡するために Cisco SD-Access ソリューションのコントロールプレーンとして使用されます。ルート配布方法に基づいて、ボーダー ゲートウェイ プロトコル（BGP）と LISP Pub/Sub を使用した LISP がサポートされています。

LISP/BGP は、LISP と BGP の同時プロトコルを使用して到達可能性情報を配信します。LISP Pub/Sub は、ネイティブ LISP を介した情報のルーティングにパブリッシュおよびサブスクライブモデルを使用します。

LISP Pub/Sub は、デバイスイメージ 17.6 以降のバージョンを使用したすべての新しい展開に推奨されます。現在、LISP/BGP から LISP Pub/Sub への移行は Catalyst Center ではサポートされていませんが、移行予定です。

エリア LISP Pub/Sub には、LISP/BGP に比べて次のような追加の利点があります。

- ファブリック内の内部 BGP（iBGP）への依存関係を取り除き、すべてのファブリック関連の操作に LISP を使用します（制御ノードがボーダーノードとは異なる非コロケーションシナリオの場合、iBGP は、2 つの外部ネットワーク間のトランジットとして使用される Cisco SD-Access をサポートするように設定されます）。
- デフォルトルートを失うボーダーノードでアップリンク障害またはアップストリームデバイス障害が発生した場合に、Cisco SD-Access エンドポイントと外部エンドポイント間の通信のコンバージェンス時間を拡張します。
- 動的なデフォルトボーダー、バックアップインターネット、アフィニティ ID、エクストラネットなどの新しいファブリック機能を有効にします（導入ガイドでは取り上げていません）。また、他の機能において、Cisco SD-Access トランジットを介したネイティブマルチキャストもサポートします。

### ダイナミック デフォルト ボーダー

ダイナミック デフォルト ボーダーは、LISP Pub/Sub ではデフォルトで有効になっています。これにより、外部ボーダーでデフォルトルートの可用性を追跡できます。ダイナミック デフォルト ボーダーにより、ファブリック

オーバーレイは、デフォルトルートに影響を与えるボーダーノードでのアップリンクまたはアップストリームデバイスの障害に迅速に適応します。

### Cisco SD-Access バックアップインターネット

マルチサイトの Cisco SD-Access トランジット展開では、いくつかのファブリックサイトがインターネットにアクセスできる場合があります。Cisco SD-Access のバックアップインターネット機能を使用すると、ファブリックサイトは、ローカル インターネット アクセスが失われた場合、インターネットへのバックアップパスとして相互に利用できます。アフィニティ ID を使用して、インターネットへのバックアップパスを確立するために最も近いリモートボーダーを選択できます。

このガイドでは、展開セクションで LISP Pub/Sub に焦点を当てています。

## LAN の自動化

LAN 自動化は、Cisco SD-Access アンダーレイネットワークの準備、計画、自動化に役立ちます。ネットワーク運用がシンプルになり、IT スタッフが時間のかかる反復的なネットワーク設定作業から解放され、エラーのない標準のアンダーレイネットワークを作成できます。LAN 自動化により、従来のネットワーク計画と実装プロセスを必要とせずに、アンダーレイネットワークの構築が迅速化されます。

LAN 自動化では、ネットワークデバイスが動的に検出およびオンボーディングされ、工場出荷時の状態からネットワークに完全に統合されるまで自動化されます。システムロールは次のとおりです。

- シードデバイス：

  ネットワークに事前に導入されたシステムであり、LAN 自動化でダウンストリームの新しいスイッチを検出してオンボードする最初のポイントとなります。シードデバイスは、シスコのプラグアンドプレイ（PnP）などのテクノロジーで自動化することも、手動で設定することもできます。LAN 自動化では、最大 2 つのシードデバイスがサポートされます。

- PnP エージェント：

  工場出荷時の設定の Cisco Catalyst スイッチです。こうしたスイッチは、組み込みの Day-0 メカニズムを活用して Catalyst Center と通信し、統合された PnP サーバー機能と連携します。Catalyst Center は、PnP プロファイルと一連の設定を動的に構築して、完全な Day-0 自動化を可能にします。

Catalyst Center での LAN 自動化では、シードデバイスから最大 5 ホップのスイッチの検出と自動化をサポートします。5 ホップを超える追加のネットワークデバイスも検出されることはありますが、自動化することはできません。

## Cisco SD-Access マルチキャスト

Cisco SD-Access は、マルチキャストを転送するための 2 つの異なる転送方式をサポートします。オーバーレイを使用するヘッドエンド レプリケーション。アンダーレイを使用するネイティブマルチキャスト。各 VN に対して、マルチキャスト転送が有効になります。ただし、VN に対してネイティブマルチキャストが有効になっている場合、同じファブリックサイト内の別の VN にヘッドエンド レプリケーションを使用することはできません。これら 2 つの方法は、ファブリックサイト内では相互に排他的です。

マルチキャスト送信元は、ファブリックサイトの外部（通常データセンター内）、またはエッジノードや拡張ノードに直接接続されたファブリックオーバーレイ内、ファブリック AP に関連付けられたファブリックオーバーレイ内のいずれかに配置できます。マルチキャスト受信者は、通常、エッジノードまたは拡張ノードに直接接続されますが、送信元がオーバーレイ内にある場合はファブリックサイトの外部に配置することもできます。

**ランデブーポイント**

PIM Any-Source Multicast（PIM-ASM）と PIM Source-Specific Multicast（PIM-SSM）は、オーバーレイとアンダーレイの両方でサポートされています。PIM-ASM ルーティングアーキテクチャでは、マルチキャスト配信ツリーのルートはランデブーポイント（RP）に置かれます。RP は、複数のマルチキャストグループに対してアクティブにできます。また、複数の RP をそれぞれのグループに展開することもできます。PIM-ASM がオーバーレイで使用され、ファブリックボーダーが RP として設定されている場合、Catalyst Center は RP での Multicast Source Discovery Protocol（MSDP）設定を自動化し、特定のファブリックサイト内の他のファブリックノードが、指定された仮想ネットワークでこれらの RP を指すように設定します。

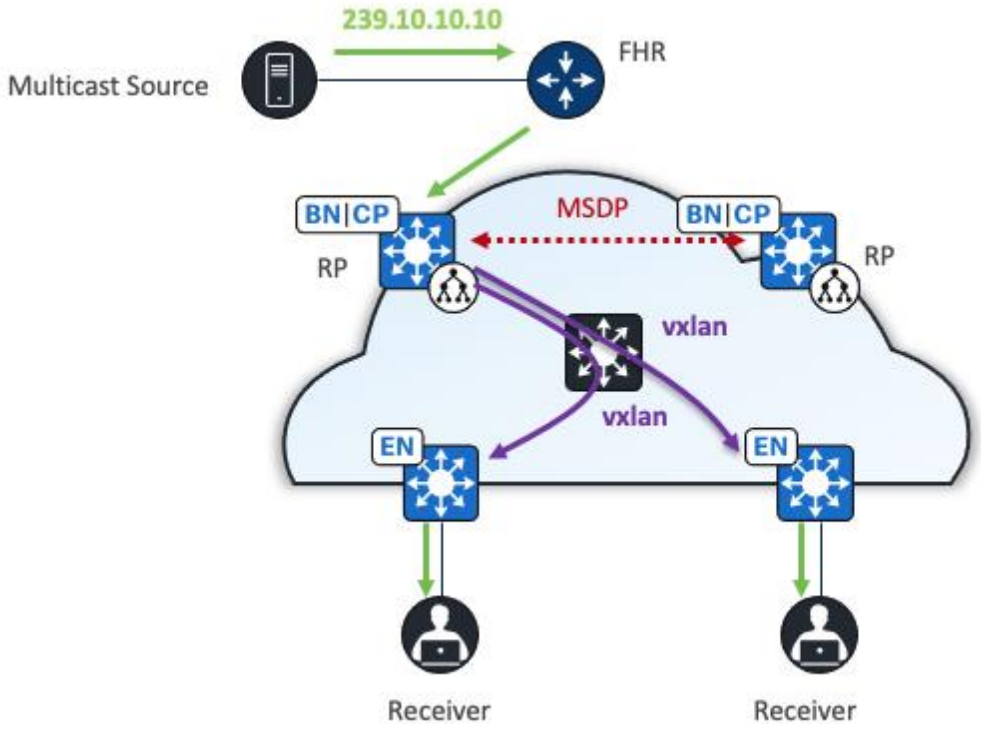
RP をファブリックサイト内のデバイスに展開する必要はありません。ファブリックサイト内のマルチキャストツリーの RP として、外部デバイスを指定できます。外部 RP アドレスは、ボーダーノードの VN ルーティングテーブルで到達可能である必要があります。外部 RP の配置により、ネットワーク内の既存の RP をファブリックで使用できます。このようにして、新しい MSDP 接続を必要とせずにマルチキャストを有効にできます。RP がネットワーク内にすでに存在している場合は、外部 RP を使用してマルチキャストを有効にする方法が推奨されます。

**ヘッドエンド レプリケーション**

ヘッドエンド レプリケーション（または入力レプリケーション）は、マルチキャスト送信元がファブリックオーバーレイ内にある場合はマルチキャスト ファーストホップ ルータ（FHR）によって行われ、送信元がファブリックサイト外にある場合はボーダーノードによって行われます。複製は RLOC ごとに実行され、オーバーレイでユニキャストパケットとして送信されます。マルチキャスト送信元がファブリックサイトの外部にある場合、ボーダーノードはファブリックサイトの FHR のロールを引き受け、関心のあるマルチキャスト サブスクライバを持つすべてのファブリックデバイスにヘッドエンド レプリケーションを実行します。

マルチキャスト送信元は、ファブリックサイトの外部にあります。コントロールプレーンノードを備えたボーダーは、各エッジノードの元のマルチキャストパケットを複製し、VXLAN でカプセル化してからユニキャストで送信します。エッジノードは VXLAN パケットのカプセル化を解除し、元のマルチキャストをクライアントに送信します。

**図 9.　　2 つの共存ボーダーおよびコントロールプレーン上のデュアル RP で、ASM を使用したヘッドエンド レプリケーション**




**ネイティブマルチキャスト**

ネイティブマルチキャストでは、入力ファブリックノードでユニキャスト レプリケーションを行う必要はありません。代わりに、中間ノード（ファブリックロールで動作しないノード）を含むアンダーレイ全体が、レプリケーションを行うために使用されます。ネイティブマルチキャストをサポートするには、FHR、ラストホップルータ、およびそれらの間のすべてのネットワーク インフラストラクチャでマルチキャストを有効にする必要があります。

ネイティブマルチキャストでは、アンダーレイマルチキャスト転送に PIM-SSM を使用します。オーバーレイ マルチキャスト メッセージは、アンダーレイ マルチキャスト メッセージ内でトンネリングされます。このアプローチでは、必要に応じて、ネットワークのオーバーレイとアンダーレイのマルチキャストグループでのオーバーラップが可能です。送受信者間のアンダーレイネットワーク全体がパケットレプリケーションを行うために機能しているため、ヘッドエンド レプリケーションと比較して、スケールとパフォーマンスが大幅に向上します。

ネイティブマルチキャストでは、マルチキャスト内マルチキャストのカプセル化が行われます。オーバーレイからのマルチキャストパケットは、アンダーレイのマルチキャストパケット内にカプセル化されます。この方法では、PIM-SSM と PIM-ASM の両方をオーバーレイで使用できます。

ネイティブ マルチキャスト アンダーレイ設定は、LAN 自動化によってアーカイブできます。アーカイブは、マルチサイトの Cisco SD-Access トランジット展開でもサポートされています。

マルチキャスト送信元がファブリックサイトの外にある場合、ボーダーノードはアンダーレイマルチキャスト SSM ツリーを使用して元のマルチキャストパケットを複製します。次に、パケットを VXLAN でカプセル化し、中間ノードに送信します。中間ノードは元のマルチキャストパケットを複製し、受信者が接続されている各エッジノードに 1 つのコピーを転送します。エッジノードは、VXLAN パケットのカプセル化を解除し、受信者に転送します。

**図 10.　ASM を使用したネイティブマルチキャスト、2 つの共存ボーダーおよびコントロールプレーン上のデュアル RP**

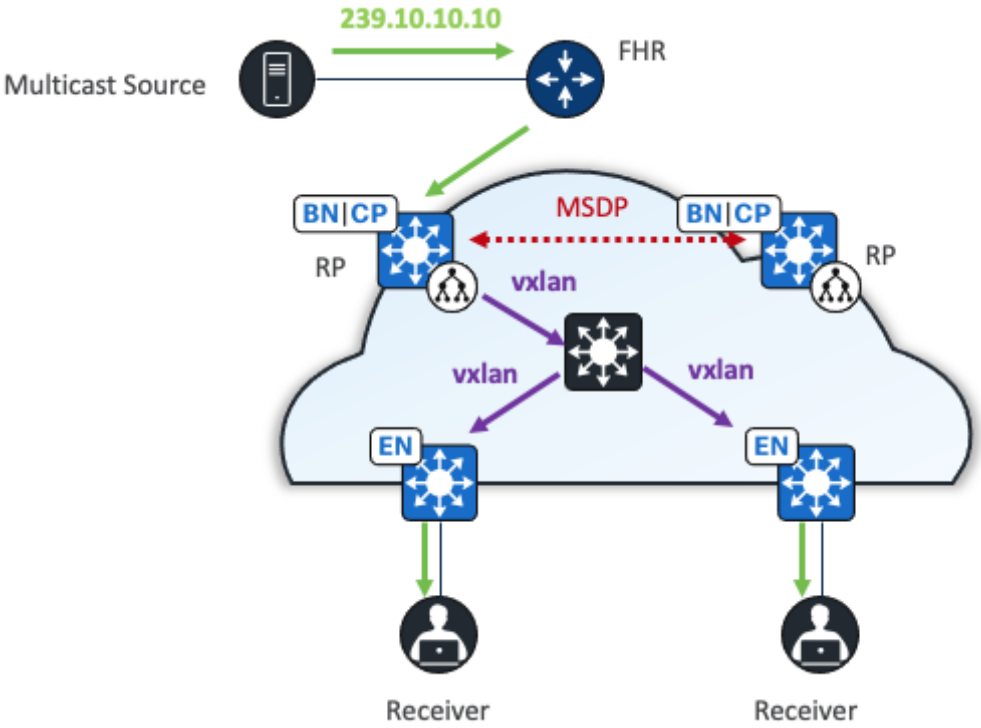



**表 2.**　ヘッドエンドとネイティブマルチキャストの比較

| | ヘッドエンド レプリケーション | ネイティブマルチキャスト |
|---|---|---|
| サポート対象モード（オーバーレイ） | ASM、SSM | ASM、SSM |
| サポート対象モード（アンダーレイ） | 該当なし | SSM（LAN の自動化または手動設定） |
| RP の配置（ASM、オーバーレイ） | ファブリックサイトの内部または外部 | ファブリックサイトの内部または外部 |
| マルチキャストソースの配置 | ファブリックサイトの内部または外部 | ファブリックサイトの内部または外部 |
| RP 冗長性（ASM、オーバーレイ、ファブリックサイト内） | MSDP | MSDP |
| マルチキャスト転送 | マルチキャストパケットは VXLAN でカプセル化され、ユニキャストとしてエッジノードに個別に転送されます | マルチキャストパケットはマルチキャストとして VXLAN 内でカプセル化され、アンダーレイ マルチキャスト ツリーを介してエッジノードに転送されます |

ヘッドエンド レプリケーションの利点は、アンダーレイネットワークでのマルチキャストを必要としないことです。これにより、マルチキャストの観点から、仮想ネットワークと物理ネットワークが完全に分離されます。ただし、FHR で高いオーバーヘッドが発生し、帯域幅の使用率が高くなる可能性があります。アンダーレイネットワークでマルチキャストを有効にできない展開では、ヘッドエンド レプリケーションを使用できます。ネイティブマルチキャストは、その効率性と機能が FHR ファブリックノードの負荷を軽減するため、推奨されています。

このガイドでは、展開セクションのネイティブマルチキャストに焦点を当てています。

### Cisco SD-Access レイヤ 2 のフラッディング

レイヤ 2 フラッディング機能は、特定のオーバーレイサブネットのブロードキャスト、リンクローカル マルチキャスト、および ARP トラフィックのフラッディングを可能にします。従来のネットワーキングでは、ブロードキャストは同じ VLAN のすべてのポートからフラッディングされます。デフォルトでは、Cisco SD-Access はレイヤ 2 ブロードキャストと不明なユニキャストのフラッディングを使用せずにフレームを処理し、代替の方法を使用して ARP ニーズを管理し、エンドポイント間の標準 IP 通信を維持します。

ただし、一部のネットワークではブロードキャストを使用する必要があります。特に、サイレントホストをサポートする場合、通常は ARP ブロードキャストを受信してサイレント状態から抜け出す必要があります。これは、相互に ARP を使用し、レイヤ 2 で直接応答を受信する必要がある、エンドポイントがあるビル管理システム（BMS）で一般的に見られます。ブロードキャストフレームのもう 1 つの一般的な使用例は、Wake on LAN（WoL）イーサネット ブロードキャストです。これは、同じブロードキャストドメイン内でスリープ状態にあるホストを復帰させます。

レイヤ 2 フラッディングは、オーバーレイサブネットをアンダーレイの専用マルチキャストグループにマッピングすることで機能します。ブロードキャスト、リンクローカル マルチキャスト、および ARP トラフィックは、ファブリック VXLAN でカプセル化され、宛先のアンダーレイ マルチキャスト グループに送信されます。PIM ASM は、トランスポートメカニズムとして使用されます。

ファブリックゾーンが設定されていない場合、ファブリックサイト内のすべてのファブリックエッジノードに、同じオーバーレイ VN とオーバーレイ IP サブネットが設定されます。ファブリックゾーンは、不要なレイヤ 2 フラッディングトラフィックを避けるために推奨されます。フラッディングは、ファブリック全体ではなく、選択したファブリックエッジに制限されます。また、独自の VLAN でフラッディングを必要とするエンドポイントを分離することも推奨されます。特定のサブネットに対してレイヤ 2 フラッディングが有効になっている場合、ファブリックエッジノードはそれぞれのアンダーレイ マルチキャスト グループに対してマルチキャスト PIM 加入を送信し、マルチキャスト共有ツリーを効果的に事前構築します。共有ツリーは RP でルート化される必要があります。レイヤ 2 フラッディングが機能するには、この RP がアンダーレイにある必要があります。LAN 自動化を使用してアンダーレイを設定できます。

LAN 自動化を使用する場合、LAN 自動化のプライマリデバイス（シードデバイス）とその冗長ピア（ピアシードデバイス）が、検出されたすべてのデバイスでアンダーレイ RP として設定されます。MSDP は、レイヤ 2 フラッディングのエニーキャスト RP を確立するためにシードデバイス間で自動的に設定されます。さらに、PIM スパースモードは、Loopback0、および LAN 自動化によって設定されたすべてのポイントツーポイント インターフェイスでアクティブになります。

レイヤ 2 フラッディングが必要で、ファブリックサイト内のすべてのデバイス検出に LAN 自動化が使用されなかった場合は、ファブリックサイト内のデバイスでマルチキャストルーティングを手動で有効にし、アンダーレイ内の RP 間で MSDP を設定する必要があります。Loopback0 は、MSDP ピアリングの connect-source および originator-ID として使用できます。

connect-source は、設定されたインターフェイスのプライマリ IP アドレスを MSDP TCP 接続の送信元 IP アドレスとして使用します。originator-ID により、source-Active（SA）メッセージのソースである MSDP スピーカーが、定義されたインターフェイスの IP アドレスを SA メッセージ内で RP アドレスとして使用できます。

originator-ID は、RPF チェックに対処するために MSDP が動作するメカニズムです。アンダーレイを手動で設定する場合、LAN 自動化を通じて行われたのと同じ設定要素をエコーするために、Loopback60000 をアンダーレイの MSDP ピアの RP アドレスとして使用できます。

### マルチサイト リモート ボーダー

マルチサイト リモート ボーダー（MSRB）により、ファブリックネットワークは、ファイアウォールや Demilitarized Zone（DMZ; 緩衝地帯）などの中央の場所に、信頼できないトラフィックを分離できます。たとえば、ネットワークに複数のサイトにまたがるゲスト VN がある場合、すべてのゲストトラフィックを DMZ のリモートボーダーにトンネリングできるため、ゲストトラフィックを企業トラフィックから分離できます。

マルチサイトネットワーク展開では、ネットワーク管理者は、共通のボーダー（MSRB）を指定して、複数のサイトにまたがる特定の VN との間のトラフィックをルーティングすることができます。これにより、管理者は、これらすべてのサイトにわたって単一のサブネットを持つ複数のファブリックサイトに VN を展開できます。複数のファブリックサイト間でサブネットを保持すると、IP アドレス空間を節約できます。

MSRB のコンテキストで使用される一般的な用語には、次のものがあります。

- アンカー仮想ネットワーク：

  ネットワーク内の複数のファブリックサイトにまたがって存在する仮想ネットワークです。関連付けられた IP サブネットとセグメントは、これらの複数のサイトで共通です。

- アンカーサイト：

  アンカー VN の共通のボーダーとコントロールプレーンをホストするファブリックサイトです。アンカーサイトは、アンカー VN の入力および出力トラフィックを処理します。

- 継承されたサイト：

  アンカー VN が展開されているアンカーサイト以外のファブリックサイトです。

- マルチサイト リモート ボーダー：

  アンカー VN との間のトラフィックの入出力場所を提供する、アンカーサイトのファブリックボーダーノードです。

- アンカー コントロール プレーン ノード：

  アンカー VN のエンドポイントの登録を受け入れ、要求に応答する、アンカーサイトのファブリック コントロール プレーン ノードです。

### 単一の Cisco ISE に対する複数の Catalyst Center

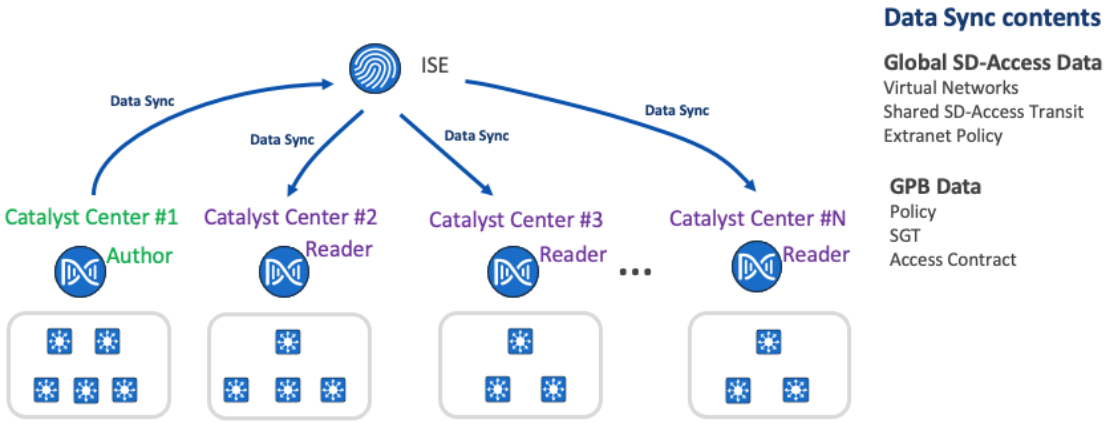
Cisco ISE は 2,000,000 エンドポイントにまで拡張できます。Catalyst Center の拡張性は、25,000 ～ 100,000 のエンドポイントのみです（DN3-HW-APL 32 コアアプライアンスの場合は 25,000、DH3-HW-APL-L 56 コアアプライアンスの場合は 40,000、DN3-HW-APL-XL 112 コアアプライアンスの場合は 100,000）。複数の Catalyst Center 機能を使用すると、大規模または分散型のエンタープライズ ファブリックを展開しているお客様向けに、複数の Catalyst Center を同じ Cisco ISE と統合できます。この機能は、作成者ノードとリーダーノードの概念を使用

して、展開におけるポリシー定義とグローバル Cisco SD-Access データの単一の管理ポイントを作成します。これらの定義の複製は、Cisco ISE を介して作成者ノードから読み取りノードに伝播されます。

### ソリューション設計

複数の Catalyst Center 機能は、Cisco ISE との既存のセキュアな接続を使用して、1 つのクラスタから別のクラスタに同じ Cisco ISE 展開と統合される VN、SGT、アクセス契約、ポリシー、共有 Cisco SD-Access トランジット、エクストラネットポリシーを複製します。Cisco ISE は、あるクラスタ（作成者ノード）から学習した情報を取得し、他のクラスタ（リーダーノード）に提供します。

**図 11.　Catalyst Center は Cisco ISE との信頼できる通信リンクを作成して、グループベースのアクセス コントロール ポリシーとグローバル Cisco SD-Access データを伝播する**




### 作成者ノード

作成者ノードは、Cisco ISE と統合される最初の Catalyst Center です。PxGRID REST API インターフェイスで ERS を使用して、グローバルの Cisco SD-Access および GPB データを Cisco ISE にプッシュします。GPB および Cisco SD-Access コンポーネントの作成、変更、または削除は、作成者ノードでのみ実行できます。作成者ノードに加えられた変更はすべて Cisco ISE に同期されてから、Cisco ISE がリーダーノードにパブリッシュします。

作成者ノードには 1 つの Catalyst Center のみ指定できます。これは、ブラウンフィールドにできる唯一のノードです（ユーザー定義の VN、共有 Cisco SD-Access トランジット、エクストラネットポリシー、SGT、アクセス契約、およびグループベース アクセス コントロール（GBAC）ポリシーを含む）。

### リーダーノード

同じ Cisco ISE リーダーノードと統合されている他のすべての Catalyst Center です。リーダーノードには、セキュリティグループとグローバル Cisco SD-Access データの読み取り専用ビューがありますが、アクセス契約またはポリシーの可視性はありません。代わりに、リーダーノードには、情報にアクセスするための作成者ノードにクロススタートするためのハイパーリンクがあります。

リーダーノードは、作成者ノードクラスタで定義されているのと同じ SGT、アクセス契約、GBAC ポリシー、グローバル Cisco SD-Access データを使用します。これらのオブジェクトは、スタンドアロンの Catalyst Center であるかのように、プロビジョニング操作に使用できます。

最大 4 つのリーダーノードがサポートされており、任意のリーダーノードを作成者ロールに昇格させることができます。Catalyst Center にリーダーノードとして追加する前に、ユーザー定義の VN を設定する必要はありません。

**注：** これは、限定のアベイラビリティ機能です。限定のアベイラビリティプログラムへの参加に関心がある場合は、Cisco SD-Access Design Council にお問い合わせください。

## Cisco SD-Access ワイヤレス

ワイヤレス コントロール プレーンを有線のオーバーレイ コントロール プレーンと統合することで、Cisco SD-Access は独自の差別化要因を提供します。Cisco SD-Access ワイヤレスは、分散データプレーンを備えた集中型コントロールおよび管理プレーンを提供し、集中型ワイヤレス設計と分散型ワイヤレス設計の両方を提供します。ワイヤレスコントローラをコントロールプレーンノードと統合します。オンボーディング時にエンドポイントを登録し、ローミング時にエンドポイントの位置を更新します。これは、ワイヤレス コントロール プレーンと有線コントロールプレーンの間に相乗作用が発生する最初のインスタンスです。

有線とワイヤレスのこの独自の統合は、ネットワークユーザーと、それらをサポートする運用チームに、いくつかの利点をもたらします。

- 簡素化：

  ネットワークは、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単一のサブネットを持つことができます。

- ポリシーの一貫性：

  広範な有線ポリシーのセットがワイヤレストラフィックにも拡張され、両方がエッジノードで適用されます。

- パフォーマンスの向上：

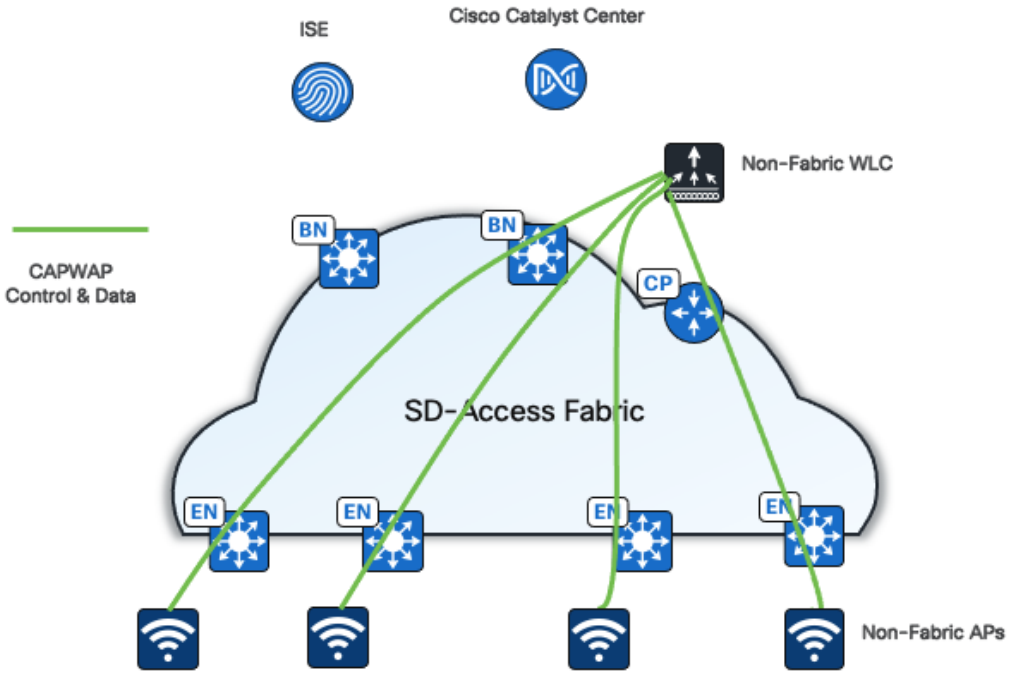
  ワイヤレスローミングはレイヤ 2 であり、アンカーリングは必要ありません。

### 統合モード

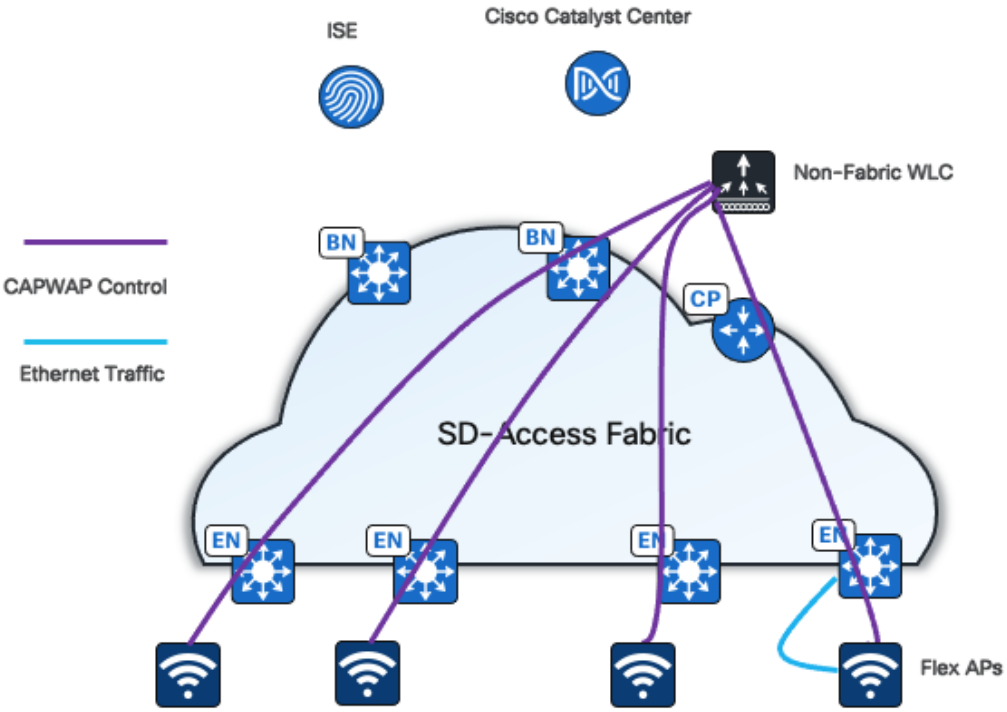
Cisco SD-Access は、ワイヤレスアクセスをネットワークに統合するために、いくつかのオプションをサポートしています。

1 つ目のオプションでは、従来の Cisco Unified Wireless Network（CUWN）のローカルモード設定であるオーバーザトップを、非ネイティブのサービスとして使用します。このモードでは、Cisco SD-Access ファブリックはワイヤレストラフィック用のトランスポートネットワークとなり、移行時に、トンネリングされた Control and Provisioning of Wireless Access Points Protocol（CAPWAP）エンドポイントトラフィックを AP からワイヤレスコントローラに転送するために役立ちます。

# CUWN Wireless Over The Top (OTT)



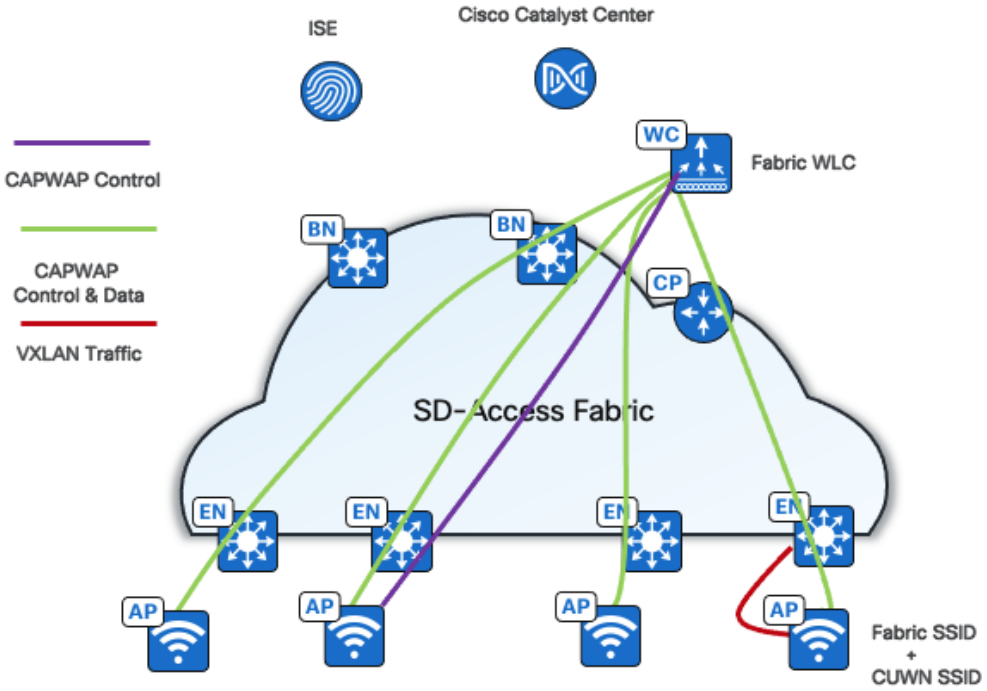

2 つ目のオプションは、FlexConnect オーバーザトップ（OTT）です。このモードでは、AP は、接続されているエッジノードにトラフィックをローカルにリダイレクトします。



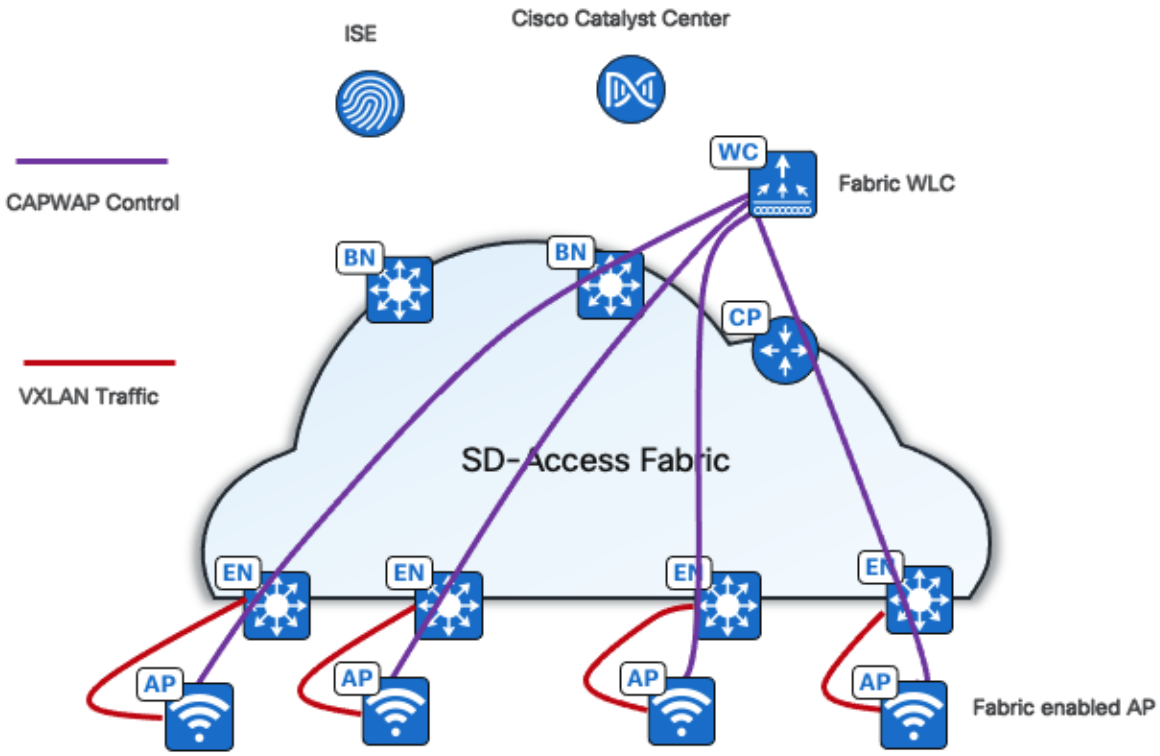

**注：** ローミング遅延を実現するには、追加の Cisco SD-Access 機能であるサブネット内ルーティング（レイヤ 2 フラッディングを無効にする）を設定する必要があります。レイヤ 2 フラッディングが必要な場合、Cisco SD-Access とのフレックス OTT 統合は、すべてのフレックス Wi-Fi ベンダーでサポートされていない可能性があります。

3 つ目のオプションは、ファブリック ワイヤレス コントローラがファブリック SSID と非ファブリック（集中型）SSID の両方をブロードキャストする混合モードです。混合モードは、同じ AP または異なる AP の両方でサポートされています。非ファブリック SSID に参加するクライアントからのトラフィックは、CAPWAP でカプセル化されてワイヤレスコントローラに送信されます。ファブリッククライアントのトラフィックは VXLAN でカプセル化され、ファブリックに送信されます。

# Mixed Mode Over The Top (OTT)




最後の最適なオプションは、Cisco SD-Access ワイヤレスの完全な統合です。Cisco SD-Access を、有線エンドポイントだけでなくワイヤレスエンドポイントまで拡張します。




ファブリックにワイヤレス LAN を統合することで、アドレッシングのシンプル化、拡張サブネットによるモビリティ、さらに有線ドメインとワイヤレスドメインにわたる一貫したポリシーによるエンドツーエンドのセグメンテーションなど、ファブリックの有線クライアントに提供されるものと同じ利点がワイヤレス クライアントにまで拡張されます。またワイヤレス統合により、ワイヤレスドメインに対するコントロールプレーンとして機能しながら、ワイヤレスコントローラによるデータプレーンの転送作業が軽減されます。

ファブリック ワイヤレス コントローラは、従来のローカルモードコントローラと同じ一般的なモデルを使用して、ファブリックモード AP を管理および制御します。そのため、モビリティ制御や無線リソース管理など、運用上の利点は同じです。大きな違いは、ワイヤレスエンドポイントからのクライアントトラフィックが、AP からワイヤレスコントローラにトンネリングされないことです。代わりに、ファブリック AP によってワイヤレスクライアントからの通信が VXLAN でカプセル化され、ファーストホップ ファブリック エッジ ノードへのトンネルが構築されます。レイヤ 3 エニーキャストゲートウェイ、ポリシー、トラフィック適用などのファブリックサービスを、エッジノードが提供するため、ワイヤレストラフィックはエッジノードにトンネル化されます。

この違いにより、統合 SGT 機能を備えた分散データ プレーンが実現します。トラフィックの転送では、Cisco SD-Access ファブリックから最適なパスを入手し、エンドポイントが有線接続かワイヤレス接続かにかかわらず、一貫したポリシーに従って宛先に送信されます。

AP のコントロールプレーン通信では、従来の CUWN コントロールプレーンに類似した、ワイヤレスコントローラへの CAPWAP トンネルを使用します。ただし、ファブリック ワイヤレス コントローラは Cisco SD-Access コン

トロールプレーン（LISP）通信に統合されます。ファブリック ワイヤレス コントローラとして追加されると、コントローラはファブリック コントロール プレーン ノードとの双方向通信を構築します。

この通信により、ワイヤレスコントローラはクライアントのレイヤ 2 MAC アドレス、SGT、およびレイヤ 2 セグメンテーション情報（レイヤ 2 VNI）を登録できます。これらすべてが連携して、ファブリックサイト全体の AP 間のワイヤレス クライアント ローミングをサポートします。Cisco SD-Access ファブリック コントロール プレーンでは、エンドポイントが新しい RLOC に関連付けられると（AP 間のワイヤレス エンドポイント ローミング）、ホストトラッキング データベースに更新することで、ローミング機能がサポートされます。

この導入ガイドでは、完全に統合された Cisco SD-Access ワイヤレスに焦点を当てています。

## Cisco SD-Access ワイヤレスプラットフォームのサポート

Cisco SD-Access ワイヤレスは、さまざまなシスコ ワイヤレス コントローラ プラットフォームおよび AP でサポートされます。次に例を示します。

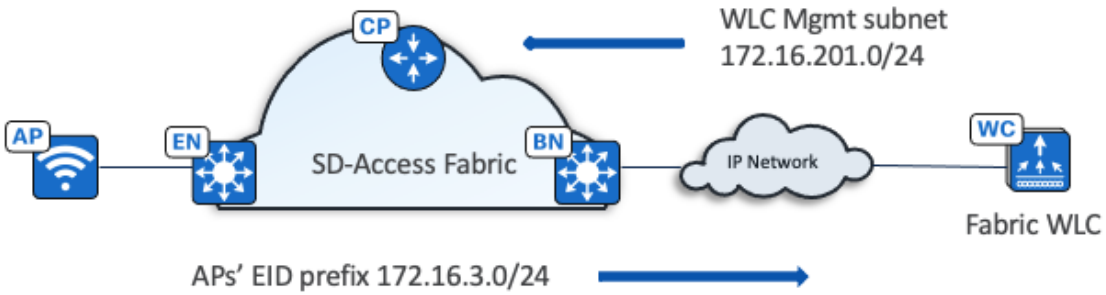
- Cisco 3504、5520、8540 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 9300/9400/9500 上の組み込みワイヤレスコントローラ
- Wi-Fi 6 AP：Cisco Catalyst 9105AX、9115AX、9117AX、9120AX、9124AX、および 9130AX シリーズ
- Wi-Fi 6 AP：Cisco Catalyst 9163E、9164、および 9166 シリーズ
- Cisco Catalyst Wireless 9162I 統合アクセスポイント
- 802.11 Wave 2 AP：Cisco Aironet 1800、2800、3800、および 4800 シリーズ
- 802.11 Wave 2 屋外 AP：Cisco Aironet 1540、1560
- Heavy Duty シリーズ AP：Cisco Catalyst IW6300、IW9165、および IW9167
- Cisco Industrial Wireless 3702 アクセスポイント

最新のサポート対象デバイスモデルとソフトウェアの情報については、「Cisco SD-Access Compatibility Matrix」を参照してください。

## Cisco SD-Access ワイヤレスの展開に関する考慮事項

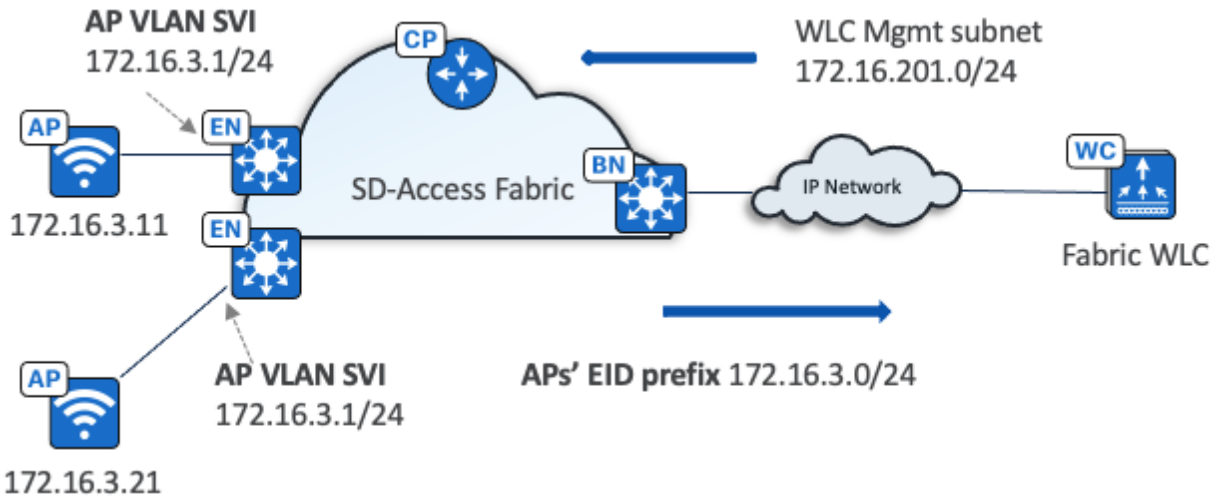
このセクションでは、Cisco SD-Access ワイヤレスネットワークにワイヤレスコントローラと AP を展開する際の重要な考慮事項について説明します。

### ワイヤレスコントローラ



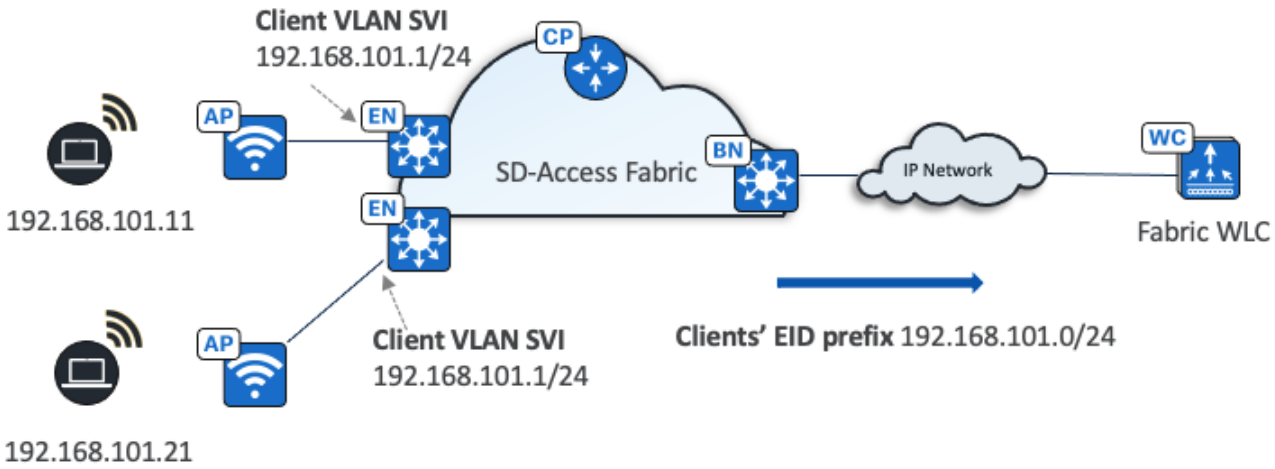

- ワイヤレスコントローラは、ファブリック外にあります。
- ファブリック AP はファブリックに対してローカルであり、ローカルモードでワイヤレスコントローラに接続します。
- ボーダーは、ワイヤレスコントローラ管理サブネットをファブリックにアドバタイズします。
- ボーダーは、ファブリックのプレフィックスをワイヤレスコントローラ管理ネットワークにアドバタイズします。

**AP**



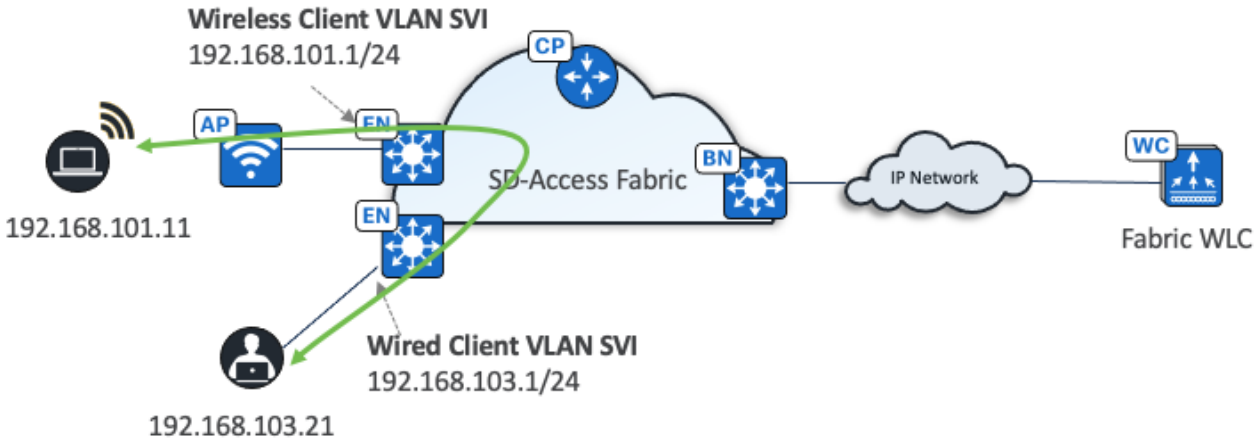

- AP は、ファブリックエッジまたは拡張ノードデバイスに直接接続されています。
- AP は、ファブリックエッジのオーバーレイスペース内にあります。
- AP は、コントロールプレーンのデータベースに登録されます。
- AP オンボーディングの IP 設計を簡素化します（AP オンボーディング用の各ファブリックサイトに 1 つのサブネット）。

**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ます。
- ワイヤレスコントローラの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のエニーキャストゲートウェイを使用して VLAN にマッピングされます。
- すべてのローミングはレイヤ 2 です。

**ワイヤレス トラフィック フロー**




- ワイヤレス クライアント トラフィックは分散処理されます
- 集中型コントローラへのヘアピニングはありません
- 有線クライアントとの通信は、ファブリックを直接使用します

**次に要約を示します。**

AP 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

- ローカルモードでワイヤレスコントローラに参加する

ワイヤレスコントローラは、次のように展開する必要があります。

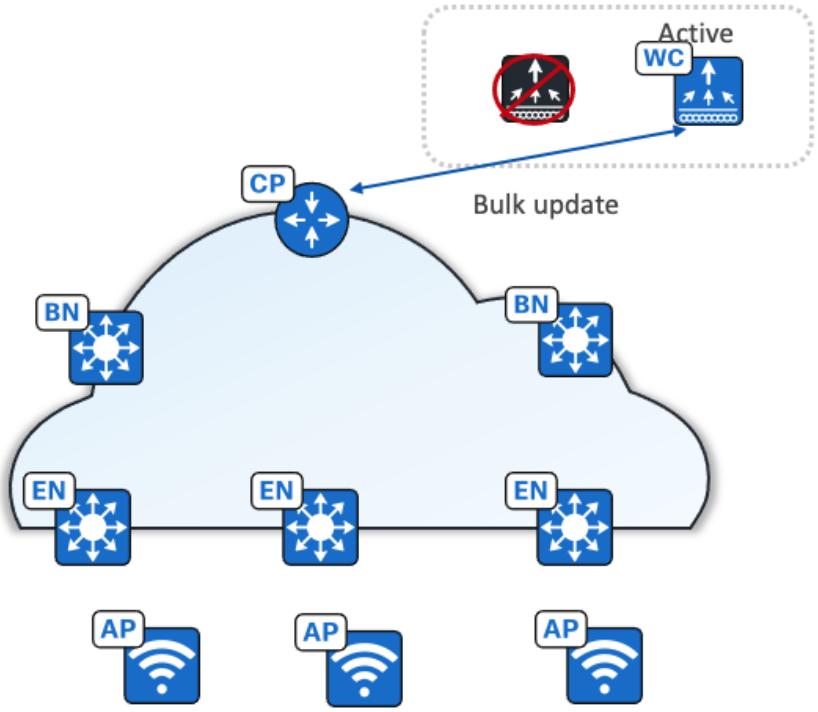
- グローバル ルーティング テーブル内に存在する
- ファブリックの外部に、スタンドアロン ワイヤレス コントローラとして接続する（必要に応じてボーダーに直接接続）
- 1 つのファブリックサイトに属する
- Cisco Catalyst 9300/9400/9500 の組み込みワイヤレスコントローラなどの制限を検討する。ここではスケールと機能のサポートに制限があるため、小規模なブランチでの展開にのみ推奨される
- 近い将来に段階的に廃止されるため、新しい展開では、Cisco 3504、5520、および 8540 シリーズ ワイヤレス コントローラの使用を避ける

**注：** ワイヤレスコントローラは、デフォルトルートを介して到達できないようにする必要があります。ファブリックノードごとにグローバル ルーティング テーブル内の特定のルートを使用します。

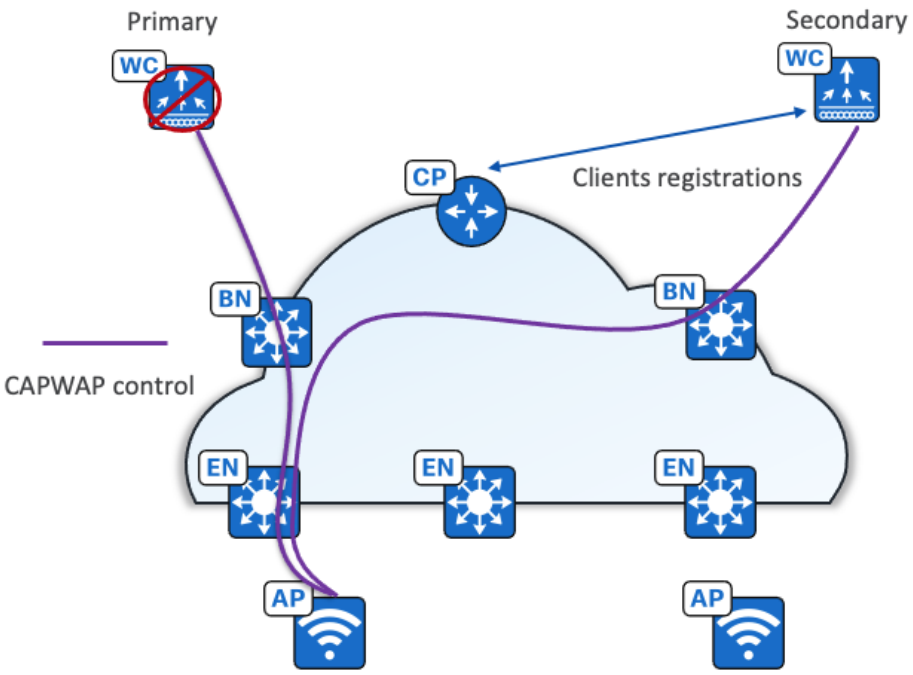
**ワイヤレスコントローラの冗長性**

ワイヤレスコントローラでは、ファブリック対応コントローラに SSO（ステートフル）アーキテクチャと N+1（ステートレス）アーキテクチャの両方を使用した高可用性（HA）がサポートされています。

SSO アーキテクチャを使用したステートフル冗長性では、ワイヤレスコントローラペアはファブリックによって 1 つのノードと見なされます。アクティブなワイヤレスコントローラのみが、ファブリック コントロール プレーン ノードと連係します。ファブリック設定およびコントロールプレーンのステータスは、アクティブ ワイヤレス コントローラとスタンバイ ワイヤレス コントローラの間で同期されます。障害が発生した場合、新しいアクティブ ワイヤレス コントローラは、ファブリッククライアントをファブリック コントロール プレーン ノード（ホスト トラッキング データベース ノード）に一括更新して、AP とクライアントが接続されたままになるようにします。




ステートレス N+1 冗長性アーキテクチャでは、AP はプライマリおよびセカンダリ ワイヤレス コントローラで設定されます。AP および関連するワイヤレスコントローラは、プライマリ ワイヤレス コントローラに登録されます。プライマリの障害時、AP は接続を解除し、セカンダリ ワイヤレス コントローラに参加します。ワイヤレス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、ファブリック コントロール プレーン ノード（ホストトラッキング）に新規のクライアント登録を行います。

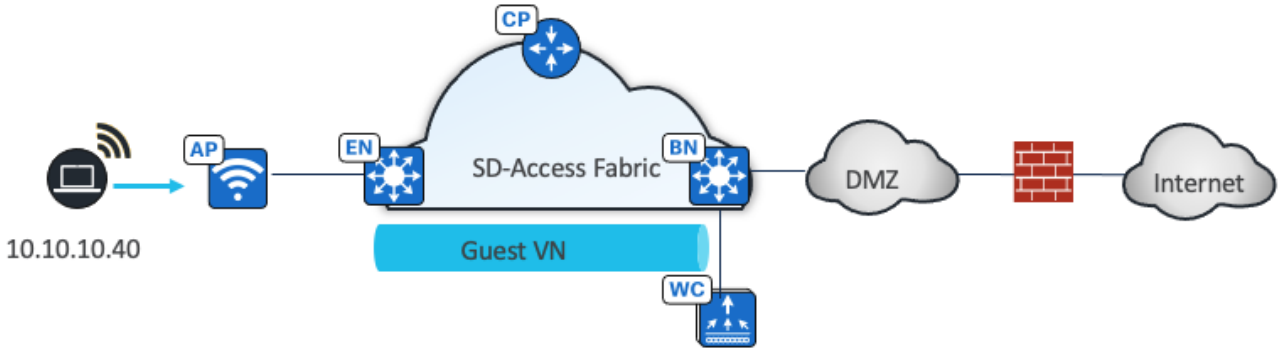


## Cisco SD-Access ワイヤレスゲストアクセス設計

完全に統合された Cisco SD-Access ワイヤレスネットワークでは、ワイヤレスゲストアクセスをさまざまなソリューションを使用して統合できます。

- 専用のゲスト VN
- 専用のゲストファブリックサイト（MSRB VN アンカーリング ソリューション）
- 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

**図 12.　　ゲストの専用 VN：**




この設計では、ゲストネットワークは Cisco SD-Access ファブリック内の別の VN として確立され、マクロセグメンテーションを使用してゲストデータプレーンを他の企業トラフィックから分離します。設定は、Catalyst Center を介して、VN を作成し、IP プールを定義し、SSID をゲスト IP プールに関連付けることで行います。マイクロセグメンテーションは、VN の 2 番目のレイヤセグメンテーションとして使用できます。異なるゲストロールに、異なる SGT を割り当てることができます。

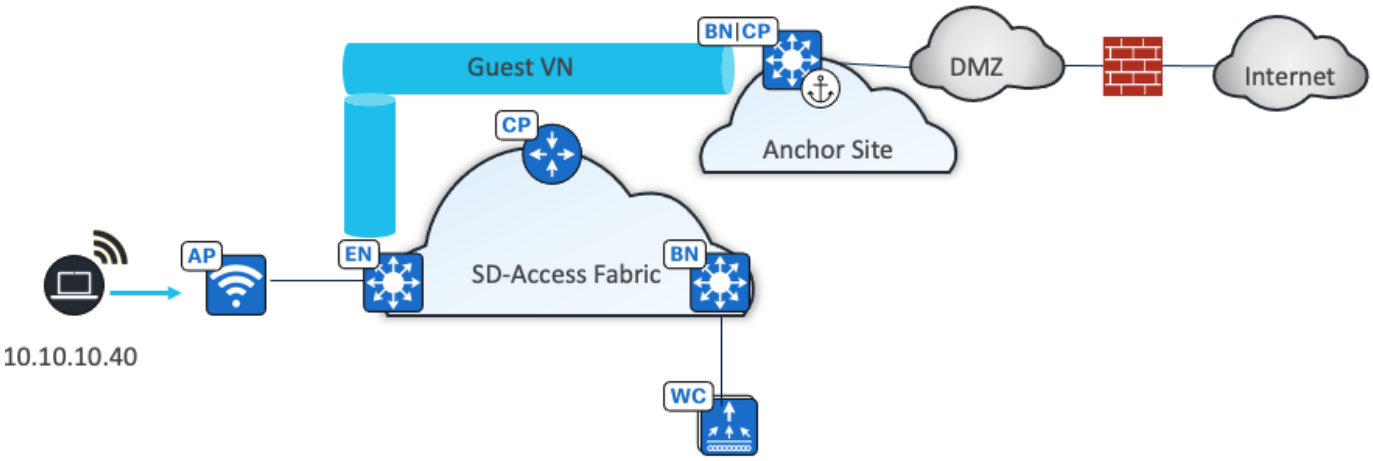
同じゲスト VN を、有線ゲストクライアントに使用することもできます。

### 個別のファブリックサイトとしてのゲスト（MSRB VN アンカーリング ソリューション）

ゲストネットワーク、データプレーントラフィック、およびコントロールプレーンを完全に分離する必要がある場合は、Catalyst Center のアンカー VN とアンカープールを使用して専用のコントロールプレーンおよびボーダー（MSRB）を設定し、ゲストユーザーを管理できます。

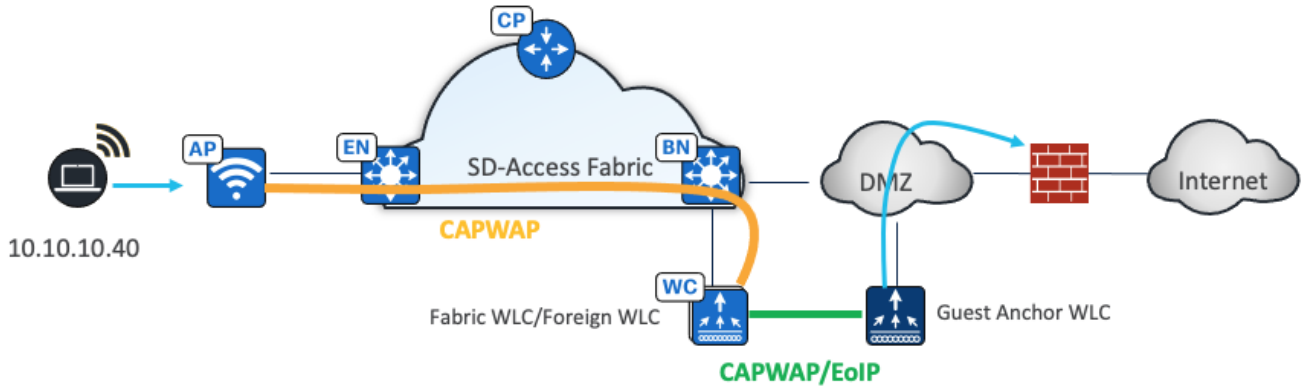
このソリューションでは、トラフィックは VXLAN の AP でファブリックエッジスイッチにカプセル化されていますが、ファブリックエッジノードは別のボーダーノードをアンカー VN に使用するように設定されています。このボーダーノードを別のファブリックサイトに配置して、トラフィックを完全に分離することができます。ゲストユーザーは、ボーダーと同じ場所に配置される場合がある専用コントロールプレーンに登録され、DMZ 内でユーザーに IP アドレスが割り当てられます。

専用 VN ソリューションと同様に、この設計は有線とワイヤレス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およびボーダーの選択は、ソリューションの拡張性によって異なります。




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

ゲスト ワイヤレス ネットワークを OTT ソリューションとして展開することで、ゲストアンカーコントローラを使用します。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でき、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展開に最適です。




## Cisco SD-Access ネットワークの展開に関する考慮事項

### アンダーレイネットワーク設計

適切に設計されたアンダーレイネットワークによって、Cisco SD-Access ネットワークの安定性、パフォーマンス、および効率的な使用状況が確保されます。アンダーレイネットワークの展開の自動化は、LAN 自動化機能を使用して Catalyst Center を介して利用できます。

LAN 自動化を使用する場合でも、ネットワークを手動で展開する場合でも、ファブリックのアンダーレイネットワークには次の一般的な設計要件があります。

- MTU と TCP MSS：

  VXLAN ヘッダーには、カプセル化により 50 バイトのオーバーヘッドが加わります。9100 のキャンパスおよびブランチ全体の MTU を有効にすると、ファブリック内でフラグメント化することなく、イーサネットジャンボフレームを転送できます。

アンダーレイネットワークが 1500 バイトを超えるパケットをサポートしていないシナリオがあります。たとえば、ファブリックサイトが、1500 バイトを超えるパケットをサポートしていない WAN 上の Cisco SD-Access トランジットを使用して接続されている場合です。これらのシナリオでは、VXLAN ヘッダーのカプセル化によるオーバーヘッドを考慮して、Transmission Control Protocol の最大セグメントサイズ（TCP MSS）を設定してパケットサイズを制限できます。推奨値は 1250 です。Catalyst Center は TCP MSS 自動化をサポートしています。この方式は TCP アプリケーションでのみ機能します。

MTU 9100 の設定は、すべての Catalyst 9000 スイッチの LAN 自動化でサポートされています。

- ポイントツーポイントリンク：

  ポイントツーポイントリンクでは、複雑なトポロジで一般的に発生する、上位層プロトコルのタイムアウトを待つ必要がなくなるため、コンバージェンス時間が最短になります。ポイントツーポイントリンクおよび推奨される物理トポロジ設計を組み合わせることで、リンクに障害が発生した場合に高速コンバージェンスが確保されます。

  ポイントツーポイント設定は、すべての Catalyst 9000 スイッチの LAN 自動化でサポートされています。

- ECMP：

  等コスト マルチパス ルーティングは、複数のベストパスを介して、1 つの宛先へのネクストホップパケット転送を実行できるルーティング戦略です。これらの ECMP パス間のロードバランシングは、Cisco Express Forwarding（CEF）を使用して自動的に実行されます。ECMP 対応ルーティングプロトコルを使用して、パラレルコストリンクを活用し、冗長転送パスを確保して復元力を強化する必要があります。

- BFD：

  Bidirectional Forwarding Detection（BFD）は、ルーティングプロトコルの障害の検出とコンバージェンスの特性を強化します。ルーティングプロトコルでは、Hello パケットの不在を利用して、隣接ネイバーがダウンしているかどうかを判断します（一般に、ホールドタイマーまたはデッドタイマーと呼ばれます）。したがって、ネイバーの活性を検出する機能は、Hello パケットの頻度に基づいています。BFD は、デバイス間の転送パスで低いオーバーヘッドの 1 秒未満の障害検出を提供し、さまざまなルーティングプロトコル（変数の Hello タイマーを持つ場合がある）を使用して、ネットワーク全体で均一のレートに設定できます。

  BFD は、（rx_min 250ms、tx_min 250ms）x 3 を使用したすべての LAN 自動化レイヤ 3 インターフェイスで、LAN 自動化によって設定されます。

- NSF：

  ノンストップ フォワーディング（グレースフルリスタート）は SSO と連動して、ルートプロセッサ（RP）のスイッチオーバー中にパケットの継続的な転送を提供します。NSF 認識 IGP ルーティングプロトコルを使用して、スイッチオーバー後にネットワークを利用できない時間を最小限に抑える必要があります。

- SSO：

  ステートフル スイッチオーバーでは、プライマリルートプロセッサとバックアップ ルート プロセッサ（ルーティング プラットフォームの RP やスイッチング プラットフォームのスーパーバイザエンジンなど）でス

テート情報を同期することによって、ユーザーセッションなどのステートフルな機能情報が維持されます。サポートされているデバイスで、SSO を NSF とともに有効にする必要があります。

- ファブリックの IGP プロセス：

  現在 LAN 自動化でサポートされているプロトコルは IS-IS のみですが、OSPF や EIGRP などの他のクラスレス ルーティング プロトコルもサポートされており、ECMP と NSF に対応しています。

- Loopback0 伝播：

  Catalyst Center は、LISP 設定で Loopback0 インターフェイスを RLOC として使用するため、/32 マスクが必要です。ループバックアドレス（RLOC）間の到達可能性は、デフォルトルートを使用できません。ファブリックサイト内の明示的なルート（/32 ルート）を使用する必要があります。

  マルチサイト Cisco SD-Access トランジット展開では、外部ボーダーとトランジット コントロール プレーン ノードの Loopback0 アドレスをアドバタイズする必要があります。MSRB 展開では、アンカーされたサイトの MSRB とファブリックエッジも相互に /32 ルートを持つ必要があります。

  LAN 自動化では、提供された LAN プールから /32 サブネットで Loopback0 が設定されます。

- ワイヤレスコントローラの到達可能性：

  ワイヤレスコントローラへの接続は、ループバックアドレスへの到達可能性と同様に扱う必要があります。アンダーレイのデフォルトルートは、ファブリックエッジをワイヤレスコントローラに到達させるために使用することはできません。ワイヤレスコントローラの IP アドレスへの特定のルート（デフォルト以外のルート）は、AP が物理的に接続されている各ファブリックエッジの GRT（アンダーレイ）に存在する必要があります。ホストルート（/32）または集約ルートを使用できます。

- 導入での LAN 自動化：

  Catalyst Center の LAN 自動化サービスを使用すれば、アンダーレイの設定をオーケストレーションすることができます。LAN 自動化は、新しいネットワークのアンダーレイの手動展開に代わるものです。IS-IS ルーテッドアクセス設計を使用します。IS-IS ルーティングプロトコルには、IP プロトコルに依存しないネイバーの確立、ループバックアドレスを使用したピアリング機能、および IPv4、IPv6、非 IP トラフィックを問わない処理など、運用上の利点があります。手動アンダーレイもサポートされているため、基本的なアンダーレイ設計原則に準拠しながら、別の IGP を選択するなど、自動アンダーレイ展開から逸脱する柔軟性を提供します。

  LAN 自動化はルータプラットフォームではサポートされておらず、IPV4 アドレッシングでのみサポートされています。最大 5 階層の PnP エージェントデバイスを検出して自動化できます。

### ピアデバイスと共有サービスルーティング

「共有サービス」セクションで説明したように、共有サービスはファブリックサイトの外部に通常あり、Cisco SD-Access ネットワーク内のクライアントに必要な要素です。Cisco SD-Access の展開では、ピアデバイスが外部ドメインからファブリックに共有サービスをアドバタイズします。ピアデバイスはファブリックの外部にあり、次を含むいくつかの技術要件を満たす必要がある真のルーティング プラットフォーム、レイヤ 3 スイッチング プラットフォーム、またはファイアウォールのいずれかになります。

- 複数の VRF：

  VRF 認識ピアモデルには、複数の VRF が必要です。ボーダーノードでハンドオフされる各 VN に対して、対応する VN とインターフェイスがピアデバイスで設定されます。選択したプラットフォームは、共有サービスへのアクセスを必要とする、ファブリックサイトで使用される VN の数をサポートする必要があります。

- サブインターフェイス（ルータまたはファイアウォール）：

  ルーテッド物理インターフェイス上の VLAN ID に関連付けられた仮想レイヤ 3 インターフェイスです。IP ルーティング機能を拡張し、IEEE 802.1Q カプセル化を使用して VLAN 設定をサポートします。

- スイッチ仮想インターフェイス（レイヤ 3 スイッチ）：

  スイッチ上の論理レイヤ 3 インターフェイスを表します。この SVI は、レイヤ 3 IEEE 802.1Q VLAN に対するレイヤ 3 インターフェイス転送です。

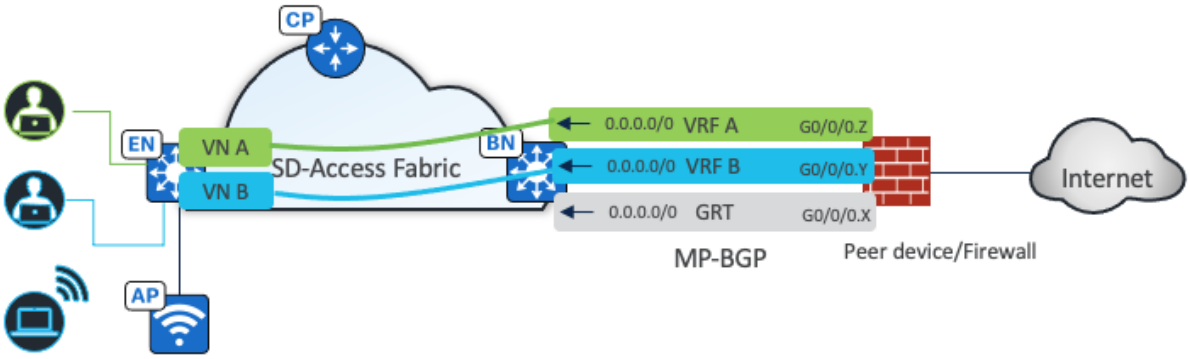
- IEEE 802.1Q：

  元のイーサネットフレームの送信元アドレスフィールドと、タイプフィールドまたは長さフィールドの間に、4 バイトのタグフィールドを挿入する内部タギングメカニズムです。SVI とサブインターフェイスをサポートするデバイスは、802.1Q タギングもサポートします。

Catalyst Center は、レイヤ 3 ハンドオフ機能により、ボーダーノードでの設定を自動化できます。この機能は、スイッチング プラットフォームの各 SVI またはルータプラットフォームのサブインターフェイスを異なるファブリック VN（例では VRF）に関連付けることによって、VRF Lite をプロビジョニングします。外部 BGP（eBGP）は、エンドポイントスペース（EID スペース）のプレフィックスをファブリックサイトから外部ルーティングドメインにアドバタイズし、トラフィックを EID スペースに引き付ける、ルーティングプロトコルとして使用されます。この BGP ピアリングは、ルートをオーバーレイにアドバタイズするためにも使用できます（内部ボーダーの共有サービスへのアクセスなど）。

図 12 に示すように、ファブリックサイトの VN はファイアウォールの VRF にマッピングされ、ルーティングの分離が実現されます。eBGP ピアは、分離とルーティングを容易にするため、ボーダーレイヤ 3 ハンドオフに基づいて各 VRF に確立されます。インターネット サービス デフォルト ルート 0.0.0.0./0 が、各 VRF のファブリックボーダーノードにアドバタイズされます。

**図 13.　ピアデバイスは、サブインターフェイスをサポートするファイアウォールであり、複数の VRF と 802.1Q を備えている**



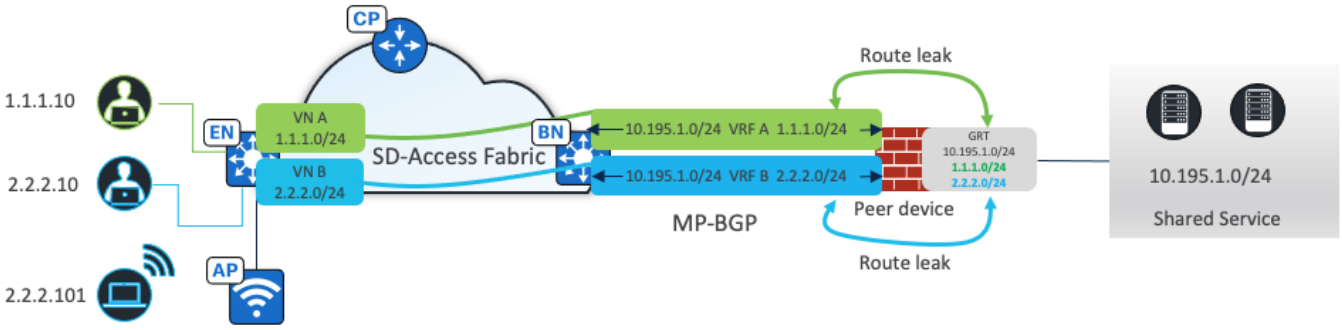
共有サービスの展開方法に応じて、ピアデバイス上の共有サービスルーティングがアーカイブされる主な方法は次のとおりです。

- ルートリーク：

  共有サービスルートがグローバル ルーティング テーブル（GRT）にある場合に使用され、ピアデバイスでは IP プレフィックスリストを使用してこれらのルートを識別します。ルートマップはこれらの IP プレフィックスリストを参照し、VRF 設定でルートマップを参照して、明確に一致したルートだけがリークされるようにします。

図 13 に示すように、ボーダーレイヤ 3 ハンドオフを使用して各 VRF に eBGP ピアが確立されます。共有サービスプレフィックスは GRT にあります。ルートリークはピアデバイスで実行され、VRF からのクライアントプレフィックスが GRT にリークされます。GRT の共有サービスプレフィックスが VRF にリークされます。

**図 14.　　ファブリックサイトの VN がピアデバイスの VRF にマッピングされる**




- VRF リーク：

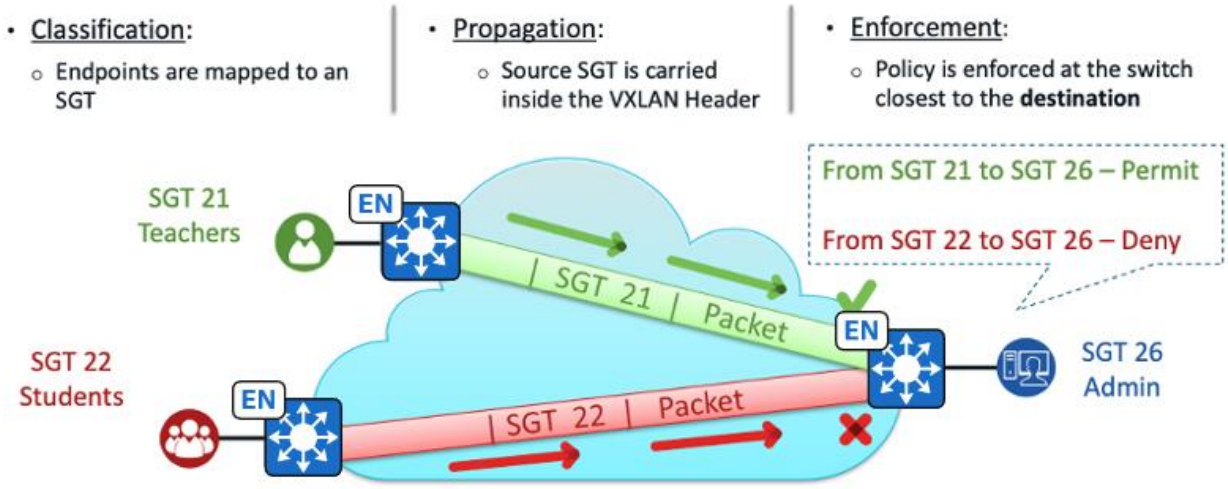
  共有サービスがピアデバイスの専用 VRF に展開されている場合に使用されます。VRF 設定のルートターゲットは、ファブリック VN と共有サービス VRF 間のリークに使用されます。

### エンドツーエンド マイクロセグメンテーション

マクロセグメンテーションでは、VN を使用してクライアントを分離します。異なる VN のクライアントは、相互に通信できません。

マイクロセグメンテーションは、SGT とセキュリティ グループ アクセス コントロール リスト（SGACL）を使用して、出力アクセスデバイスでトラフィックポリシーを適用します。

**図 15.　エンドポイントトラフィックの Cisco SD-Access の展開におけるマイクロセグメンテーションの仕組み**




- 分類：

  クライアントは同じ VN でオンラインになり、異なる SGT（SGT 21（教師）、SGT 22（学生）、および SGT 26（管理者））が割り当てられます。SGT の割り当ては、認証および認可ルールを使用して Cisco ISE を通じてアーカイブするか、接続されたポートまたは IP アドレスプール（Catalyst Center から設定可能）に基づいて静的に割り当てることができます。SGACL ルールは、Cisco ISE から、クライアント管理者が接続されているファブリックエッジにダウンロードされます。

- 伝播：

  同じファブリックサイト内にあるが、異なるファブリックエッジ間、または Cisco SD-Access トランジットを介して接続されている異なるファブリックサイト間では、送信元 SGT は VXLAN ヘッダー内にカプセル化されます。その後、トラフィックはクライアント管理者が接続されているファブリックエッジに転送されます。

- 適用：

  クライアント管理者が接続されているファブリックエッジで発生します。SGACL に基づいて、クライアント教師からのトラフィックは許可されますが、クライアント学生からのトラフィックは拒否されてドロップされます。

クライアントが同じファブリックエッジに接続されている場合、伝播は必要ありません。適用は、このファブリックエッジで直接行われます。

ファブリック ワイヤレス クライアントの場合、認証と認可を使用して、または SSID に静的に割り当てて（Catalyst Center から設定可能）、クライアントが Cisco ISE を介して参加すると、ワイヤレスコントローラは SGT を AP に送信します。AP は、ワイヤレスクライアントから入力ファブリックエッジに VXLAN トンネル経由でデータトラフィックを転送するときに、VXLAN ヘッダーにこの SGT を追加します。出力で、ファブリックエッジポリシーの適用が行われます。同じ VLAN 上の同じ AP に接続されたクライアントの場合、トラフィックフローは常にファブリックエッジでスイッチングされます。AP は、ファブリックエッジに向けられた VXLAN トンネル内にトラフィックをカプセル化します。これにより、同じ AP に戻すトラフィックのスイッチングを処理します。

VXLAN データプレーンはネイティブに SGT を伝送するため、マイクロセグメンテーションは、同じファブリックサイト内または Cisco SD-Access トランジットを使用する複数のファブリックサイト内で直接使用できます。IP ベースのトランジットでは、ファブリックパケットのカプセル化解除により、SGT ポリシー情報が失われる可能性があります。インラインタギングと SXP は、IP トランジットを使用して接続されている 2 つのファブリックサイト間で SGT 情報を伝送できます。

### インラインタギング

インラインタギングは、イーサネットフレームのヘッダーに挿入できる Cisco メタデータ（CMD）と呼ばれる特別なフィールド内で SGT を伝送するプロセスです。これにより、フレームのイーサタイプが 0x8909 に変更されます。ネクストホップデバイスがこのイーサタイプを認識できない場合、フレームは不正な形式と見なされ、廃棄されます。SGT のエンドツーエンドのインラインタギングを伝播する方法は次のとおりです。

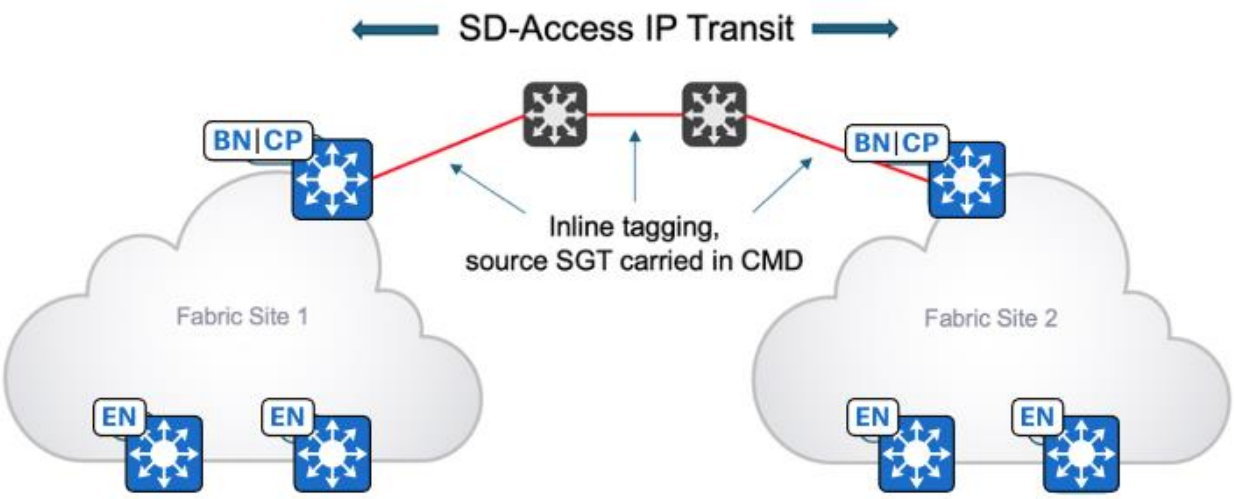
- ホップバイホップ：

  エンドツーエンドチェーン内の各デバイスは、インラインタギングをサポートし、SGT を伝播する必要があります。

- トンネルで保持：

  SGT は Generic Routing Encapsulation（GRE）トンネリングプロトコル内の CMD 内、または IPsec トンネルカプセル化内の CMD 内に保持できます。

**図 16.　　ファブリックサイト間で有効になっているインラインタギング**




インラインタギングの場合、SGT はイーサネットフレームに組み込まれます。イーサネットフレーム内に SGT を埋め込む機能には、特定のハードウェアサポートが必要です。ハードウェアのサポートがないネットワークデバイスは SXP を使用できます。

### TCP を介した SXP

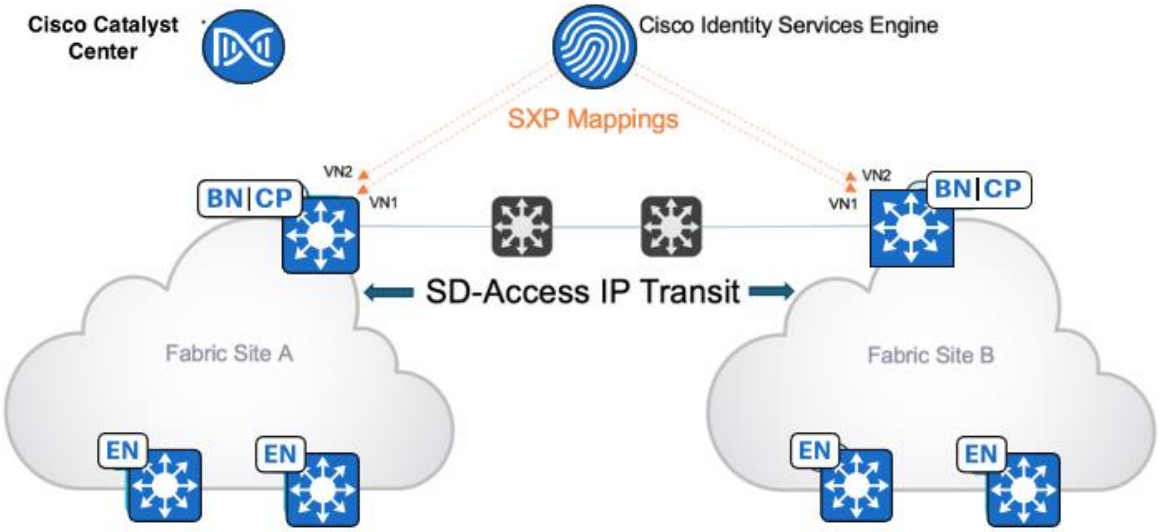
SXP は、データプレーンでの SGT の伝送をサポートしていないインターコネクト ネットワーク全体のボーダーノードに SGT を配布するために使用されます。これにより、ボーダーは着信 IP パケットを再分類し、パケットが

宛先エンドポイントに向かってファブリックエッジに転送されるときに、SGT を VXLAN データプレーンに挿入できます。

ユーザーとエンドポイントが認証され、ネットワークで認可されると、Cisco ISE は認証テーブルを使用して SGT を割り当て、アカウンティングを使用してユーザーとエンドポイントの IP アドレスを学習します。Cisco ISE が他のサイトのデバイスと SXP 接続している場合、Cisco ISE はそのユーザーとエンドポイントの IP-SGT マッピングの関連付けを作成し、別のファブリックサイトに送信します。

たとえば、図 16 に示すように、サイト A から作成されたマッピングは SXP を使用してサイト B に送信されます。このマッピングにより、サイト A からサイト B に流れるトラフィックは、元の送信元 SGT を持つサイト B のボーダーで分類され、VXLAN を介して伝送され、ファブリックエッジで適用されます。

**図 17.　　リモートボーダーへの SXP マッピングの送信**




### インラインタギングと SXP の比較

使用される SGT の伝播方法は、パス内のプラットフォームによって異なります。すべてのデバイスが、インラインタギングに対応しているわけではありません。ただし、デバイスがインラインタギングと SXP の両方をサポートしている場合は、インラインタギングが優先されます。

インラインタギングは、パフォーマンスに影響を与えることなく、データプレーン内で実行されます。SXP は、CPU とメモリのパフォーマンスに影響を与えるコントロールプレーン機能です。

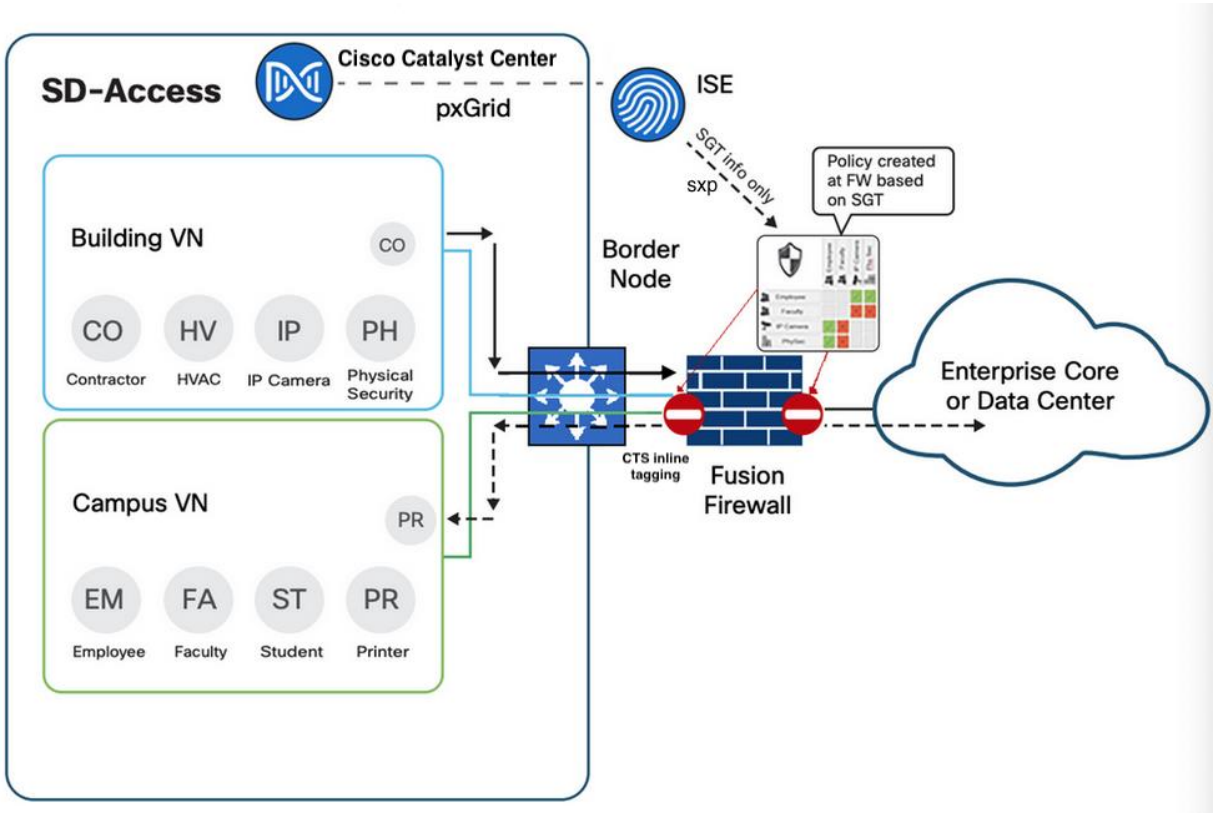
SXP のスケーラビリティも考慮すべき事項です。さまざまなプラットフォームの SXP ピアの数と IP-SGT マッピングの数は、ポリシープラットフォームの機能マトリックスで確認できます。

### ピアデバイスとしてのファイアウォール

ファイアウォールは、従来のネットワークで事前に設定されたセキュリティルールに基づいて、ネットワークの発着信トラフィックを監視および制御するセキュリティ方法として使用されます。信頼できる内部ネットワークとインターネットなどの信頼できない外部ネットワーク間のバリアとして機能します。

ファブリック展開では、ファブリック ボーダー デバイスに接続されたピアデバイスとしてファイアウォールを使用して、共有サービスやインターネットへのアクセスを提供したり、内部ネットワークからゲストネットワークをセグメント化したり、または VN 間通信に使用したりできます。

**図 18.　　Cisco SD-Access の導入における一般的なファイアウォール機能**




### 共有サービス/インターネットへのアクセスの提供

ファイアウォールは、ファブリックボーダーとデータセンターの両方に接続されます。共有サービスプレフィックスは、データセンターからファイアウォールにアドバタイズされます。BGP ピアは、ファブリックボーダー（レイヤ 3 ハンドオフを通じて）とファイアウォール（手動設定）の間で設定され、共有サービスプレフィックスをファイアウォールから各 VN のボーダーにアドバタイズできるようになります（図 17 に示す建物とキャンパス）。これら 2 つの VN のクライアントプレフィックスは、ファイアウォールにアドバタイズされます。ファイアウォールでは、単一の VRF ソリューションまたはマルチ VRF ソリューションを使用できます。マルチ VRF の場合、共有サービスプレフィックスは、グローバルなどの専用 VRF にあります。建物とグローバルの間、およびキャンパスとグローバルの間でルートリークが必要であるため、共有サービスプレフィックスは建物とキャンパスにリークされ、クライアントプレフィックスはグローバルにリークされます。

インターネットアクセスの場合と同様、ファイアウォールは、各 VN（建物とキャンパス）のボーダーにデフォルトルートをアドバタイズします。マルチ VRF ソリューションが使用されている場合、クライアントプレフィックスがグローバルにリークされます。

### VN 間通信

ほとんどの展開では、相互での直接通信を必要とするエンドポイント、ユーザー、またはデバイスは、同じ VN に配置する必要があります。ただし、一部のネットワークには VN 間通信に関する特定の要件がある場合があります。VN 間の要件は、多くの場合、企業の合併時、一部の企業または政府組織、または各機関、テナント、または部門が独自の VN スペースを持つ必要がある同様のマルチテナント環境で見られます。図 17 に示すように、ファイアウォールはキャンパスおよび建物 VN のボーダーデバイスにデフォルトルートをアドバタイズできます。各 VN のクライアントプレフィックスに関する到達可能性情報があるため、キャンパスと建物間のトラフィックをファイアウォールを介してルーティングできます。

**ポリシーの実施**

ファイアウォールはポリシー指向のデバイスであり、トラフィック適用のルールで SGT を使用するように設定できます。この図では、ファイアウォールは Cisco ISE から SXP（SGT Exchange Protocol over TCP）を介して SGT 情報を受信し、インラインタギングを介してボーダーからイーサネット CMD の SGT 情報を持つトラフィックを受信します。ただし、ファブリックデバイスとは異なり、SGT ベースのルールとポリシーは Cisco ISE からダウンロードされません。これらは、ファイアウォールで手動で設定されます。ポリシーの適用により、VN 間通信を特定のクライアント間でのみ制限できます。

図 18 に示すように、ゲストネットワークでは、ファイアウォールを使用して、訪問者の機密性の高いリソースへのアクセスのみを制限することができます。ゲストトラフィックは企業トラフィックから分離され、専用ゲスト VN に配置されます。

**図 19.　ゲストネットワークに展開されたファイアウォール**

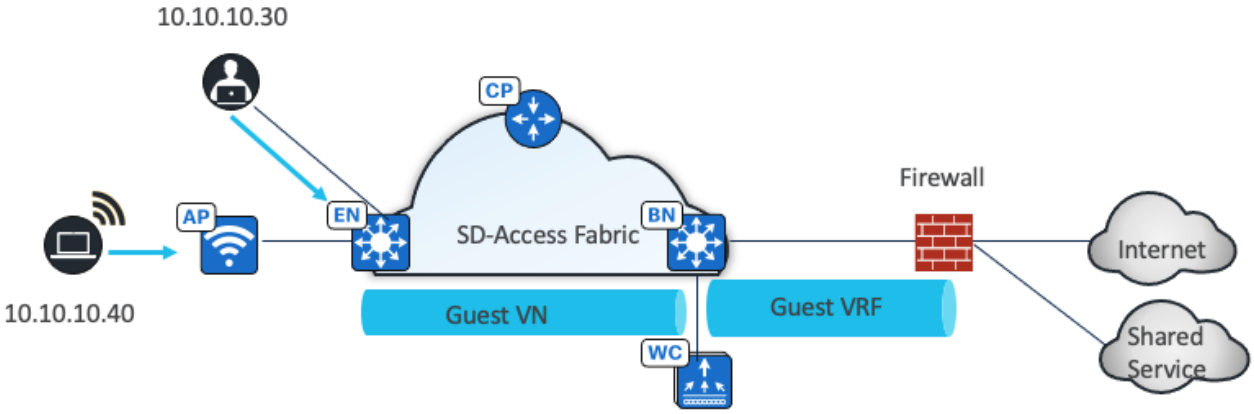
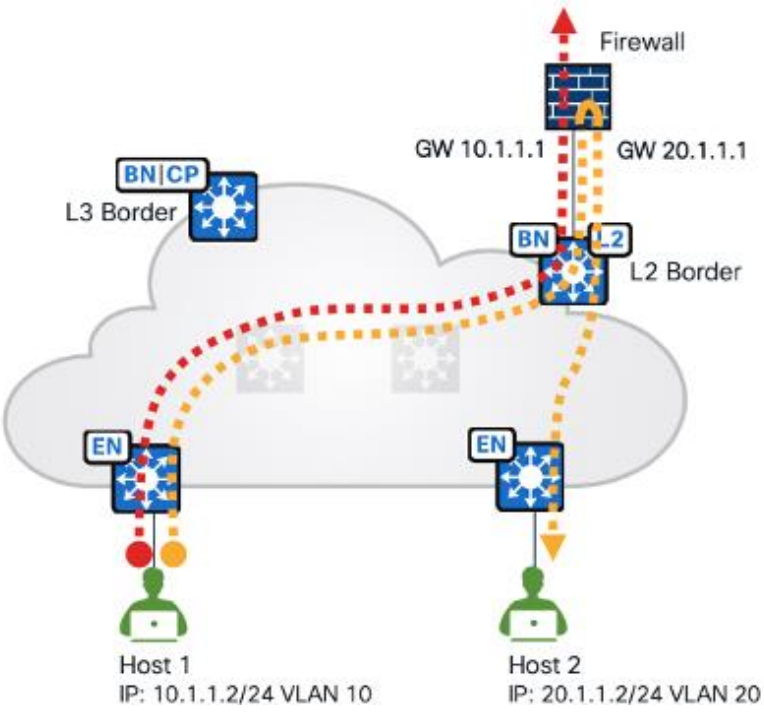



図 19 に示すように、もう 1 つの展開シナリオはレイヤ 2 ボーダーであり、ゲートウェイはファイアウォール上で設定され、ファブリックの外部にあります。ゲートウェイとしてのファイアウォールは、VLAN 間トラフィック、およびファブリックから出るトラフィックを検査できます。

**図 20.　　ファイアウォールのゲートウェイ**




Cisco ASA と Cisco Firepower Threat Defense（FTD）が推奨されます。限定的なサポート（ポリシー、ルーティングなどはサポートされていません）を利用して Catalyst Center で管理でき、Cisco ISE と統合できます。これらは、VN 間通信のステートフルな検査の提供、侵入防御システム（IPS）機能、高度なマルウェア防御（AMP）、詳細な Application Visibility and Control（AVC）、および URL フィルタリングの提供が可能です。また、トラフィックの送信元、宛先、ユーザー名、グループ、およびファイアウォールアクションに関する情報を含む、詳細なレポート機能を備え、許可とドロップのロギングが保証されています。

それらは、クラスタ（単一の論理ユニットとして機能する複数のデバイス）として、HA ペア（通常はアクティブとスタンバイ）として、またはスタンドアロンデバイスとしても展開できます。

サポートされているファイアウォール プラットフォームの完全なリストについては、「Cisco Catalyst Center Compatibility Matrix」を参照してください。

### ファブリックサイトのサイズ：設計戦略

Cisco SD-Access の設計における具体的な目標は、複数のより小さなファブリックサイトではなく、より大きなファブリックサイトを作成することです。設計戦略は、サイトの総数を最小限に抑えながら、ファブリックサイトのサイズを最大化することです。ビジネス要件によっては、ロケーションを複数のサイトに分割する必要があります。たとえば、病院の残りの部分で表されるファブリックサイトとは別の緊急ルーム（ER）用のファブリックサイトを作成する場合などです。

存続可能性、高可用性（HA）、エンドポイントの数、サービス、および地域の多次元の要因はすべて、単一の大規模サイトではなく、複数のより小さなファブリックサイトの要件を満たす要因です。さまざまなサイズのファブリックサイトの設計に役立つように、次のような参照モデルが作成されました。

- 一体型ファブリック（FiaB）サイト

- 小規模サイト
- 中規模サイト
- 大規模サイト
- 超大規模サイト

各ファブリックサイトには、リストされているカテゴリから適切にサイズ設定された、コントロールプレーンノード、エッジノード、ボーダーノード、およびワイヤレスコントローラのサポートセットが含まれます。また、Cisco ISE PSN は、存続可能性の要件を満たすためにサイト全体に分散されます。

### FiaB サイト

FiaB サイトのリファレンスモデルは、200 未満のエンドポイントをターゲットにする必要があります。この設計のセントラルコンポーネントは、コントロールプレーンノード、ボーダーノード、およびエッジノードの 3 つのファブリックロールすべてを担うスイッチスタックまたは StackWise Virtual です。スイッチスタック FiaB 展開では、Catalyst 9000 の Cisco SD-Access EWC を使用してサイトローカル ワイヤレス コントローラ機能を提供します。WAN およびインターネット回線と遅延に応じて、サイトに Cisco ISE PSN が含まれている場合があります。

サイト設計を同様のサイズにするために、表のガイドラインに従ってください。数値はガイドラインとして使用され、このサイトサイズの設計で使用されるデバイスの特定の制限と必ずしも一致するものではありません。

**表 3.** 一体型ファブリックサイト参照モデルのガイドライン

| コンポーネント | 番号 |
|---|---|
| エンドポイント、ターゲットの上限 | 200 |
| 仮想ネットワーク、ターゲットの上限 | 5 |
| IP プール、ターゲットの上限 | 8 |
| AP、ターゲットの上限 | 40 |

この設計の HA は、スイッチスタックまたは StackWise Virtual を通じて提供されます。両方とも、複数の物理スイッチを 1 つの論理スイッチに結合します。StackPower は、スイッチスタックのメンバー間に電源の冗長性を提供するために使用されます。StackWise Virtual の導入では、各スイッチでデュアル電源を使用することにより、電源の冗長性を確保しています。シャーシベースのスイッチを使用する場合、HA は冗長スーパーバイザと冗長電源によって提供されます。電源の冗長性をサポートするには、電源、シャーシ、スーパーバイザ、およびラインカードをサポートするスイッチの要件を超えた冗長性の電源が必要です。

**技術的なヒント：** クライアント SSO は、アクティブコントローラからスタンバイコントローラへのクライアントのシームレスな移行を提供します。クライアント情報はアクティブからスタンバイに同期され、スイッチオーバーイベント中のクライアントの再アソシエーションを回避します。

ワイヤレスコントローラは、一体型ファブリックに直接接続された物理ユニットとして展開することも、組み込み Catalyst 9800 コントローラとして展開することもできます。スイッチスタックまたは冗長スーパーバイザを備えた組み込み Catalyst 9800 を使用すると、AP とクライアント SSO が自動的に提供されます。一体型ファブリックの StackWise Virtual 展開には、物理ワイヤレスコントローラが必要です。

スタックを使用する場合、アップストリーム ルーティング インフラストラクチャへのリンクは、さまざまなスタックメンバーからのものである必要があります。理想的には、アップリンクはアクティブスタックからではなく、メンバースイッチから取得する必要があります。シャーシスイッチでは、リンクは異なるスーパーバイザを介して接続する必要があります。最初の IP 到達可能性を確保するとともにボーダーノードハンドオフの自動化を準備するために、SVI とトランクリンクは通常、小規模なサイトスイッチとアップストリーム ルーティング インフラストラクチャの間に展開されます。

### 小規模サイト

小規模サイト参照モデルがサポートするエンドポイントは、2,000 未満です。物理ネットワークは通常、複数の配線用ボックスにサービスを提供するアクセスレイヤと、2 層のコラプストコアまたはディストリビューション レイヤです。小規模サイトのモデルでは、すべてのロールを 1 つのデバイスにコロケーションさせずに、アクセスレイヤの専用デバイスにエッジノードロールを分離することで、より多くのエンドポイントを使用しながらレジリエンスと冗長性を強化できます。ボーダーノードとコントロールプレーンノードは、コラプストコアレイヤでコロケーションしています。Cisco SD-Access ワイヤレスでは、組み込み型ワイヤレスコントローラが、共存ボーダーおよびコントロールプレーンノードの 1 つでプロビジョニングされます。必要に応じて、仮想またはハードウェアベースのワイヤレスコントローラが使用されます。200 未満の AP と 4,000 未満のクライアントがある場合は、Cisco SD-Access 組み込み型ワイヤレスを、コラプストコアスイッチ上の共存ボーダーノードおよびコントロールプレーンノードの機能とともに展開できます。ワイヤレス HA には、ハードウェアまたは仮想ワイヤレスコントローラを使用します。

サイト設計を同様のサイズにするために、表のガイドラインに従ってください。数値はガイドラインとして使用され、このサイトサイズの設計で使用されるデバイスの特定の制限と必ずしも一致するものではありません。

**表 4.** 小規模サイト参照モデルのガイドライン

| コンポーネント | 番号 |
|---|---|
| エンドポイント、ターゲットの上限 | 2,000 |
| 仮想ネットワーク、ターゲットの上限 | 8 |
| IP プール、ターゲットの上限 | 20 |
| AP、ターゲットの上限 | 100 |
| コントロールプレーンノード、コロケーション | 2 |
| ボーダーノード、コロケーション | 2 |
| ファブリックノード、ターゲットの上限 | 50 |

### 中規模サイト

中規模サイト参照モデルは、コアおよびディストリビューション レイヤとアクセスレイヤを組み合わせた 2 層ネットワーク構造を使用して、複数の配線用ボックスがある建物向けに設計されています。

中規模サイトは、25,000 未満のエンドポイントと 2,000 未満の AP をサポートします。ボーダーノード機能は、1 つまたは 2 つのデバイスでコントロールプレーンノード機能とコロケーションします。理想的には、HA 設定では、復元力の高い単一のデバイスと個別のワイヤレスコントローラを展開します。

サイト設計を同様のサイズにするために、表のガイドラインに従ってください。数値はガイドラインとして使用され、このサイトサイズの設計で使用されるデバイスの特定の制限と必ずしも一致するものではありません。

**表 5.** 中規模サイト参照モデルのガイドライン

| コンポーネント | 番号 |
|---|---|
| エンドポイント、ターゲットの上限 | 25,000 |
| 仮想ネットワーク、ターゲットの上限 | 50 |
| IP プール、ターゲットの上限 | 200 |
| AP、ターゲットの上限 | 2,000 |
| コントロールプレーンノード、コロケーション | 2 |
| ボーダーノード、コロケーション | 2 |
| ファブリックノード、ターゲットの上限 | 450 |

### 大規模サイト

大規模サイトの参照モデルは、複数の建物、または複数の配線用ボックスがある単一の建物向けに設計されています。物理ネットワークは、通常、コア、ディストリビューション、およびアクセスレイヤの 3 層です。多くの建物を集約し、WAN とインターネットへのネットワーク出力ポイントとして機能する、ルーテッドスーパーコアを備えている場合もあります。ボーダーノードとコントロールプレーンノードは、コロケーションせずに、個別のデバイスでプロビジョニングされます。

大規模なサイトでは、最大 100,000 のエンドポイントと 6,000 の AP がサポートされます。ボーダーは、コントロールプレーン機能からの冗長デバイスと、HA 設定の個別のワイヤレスコントローラを使用して分散されます。

サイト設計を同様のサイズにするために、次の表を使用してガイドラインを理解してください。数値はガイドラインとしてのみ使用され、このサイトサイズの設計で使用されるデバイスの特定の制限は必ずしも一致しません。

**表 6.** 大規模サイト参照モデルのガイドライン

| コンポーネント | 番号 |
|---|---|
| エンドポイント、ターゲットの上限 | 100,000 |
| 仮想ネットワーク、ターゲットの上限 | 64 |
| IP プール、ターゲットの上限 | 450 |
| AP、ターゲットの上限 | 6,000 |
| コントロール プレーン ノード数 | 2 ～ 4 |
| ボーダーノード（内部として 2 つ、外部として 2 つ） | 2 ～ 4 |
| ファブリックノード、ターゲットの上限 | 750 |

### 超大規模サイト

超大規模サイト参照モデルは、複数の配線用ボックスがある建物、または大規模キャンパスにまたがる複数の施設がある建物向けに設計されています。物理ネットワークは、コア、ディストリビューション、およびアクセスレイヤからなる 3 層ネットワークです。4 層のスーパーコアを持つ場合もあります。超大規模ネットワークでは、専用のデータセンター、共有サービスブロック、インターネットサービスなど、専用のサービスイグジットポイントが必要です。

超大規模サイトでは、最大 200,000 のエンドポイントと 10,000 の AP がサポートされます。複数のボーダーノードが、冗長デバイス上のコントロールプレーンノード機能と、HA 設定の個別のワイヤレスコントローラから分散されます。

## エコシステム

Catalyst Center には、さまざまなパラレルソリューションとサードパーティ製アプリケーションによるエコシステムがあります。このセクションでは、Cisco SD-Access のコンテキストで、これらのエコシステムソリューションについて説明します。

### Wide Area Bonjour

Bonjour は、ネットワーク設定をシンプルにする設定不要のソリューションであり、接続デバイス、サービス、およびアプリケーション間の通信を確立します。Bonjour は、小規模でフラットなネットワークなどの単一のレイヤ 2 ドメイン用に設計されています。

Catalyst Center の Cisco Wide Area Bonjour アプリケーションは、単一のレイヤ 2 ドメインの制約を排除し、Cisco SD-Access の有線およびワイヤレスネットワークで使用される、より大きなレイヤ 3 ドメインに範囲を拡大します。

### ThousandEyes

ThousandEyes アプリケーションは Catalyst 9000 シリーズ スイッチでホストされ、Catalyst Center のワークフローを通じてプロビジョニングされます。ThousandEyes は、ネットワーク内のデバイスとアプリケーションを監視および観察するための方法を提供します。

ファブリックエッジノードの ThousandEyes エージェントは、クライアントサブネットからサービスまで、ネットワークとアプリケーションの可視性を提供します。また、ボーダーノードからファブリックサイト外のサービスに、ネットワークとアプリケーションの可視性を提供します。

### Cisco AI Endpoint Analytics

Cisco AI エンドポイント分析は、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプに基づいて、エンドポイントおよび IoT デバイスを検出して、さまざまなカテゴリに分類するソリューションです。Cisco AI エンドポイント分析エンジンとユーザーインターフェイスは Catalyst Center 上で実行され、ネットワーク インフラストラクチャからテレメトリを受信することでエンドポイントにラベルを割り当てます。

### 返品許可（RMA）のワークフロー

Catalyst Center 返品許可（RMA）のワークフローにより、デバイスの交換はゼロタッチプロセスになります。お客様が、Catalyst Center で障害が発生したデバイスにフラグを立てます。新しいデバイスを物理的に設置し、基本的なゼロタッチワークフローを実行して、PnP プロセスでデバイスを起動します。このプロセスを使用して、Catalyst Center はソフトウェアイメージのアップグレードを自動化し、適切なライセンスと証明書をインストールして、基本設定を適用します。デバイスが Catalyst Center によって検出されると、古いデバイスの設定で交換用デバイスが設定されます。Catalyst Center は、ファブリックデバイスと非ファブリックデバイスの両方の RMA をサポートしています。

RMA ワークフローは、Day-*N* の運用 - RMA のセクションで説明されています。

### ファブリックアシュアランス

Cisco SD-Access アシュアランスは、アンダーレイとオーバーレイを可視化し、ファブリック インフラストラクチャの重要なネットワークサービスへの到達可能性を実現します。ファブリック ネットワーク デバイスは、特定の

プロトコル状態のステータスを監視するモデル駆動型のストリーミングテレメトリでプロビジョニングされます。プロトコル状態の変更は、ネットワークデバイスによって Catalyst Center に報告されます。アシュアランス ダッシュボードの推奨アクションは、ネットワークオペレータが問題のドメインを絞り込み、最終的に問題を修正するのに役立ちます。

Cisco SD-Access アシュアランスは、ファブリックサイト、仮想ネットワーク、および Cisco SD-Access トランジットの正常性と状態を可視化します。

ファブリックアシュアランスについては、「Cisco SD-Access ネットワークと Cisco SD-Access アプリケーションの監視」 セクションで説明しています。

## サードパーティ統合

### IP アドレス管理システム

サードパーティの IP アドレス管理（IPAM）システムの統合により、DNS や DHCP など、IPAM のすべての側面は 1 つの統合プラットフォームを使用して実行できます。この統合により、手作業のプロセスやパッチワークツールが不要になり、IP アドレス管理の効率が向上します。Catalyst Center は、サードパーティ IPAM システム Infoblox と BlueCat の統合機能をサポートしています。

### ServiceNow

Cisco SD-Access と ServiceNow の統合により、すべてのファブリック プロビジョニング イベントが監視および公開されます。これにより、IT サービス管理システムにセキュリティおよびその他の操作トリガーが提供されます。

## 遅延とスケール

ネットワークでの遅延は、パフォーマンス上の重要な考慮事項であり、Catalyst Center とそこで管理するネットワークデバイスとの間のラウンドトリップ時間（RTT）について、厳密に考慮する必要があります。Cisco SD-Access を含む Catalyst Center が提供するすべてのソリューションで最適なパフォーマンスを実現するには、RTT を 100 ミリ秒以下にする必要があります。最大遅延は 200 ミリ秒 RTT です。100 ミリ秒から 200 ミリ秒の遅延に対応していますが、インベントリ収集、ファブリック プロビジョニング、管理対象デバイスとの連携を伴うその他のプロセスなど、特定の機能では実行時間が長くなる可能性があります。

**図 21.　Catalyst Center とネットワーク要素間の RTT 要件**

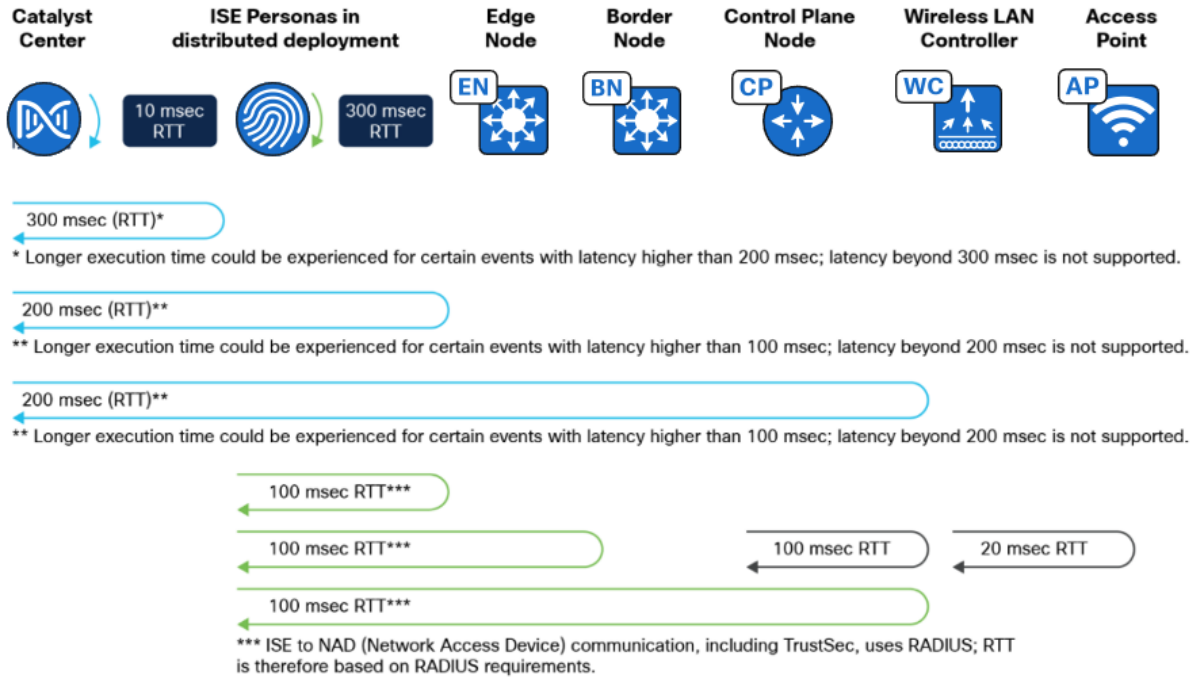



**表 7.**　Cisco SD-Access の導入でシスコが推奨する RTT

| 送信元デバイス | ターゲットデバイス | サポートされる最大ラウンドトリップ時間 |
|---|---|---|
| Catalyst Center ノード | FE/ワイヤレスコントローラ/ボーダー/コントロールプレーン | 200 ミリ秒 |
| Catalyst Center ノード | Cisco ISE | 300 ミリ秒 |
| Cisco ISE | FE/ワイヤレスコントローラ/ボーダー/コントロールプレーン | 100 ミリ秒 |
| ワイヤレスコントローラ | AP | 20 ミリ秒 |
| ワイヤレスコントローラ | コントロールプレーンノード | 100 ミリ秒 |

表 8 から表 12 に、一般的に使用されているデバイスファミリと Catalyst Center のさまざまなファブリックロールでサポートされるエンドポイント、AP、VN などのスケール数を示します。デバイスファミリの詳細と完全なリストについては、Catalyst Center データシートを参照してください。

**表 8.**　ファブリックエッジノードの Cisco SD-Access スケール数

| デバイスファミリ | 仮想ネットワーク | 有線エンドポイント | 直接接続された AP |
|---|---|---|---|
| 9200-L | 1 | 2,000 | サポート対象外 |
| 9200 | 4 | 4,000 | 25 |
| 9300/L | 256 | 6,000 | 50 |
| 9300 | 256 | 6,000 | 200 |
| 9400 | 256 | 6,000 | 200 |
| 9500/H | 256 | 6,000 | 200 |

**表 9.**　ファブリックボーダーノードの Cisco SD-Access スケール数

| デバイスファミリ | 仮想ネットワーク | ファブリックホストエントリ（/32 または /128） |
|---|---|---|
| 9300/L | 256 | 16,000 |
| 9400 | 256 | 70,000 |
| 9500 | 256 | 70,000 |
| 9500-H | 256 | 150,000 |
| 9600 | 256 | 150,000 |
| ASR1K、4K、ISR（8 GB RAM） | 128 | 1,000,000 |
| ASR1K、4K、ISR（16 GB RAM） | 128 | 4,000,000 |

**表 10.** ワイヤレス コントローラ モデルの Cisco SD-Access スケール数

| ワイヤレス コントローラ モデル | AP の最大数 | クライアントの最大数 |
|---|---|---|
| Catalyst 9800-L | 250 | 5,000 |
| Catalyst 9800-40 | 2,000 | 32,000 |
| Catalyst 9800-80 | 6,000 | 64,000 |
| Catalyst 9800-CL（4 CPU/8 GB RAM） | 1,000 | 10,000 |
| Catalyst 9800-CL（6 CPU/16 GB RAM） | 3,000 | 32,000 |
| Catalyst 9800-CL（10 CPU/32 GB RAM） | 6,000 | 64,000 |
| Catalyst 9000 の組み込みワイヤレスコントローラ（9300L） | 50 | 1,000 |
| Catalyst 9000 の組み込みワイヤレスコントローラ（9300、9400、9500、9500H） | 200 | 4,000 |

**表 11.** Catalyst Center Cisco SD-Access システムのスケール

| SKU | DN-SW-APL（仮想アプライアンス） | DN3-HW-APL（C220 M5 44 コア）<br>DN3-HW-APL（C220 M6 32 コア） | DN3-HW-APL-L（C220 M6 56 コア）<br>DN3-HW-APL-L（C220 M6 56 コア） | DN2-HW-APL-XL（C480 M5 112 コア）<br>DN3-HW-APL-XL（C480 M6 80 コア） |
|---|---|---|---|---|
| デバイス（スイッチ、ルータ、WLC）（ファブリック） | 2000 | 2000 | 4000 | 8000 |
| ワイヤレスアクセスポイント（ファブリック） | 3000 | 3000 | 4000 | 10000 |
| 同時エンドポイント | 25,000 | 25,000 | 40,000 | 100,000 |
| 一時エンドポイント（14 日間以上） | 75,000 | 75,000 | 120,000 | 250,000 |
| エンドポイントの比率： | | | | |
| 有線 | 任意 | 任意 | 任意 | 任意 |
| ワイヤレス | 任意 | 任意 | 任意 | 任意 |
| ファブリックサイト | 500 | 500 | 1000 | 2000 |
| 拡張可能グループ数 | 4000 | 4000 | 4000 | 4000 |
| グローバル IP プール | 100 | 100 | 100 | 200 |
| サイトあたりのレイヤ 3 VN | 64 | 64 | 128 | 256 |
| サイトあたりのレイヤ 2 VN | 200 (1) | 200 (1) | 600 (2) | 1000 (3) |

| SKU | DN-SW-APL（仮想アプライアンス） | DN3-HW-APL（C220 M5 44 コア）<br><br>DN3-HW-APL（C220 M6 32 コア） | DN3-HW-APL-L（C220 M6 56 コア）<br><br>DN3-HW-APL-L（C220 M6 56 コア） | DN2-HW-APL-XL（C480 M5 112 コア）<br><br>DN3-HW-APL-XL（C480 M6 80 コア） |
|---|---|---|---|---|
| サイトあたりの IP プール | 100 (1) | 100 (1) | 300 (2) | 1000 (3) |
| サイトあたりのファブリックデバイス | 500 | 500 | 600 | 1200 |

**注：**

(1) IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 200 以下である必要があります。

(2) IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 300 以下である必要があります。

(3) IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 1000 以下である必要があります。

**表 12.** 3 ノード DN3-HW-APL-XL クラスタのスケール

| 説明 | サポートされるスケール |
|---|---|
| デバイス（スイッチ、ルータ、ワイヤレスコントローラ） | 10,000 |
| ワイヤレス アクセス ポイント | 25,000 |
| 同時エンドポイント | 300,000 |
| 一時エンドポイント（14 日間以上） | 750,000 |

## Cisco SD-Access ネットワークの設計

このセクションでは、Catalyst Center を使用して Cisco SD-Access ネットワークを設計するプロセスと手順について説明します。

Cisco SD-Access ネットワークの設計プロセスは次のとおりです。

- Cisco ISE を Catalyst Center と統合します（マイクロセグメンテーションに必要）。
- サイト階層を設定します。
- Cisco SD-Access ネットワークの運用に必要なネットワークサービスを設定します。
- IP プールを設定します。
- WLAN 展開用のワイヤレス設定を構成します（ファブリック ワイヤレス ネットワークに必要）。

Catalyst Center をインストールするプロセスと手順については、Catalyst Center のインストールガイドを参照してください。

Cisco ISE をインストールするプロセスと手順については、Cisco ISE のインストールガイドを参照してください。

### Cisco ISE と Catalyst Center の統合

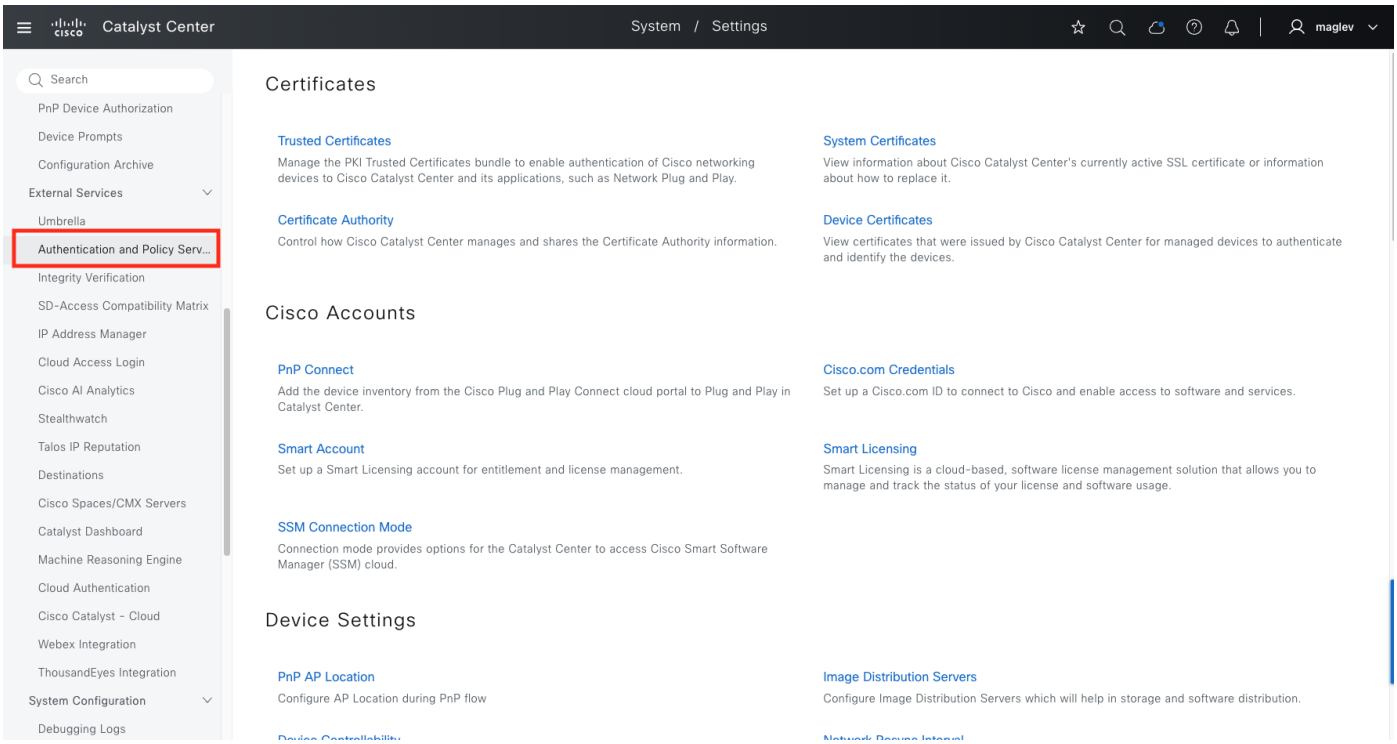
Cisco ISE と Catalyst Center を統合することで、2 つのプラットフォーム間で、デバイスやグループなどの情報を共有できます。これは、マイクロセグメンテーション ソリューションでは必須ですが、マクロセグメンテーション ソリューションではオプションです。

Cisco ISE を Catalyst Center と統合するための手順には、次のものが含まれます。

- 認証およびポリシーサーバーとして Cisco ISE を Catalyst Center に設定します。
- Catalyst Center から Cisco ISE への pxGrid 接続を許可します。

## 手順 1。　認証およびポリシーサーバーとしての Cisco ISE の設定

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [System] > [Settings] を選択し、左側のパネルで [External Services] > [Authentication and Policy Servers] を選択します。




**ステップ 2.** [Add] をクリックし、ドロップダウンメニューから [ISE] を選択します。

**ステップ 3.** [Add ISE server] ペインに情報を入力します。

表 13 に、[Add ISE server] ペイン内のフィールドの説明を示します。

**表 13.**　[Add AAA with ISE server] ペインのフィールド

| フィールド | 設定 | 説明 |
|---|---|---|
| Server IP Address | テキスト フィールド | Cisco ISE サーバーの IP アドレス（複数の IP アドレスが設定されている場合は、この IP アドレスが Cisco ISE 展開インスタンスに表示されていることを確認します）。 |
| Shared Secret | テキスト フィールド | Cisco ISE サーバーと通信するためにネットワークデバイスで使用されます。IOS XE デバイス設定内では PAC キーとも呼ばれます。 |
| Username | テキスト フィールド | Cisco ISE のインストール時に作成したデフォルトのネットワーク管理者アカウントのユーザー名です。 |
| Password | テキスト フィールド | Cisco ISE のインストール時に作成したデフォルトのネットワーク管理者アカウントのパスワードです。 |
| FQDN | テキスト フィールド | Cisco ISE サーバーの完全修飾ドメイン名です。 |
| Virtual IP Address | テキスト フィールド | 1 つのロードバランサの背後に 1 つ以上の PSN を持つことができます。その場合、[Virtual IP] フィールドにロードバランサの IP を追加できます。 |

| フィールド | 設定 | 説明 |
|---|---|---|
| [Advanced Settings] > [Protocol] | [Multiple Choice] オプションボタン | 使用する認証プロトコルを決定します。次の選択肢があります。<br>[RADIUS]：デフォルト設定です。RADIUS プロトコルを使用します。<br>[TACACS]：TACACS プロトコルを使用します。 |
| [Advanced Settings] > [Authentication Port] | テキストフィールド | [RADIUS] を選択した場合、デフォルトポートには 1812 を使用します。 |
| [Advanced Settings] > [Accounting Port] | テキストフィールド | [RADIUS] を選択した場合、デフォルトポートには 1813 を使用します。 |
| [Advanced Settings] > [Port] | テキストフィールド | このフィールドは、[TACACS] が選択されている場合にのみ表示されます。デフォルトポートは 49 です。 |
| Retries | 番号 | 失敗までの認証再試行の回数です。デフォルトは 3 です。 |
| Timeout (seconds) | 番号 | 試行がタイムアウトするまでの秒数です。デフォルトは 4 秒です。 |

この設計および導入ガイドでは、表 14 の情報が入力されています。

**表 14.** [Add AAA with ISE server] ペインのフィールド

| フィールド | 値 |
|---|---|
| Server IP Address | 10.195.221.144 |
| Shared Secret | **** |
| Cisco ISE Server | On |
| Username | Admin |
| Password | **** |
| FQDN | FANIU-ISE-V3.cisco.cpm |
| Subscriber Name | Admin |
| SSH Key | なし（空） |
| Virtual IP Address | なし（空） |
| [Advanced Settings] > [Protocol] | RADIUS |
| [Advanced Settings] > [Authentication Port] | 1812 |
| [Advanced Settings] > [Accounting Port] | 1813 |
| Retries | 3 |
| Timeout (seconds) | 4 |

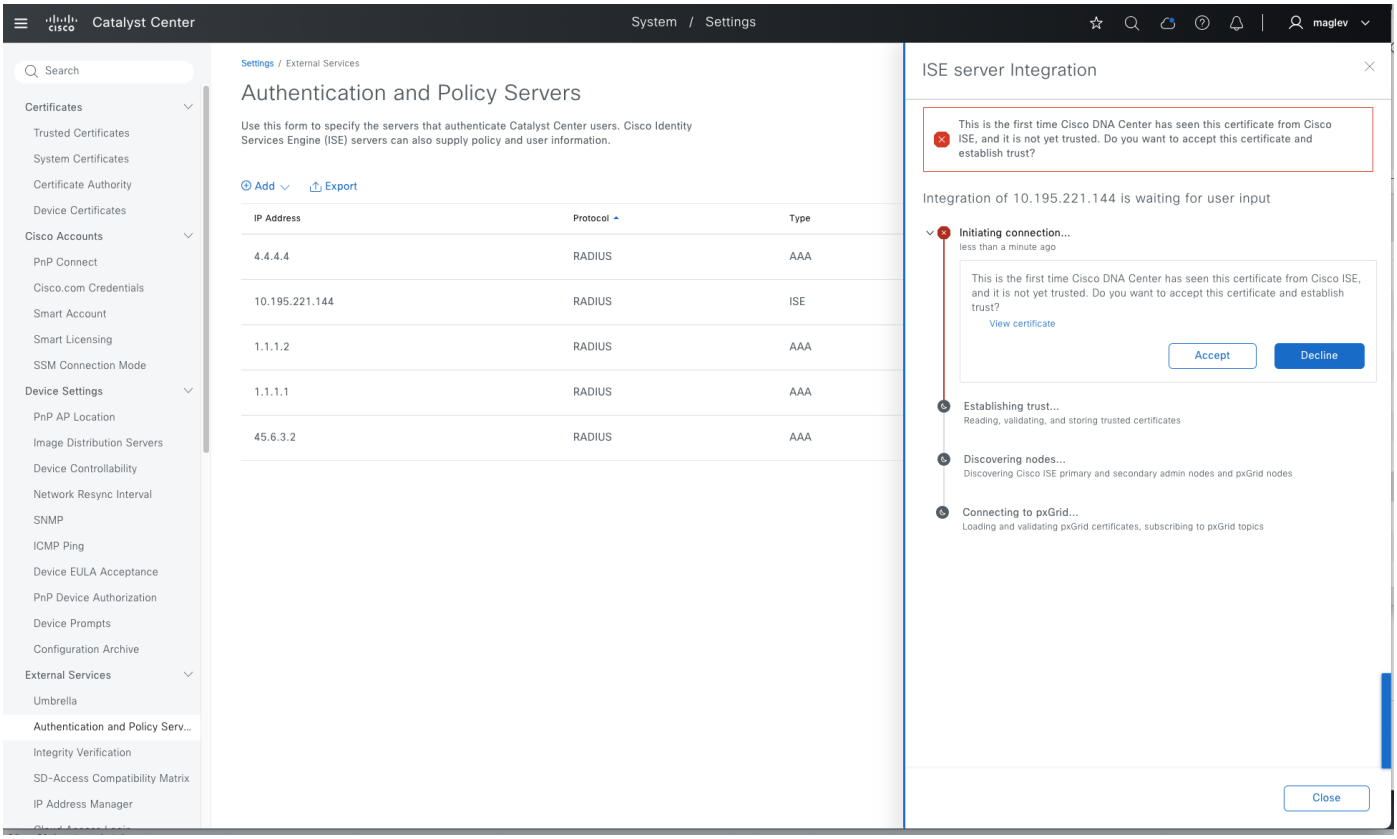
Cisco ISE を追加する前に、次の前提条件を満たしていることを確認します。

- Cisco ISE と Catalyst Center に互換性のあるバージョンがある（「Cisco Catalyst Center Compatibility Matrix」を参照）。
- Cisco ISE GUI パスワードが Cisco ISE CLI パスワードと一致する（この制限は Catalyst Center 2.3.7.6 以降のリリースでは削除されています）。
- Cisco ISE 展開インスタンスに対して pxGrid が有効になっている。
- Cisco ISE では、ERS が [Read/Write Enabled] になっている。

**ステップ 4.** [Add] をクリックして、Catalyst Center 内に Cisco ISE サーバーを作成します。

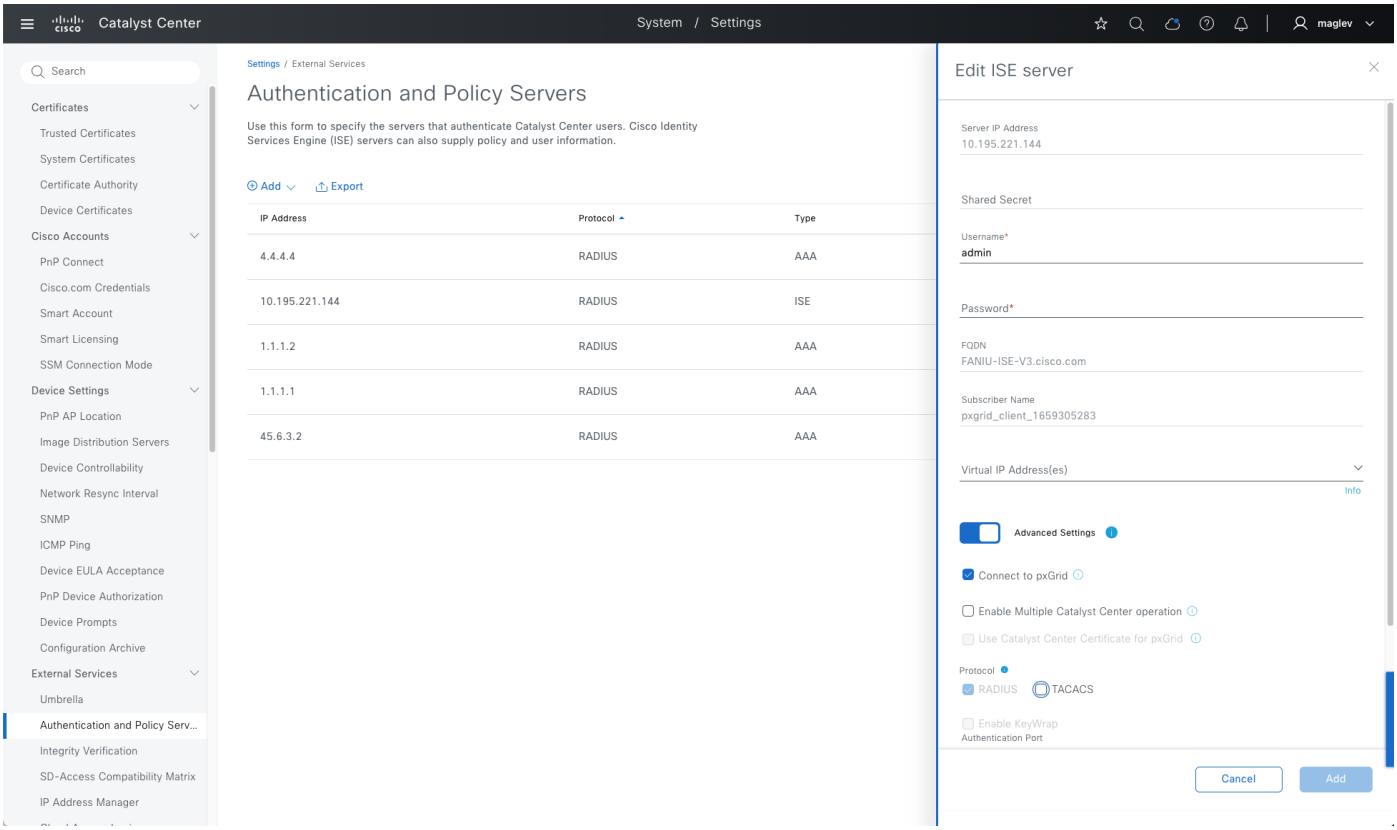
**ステップ 5.** 信頼できる Cisco ISE の証明書がサイドバーに表示されたら、[Accept] をクリックします。

**図 22.　　初めて信頼できる Cisco ISE 証明書が表示されているサイドパネル**




統合が終了したら、[Authentication and Policy Servers] ダッシュボードに戻ります。新しい Cisco ISE サーバーの [Status] が [Active] で表示されます。設定を変更または修正する必要がある場合は、それを選択して [Edit] をクリックします。

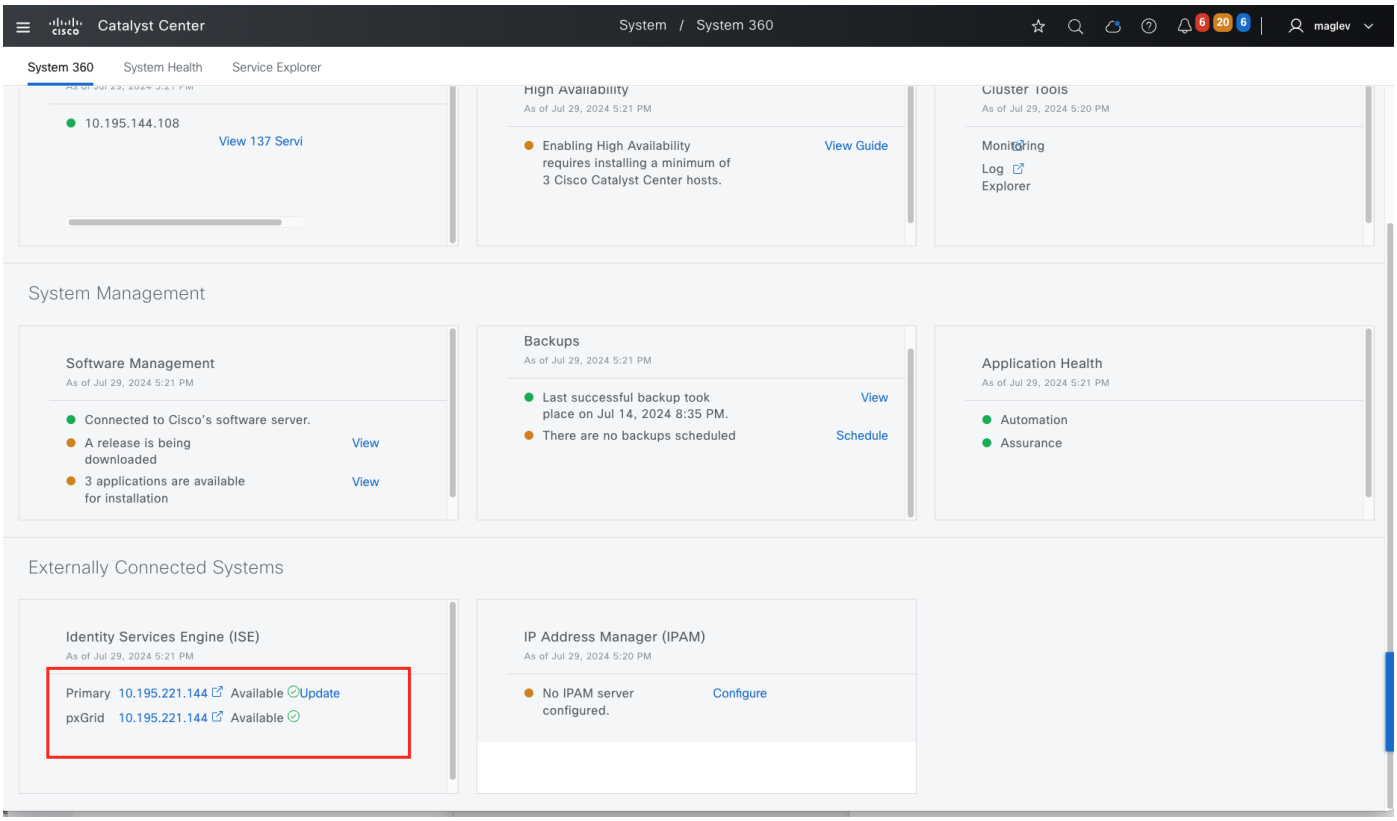
**図 23.　　既存の ISE サーバーの編集**



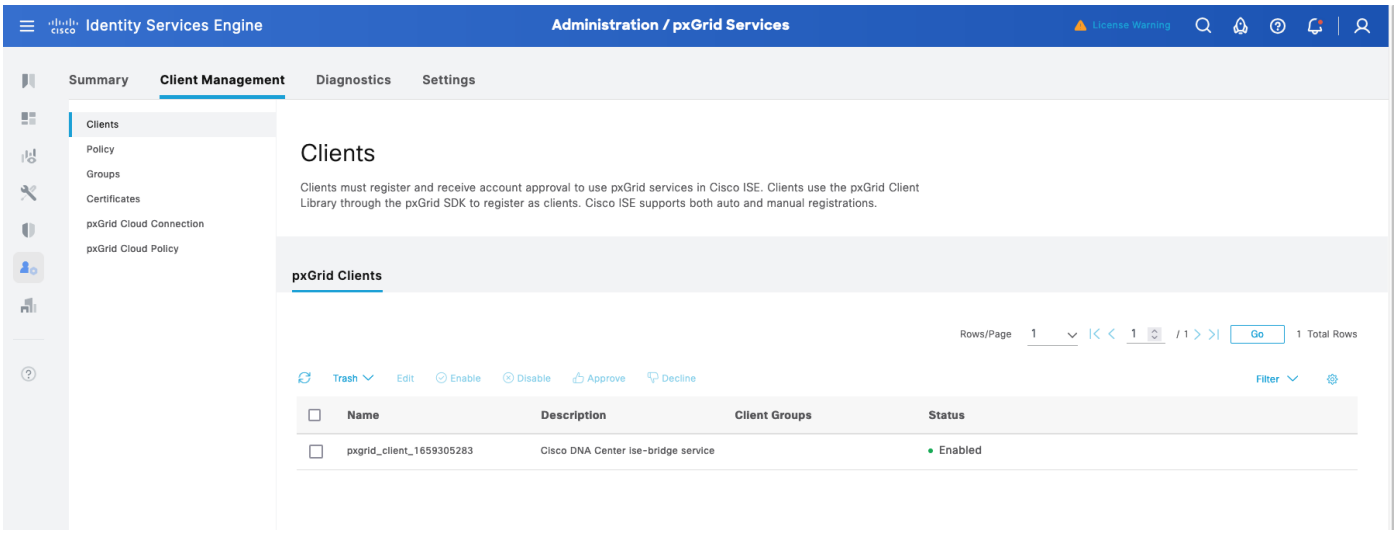

Catalyst Center が Cisco ISE と統合されていることを確認するには、Catalyst Center 内で次の手順を実行します。

**ステップ 6.** 左上隅にあるメニューアイコンをクリックして [System] > [System 360] の順に選択し、[Externally Connected Systems] > [Identity Services Engine (ISE)] セクションまでスクロールします。

[Primary] と [pxGrid] の両方が [Available] と表示されている必要があります。




**ステップ 7.** Cisco ISE で、左上隅にあるメニューアイコンをクリックして [Administration] > [pxGrid Services] の順に選択し、[Client Management] タブをクリックします。Cisco Catalyst セッションでの pxGrid セッションが作成され、[Status] が [Enabled] と表示されていることを確認します。

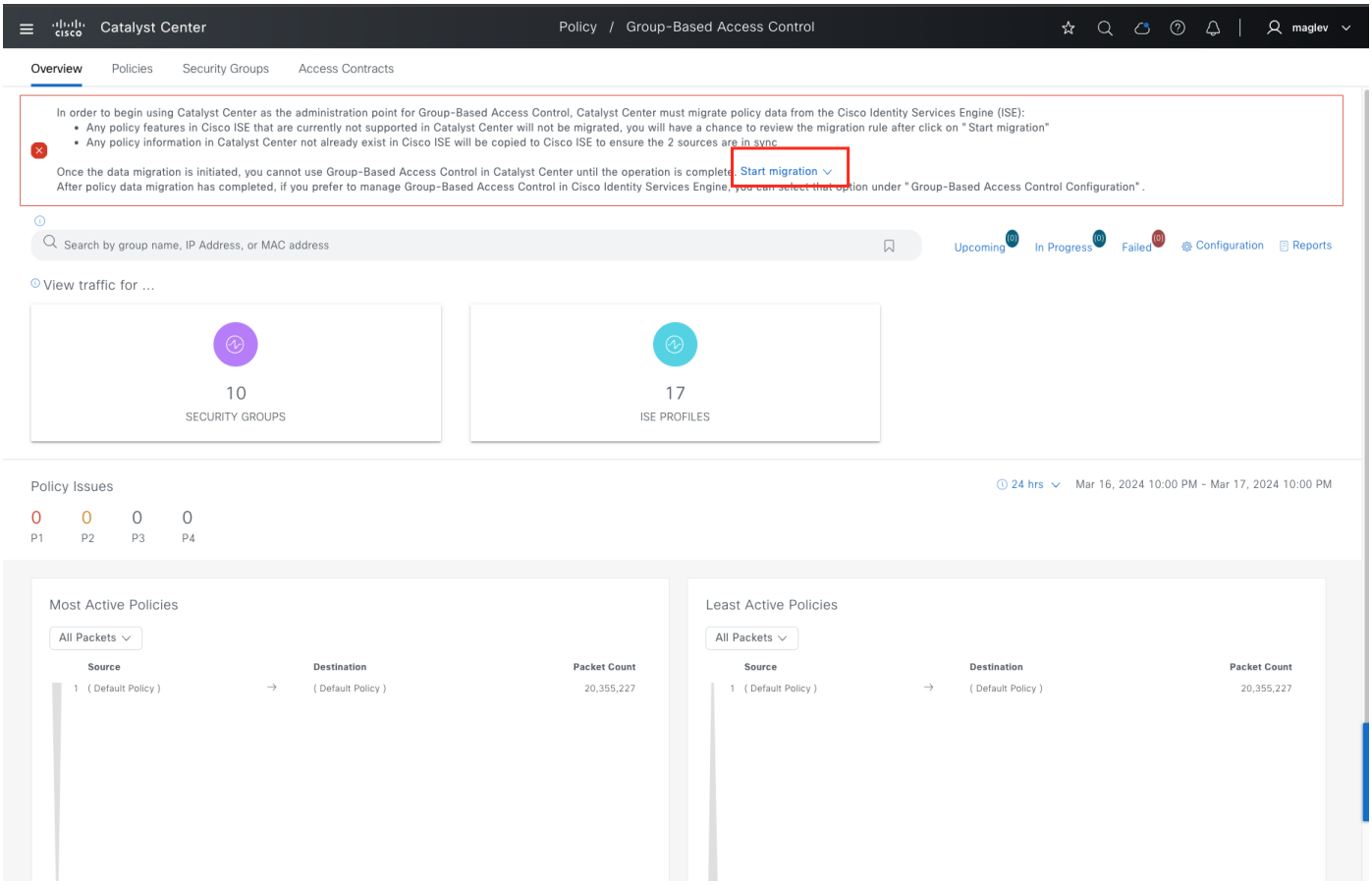


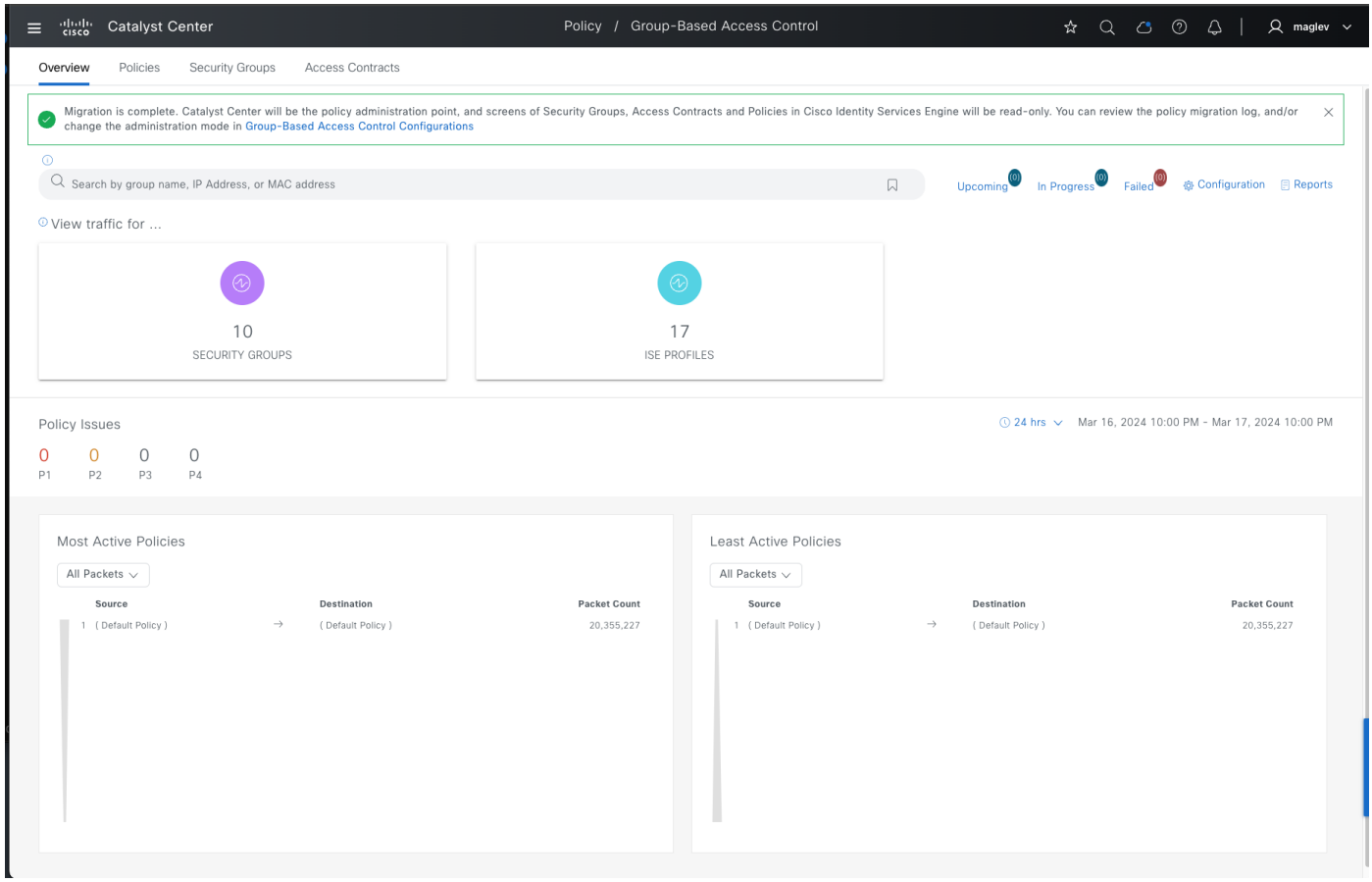
## 手順 2。 Catalyst Center ポリシーウィンドウでの統合

Catalyst Center を GBAC の管理者として使用するには、Catalyst Center はポリシーデータを ISE から移行する必要があります。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Policy] > [Group-Based Access Control] の順に選択します。

**ステップ 2.** バナーから [Start migration] をクリックします。移行は、後でスケジュールすることも、すぐに開始することもできます。データスケールによっては最大 1 時間かかることがあります。






**注：**
Catalyst Center で現在サポートされていない Cisco ISE のポリシー機能は移行されません。ネットワーク管理では、[Start migration] をクリックした後に、移行ルールを確認できます。

Cisco ISE にまだ存在しない Catalyst Center のポリシー情報はすべて Cisco ISE にコピーされ、2 つのソースが確実に同期されます。

アップグレード後、同じ場所に移動します。Catalyst Center と Cisco ISE を確実に同期させるには、移行を再度行う必要があります。

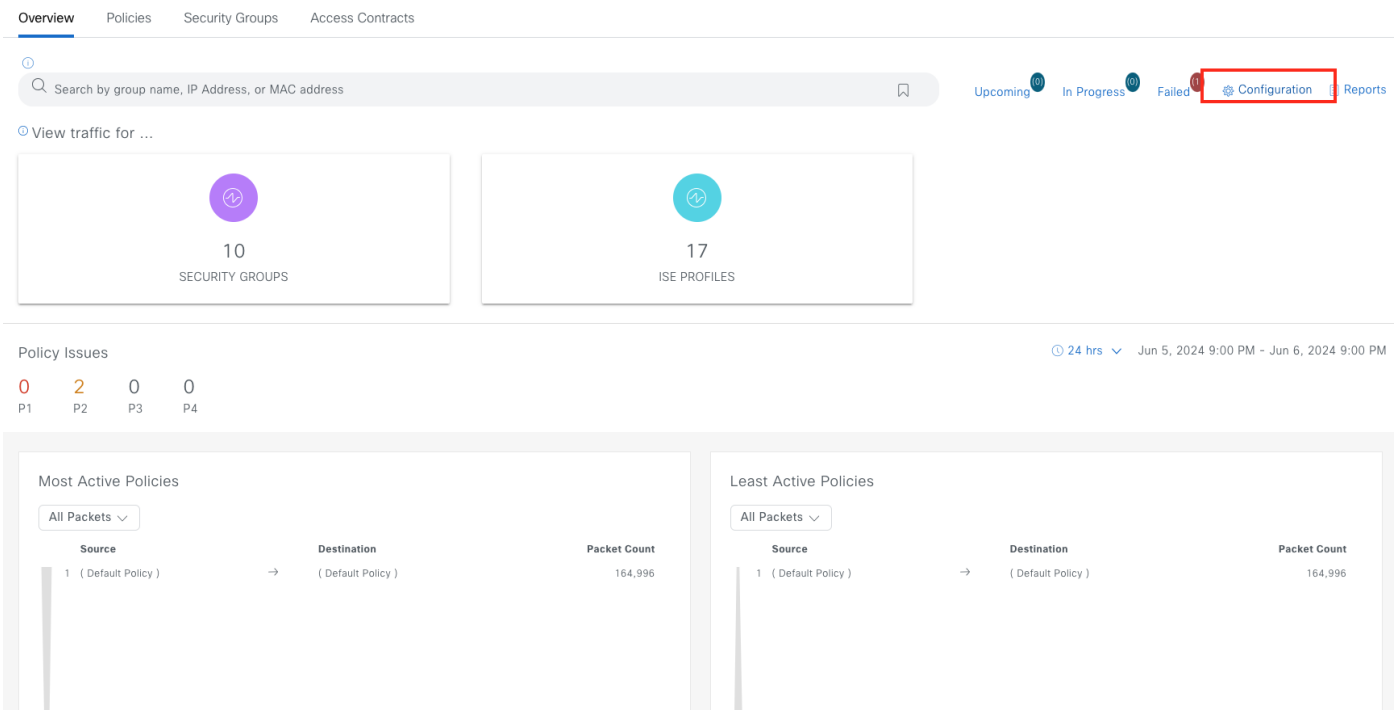
## 手順 3。　管理モードの変更

Catalyst Center には、管理モードを定義するオプションがあります。

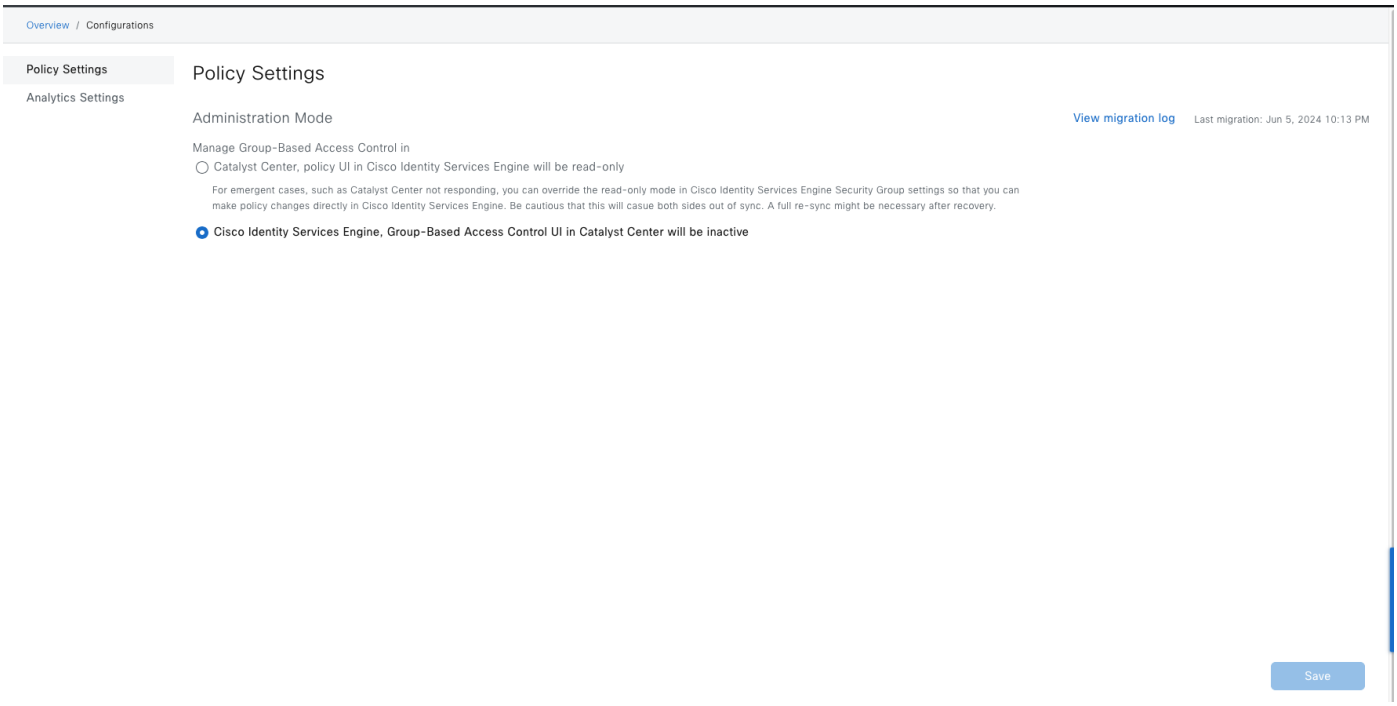
Cisco ISE を管理ポイントとして優先し、Cisco ISE と Catalyst Center の間で管理ポイントを切り替える場合は、次の手順を実行します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Policy] > [Group-Based Access Control] の順に選択し、[Overview] タブをクリックします。

**ステップ 2.** [Configuration] をクリックします。




**ステップ 3.** 管理ポイントのいずれかのオプションを選択します。



## サイト階層の設定

サイト階層の設定には、展開用のネットワークサイトとそれらの階層関係の定義が含まれます。ネットワークサイトは、エリア、建物、およびフロアで構成されます。子サイトは親サイトから特定の属性を自動的に継承するため、それらの階層関係は重要です。ただし、これらの属性は、子サイト内でオーバーライドされる可能性があります。

表 15 に、この設計および導入ガイドのサイト階層を示します。複数の**建物**（**Cisco-buidling-24**）、（**フロア 1** と **フロア 2**）がある単一のエリア（**Milpitas**）がプロビジョニングされます。

**表 15.** 設計および導入ガイドのサイト階層

| 名前 | サイトのタイプ | 親 | その他の情報 |
|---|---|---|---|
| Milpitas | Area | Global | |
| Building 24 | Building | Milpitas | 住所：510 McCarthy Boulevard、Milpitas、California、95035 |

この設計および導入ガイドのサイト階層の設定手順には、次のものが含まれます。

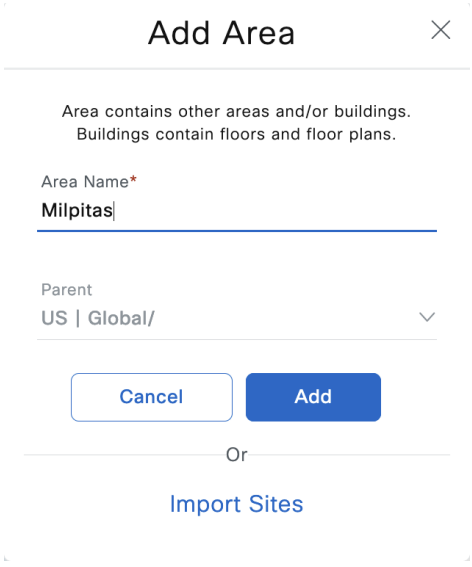
- エリアの作成。
- エリア内の建物の作成。
- 各建物内のフロアの作成とフロアマップのインポート（オプション）。

### 手順 1。 エリアの作成

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Design] > [Network Hierarchy] の順に選択します。

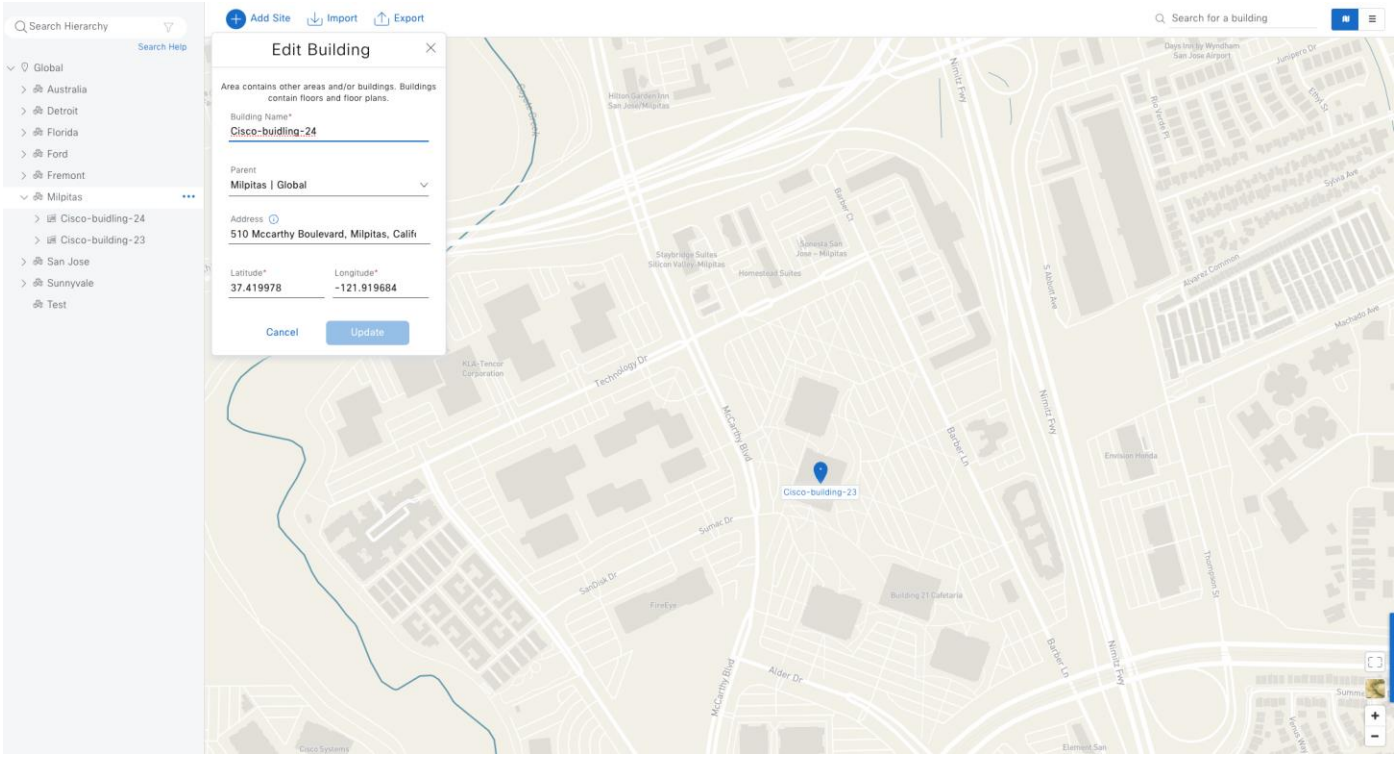
**ステップ 2.** ネットワーク階層ダッシュボードで、[Add Site] > [Add Area] の順に選択します。

**図 24.** **[Add Area] ダイアログ**



## 手順 2。　エリア内の建物の作成

建物の追加は、[Add Site] ドロップダウンリスト、または左側のナビゲーションペインの [Global] > [Milpitas] から行います。




**ステップ 1.** フィールドの [Building Name] に入力します。この例では、「**Cisco-building-24**」と入力します。

**ステップ 2.** **Cisco-building-24** の場合、フィールドの [Address] に入力します。

**ステップ 3.** [Parent] > [Milpitas] を選択します。

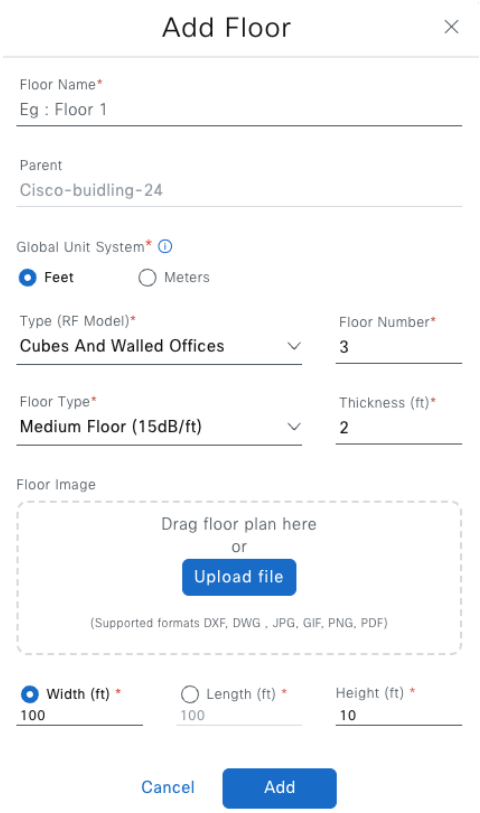
**ステップ 4.** ステップ 1 とステップ 2 を繰り返して、2 番目の建物の例を追加します。この例では、「**Cisco-Building-23**」と入力します。

## 手順 3。　建物内のフロアの作成

AP の場所とワイヤレスカバレッジ（ヒートマップ）は、フロアマップから表示できます。フロアはワイヤレスプロビジョニング時に参照されます。

フロアの追加は、[Add Site] ドロップダウンリストか、左側のナビゲーションペインの [Global] > [Cisco-building-24] および [Global] > [Cisco-Building-23] から行います。

**図 25.　[Add Floor] ダイアログ**




**ステップ 1.**　フィールドの [Floor Name] に [Parent]（例：**Cisco-building-24**）の最初のフロアを入力します。

**ステップ 2.**　（オプション）**フロア画像**のマップをアップロードします。

**ステップ 3.**　ステップ 1 とステップ 2 を繰り返して、2 番目のフロアを追加します。

## ネットワーク運用に必要なネットワークサービスの設定

Catalyst Center では、共通のネットワークリソースおよび設定が設計アプリケーションの [Network Settings] タブに保存されます。

設計アプリケーションで設定できる共通ネットワーク設定には、認証、許可、およびアカウンティング（AAA）サーバー、DHCP サーバー、DNS サーバー、Syslog サーバー、SNMP サーバー、NetFlow コレクタ、NTP サーバー、タイムゾーン、本日のメッセージ、テレメトリなどがあります。これらの機能のいくつかは、Catalyst Center Assurance の展開に使用されます。

デフォルトでは、[Network Settings] タブをクリックすると、新しい設定が**グローバル**ネットワーク設定として割り当てられます。それらは階層全体に適用され、各サイト、建物、およびフロアによって継承されます。[Network Settings] では、階層内のデフォルトの選択ポイントは [Global] です。

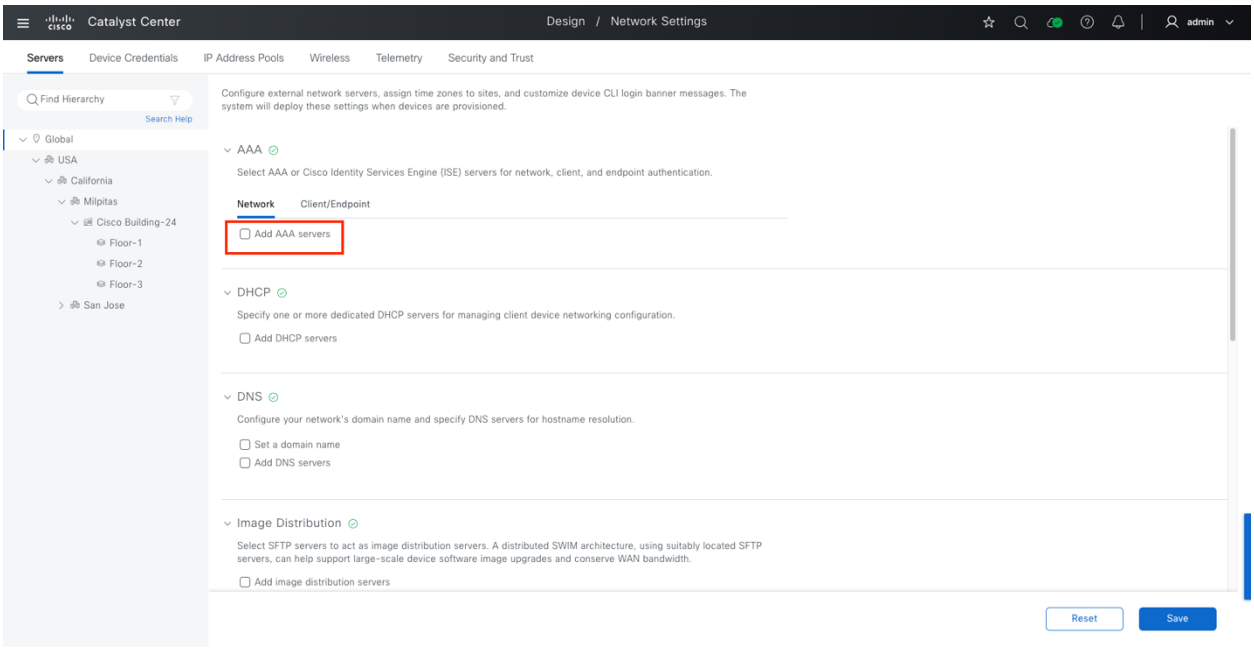
**技術的なヒント：**　特定のサイトの特定のネットワーク設定およびリソースを定義できます。

## 手順 1。　AAA、DHCP、DNS、NTP の設定

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Design] > [Network Settings] の順に選択し、左側のナビゲーションペインで [Global] をクリックします。

**ステップ 2.** [AAA] セクションを見つけて、[Add AAA servers] チェックボックスをオンにします。

**図 26.　[Network Settings] ウィンドウ**




このガイドでは、ネットワークデバイスとクライアントの両方で、RADIUS プロトコルを使用する AAA サーバーとして Cisco ISE を使用します。

**ステップ 3.** 表 16 に示す必要な情報を入力します。

**表 16.　AAA サーバーのフィールド**

| フィールド | 値 |
|---|---|
| Network | Checked |
| Client/Endpoint | Checked |
| [Network] > [Servers] | ISE |
| [Network] > [Protocol] | RADIUS |
| [Network] > [Network] | 10.195.221.144 |
| [Network] > [IP Address (Primary)] | 110.2.2.1 |
| [Network] > [Shared Secret] | ****** |
| [Client/Endpoint] > [Servers] | ISE |
| [Client/Endpoint] > [Protocol] | RADIUS |
| [Client/Endpoint] > [Network] | 10.195.221.144 |
| [Client/Endpoint] > [IP Address (Primary)] | 110.2.2.1 |
| [Client/Endpoint] > [Shared Secret] | ****** |

**ステップ 4.** [DHCP Server] セクションを見つけて、必要な情報を入力します。

Catalyst Center は IPV4 と IPV6 の両方の DHCP サーバーをサポートしており、複数の DHCP サーバーを追加できます。

| フィールド | 値 |
|---|---|
| DHCP server | 110.10.2.1, 2000::1 |
| | 110.10.3.1, 2003::1 |

**ステップ 5.** [DNS Server] セクションを見つけて、必要な情報を入力します。

**表 17.** DNS Server

| フィールド | 値 |
|---|---|
| Domain Name | cagelab.local |
| Primary | 110.2.2.4 |

**ステップ 6.** [NTP Servers] セクションを見つけて、必要な情報を入力します。

復元力と精度を得るために複数の NTP サーバーを追加できます。ネットワーク内の時刻同期は、ロギング機能や、SSH などのセキュアな接続に不可欠です。

**表 18.** NTP サーバーのフィールド

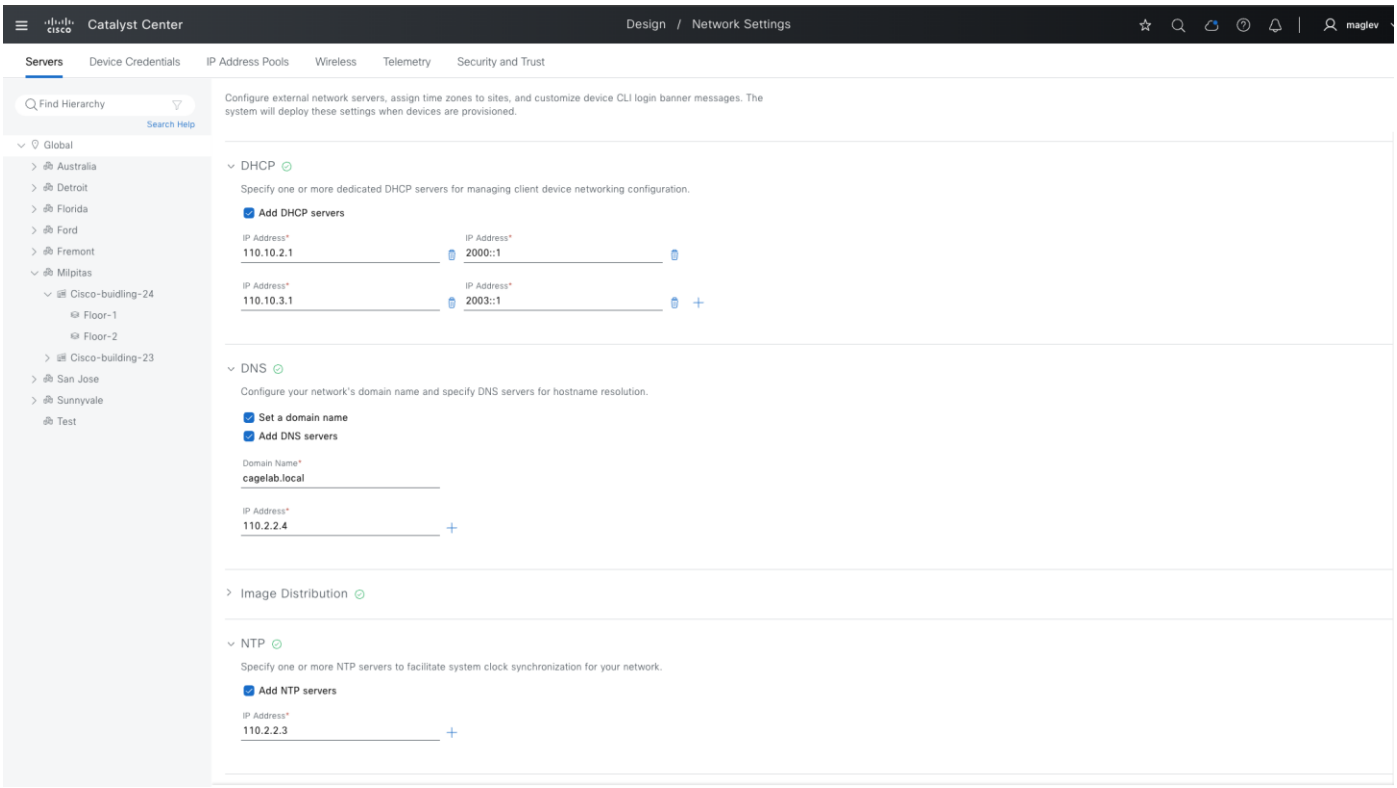
| フィールド | 値 |
|---|---|
| IP Address | 110.2.2.3 |

**ステップ 7.** [Time Zone] セクションを見つけて、必要な情報を入力します。

**表 19.** タイムゾーンのフィールド

| フィールド | 値 |
|---|---|
| Time Zone | GMT |

**ステップ 8.** すべてのセクションに入力したら、[Save] をクリックしてネットワークサービスへの変更を保存します。




## 手順 2。 テレメトリ、SNMP、Syslog の設定

Catalyst Center は SNMP および Syslog サーバーとして設定でき、外部 SNMP および Syslog サーバーもサポートされています。Catalyst Center が SNMP および Syslog サーバーとして設定されている場合、SNMP トラップと Syslog は Catalyst Center アシュアランス アプリケーションによって処理され、アシュアランス ダッシュボードでレポートされます。

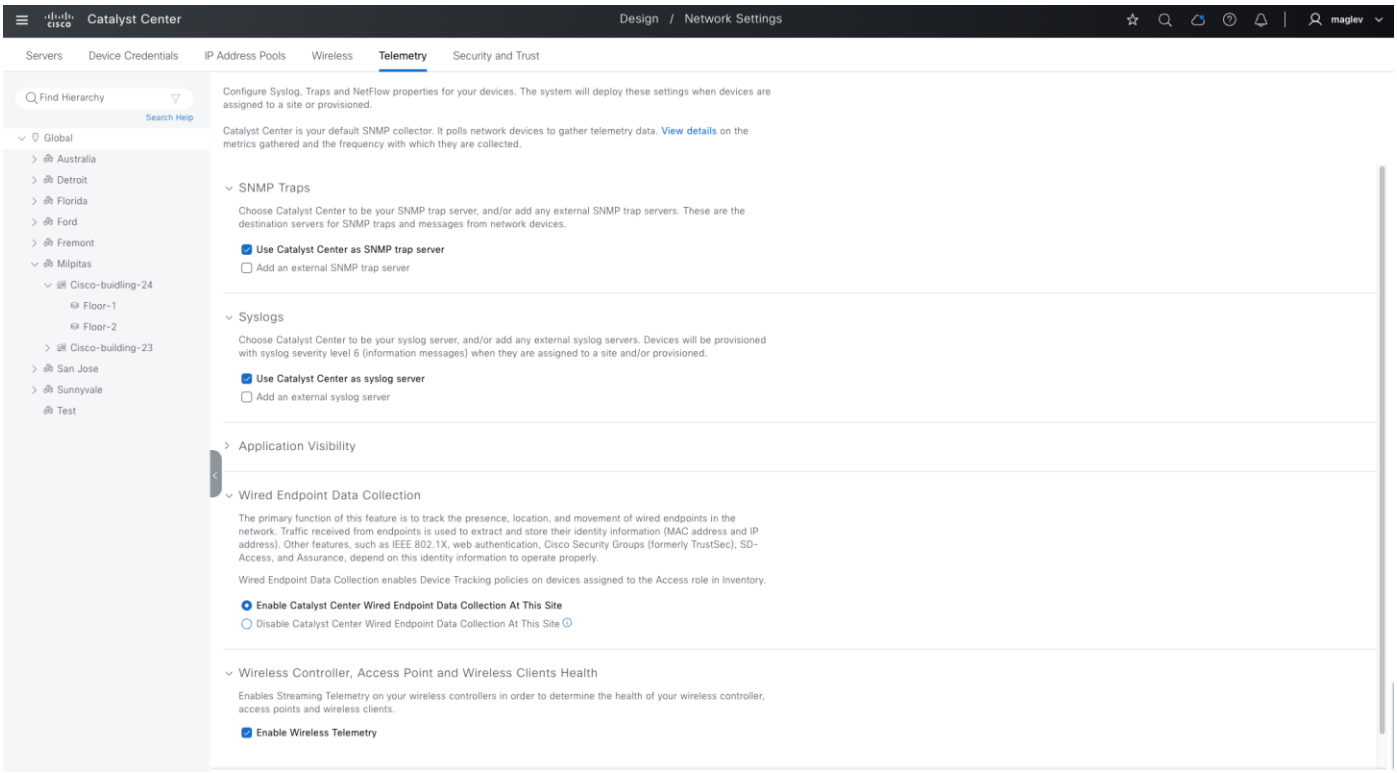
[Wired Endpoint Data Collection] オプションは、ネットワーク内の有線エンドポイントのプレゼンス、場所、移動を追跡します。エンドポイントから受信したトラフィックは、アイデンティティ情報（MAC アドレスと IP アドレス）を抽出して保存するために使用されます。これは、ファブリックサイトに必須です。設定は、**アクセス**ロールを持つすべてのデバイスにプッシュされます。

[Wireless Controller, Access Point and Wireless Clients Health] オプションは、ワイヤレスコントローラのストリーミングテレメトリを有効にして、ワイヤレスコントローラ、AP、ワイヤレスクライアントの正常性を決定します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Design] > [Network Settings] の順に選択します。

**ステップ 2.** [Telemetry] タブをクリックします。

**図 27.　　Catalyst Center を SNMP および Syslog サーバーとして使用した例**




## IP プールの設定

Catalyst Center IPAM（IP アドレス管理）ツールを使用して、IP アドレスプールを作成および予約します。SD アクセスネットワークの IP アドレスプールは、有線クライアント、ワイヤレスクライアント、AP、拡張ノードなどのエンドポイントに IP アドレスを割り当てるために使用されます。さらに、Catalyst Center では、LAN 自動化やボーダー自動化レイヤ 3 ハンドオフ、マルチキャスト RP の設定などに IP プールを使用します。

IP アドレスプールはグローバルレベルで定義され、ファブリックオプションが有効になっているエリア、建物、またはフロアレベルで予約されます。

Catalyst Center は、グローバルレベルでの IPv4 および IPv6 プールの追加をサポートしていますが、サイトレベルで予約する場合は、IPv4 または IPv4 および IPv6 デュアルスタックプールのみをサポートしています。純粋な IPv6 プールはサポートされていません。

**注：**　デュアルスタックプールは、LAN 自動化、AP、および拡張ノードのオンボーディングではサポートされていません。

このセクションの手順では、**Cisco-building-24** の LAN 自動化、クライアント、AP、拡張ノード、レイヤ 3 ハンドオフ、およびマルチキャスト用に IP プールを追加および予約します。

## 手順 1。　グローバルレベルでの IP プールの追加

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Design] > [Network Settings] の順に選択します。

**ステップ 2.** [IP Address Pools] タブをクリックして、左側のナビゲーションウィンドウで [Global] をクリックします。

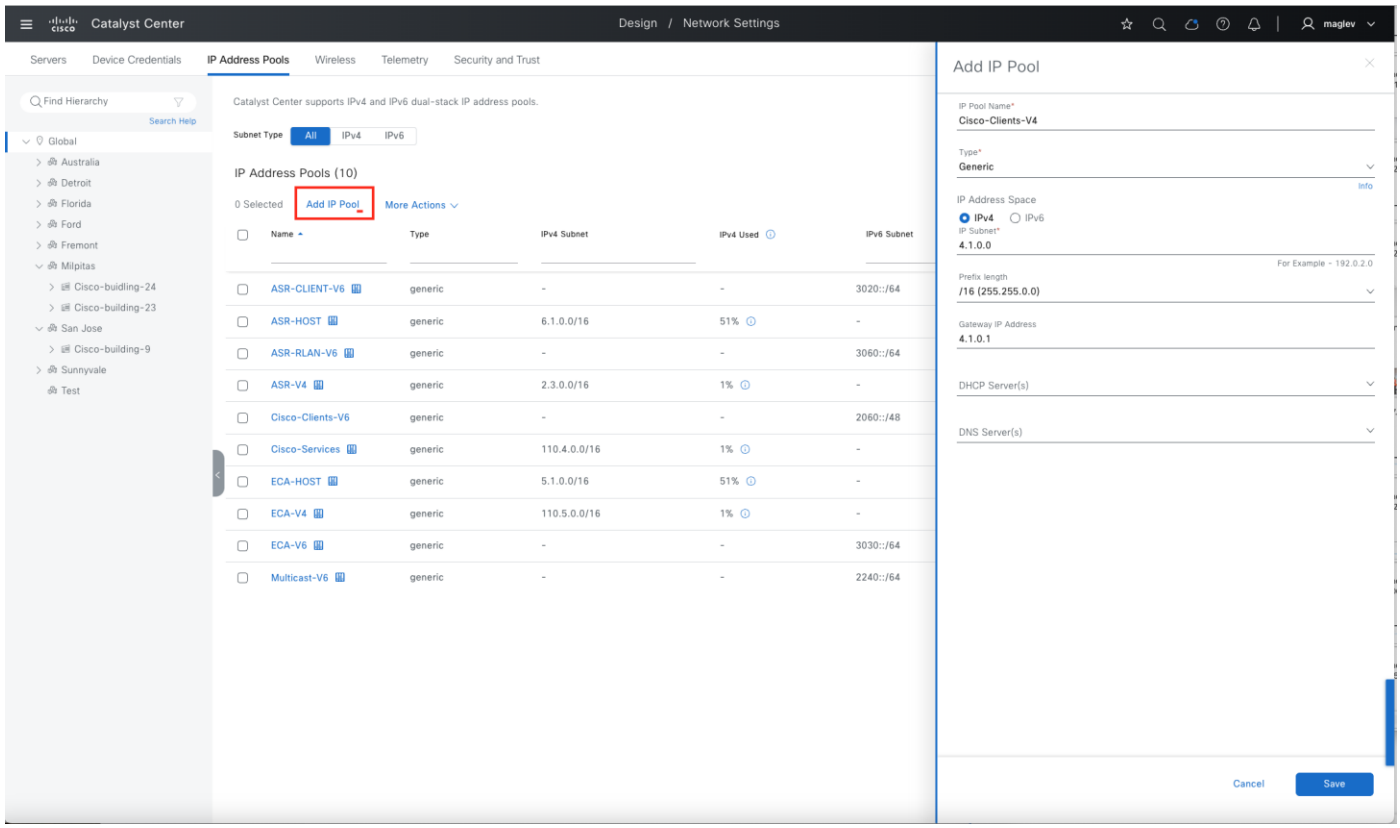
**ステップ 3.** [Add IP Pool] をクリックします。

**ステップ 4.** 右側のスライドインペインで [IPv4] をクリックし、必要なフィールド情報を入力して、[Save] をクリックします。

**ステップ 5.** [Add IP Pool] をクリックします。

**ステップ 6.** 右側のスライドインペインで [IPv6] をクリックし、必要なフィールド情報を入力して、[Save] をクリックします。

| グローバルプール | IP サブネット | ゲートウェイ |
|---|---|---|
| Cisco-Clients-V4 | 4.1.0.0/16 | 4.1.0.1 |
| Cisco-Clients-V6 | 2060: :/48 | 2060::1 |
| Cisco-Services | 110.4.0.0/16 | 110.4.0.1 |




**注：**　DHCP サーバーと DNS サーバーはオプションであり、サイトレベルで設定できます。

## 手順 2。　ファブリックサイト用 IP プールの予約

ファブリックサイト **Cisco-building-24** は、次の計画済み IP アドレスプールを使用します。

| 使用するプール | 名前 | IP サブネット | ゲートウェイ | DHCP | DNS |
|---|---|---|---|---|---|
| アクセスポイント | Building-24-AP | 110.4.120.0/24 | 110.4.120.1 | 110.10.2.1 | 110.2.2.4 |
| 拡張ノード | Building-24-EN | 110.4.60.0/24 | 110.4.60.1 | 110.10.2.1 | 110.2.2.4 |
| クライアントプール -1 | Building-24-Emp | 4.1.64.0/18 | 4.1.64.1 | 110.10.2.1 | 110.2.2.4 |
| クライアントプール -2 | Building-24-Guest | 4.1.0.0/18 | 4.1.0.1 | 110.10.2.1 | 110.2.2.4 |
| LAN の自動化 | Building-24-Lan | 110.4.0.0/24 | 110.4.0.1 | 110.10.2.1 | 110.2.2.4 |
| L3 ハンドオフ | Building-24-L3 | 110.4.100.0/24 | 110.4.100.1 | | |
| マルチキャスト | Building-24-RP | 110.4.224.0/24 | 110.4.224.1 | | |

**注：**　複数の DHCP と DNS を 1 つのプールに設定できます。レイヤ 3 ハンドオフおよびマルチキャストでの IP アドレスの割り当ては、Catalyst Center によって行われます。DHCP と DNS は必要ありません。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Design] > [Network Settings] の順に選択します。

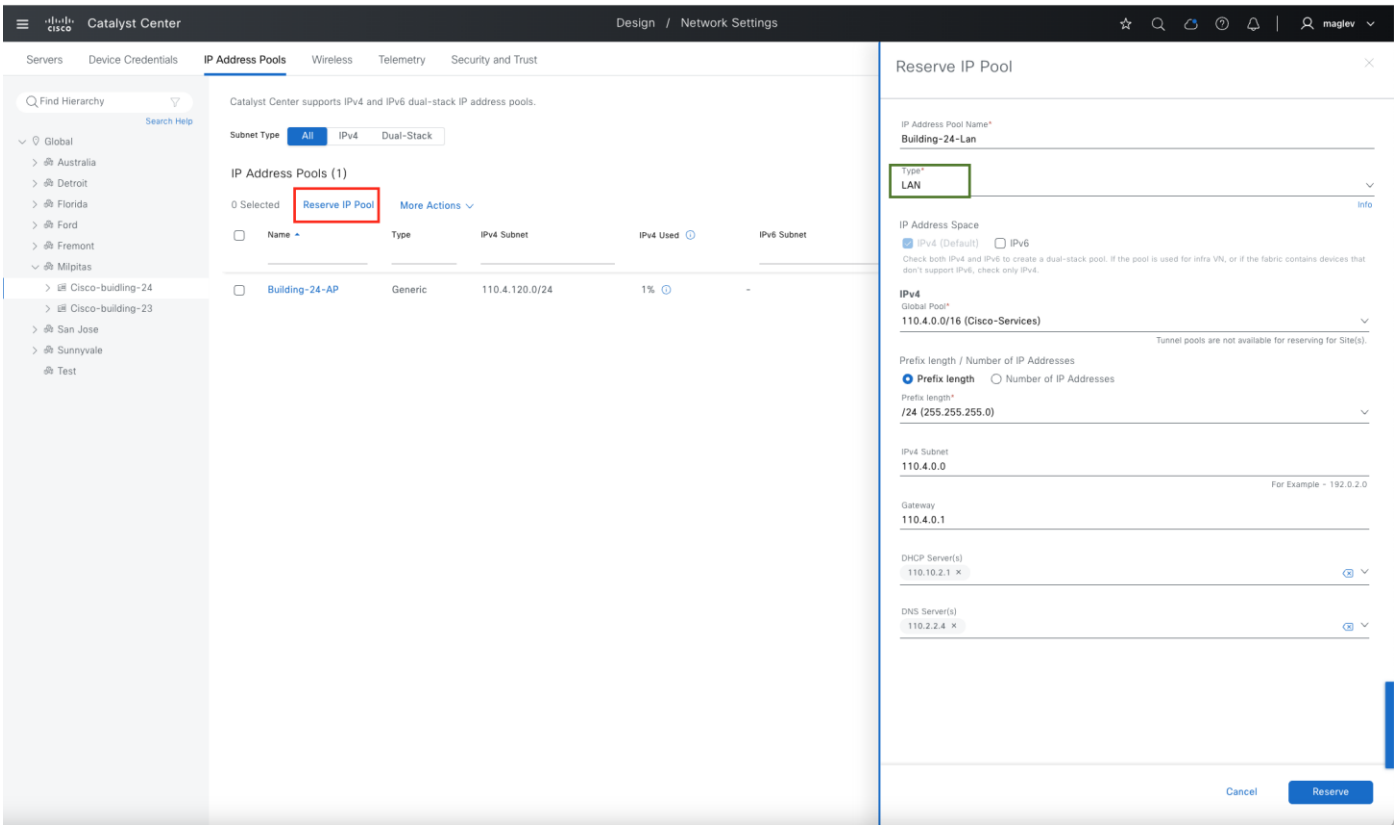
**ステップ 2.** [IP Address Pools] タブをクリックします。

**ステップ 3.** 左側のナビゲーションウィンドウで、[Milpitas] > [Cisco-building-24] を選択します。

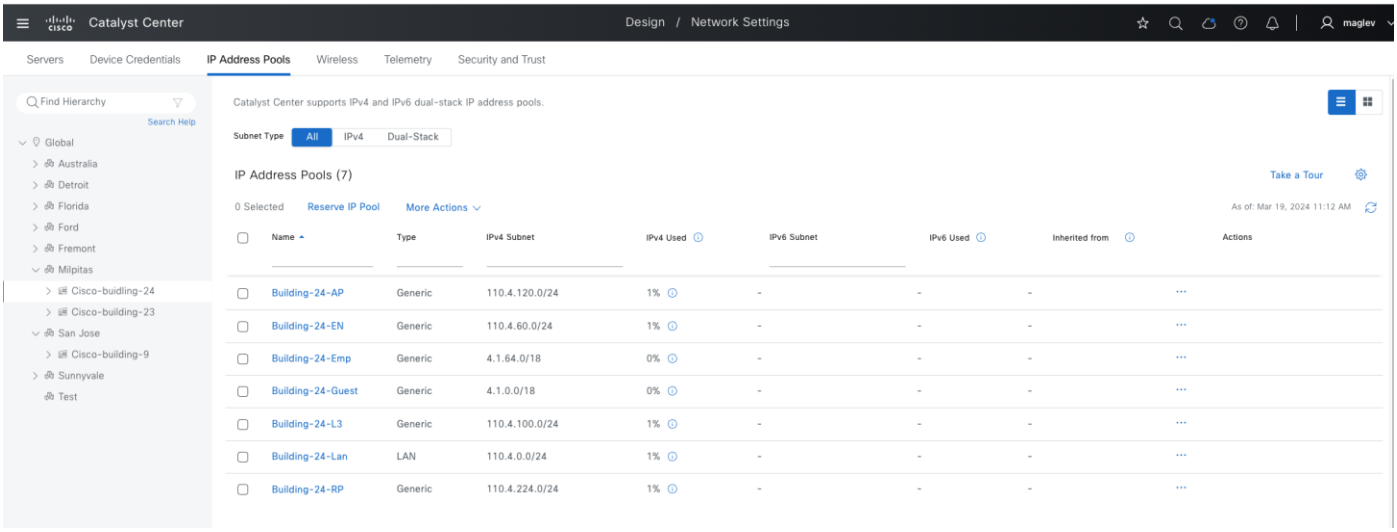
**ステップ 4.** [Reserve IP Pool] をクリックします。

**ステップ 5.** 右側の [Reserve IP Pool] スライドインペインで、表の情報を使用してフィールドに入力します。

LAN の自動化プールを使用する場合は、[Type] フィールドで [LAN] を選択します。その他のすべてのプールの場合は、[Type] フィールドで [Generic] を選択します。




**ステップ 6.** テーブルにリストされているすべてのプールを予約します。




## ワイヤレス SSID の設定

SSID を持つ WLAN は、展開全体で使用可能なワイヤレスネットワークをブロードキャストするために使用されます。サイト階層のグローバルレベルで定義し、サイトレベルで継承して使用する必要があります。サイトレベルで、継承された SSID のパラメータを編集および調整できます。

Catalyst Center は、エンタープライズ SSID とゲスト SSID の作成をサポートしています。

SSID の作成には、名前に加えてワイヤレスネットワークのタイプ（音声、データ、または両方）、ワイヤレスバンド、セキュリティタイプ、および詳細オプションの定義が含まれます。

ワイヤレスプロファイルは、ワイヤレスネットワークがファブリックか非ファブリックかを定義し、プロファイルが割り当てられる階層内のサイトとロケーションを定義します。IP アドレスプールなどのワイヤレス設定は、階層のグローバルレベルで設定されます。

ワイヤレス SSID の詳細については、「Cisco Catalyst Center User Guide」の「Configure Global Wireless Settings」のセクションを参照してください。

## 手順 1。 エンタープライズ SSID の設定

エンタープライズワイヤレス SSID を作成するワイヤレスワークフローには、次の作業が含まれます。

1. SSID とそのパラメータを作成します。
2. ワイヤレスプロファイルを作成します。

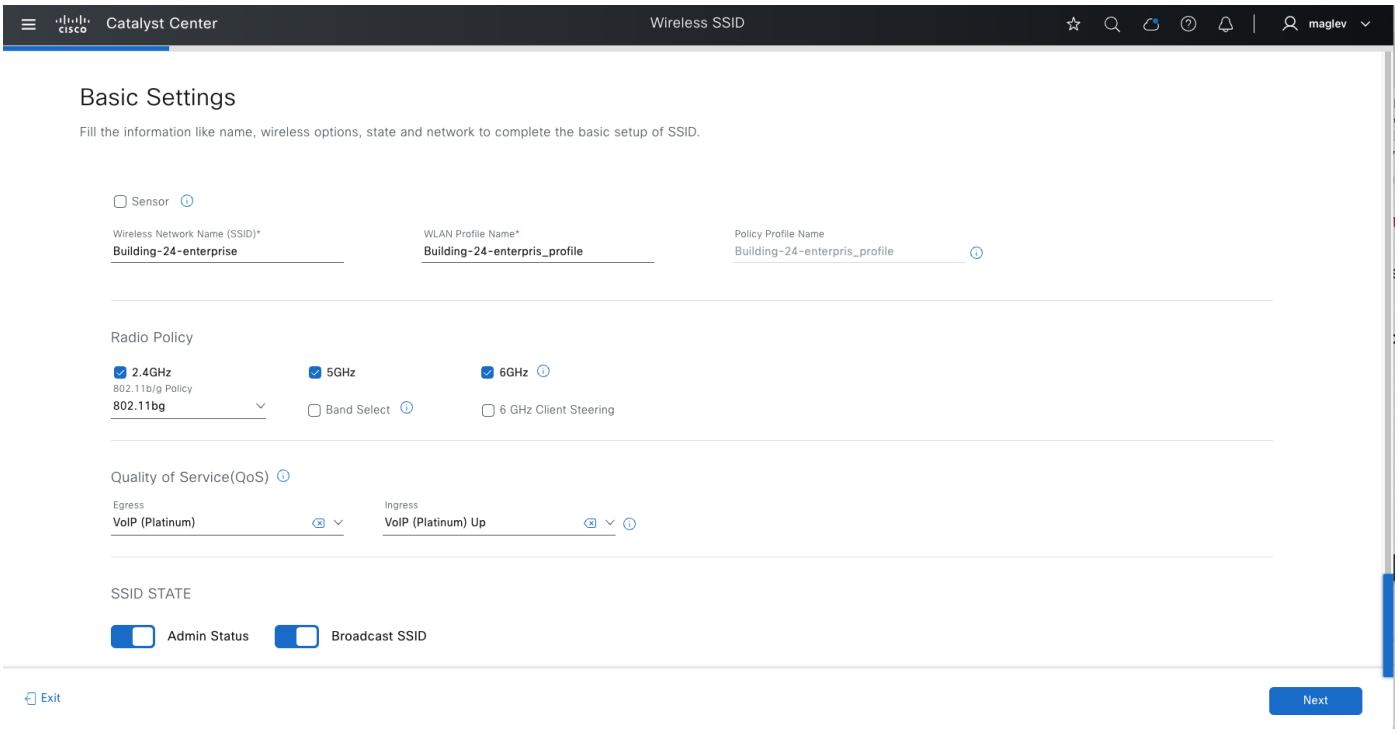
この導入ガイドでは、**Building-24-enterprise** という名前の SSID を使用して単一のエンタープライズ WLAN を設定します。

Catalyst Center 内でエンタープライズ ワイヤレス ネットワークを設定するには、次の手順を実行します。

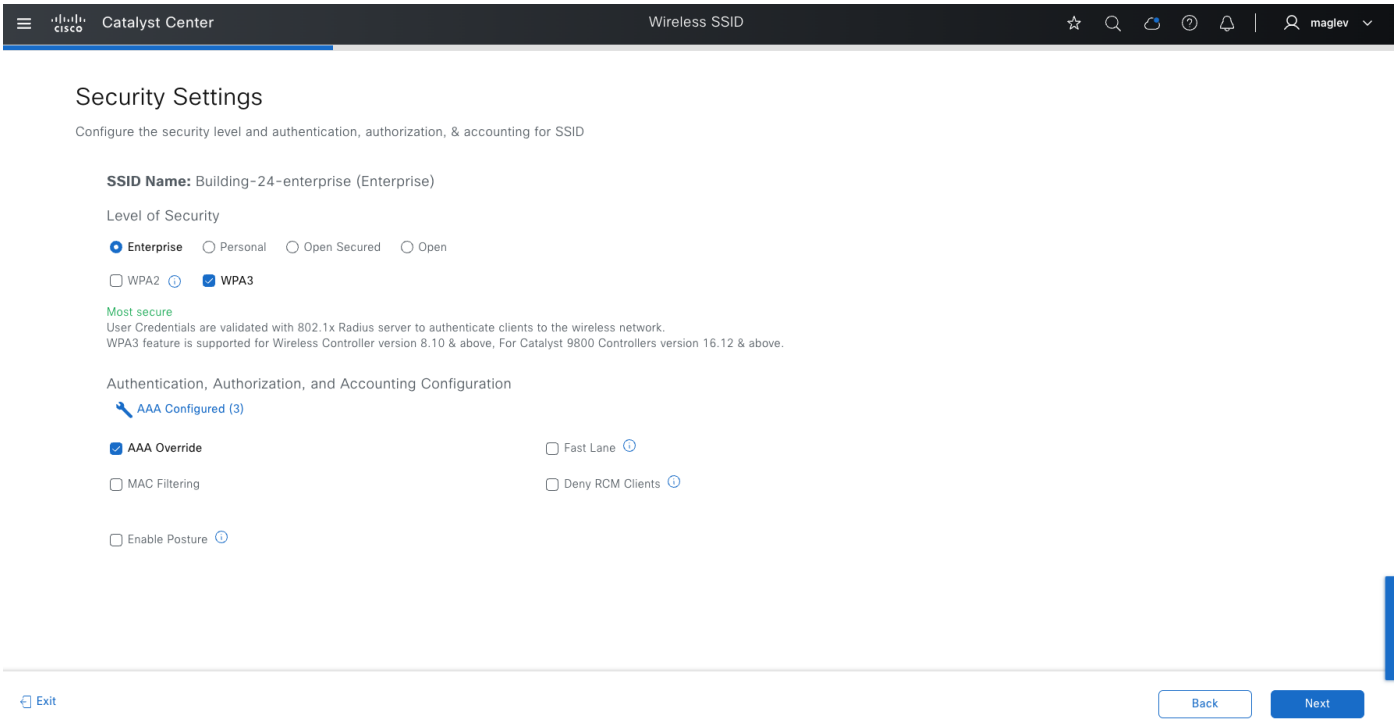
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Design] > [Network Settings] の順に選択し、[Wireless] タブをクリックしてダッシュボードを開きます。

**ステップ 2.** [SSID]、[Add]、[Enterprise] の順にクリックします。

[Create an Enterprise Wireless Network] ワークフローの最初のステップが表示されます。

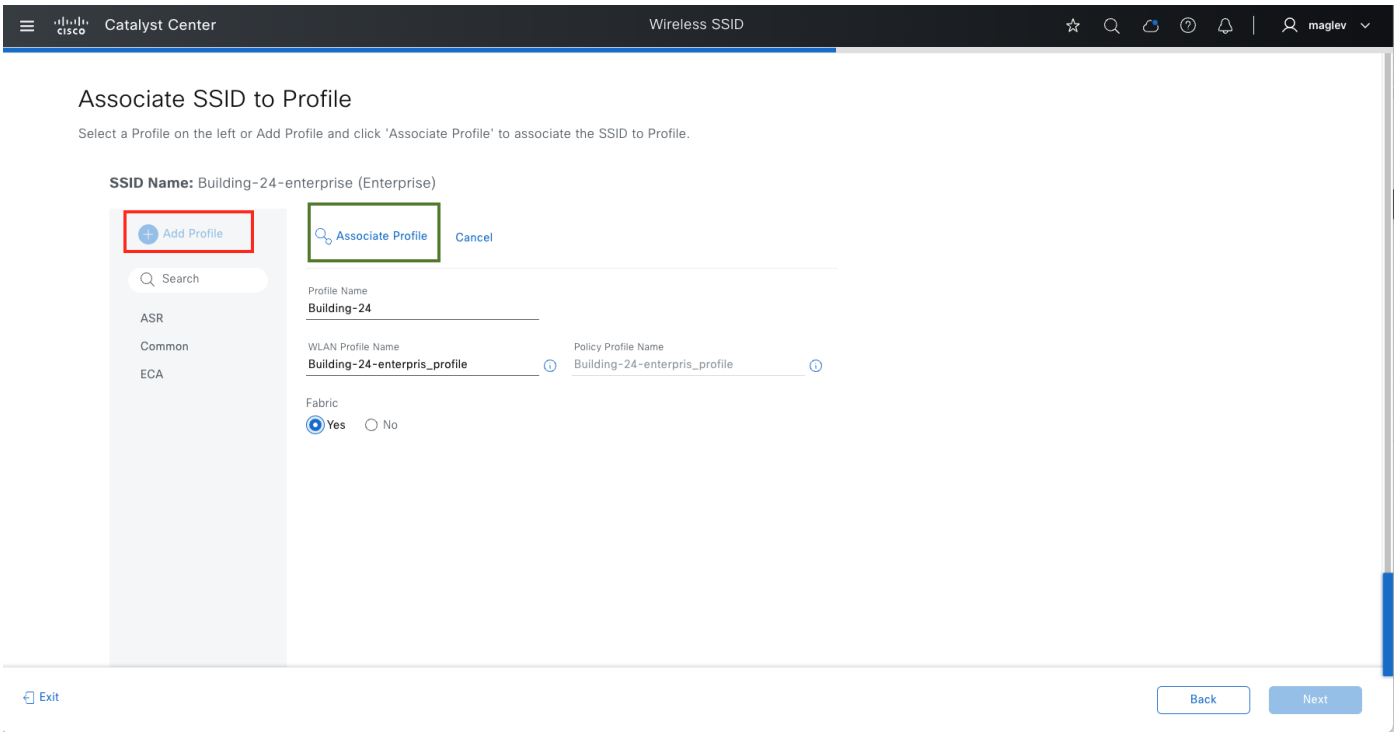



**ステップ 3.** **AAA** サーバーで**エンタープライズ** SSID の**セキュリティ設定**を設定します。




**ステップ 4.** [Advanced Settings]、[Model Config] アソシエーション（オプション）、[Associate SSID to Profile] に進みます。

1. [Add Profile] をクリックして新しいプロファイル（**Building-24**）を作成し、[Fabric] オプションとして [Yes] をクリックします。
2. SSID に関連付ける [Associate Profile] をクリックします。




**技術的なヒント：** SSID を作成する前に、[Network Profiles] ウィンドウ（[Design] > [Network Profiles]）から新

しいプロファイルを作成し、サイトに割り当てることができます。

**ステップ 5.** ワークフローを実行します。SSID ダッシュボードに新しい SSID **Building-24-enterprise** が表示されます。

## 手順 2。 ゲスト SSID の設定

ゲストワイヤレス SSID の設計は、エンタープライズワイヤレス SSID の設計に似ています。主な違いは、ワークフローのゲスト Web 認証のセクションです。Catalyst Center は、外部 Web 認証と中央 Web 認証をサポートしています。

外部 Web 認証は、指定された URL を使用してゲストユーザーをリダイレクトします。中央 Web 認証では Identity Services Engine のゲストポータルシーケンスを使用して、Cisco ISE でホストされているキャプティブポータルにゲストユーザーをリダイレクトします。

ゲストワイヤレス SSID の作成ワークフローは、次の 3 段階のプロセスです。

1. SSID とそのパラメータを作成します。
2. ワイヤレスプロファイルを作成します。
3. ポータルを作成します。

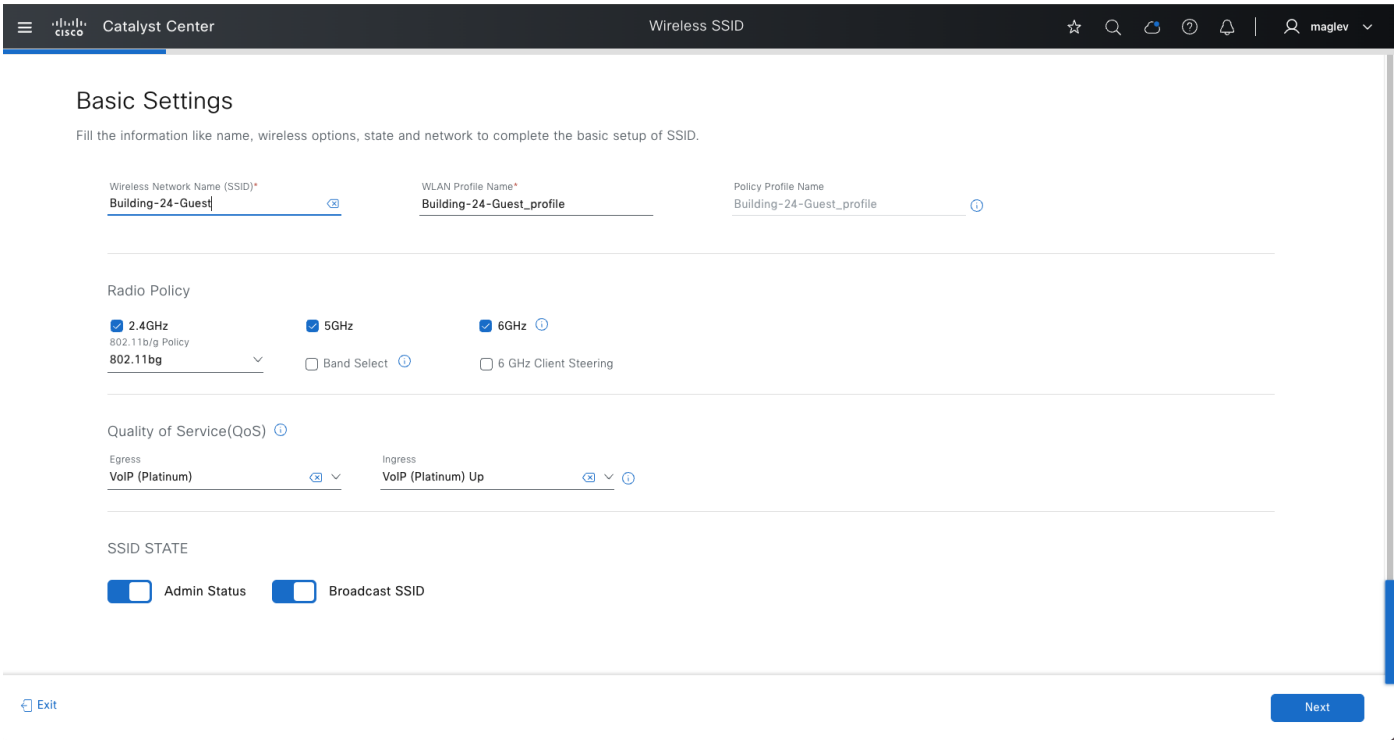
この導入ガイドでは、**Building-24-Guest** という名前の単一のゲスト ワイヤレス ネットワーク（SSID）がプロビジョニングされます。

Cisco Catalyst Center 内でゲスト ワイヤレス ネットワークを設定するには、次の手順を実行します。

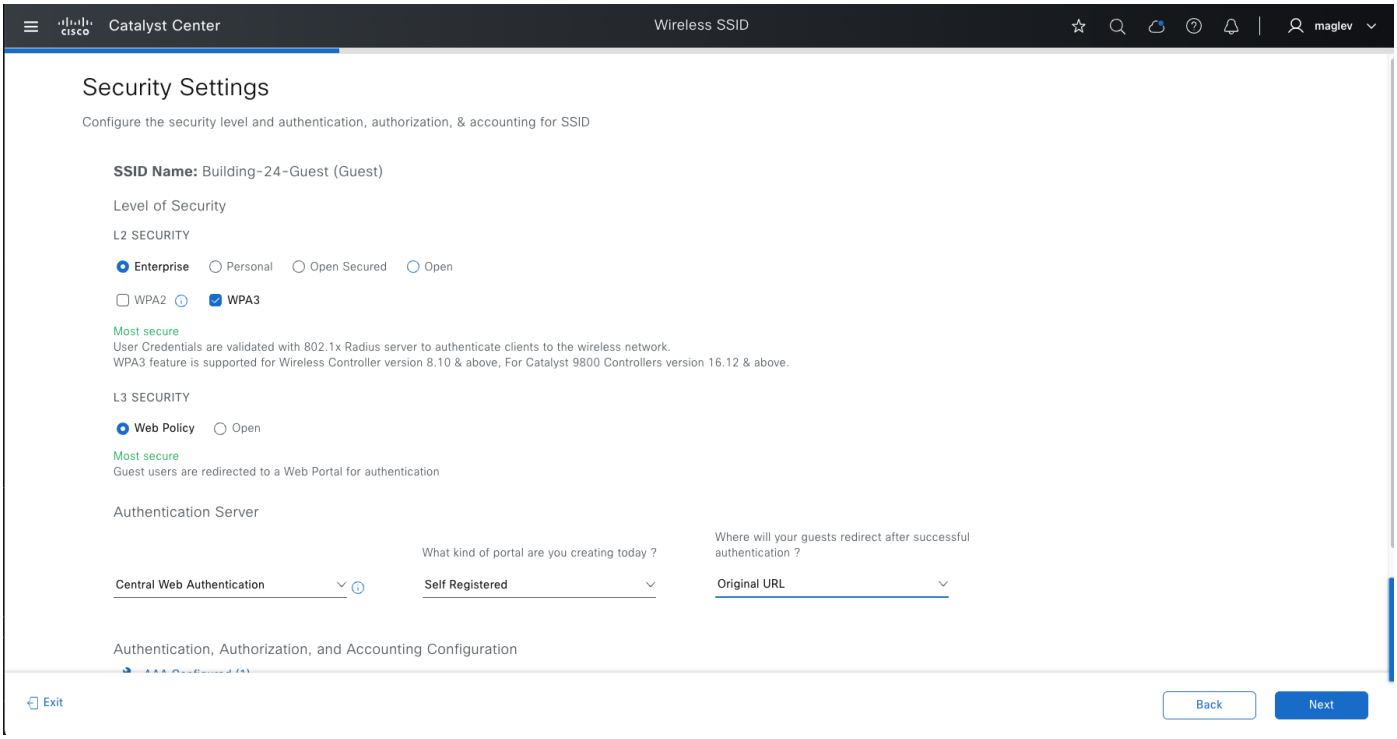
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Design] > [Network Settings] の順に選択し、[Wireless] タブをクリックしてダッシュボードを開きます。

**ステップ 2.** [SSID]、[Add]、[Guest] の順にクリックします。

このオプションにより、**ゲスト ワイヤレス ネットワークの作成**ワークフローの最初のステップが表示されます。

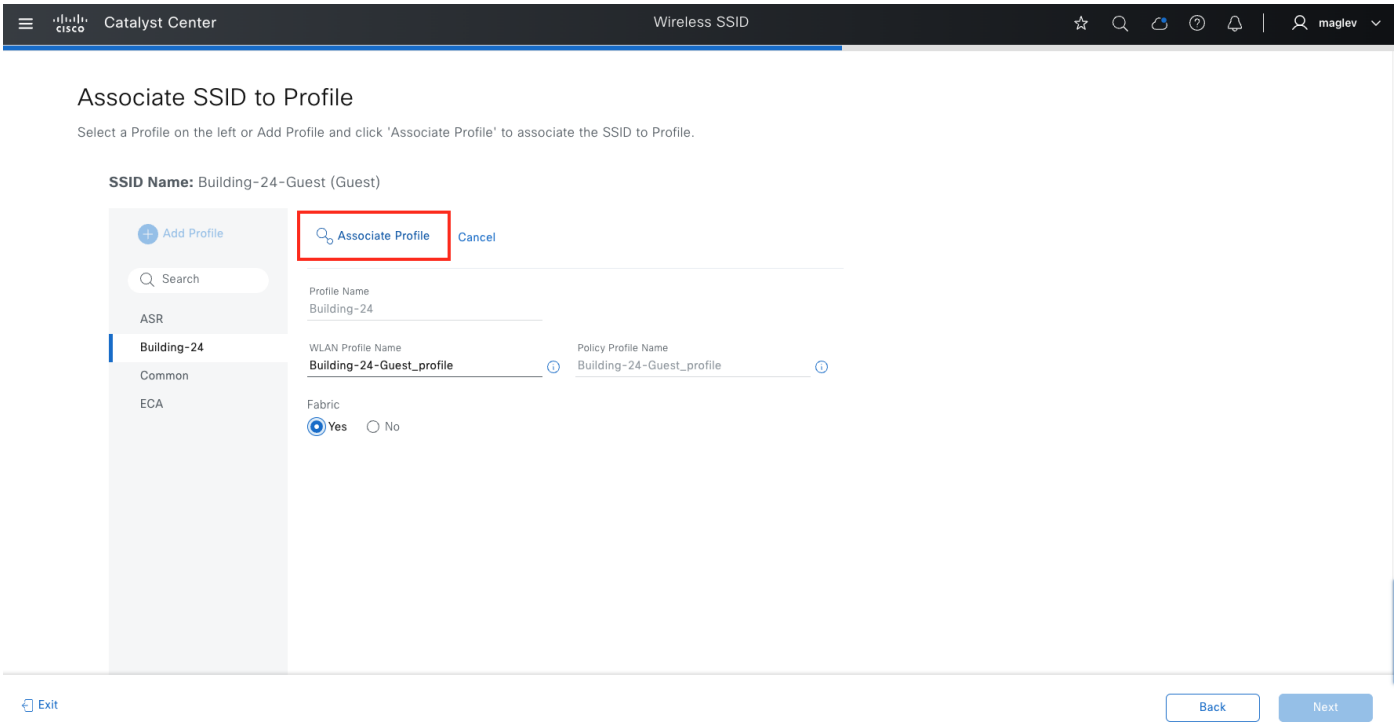



**ステップ 3.** AAA サーバーおよび認証サーバーのフィールド（[Central Web Authentication]、[Self-Registered]、[Original URL]）を使用して、ゲスト SSID のセキュリティ設定を設定します。



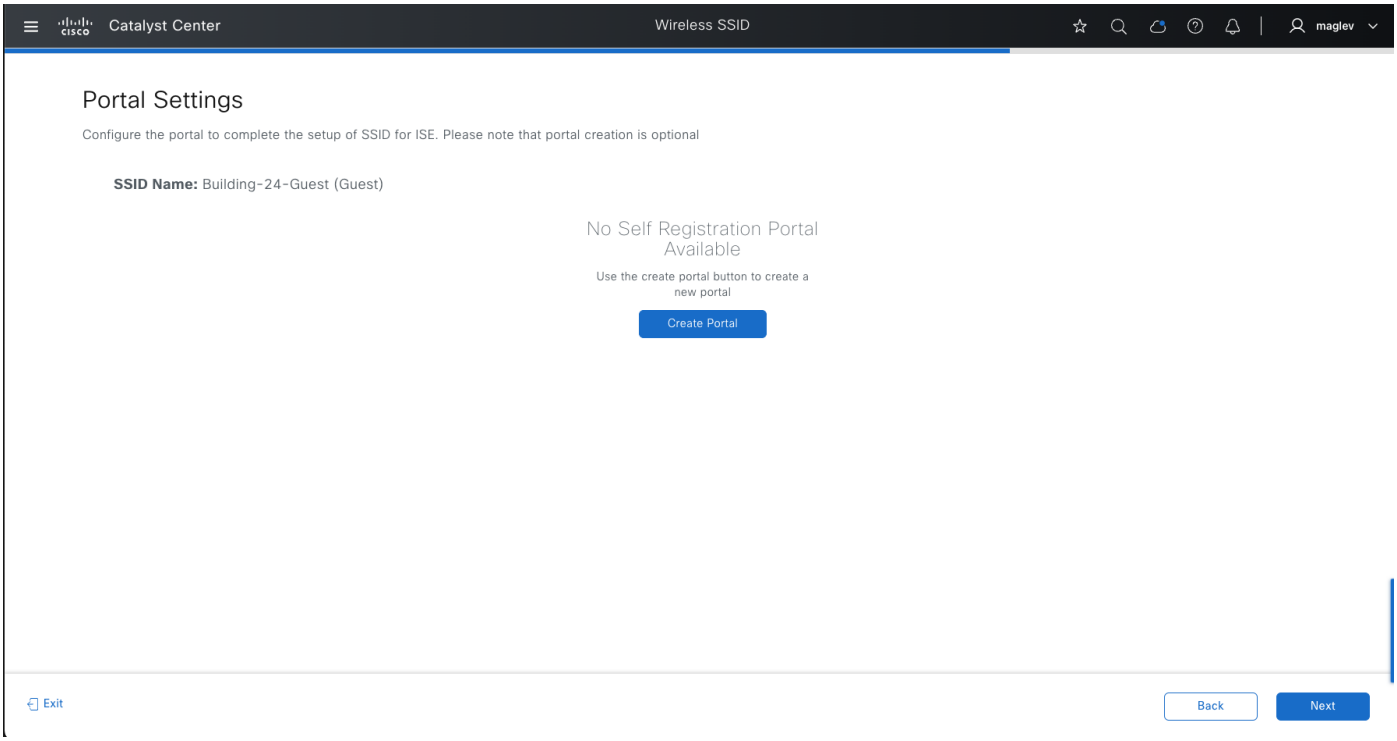

**ステップ 4.** [Advanced Settings]、[Model Config] アソシエーション（オプション）、[Associate SSID to Profile] に進みます。

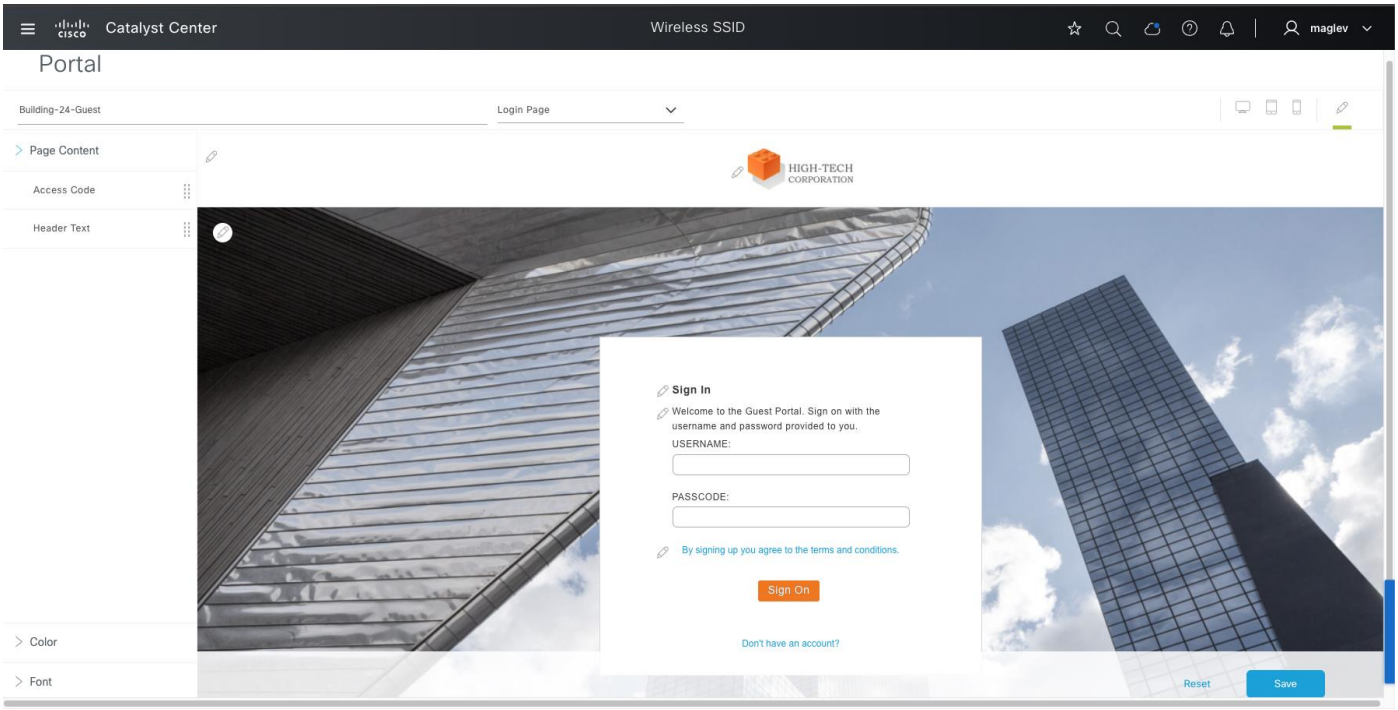
1. [Building-24]（前の手順で定義）を選択し、[Fabric] オプションで [Yes] をクリックします。
2. SSID に関連付ける [Associate Profile] をクリックします。




**ステップ 5.** Cisco ISE 内に新しいゲストポータルを追加します。

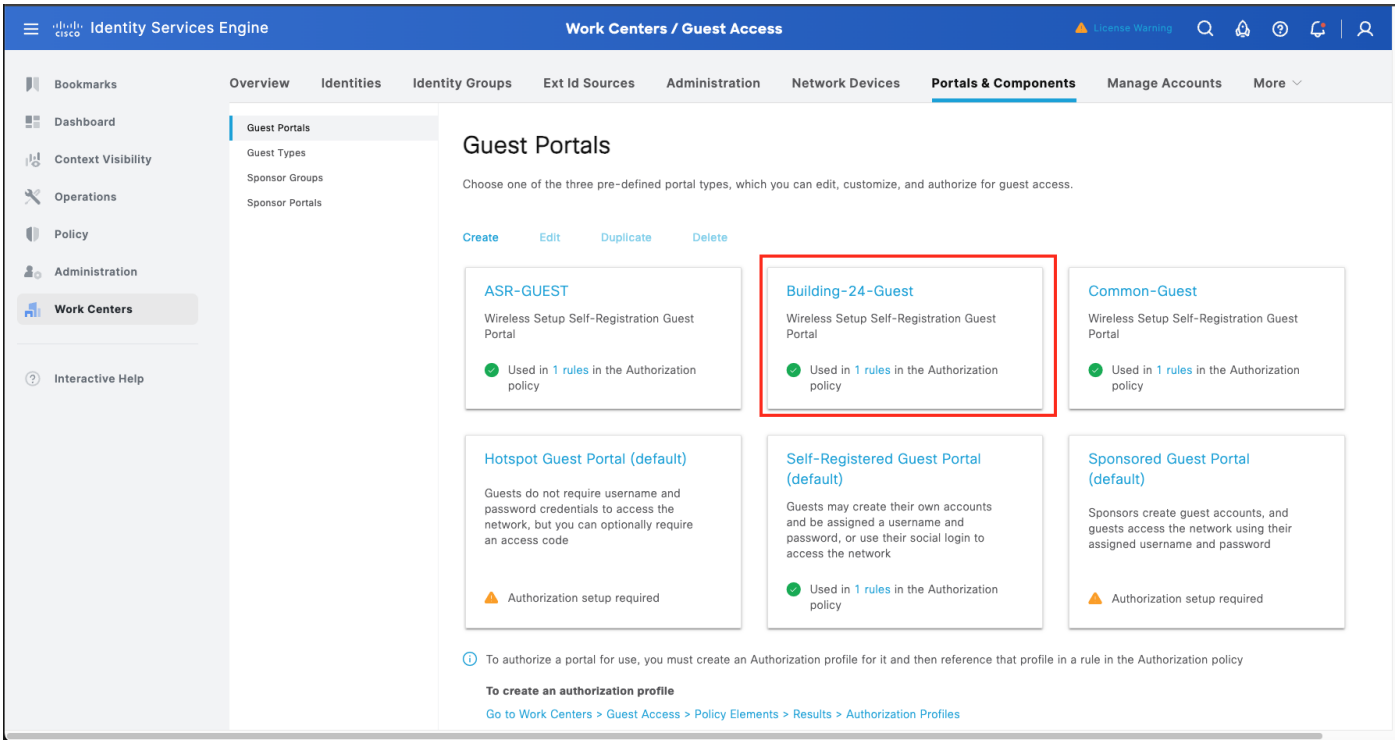
1. [Create Portal] ボタンをクリックします。
2. [Portal Builder] ウィンドウで、[Portal Name] に「**Building-24-Guest**」と入力します。
3. [Login Page] をクリックして、ワークフローを終了します。






ゲストポータルでゲスト SSID を作成後、Catalyst Center は、ゲスト SSID プロファイルの設定に従って、必要な認証、許可、およびゲストポータルの設定を Cisco ISE にプッシュします。

**図 28.　[Cisco ISE] > [Work Centers] > [Portals & Components] で設定を確認する例**

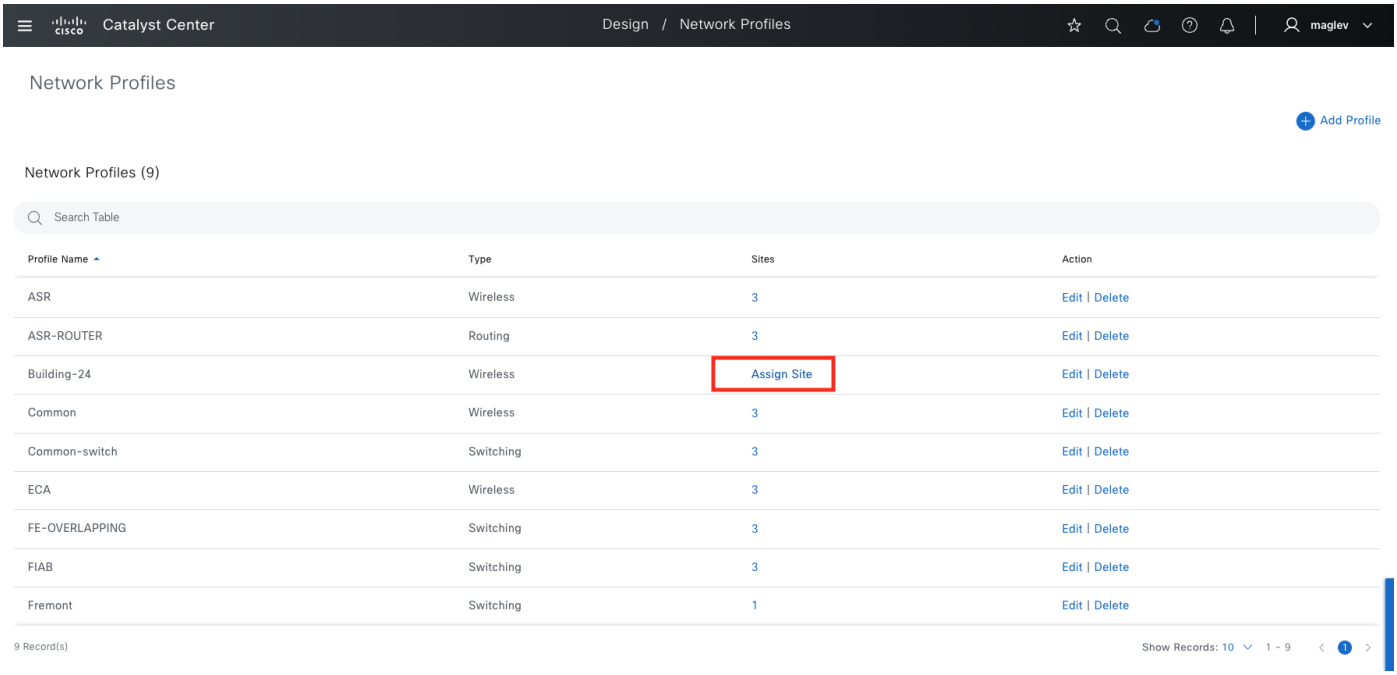



## 手順 3。　サイトへのネットワークプロファイルの割り当て

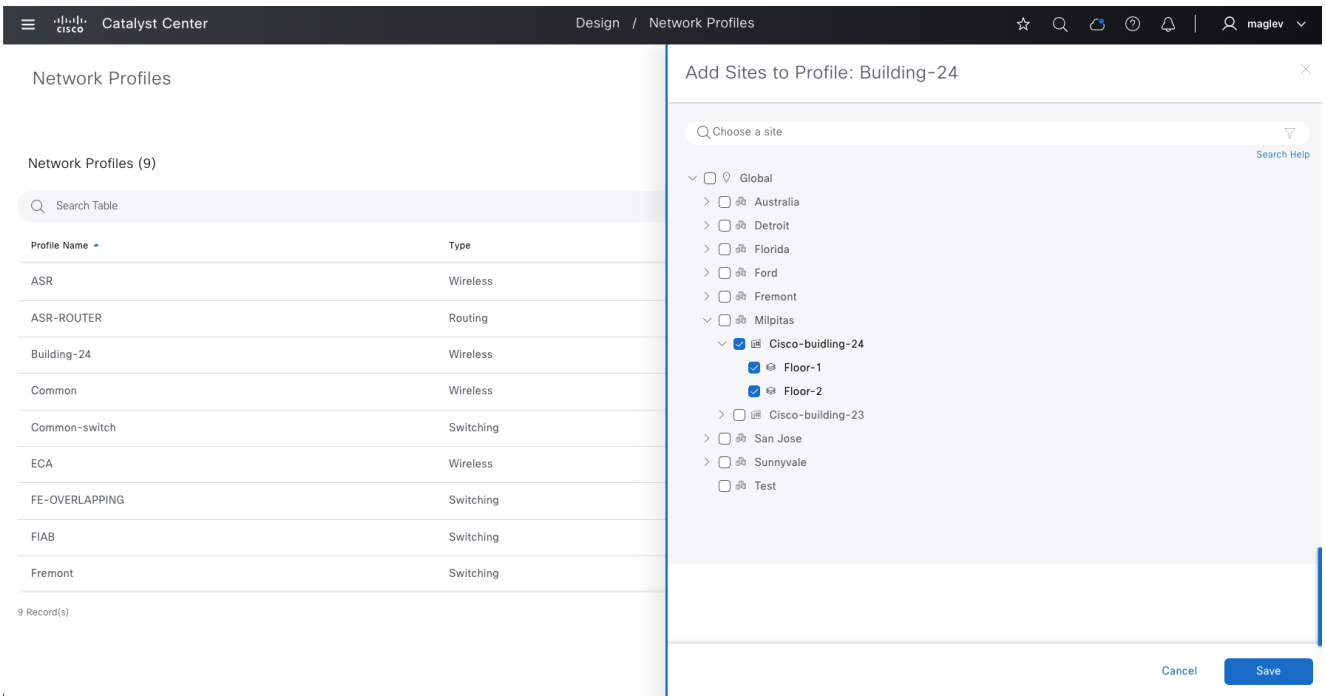
SSID を作成したら、ロケーション要件を定義するネットワークプロファイルをサイトに割り当てます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Design] > [Network Profiles] の順に選択します。

**ステップ 2.** **Building-24** としてリストされている**プロファイル名**（前の手順で作成済み）を見つけて、[Assign Site] をクリックします。




**ステップ 3.** スライドインペインで、[Building-24] チェックボックスをオンにして [Save] をクリックします。




## ファブリックサイトとファブリックゾーンの設定

ファブリックサイトは、コントロールプレーン、ボーダーノード、エッジノード、ワイヤレスコントローラ、Cisco ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計する

ことができます。ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることもできます。

ファブリックゾーンでは、指定されたファブリックエッジノードの含まれたセットに VN または IP プールを制限できます。この概念は、単一のファブリックサイトにファブリックエッジノードを大規模に展開し、より小さなロケーション、またはゾーンに基づいて、ネットワークを管理する方法を必要とするお客様に役立ちます。これらのゾーンは、複数の建物または建物内の複数のフロアである場合があります。

**注：**
ファブリックゾーンは、設計の考慮事項に基づいて、ネットワーク管理者が手動で有効にする必要があります。

ファブリックゾーンは親ファブリックサイトの子サイトであり、ファブリックサイト内の建物レベルまたはフロアレベルで設定できます。ファブリックゾーンが建物レベルで有効になっている場合、この建物内のすべてのフロアが同じファブリックゾーンの一部になります。

ファブリックゾーンは、Day-0 または Day-*N* の運用で有効にできます。Day-0 運用の場合、デフォルトでは、ファブリックゾーンに VN または IP プールはありません。具体的には、必要な VN プールと IP プールをファブリックゾーンに追加します。Day-*N* 運用の場合、ファブリックゾーンはファブリックサイトにマッピングされているすべての VN とプールを継承します。ファブリックゾーンで不要な VN または IP プールを削除します。

ファブリックゾーンは、ファブリックワイヤレス展開には適用できません。ファブリック SSID にマッピングされた IP プールは、すべてのファブリックエッジで設定する必要があります。

## 手順 1。　サイトでのファブリックの有効化

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Fabric Sites] の順に選択します。**サマリー**ビューは、デフォルトのランディングウィンドウです。

[Fabric Site] は、次のようなさまざまな場所から作成できます。

**図 29.　（場所 1）[Overview] > [Create Fabric Site]**

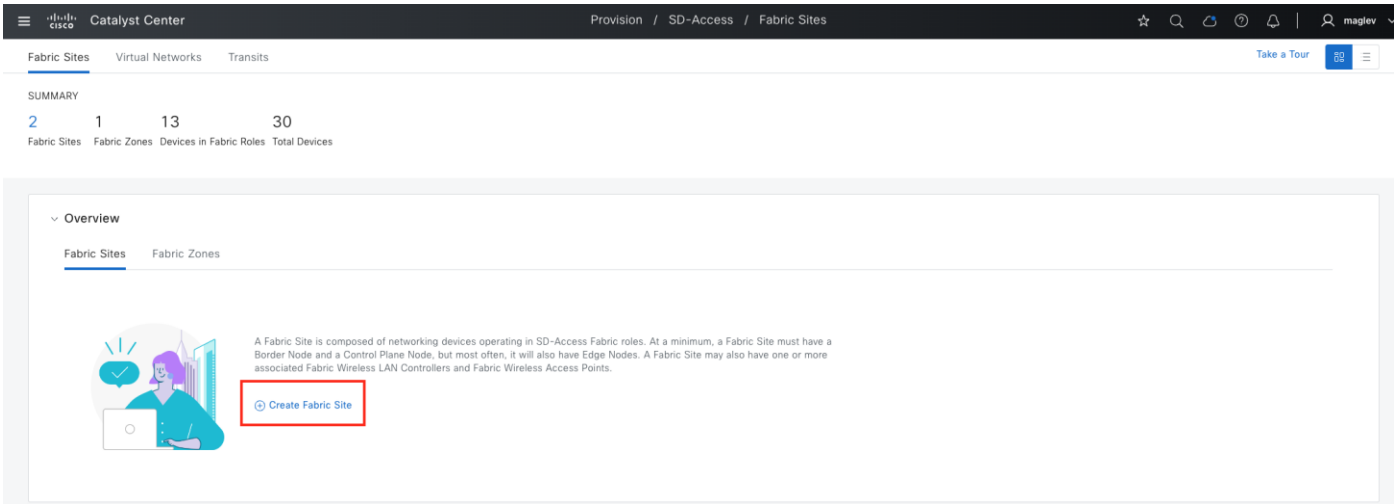


**図 30.　（場所 2）[Table Preview] > [Create Fabric Site]**

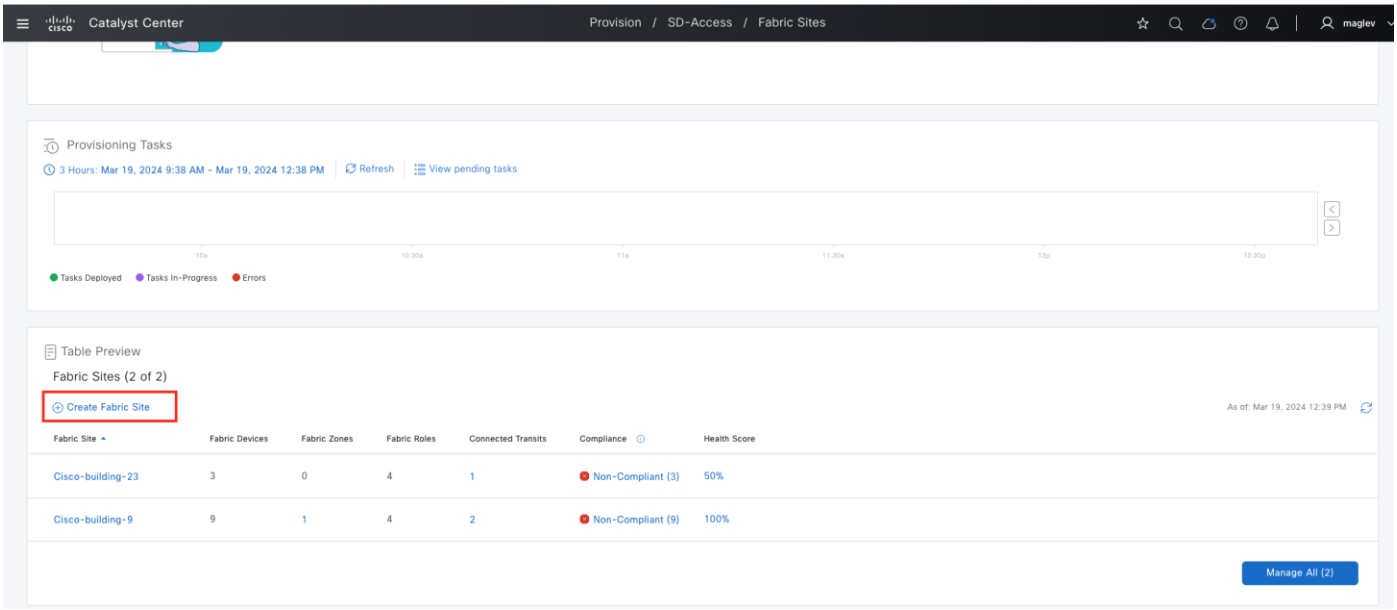
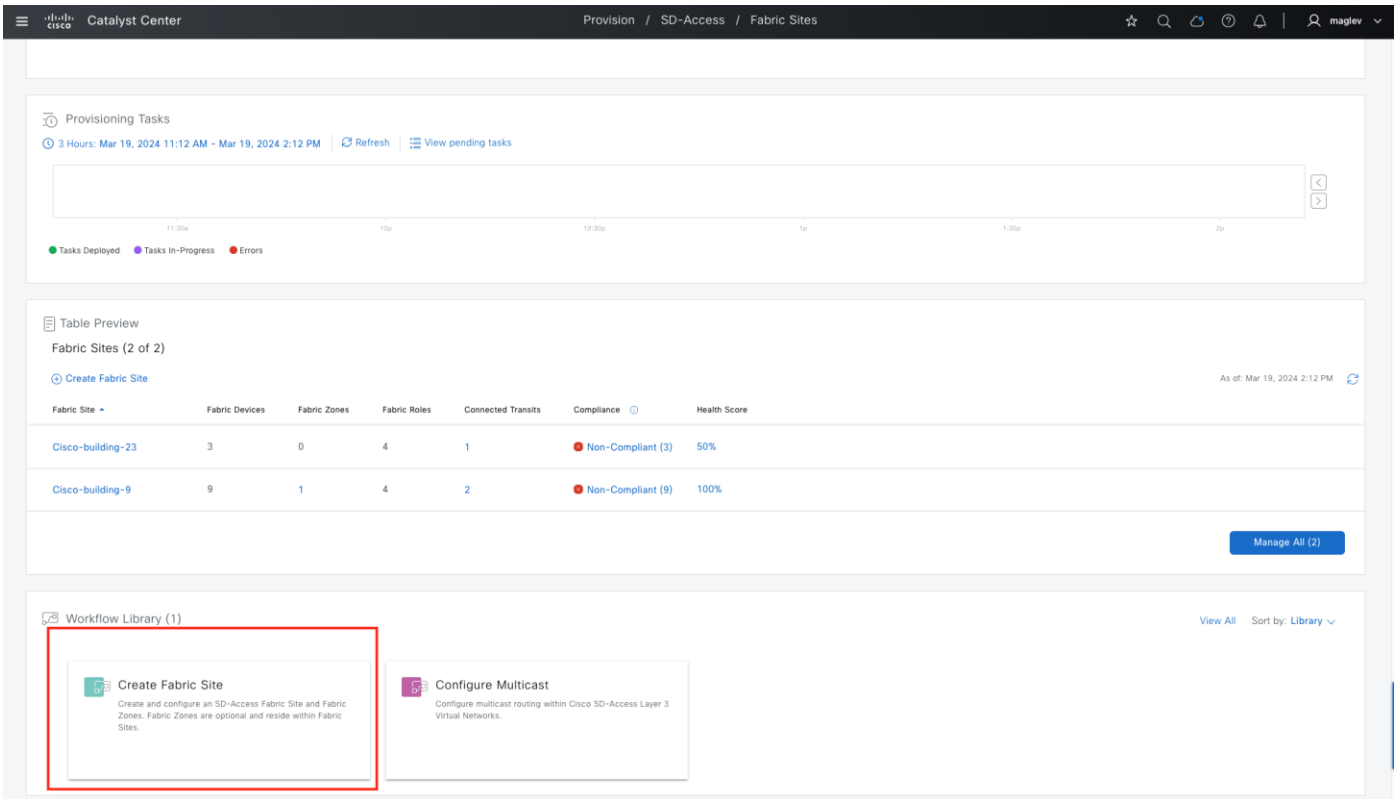
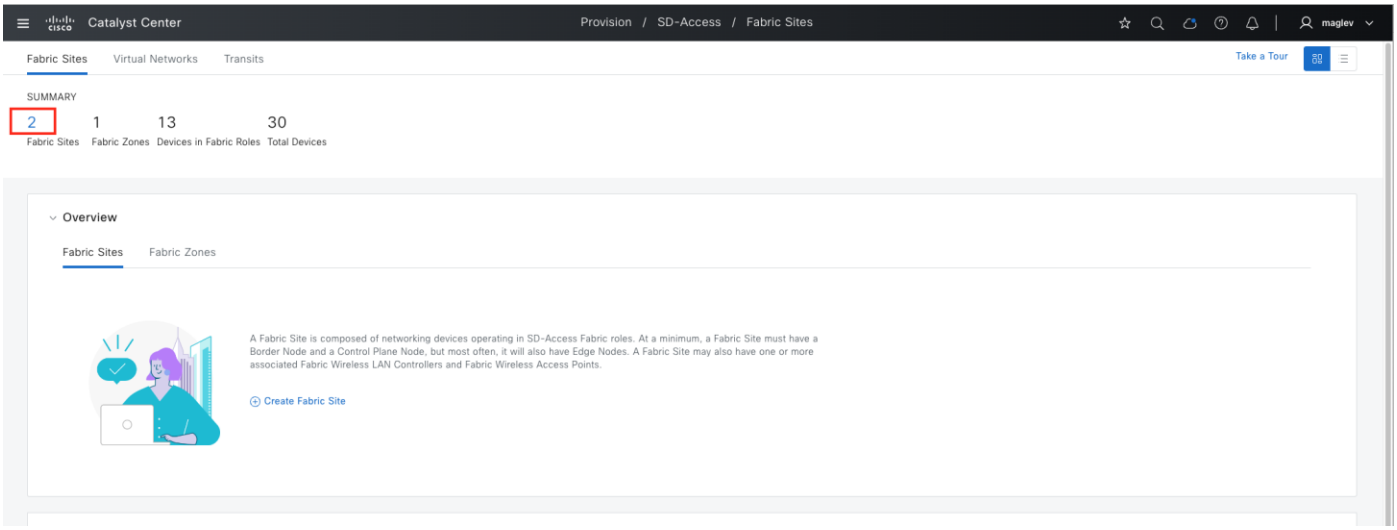



**図 31.　（場所 3）[Workflow Library] > [Create Fabric Site]**



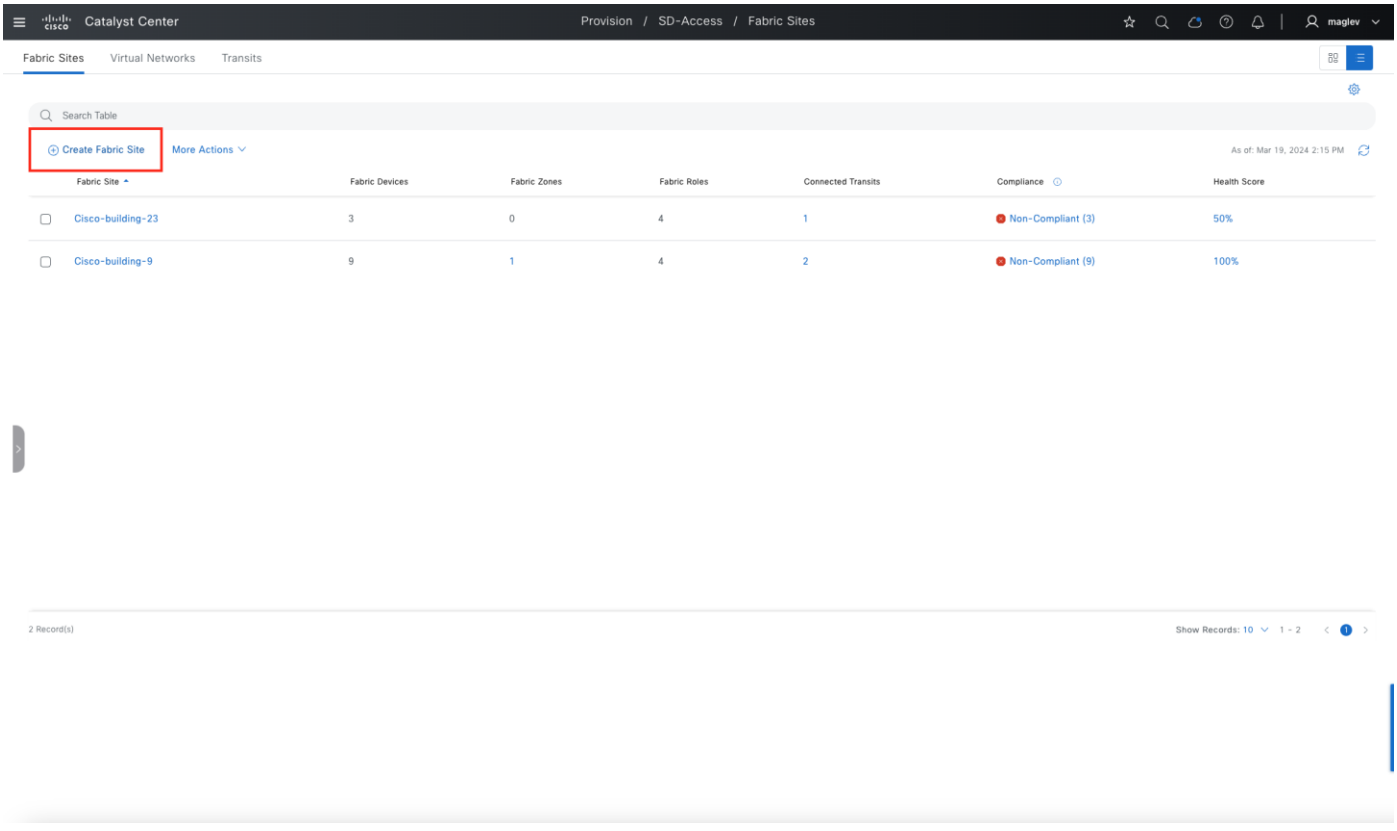

- Catalyst Center で他のファブリックサイトがすでに設定されている場合は、[Fabric Sites] ウィンドウから、[SUMMARY] の下の数字をクリックします（この例では 2 つのファブリックサイトが設定されているため、[2] をクリックします）。

**図 32.　　（場所 4a）**

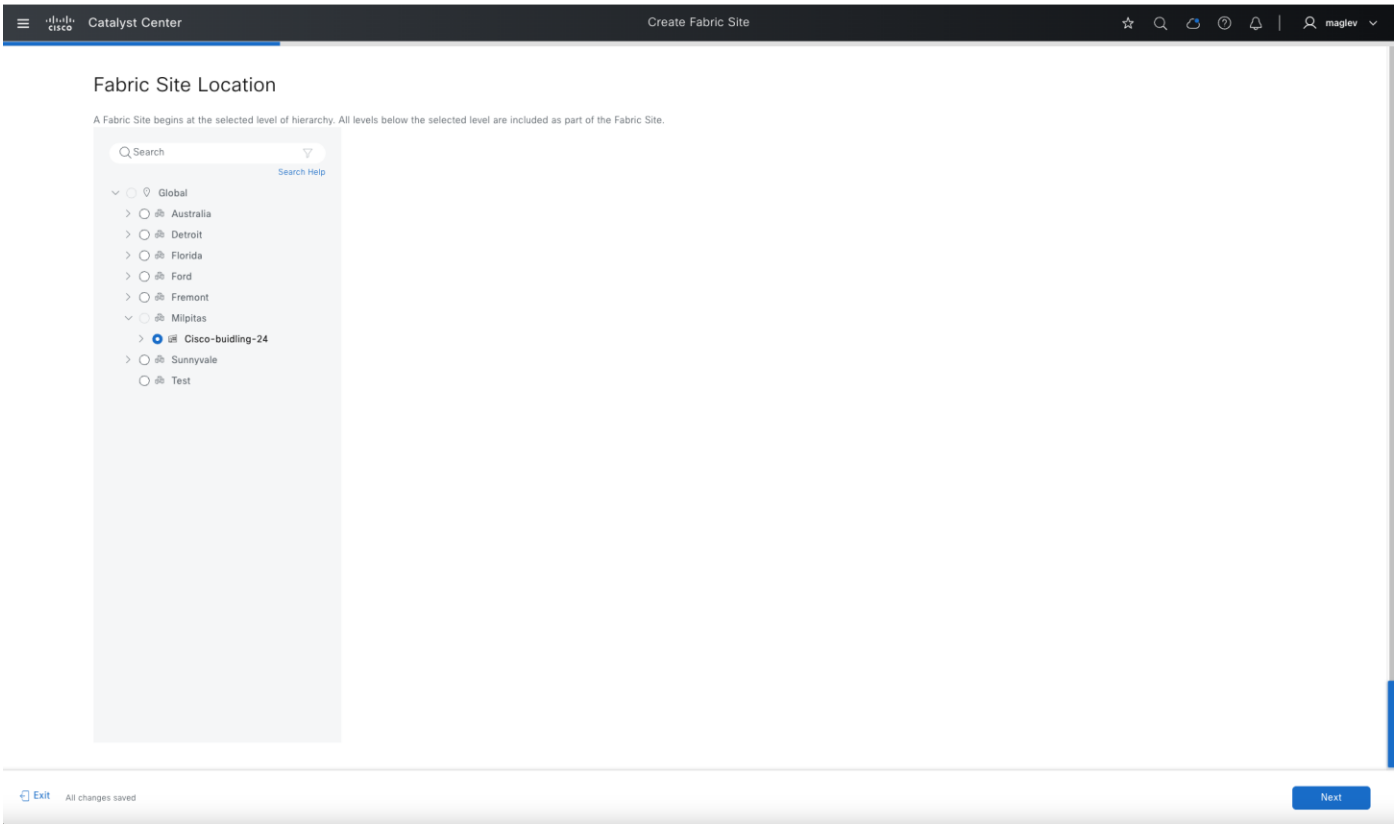



- リダイレクトされたウィンドウで、[Create Fabric Site] をクリックします。

**図 33.　　（場所 4b）**



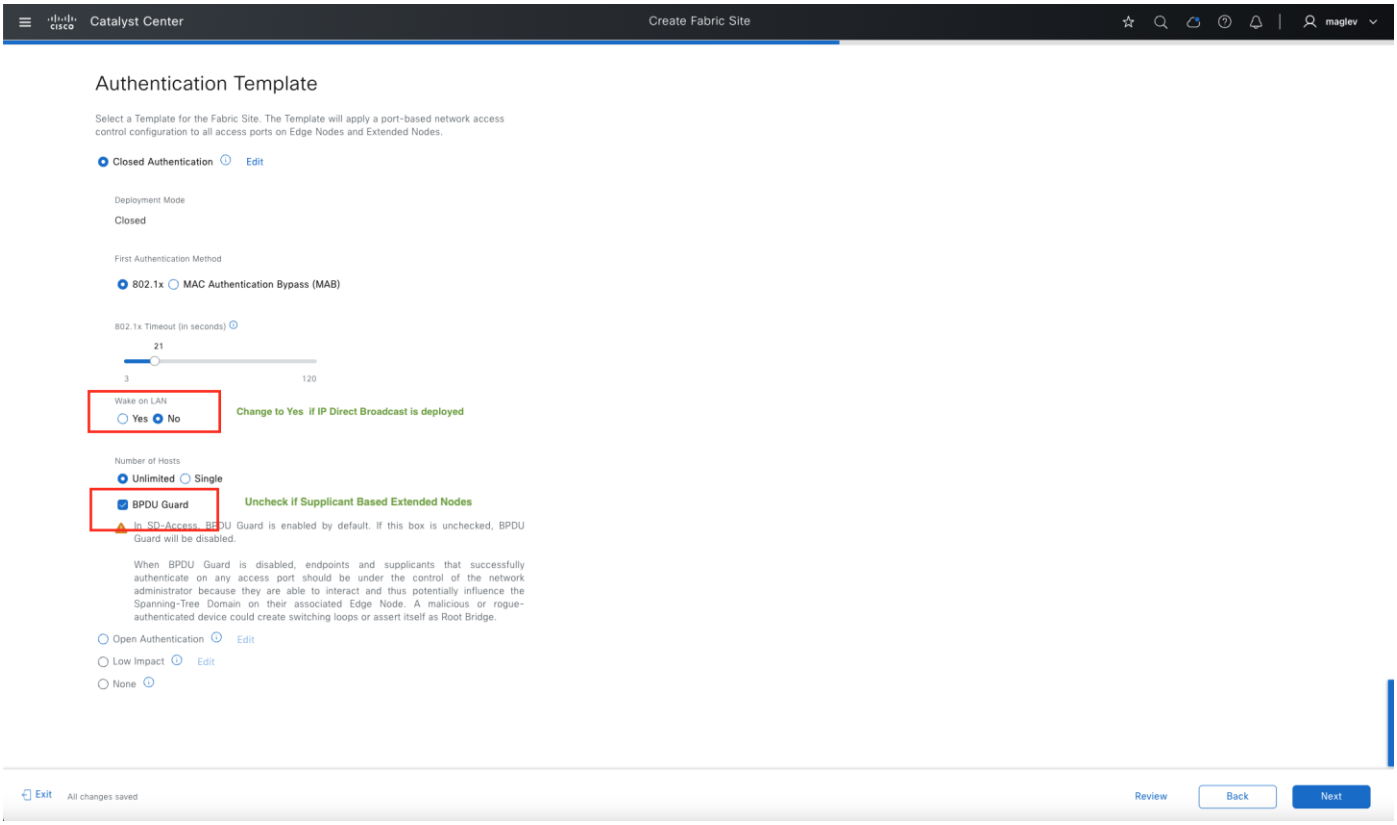
**ステップ 2.** ワークフローに従って、[Cisco-building-24] でファブリックを設定します。



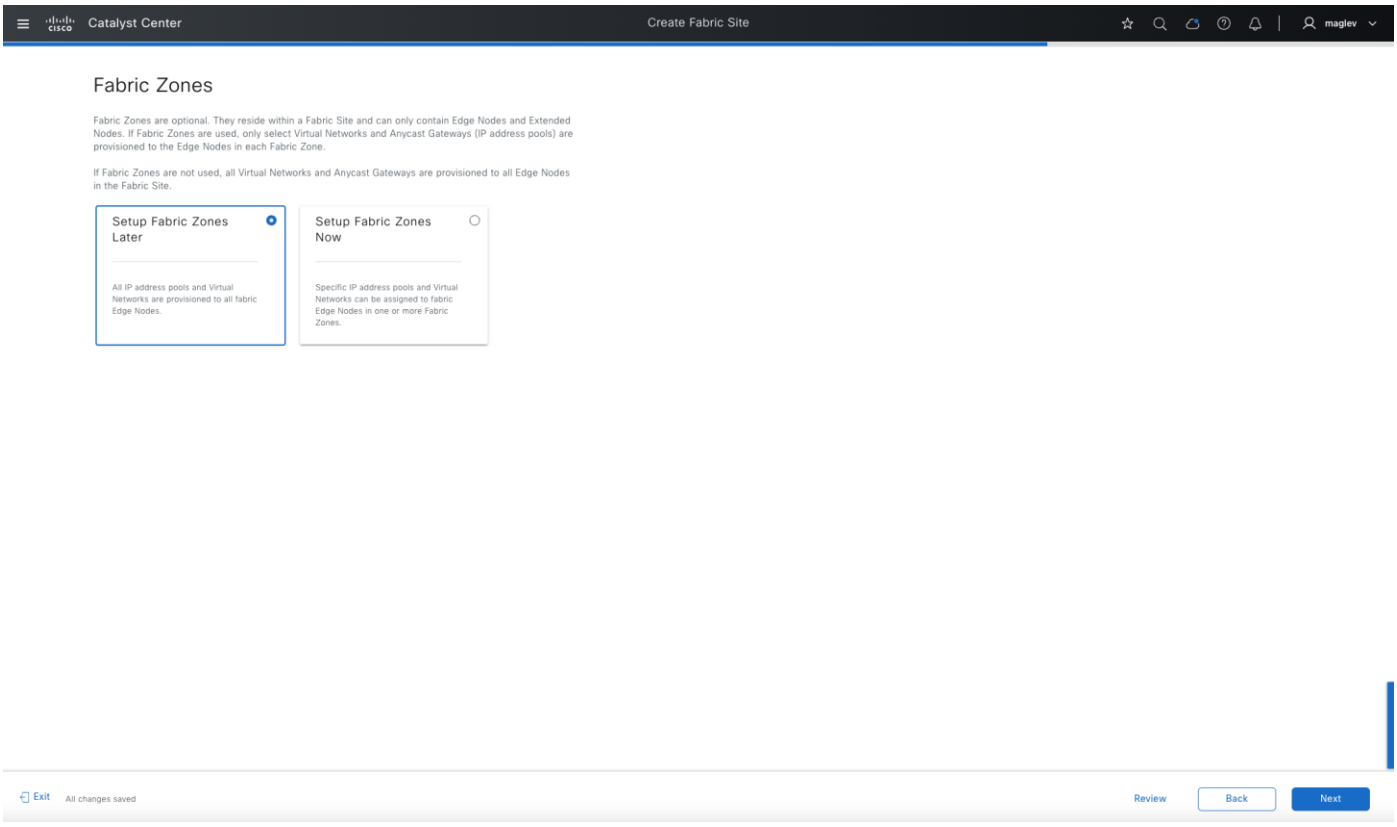

サイトレベルの認証テンプレートが必要です。サイトレベルの認証テンプレートの設定は、エッジノード（FiaB を含む）と拡張ノードのすべてのアクセスポートにプッシュされます。サポートされている Catalyst Center 認証テンプレートには次が含まれます。

- [Closed Authentication]：ネットワークアクセスには完全な 802.1x 認証が必要です
- [Open Authentication]：802.1x 認証の前に一時的なアクセスが許可されます（例：PXE、DHCP）
- [Low Impact]：MAB 認証
- [None]：ネットワークアクセスに認証は必要ありません

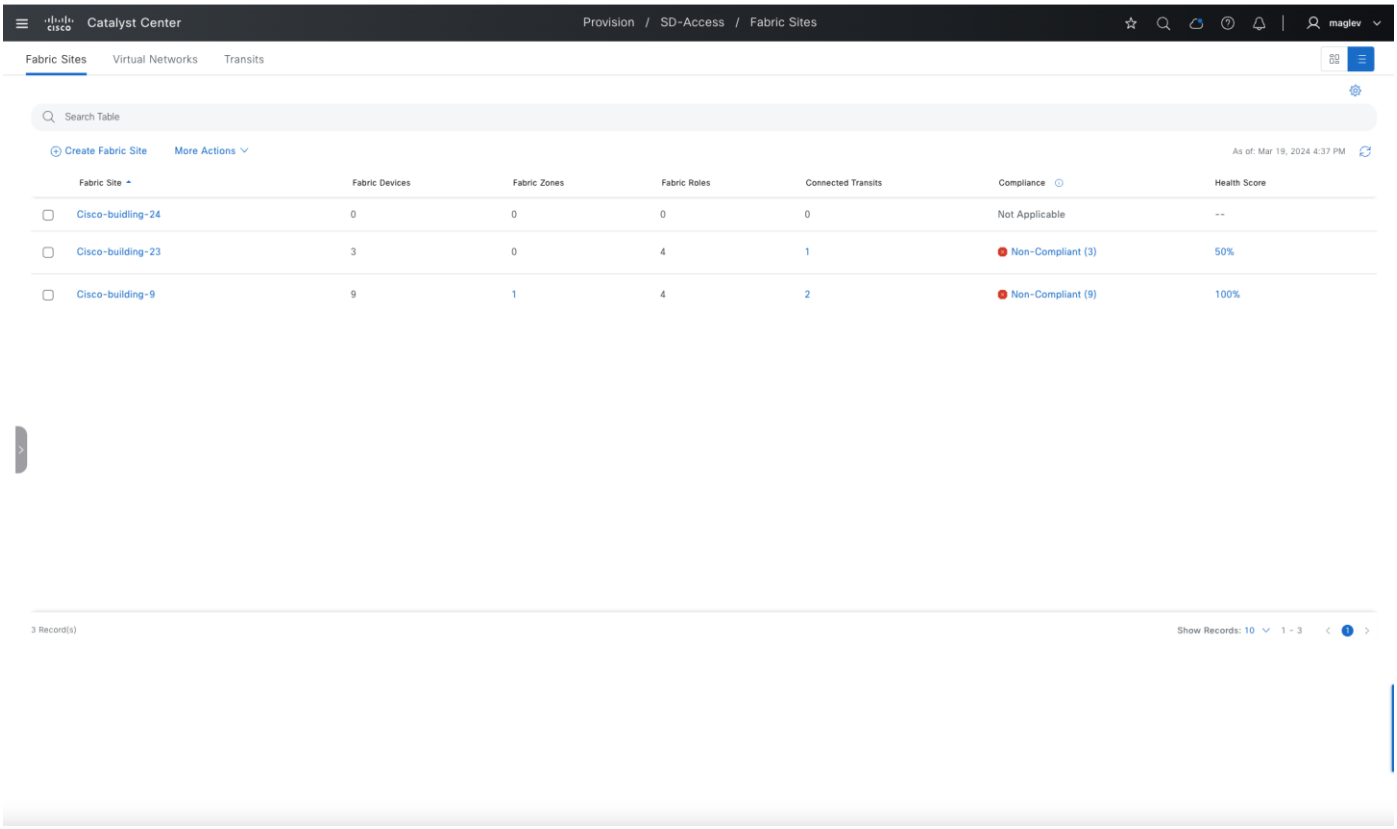
[Closed Authentication]、[Open Authentication]、および [Low Impact] のパラメータは変更できます。IP ダイレクトブロードキャストやサプリカントベースの拡張ノード（SBEN）などの特定の Cisco SD-Access 機能では、[Closed Authentication] のパラメータを変更する必要があります。サイトレベルの認証テンプレートとパラメータは、Day-*N* 運用で後で変更できます（Cisco SD-Access ネットワークの Day-*N* 運用を参照してください）。




ファブリックゾーンは、ファブリックサイトを作成するのと同じワークフローで設定することも、後で個別に設定することもできます（手順 **2** で説明）。



ファブリックを有効にしても、デバイスに設定はプッシュされません。タスクを送信すると、**Cisco-buidling-24** が正式なファブリックサイトになります。

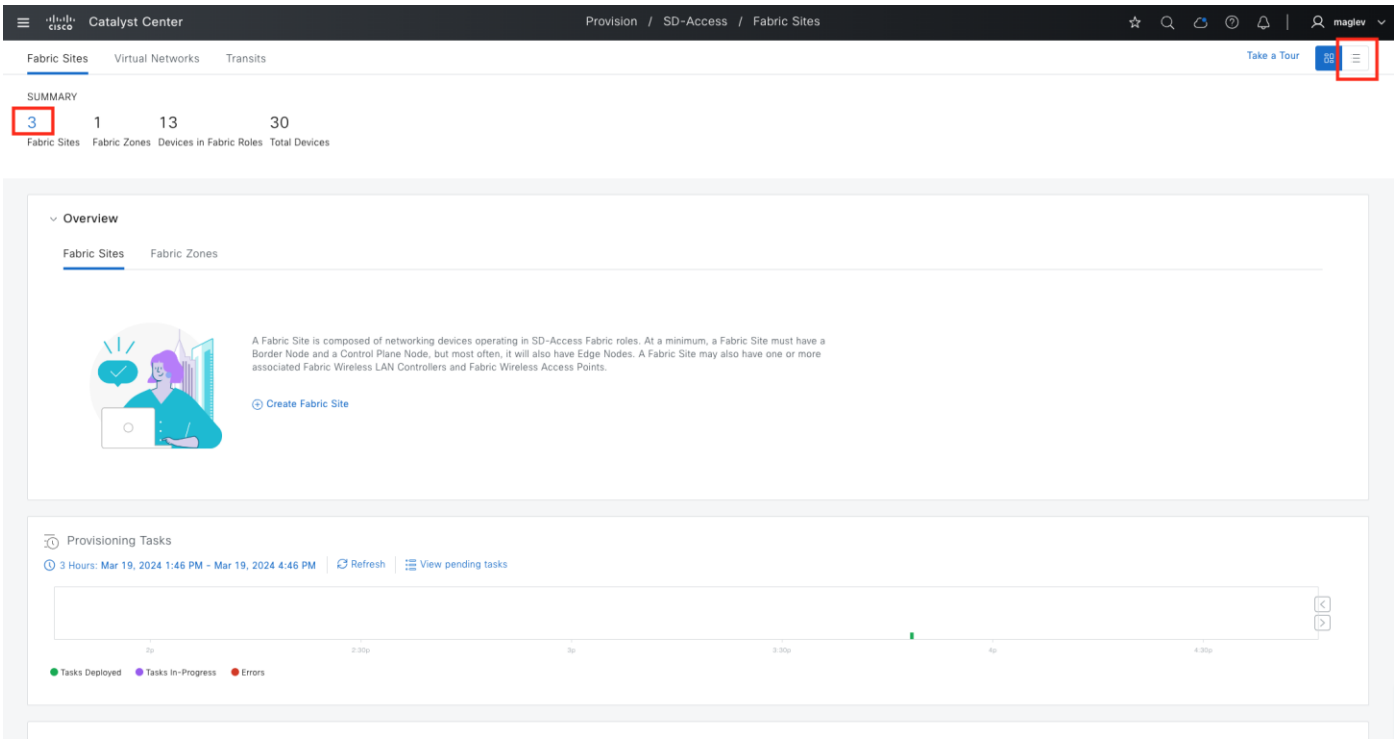



## 手順 2。 ファブリックゾーンの設定

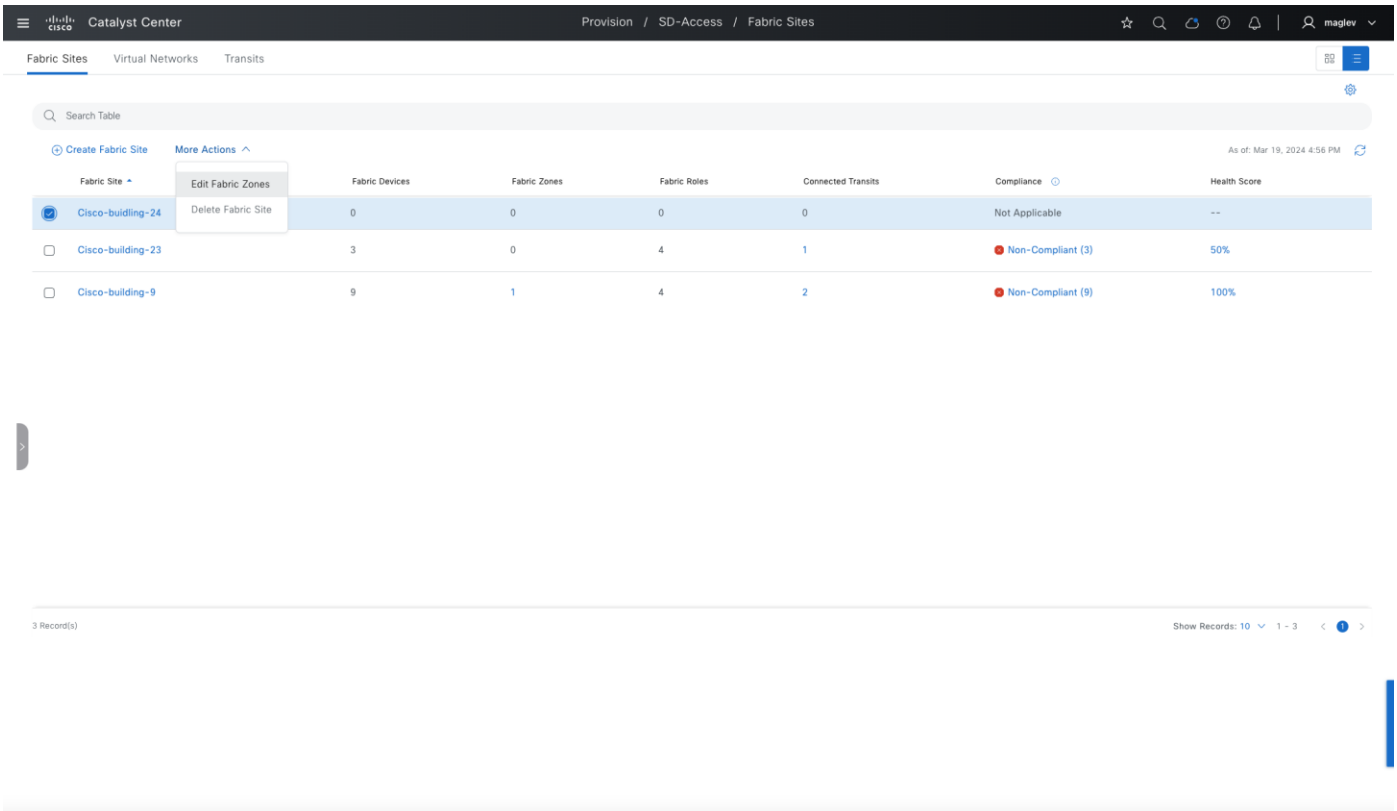
ファブリックゾーンは、ファブリックサイトと一緒に設定することも、ファブリックデバイスの有無にかかわらず後で設定することもできます。サイト階層では、**Cisco-buidling-24** がファブリックサイトとして設定されます。ファブリックゾーンは、**Floor-1** や **Floor-2** などの下位レベルで有効にすることができます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Fabric Sites] の順に選択します。

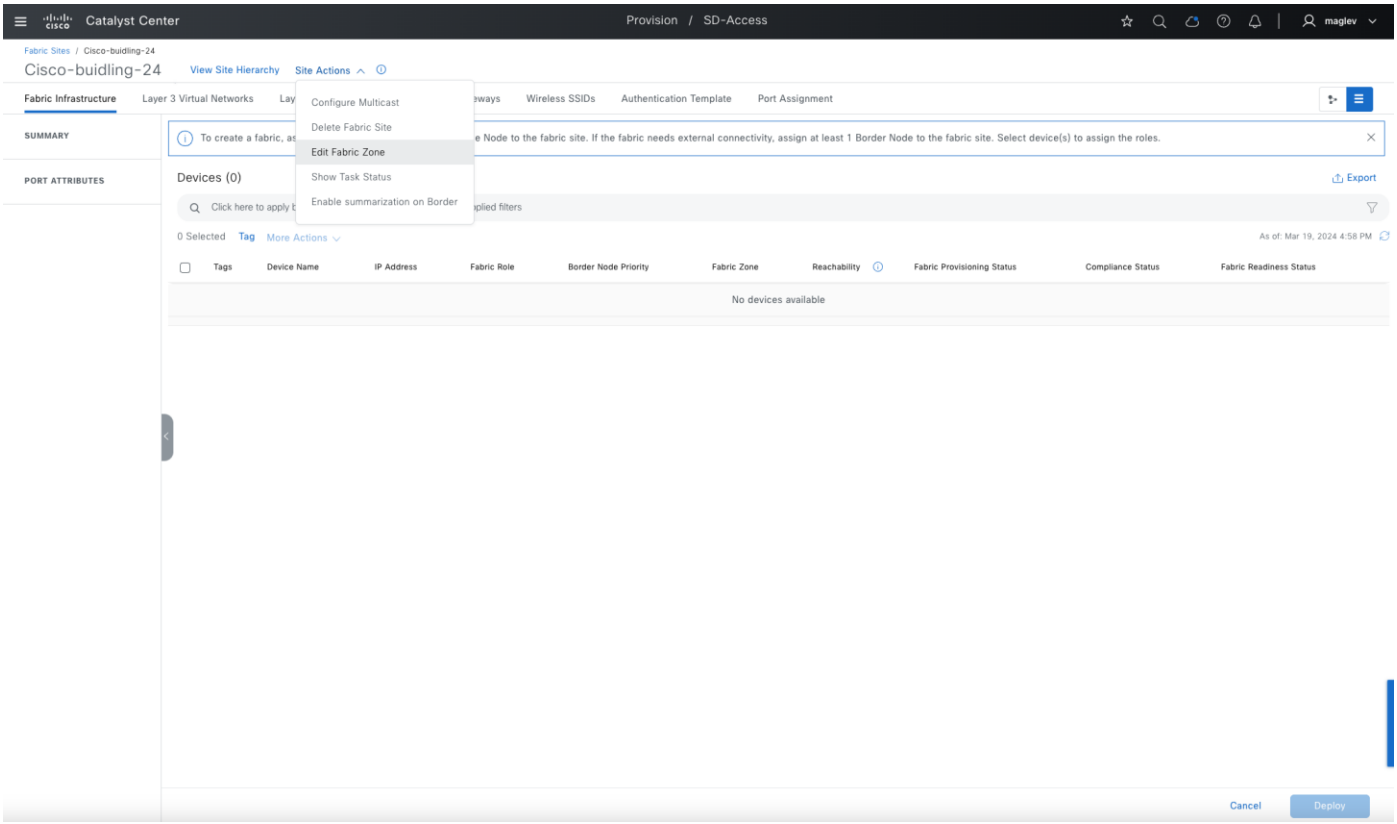
**ステップ 2.** デフォルトの [SUMMARY] ビューウィンドウで、[3] をクリックしてファブリック サイト テーブル ビューに移動します。または、右上のテーブルビューアイコンをクリックします。



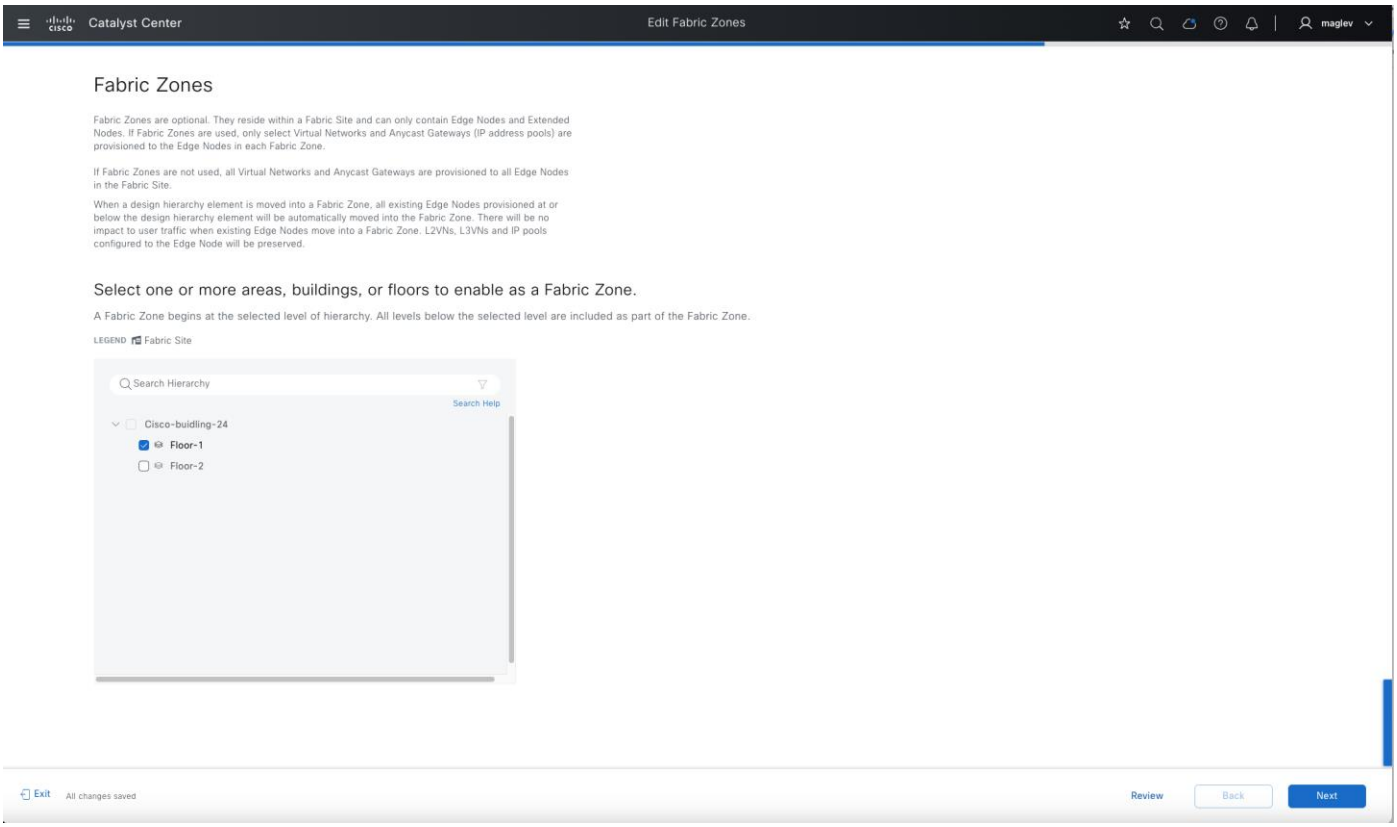

**ステップ 3.** テーブルビューで [Cisco-building-24] をクリックし、[More Actions] > [Edit Fabric Zones] の順に選択します。



**ステップ 4.** オプションで、[Cisco-building-24] > [Site Actions] > [Edit Fabric Zone] の順に選択します。

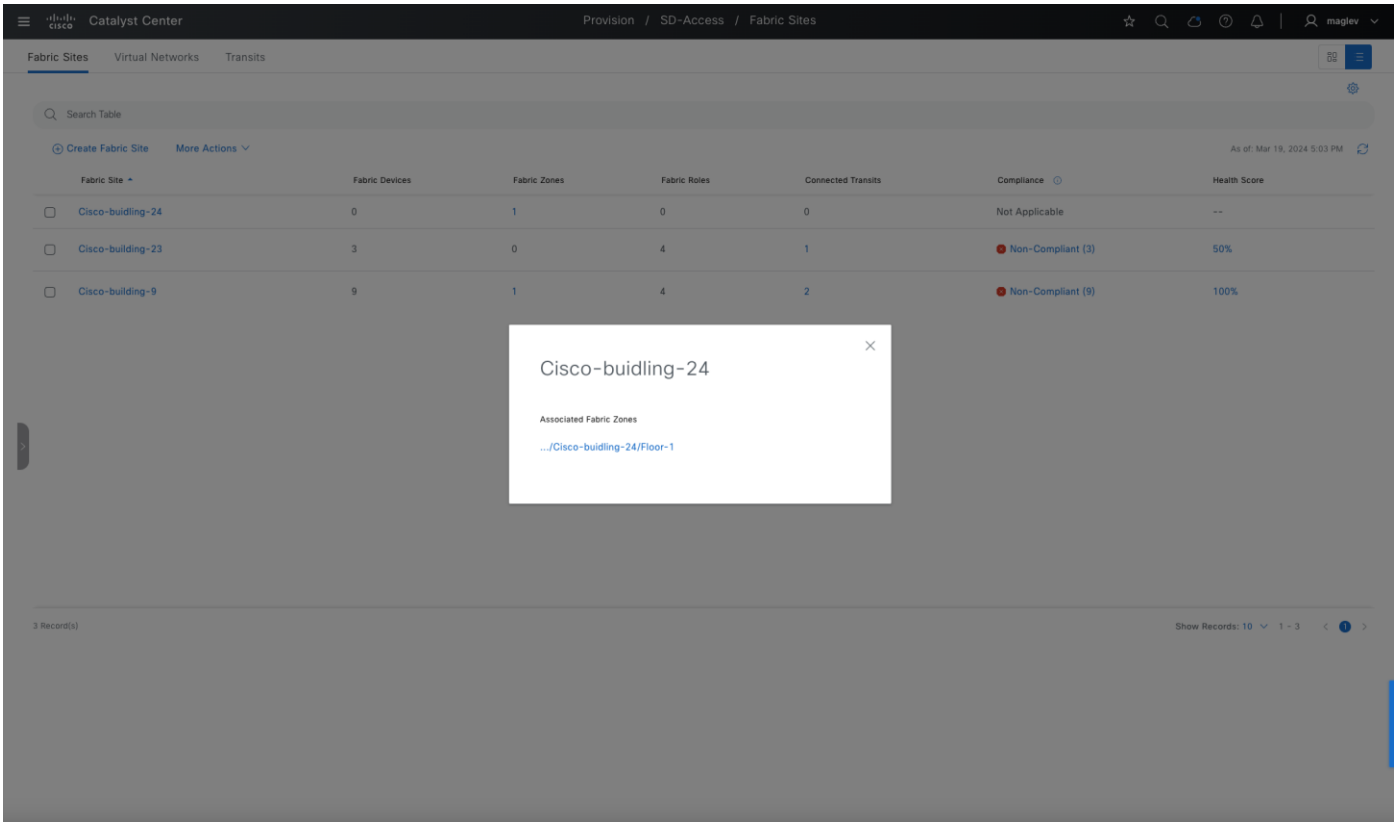



**ステップ 5.** [Fabric Zone] ウィンドウで、[Floor-1] を設定します。



**ステップ 6.** ワークフローを完了し、テーブルビューに戻ります。

**ステップ 7.** [Cisco-building-24] で、[Fabric Zones] > [1] を選択して詳細を表示します。




## トランジットの設定

トランジットネットワークは、2 つ以上のファブリックサイトを相互に接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続します。トランジットネットワークのタイプには次のものがあります。

- IP トランジット：

  通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。

- SD-Access トランジット：

  VXLAN カプセル化で LISP を使用して、ファブリックサイトを接続します。SD-Access トランジットを使用すると、エンドツーエンド ポリシー プレーンは SGT グループタグを使用して維持されます。

## 手順 1。 Cisco SD-Access トランジットの作成

### トランジット コントロール プレーン ノード

トランジット コントロール プレーン ノードは、ファブリックドメインのすべての集約ルートを追跡し、それらのルートをファブリックサイトに関連付けます。1 つのサイトのエンドポイントからのトラフィックを別のサイトのエンドポイントに送信する必要がある場合は、どのサイトのボーダーノードにこのトラフィックを送信するかがトランジット コントロール プレーン ノードに確認されます。トランジット コントロール プレーン ノードのロールは、各ファブリックサイトに関連付けられているプレフィックスを学習し、コントロール プレーン シグナリングを使用して Cisco SD-Access トランジットを介してこれらのサイトにトラフィックを転送することです。最大 4 つのトランジット コントロール プレーン ノードがサポートされます。

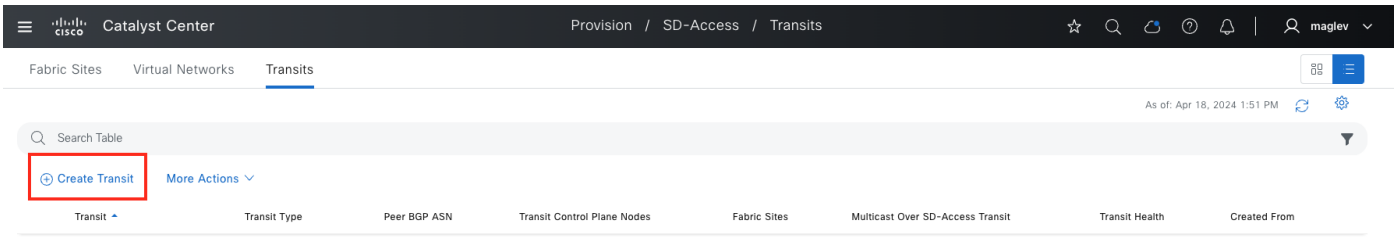
### トランジット コントロール プレーンの展開場所

トランジット コントロール プレーン ノードは、トランジットエリアに物理的に展開する必要も、独自のファブリックサイト専用にする必要もありませんが、一般的なトポロジドキュメントではしばしばその方法で表されます。このガイドの規範的な設定では、Catalyst 9500 スイッチがトランジット コントロール プレーン ノードとして使用されます。

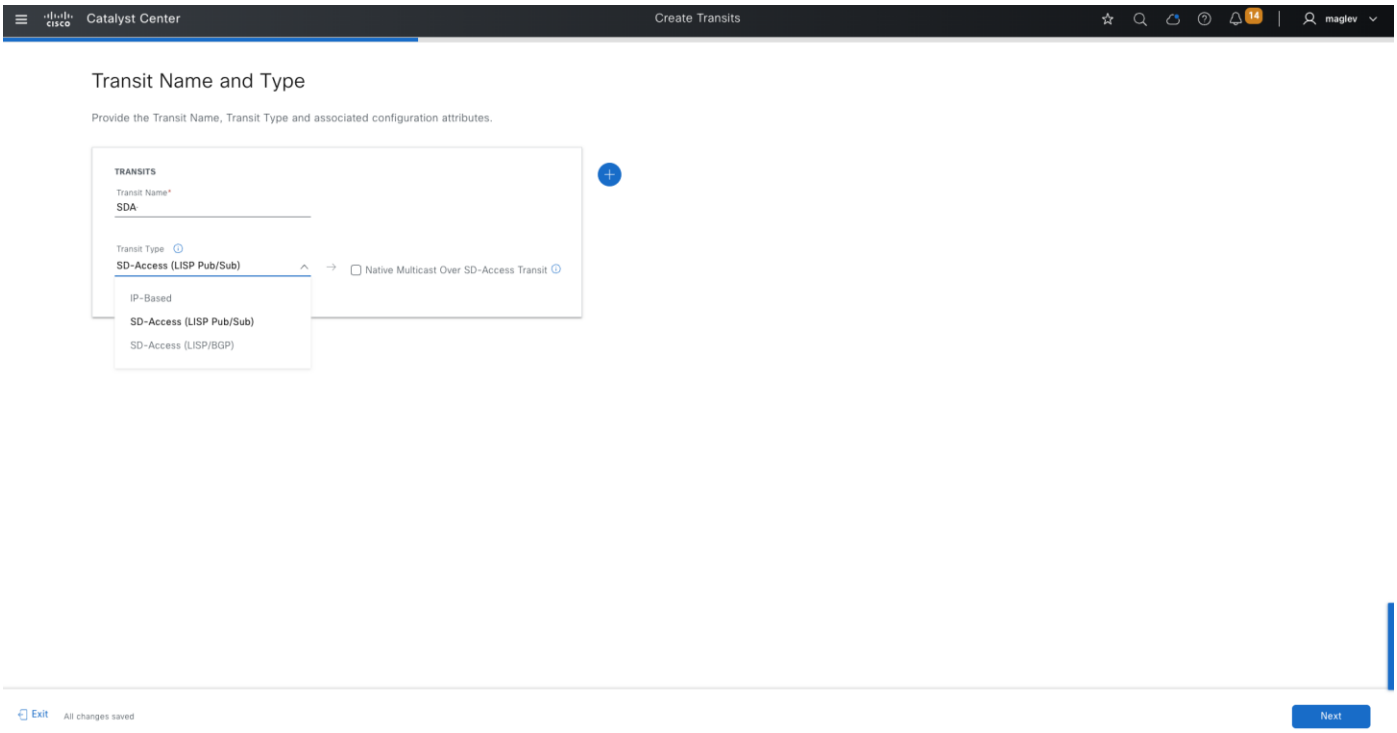
トランジットノードは、トランジットエリアを使用してのみアクセスできますが、データパケット転送パスの物理的なトランジットホップとして機能しません。代わりに、データパケットは通過しなくても、情報を照会する DNS サーバーと同様に機能します。

デバイスをコントロールプレーンノードとして使用するには、デバイスを管理およびプロビジョニングする必要があります。「デバイスの検出およびプロビジョニング」を参照してください。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Transits] の順に選択し、右上のテーブルビューアイコンをクリックして [Transits] タブをクリックし、[Create Transits] をクリックしてワークフローを開始します。



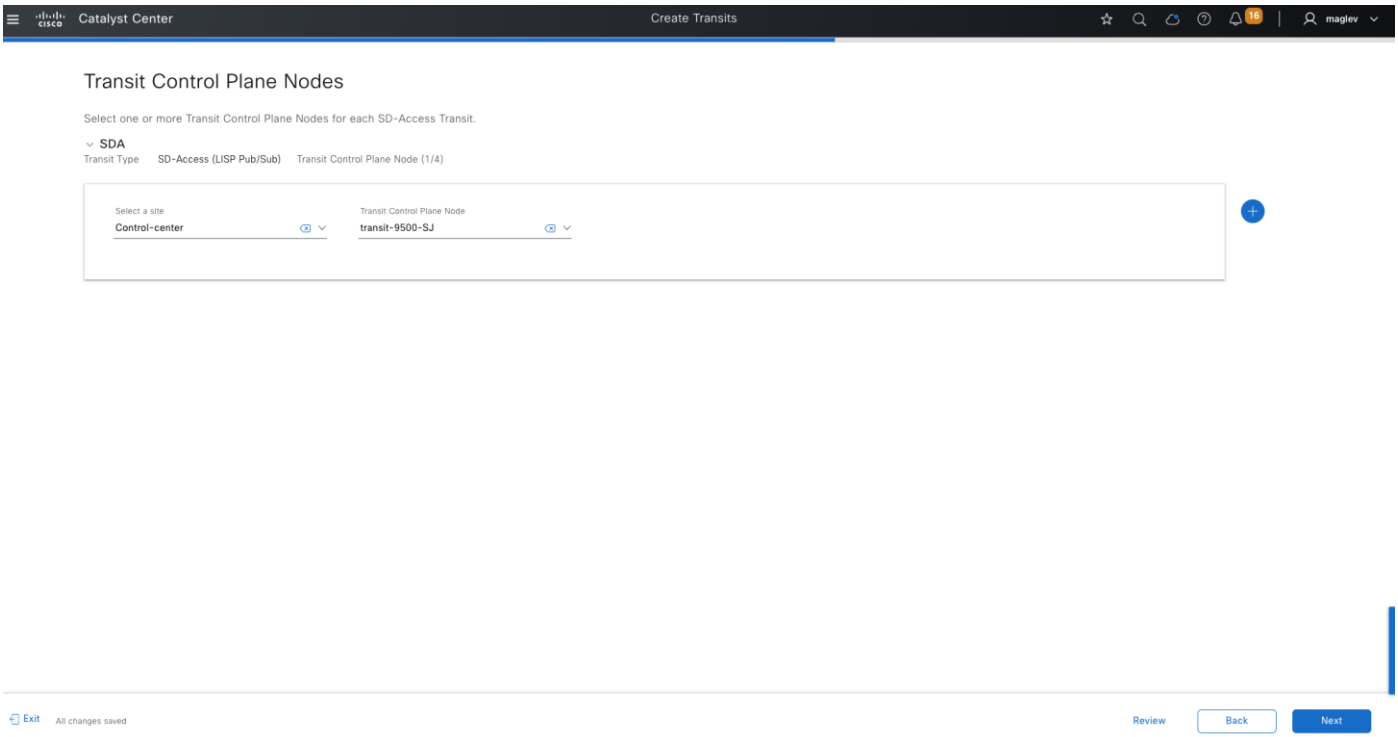
**ステップ 2.** [Transit Name] フィールドに「SDA」と入力し、[Transit Type] > [SD-Access (LISP Pub/Sub)] を選択して、[Next] をクリックします。



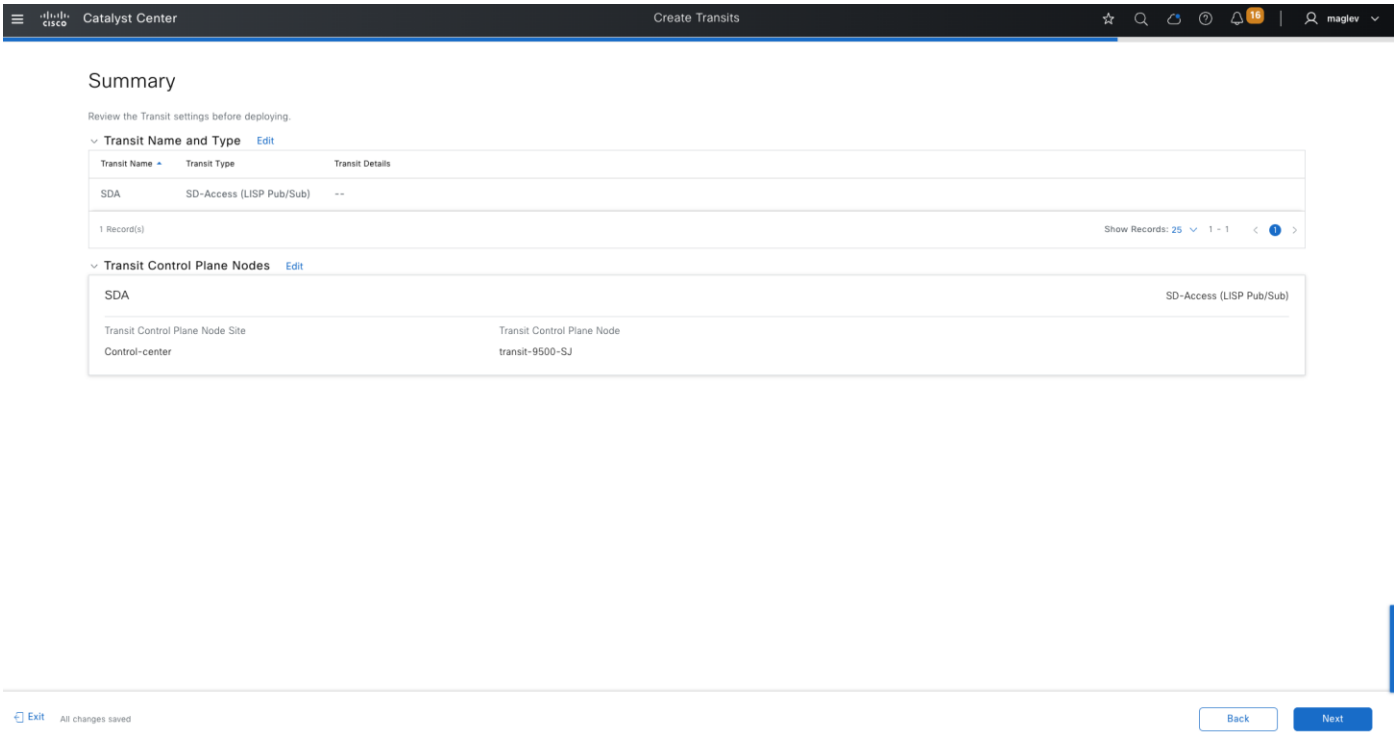

**技術的なヒント：**

1. Cisco SD-Access トランジットを介したネイティブマルチキャストは、必要に応じて、Day-*N* 運用で後で有効にすることができます。
2. Cisco SD-Access のトランジットタイプは、ファブリックサイトタイプと同じである必要があります。
3. Cisco SD-Access トランジットを使用した LISP Pub/Sub および LISP/BGP サイトの接続はサポートされません。

**ステップ 3.** Catalyst 9500 デバイスがプロビジョニングされているサイトを選択し、それを**トランジット コントロール プレーン ノード**として選択して、[Next] をクリックします。



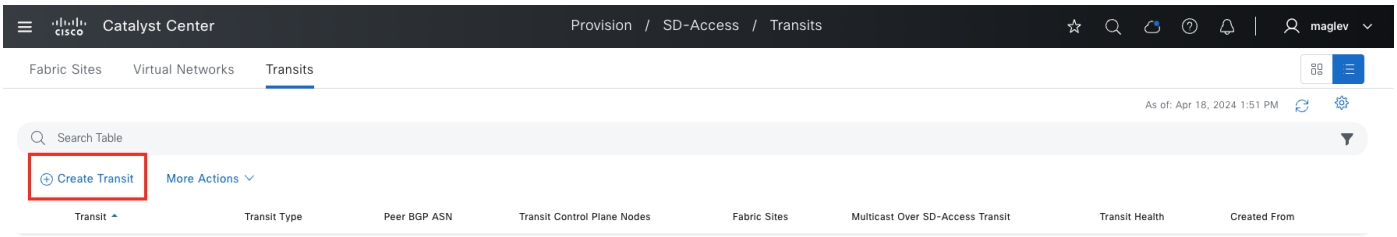

**ステップ 4.** [Summary] ウィンドウの情報を確認してから [Next] をクリックし、ワークフローを完了してタスクを展開します。



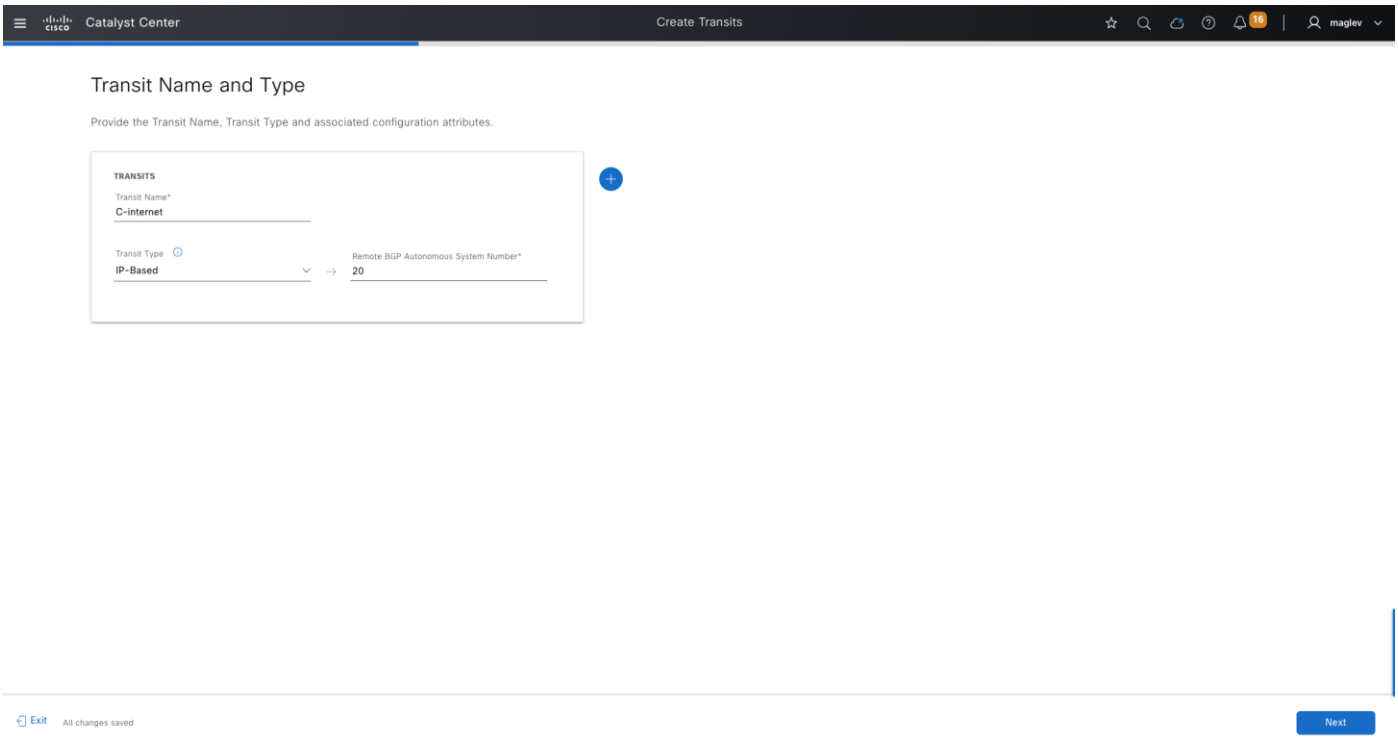
## 手順 2。　IP トランジットの作成

IP ベースのトランジットは、リモート BGP 自律システム（AS）を表します。通常、リモート BGP AS はピアデバイスで設定されます。共有サービスのルートまたはデフォルトルートは、BGP プロトコルを使用してピアデバイスからボーダーデバイスにアドバタイズされます。ローカル BGP AS は、後のステップでプロビジョニングするファブリックボーダーの一部として設定されます。

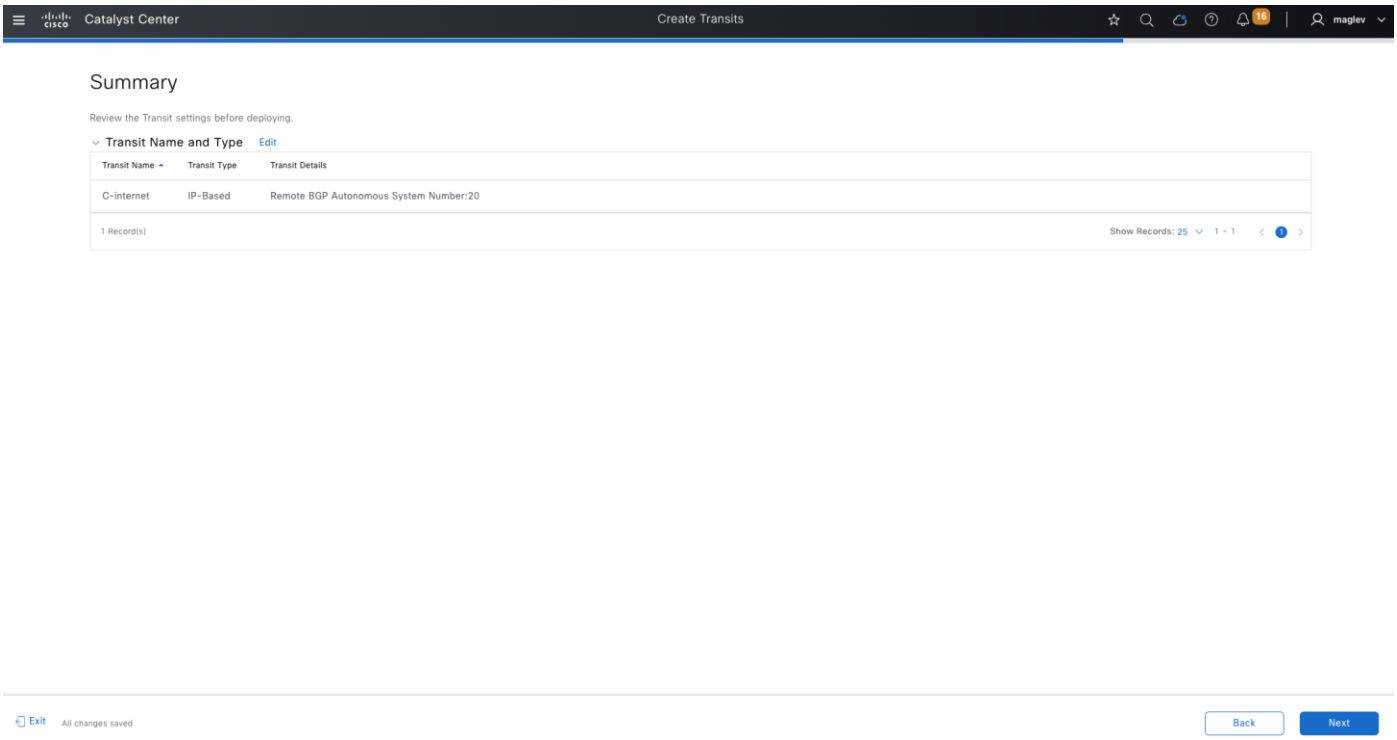
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Transits] の順に選択し、右上のテーブルビューアイコンをクリックして [Transits] タブをクリックし、[Create Transits] をクリックしてワークフローを開始します。




**ステップ 2.** [Transit Name] に入力し、[Transit Type] > [IP-Based] の順に選択し、AS 番号を（ピアデバイス上で）指定して [Next] をクリックします。



**ステップ 3.** [Summary] ウィンドウの情報を確認してから [Next] をクリックし、ワークフローを完了してタスクを展開します。




## VN の設定

レイヤ 3 VN とレイヤ 2 VN は、グローバルレベルから設定してファブリックサイトに追加するか、ファブリックサイトから直接設定できます。

レイヤ 3 VN の **DEFAULT_VN** と **INFRA_VN** は、Catalyst Center によって作成されます。**INFRA_VN** は、グローバル ルーティング テーブルにマッピングされ、AP と拡張ノードに使用されます。

レイヤ 3 VN を作成すると、レイヤ 2 VN も作成されます。レイヤ 3 が必要ない場合、Catalyst Center ワークフローを使用して純粋なレイヤ 2 VN を作成できます。

このセクションでは、レイヤ 3 VN の **VN_Guest** と **VN_EMP** が作成され、**INFRA_VN** とともに **Cisco-building-24** に追加されます。VLAN 4000 設定の純粋なレイヤ 2 VN **ゲスト**が作成され、**Cisco-buidling-24** に追加されます。

### 手順 1。 レイヤ 3 VN の設定、およびレイヤ 3 VN のファブリックサイトとファブリックゾーンへの追加

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Virtual Networks] の順に選択します。

**ステップ 2.** 図に示されているように、[Create Layer 3 Virtual Networks] をクリックします。または、下記の手順も実行できます。

- テーブルビューにリダイレクトするには、[SUMMARY] の下の番号をクリックします。
- 右上にあるテーブル ビュー アイコン ボタンをクリックします。

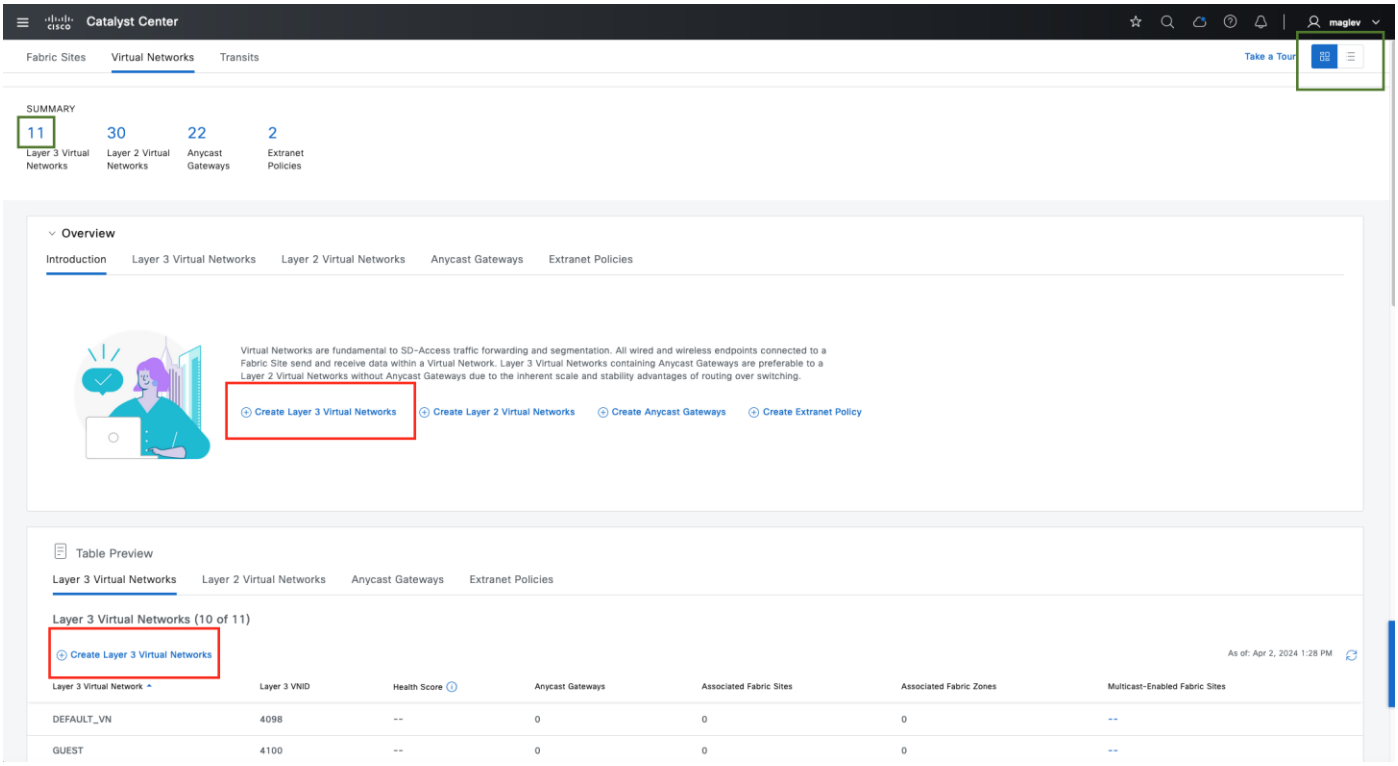
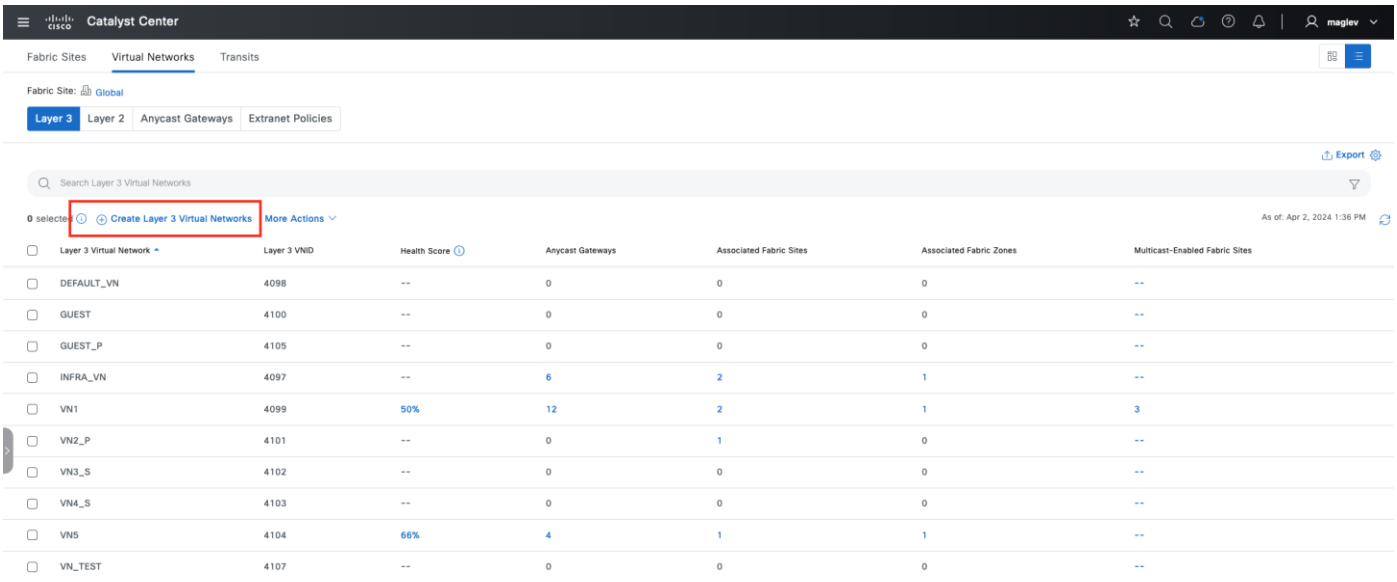
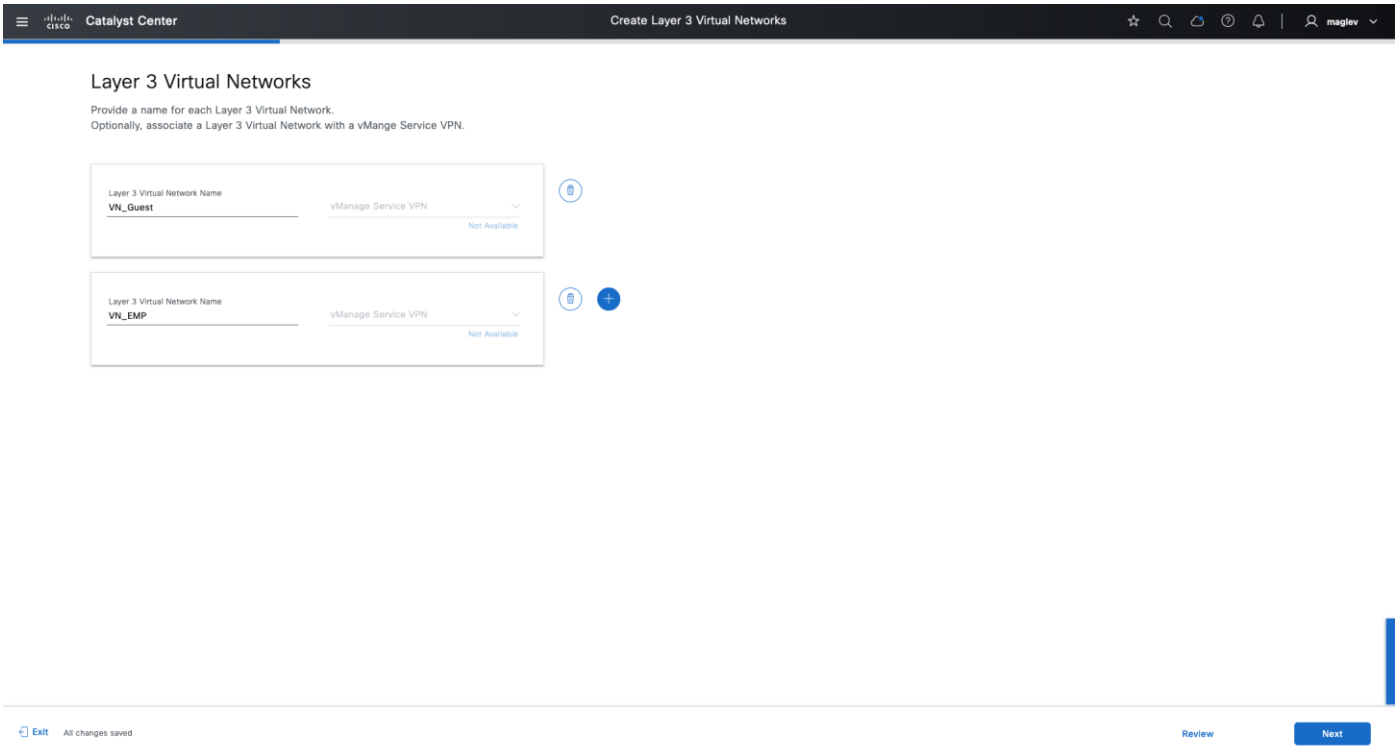


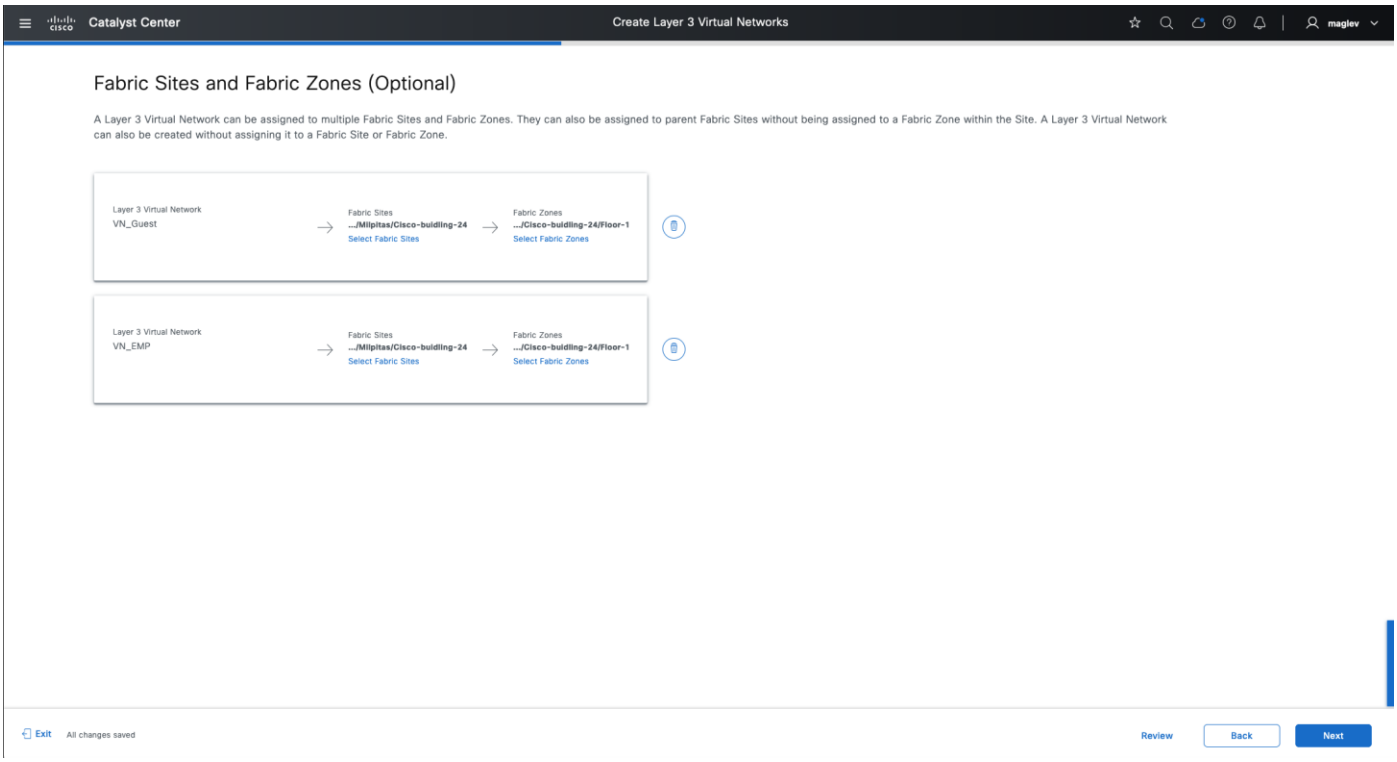

**図 34.　　テーブルビュー**



**ステップ 3.** **VN_Guest** と **VN_EMP** を作成し、[Next] をクリックします。

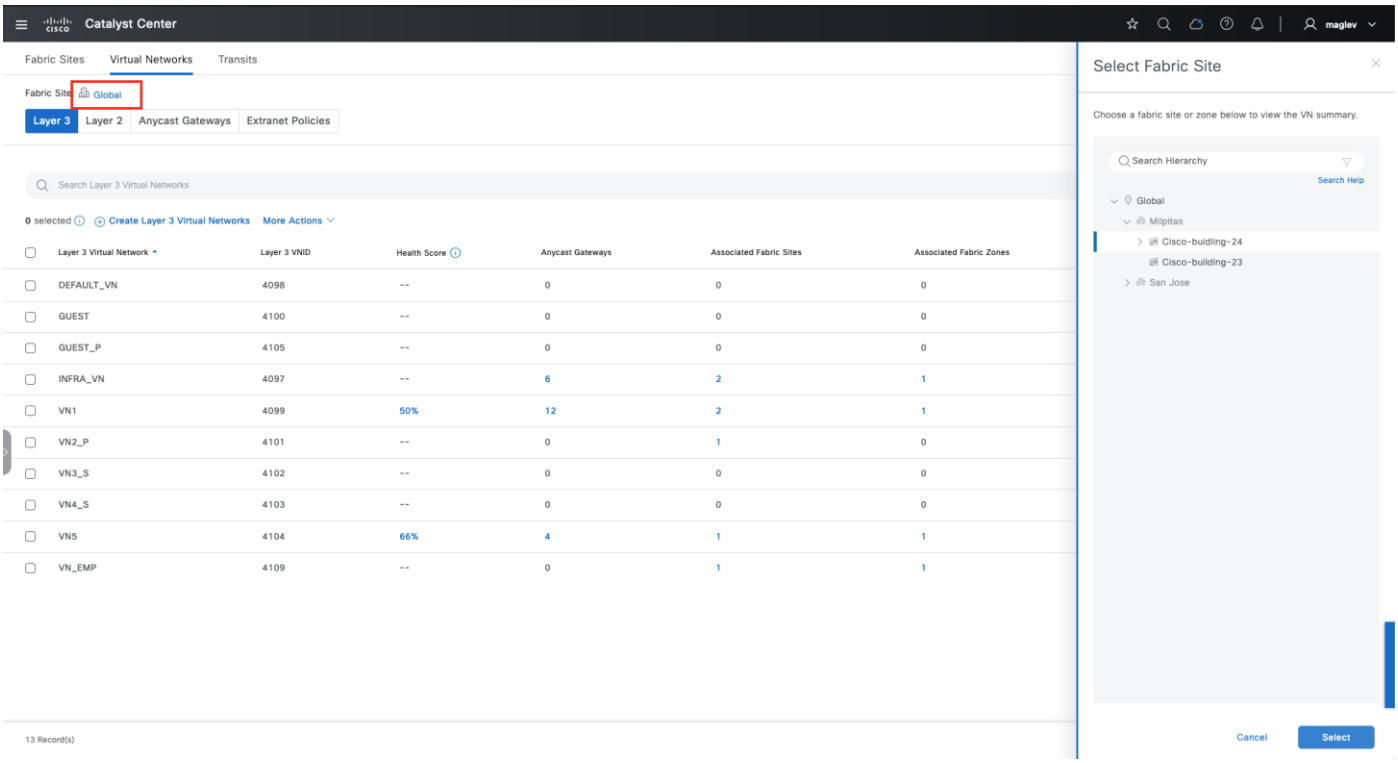



**ステップ 4.** [Fabric Site and Fabric Zone (Optional)] ウィンドウで、Cisco-building-24 と Floor-1 を追加し、[Next] をクリックしてワークフローを完了します。

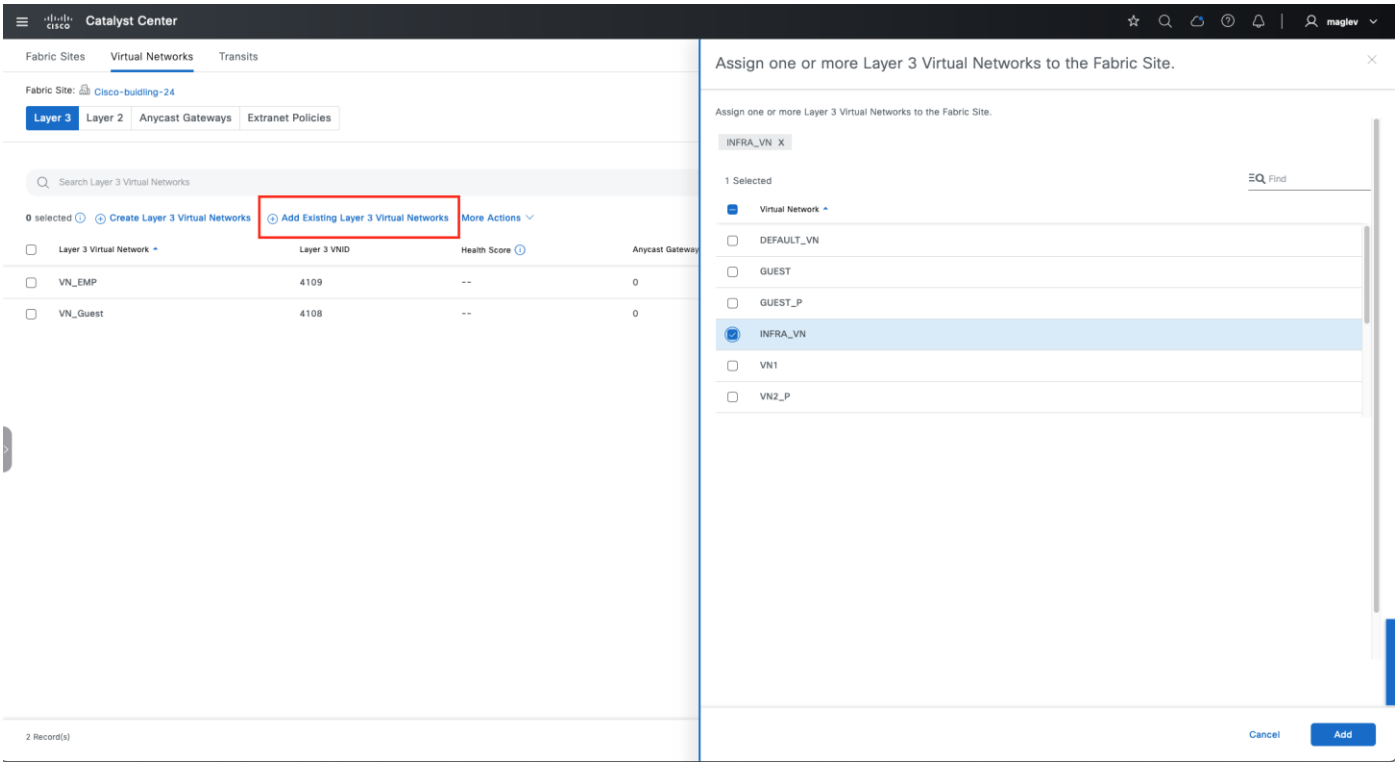



**技術的なヒント：** VN を作成しても、設定はデバイスにプッシュされません。

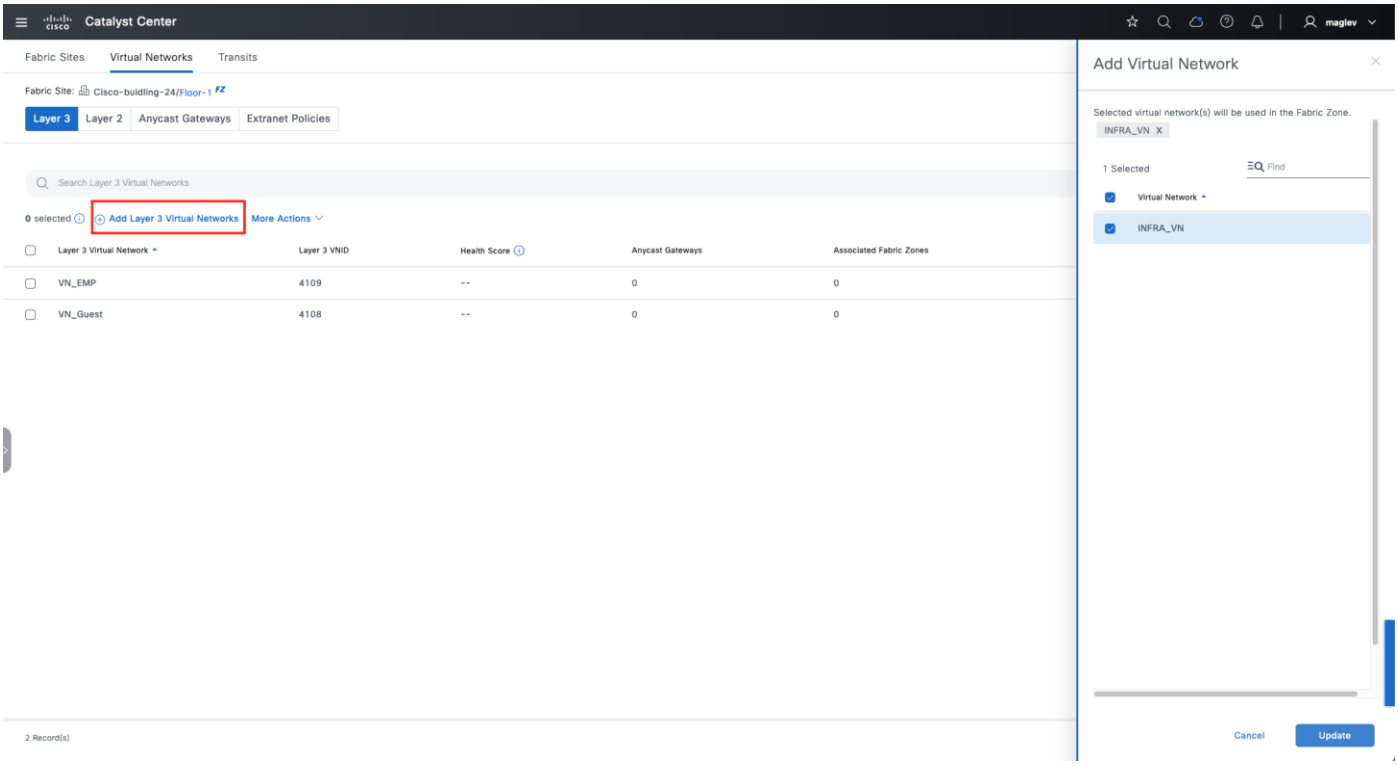
**ステップ 5.** **INFRA_VN** をファブリックサイト **Cisco-building-24** とファブリックゾーン **Floor-1** に追加するには、[Global] をクリックして [Cisco-building-24] に切り替えます。



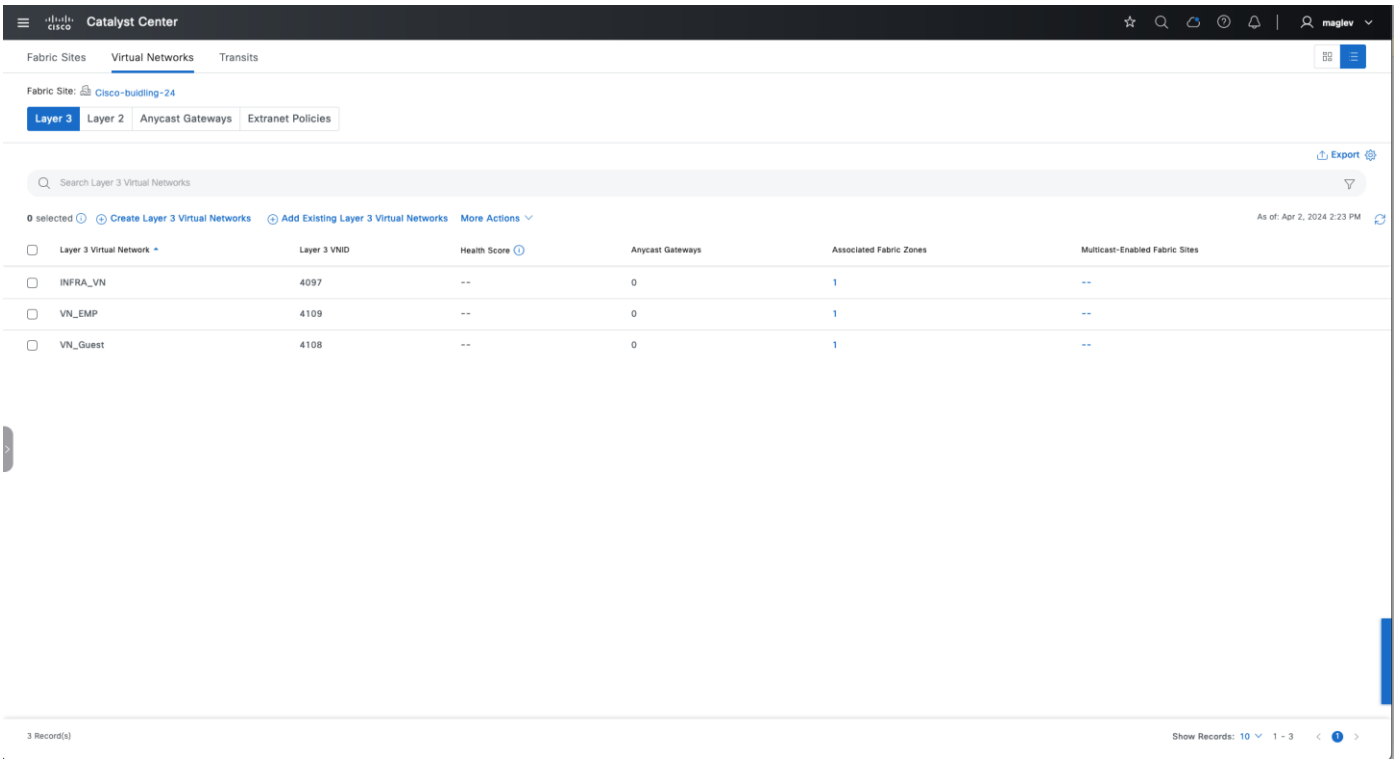

**ステップ 6.** [Add Existing layer 3 Virtual Networks] > [INFRA_VN] の順に選択し、ワークフローを終了します。



**ステップ 7.** ファブリックゾーン **Floor-1** に切り替えて、[INFRA_VN] チェックボックスをオンにします。



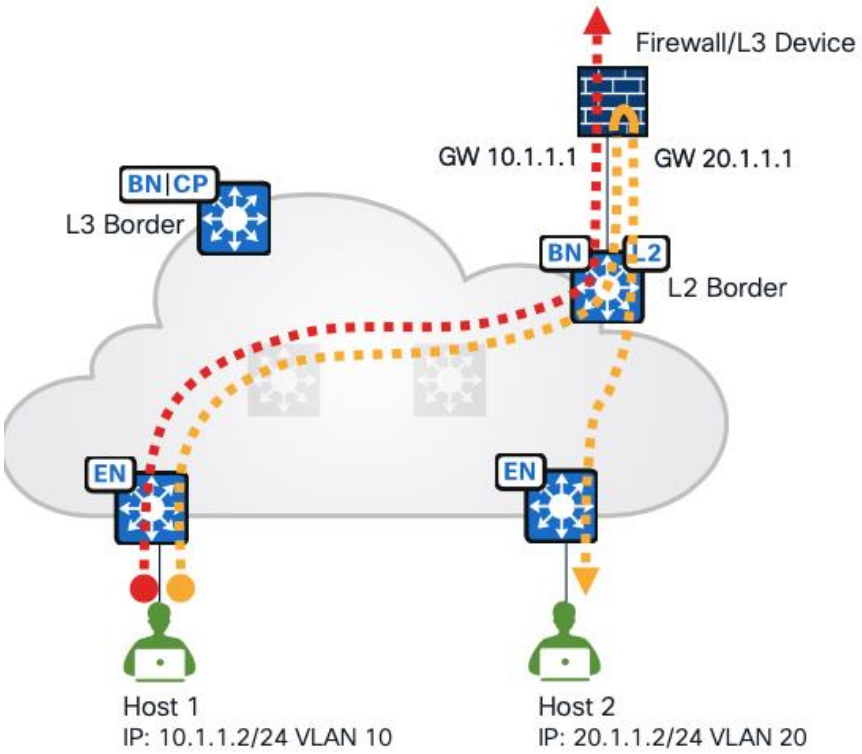

**INFRA_VN**、**VN_EMP**、および **VN_Guest** がファブリックサイトとファブリックゾーンに追加されます。



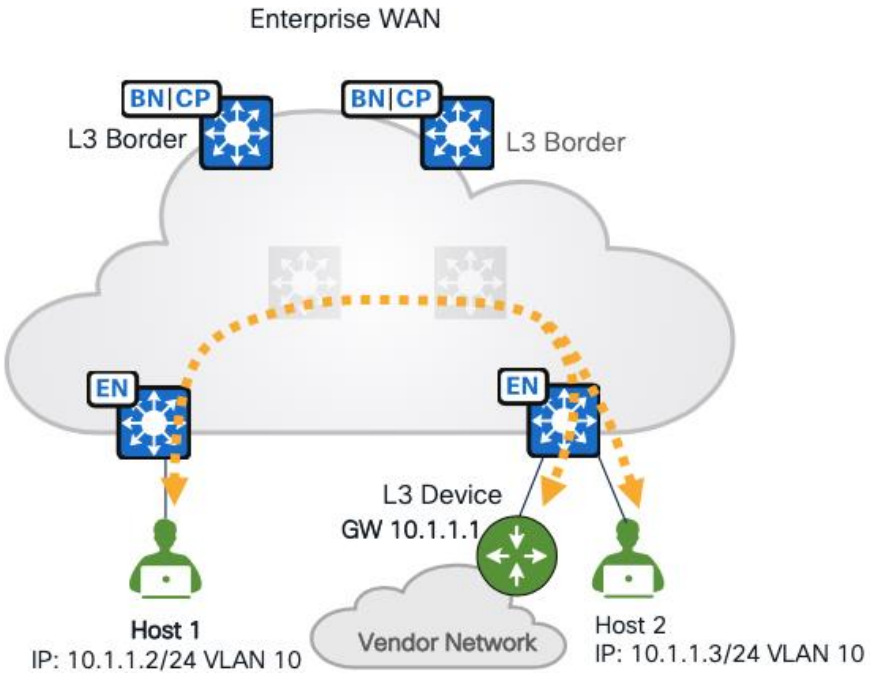
**手順 2。** レイヤ 2 VN の設定、およびレイヤ 2 VN のファブリックサイトとファブリックゾーンへの追加

レイヤ 3 VN でエニーキャストゲートウェイを作成すると、デフォルトでレイヤ 2 VN も作成されます。Catalyst Center は、主にゲートウェイがファブリックの外部にある場合に使用されるレイヤ 2 専用 VN もサポートしています。

- サブネットのゲートウェイは、ファイアウォール、またはレイヤ 2 ボーダーに接続されたレイヤ 3 デバイスにすることができます。エンタープライズ WAN へのトラフィックは、レイヤ 2 ボーダーを通過します。

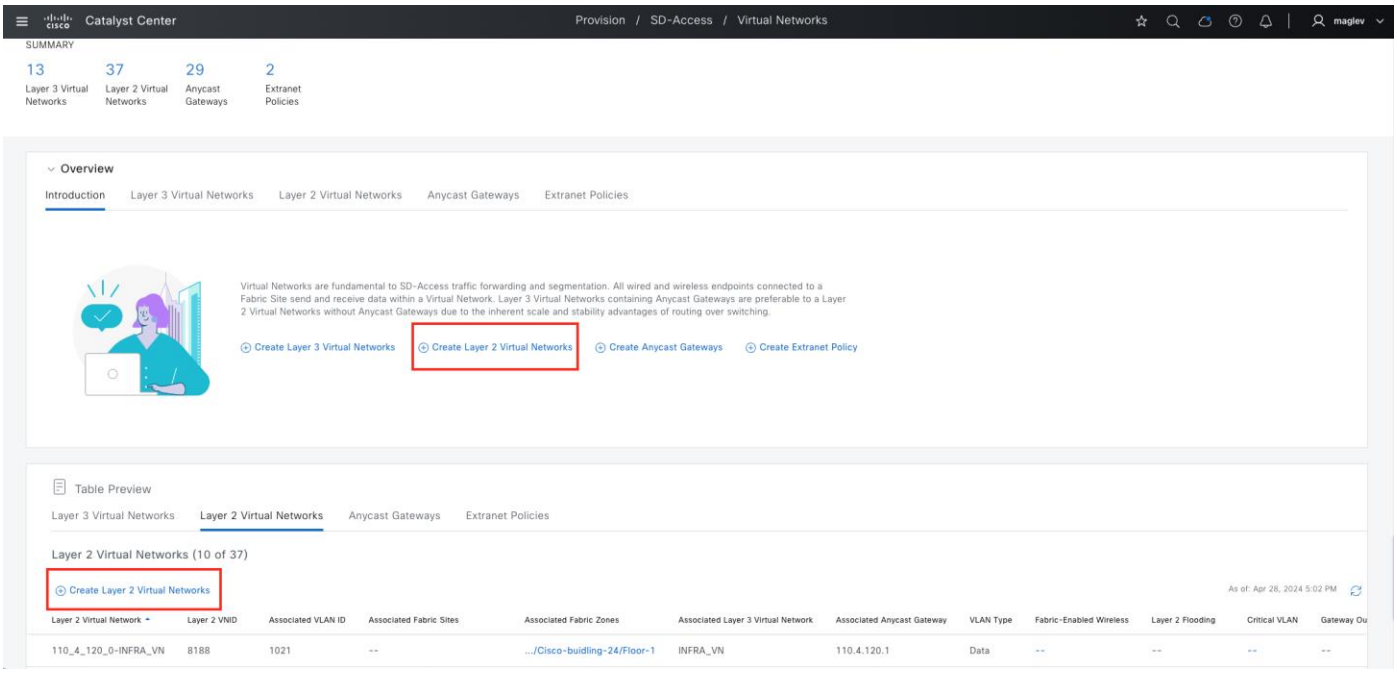



- ゲートウェイはファブリックの外部にありますが、レイヤ 3 デバイスではファブリックエッジに接続されます。

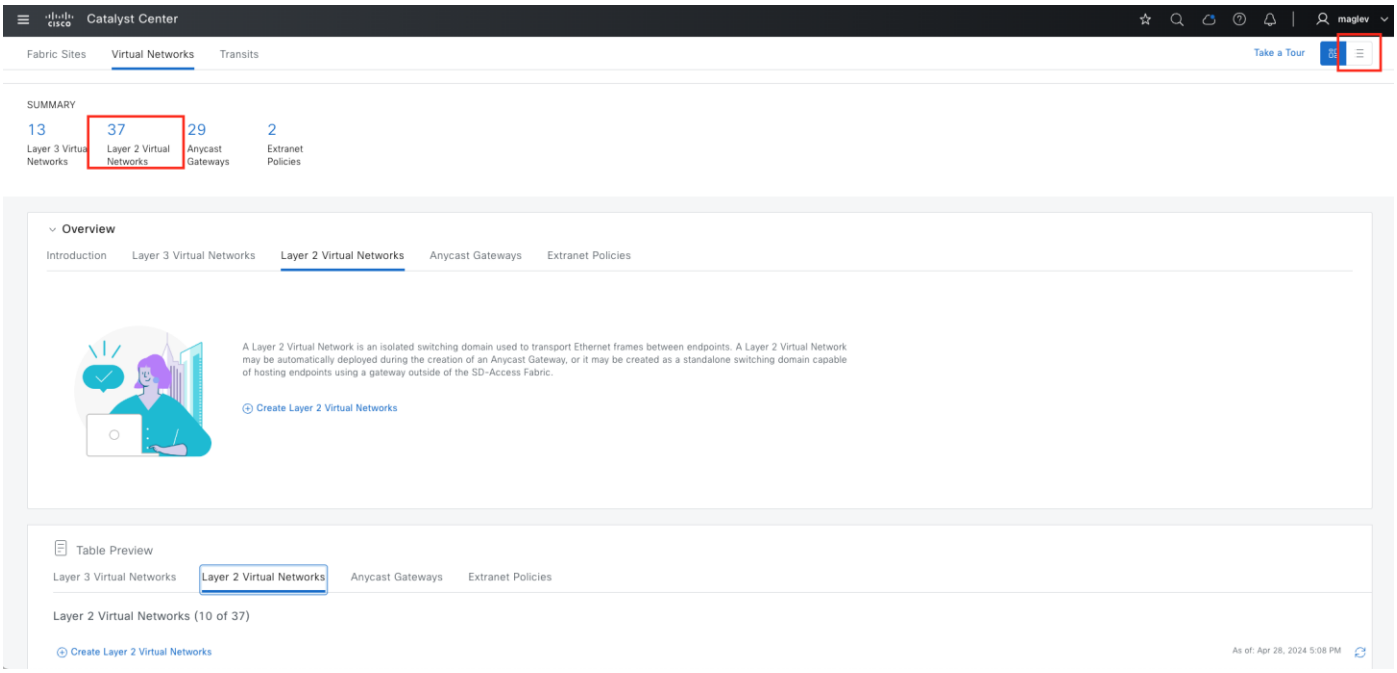


レイヤ 2 専用 VN を作成するには、以下の手順を実行します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Virtual Networks] の順に選択します。デフォルトでは、[Summary] ビューから開始します。レイヤ 3 VN の作成と同様に、デフォルトウィンドウには、**レイヤ 2 仮想ネットワークを作成**（[Create Layer 2 Virtual Networks]）する場所がいくつかあります。



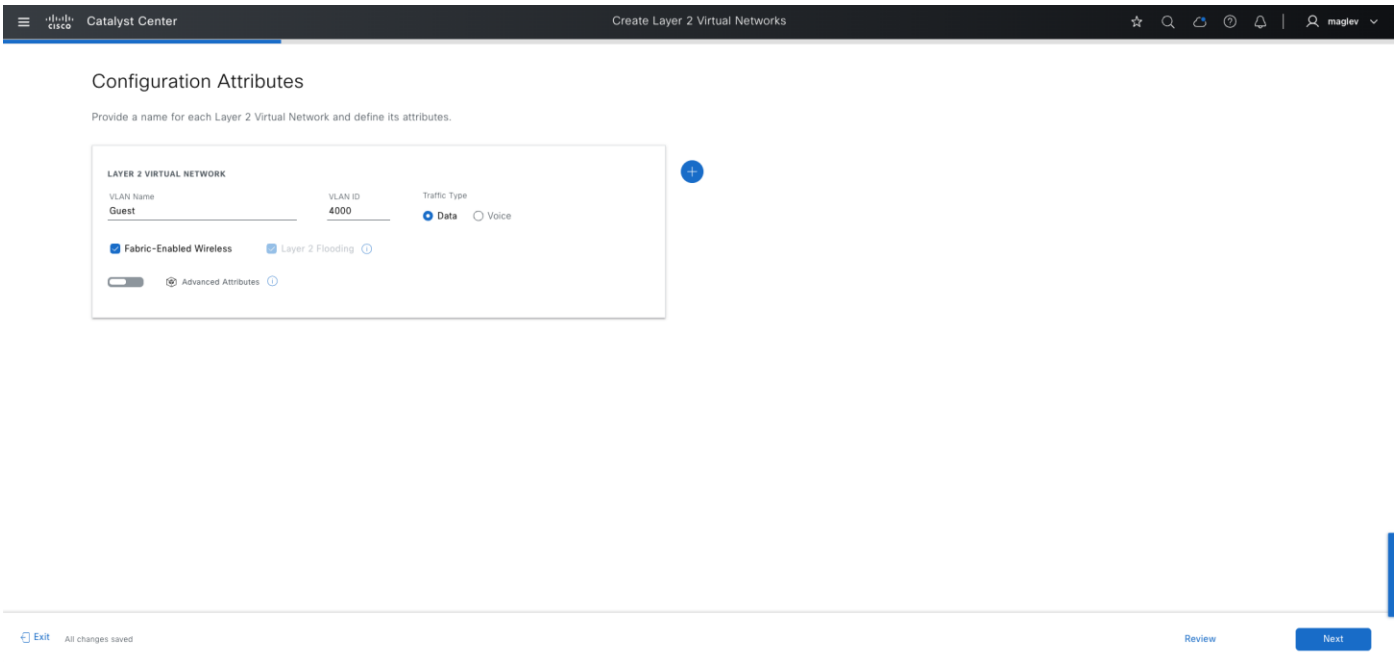

- または、図に示すように [Create Layer 2 Virtual Networks] をクリックするか、[SUMMARY] の下にある番号をクリックしてテーブルビューにリダイレクトするか、右上のアイコンボタンからテーブルビューに変更します。



**ステップ 2.** テーブルビューで、[Create Layer 2 Virtual Networks] をクリックし、必要なフィールドに入力します。

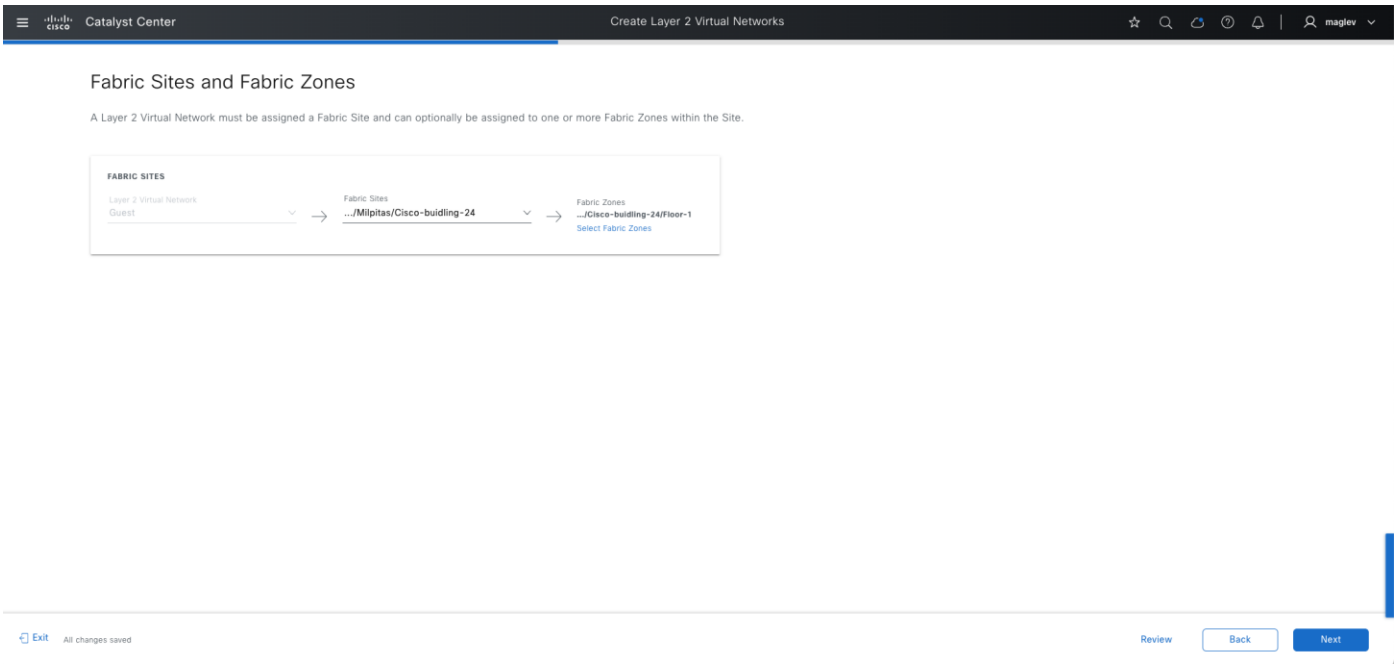
| フィールド | 値 |
|---|---|
| VLAN Name | Guest |
| VLAN ID | 4,000 |
| Traffic Type | Data |

**ステップ 3.** ワイヤレスクライアントをオンボーディングするには、[Fabric-Enabled Wireless] チェックボックスもオンにします。

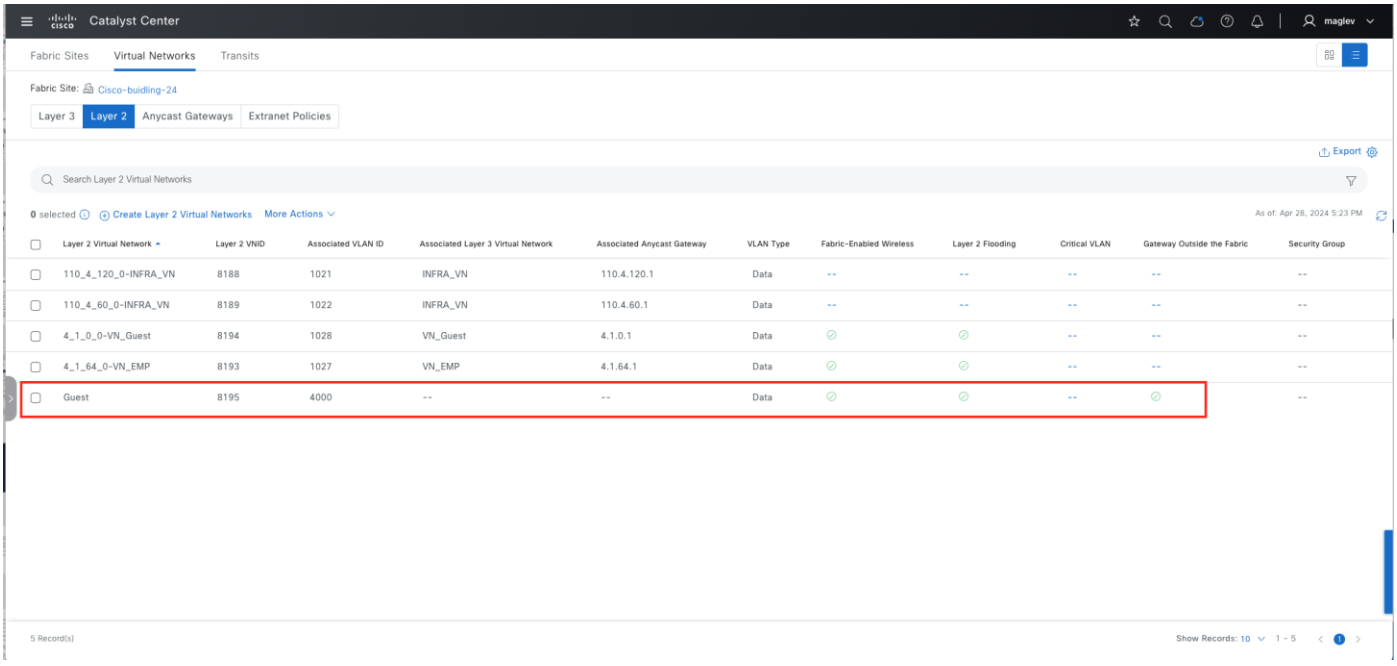



**ステップ 4.** クライアントが存在する場合は、[Advanced Attributes] ダイアログで [Wireless Bridge VM] チェックボックスをオンにします。

**ステップ 5.** **Cisco-building-24** およびゾーン **Floor-1** に割り当て、タスクを展開するためのワークフローを完了します。




**ステップ 6.** VN が [Layer 2] でのみ作成されていることを確認します。



## エニーキャストゲートウェイの作成、およびファブリックサイトとファブリックゾーンへの追加

エニーキャストゲートウェイの作成は、IP アドレスプールを VN に関連付けるプロセスです。IP アドレスプールは、デフォルトゲートウェイと、エンドポイントの基本的な IP サービスを提供します。このデフォルトゲートウェイは、エニーキャストゲートウェイです。エニーキャストゲートウェイは、Cisco SD-Access を使用していない従来のネットワークのファーストホップスイッチド仮想インターフェイスに似ています。

エニーキャストゲートウェイの追加は、**グローバル**レベルまたはサイトおよびゾーンレベルで実行できます。

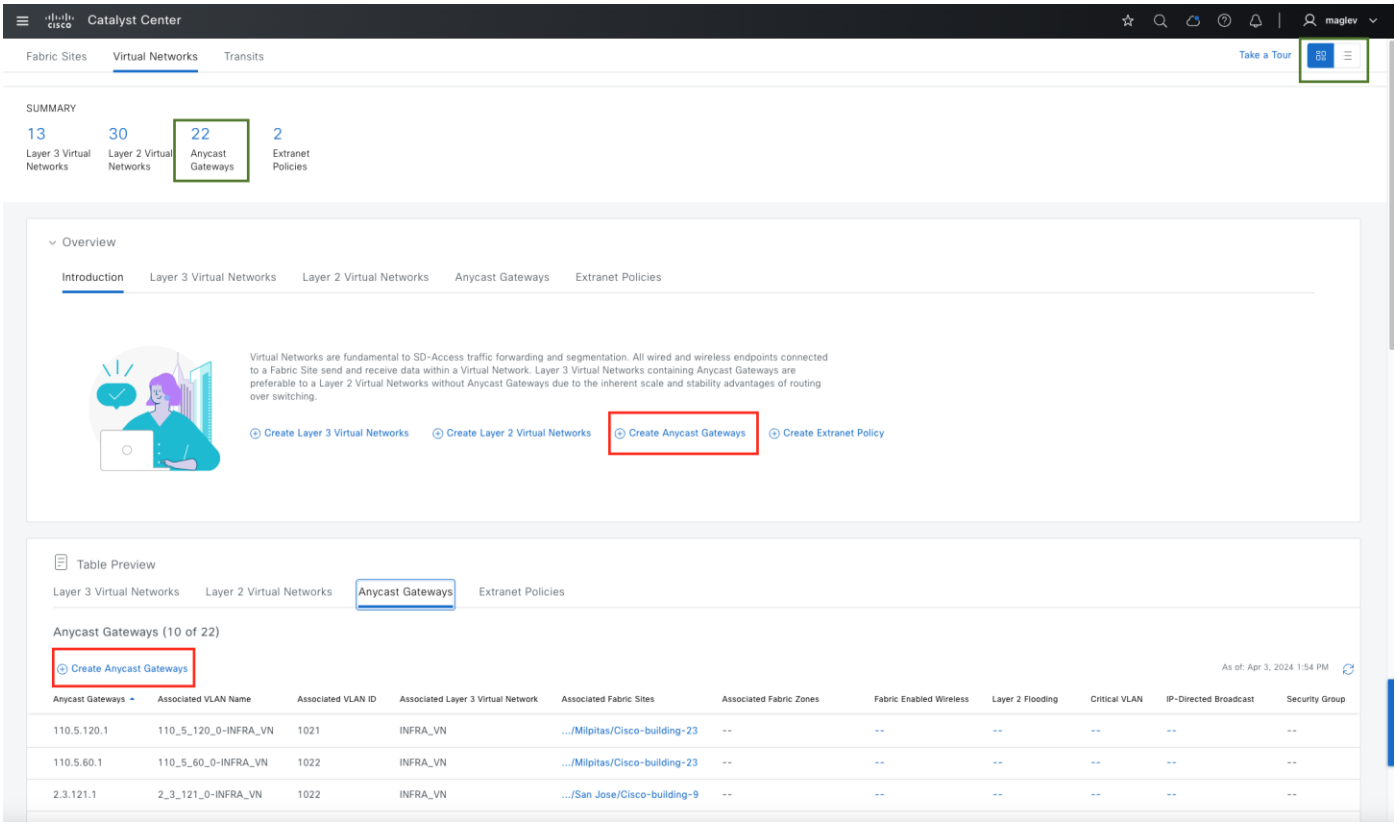
このセクションでは、AP のエニーキャストゲートウェイ、**INFRA_VN** の拡張ノード、およびカスタム VN の **VN_Guest** と **VN_EMP** のエニーキャストゲートウェイが **Cisco-building-24** サイトとゾーン **Floor-1** に追加されます。

### 手順 1。　INFRA_VN でのエニーキャストゲートウェイの追加

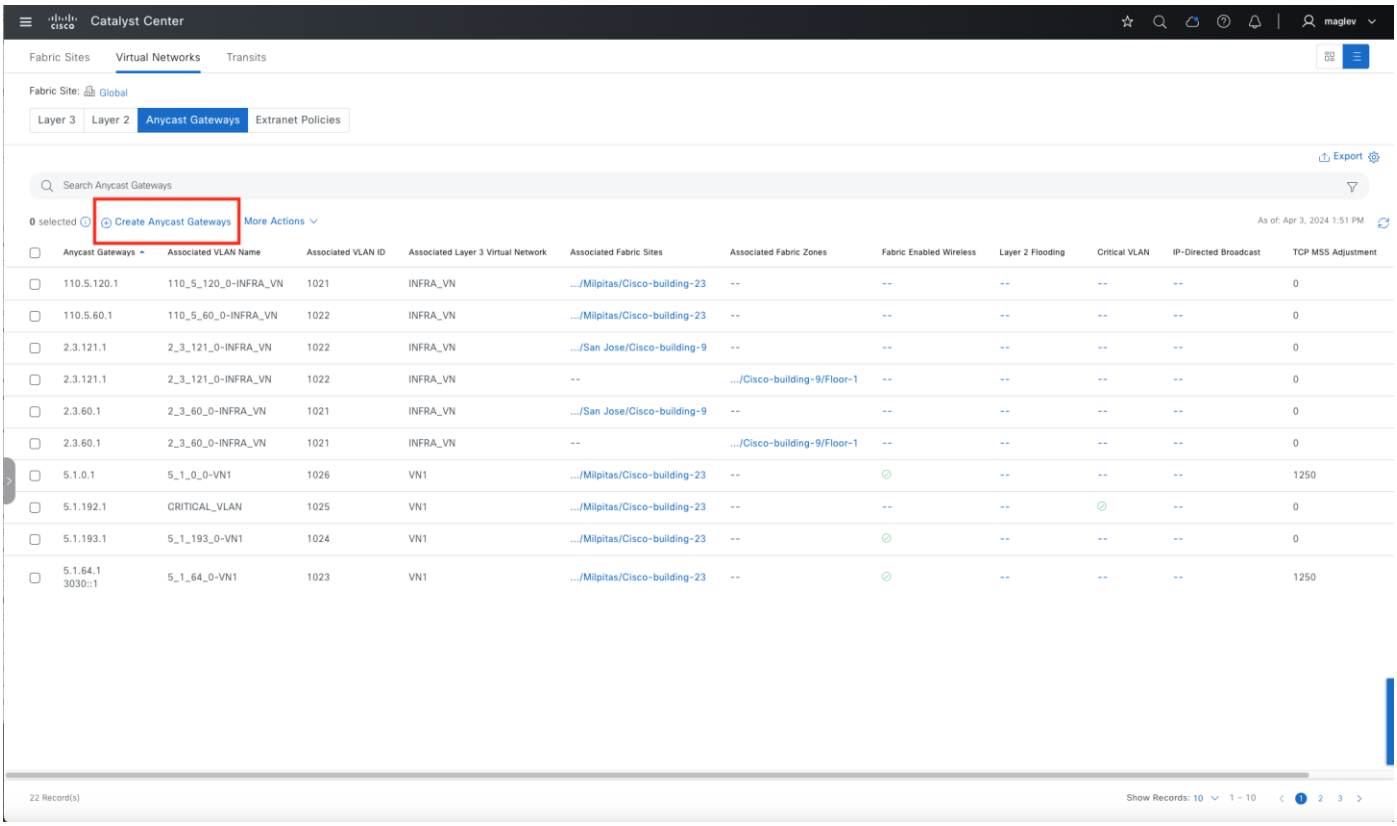
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Virtual Networks] の順に選択します。デフォルトでは、ランディングウィンドウは [Summary] ビューです。

エニーキャストゲートウェイは、[Overview] セクションと [Table Preview] セクションから作成できます。テーブルビューから作成することもできます。

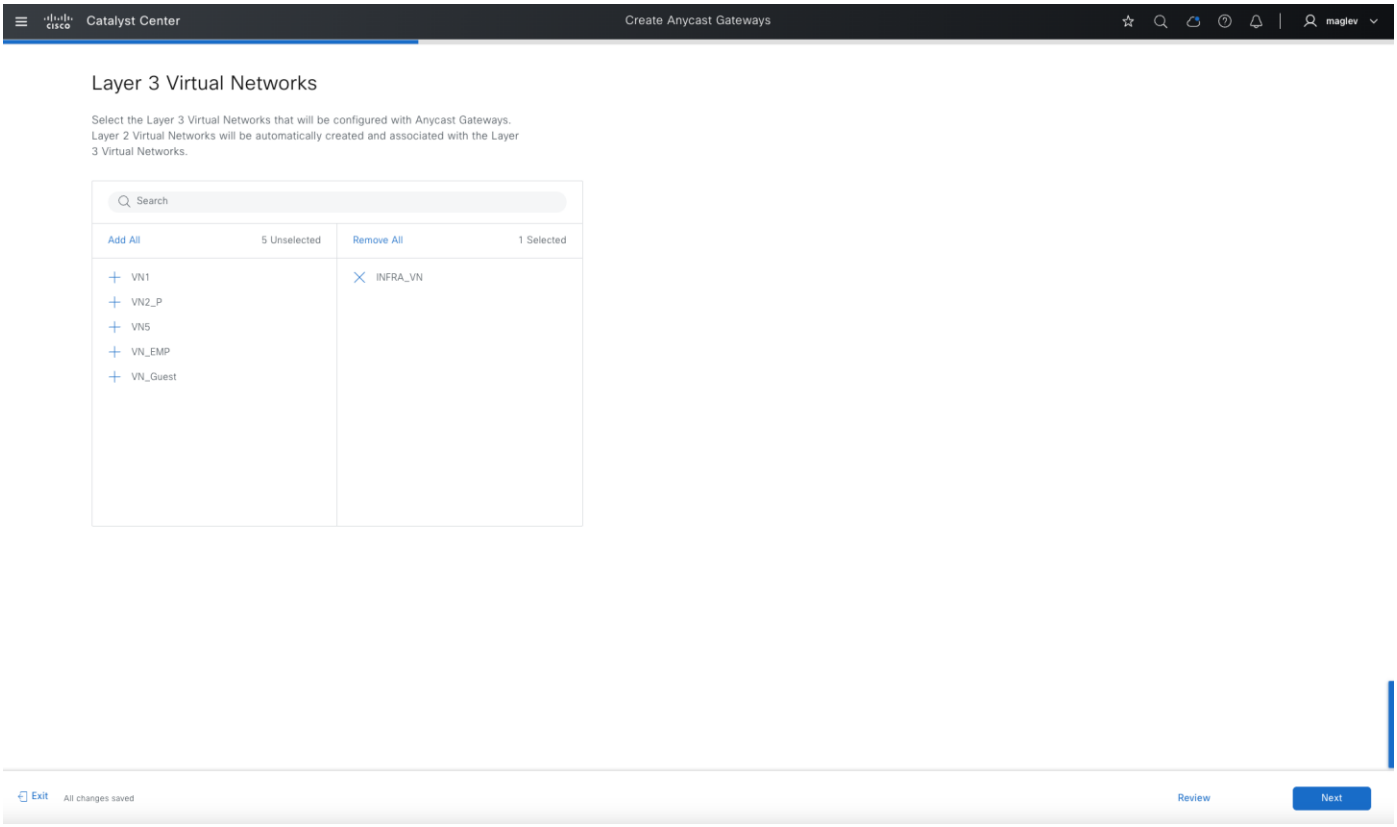
**図 35.　[Overview] セクションと [Table Preview] セクション**



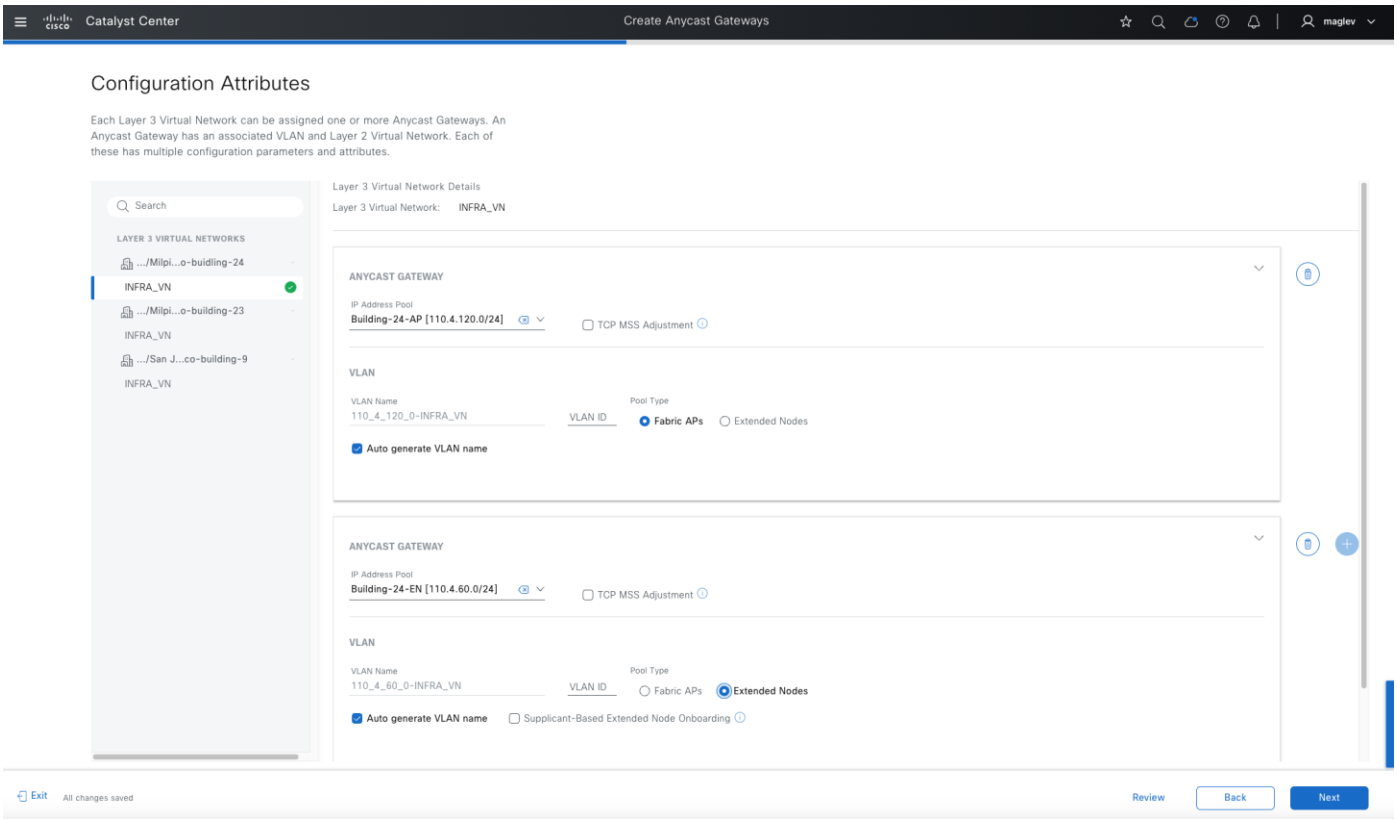
**ステップ 2.** 右上のアイコンボタンをクリックしてテーブルビューレイアウトに切り替えてから、[Create Anycast Gateways] をクリックします。




**ステップ 3.** [Create Anycast Gateways] ワークフローを開始し、[INFRA_VN] を選択します。



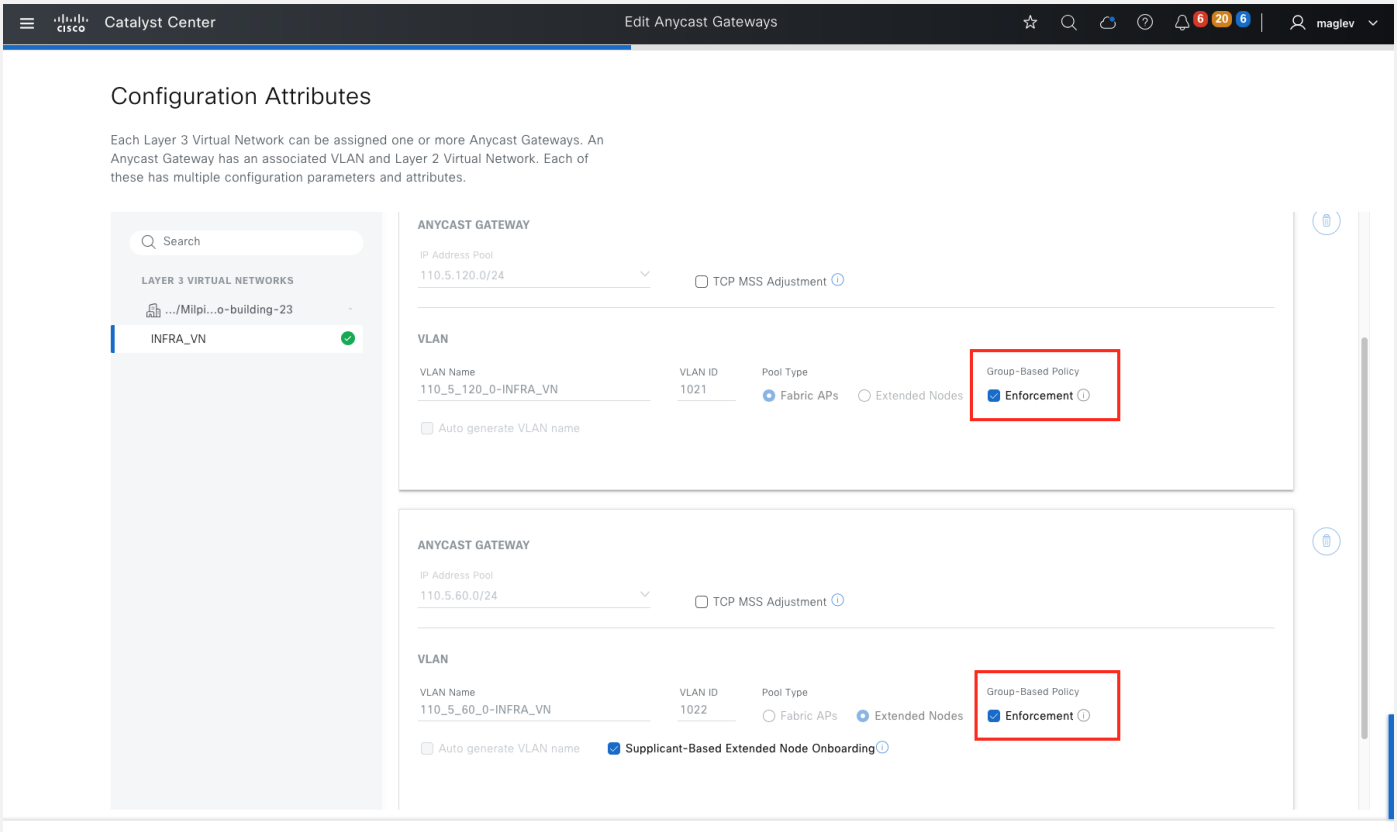
**ステップ 4.** ステップ 2 で作成した IP アドレスプールを追加し、**Cisco Building-24** に [Fabric APs]、[Pool Type] に [Extended Nodes] を選択します（左ペインから選択します）。



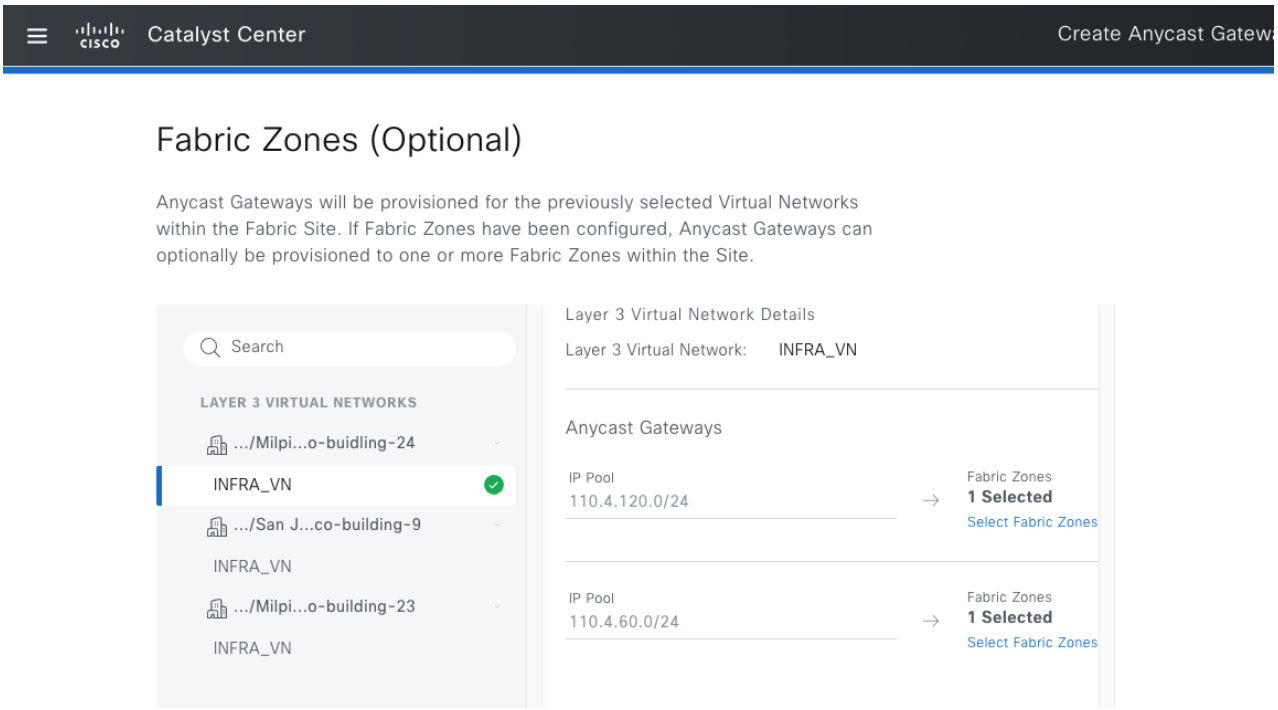
**注：**
1.**プールタイプ、VLAN 名**は、エニーキャストゲートウェイの作成後は変更できません。**TCP MSS の調整、サプリカントベースの拡張ノードオンボーディング**は、Day-*N* 運用で後で追加および変更できます。

2. 2.3.7.6 リリースより前に AP および EN プールが Catalyst Center に追加された場合、2.3.7.6 にアップグレードした後、これらの 2 つのプールで [Enforcement] オプションを使用できます。このオプションをオフにすることにした場合、「no cts role-based enforcement *VLAN AP-VLAN/EN-VLAN*」は、ファブリックエッジ、ポリシー拡張ノード、サプリカント拡張ノードなどのすべてのファブリック アクセス デバイスにプッシュされます。このオプションをオフにして設定を展開すると、このオプションは表示されません。このオプションは、2.3.7.6 以降のリリースで追加された AP および EN プールには表示されません。2.3.7.6 リリース以降、Catalyst Center はデフォルトで AP および EN プールの適用を無効にしています。

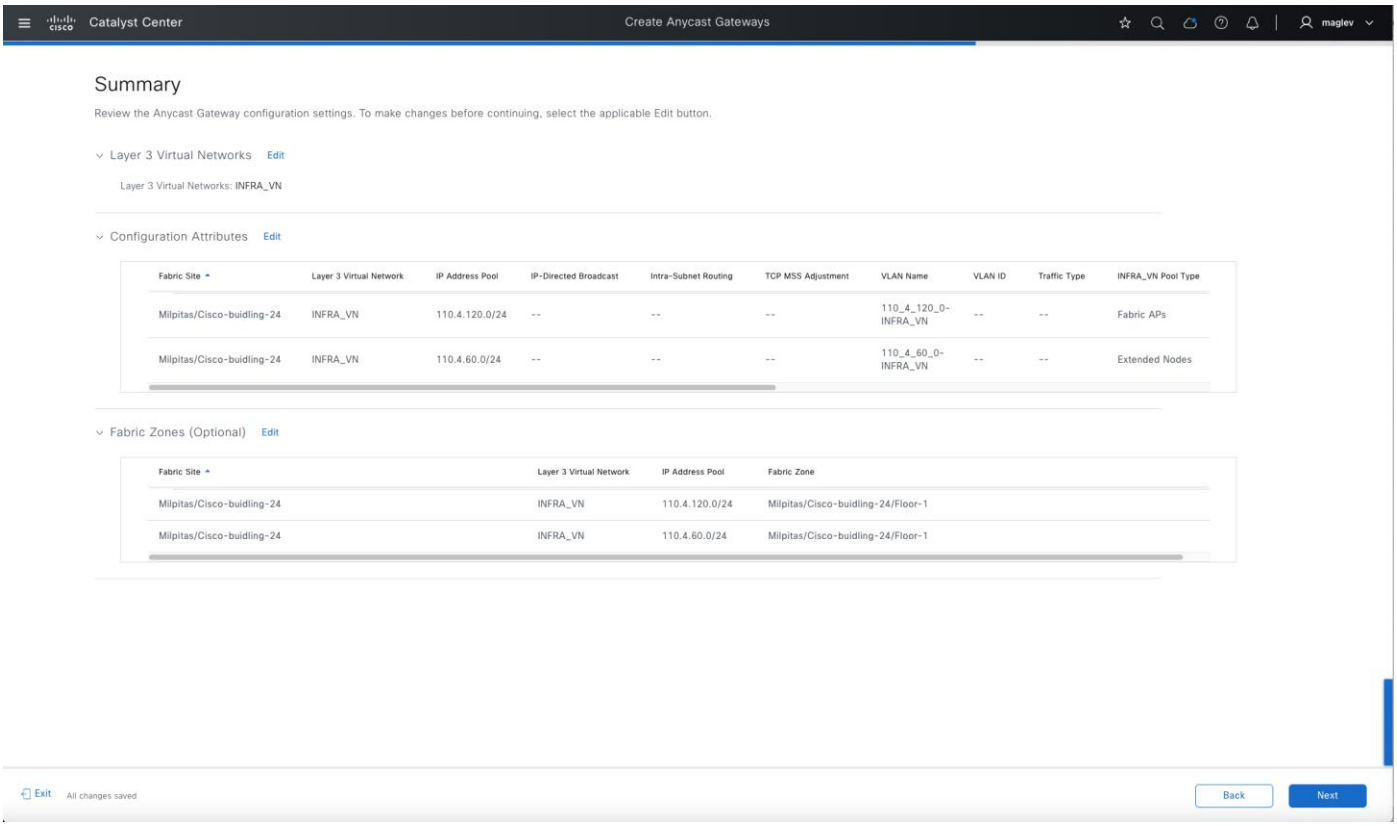
「cts role-based enforcement」は、マイクロセグメンテーションと、クライアントトラフィックの管理に使用されます。INFRA_VN の AP と EN は通常、ポリシーの適用を必要とせず、「deny IP」がファブリックサイトのデフォルトポリシーである場合、この設定は手動で削除する必要があります。このオプションは、「deny IP」がデフォルトポリシーとして設定されているファブリック展開に役立ちます。



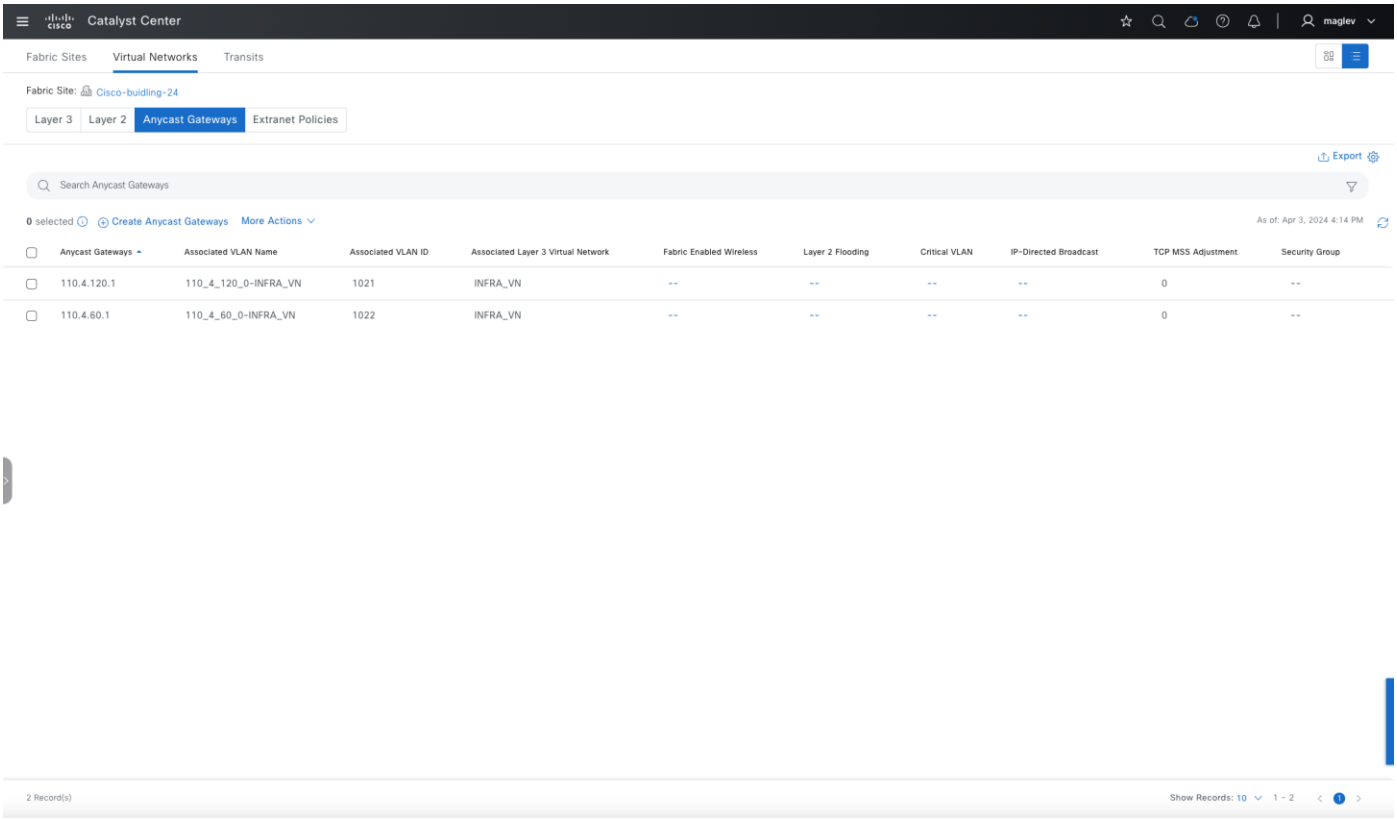
**ステップ 5.** ファブリックゾーン **Floor-1** に追加します。

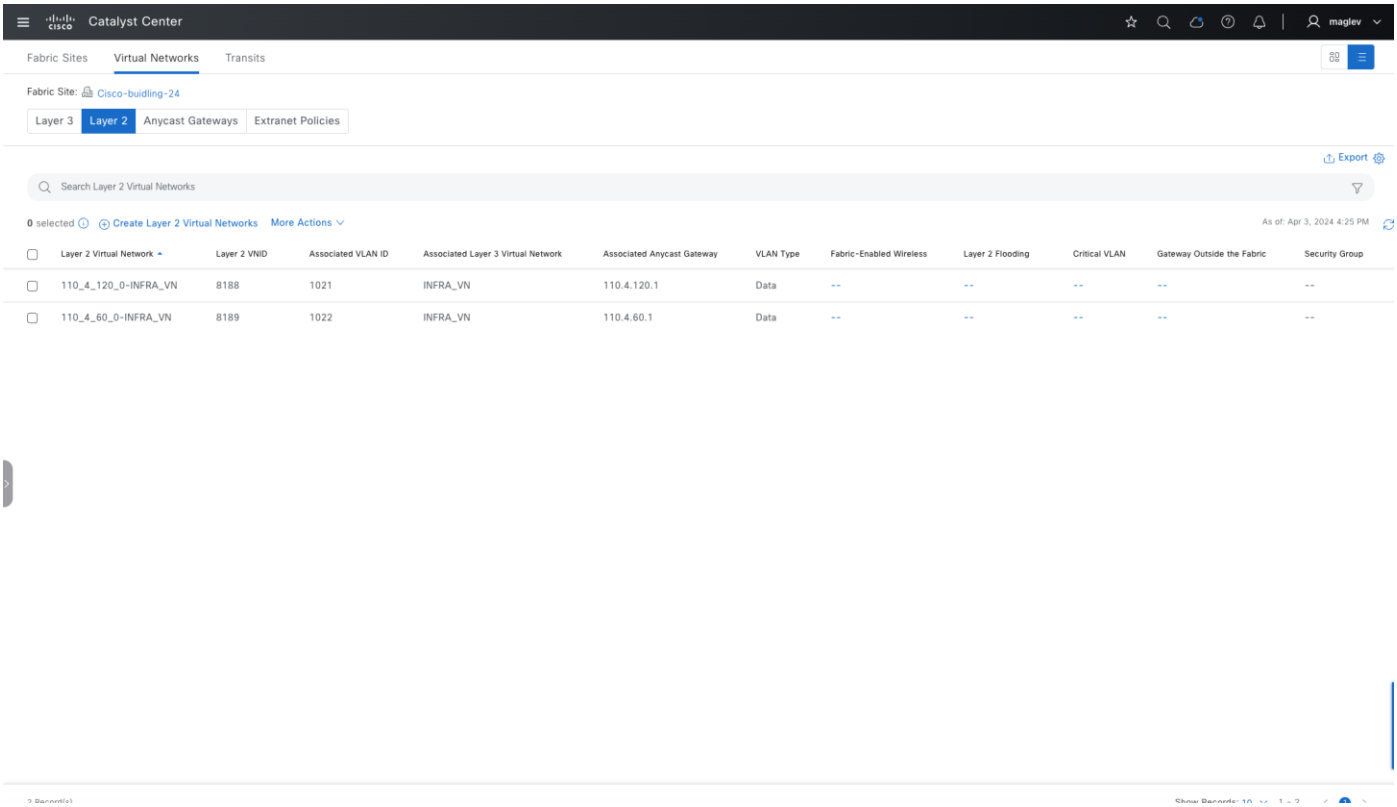



**ステップ 6.** [Summary] ウィンドウで設定情報を確認し、タスクを展開します。



**ステップ 7.** [Cisco-buidling-24] に切り替え、[Anycast Gateways] タブと [Layer 2] タブをクリックして、新しく作成された 2 つのエニーキャストゲートウェイとレイヤ 2 VN を確認します。

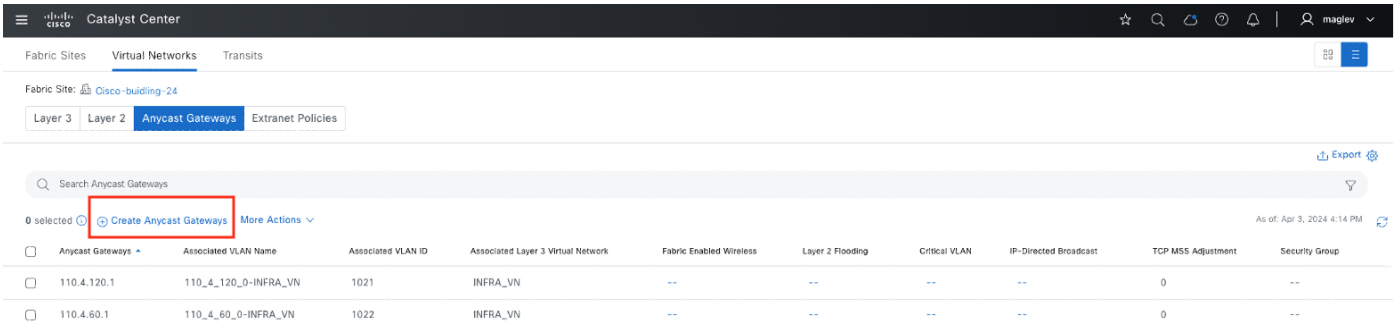


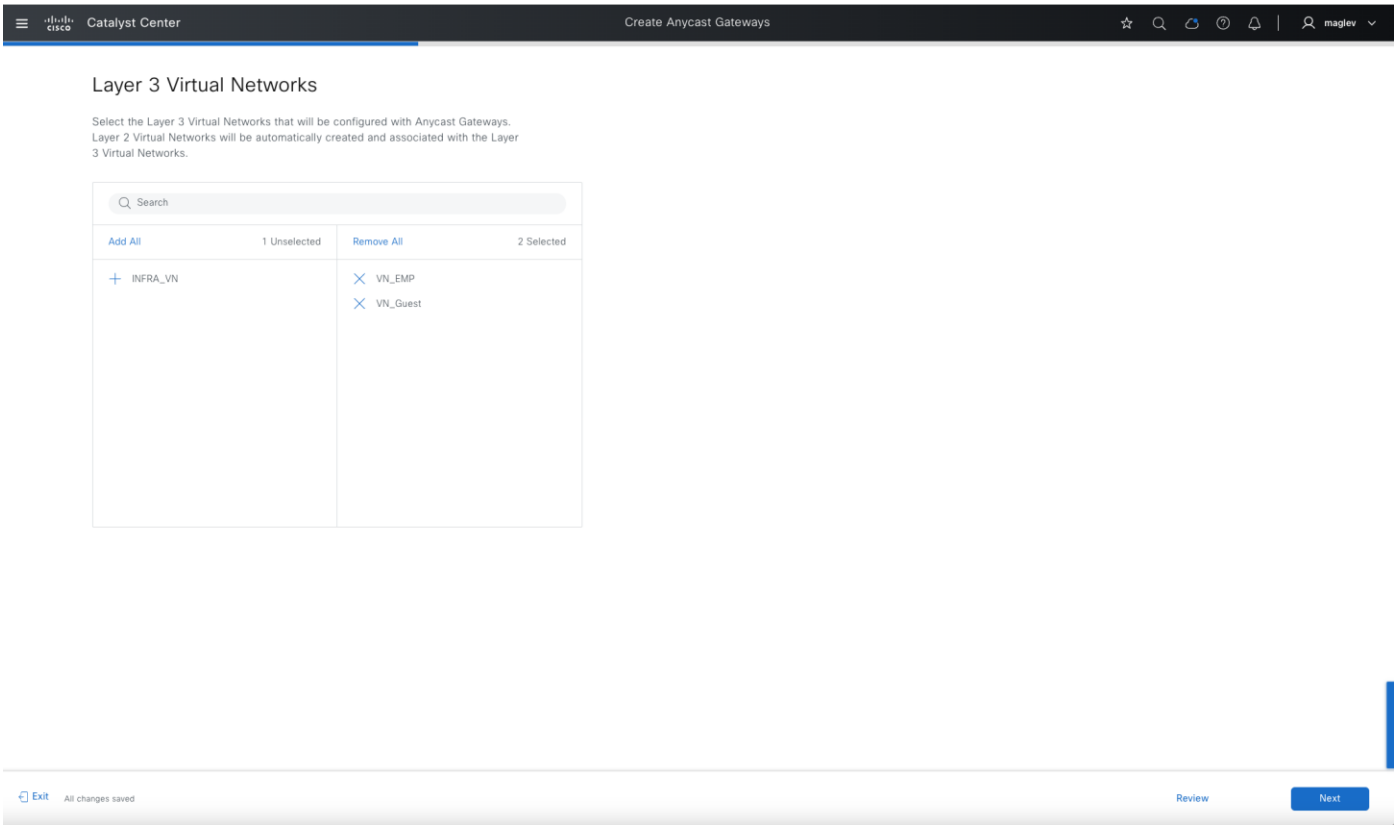
## 手順 2。　カスタム VN でエニーキャストゲートウェイの追加

前の手順では、グローバルレベルでのエニーキャストゲートウェイの作成について説明しました。この手順では、サイトレベルでのエニーキャストゲートウェイの作成について説明します。

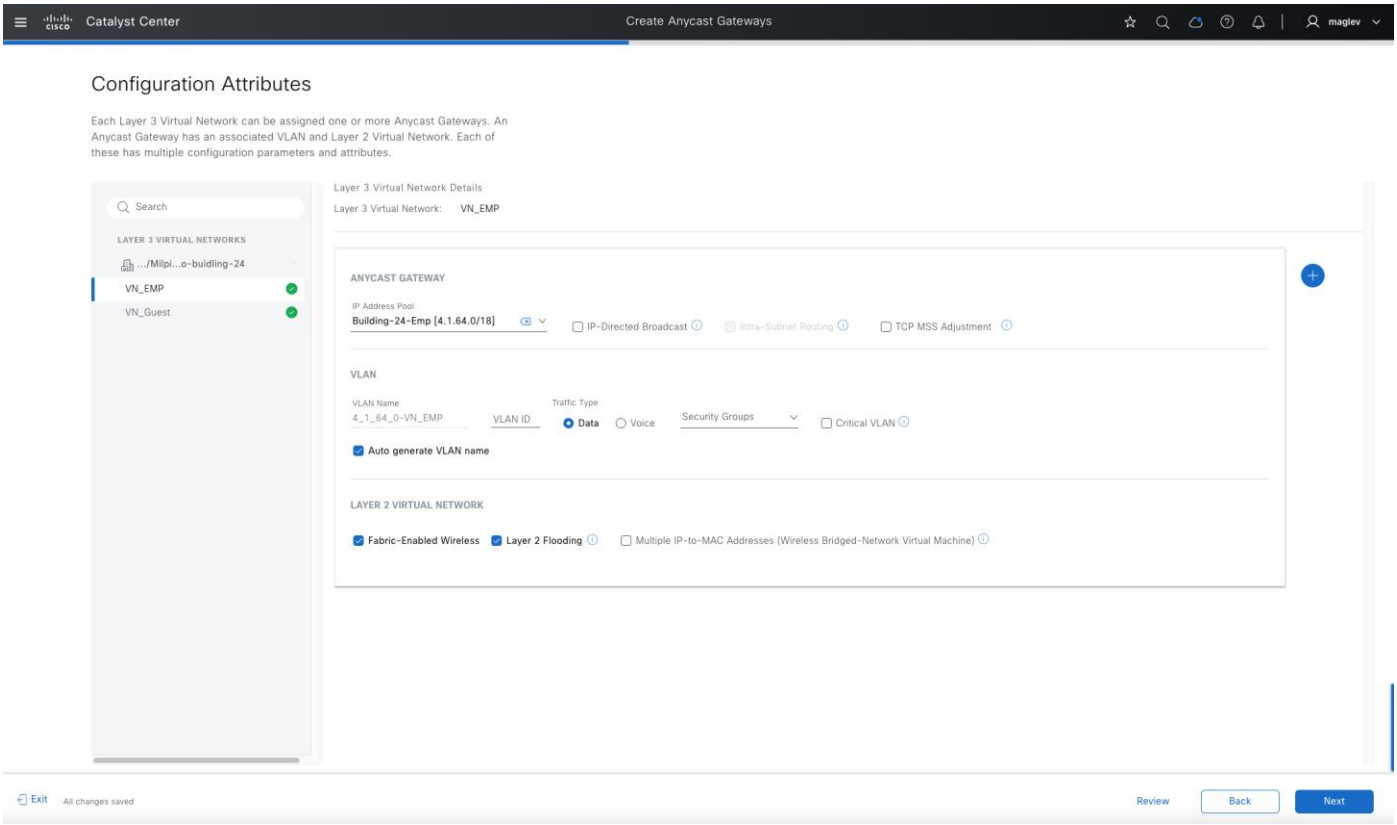
**ステップ 1.** **Cisco-building-24** の [Anycast Gateway] タブをクリックし、[Create Anycast Gateways] をクリックして、ワークフローを開始します。




**ステップ 2.** ワークフローで **VN_EMP** と **VN_Guest** の両方を選択します。



**ステップ 3.** IP アドレスプールを VN に個別に追加します。左側のペインで VN を切り替えます。



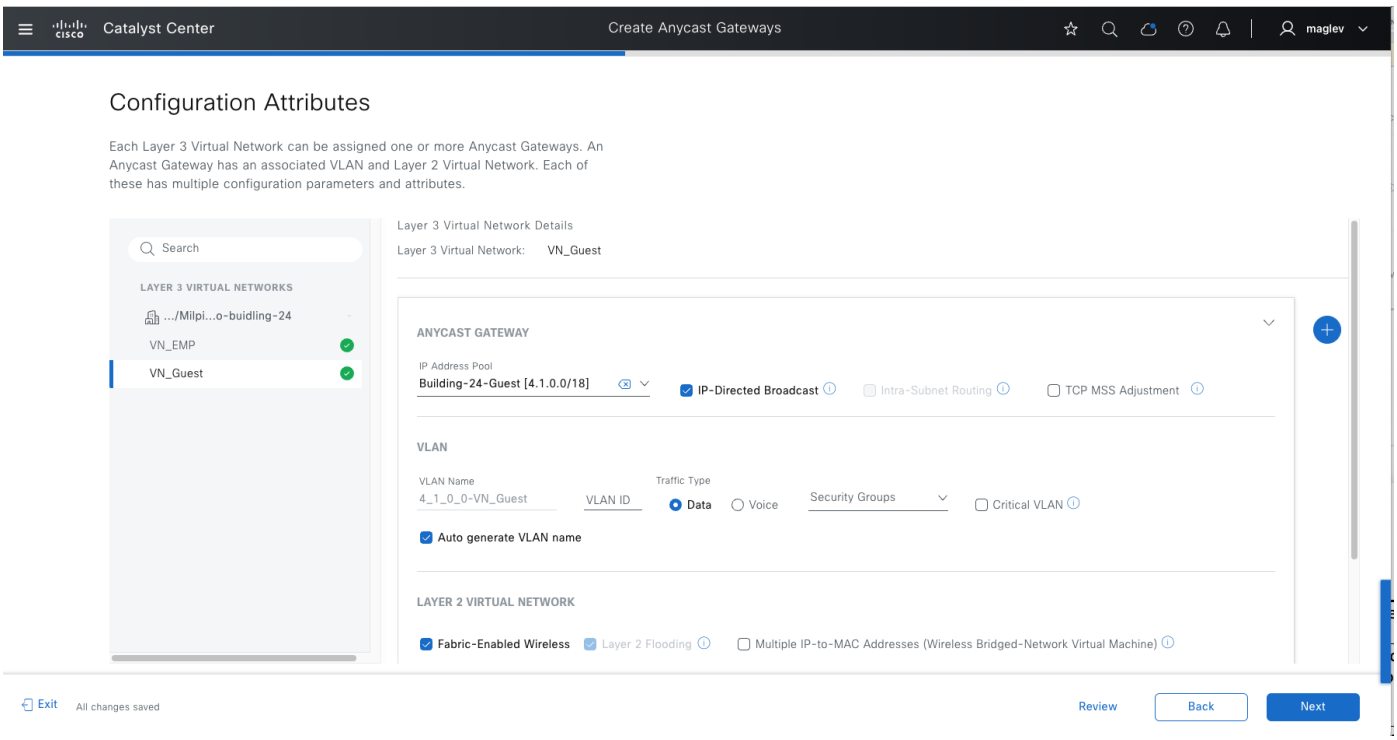




**表 20.** IP プールの属性

| 属性 | 使用目的 | 制約事項 |
|---|---|---|
| IP ダイレクトブロー | Wake on LAN マジックパケット（サーバーはファブリックの外部にあります）は、ファブリック内のス | ボーダーとしてルータプラットフォームと Cisco Nexus 7000 シリーズ ス |

| 属性 | 使用目的 | 制約事項 |
| --- | --- | --- |
| ドキャスト | リープ状態のホストをウェイクアップします。<br><br>有効にすると、レイヤ 2 フラッディング機能が自動的に有効になります。<br><br>WoL のシナリオ：<br><br>1. 送信元（WoL イニシエータ）が、Cisco SD-Access ファブリックの外部にあるが、レイヤ 3 ハンドオフを介してファブリックに接続されているネットワーク内にあり、宛先が、同じ VN 内の IP ダイレクトブロードキャストが有効になっている Cisco SD-Access サブネット内にあります。<br><br>2. たとえば、送信元（WoL イニシエータ）と宛先（スリープ状態のホスト）の両方が同じサブネットおよび同じ VN にある場合、両方ともファブリックエッジに接続されています。この機能は必須ではありませんが、レイヤ 2 フラッディングは必須です。 | イッチを使用するファブリックサイトではサポートされません。 |
| サブネット内ルーティング | レイヤ 3 専用 VN 属性（有効である場合）の L2VN とその属性（レイヤ 2 フラッディングなど）、およびファブリックワイヤレスは無効になります。パケット転送は、宛先 IP アドレスに基づいてサブネット内トラフィックをルーティングするように最適化されています。IP/MAC 盗難チェックはバイパスされます。<br><br>この機能は、VoWLAN（Voice over WLAN）などのローミング遅延要件が低いアプリケーションの Cisco SD-Access ワイヤレス Flex OTT 展開で検討できます。この機能が有効になっている場合、（同じまたは異なるファブリックエッジ上の）ある AP から別の AP に Flex OTT ワイヤレスクライアントをローミングする遅延は 200 ミリ秒以内です。<br><br>この機能はレイヤ 2 フラッディングを無効にするため、この機能を備えたシスコのワイヤレスデバイスのみを使用することが推奨されます。ワイヤレス展開のクライアント VLAN にレイヤ 2 フラッディングが必須の場合は、この機能を使用しないでください。 | デュアルスタックプール（IPv6 クライアント）ではサポートされません。<br><br>ファブリックエッジノードは、17.9.2 以降を実行している必要があります。 |
| TCP MSS 調整 | Cisco SD-Access VXLAN のカプセル化により、元のパケットに 50 バイトのオーバーヘッドが追加され、フラグメント化できなくなります。ジャンボ MTU（1500 を超える）に対応できない回線の場合は、TCP セッションに入力 MTU を実装して、ファブリックカプセル化を可能にします。<br><br>[TCP MSS Adjustment] には 500 ～ 1440 の範囲内で値を入力できます。[TCP MSS Adjustment] の値は、IPv4 と IPv6 の両方の TCP セッションに適用されます。<br><br>[TCP MSS Adjustment] の値は、すべてのエニーキャスト ゲートウェイ スイッチ仮想インターフェイス（SVI）に適用されます。 | なし |

**注：** 同じ **IP プール**を、同じファブリックサイト内の複数のカスタム VN で設定できます。これは、重複プールと呼ばれます。重複プールは、Catalyst Center による自動ワイヤレス展開ではサポートされません。トラフィックの中断を避けるために、重複プールを使用する際は注意が必要です。

**表 21.** VLAN 属性

| 属性 | 使用目的 |
| --- | --- |
| VLAN 名/VLAN ID | 自動で生成または手動で追加されます。 |
| トラフィック タイプ | データまたは音声 |
| セキュリティ グループ | 静的に割り当てられた SGT 値。Cisco ISE がサブネット内のクライアントに異なる値を割り当てた場合に、Cisco ISE によって上書きされます。 |
| クリティカル VLAN | 認証サーバーをクローズド認証プロファイルで使用できない場合、クライアントの配置に使用されます。VLAN の名前は固定のため、変更できません。詳細については、「クリティカル VLAN のエニーキャストゲートウェイの作成」を参照してください。 |

**注：**
1. 音声 VLAN を使用してデータ VLAN からトラフィックを分散させ、大規模な展開での音声品質を向上させることができます。

2. Cisco Discovery Protocol（CDP）は、Cisco SD-Access 展開で有効になっています。CDP をサポートする IP Phone では、CDP 経由で音声 VLAN 情報を学習できます。

**表 22.** レイヤ 2 VN 属性

| 属性 | 使用目的 |
| --- | --- |
| ファブリック対応ワイヤレス | ファブリックワイヤレスが存在する場合に選択します。この属性が有効になっている場合にのみ、IP プールをファブリック SSID にマッピングできます。 |
| レイヤ 2 フラッディング | フラッディングしている BUM トラフィック（イーサネット ブロードキャスト、不明なユニキャストおよびマルチキャスト）を選択します。これには、LAN の自動化を介して設定できる、または手動で設定できるアンダーレイマルチキャストの設定が必要です。LAN の自動化が使用されていない場合の手動設定については、注を参照してください。 |
| 複数の IP-to-MAC アドレス | ブリッジネットワーク仮想マシンの展開に使用されます。詳細と制限については、情報アイコンを確認してください。 |

**注：** レイヤ 2 フラッディングアンダーレイの設定に LAN の自動化を使用しない場合は、Catalyst Center CLI テンプレートを使用して展開します。
この設計および導入ガイドでは、テンプレートについては取り上げていません。「Cisco Catalyst Center User Guide」の「Create Templates to Automate Device configuration Changes」セクションを参照してください。

RP デバイス（通常は冗長ファブリックボーダーノード）でのテンプレート設定例：

- **ip_address**：ファブリックエッジ、中間ノード、その他の非冗長ファブリックボーダーなどを含む、他のファブリックデバイスから到達可能な loopback60000 IP アドレス。同じ IP アドレスを持つ同じ Loopback60000 を冗長ファブリックボーダーノードで設定する必要があり、RP アドレスとして使用されます。
- **Peer-loopback0**：冗長ファブリックボーダーノードの loopback0 IP アドレス
- **layer3_interface**：アンダーレイレイヤ 3 インターフェイス全体

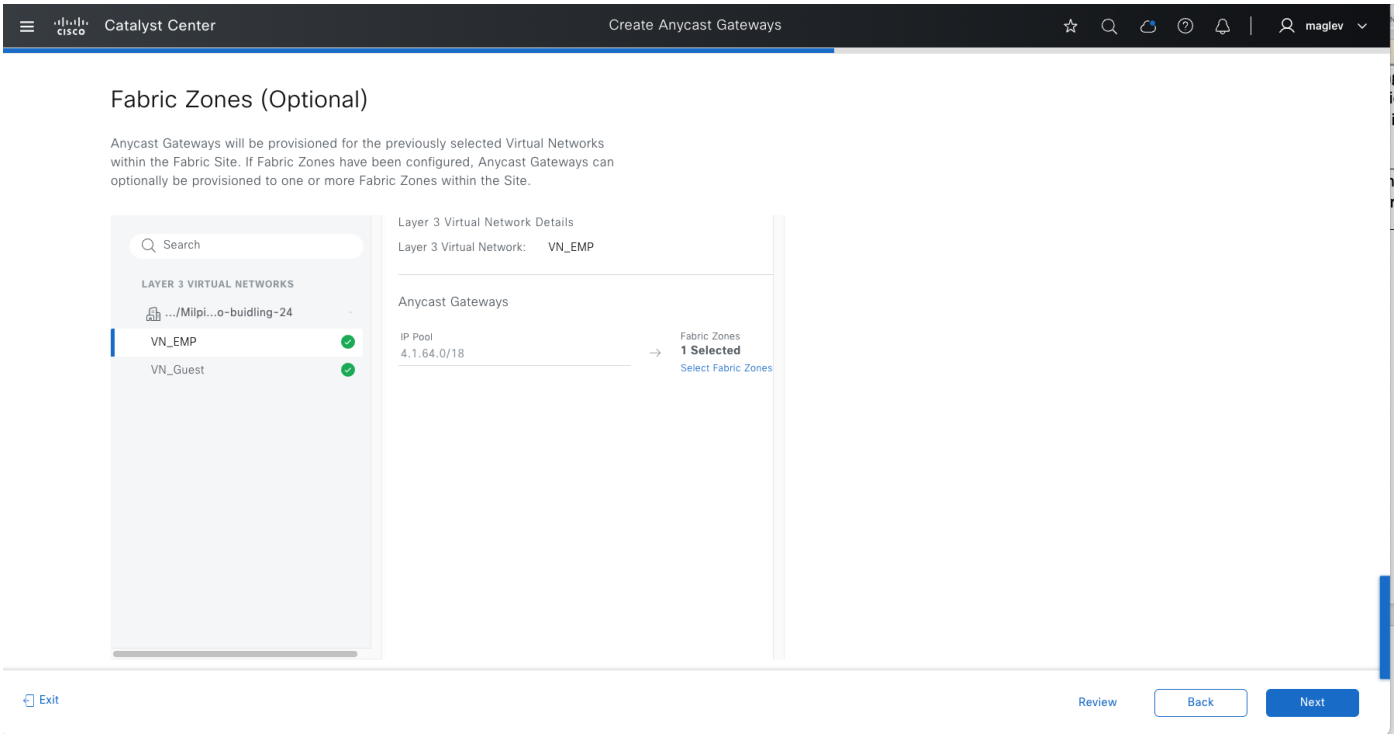
```
interface Loopback60000
 ip address $ip-Address 255.255.255.255
 ip router isis
 ip pim sparse-mode

ip multicast-routing
ip pim rp-address $ip-Address
ip pim register-source Loopback60000

ip msdp peer $peer-loopback0 connect-source Loopback0
ip msdp originator-id Loopback0

interface $layer3_interface
 ip pim sparse-mode
```

ファブリックエッジ、中間ノード、非 RP ファブリックボーダーなどの非 RP デバイスでのテンプレート設定例：

- **rp-address**：冗長ボーダーデバイスの loopback60000 IP アドレス
- **layer3_interface**：アンダーレイ L3 インターフェイス全体

```
ip multicast routing
ip pim rp-address $rp-address
ip pim register-source Loopback0

interface $layer3_interface
 ip pim sparse-mode
```

**ステップ 4.** ファブリックゾーン **Floor-1** に追加し、ワークフローを完了します。



## サイトレベルでの認証テンプレートを使用した設定

Catalyst Center は、ネットワークでの認証の実装プロセスを簡素化するために、事前定義された認証テンプレートをサポートしています。ファブリックエッジは、テンプレートの選択後に自動的に設定します。

事前定義されている認証テンプレート：

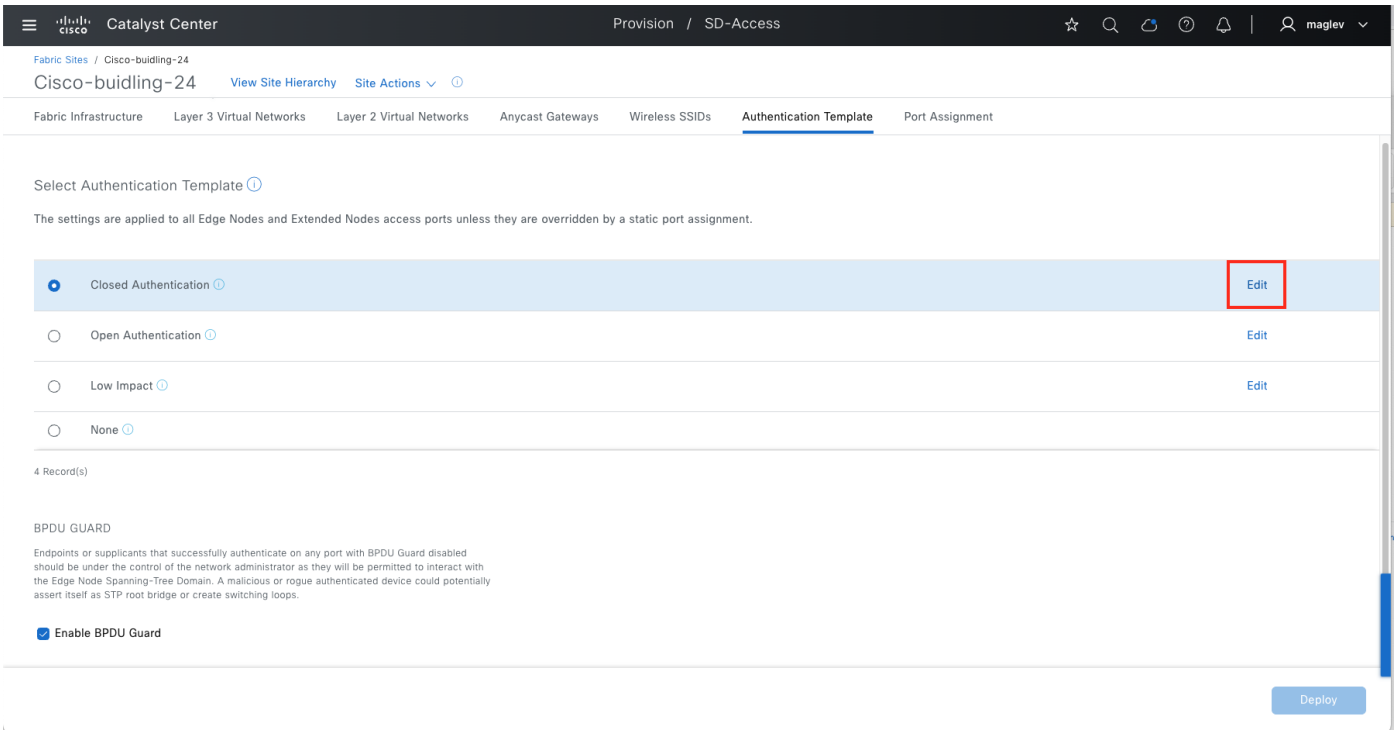
- [Closed Authentication]：802.1X + MAB（IBNS 2.0 テンプレート）。認証前の DHCP/ARP はありません。
- [Open Authentication]：802.1X + MAB。Dot1x 認証の前に一時的なアクセスが許可されます。
- [Low Impact]：LDAP + MAB
- [None]：認証はありません。すべてのポートは静的に設定されます。

サイトレベルの認証テンプレートは Day-*N* 運用で変更でき、[Closed Authentication]、[Open Authentication]、および [Low Impact] の認証パラメータを編集できます。

この例では、デフォルトのパラメータ値を持つ [Closed Authentication] は、ファブリックサイト **Cisco-building-24** とファブリックゾーン **Floor-1** に対して設定されます。WoL マジックパケットを許可するには、[Wake on LAN] 設定を有効にする必要があります。

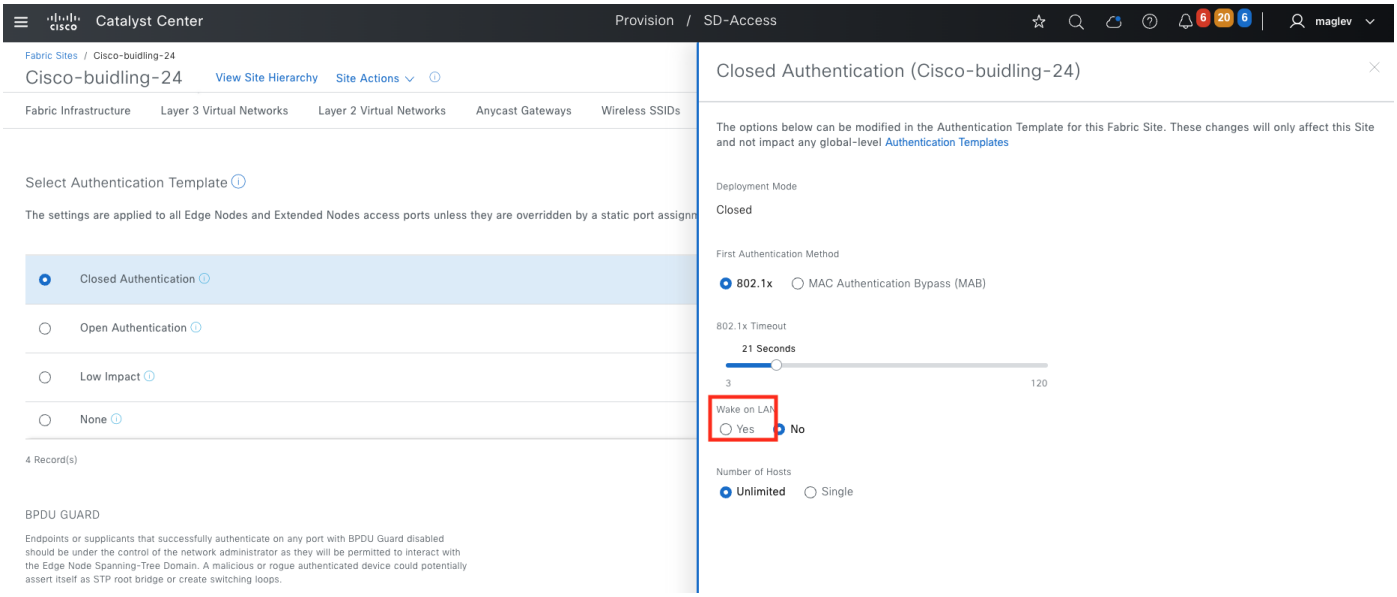
**ステップ 1.** メニューアイコンボタンから [Provision] > [Fabric sites] を選択して、テーブルビューアイコンをクリックし、[Cisco-building-24] をクリックして [Authentication Template] タブをクリックします。

**ステップ 2.** 必要に応じて、[Closed Authentication] を選択し、[Edit] をクリックしてパラメータを変更します。




**ステップ 3.** **BPDU ガード**機能は、デフォルトで有効になっています。不要な場合は、チェックボックスをオフにします。

**ステップ 4.** スリープ状態のホストが接続されている場合は、**Wake on LAN** を有効にすると、WoL マジックパケットをスリープ状態のホストに送信できます。デフォルトでは、このオプションは無効になっています。



## Cisco SD-Access ネットワークの展開

このセクションでは、デバイスの検出からファブリックの自動化に至るまでの完全な展開ワークフローとガイドラインに焦点を当てます。

ネットワークデバイスが検出されてインベントリに追加されると、プロビジョニング アプリケーションはデバイスをサイトに割り当て、[Design] ウィンドウで定義された設定をプロビジョニングします。

Cisco SD-Access アプリケーションは、ファブリックサイトにデバイスを追加し、Cisco SD-Access オーバーレイを設定するために使用されます。

オプションですが、推奨されています。LAN の自動化を使用してアンダーレイを設定します。

Cisco SD-Access ネットワークを展開するプロセスは次のとおりです。

- 2 台の Catalyst 9300 デバイスの検出および Cisco-building-24 サイトへのプロビジョニング
- ボーダーおよびコントロールプレーンノードとしての Catalyst 9300 の設定
- アクセスノードの 2 つのレイヤ（中間ノードとエッジノード）をオンボードする LAN の自動化
- ファブリックエッジの設定
- 組み込みワイヤレスコントローラの有効化
- レイヤ 3 ハンドオフ、レイヤ 2 ハンドオフ、SD-Access トランジットの設定
- マルチキャストの設定
- ボーダーの高度なファブリック機能
- VN アンカー
- Critical VLAN
- Catalyst 9800 ワイヤレスコントローラ

Loopback0 インターフェイスは、Catalyst Center Cisco SD-Access の自動化では必須です。デバイスは、管理インターフェイス gi0/0 などの任意のタイプのインターフェイスで検出して管理できます。ただし、デバイスを Cisco SD-Access ネットワークでプロビジョニングするには、loopback0 が必要であり、Catalyst Center によって LISP プロトコルで RLOC として設定されます。唯一の例外は、スタンドアロン ワイヤレス コントローラです。ファブリック ワイヤレス コントローラは LISP を実行しません。

この導入ガイドでは、検出、インベントリの同期、およびプロビジョニングに Loopback0 インターフェイスが使用されます。

## デバイスの検出およびプロビジョニング

このセクションでは、**Cisco-building-24** のデバイスを検出およびプロビジョニングする手順について説明します。これらの各手順については、以降のセクションで説明します。

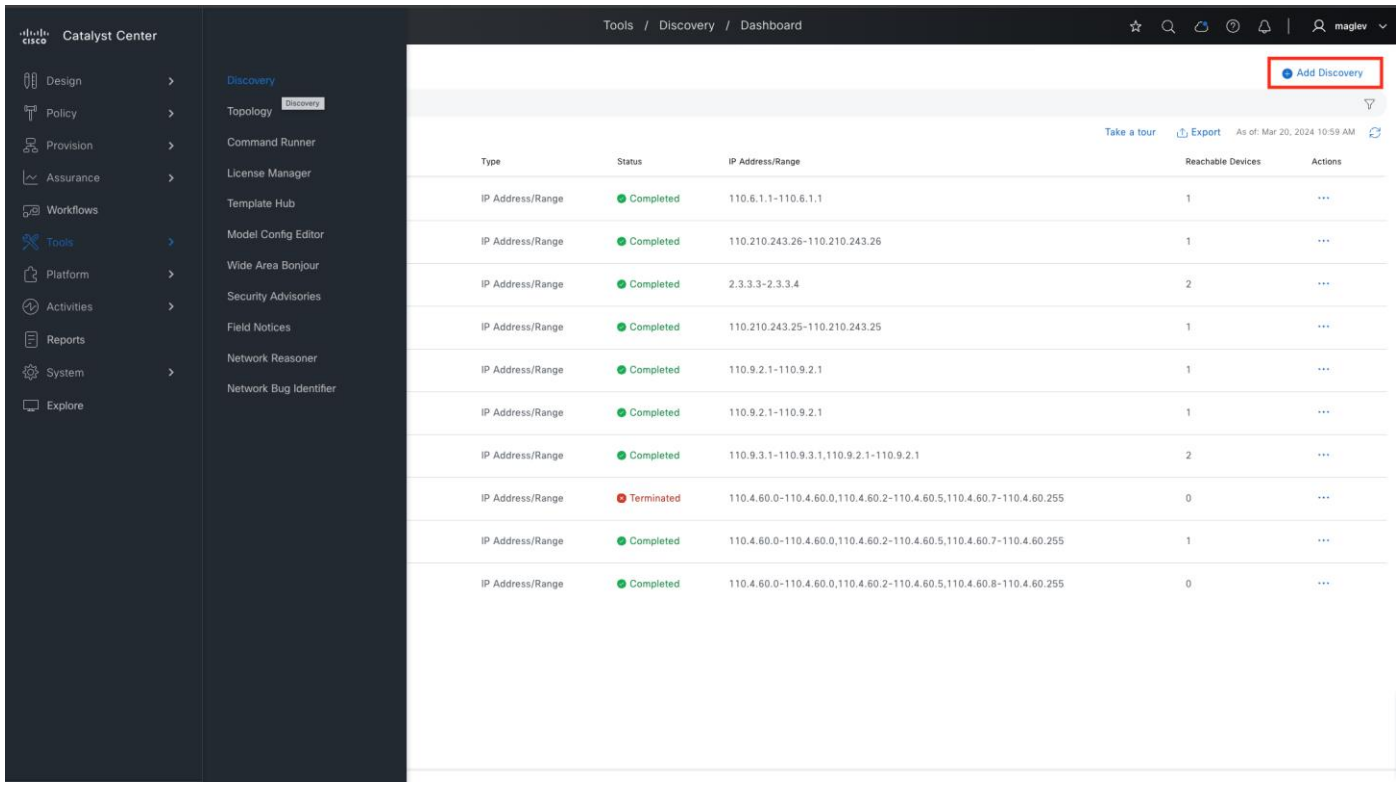
### 手順 1。 Catalyst 9300 デバイスの検出

ネットワーク内のデバイスを検出するために、Catalyst Center は、これらのデバイスへの IP 到達可能性、およびこれらのデバイスの CLI クレデンシャルを持っている必要があります。SNMP および Netconf Yang のログイン情報は、Catalyst Center で定義し、サイト割り当ての検出中にプッシュできます。検出されると、デバイスがインベントリに追加され、コントローラがプロビジョニングを通じて設定を変更できるようになります。

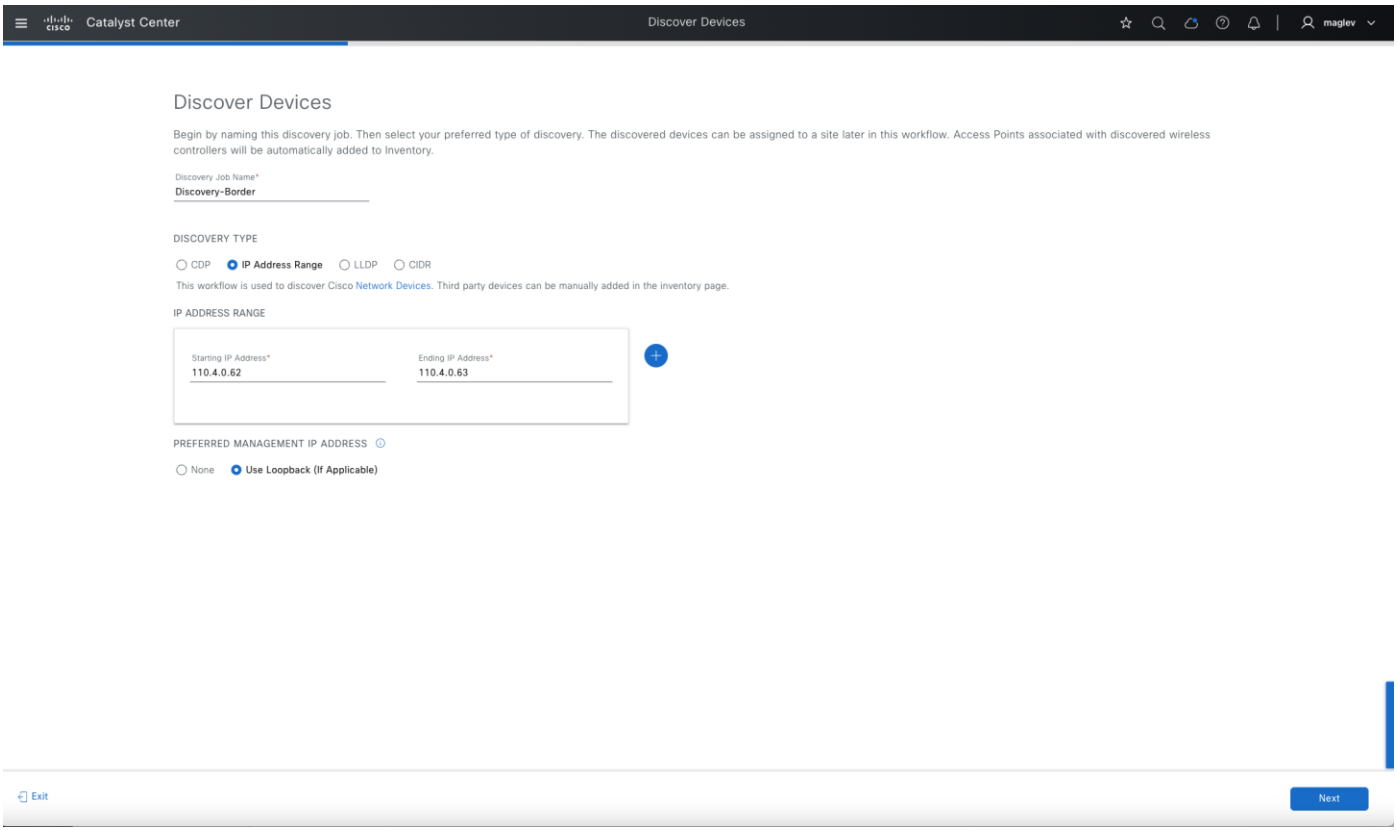
2 つの Catalyst 9300 スイッチが検出され、ファブリックボーダーとして機能します。

| デバイス | IP |
|---|---|
| Common-A | Loopback0：110.4.0.62 |
| Common-B | Loopback0：110.4.0.63 |

**ステップ 1.** メニューアイコンボタンから [Tools] > [Discovery] の順に選択し、右上の [Add Discovery] をクリックします。



**ステップ 2.** ワークフローに従います。必要な情報を入力してから、[Next] をクリックします。

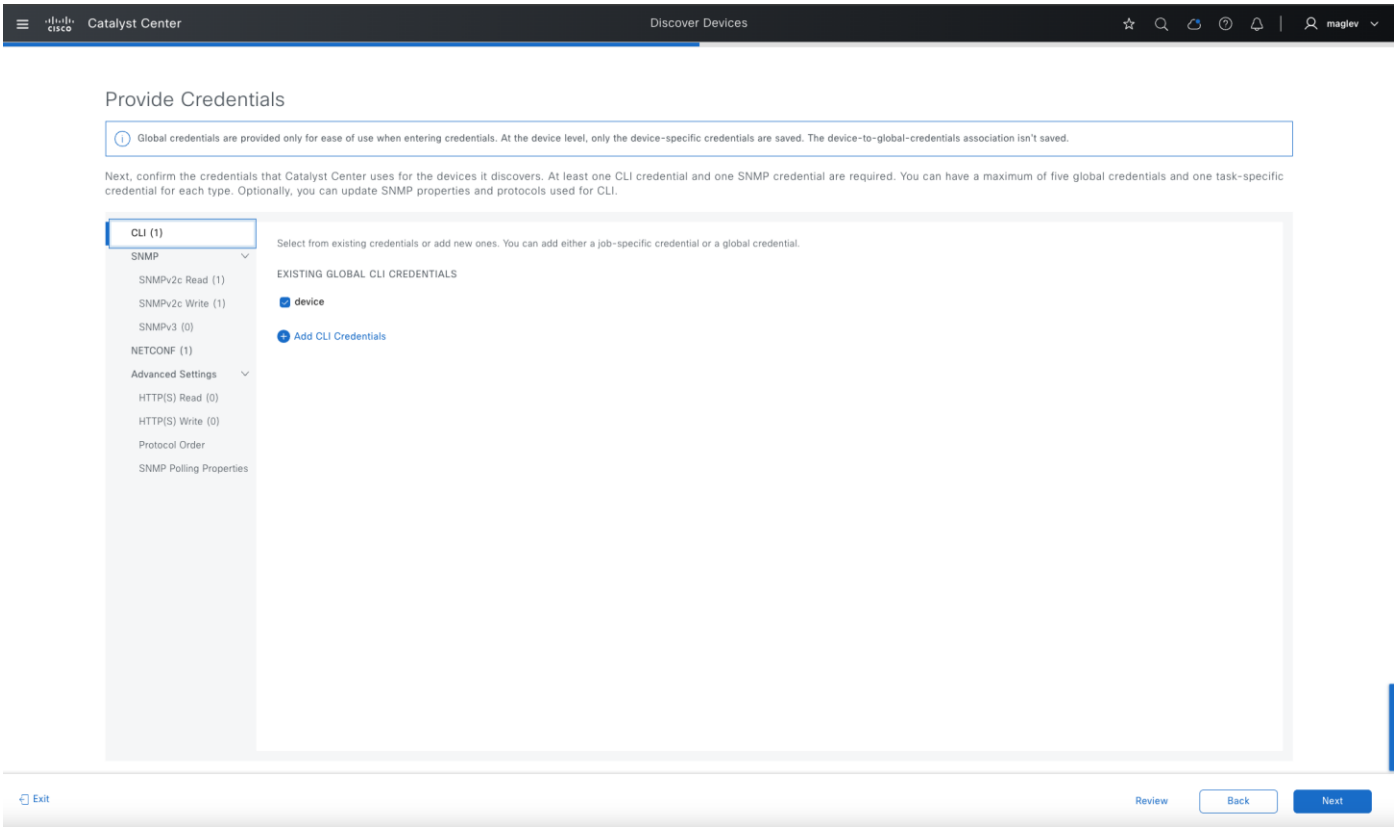



**ステップ 3.** ログイン情報を入力し、[Next] をクリックします。

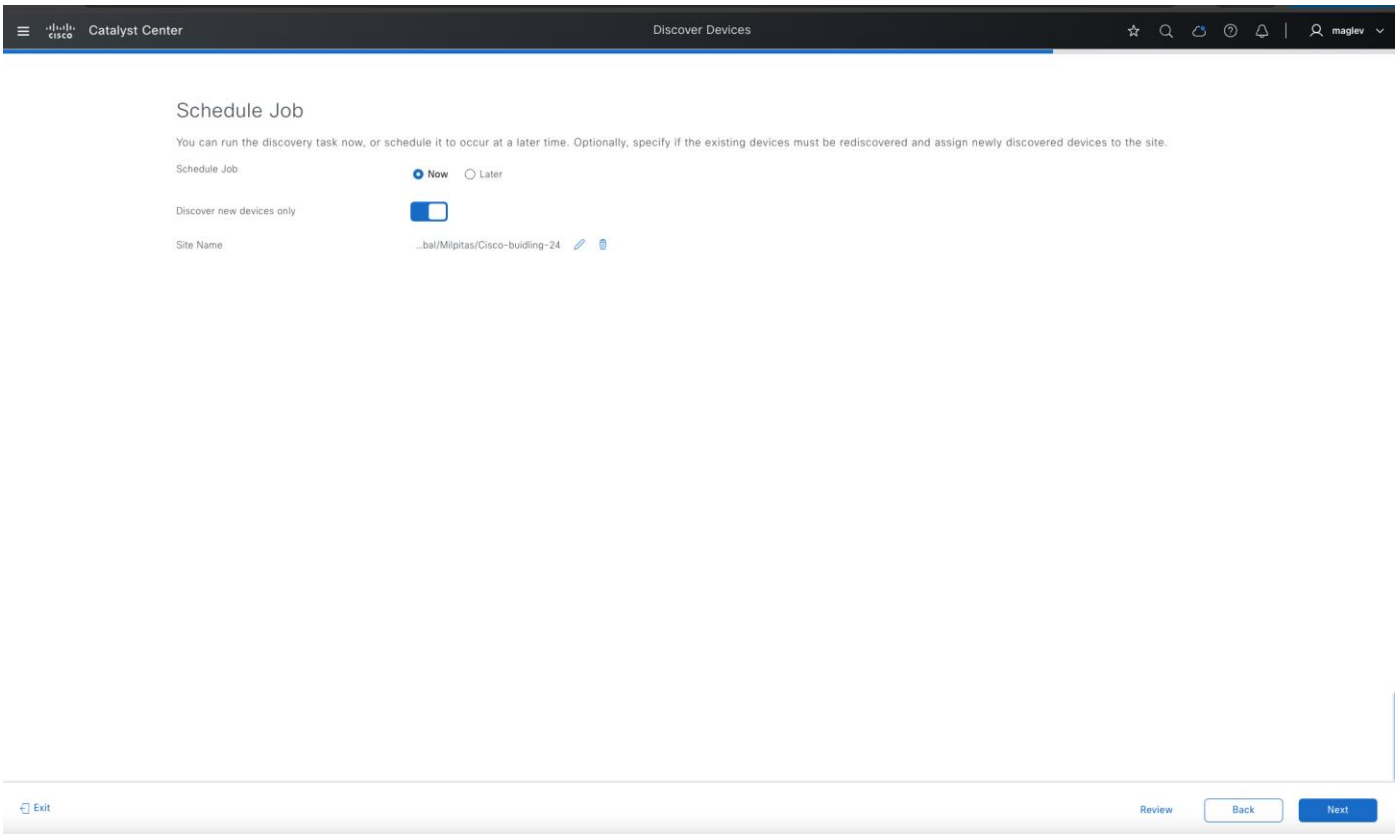
CLI および SNMP のログイン情報は必須です。Netconf は、Catalyst 9800 シリーズなどの IOS-XE ベースのワイヤレスコントローラには必須であり、オプションですが、アシュアランスを使用する IOS XE ベースの有線デバイスに推奨されます。

CLI ログイン情報は、デバイスの設定と一致する必要があります。

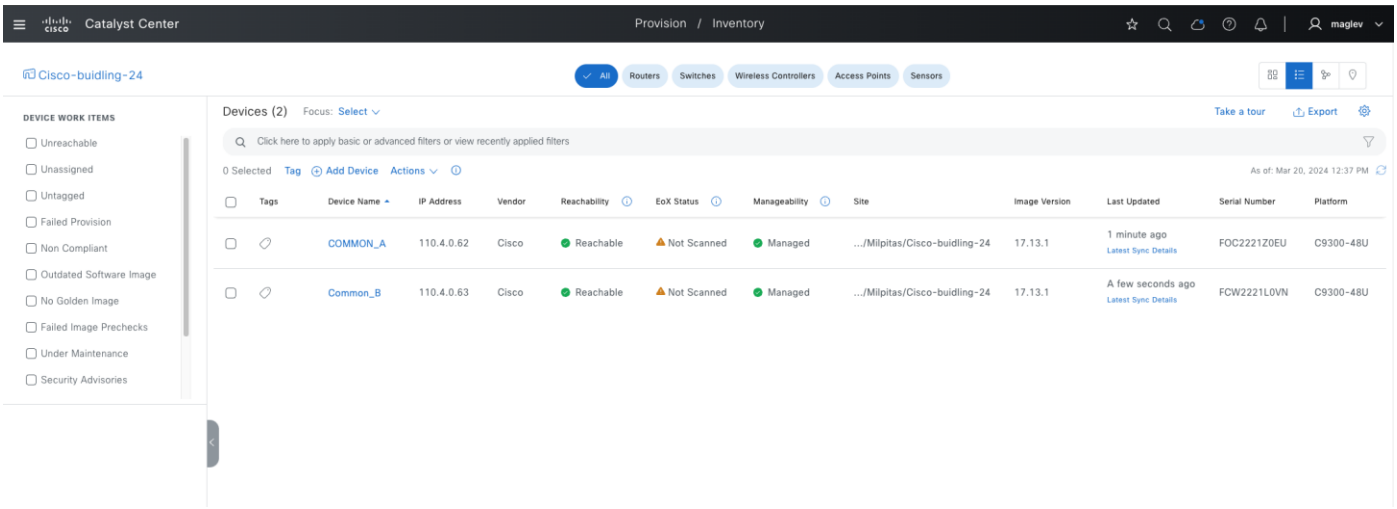
デバイスに設定されていない場合、サイト割り当てでの検出中に SNMP および Netconf のログイン情報がプッシュされます。




**ステップ 4.** サイトの割り当てを検出します。[Site Name] を **Cisco-building-24** に設定し、[Next] をクリックして検出を開始します。



**ステップ 5.** 検出完了後、[Inventory] ウィンドウで、両方のデバイスが追加され、[Manageability] ステータスが [Managed] になっていることを確認します。

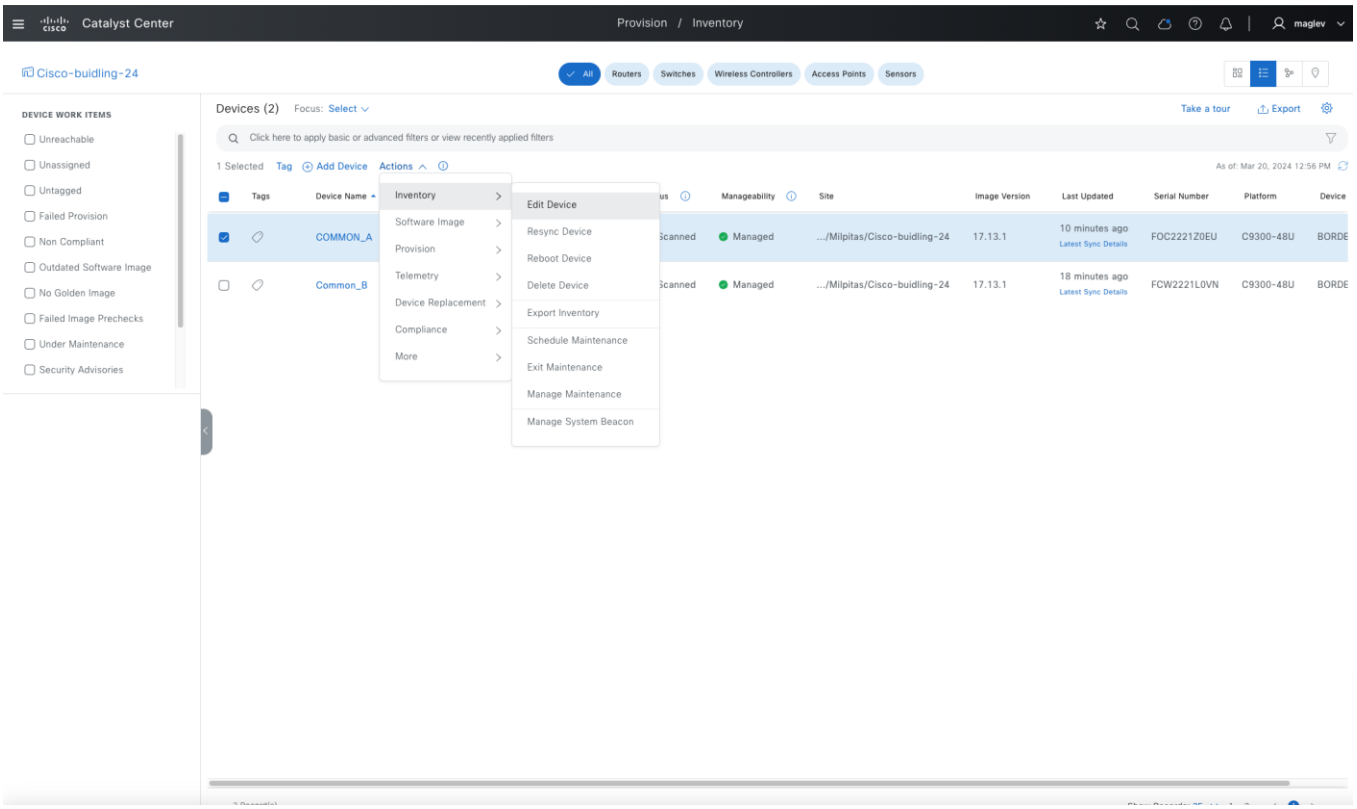



**ステップ 6.** デバイスロールを表示および変更します。

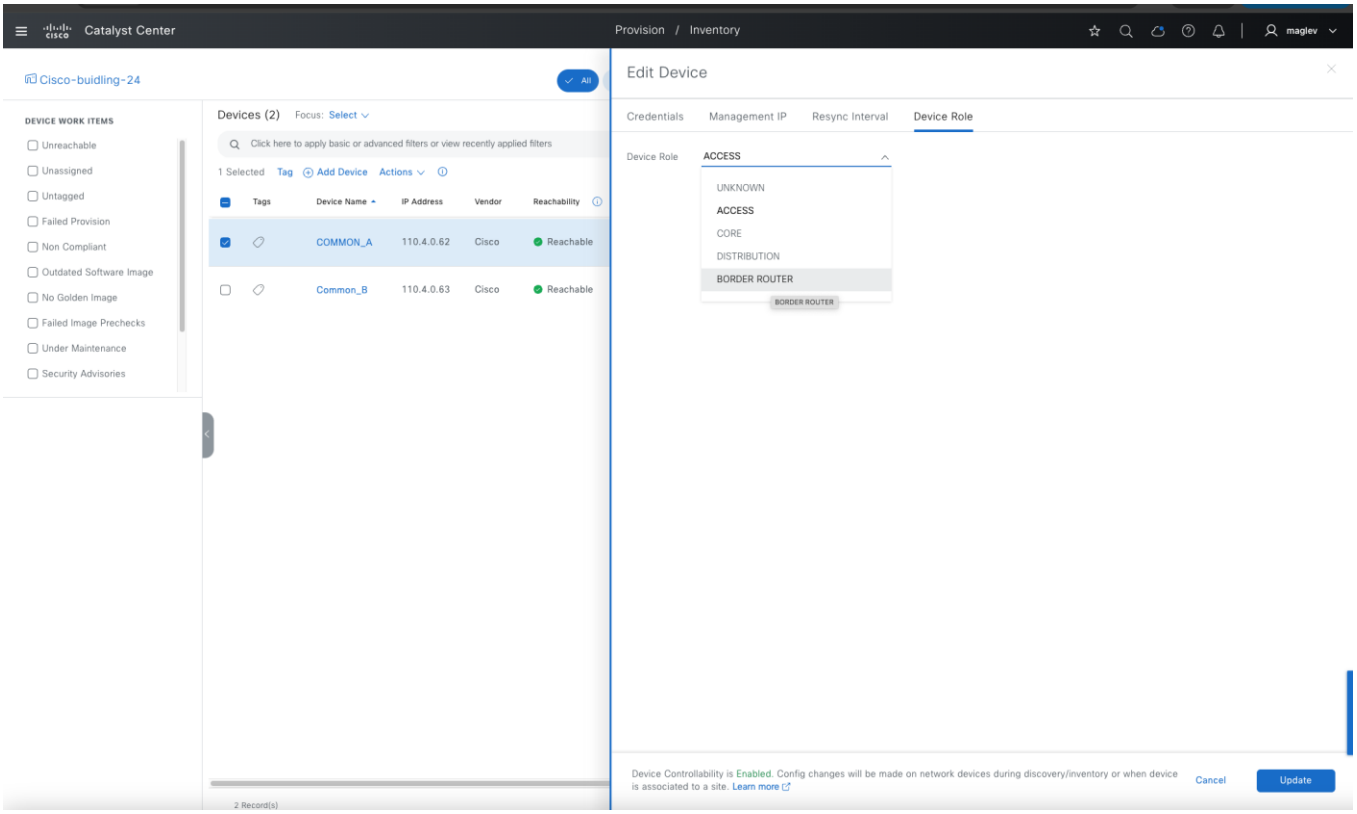
デバイスロールは、ファブリックサイトおよびトポロジツールの Catalyst Center トポロジマップにデバイスを配置するために使用されます。これらのアプリケーションおよびツールでのデバイス位置は、従来の 3 階層のコア、ディストリビューション、アクセスのレイアウトを使用して表示されます。

デバイスの制御性の設定（[Network Setting] > [Telemetry] > [Wired Endpoint Data Collection] で定義）も、アクセスロールを持つデバイスにプッシュされます。Catalyst 9300 スイッチには、デフォルトの「アクセス」デバイスロールがあります。サイトの割り当てによる検出中に、デバイスの制御性の設定を取得します。境界ルータに変更すると、これらの設定は削除されます。

**ステップ 7.** [Inventory] ウィンドウでデバイスを選択し、[Actions] > [Inventory] > [Edit Device] の順にクリックします。



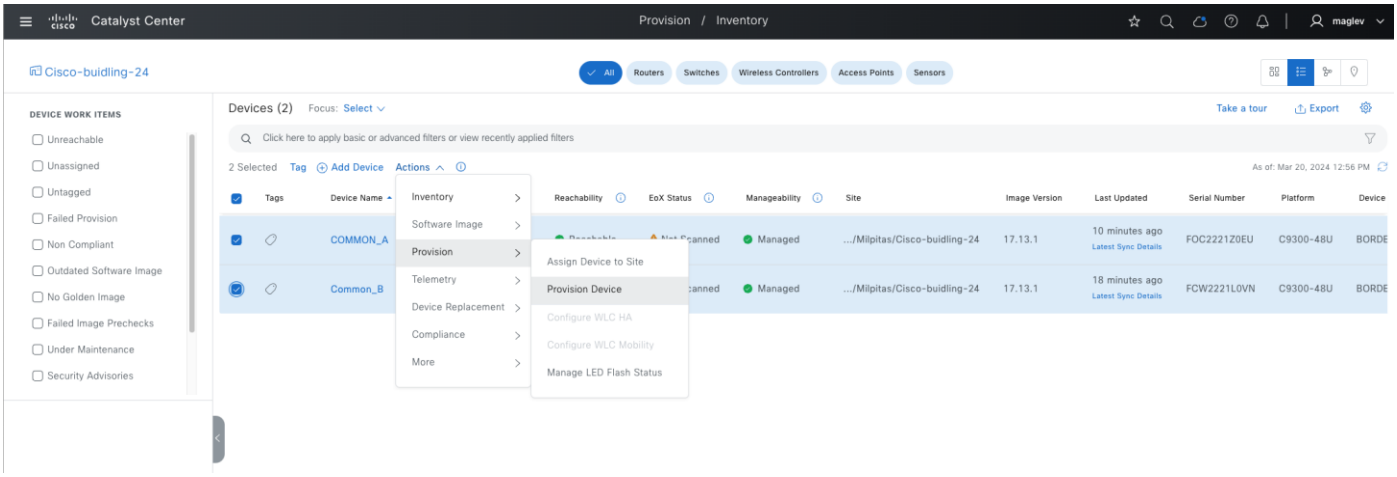

**ステップ 8.** [Device Role] タブで、両方のデバイスのロールを [Border Router] に変更します。



## 手順 2。　サイトへの Catalyst 9300 デバイスのプロビジョニング

サイトにデバイスをプロビジョニングすると、[Network Design] ウィンドウで定義された設定（AAA、DNS、NTP、テレメトリなど）がプッシュされます。デバイスは、プロビジョニング後にのみファブリックロールを割り当てることができます。

**ステップ 1.** 両方のデバイスのチェックボックスをオンにしてから、[Actions] > [Provision] > [Provision Device] を選択し、ワークフローを完了します。



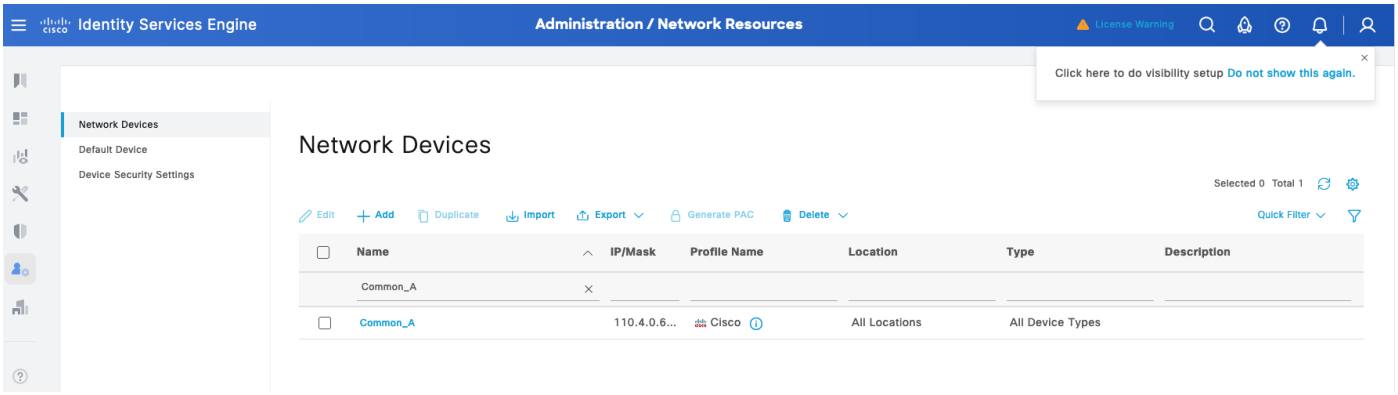

プロビジョニング後、デバイスが Cisco ISE に追加され、Cisco ISE から Cisco TrustSec 情報がダウンロードされます。

**ステップ 2.** デバイスから表示するには、`show cts environment-data` および `show cts pacs` コマンドを使用します。

**図 36.　Common_A からの出力**

```
Common_A#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-01:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 1 server(s):
 Server: 110.2.1.1, port 1812, A-ID AB6BE34E1352480E8C7702BED84235D3
         Status = ALIVE
         auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-01:Unknown
    2-01:TrustSec_Devices
    3-02:Network_Services
    4-05:Employees
    5-20:Contractors
    6-11:Guests
    7-00:Production_Users
    8-07:Developers

Common_A#show cts pacs
AID: AB6BE34E1352480E8C7702BED84235D3
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: AB6BE34E1352480E8C7702BED84235D3
  I-ID: 99f5296b57c64b32aea08ee983faae9e
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 22:00:40 UTC Fri Oct 18 2024
PAC-Opaque: 000200C80003000100040010AB6BE34E1352480E8C7702BED84235D3000600AC00030100F4CEBB1E5C1285B189BB83F3538089CE00000013669B041900093A80495D558499D6550F9927
077331FE8A7C23EECCBB9462FDE41950FE897D3AF83F564CD8747E6F5D434C9471C05A479EB4F569CF23D16F890E032A42520F7CDB3642837EB688C02DE32B08F3DF00DC317F498EDA30C675A
Refresh timer is set for 11w5d
```

**図 37.　Cisco ISE の Common_A。[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]**




## 手順 3。　ボーダーおよびコントロールプレーンノードとしての Catalyst 9300 の設定

ファブリックネットワークが機能するには、少なくともエッジノードとコントロールプレーンノードが必要です。これにより、エンドポイントはオーバーレイを介してパケットをトラバースして相互に通信できます（ポリシーに依存します）。ボーダーノードにより、ファブリック内部のエンドポイントからファブリック外部の宛先への通信が、外部から内部への逆フローとともに可能になります。

ファブリックサイトに最初に追加されるデバイスには、コントロールプレーンロールが必要です。スタンドアロン コントロール プレーン ノード、共存ボーダーおよびコントロールプレーンノードまたは FiaB になります。コントロール プレーン デバイスが追加されると、Catalyst Center は、ファブリックサイトを LISP/BGP または LISP Pub/Sub（推奨）として設定するためのオプションを提供します。ファブリックサイトでは、最大 6 つのコントロールプレーンノードがサポートされます。

ボーダーノードをプロビジョニングする場合、GUI には異なる自動化オプションがいくつか表示されます。

- レイヤ 3 ハンドオフ、レイヤ 2 ハンドオフ、またはその両方を使用できます（プラットフォームに依存）。
- IP トランジット、SD-Access トランジット、またはその両方に接続できます（プラットフォームに依存）。
- インターネットへの接続（外部ボーダー）、ファブリックサイトの外部にある他の非インターネットの場所への接続（内部ボーダー）、またはその両方（内外ボーダー）を提供できます。

**外部ボーダー**

インターネット、WAN、MAN などの不明なルートに接続されます。これは、ローカルサイトのファブリックオーバーレイ用ラストリゾートゲートウェイです。外部ボーダーは、すべてのファブリックサブネットを eBGP サマリールートとしてファブリックサイトの外部にエクスポートします。Cisco SD-Access トランジットに接続されたボーダーでは、常に外部ボーダー機能を使用する必要があります。

**内部ボーダー**

データセンター（DNS を使用した DHCP などの共有サービス）など、展開内の既知のルートに接続されます。このボーダーは、すべてのファブリックサブネットを eBGP サマリールートとしてファブリックサイトの外部にエクスポートし、これらの eBGP で学習したルートをファブリックサイトの外部からサイトローカルのコントロールプレーンノードにインポートして登録します。

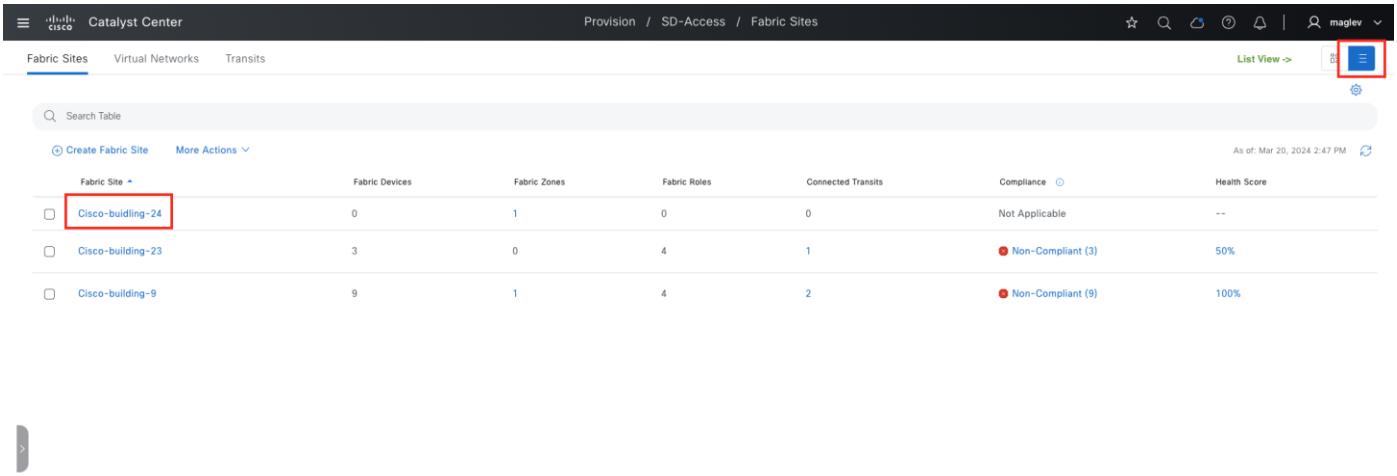
**内外ボーダー**

内部と外部の両方のボーダーとして機能し、ネットワークが 1 セットのデバイスを使用してサイトから出る場合に使用されます。既知のルートと不明なルートの両方に直接接続されます。

このセクションでは、2 つの Catalyst 9300 スイッチをファブリックサイト **Cisco-building-24** に追加し、ボーダーロールとコントロールプレーンロールをコロケーションさせます。LISP Pub/Sub が設定されています。IP トランジットと Cisco SD-Access トランジットについては、「トランジットの設定」で説明しています。

**注：** ファブリックサイトにデバイスを追加するには、Loopback0 インターフェイスが必要です。前に loopback0 アドレスを設定するか、LAN の自動化を使用して設定します。

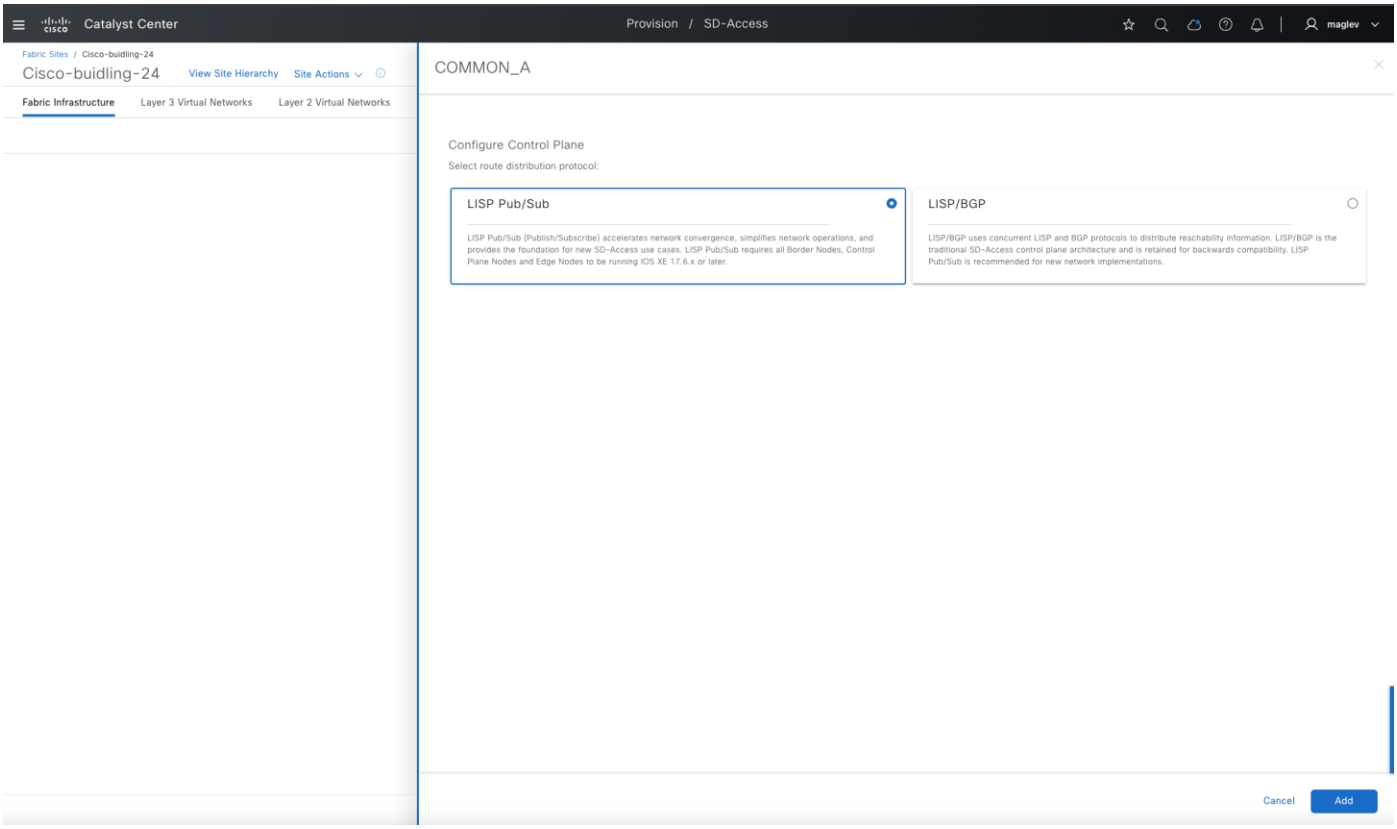
**ステップ 1.** メニューアイコンボタンから [Provision] > [Fabric Sites] の順に選択し、テーブルビューアイコンをクリックして [Cisco-building-24] をクリックします。




**ステップ 2.** デバイスの 1 つをクリックします（ファブリックロールのないデバイスはグレー表示されます）。

**ステップ 3.** 右のサイドバーで、**コントロールプレーンノード**と**ボーダーノード**を有効にします。

- **コントロールプレーンノード**の場合は、[LISP Pub/Sub] > [Add] の順にクリックします。



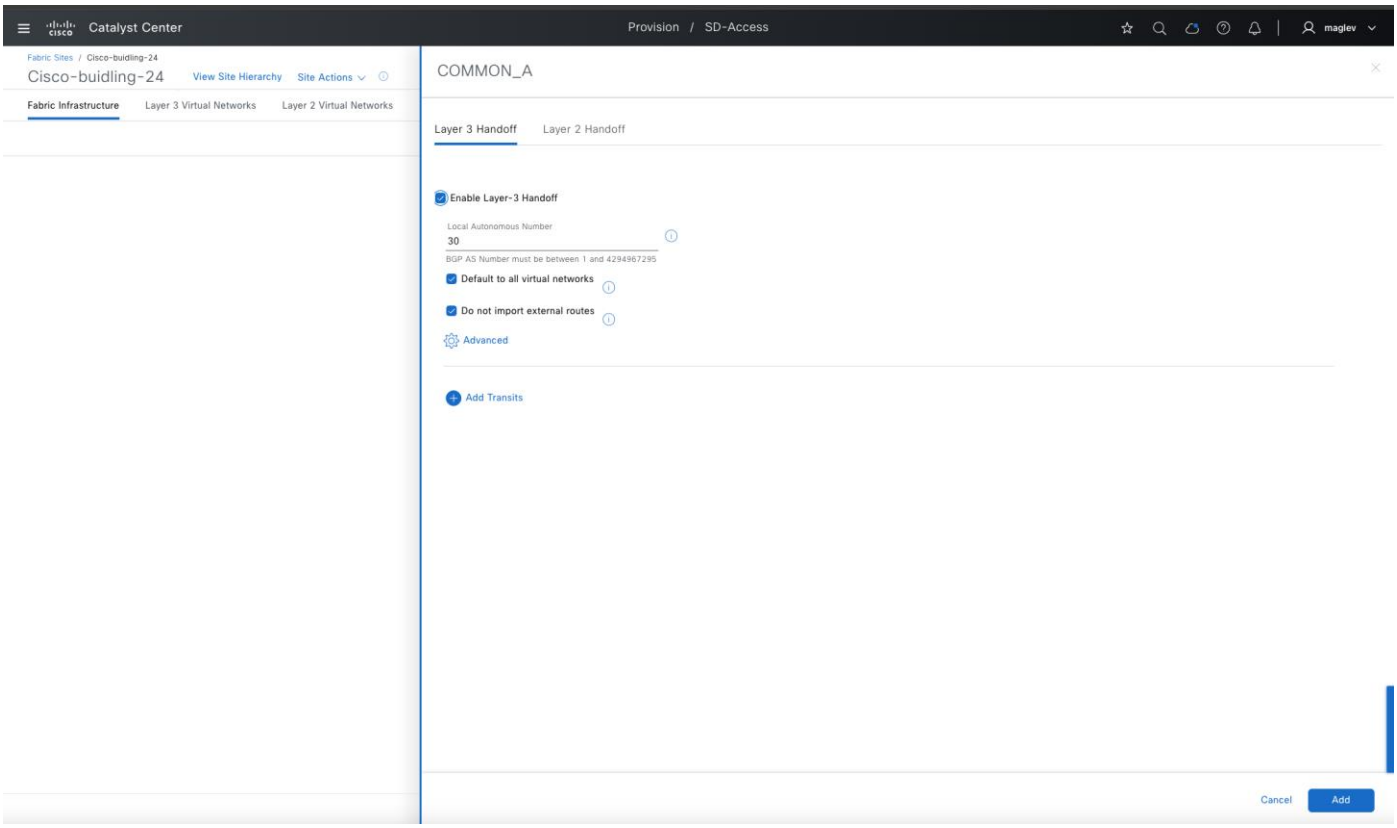

- **ボーダーノード**の場合は、[Enable Layer-3 Handoff] チェックボックスをオンにします。

ローカル AS 番号は、ボーダーデバイスの BGP AS 番号です。事前設定することができますが、事前設定しない場合は、Catalyst Center が設定をデバイスにプロビジョニングします。

**表 23.** 内部ボーダー、外部ボーダー、内外ボーダーのオプション

| | すべての仮想ネットワークをデフォルトで設定 | 外部ルートをインポートしない |
|---|---|---|
| 内部ボーダー | – | 適用対象外 |
| 外部ボーダー | ✓ | ✓ |
| 内外ボーダー | ✓ | – |

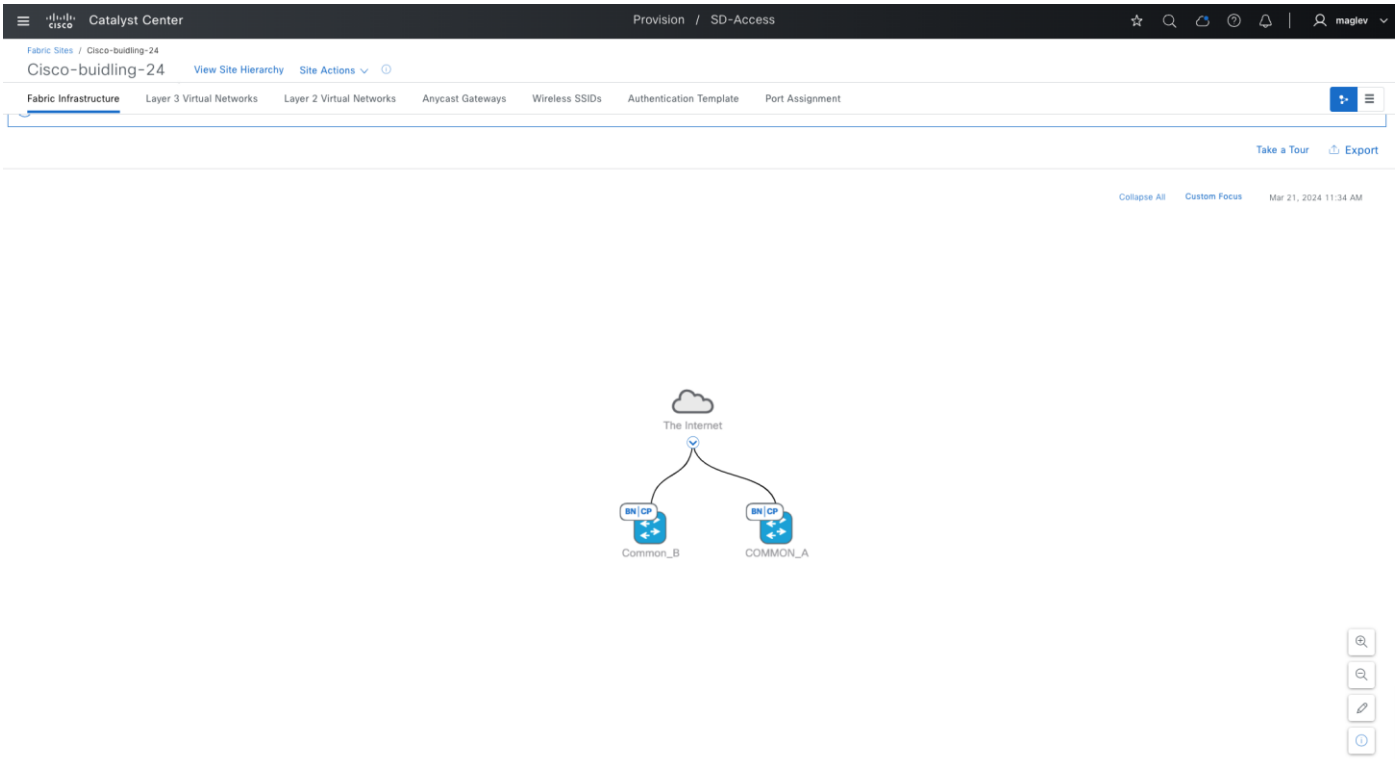
**ステップ 4.** Catalyst 9300 を外部ボーダーとして設定します。[Default to all virtual networks] および [Do not import external routes] チェックボックスをオンにしてから [Add] をクリックします。




**ステップ 5.** ワークフローを完了して設定を **Common-A** にプロビジョニングし、**Common-B** で同じ手順を繰り返します。

**注：** **Common-A** はすでに LISP Pub/Sub のコントロールプレーンノードとして設定されているため、**Common-B** を 2 番目のコントロールプレーンノードとして設定すると、LISP BGP と LISP Pub/Sub を選択するオプションは無効になります。

プロビジョニング後、トポロジビューの両方のデバイスは、ファブリックロールが **BN|CP** としてタグ付けされて青色に表示されます。




## LAN の自動化による中間スイッチとファブリックエッジのオンボーディング

LAN の自動化では最大 2 台のシードデバイスが使用され、シードデバイスから開始すると、ネットワーク階層内で最大 5 つのレイヤまで「ウォークアウト」でき、PnP プロセスで検出された新しいデバイスの展開を自動化できます。LAN の自動化は、直接接続されたネイバーでのみ開始され、後で Cisco SD-Access ファブリックのオーバーレイに適したアンダーレイの展開をサポートすることを目的としています。

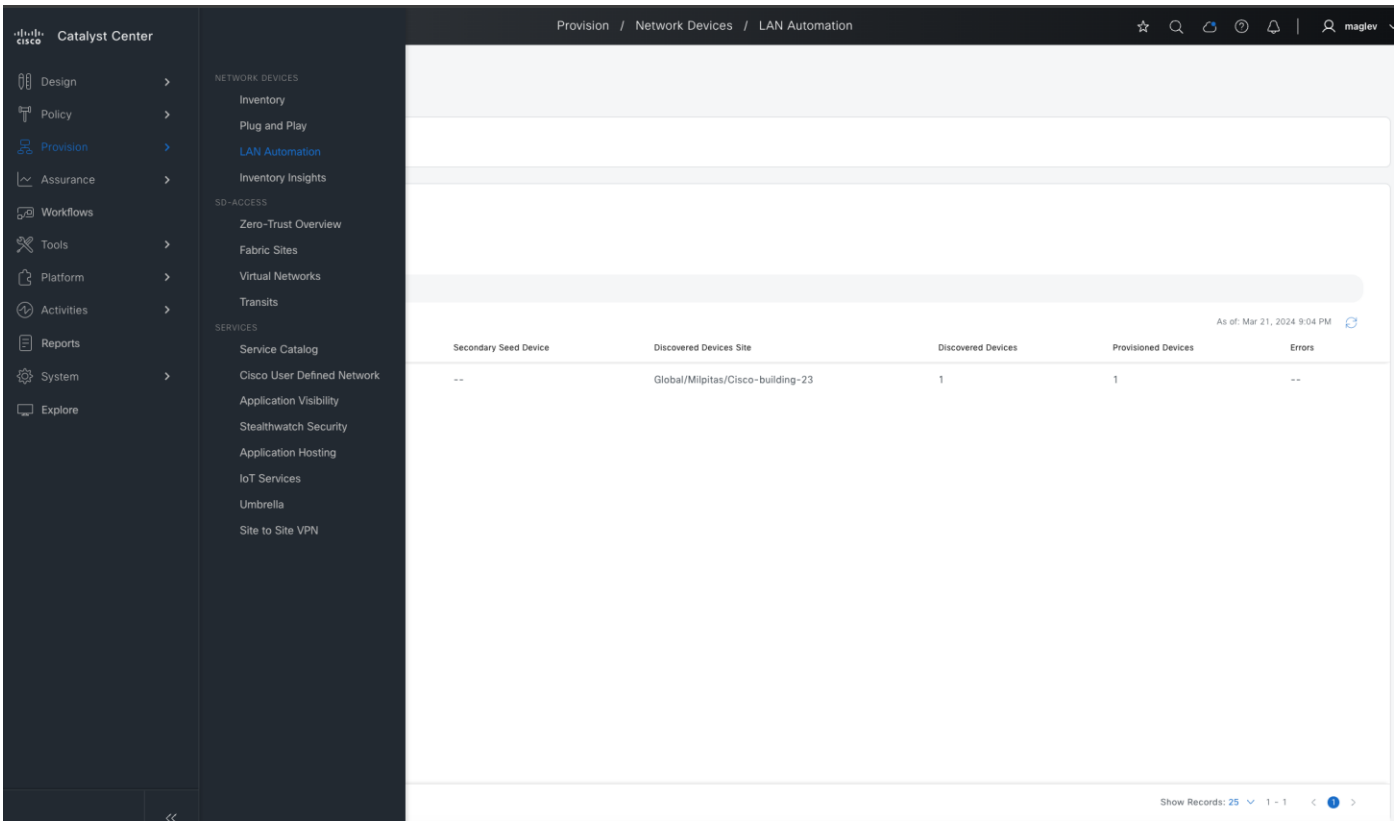
LAN の自動化を開始するには、シードデバイスと LAN プールが必要です。Catalyst Center は、LAN プールサブネットに到達できる必要があります。

現在、LAN の自動化は ISIS プロトコルのみをサポートしており、ルータプラットフォームはシードデバイスとしてサポートされていません。LAN の自動化の詳細については、「Cisco Catalyst Center SD-Access LAN Automation Deployment Guide」を参照してください。

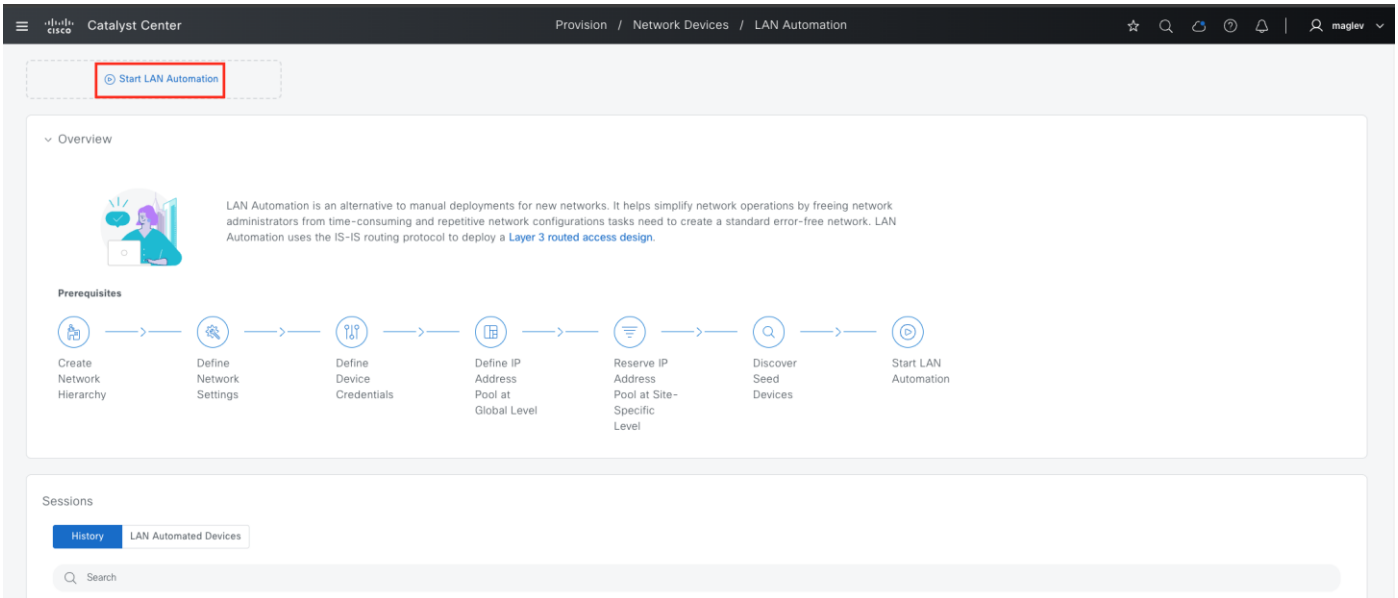
このセクションでは、**Common-A** と **Common-B** をシードデバイスとして使用し、2 階層のデバイスがオンボードされます。階層 1 は、中間スイッチとして使用されます。階層 2 は、ファブリックエッジとして使用されます。

## 手順 1。　デバイスを検出するための LAN の自動化

**ステップ 1.** LAN の自動化を開始するには、左上隅にあるメニューアイコンをクリックし、[Provision] > [LAN Automation] の順に選択します。

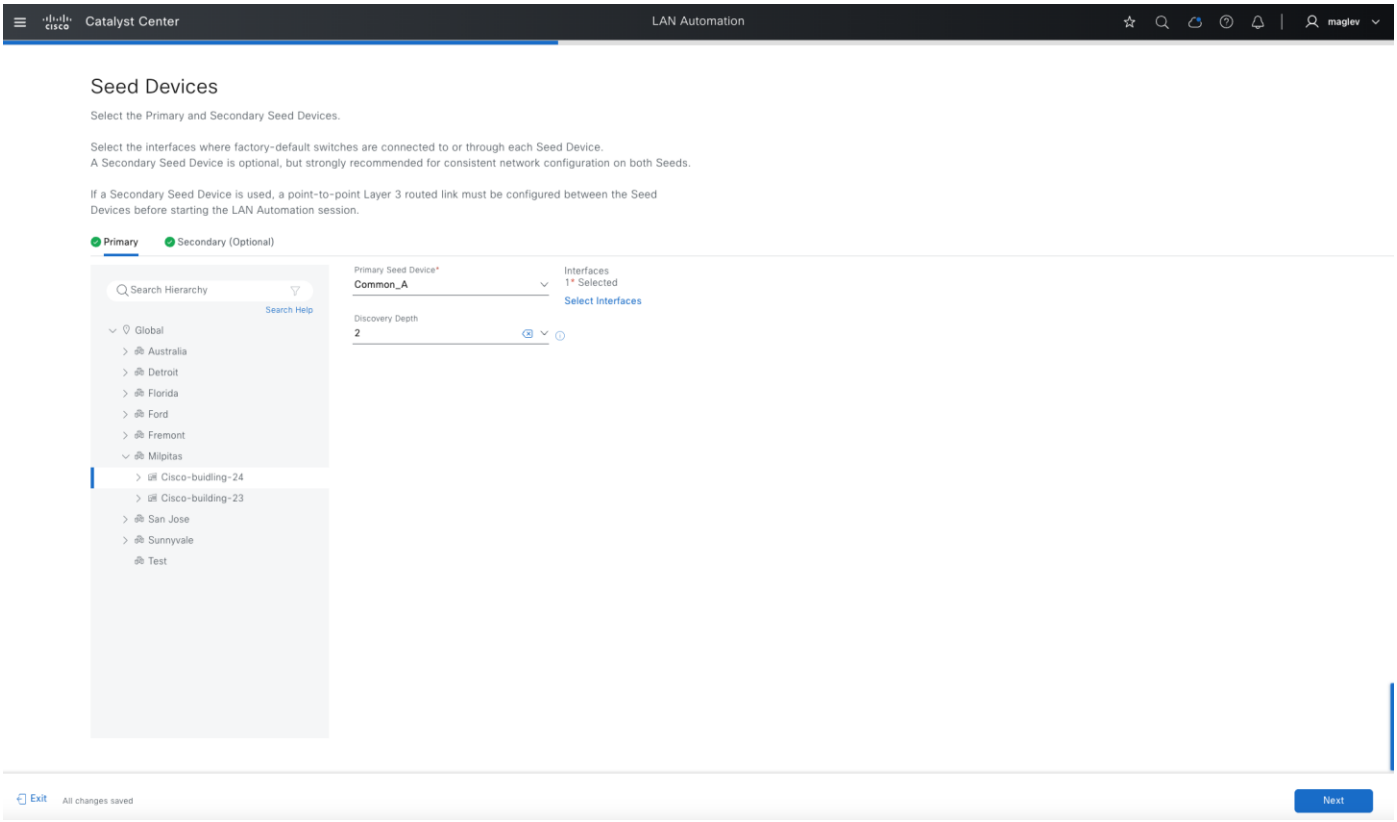


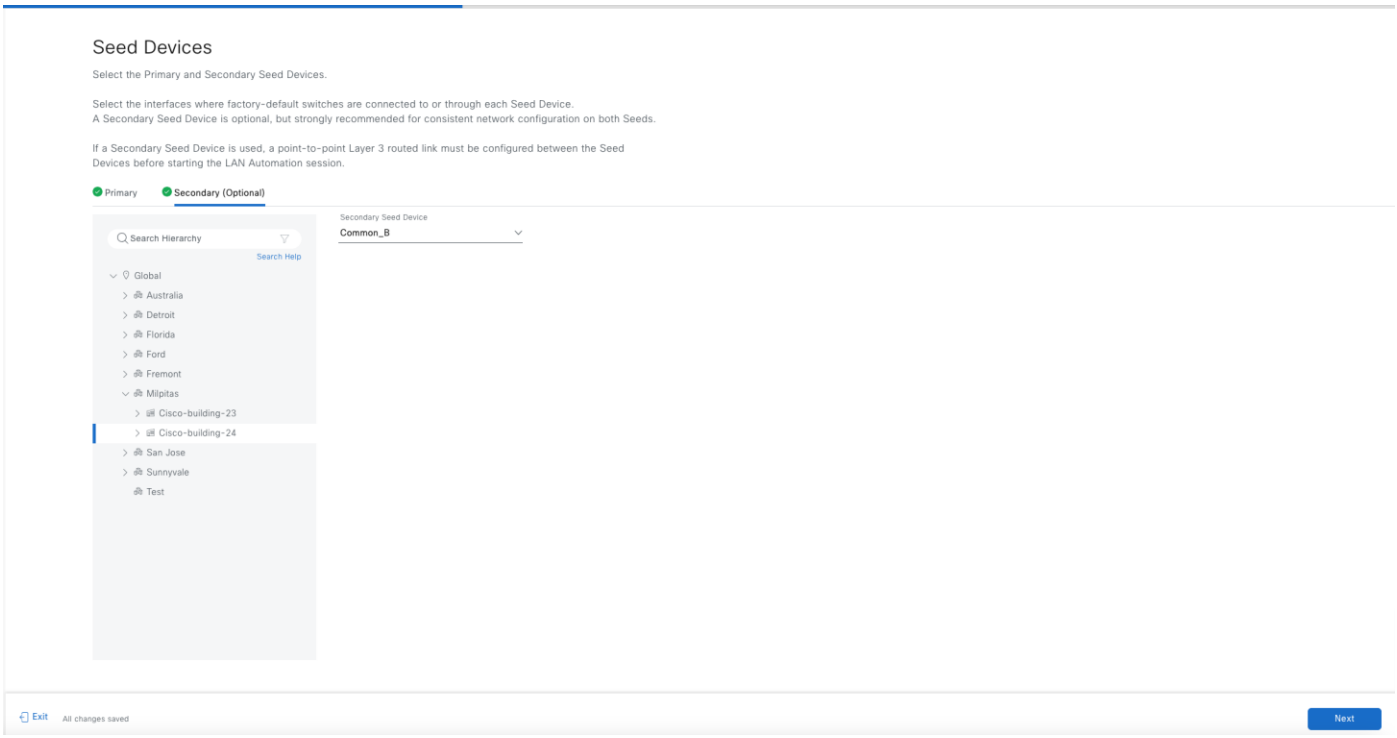

**ステップ 2.** [Start LAN Automation] をクリックします。



**ステップ 3.** [Hierarchy] ペインから [Cisco-building-24] を選択します。必要なフィールド情報を入力し、[Seed Devices] ウィンドウで [Next] をクリックします。

| フィールド | 値 |
|---|---|
| Primary | Common-A |
| Interfaces | GigabitEthernet1/0/10 |
| Discovery Depth | 2 |
| Secondary | Common-B |

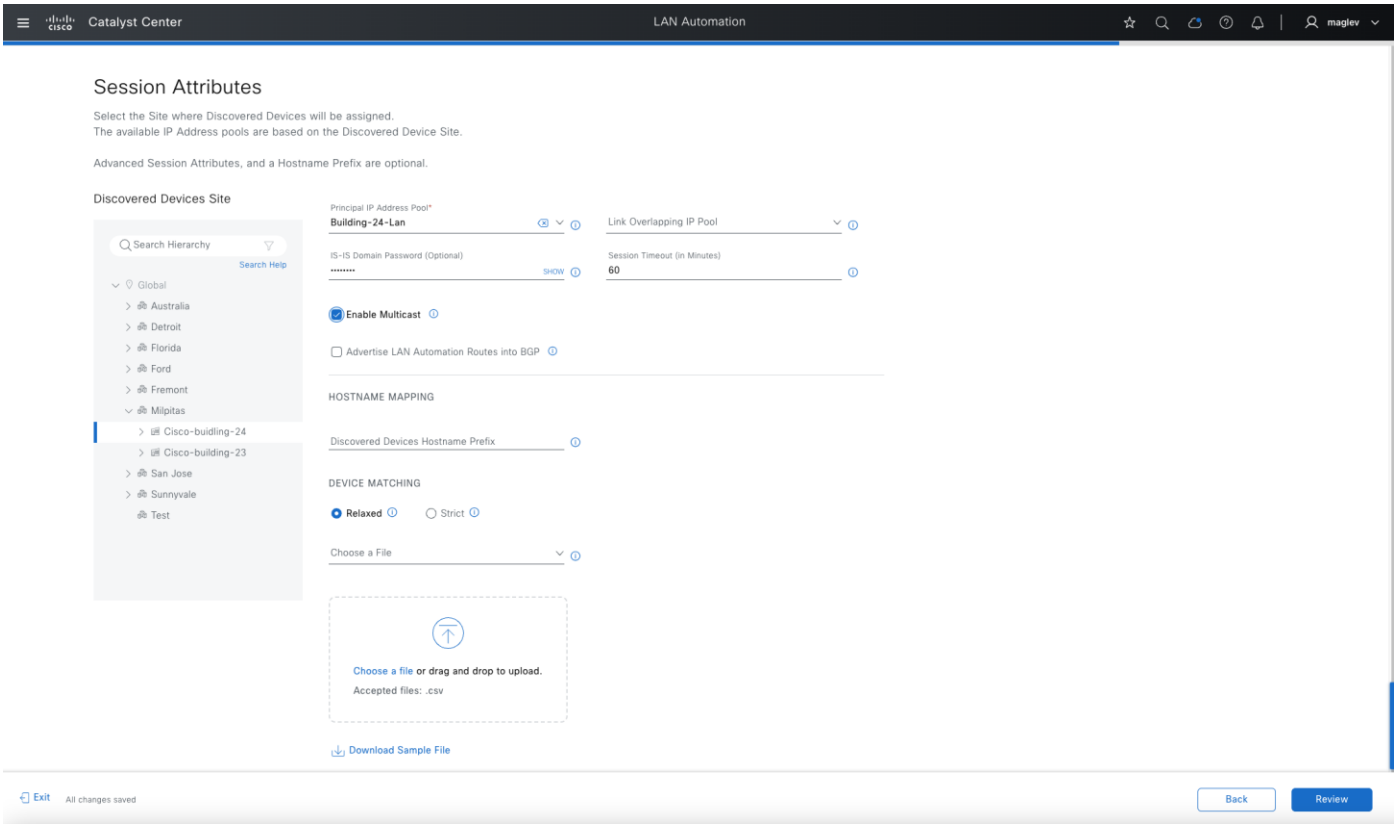





**ステップ 4.** セッション属性は、高度な設定とセッション制御を定義します。

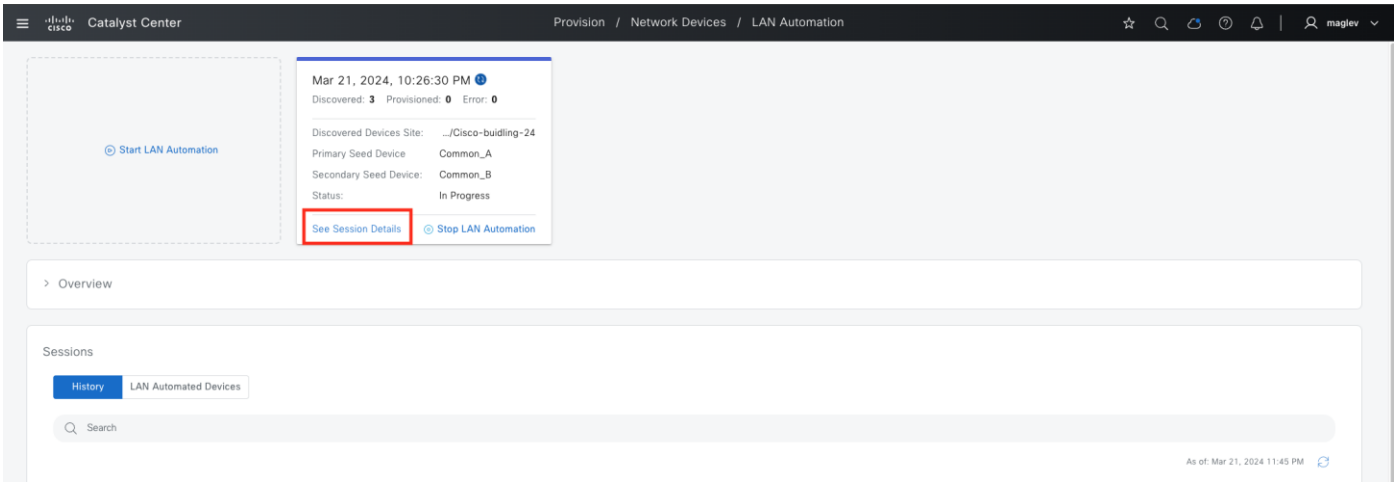
**表 24.** この展開で使用されるセッション属性

| フィールド | 値 | 使用目的 |
|---|---|---|
| Principal IP Address Pool | Building-24-Lan | レイヤ 3 リンク、ループバック IP、ネイティブ マルチキャスト アンダーレイ |
| IS-IS Domain Password（オプション） | Cisco123 | IS-IS |
| Session Timeout | 60 分 | 60 分後に LAN の自動化を自動停止します。指定されていない場合は、手動で停止する必要があります。安定したネットワークでのみの推奨です。安定していない場合は、より長いタイムアウト（最大 1 週間）を使用します |
| Enable Multicast | ✓ | シードデバイスをネイティブマルチキャスト RP として設定し、検出されたデバイスをマルチキャストトラフィックのサブスクライバとして設定します |

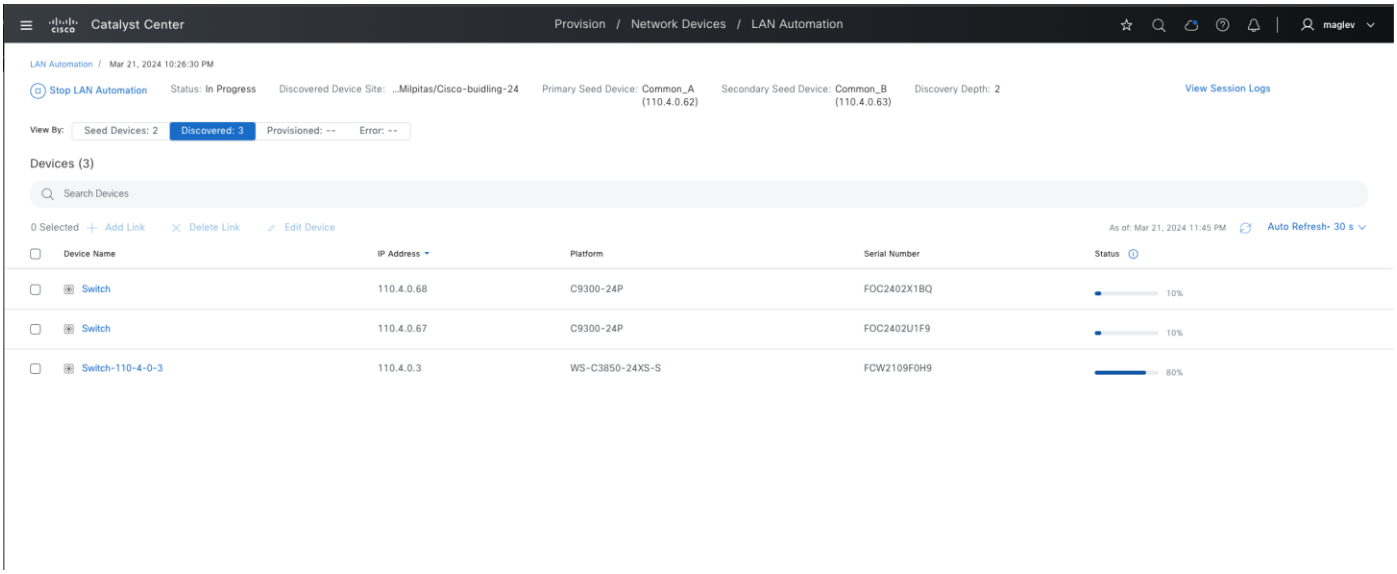



**ステップ 5.** [Review] ウィンドウで、情報が正しいことを確認し、[Start] をクリックします。

**ステップ 6.** [LAN Automation] ダッシュボードで、[Session] ステータスを監視するか、[See Session Details] をクリックします。



**ステップ 7.** [Discovered] を選択し、各デバイスの進行状況を確認します

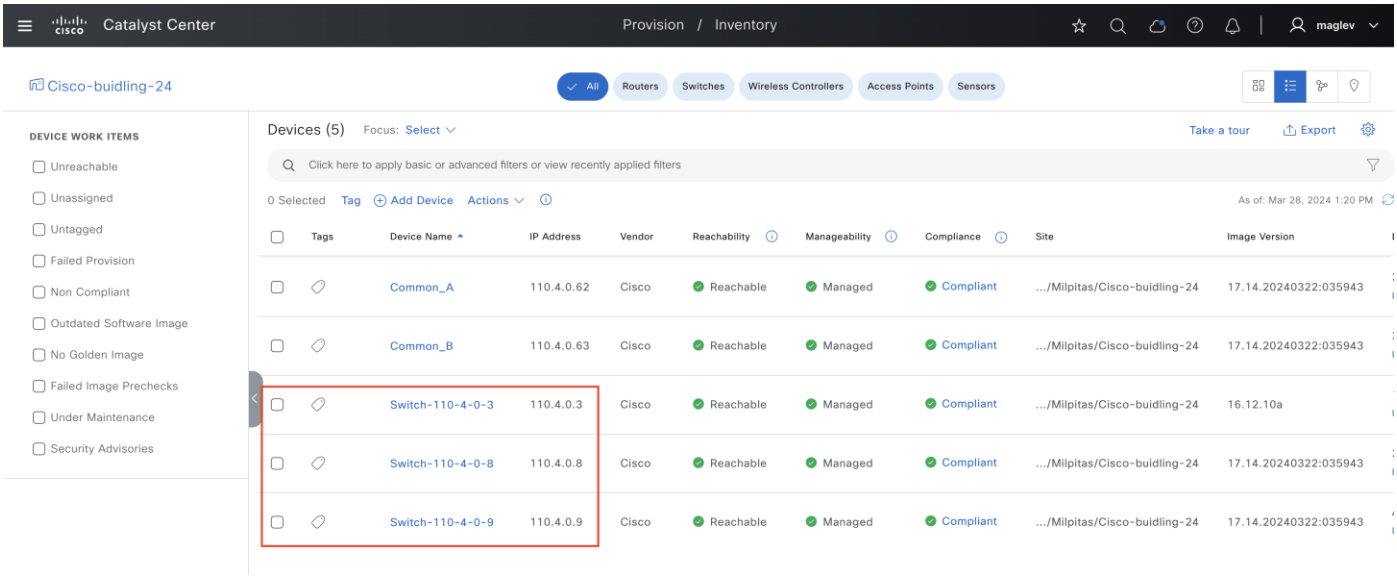



**注：** この展開の Catalyst 3850 スイッチは階層 1 スイッチ（中間ノードとして使用）であり、階層 2 スイッチ（2x Catalyst 9300）は、階層 1 スイッチがインベントリで管理ステータスになった後、LAN の自動化で処理されます。

すべてのデバイスがインベントリで検出されて管理されたら、LAN の自動化を停止してリンクをレイヤ 3 リンクに変換できます。または、セッションタイムアウトの期限が切れたときに、オンボーディングプロセスにデバイスがない場合は、LAN の自動化が自動的に停止します。

**技術的なヒント：** ゴールデンイメージが**イメージリポジトリ**でマーク付けされている場合、PnP プロセス中に、検出されたデバイスはゴールデンイメージにアップグレードされます。

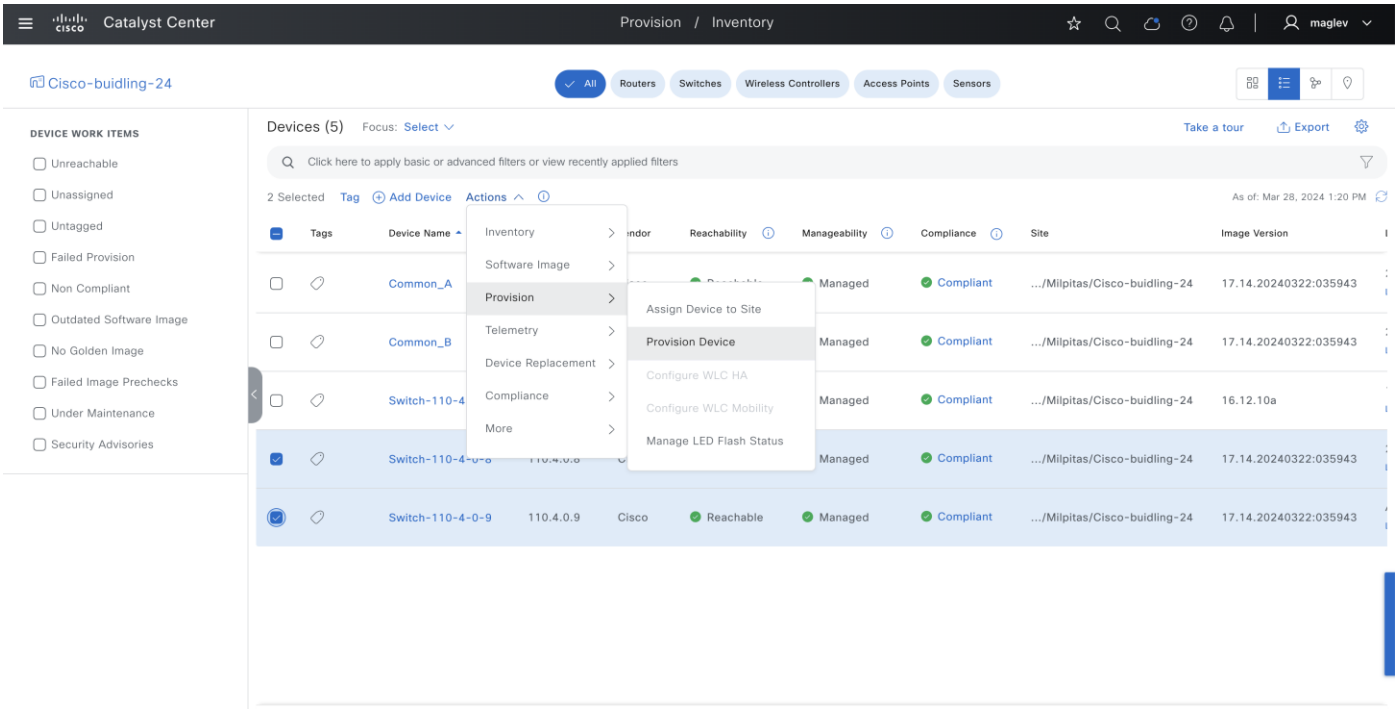
3 台のデバイスすべてが Catalyst Center にオンボーディングされます。



## 手順 2。　ファブリックエッジとしてのファブリックへの検出されたデバイスのプロビジョニング

LAN の自動化によってオンボードされたデバイスは、ファブリックロールの割り当てを使用してファブリックに追加する前に、[Provision/Inventory] ウィンドウからプロビジョニングする必要があります。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] を選択し、[Actions] > [Provision] > [Provision Device] を選択します。

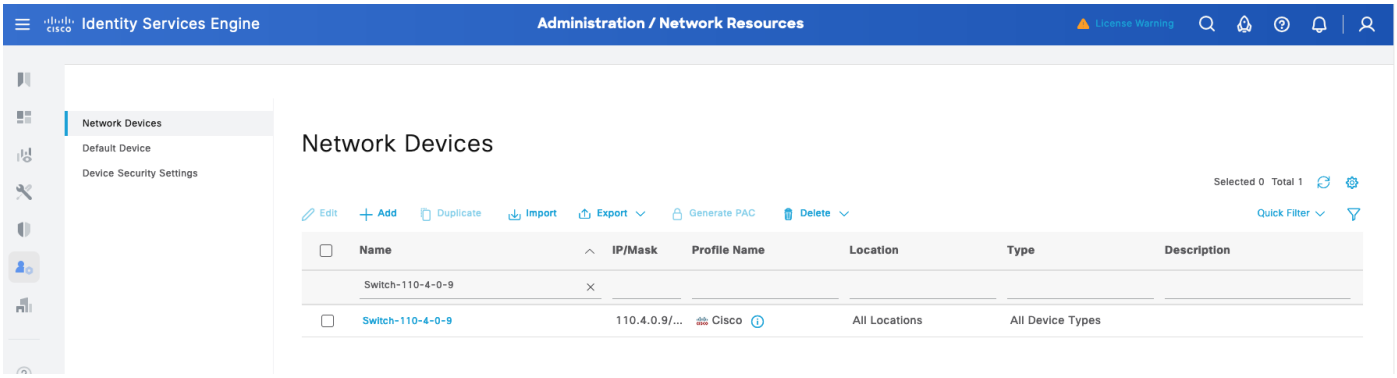



ボーダーデバイスと同様に、LAN の自動化デバイスは Cisco ISE に追加され、Cisco TrustSec 情報がダウンロードされます。

**図 38.　デバイスの出力例**

```
Switch-110-4-0-9#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-01:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 1 server(s):
 Server: 110.2.1.1, port 1812, A-ID AB6BE34E1352480E8C7702BED84235D3
         Status = ALIVE
         auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-01:Unknown
    2-01:TrustSec_Devices
    3-02:Network_Services
    4-05:Employees
    5-20:Contractors
    6-11:Guests
    7-00:Production_Users
    8-07:Developers

Switch-110-4-0-9#show cts
Switch-110-4-0-9#show cts pac
Switch-110-4-0-9#show cts pacs
AID: AB6BE34E1352480E8C7702BED84235D3
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: AB6BE34E1352480E8C7702BED84235D3
  I-ID: FOC2402U1F9
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 22:00:47 UTC Fri Oct 18 2024
PAC-Opaque: 000200B80003000100040010AB6BE34E1352480E8C7702BED84235D30006009C00030100F7B5926B4869952CFA281FC52B12400E00000013669B041900093A80495D558499D6550F9927B2FD7956750C6E6
4EF4E4373581881DC13691F8BCC7DCB6C1E5E70238D95DB9CBA4AF584D342669431BA9349FE51C7DA1D9EAACAA3C45B630C996319B577B4D936ECCDCD
Refresh timer is set for 11w5d
```

**図 39.　　デバイスが Cisco ISE に追加される**




**ステップ 2.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] を選択し、デバイスを右クリックして [Edge Node] を有効にし、[Add] をクリックします。

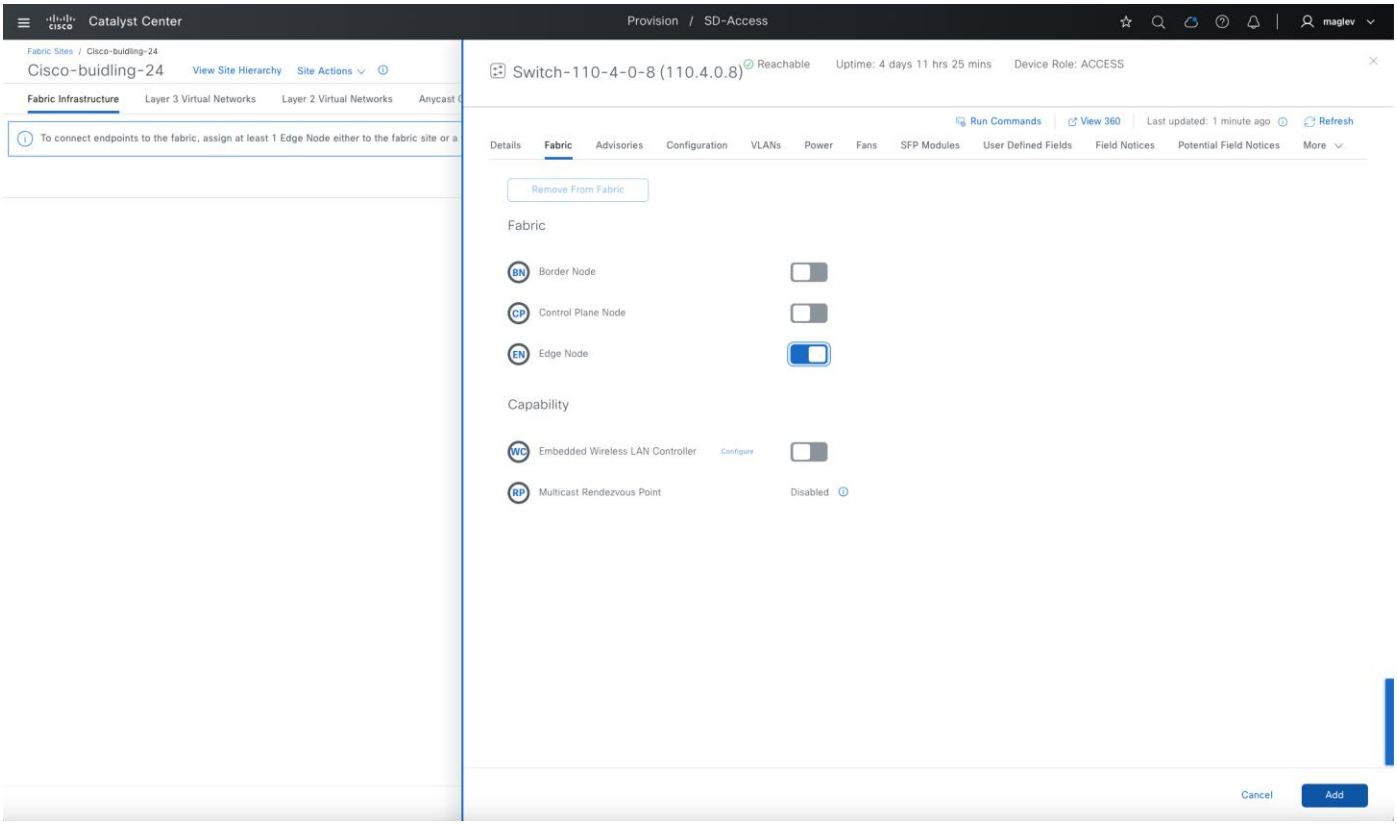
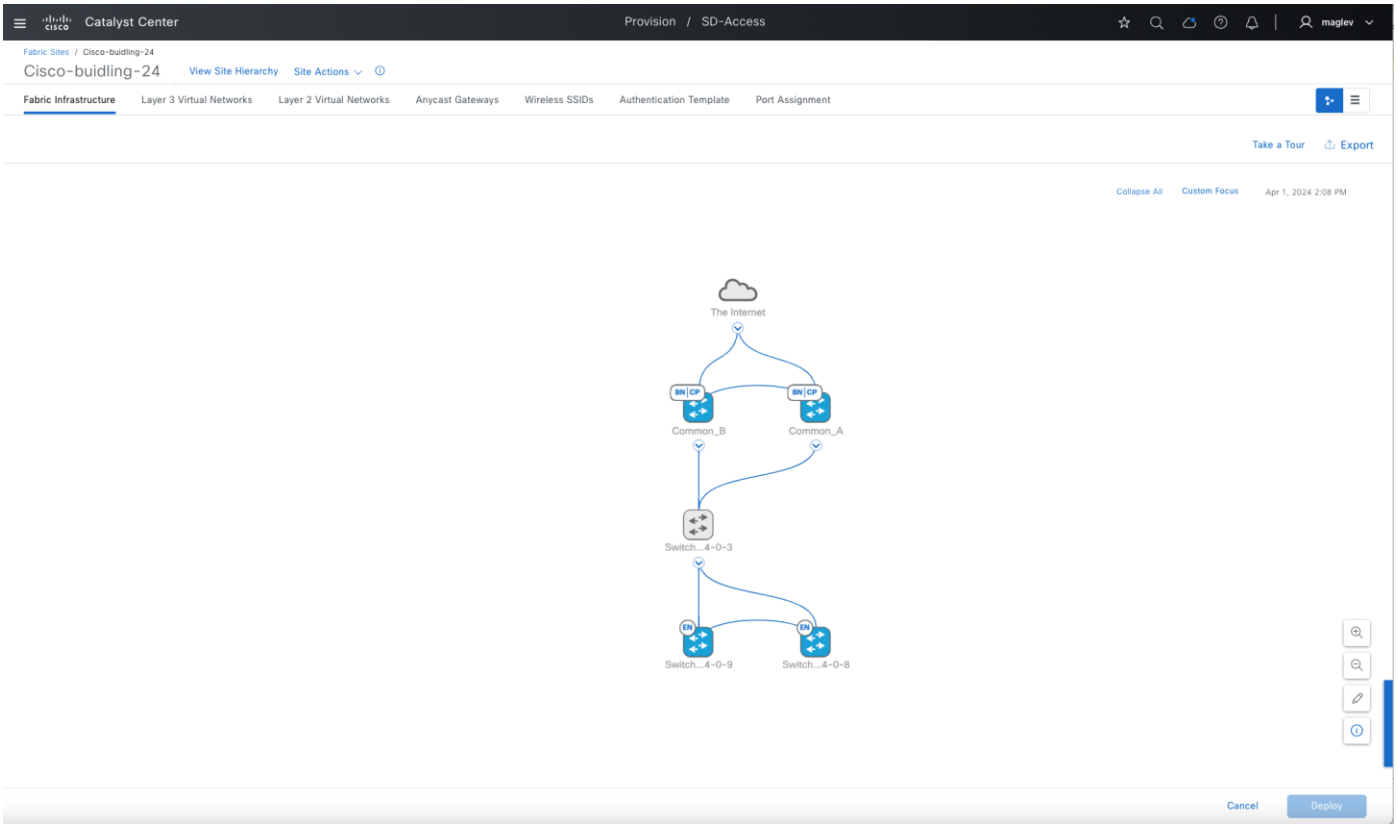


**図 40.　　両方のデバイスをエッジノードとして追加すると、それらは EN ロールでマーク付けされる**




**ステップ 3.**　[Deploy] をクリックします。

## 組み込みワイヤレスコントローラを使用した Cisco SD-Access ワイヤレスの設定

組み込みワイヤレスコントローラは、ボーダーロールおよびコントロールプレーンロール、エッジロール、または FiaB を持つ Catalyst 9000 デバイスで有効にできます。ワイヤレスサブパッケージと Netconf-yang が必要です。

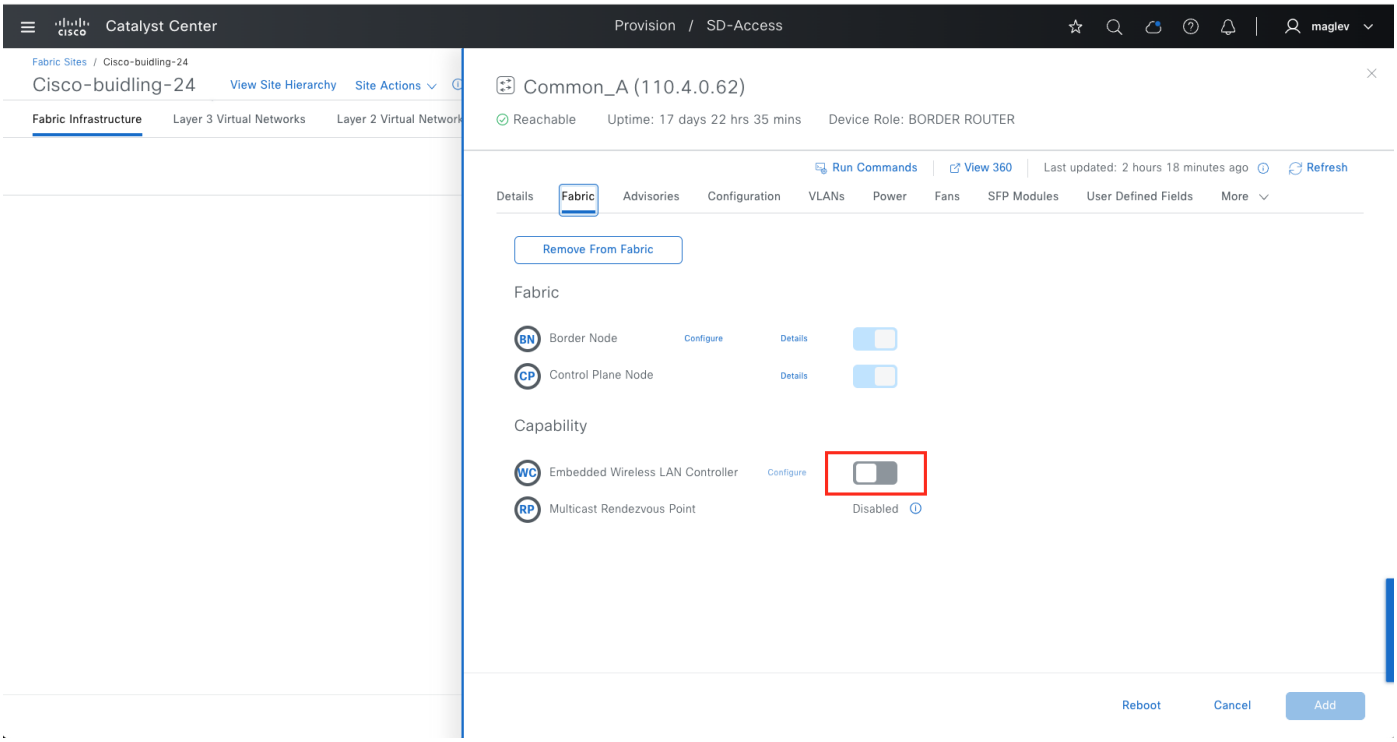
Catalyst Center には、組み込みワイヤレスコントローラを設定するときに、ワイヤレスサブパッケージをインポート、インストール、およびアクティブ化するオプションがあります。

組み込みワイヤレスコントローラは、**Common-A** と **Common-B** のデバイスを有効にし、N+1 ピアとして設定します。

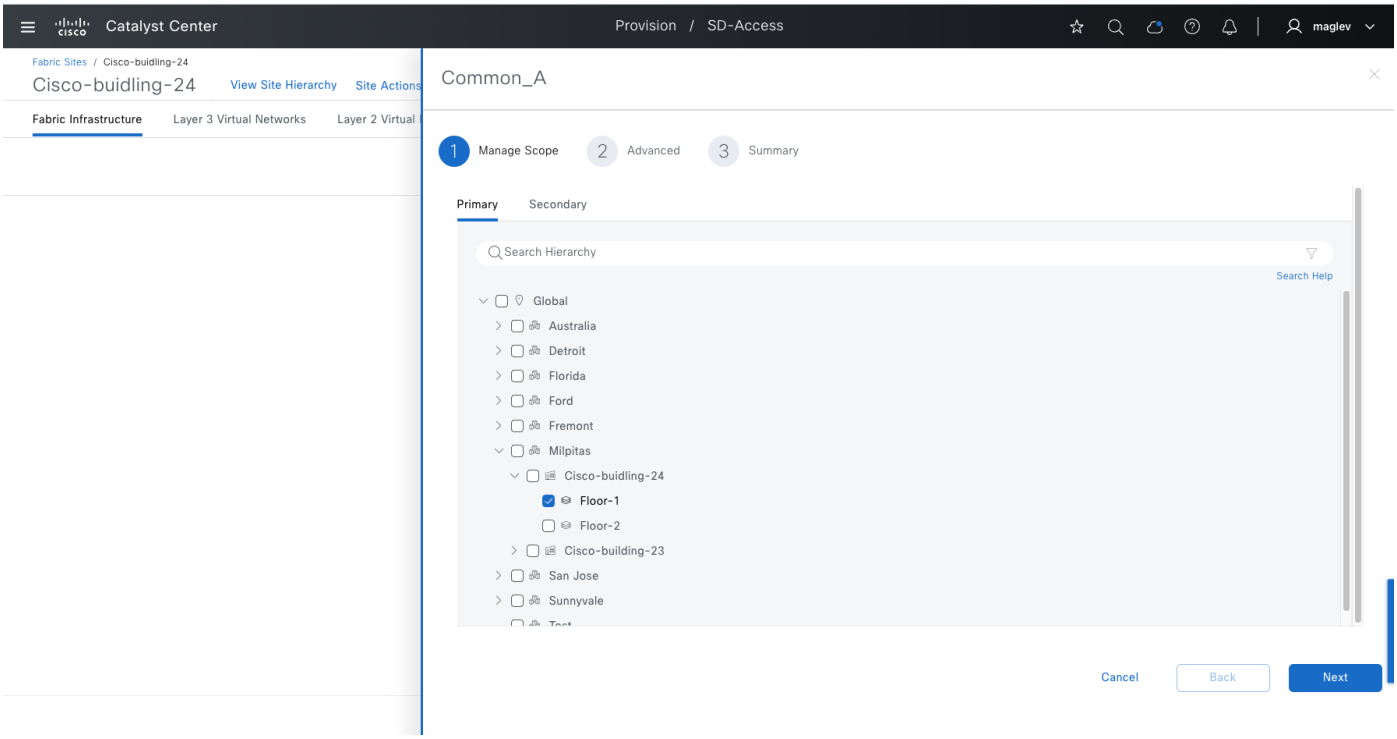
| デバイス | プライマリ管理対象ロケーション | セカンダリ管理対象ロケーション |
|---|---|---|
| Common-A | Cisco-building-24/Floor-1 | Cisco-building-24/Floor-2 |
| Common-B | Cisco-building-24/Floor-2 | Cisco-building-24/Floor-1 |

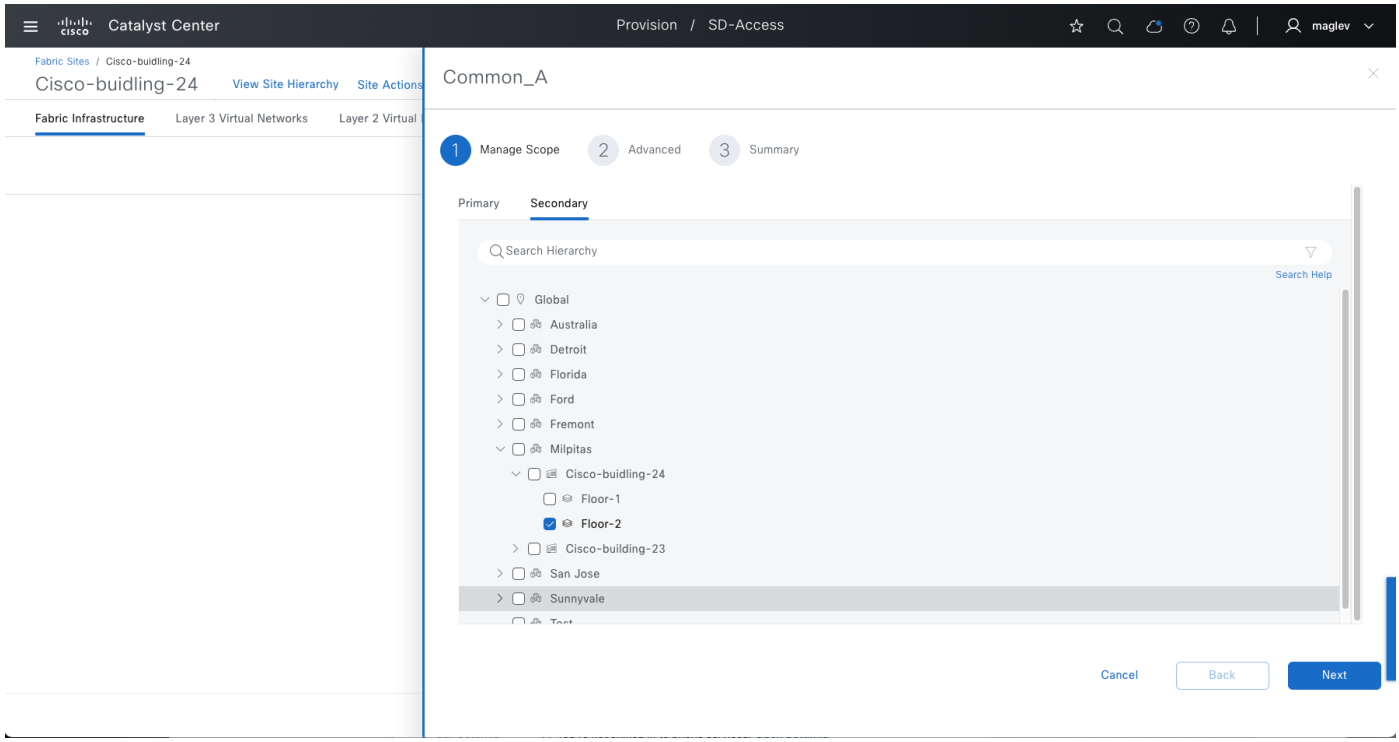
## 手順 1。　Catalyst 9000 での EWC の有効化

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして、[Cisco-building-24] を選択し、デバイス [Common-A] を右クリックして、[Embedded Wireless Controller] を有効にします。

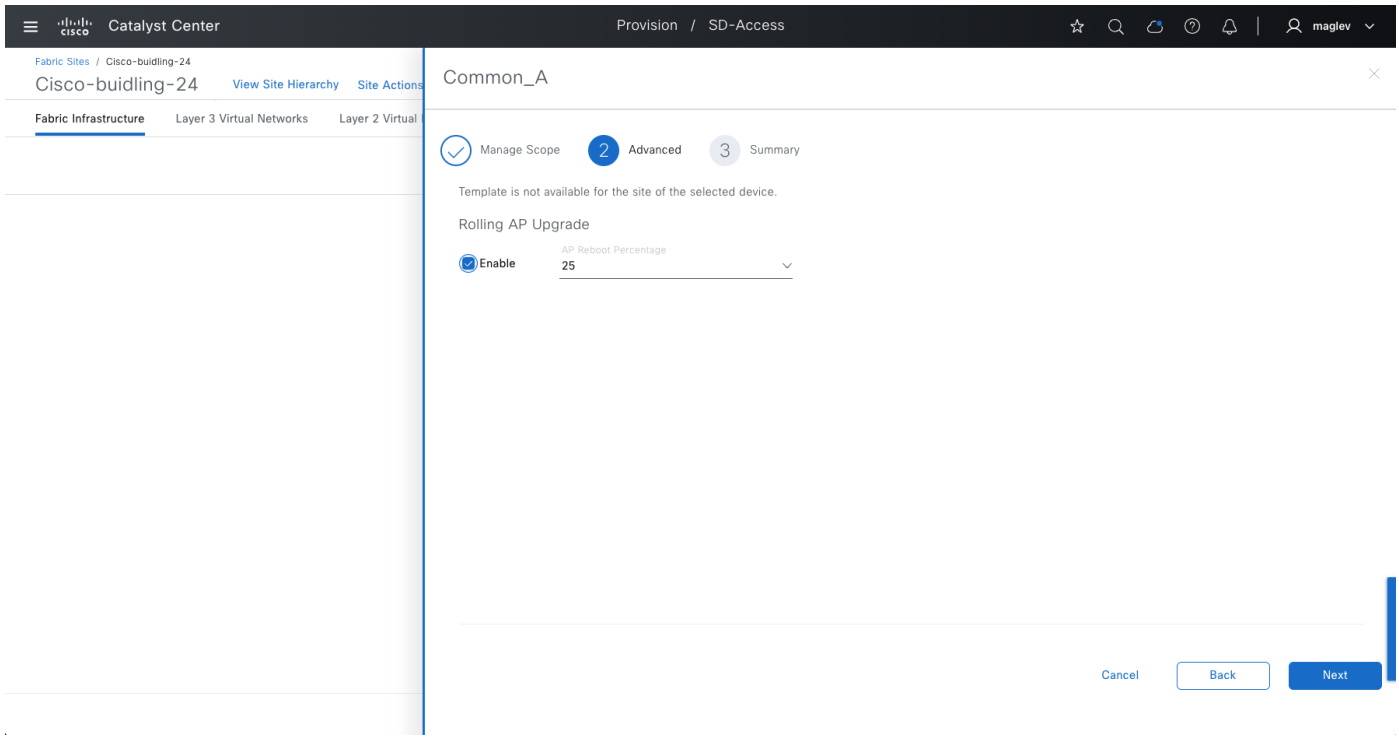



**ステップ 2.** [Primary] > [Floor-1] の順にクリックし、[Secondary] > [Floor-2] の順にクリックします。



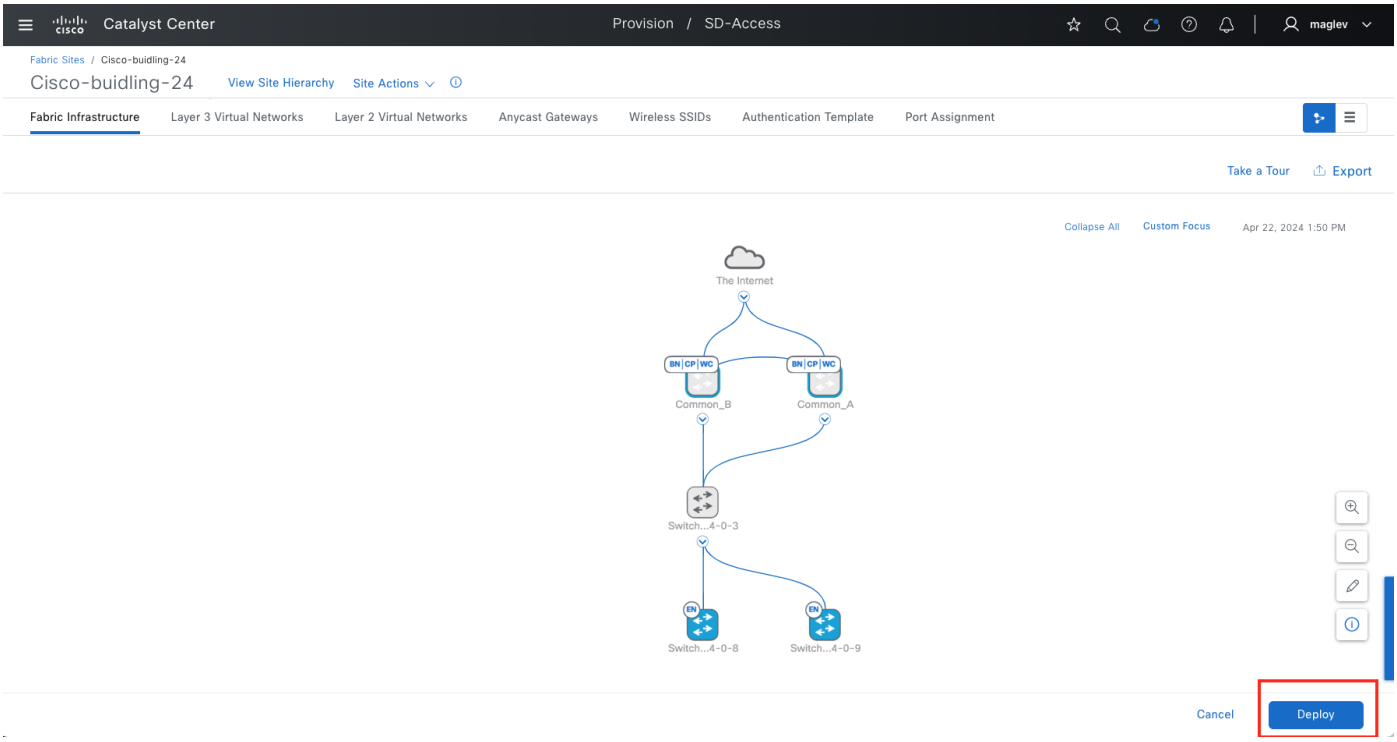



**ステップ 3.** [Rolling AP Upgrade] を有効にします（オプションだが推奨）。



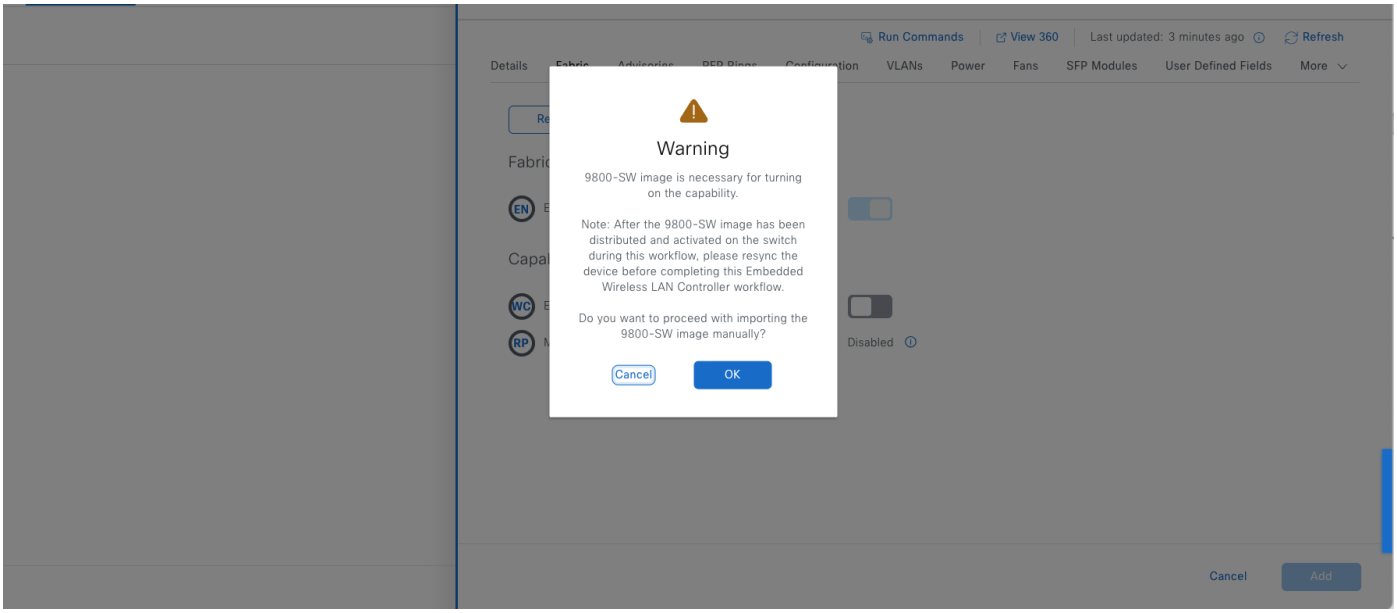

**ステップ 4.** ワークフローを完了し、[Common-B] で同じことを繰り返します（[Primary] > [Floor-2]、[Secondary] > [Floor-1]）。

**ステップ 5.** [Deploy] をクリックし、設定をプッシュします。

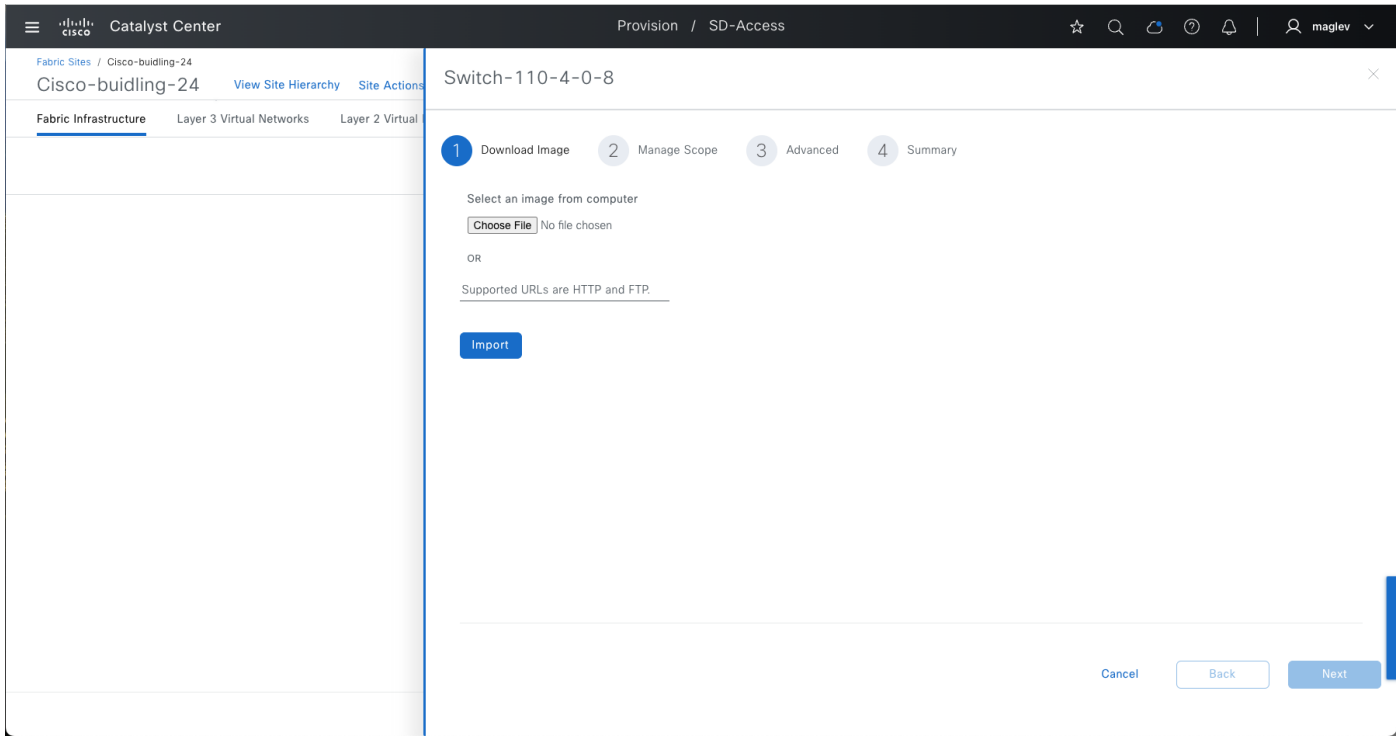



**技術的なヒント：** ワイヤレスサブパッケージがインストールされていない場合、Catalyst Center には、ワイヤレスサブパッケージをインストールしてアクティブにするワークフローが用意されています。例の画像を参照してください。

**ステップ 6.** [OK] をクリックして作業を続行します。



**ステップ 7.** コンピュータまたは HTTP/FTP サーバーからワイヤレスパッケージをインポートします。



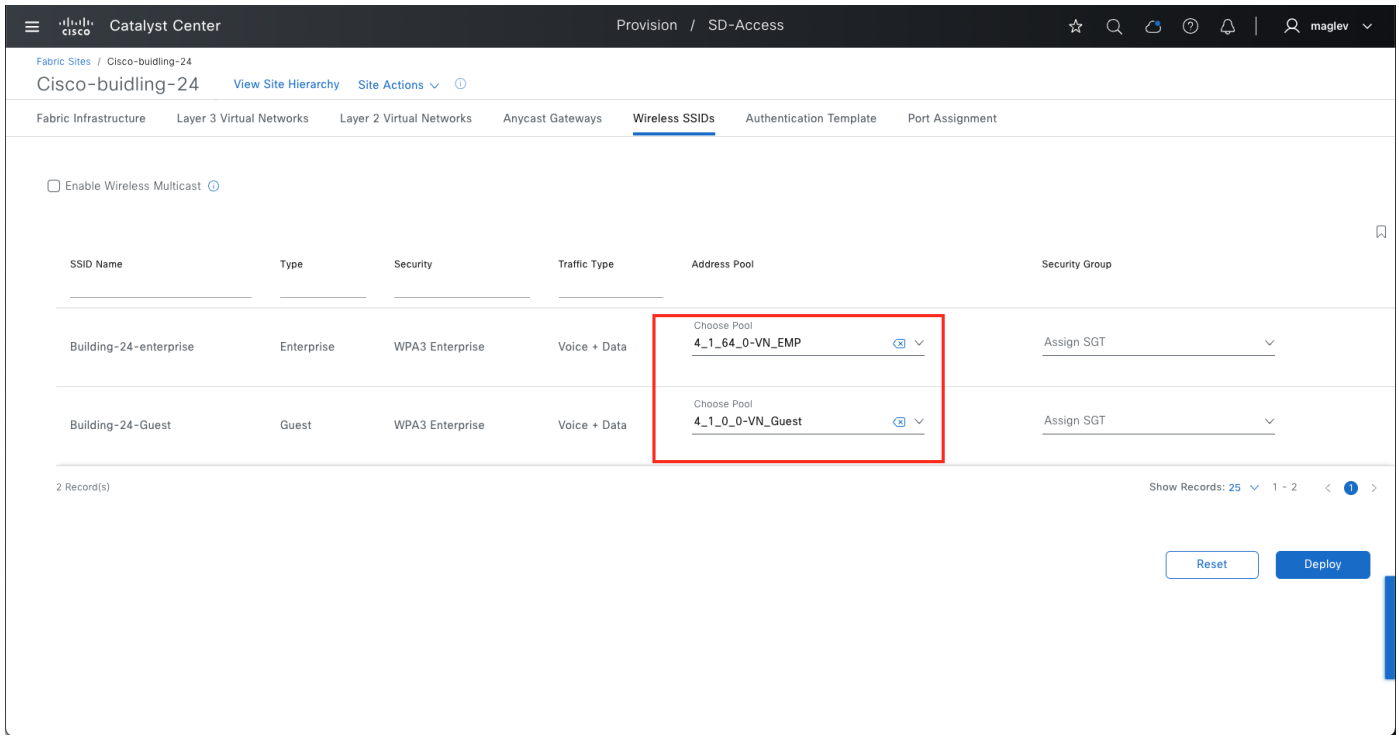

画像をインポートすると、同じワークフローで、Catalyst Center によってワイヤレスサブパッケージがインストールおよびアクティブ化され、プライマリおよびセカンダリの管理対象ロケーションを設定して、デバイスに設定をプロビジョニングできるようになります。

## 手順 2。 SSID への IP アドレスプールの関連付け

ワイヤレスネットワークに接続するときにワイヤレスホストが正しいサブネットに関連付けられるように、ファブリックサイトの各 SSID に IP アドレスプールを割り当てる必要があります。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] を選択し、[Wireless SSID] タブをクリックして、IP プールを SSID に関連付けて [Deploy] をクリックします。

**ステップ 2.** ワークフローを実行します。[Security Group] はオプションです。




**技術的なヒント：**

1. SSID と IP プールの関連付けには、ファブリックワイヤレスが有効になっている IP アドレスプールのみを使用できます。
2. 1 つの IP アドレスプールを使用して、異なる SSID に関連付けることができます。
3. Cisco ISE は、クライアントのオンボーディング中に IP アドレスプールを上書きできます。

**ステップ 3.** コマンド `show fabric wlan summary` を使用して、WLAN が **Common_A** と **Common_B** で稼働していることを検証します。

```
Common_A#show fabric wlan summary
Number of Fabric wlan : 2

WLAN Profile Name                    SSID                          Status
-----------------------------------------------------------------------------
17   Building-24-enterpris_profile   Building-24-enterprise          UP
18   Building-24-Guest_profile       Building-24-Guest               UP

Common_B#show fabric wlan summary
Number of Fabric wlan : 2

WLAN Profile Name                    SSID                          Status
-----------------------------------------------------------------------------
17   Building-24-enterpris_profile   Building-24-enterprise          UP
18   Building-24-Guest_profile       Building-24-Guest               UP
```

## IP トランジットを使用した共有サービスとインターネットサービスへのアクセスの提供

データセンターの DHCP と DNS、またはインターネットサービスなどの共有サービスは通常、Cisco SD-Access ファブリックの外部に存在します。レイヤ 3 ハンドオフによる IP トランジットは、ファブリック内のエンドポイントがそれらにアクセスできるように、これらの共有サービスルートをアドバタイズするか、ピアデバイスからデフォルトルートをアドバタイズするために使用されます。

デフォルトルートを使用した共有サービスへのアクセスは、ピアデバイスの主にコマンドライン インターフェイス（CLI）で実行されるマルチステップのワークフローです。

a. ピアデバイスとボーダーノード間に VRF-Lite 接続を作成します。
b. ピアデバイス上で VRF から GRT へ、およびその逆方向に双方向のルートリークを実行します。
c. ピアデバイスとボーダーノード間の GRT を使用して、各 VRF の BGP ピアリングを確立します。

ステップ a とステップ b は、ピアデバイス上に手動で設定する必要があります。ステップ c は、レイヤ 3 ハンドオフワークフローを使用して Catalyst Center を介して実行できます。次の手順例は、ファブリック ボーダー デバイス **Common_A** および **Common_B** での **VN_EMP** と **VN_Guest** のレイヤ 3 ハンドオフの追加を示しています。

IP トランジット **C-INTERNET** は、「手順 2：IP トランジットの作成」で設定されています。

**ステップ 1.** ボーダー設定に移動して、最初に準備されたこの表の情報を使用し、レイヤ 3 ハンドオフとして追加します。

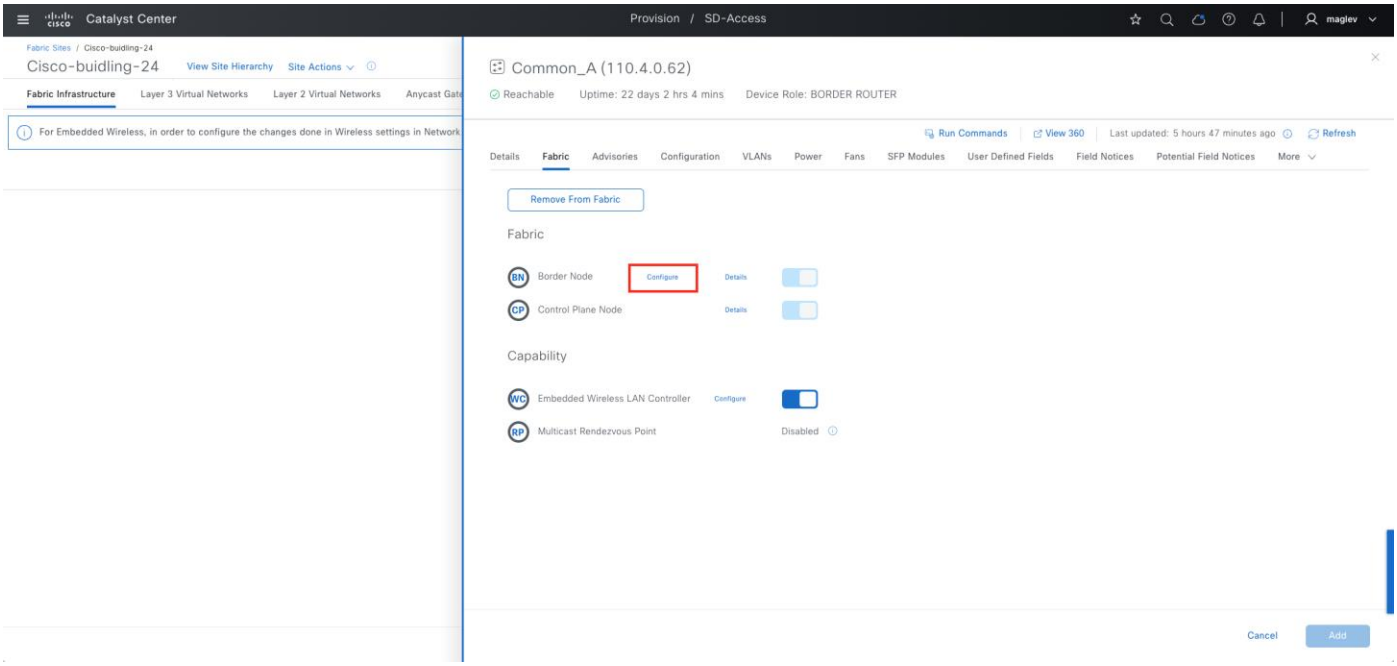
| 必要な情報 | 使用目的 |
|---|---|
| ボーダーとリモート BGP ピアデバイス間のインターフェイス | インターフェイスをトランクポートとしてスイッチプラットフォームで設定します。 |
| 各 VN の VLAN | ピアデバイスと通信するために、ルータプラットフォーム上の VLAN カプセル化を使用して、スイッチプラットフォームまたはサブインターフェイスに VLAN と SVI を作成します。 |
| IP アドレスピアを持つ IP プール | ピアデバイスと通信するために、スイッチプラットフォーム上の SVI またはルータプラットフォーム上のサブインターフェイスに IP アドレスを設定します。 |

**注：** Catalyst Center には、ボーダーとリモート BGP ピアデバイス間で通信するためにボーダーの IP アドレスを自動化する、次のようなオプションがあります。
1. Catalyst Center では、事前定義された IP プールから IP アドレス（/30 サブネット）を割り当てます。
2. カスタマイズされた IP アドレスピアでは、eBGP ピアに IP アドレスを割り当てることができます。

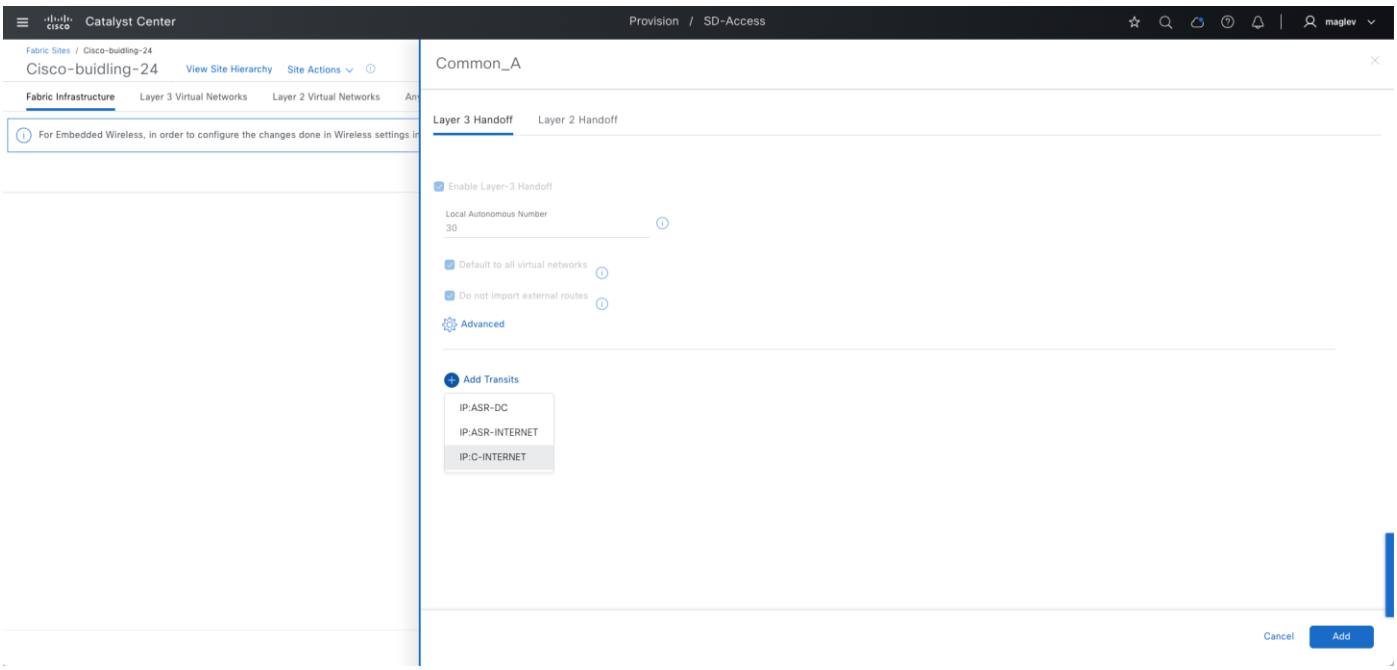
Catalyst Center を使用して IP アドレスピアを割り当てるか、カスタマイズされた IP アドレスピアを使用できます。同じデバイスで両方を組み合わせた場合、サポートはされません。

**ステップ 2.** ファブリックサイト **Cisco-building-24** で、[Fabric Infrastructure] タブをクリックし、ボーダー [Common-A] をクリックします。

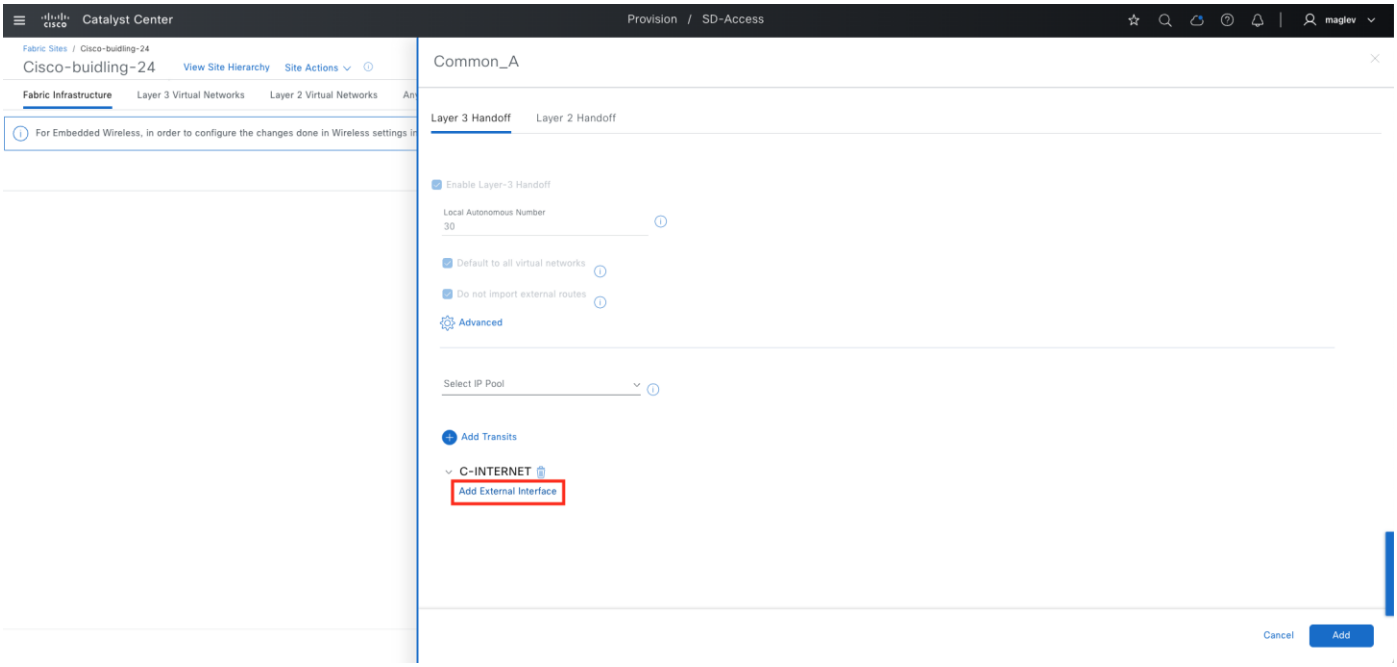
**ステップ 3.** スライドインペインで、[Border Node] > [Configure] をクリックします。




**ステップ 4.** [Layer 3 Handoff] タブをクリックし、[Add Transits] > [IP:C-INTERNET] をクリックします。



**ステップ 5.** [Add External Interface] をクリックし、ボーダーとピアデバイス間で接続されているインターフェイスを使用します。

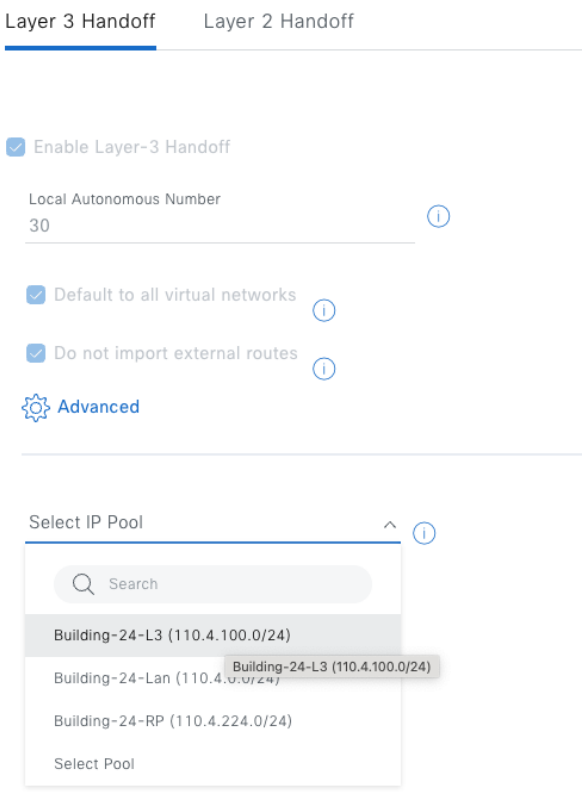



**ステップ 6.** IP アドレスを割り当てます。動的にまたは手動で割り当てを行います。

- システムが Catalyst Center を介して IP アドレスを動的に割り当てることができるようにするには、[Select IP Pool] を使用して IP プールを追加します。

  IP アドレスプール **Building-24-L3** は、「手順 2：ファブリックサイト用 IP プールの予約」で定義されています。

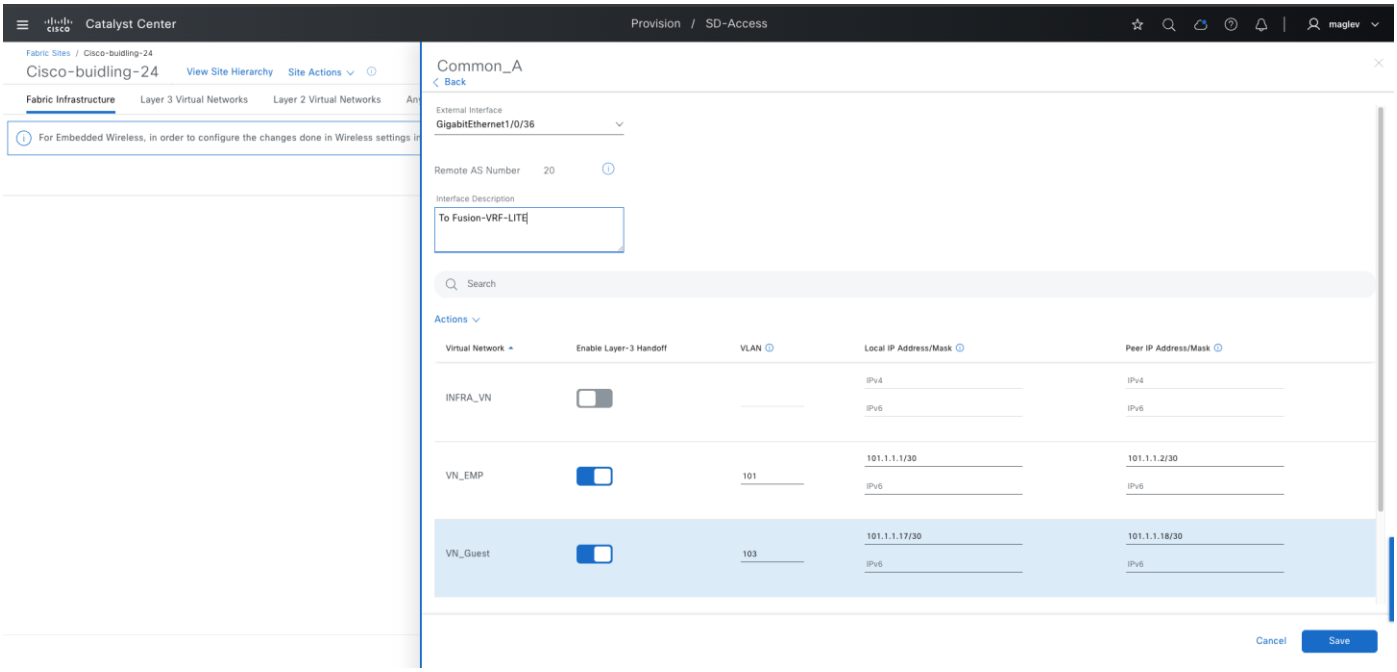
**図 41.　　IP プールの関連付け**




- IP アドレスを手動で割り当てるには、選択した VN（**VN_EMP** と **VN_Guest**）で、接続された物理インターフェイス、VLAN、およびカスタマイズされた IP アドレスピアを設定します。

| 必須フィールド | 値 |
|---|---|
| External Interface | Gig 1/0/36 |
| VN_EMP | VLAN 101、ローカル IP：101.1.1.1/30、ピア IP：101.1.1.2/30 |
| VN_Guest | VLAN 103、ローカル IP：101.1.1.17/30、ピア IP：101.1.1.18/30 |

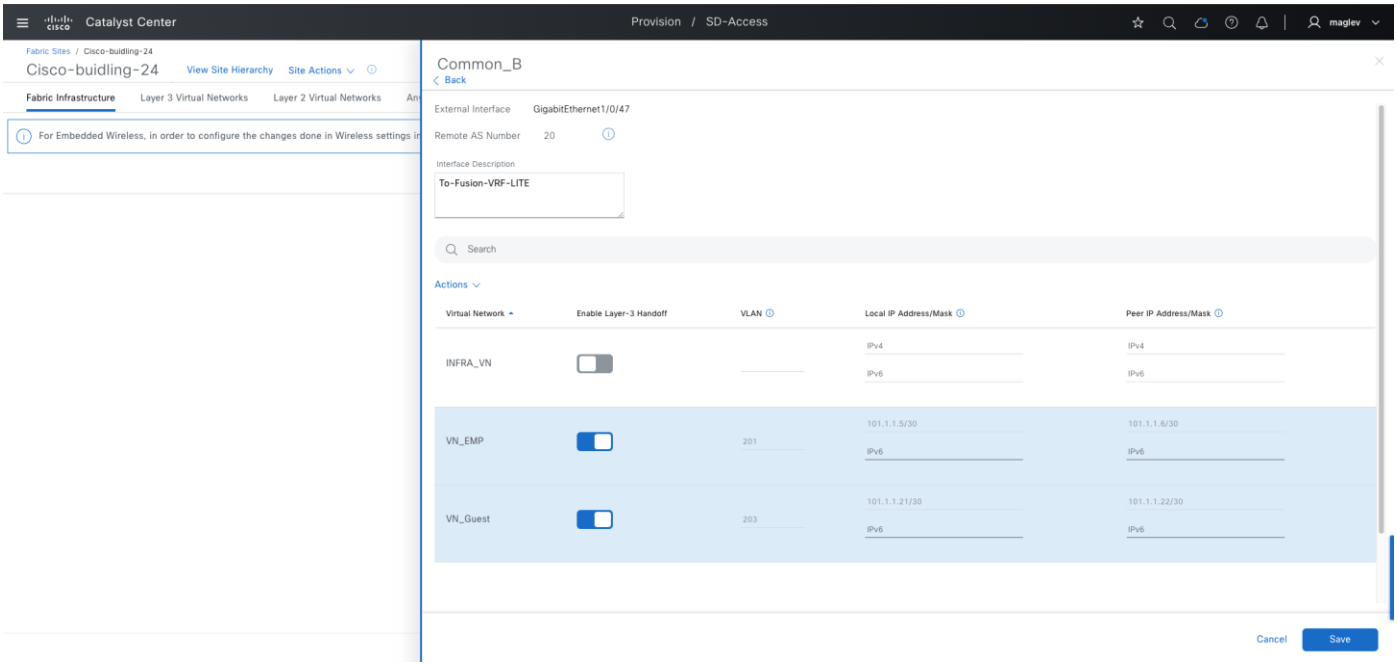
| オプションフィールド | 値 |
|---|---|
| Interface Description | To-Fusion-VRF-LITE |




**技術的なヒント：** 前の手順でレイヤ 3 ハンドオフを選択した場合は、VLAN 情報のみ必要です。

**ステップ 7.** ワークフローを完了し、**Common_A** にプロビジョニングします。

**ステップ 8.** **Common_B** で同じ手順を繰り返します。



**注：**
1. LISP Pub/Sub 外部ボーダーが機能するには、外部ボーダーのルーティングテーブルにデフォルトルートが必要です。すべての VRF にデフォルトルートがあることを確認します。DNS サーバーを使用する DHCP もインターネット経由で接続でき、これは不明な接続先と見なされます。

2. 内部ボーダーでは、ピアデバイスから学習した BGP ルートが LISP にインポートされ、コントロールプレーンに登録されます。DHCP や DNS などの共有サービスがデータセンターを介して接続されている場合、それらの IP アドレスはピアデバイスによってアドバタイズされる必要があります。

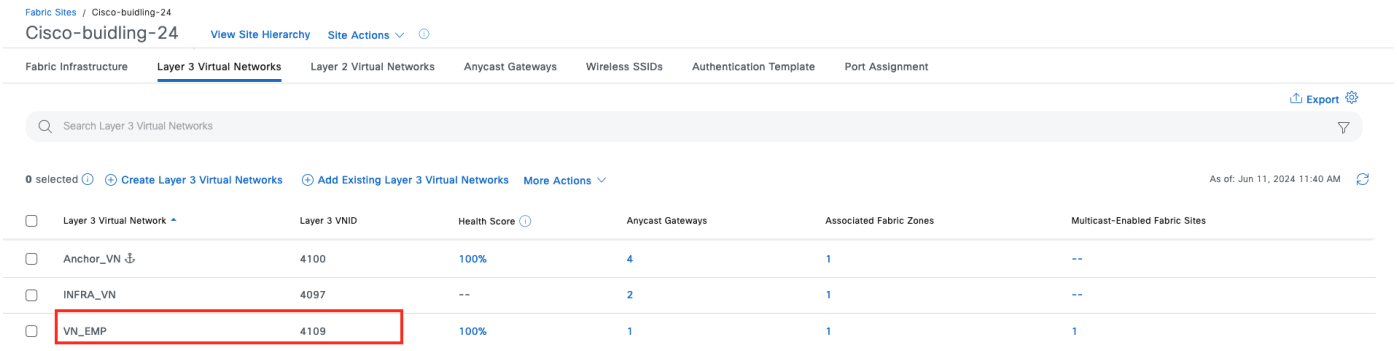
**ステップ 9.** VN **VN_EMP** の **Common_A** と **Common_B** を検証します。

a. ルーティングテーブルのデフォルトルートを検証します。

```
Common_A#show ip route vrf VN_EMP

Routing Table: VN_EMP


Gateway of last resort is 101.1.1.2 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 101.1.1.2, 1w4d      ---------------> default route , advertised from peer
      4.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
B        4.1.64.0/18 [200/0], 1w4d, Null0
C        4.1.64.1/32 is directly connected, Loopback1027

Common_B#show ip route vrf VN_EMP


Gateway of last resort is 101.1.1.6 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 101.1.1.6, 5w3d     ---------------> default route , advertised from peer
      4.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
B        4.1.64.0/18 [200/0], 5w3d, Null0
```

b. VN **VN_EMP** の LISP データベースでデフォルトルートを検証します。

[Layer 3 Virtual Networks] タブから [VN_EMP] のレイヤ 3 インスタンス ID を見つけます。



**ステップ 10.** CLI を実行します。

```
Common_A#show lisp instance-id 4109 ipv4 database
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_EMP (IID 4109), LSBs: 0x3
Entries total 8, no-route 0, inactive 0, do-not-register 0

0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR, default-ETR
  Uptime: 1w4d, Last-change: 1w4d
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator     Pri/Wgt  Source     State
  110.4.0.62   10/10   cfg-intf   site-self, reachable

Common_B#show lisp instance-id 4109 ipv4 database
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_EMP (IID 4109), LSBs: 0x3
Entries total 8, no-route 0, inactive 0, do-not-register 0

0.0.0.0/0, locator-set DEFAULT_ETR_LOCATOR, default-ETR
  Uptime: 5w3d, Last-change: 1w4d
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator     Pri/Wgt  Source     State
  110.4.0.63   10/10   cfg-intf   site-self, reachable
```

**ステップ 11.** ファブリックエッジノードで **VN VN_EMP** を検証します。

```
Switch-110-4-0-9#show lisp instance-id 4109 ipv4 map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_EMP (IID 4109), 3 entries

0.0.0.0/0, uptime: 5w3d, expires: 00:08:49, via map-reply, unknown-eid-forward
 action: send-map-request + Encapsulating to proxy ETR
  PETR        Uptime    State      Pri/Wgt     Encap-IID  Metric
  110.4.0.62  1w4d      up          10/10        -         0
  110.4.0.63  5w3d      up          10/10        -         0
```

**注：** データセンターへのレイヤ 3 ハンドオフを使用する内部ボーダーの場合、共有サービスは BGP を介してピアデバイスによってアドバタイズされます。

**図 42. DHCP IP（サブネット 110.10.2.0/24 の 110.10.2.1）の内部ボーダーでの検証（出力のみを表示するために Common_B が内部ボーダーとして再設定された）**

```
Common_B#show lisp instance-id 4109 ipv4 database 110.10.2.0/24
LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf VN_EMP (IID 4109), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0

110.10.2.0/24, route-import, inherited from default locator-set rloc_23c67995-7b91-4114-987a-6f49b3481aea, auto-discover-rlocs
  Uptime: 00:07:44, Last-change: 00:07:44
  Domain-ID: local, tag: 733777
  Service-Insertion: N/A
  Locator     Pri/Wgt  Source     State
  110.4.0.63   10/10   cfg-intf   site-self, reachable
  Map-server  Uptime         ACK  Domain-ID
  110.4.0.62  00:07:44       Yes  3283456652
  110.4.0.63  00:07:44       Yes  3283456652
```

**図 43.　　クライアントがオンボーディングを試行した後のファブリックエッジでの検証**

```
Switch-110-4-0-9#show lisp instance-id 4109 ipv4 map-cache 110.10.2.0/24
LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN_EMP (IID 4109), 1 entries

110.10.2.0/24, uptime: 00:00:14, expires: 23:59:45, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 00:00:14, map-source: 110.4.0.63
  Active, Packets out: 1(576 bytes), counters are not accurate (~ 00:00:03 ago)
  Locator     Uptime    State  Pri/Wgt     Encap-IID
  110.4.0.63  00:00:14  up      10/10        -
    Last up-down state change:         00:00:14, state change count: 1
    Last route reachability change:    00:00:14, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            00:00:14 (rtt 1ms)
```

## レイヤ 2 ハンドオフを使用した従来のレイヤ 2 ネットワークへのファブリックアクセスの提供

レイヤ 2 ボーダーハンドオフにより、同じサブネットを使用してファブリックサイトと従来のネットワーク VLAN セグメントを運用できます。2 つの間の通信は、ファブリックと非ファブリック間の VLAN 変換を提供するこのハンドオフにより、ボーダーノード全体に提供されます。Catalyst Center は、VLAN 変換、スイッチ仮想インターフェイス（SVI）、CTS 適用、およびこのボーダーノードで従来のネットワークに接続されたトランクポート（すべての VLAN を許可）とともに LISP コントロールプレーンの設定を自動化します。

レイヤ 2 ハンドオフでサポートされるタイプは次のとおりです。

- ファブリック外のゲートウェイ：ボーダーに接続されたファイアウォールまたはレイヤ 3 デバイスに手動で設定されます
- ファブリック内のゲートウェイ：レイヤ 2 ハンドオフボーダーに設定されます。レイヤ 3 VN で使用されるエニーキャストゲートウェイです

レイヤ 2 ボーダーハンドオフデバイスは、専用にして、他の機能とコロケーションさせないことをお勧めします。従来のネットワークの VLAN の意図しない変更を避けるために、VLAN トランキングプロトコル（VTP）のデバイスはトランスペアレントモードで動作する必要があります。従来のネットワークは、Catalyst Center で予約されているか、シスコソフトウェアでの特別な使用のために予約されている、1、1002 ～ 1005、2045 ～ 2047、および 3000 ～ 3500 を除く任意の VLAN を使用できます。

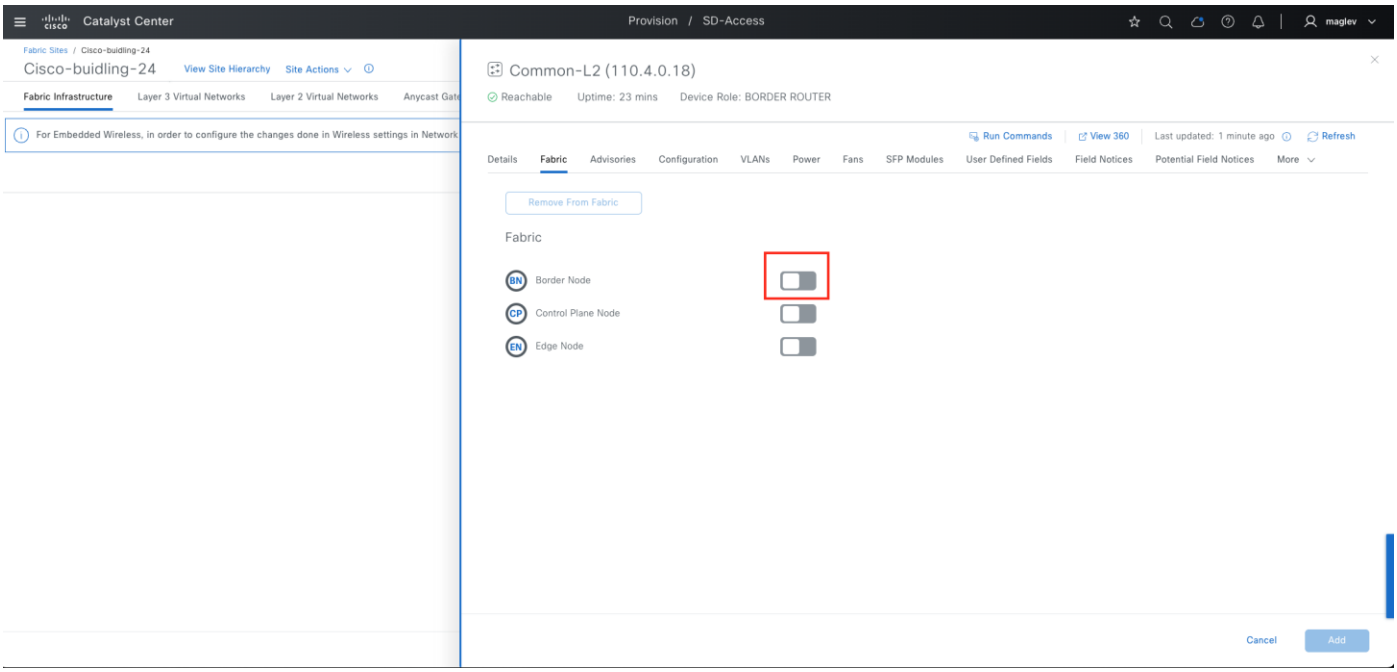
前のセクションに従って、**ディスカバリ**ワークフローまたは **LAN 自動化**を使用して新しいデバイスをオンボーディングし、[Inventory] ウィンドウでデバイスを **Cisco-building-24** サイトにプロビジョニングします。

### 手順 1。　ゲートウェイがファブリック内にある場合のレイヤ 2 ハンドオフを使用したレイヤ 2 ボーダーのプロビジョニング

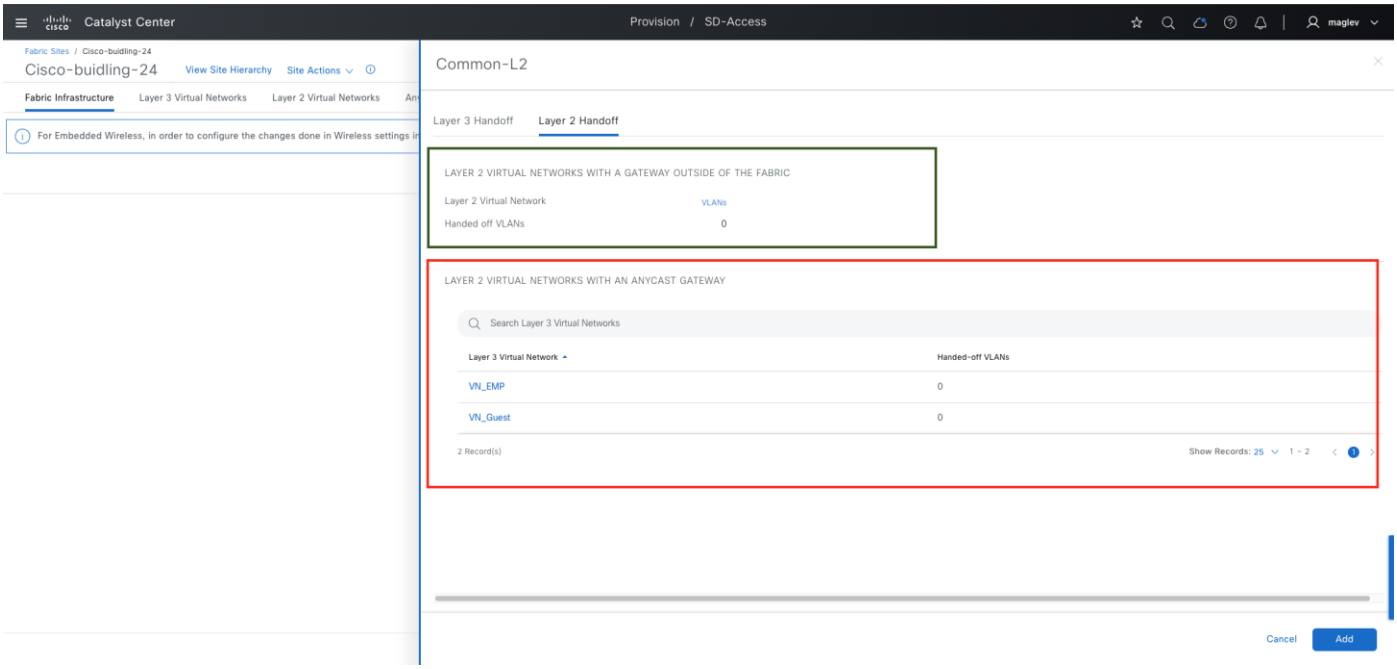
この手順では、新しいボーダーデバイス **Common-L2** にさまざまなタイプのレイヤ 2 ハンドオフを追加する方法を示します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックしてから、[Fabric Infrastructure] タブをクリックします。

**ステップ 2.** スライドオンペインで [Common-L2] をクリックし、[Border Node] を有効にします。



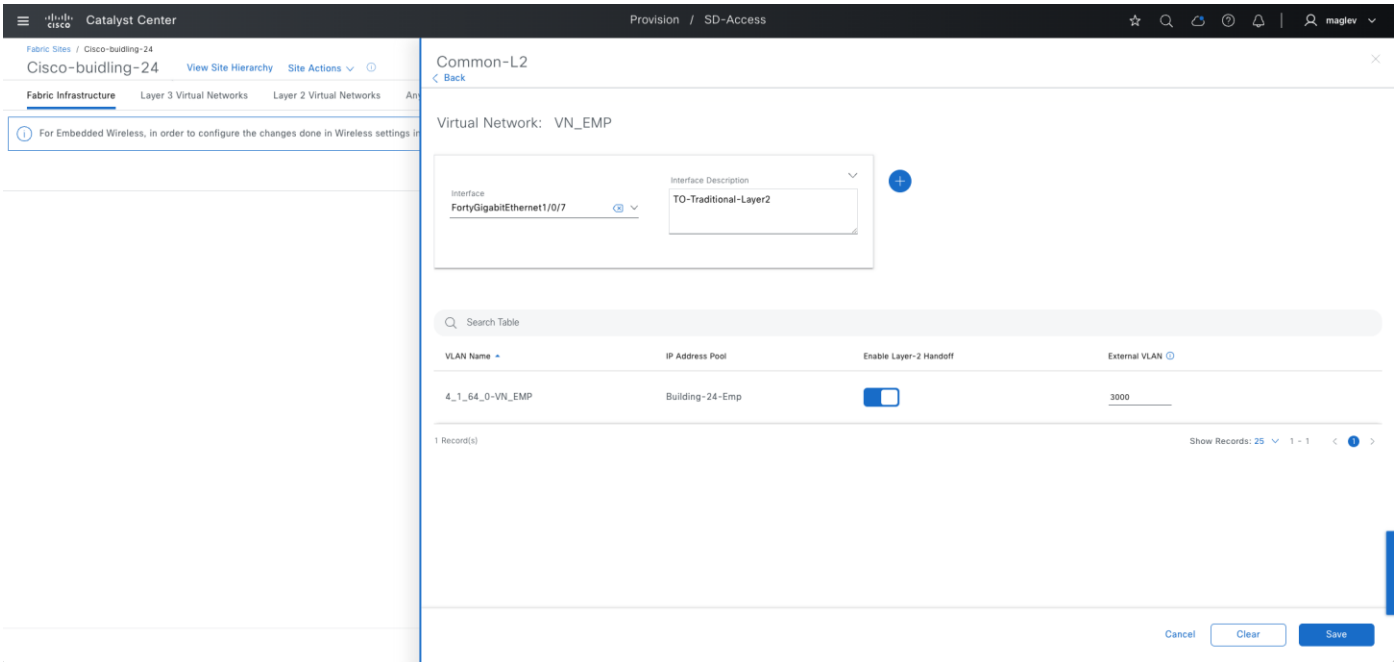

**ステップ 3.** スライドインペインで、[Layer 2 Handoff] タブをクリックします。




緑色のボックス領域の設定は、ゲートウェイがファブリック外にある場合にレイヤ 2 ハンドオフを自動化することです。赤色のボックス領域の設定は、ゲートウェイがファブリック内にある場合にレイヤ 2 ハンドオフを自動化することです。

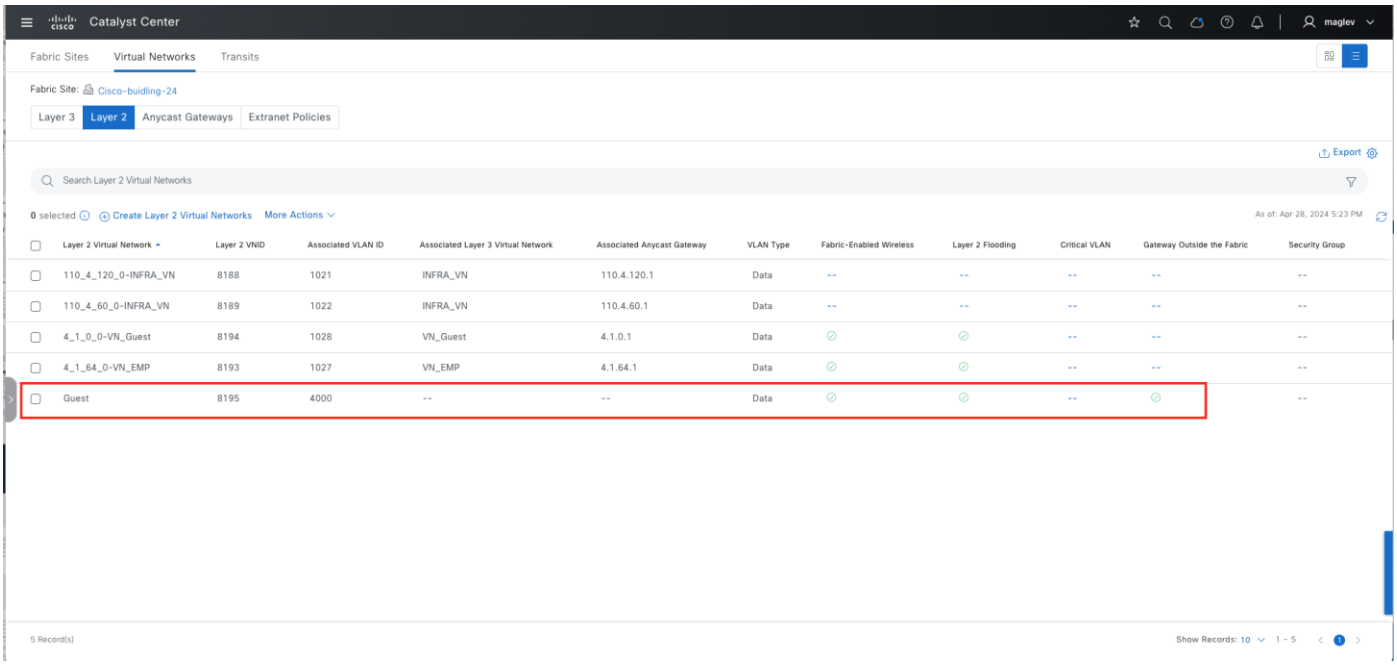
**ステップ 4.　VN EN_EMP** でレイヤ 2 ハンドオフを設定し、タスクを展開するためのワークフローを完了します。

| 必須フィールド | 値 | 使用目的 |
|---|---|---|
| Interface | 1/0/7 の場合 | 従来のレイヤ 2 ネットワークに接続 |
| External VLAN | 3000 | 従来のレイヤ 2 ネットワークのアクセス VLAN |



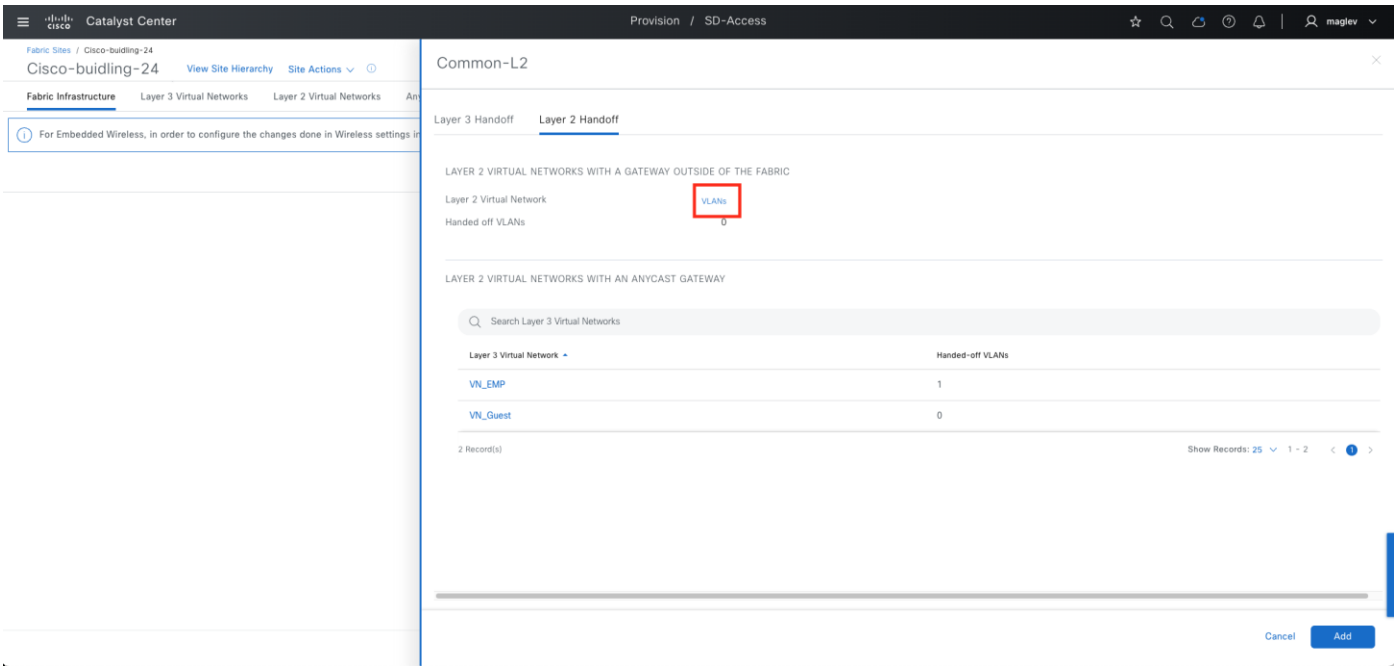
## 手順 2。 ゲートウェイがファブリック外にある場合のレイヤ 2 ハンドオフを使用したレイヤ 2 ボーダーのプロビジョニング

ゲートウェイがファブリック外にある場合、ファブリックオーバーレイを拡張するには、レイヤ 2 専用 VN が必要です。前のセクションでは、レイヤ 2 専用ネットワーク **Guest** を設定しました。

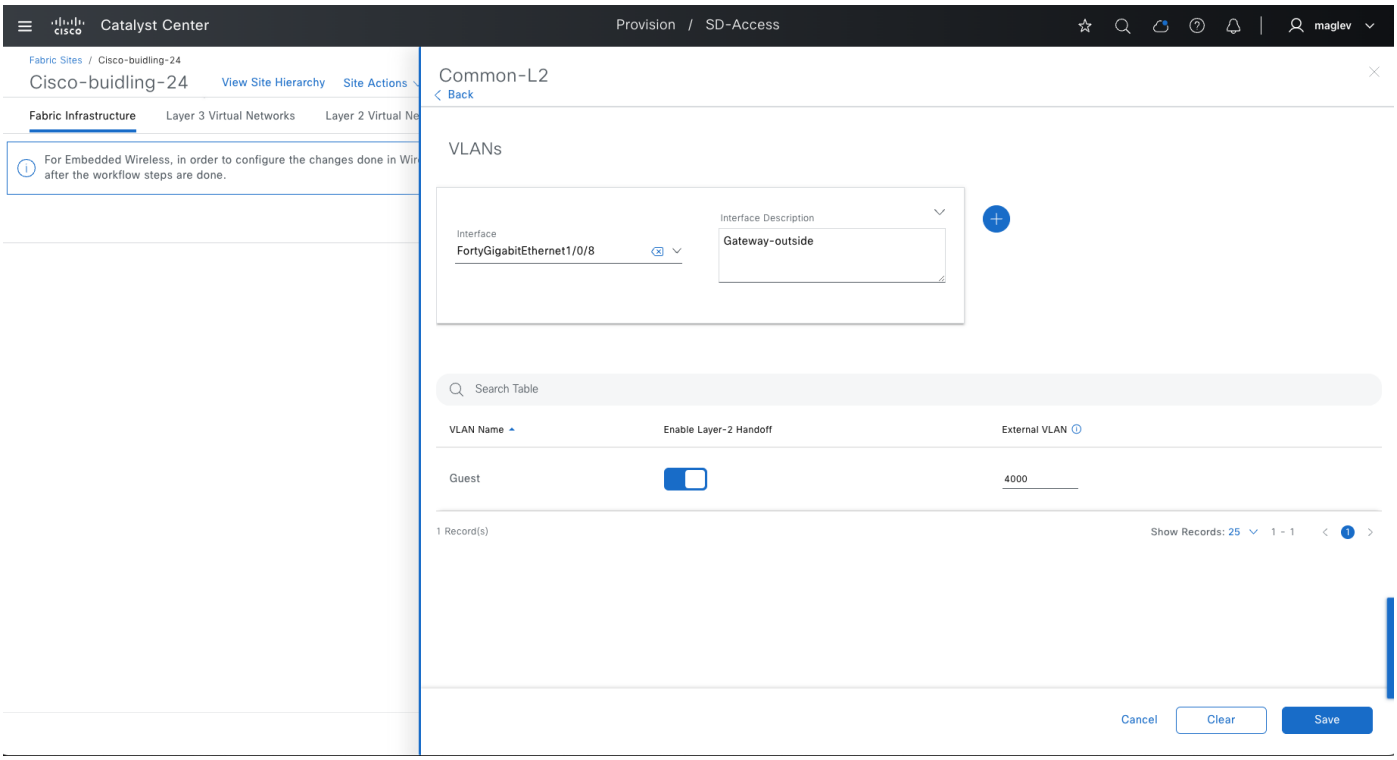



**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックしてから、[Fabric Infrastructure] タブをクリックします。

**ステップ 2.** **[Common-L2] > [Layer 2 Handoff] > [VLANs]** の順に選択します。



**ステップ 3.** [Guest] で、**インターフェイス**を追加し、[Enable Layer-2 Handoff] をクリックします。**外部 VLAN** 情報が自動的に提供されます。




**ステップ 4.** ワークフローを完了し、タスクを展開します。

**注：** ゲートウェイはファブリック外にあるため、Catalyst Center はゲートウェイの設定を自動化しません。

## Cisco SD-Access トランジットを使用してファブリック通信を交差する複数のファブリックサイトの接続

Cisco SD-Access トランジットは複数のファブリックサイトを接続し、SGT ポリシーが適用されたファブリック通信の交差を可能にします。外部ボーダー（または内外ボーダー）で Cisco SD-Access トランジットを設定します。内部ボーダーとレイヤ 2 ボーダーではサポートされません。

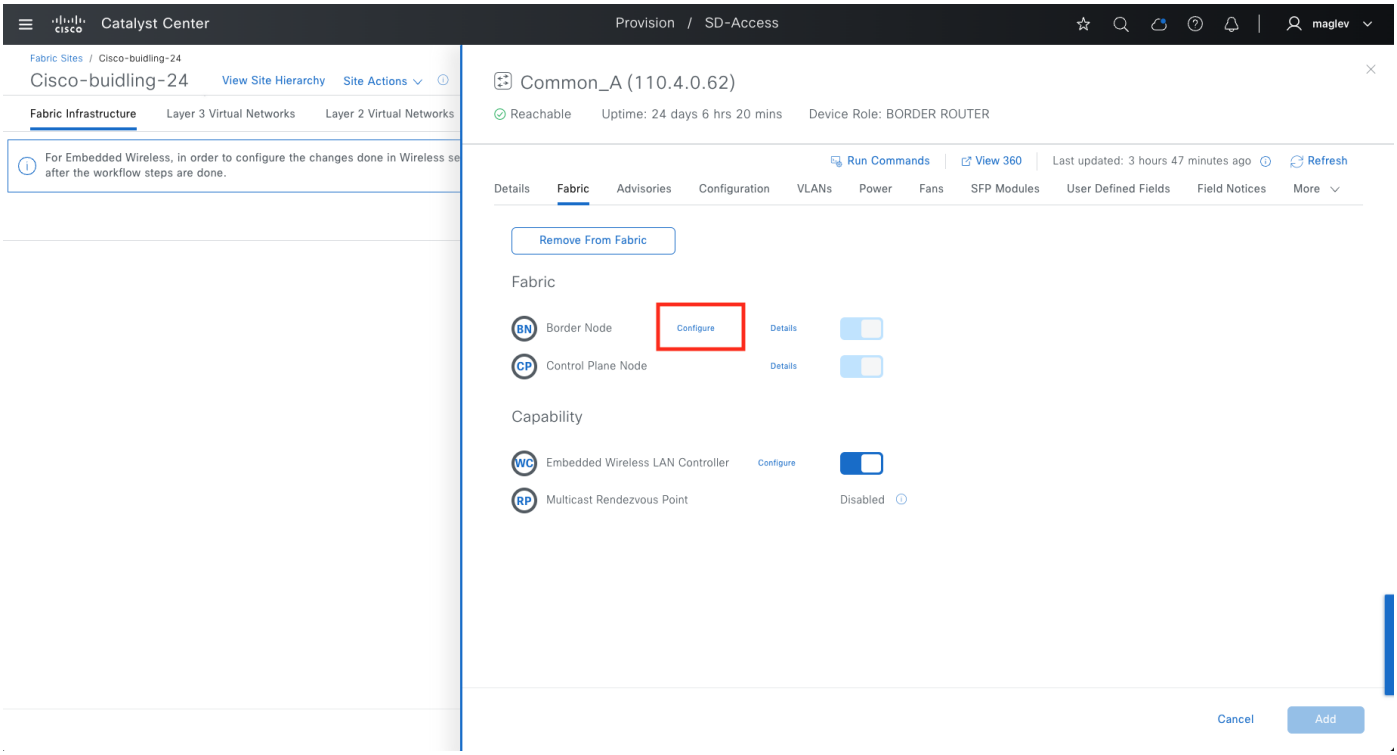
ファブリックサイトを Cisco SD-Access トランジットに接続すると、このサイトのすべての VN は、同じ Cisco SD-Access トランジットに接続されている他のファブリックサイトに対して開かれます。同じ VN 内のクライアントは、すべてのサイトで通信できます。SGT の適用を使用して、他のサイトからの不要なトラフィックをブロックします。

Cisco SD-Access トランジットには、同じ Cisco SD-Access トランジットに接続されている他のサイトにインターネットアクセスを提供できるようにするオプションも用意されています。これは、一部のファブリックサイトにローカル インターネット アクセスがない場合や、ローカル インターネット アクセスがダウンしている場合に役立ちます。

前のセクションでは、Cisco SD-Access トランジット **SDA** をコントロールプレーンノードで作成しました。この手順では、この Cisco SD-Access トランジットを **Cisco-building-24** の **Common_A** と **Common_B** に追加します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックしてから、[Fabric Infrastructure] タブをクリックします。

**ステップ 2.** [Common_A] をクリックし、[Border Node] の横にあるスライドオンペインで [Configure] をクリックします。




**ステップ 3.** [Add Transits] > [SDA:SDA] の順にクリックします。

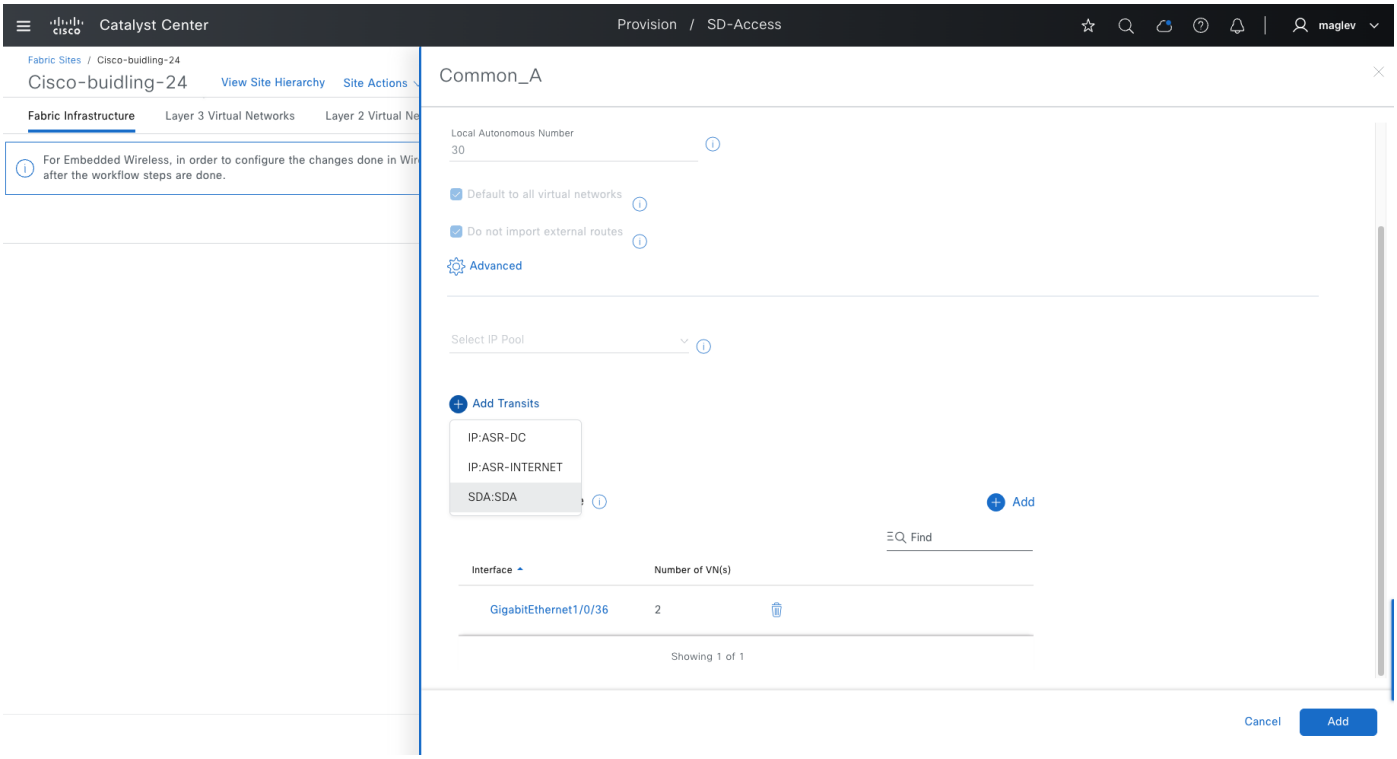
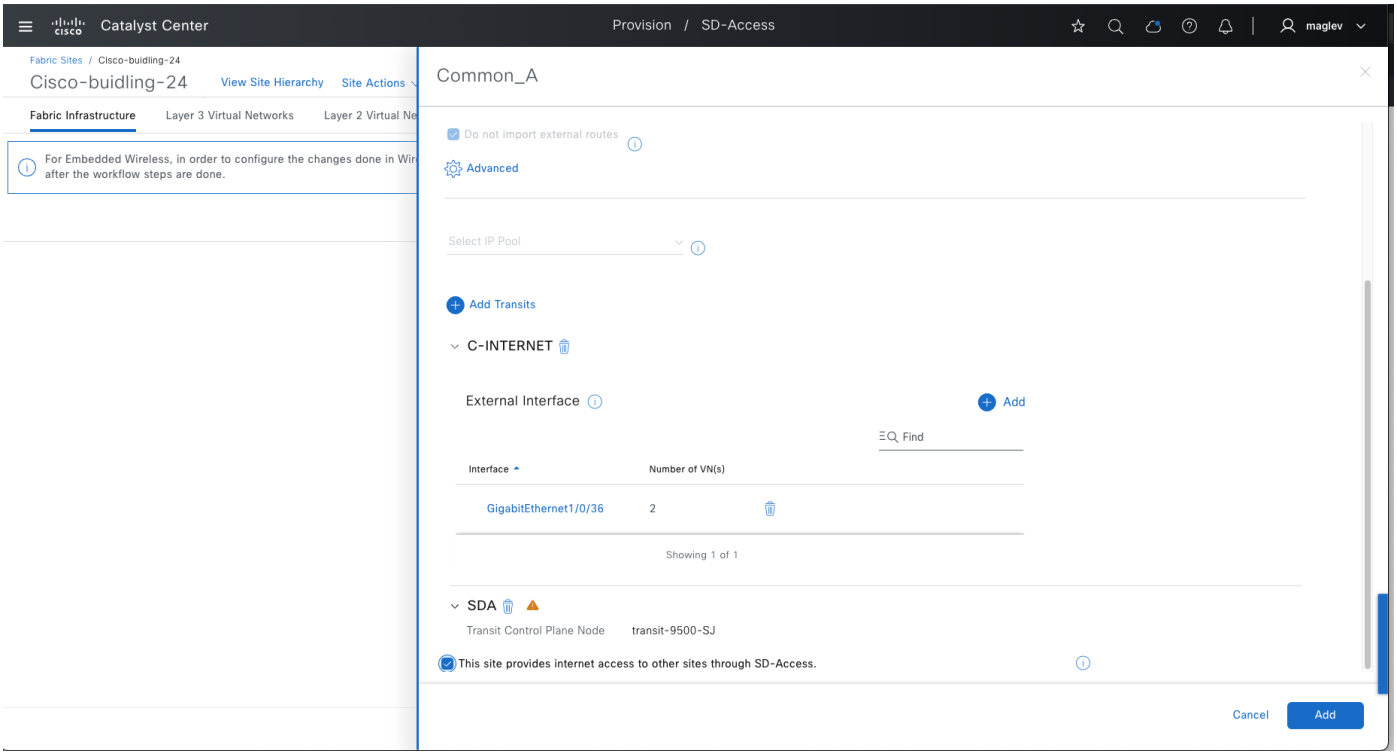


**図 44.　　Cisco SD-Access トランジットが追加され、下部に表示される**




**ステップ 4.**　[This site provide Internet access to other sites through SD-Access] チェックボックスをオンにし、[Add] をクリックします。

**ステップ 5.**　ワークフローを完了し、タスクを展開します。

**ステップ 6.**　**Common_B** で同じステップを繰り返し、タスクを展開します。

**注：**　Cisco SD-Access トランジットに接続されているすべてのボーダーに、他のサイトにインターネットアクセスを提供する同じ設定があることを確認します。

**ステップ 7.**　トランジット コントロール プレーンで検証します。

1. **Common_A**、**Common_B**、およびトランジット コントロール プレーン間の LISP セッションステータスを確認します。

```
transit-9500-SJ#show lisp session

Sessions for VRF default, total: 10, established: 5
Peer              State      Up/Down        In/Out    Users

110.4.0.62:37533 Up         1w5d           122/695    10
110.4.0.63:44171 Up         5w4d           147/1049   10
```

2. **Common_A** と **Common_B** は、他のサイトにインターネット接続を提供するために、トランジット コントロール プレーン上のデフォルトの出力トンネルルータ（ETR）として登録されます。

```
transit-9500-SJ#show lisp remote-locator-set default-etrs


LISP remote-locator-set default-etr-locator-set-ipv4 Information

 RLOC         Pri/Wgt/Metric     Inst       Domain-ID/MH-ID  ETR       SI/ID
 110.4.0.62    10/10 /0          4100      3283456652/37516  Default   PB/-
 110.4.0.62    10/10 /0          4109      3283456652/37516  Default   PB/-
 110.4.0.63    10/10 /0          4100      3283456652/37516  Default   PB/-
 110.4.0.63    10/10 /0          4109      3283456652/37516  Default   PB/-
```

**注：** [This site provides internet access to other sites through SD-Access] 機能のみがボーダーで有効になり、ボーダーノードはトランジット コントロール プレーンのこのコマンドの下にリストされます。

3. クライアントサブネットがトランジット コントロール プレーンに登録されていることを確認し、デュアルスタックが有効になっている場合は、コマンドで ipv4 を ipv6 に置き換えます。

```
transit-9500-SJ#show lisp instance-id 4109 ipv4 server
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4109     0.0.0.0/0
               00:19:10  yes#   110.4.0.62:29755     4109     4.1.64.0/18
               00:19:10  yes#   110.4.0.62:29755     4109     101.1.1.0/30
               00:19:10  yes#   110.4.0.63:25632     4109     101.1.1.4/30
               00:19:10  yes#   110.4.0.63:25632     4109     110.4.224.1/32
               00:19:10  yes#   110.4.0.62:29755     4109     110.4.224.2/32
               00:19:10  yes#   110.4.0.63:25632     4109     110.4.224.3/32
               00:19:10  yes#   110.4.0.62:29755     4109     110.4.224.4/32
               00:19:10  yes#   110.4.0.62:29755     4109     110.4.224.6/32
               00:19:10  yes#   110.4.0.62:29755     4109     110.4.224.8/32
```

**ステップ 8.** ローカルインターネットを持たず、Cisco SD-Access トランジットに接続されている別のサイト（FiaB サイト）で検証します。

```
9300B-stack-BJ#show lisp instance-id 4109 ipv4  map-cache
LISP IPv4 Mapping Cache for LISP 0 EID-table default (IID 4109), 7 entries

0.0.0.0/0, uptime: 00:22:31, expires: never, via pub-sub, unknown-eid-forward, remote-to-site
  PETR        Uptime    State      Pri/Wgt     Encap-IID  Metric
  110.4.0.62  00:22:31  up          10/10        -         10
  110.4.0.63  00:22:31  up          10/10        -         10
```

## ネイティブマルチキャストの設定

このセクションでは、ファブリックサイト **Cisco-building-24** での **VN_EMP** のネイティブマルチキャストの設定、ワイヤレスのマルチキャストの有効化、および Cisco SD-Access トランジットを介したネイティブマルチキャストの設定に焦点を当てます。

ネイティブマルチキャストには、PIM SSM アンダーレイ設定が必要です。これは、前のセクションで LAN の自動化によって行いました。LAN の自動化を使用しない場合、ファブリックボーダー、中間ノード、ファブリックエッジなどのすべてのファブリックデバイスで、これらの設定を手動で行う必要があります。Catalyst Center CLI テンプレートを使用して設定を展開します。

この設計および導入ガイドでは、テンプレートについては取り上げていません。「Cisco Catalyst Center User Guide」の「Create Templates to Automate Device configuration Changes」セクションを参照してください。

テンプレートの設定例：

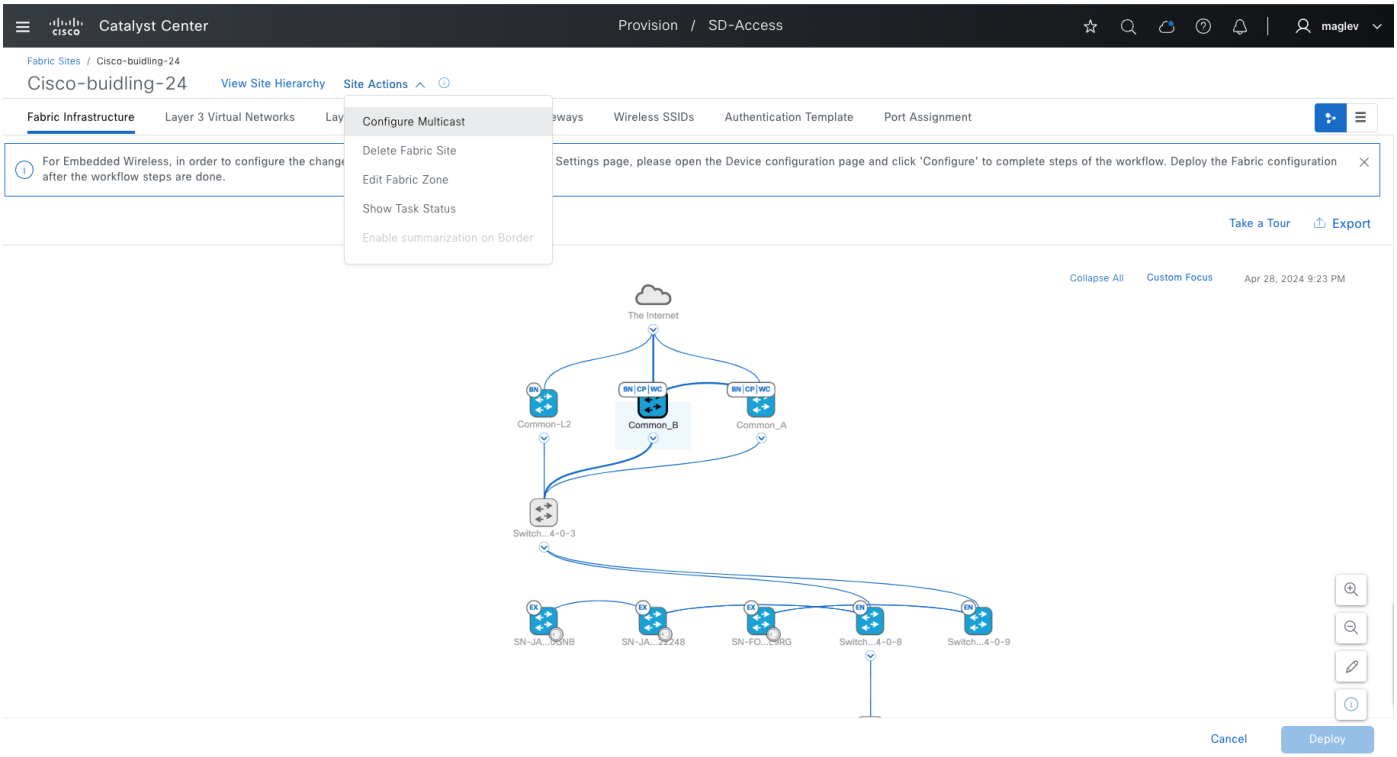
- layer3_interface：すべてのアンダーレイレイヤ 3 インターフェイス

```
ip multicast routing
ip pim ssm default

interface $layer3_interface
 ip pim sparse-mode
```

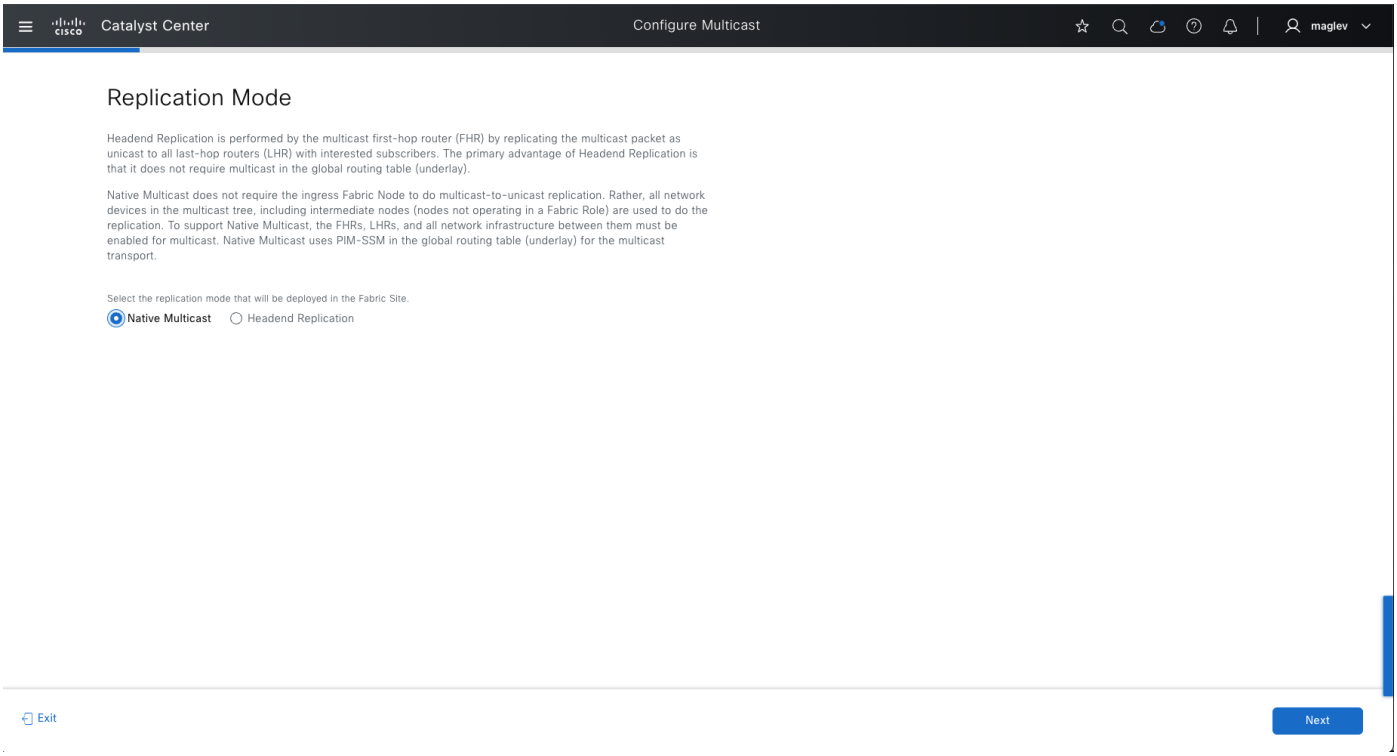
### 手順 1。　ファブリックサイト内のネイティブマルチキャストの設定

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックしてから、[Fabric Infrastructure] タブをクリックします。

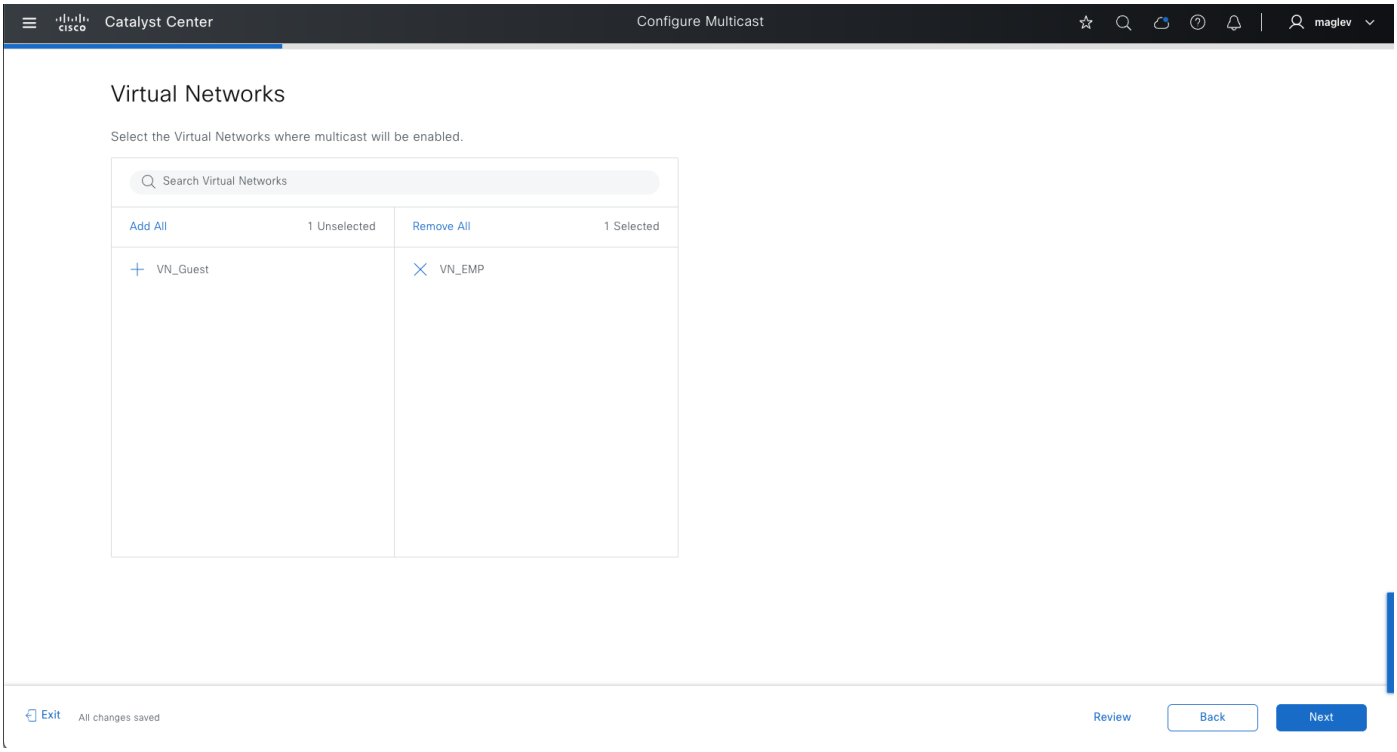
**ステップ 2.** [Site Actions] > [Configure Multicast] の順にクリックします。



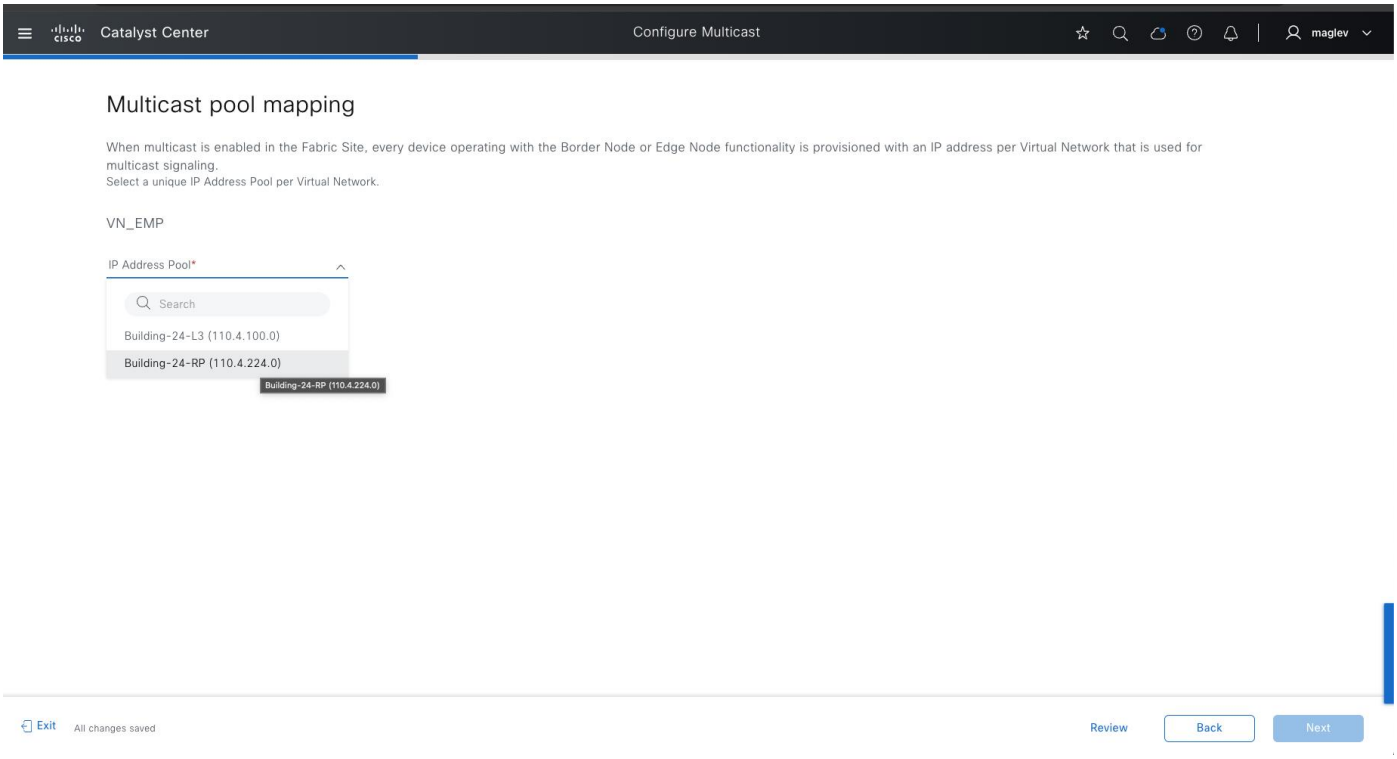

**ステップ 3.** [Native Multicast] を選択し、[Next] をクリックします。




**ステップ 4.** [VN_EMP] を選択し、[Next] をクリックします。

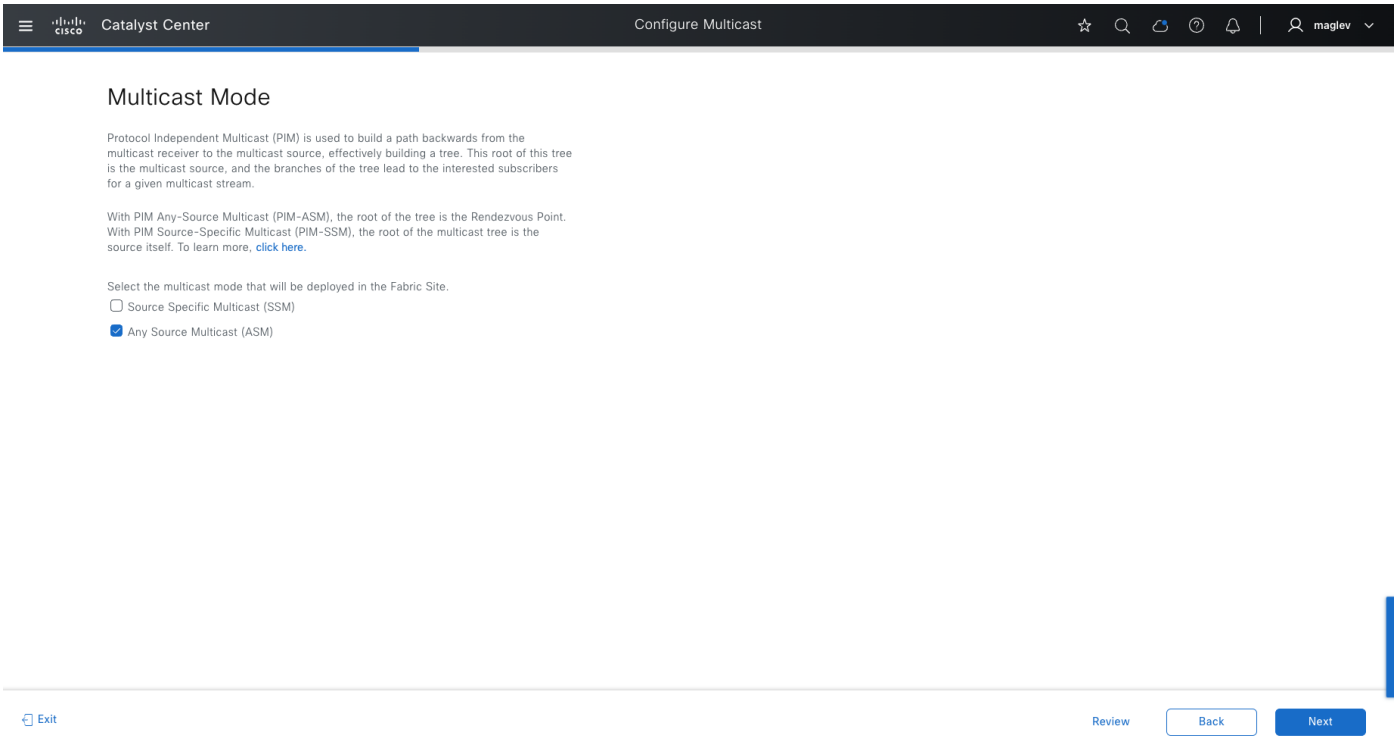



**ステップ 5.** 定義済みの **IP アドレスプール**を追加し、[Next] をクリックします。

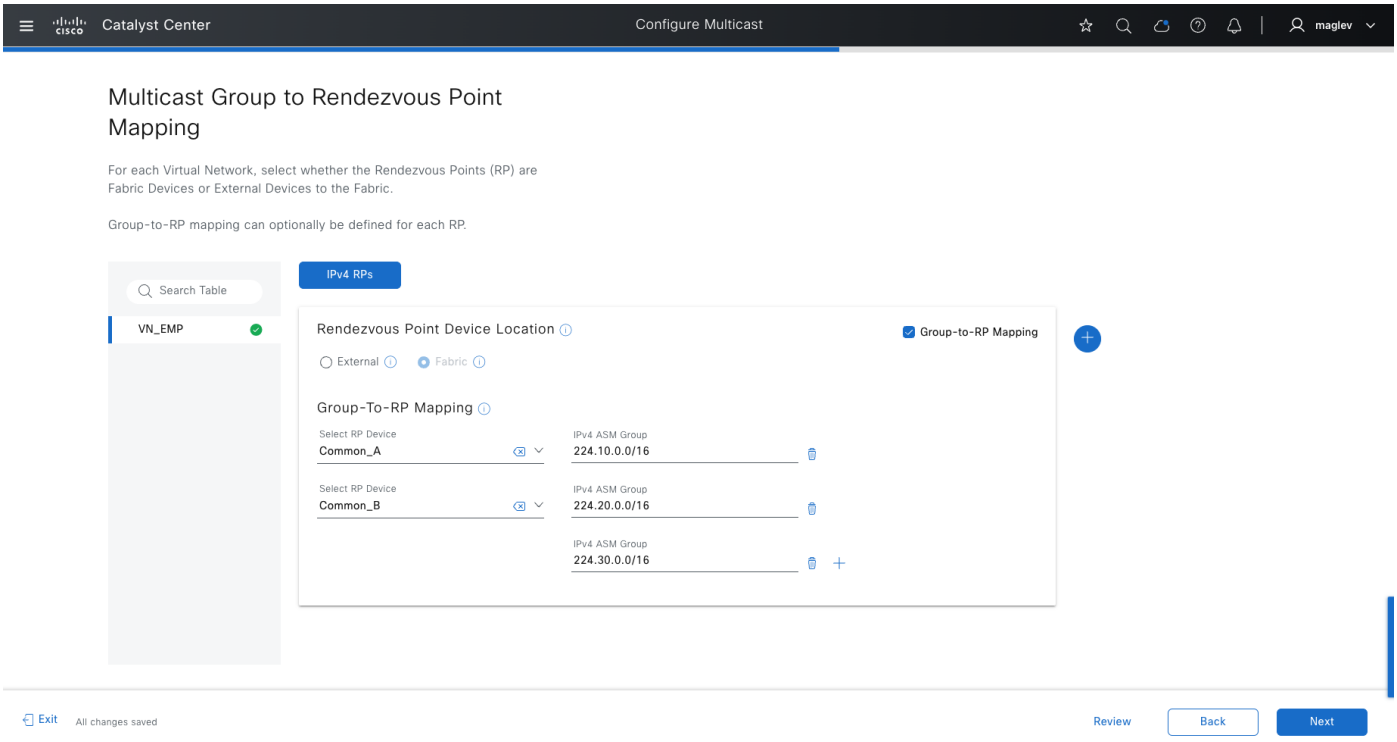



**技術的なヒント：** マルチキャストが複数の VN で有効になっている場合、各 VN には一意の IP アドレスプールが必要です。

**ステップ 6.** [Any Source Multicast（ASM）] モードを選択します。ASM モードは RP を設定します。




**ステップ 7.** RP マッピングとマッピングされた RP グループ（オプション）を設定し、タスクを展開するためのワークフローを完了します。




**注：**

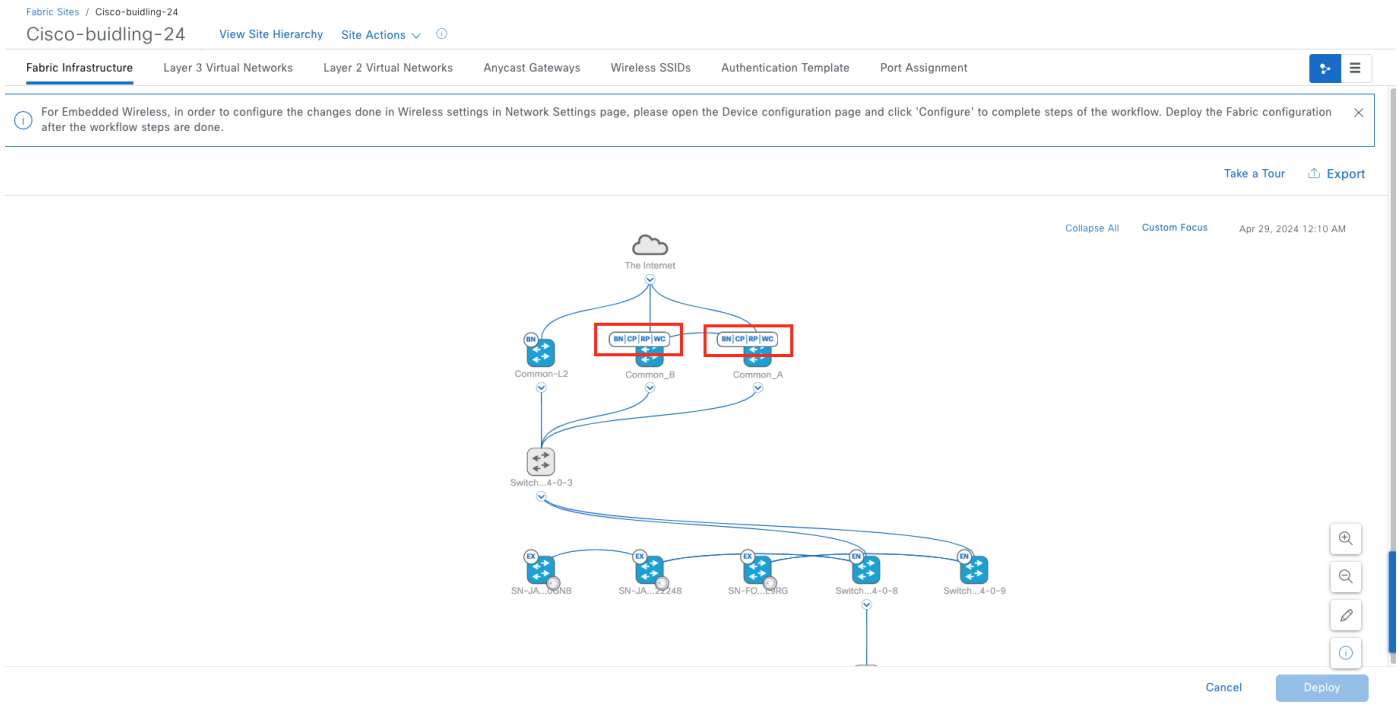
1. RP がファブリック内にある場合、ボーダーデバイスまたはエッジデバイスで RP 機能を有効にできます。ボーダーデバイスとエッジデバイスの組み合わせはサポートされていません。ボーダーデバイスで RP が有効になってい

る場合、同じ ASM グループによるデュアル RP の設定がサポートされています。RP がエッジデバイスで有効になっている場合、サポートされている RP は 1 つだけです。RP がファブリック内にある場合、各 VN に対して追加できる RP は 1 つだけです。ボーダーノードは、より多くの CPU、RAM、および ASIC リソースを備えたハイエンドプラットフォームであるため、エッジノードではなくボーダーノードで RP を設定することをお勧めします。

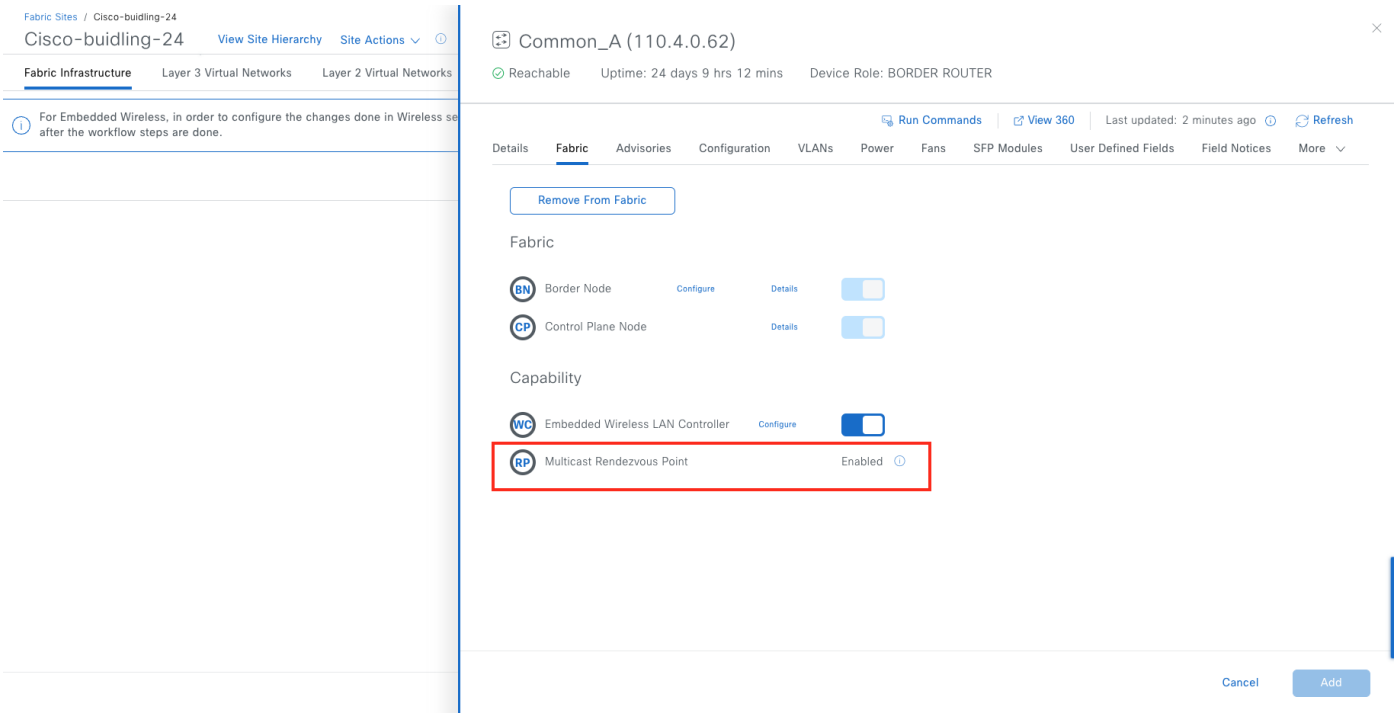
2. RP がファブリック外にある場合、異なる ASM グループマッピングを使用して複数の外部 RP を追加できます。

3. [Group-To-RP Mapping] はオプションです。オプションをオフにすると、RP はすべてのマルチキャストグループにマッピングされます。

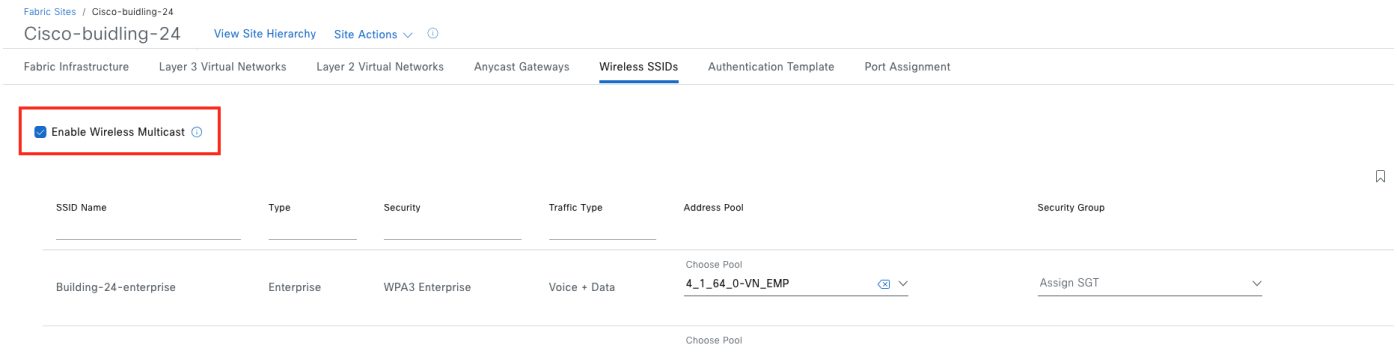
その後、設定がすべてのファブリックデバイスにプッシュされます。トポロジビューでは、RP として設定されている **Common_A** と **Common_B** に **RP** ファブリックロールがマーク付けされます。




**ステップ 8.** Common_A または Common_B をクリックし、マルチキャスト ランデブー ポイントのボーダー機能ステータスが有効になっていることを確認します。




**ステップ 9.** Cisco SD-Access ワイヤレスのマルチキャストを有効にします。[Wireless SSIDs] タブに移動して [Enable Wireless Multicast] をクリックし、ワイヤレスコントローラでグローバル 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します。



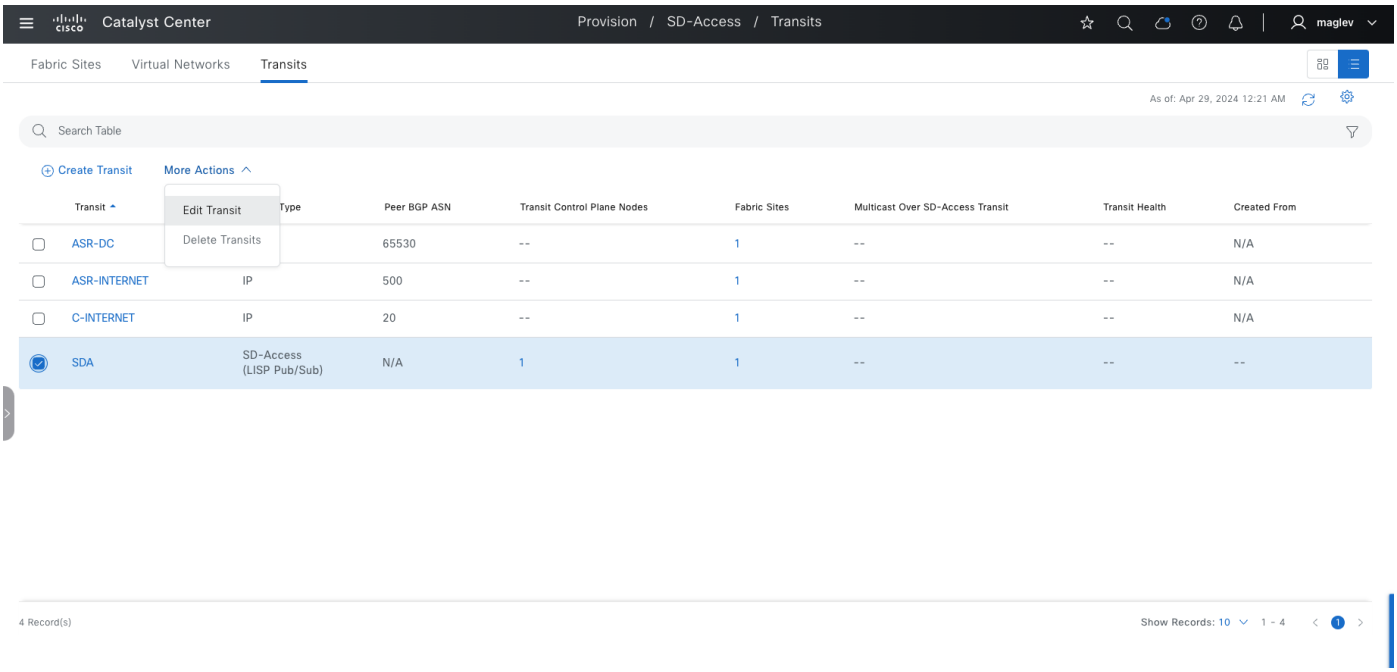

## 手順 2。 ネイティブ マルチキャスト オーバー SD-Access トランジットの有効化

ネイティブマルチキャストは、LISP Pub/Sub を使用したマルチサイト Cisco SD-Access トランジットトポロジでサポートされています。同じ VN でネイティブマルチキャストが有効になっていて、Cisco SD-Access トランジットに接続されているファブリックサイトのマルチキャスト受信者は、同じ送信元からマルチキャストトラフィックを受信できます。

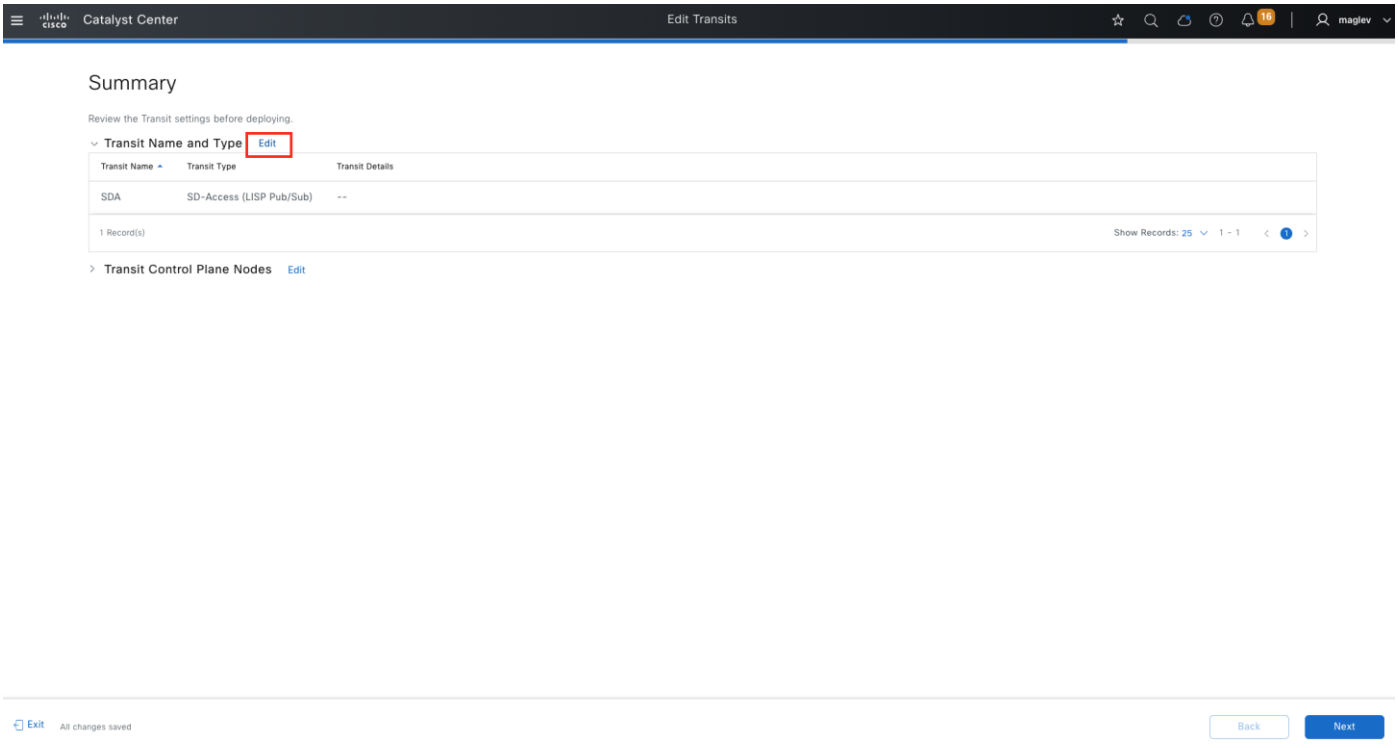
RP は、ファブリックと、共通 RP を指すすべてのファブリックサイトの外部で設定できます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Transits] の順に選択し、右上のテーブルビューアイコンをクリックします。

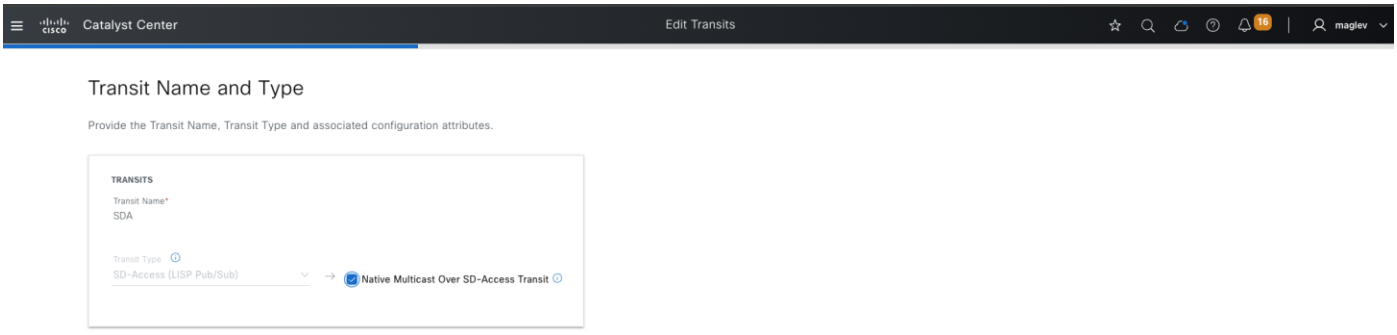
**ステップ 2.** リストの [SDA] をオンにし、[More Actions] > [Edit Transit] の順にクリックします。




**ステップ 3.** [Transit Name and Type] の横にある [Edit] をクリックし、[Next] をクリックします。



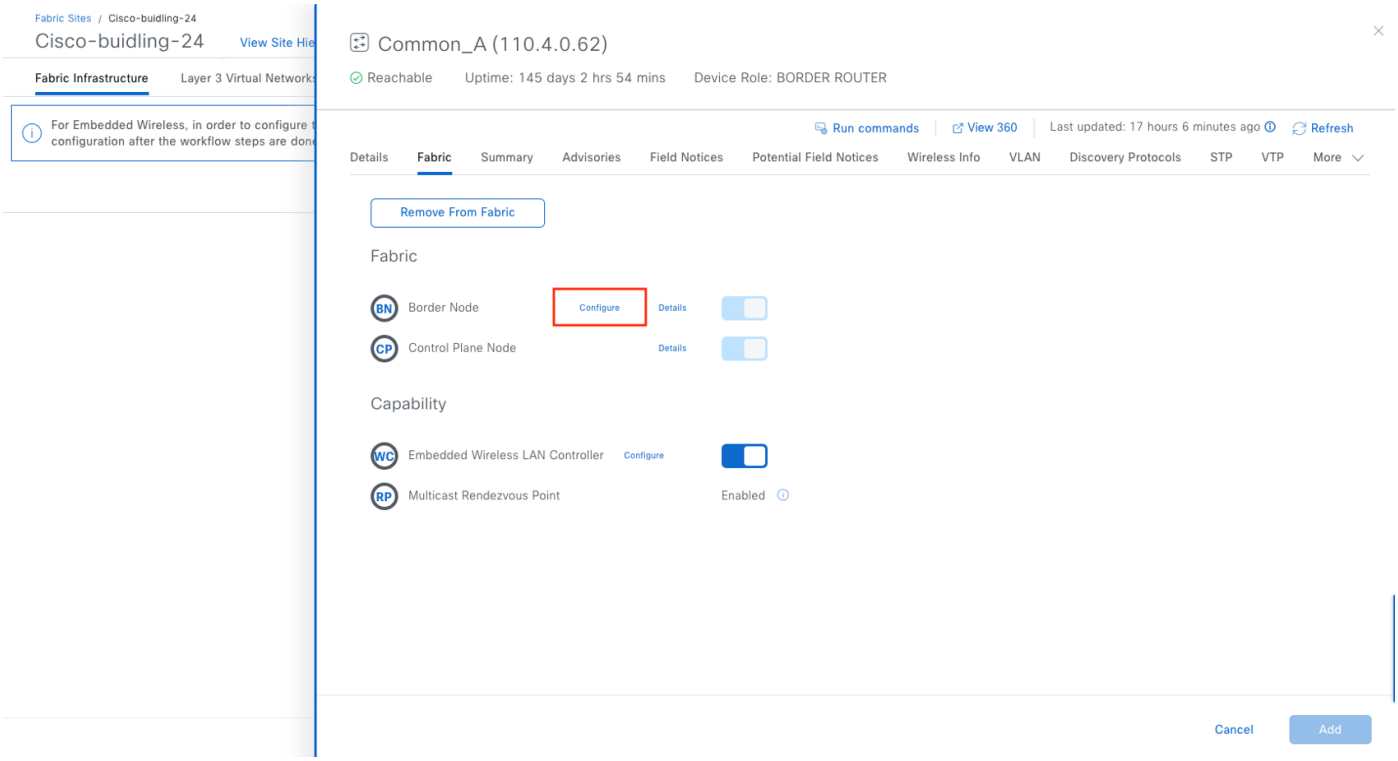

**ステップ 4.** [Native Multicast Over SD-Access Transit] チェックボックスをオンにしてから、[Next] をクリックしてタスクを展開するワークフローを完了します。



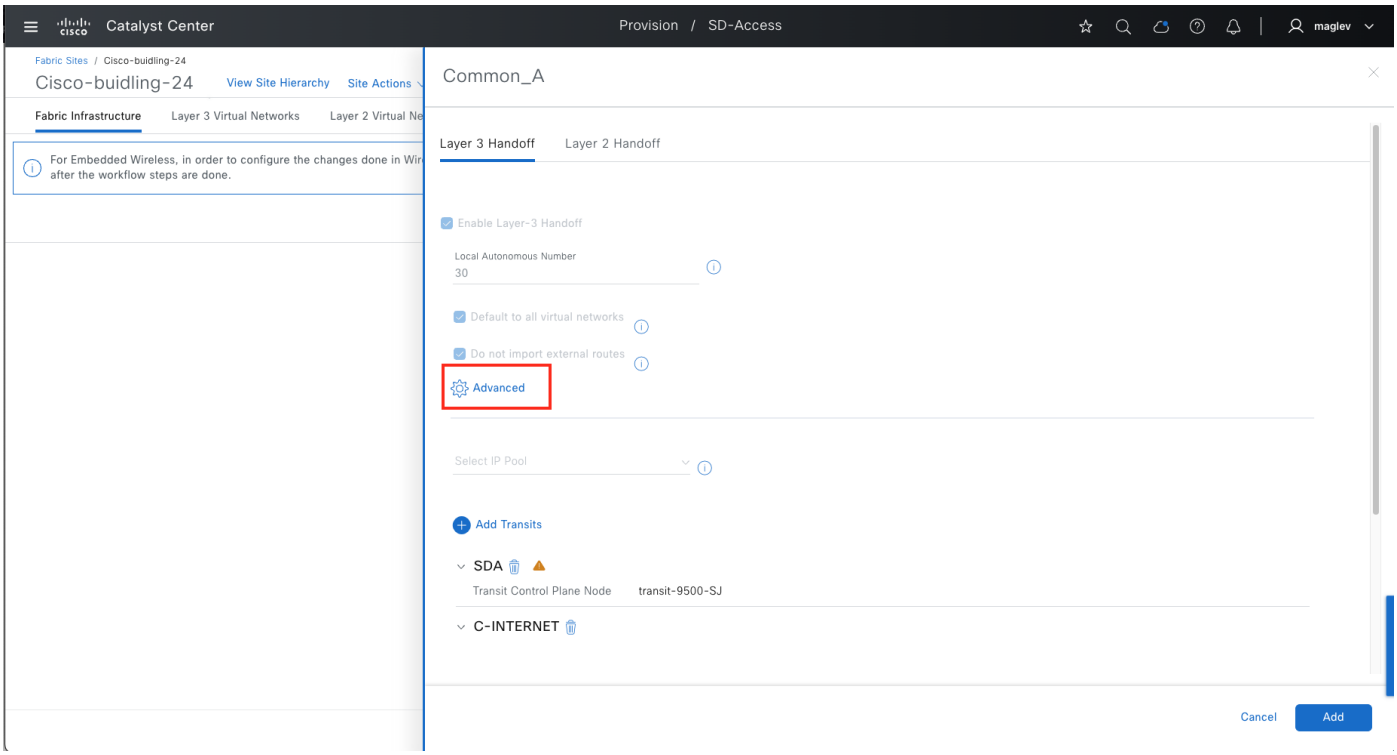


**ステップ 5.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックしてから、[Fabric Infrastructure] タブをクリックします。

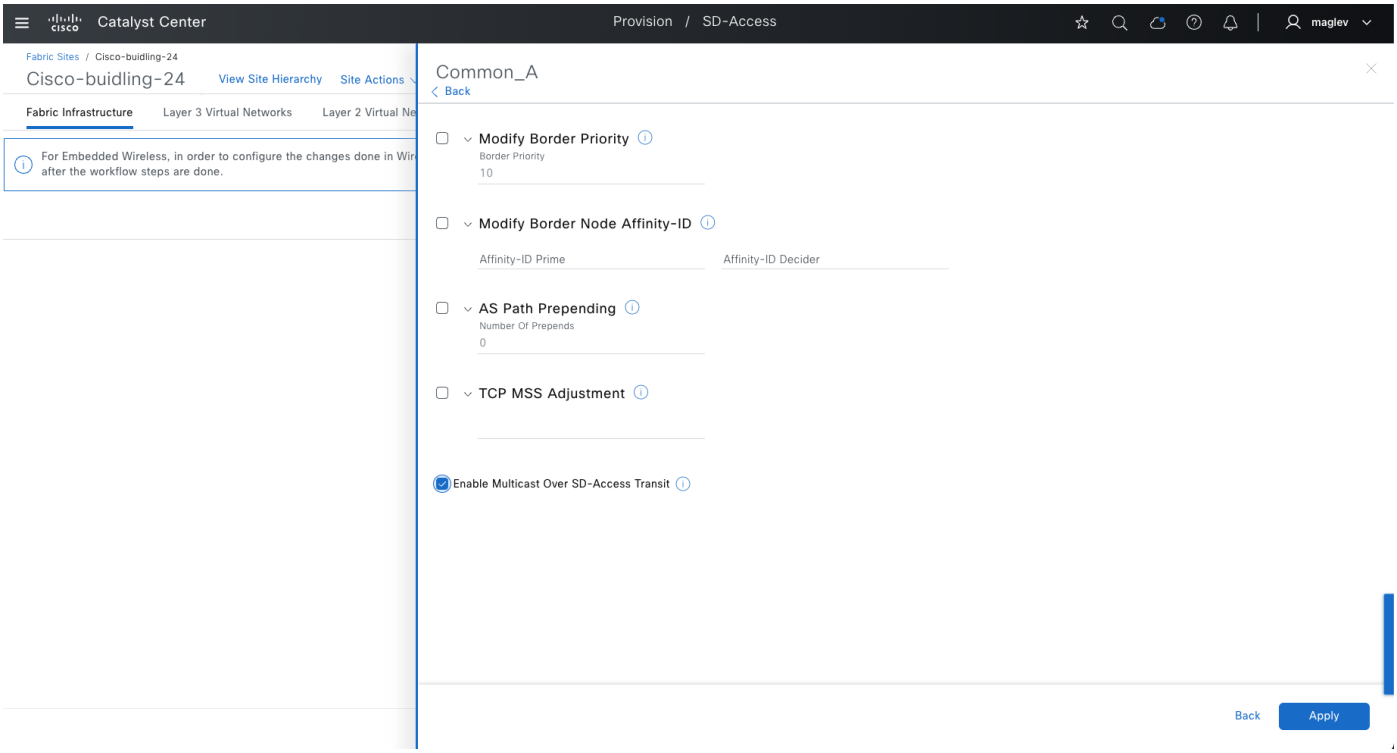
**ステップ 6.** スライドインペインで [Common_A] をクリックしてから、[Border Node] の横にある [Configure] をクリックします。



**ステップ 7.** [Advanced] をクリックします。



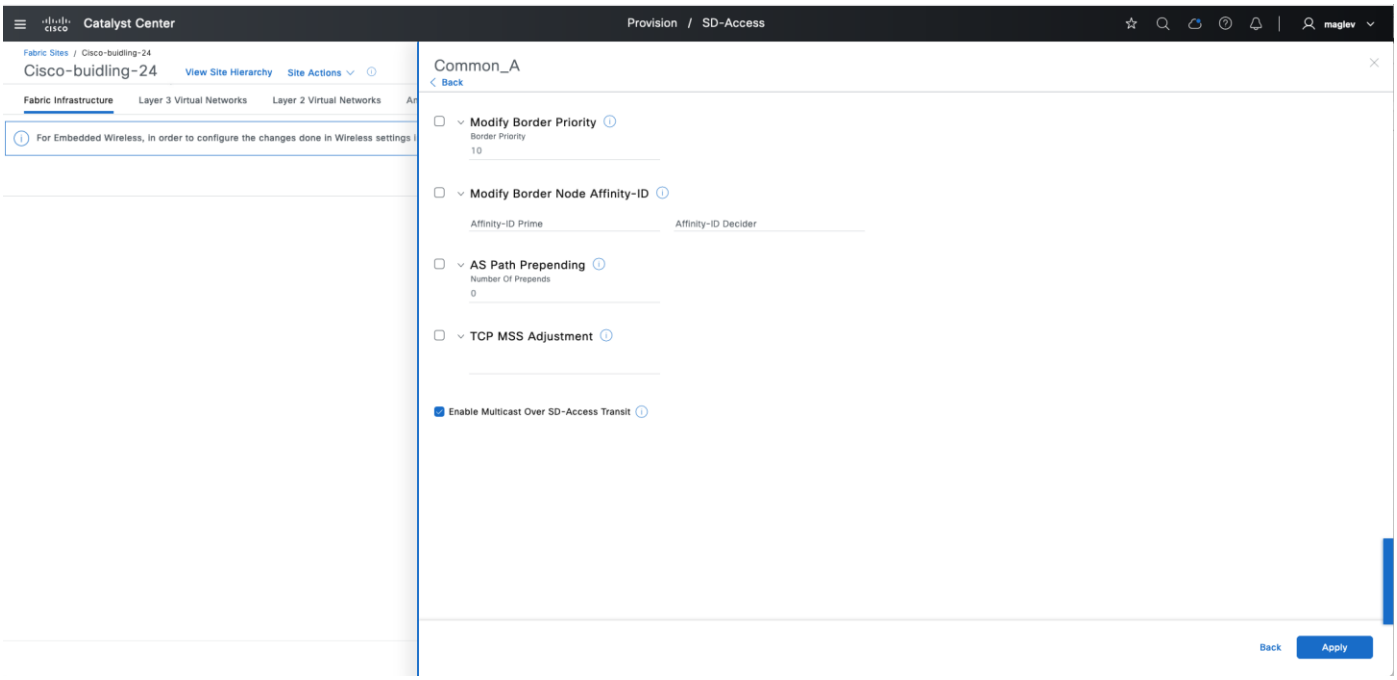

**ステップ 8.** [Enable Multicast Over SD-Access Transit] オプションをオンにしてから、[Apply] をクリックしてワークフローを完了し、タスクを展開します。




**ステップ 9.** **Common_B** ボーダーで同じステップを繰り返します。

## ファブリックボーダーでの高度なファブリック機能の使用

**図 45.　　ファブリックボーダーの高度な機能オプション**




### ボーダーの優先順位

Catalyst Center には、ファブリック ネットワーク トラフィックを出力するボーダーノードを選択する機能があります。

優先順位値は 1 ～ 9 の間で設定できます。1 が最も高く、9 が最も低くなります。ボーダーの数値が小さいほど優先されます。優先順位値を設定しない場合、デフォルトで、ボーダーには優先順位値 10 が割り当てられます。ボーダーの優先順位が設定されていない、またはボーダー間で同じ場合、トラフィックはボーダーノード間で負荷分散されます。

ボーダーの優先順位は LISP 設定であり、ファブリックからデバイスを削除せずに Day-*N* 運用で変更できます。ボーダーに設定された優先順位値は、そのボーダーからハンドオフされるすべての仮想ネットワークに適用されます。Cisco SD-Access トランジットでファブリックサイトが相互接続されている場合、トラフィックを外部ネットワークに送信するために、最も優先順位の低い外部ボーダーが選択されます。

このオプションは、3 種類のレイヤ 3 ボーダーのすべてで使用できます。

### アフィニティ ID

アフィニティ ID は、ローカルインターネットが利用できない場合に、Cisco SD-Access トランジットを介して到達可能な最も近いリモートデフォルト ETR（インターネットサービスを備えたデフォルトルート）を選択するために使用されます。参加しているすべてのファブリックサイトは、Cisco SD-Access トランジットが設定されているボーダーでアフィニティ ID を設定する必要があります。デフォルトでは、この機能は無効になっています。

アフィニティ ID には Prime（X）値と Decider（Y）値が含まれています。0 ～ 2147483647 の Prime と Decider の値を設定できます。参加しているボーダーが他のサイトのボーダーからアフィニティ ID 値を受信した場合、次のようにアフィニティ値を計算します。

- 相対的な Prime 値：abs（X-X'）相対的な Prime 値が小さいほど、優先順位が高くなります。
- 相対的な Decider 値：abs（Y-Y'）2 つのボーダーノードの Prime 値が同じ場合、ボーダーノードの優先順位を決定するタイブレーカーとして Decider 値が使用されます。

アフィニティ ID は、Day-*N* 運用で変更できる LISP 設定であり、インターネットサービスを必要とするすべての VN に適用できます。アフィニティ ID が設定されている場合、優先順位を決定するためにボーダーの優先順位が優先されます。計算されたアフィニティ値が同じ場合、ボーダーの優先順位を使用してボーダーノードの優先順位が決定します。

このオプションは、外部ボーダーまたは内外ボーダーでのみ使用できます。

SD-Access トランジット展開を介したマルチサイトの一般的なユースケースでは、地理位置情報または距離に基づいてアフィニティ ID が設定されます。複数のサイトからインターネットにアクセスできます。距離に基づくアフィニティ ID で、インターネットトラフィックのクローズドリモートボーダーを選択するように設定できます。

**AS-Path プリペンド**

AS-Path プリペンド技術は、ボーダーノード上の BGP 設定であり、入力トラフィックのファブリックボーダーを選択するために eBGP ピアデバイスにアドバタイズされます。デフォルトでは、このオプションは無効になっています。設定は Day-*N* 運用で変更され、レイヤ 3 ハンドオフワークフローを通じて設定されたすべての eBGP ピアにアドバタイズするように設定できます。

このオプションは、すべてのタイプのレイヤ 3 ボーダーで使用できます。

**TCP MSS 調整**

Cisco SD-Access では、エンドポイントデータの転送にファブリック VXLAN カプセル化が使用されます。このカプセル化により、元のパケットに 50 バイトのオーバーヘッドが追加され、フラグメント化できなくなります。ジャンボ MTU に対応できない展開では、TCP MSS 調整機能を使用して、TCP セッションで入力 MTU を適用します。

TCP MSS 調整機能は、ファブリック エニーキャスト ゲートウェイまたはレイヤ 3 ハンドオフインターフェイスで設定できます。ボーダーで有効にすると、すべてのレイヤ 3 インターフェイスにこの値が適用されます。

このオプションは、3 種類のレイヤ 3 ボーダーすべてで使用可能で、Day-*N* 運用中に変更できます。

## VN のアンカー

前の MSRB セクションで説明したように、VN アンカーリングを検討してください。

- 各 VN の出力設定：DMZ へのゲストトラフィックなど、特定の VN の入力および出力ファブリックサイトを指定します。
- 複数のファブリックサイトで同じサブネット：IP アドレス空間を保持および節約します。

**技術的なヒント：**

1. ボーダーノードとコントロールプレーンノードは、アンカーサイトに分散またはコロケーションできます。

2. VN は、1 つのファブリックサイトにのみアンカーできます。

3. アンカーサイトとアンカーリングサイト間のシームレス ワイヤレス ローミングはサポートされていません。

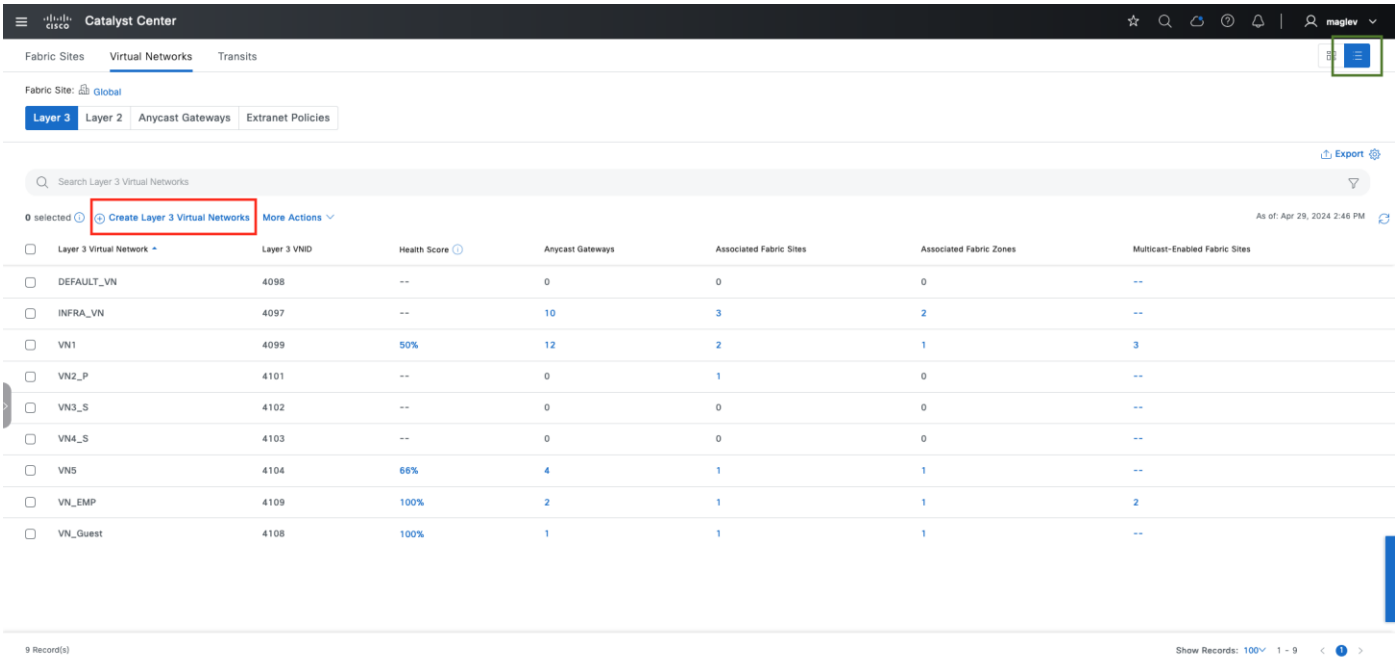
4. Catalyst 9800 ワイヤレスコントローラは、最大 16 のコントロール プレーン ノード ペアをサポートしていますが、アンカーサイトを設定しすぎないようにしてください。

5. 通常の VN のアンカー VN への変更はサポートされていません。VN アンカーリング設定は、グリーンフィールド VN 専用です。

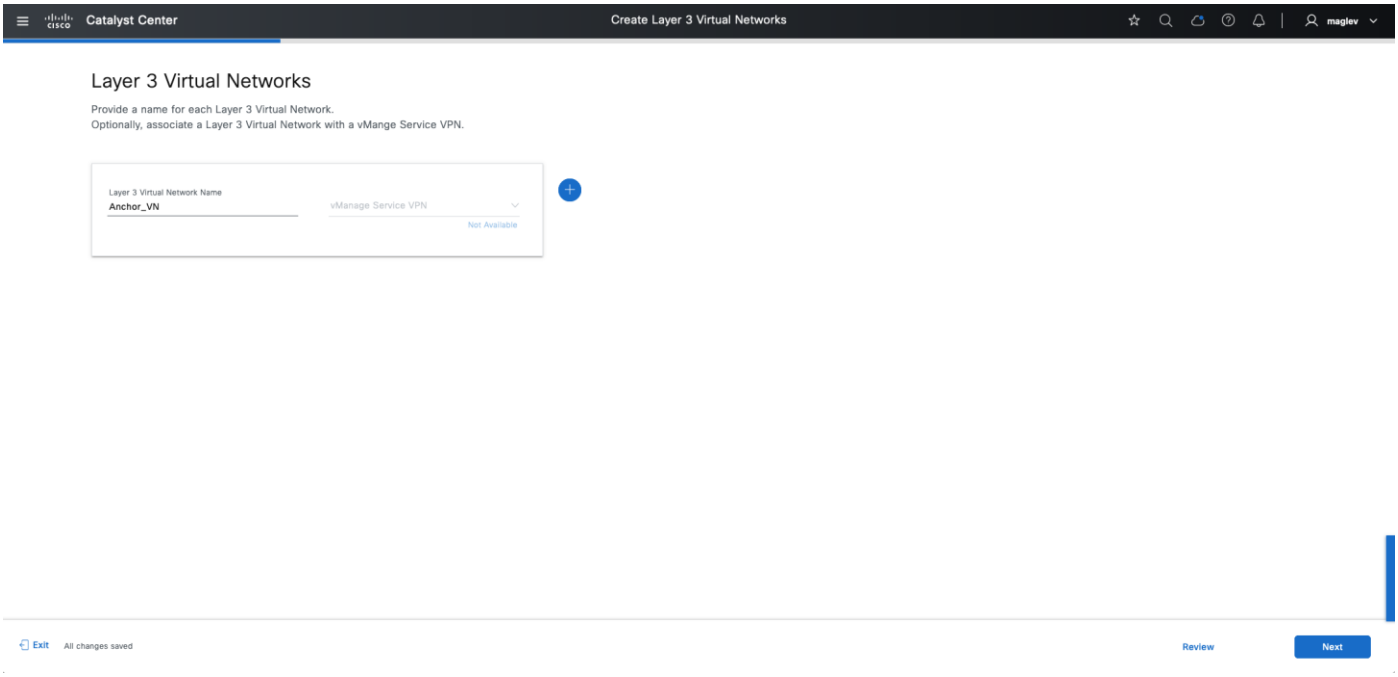
このセクションでは、ファブリックサイト **Cisco-building-24** に関連付けられた IP アドレスプールを使用してアンカー VN を作成し、**Cisco-Building-9** という名前の別のファブリックサイトで使用する方法を説明します。

## 手順 1。 アンカー VN の作成

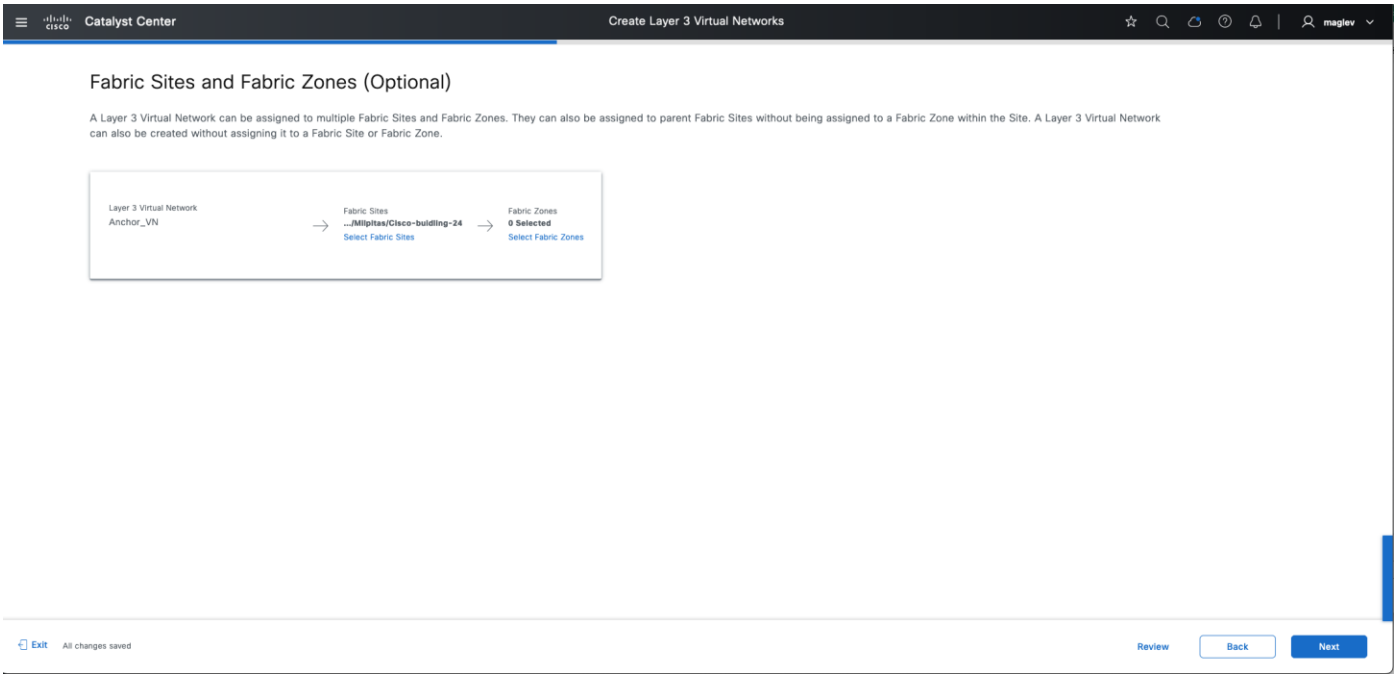
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Virtual Networks] の順に選択し、テーブルビューに変更してから [Create Layer 3 Virtual Networks] をクリックします。




**ステップ 2.** 新しい VN **Anchor_VN** を作成してから、[Next] をクリックします。

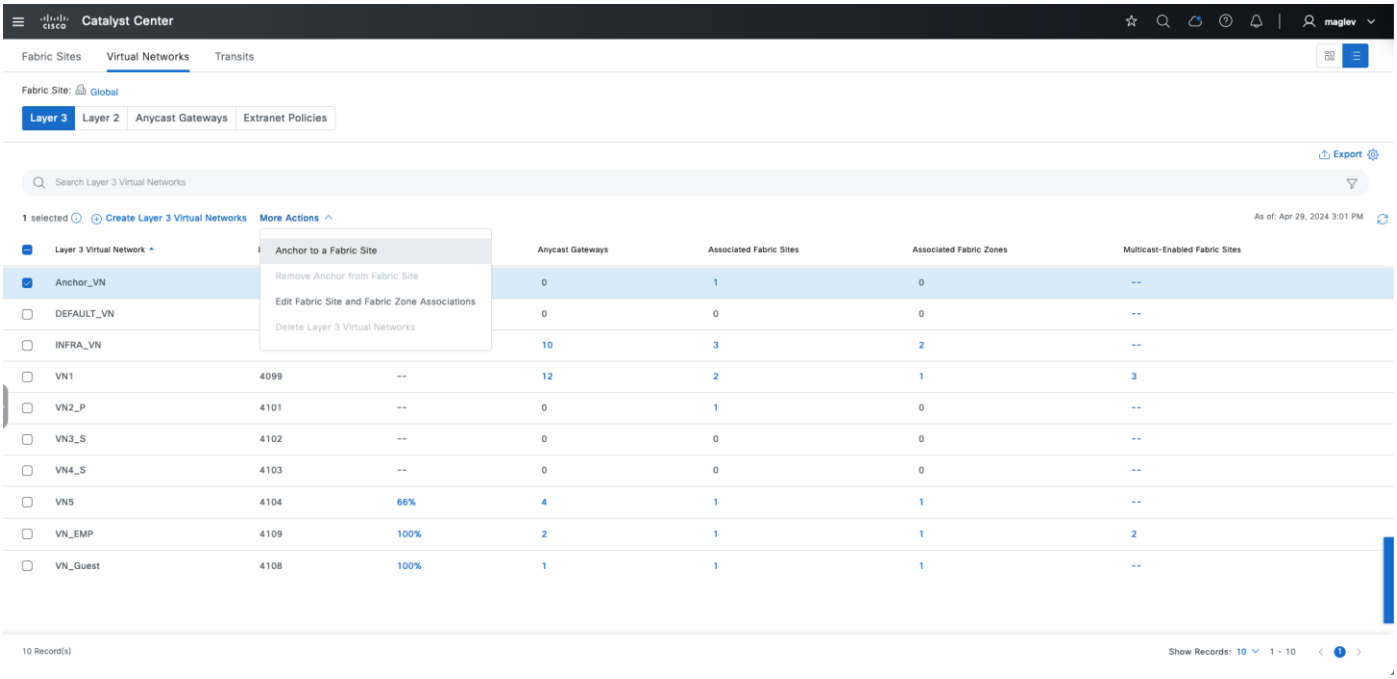



**ステップ 3.** **Cisco-building-24** をアンカーサイトに関連付けてから [Next] をクリックし、ワークフローを完了してタスクを展開します。

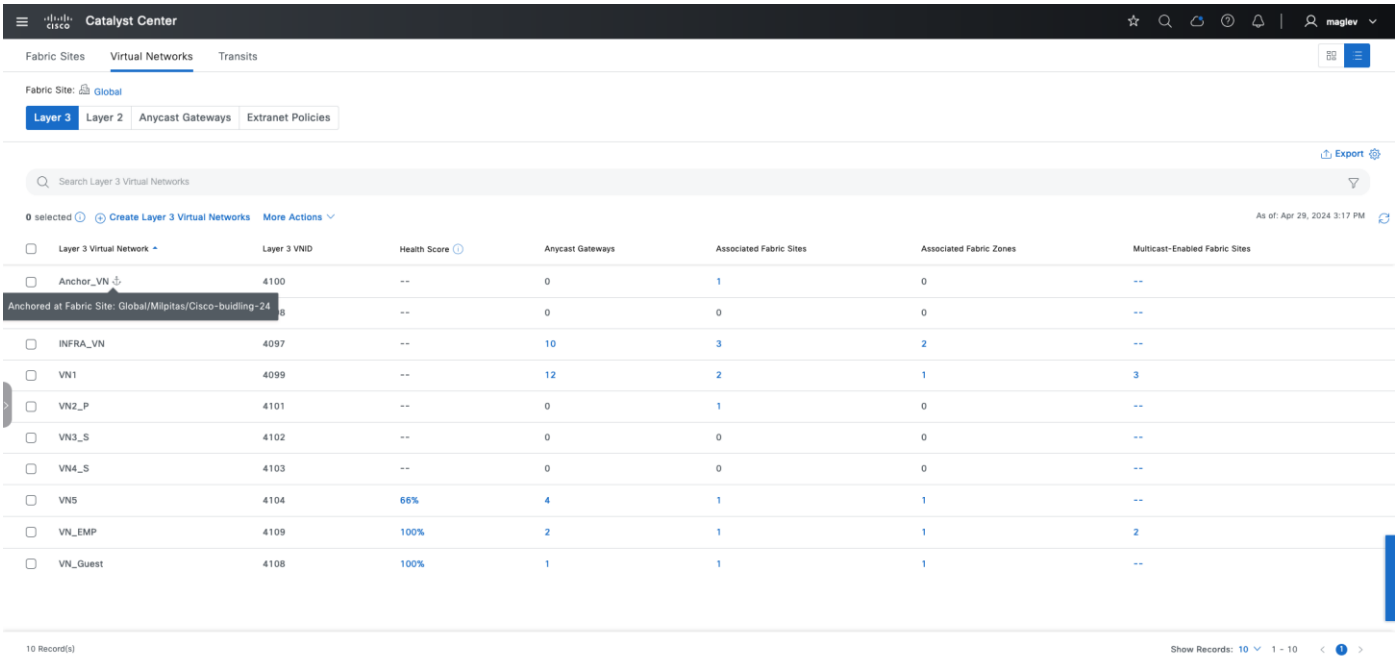



**注：** **Anchor_VN** を有効にする前に、ファブリックゾーンを関連付けないでください。

**ステップ 4.** [Virtual Networks] ウィンドウに戻り、新しい VN [Anchor_VN] チェックボックスをオンにしてから、[More Actions] > [Anchor to a Fabric Site] の順にクリックしてタスクを展開します。




**ステップ 5.** タスクが完了すると、**Anchor_VN** に新しいアンカーアイコンが表示されます。アイコンをクリックし、アンカーサイト情報を表示します。

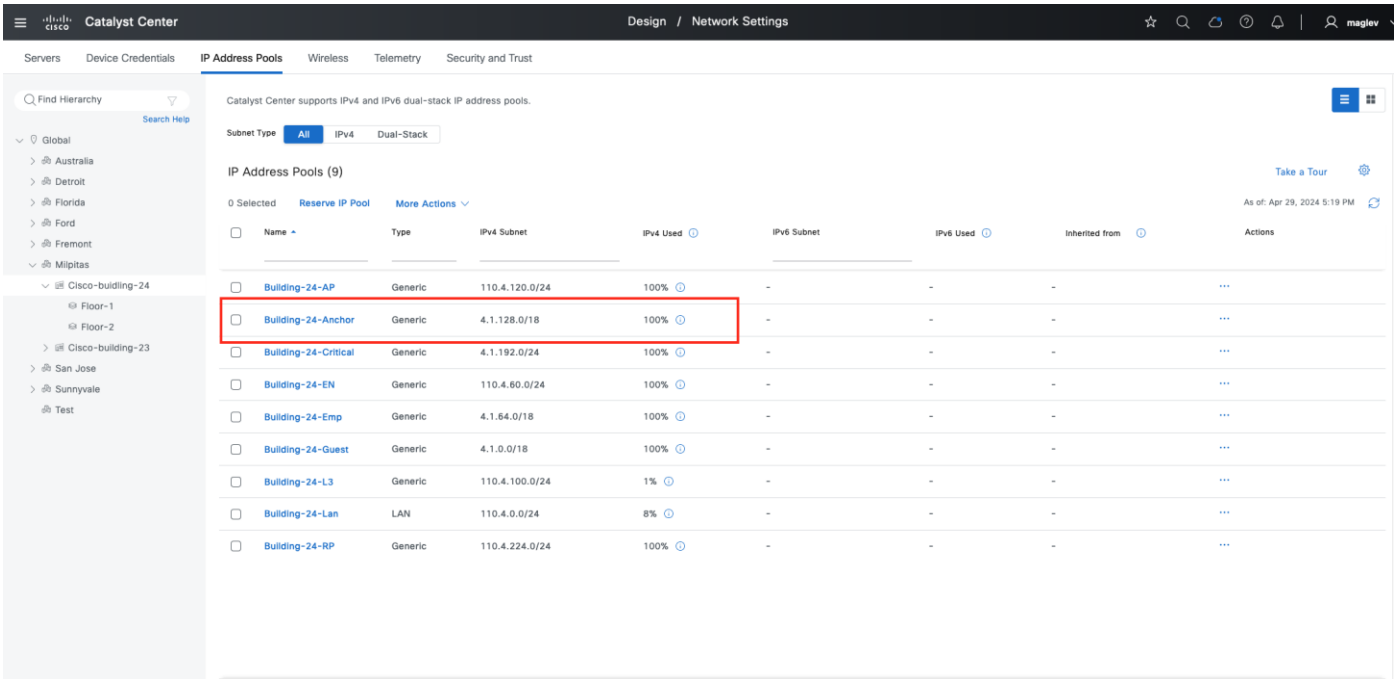



**ステップ 6.** エニーキャストゲートウェイを作成し、アンカー VN の IP プールを追加します。

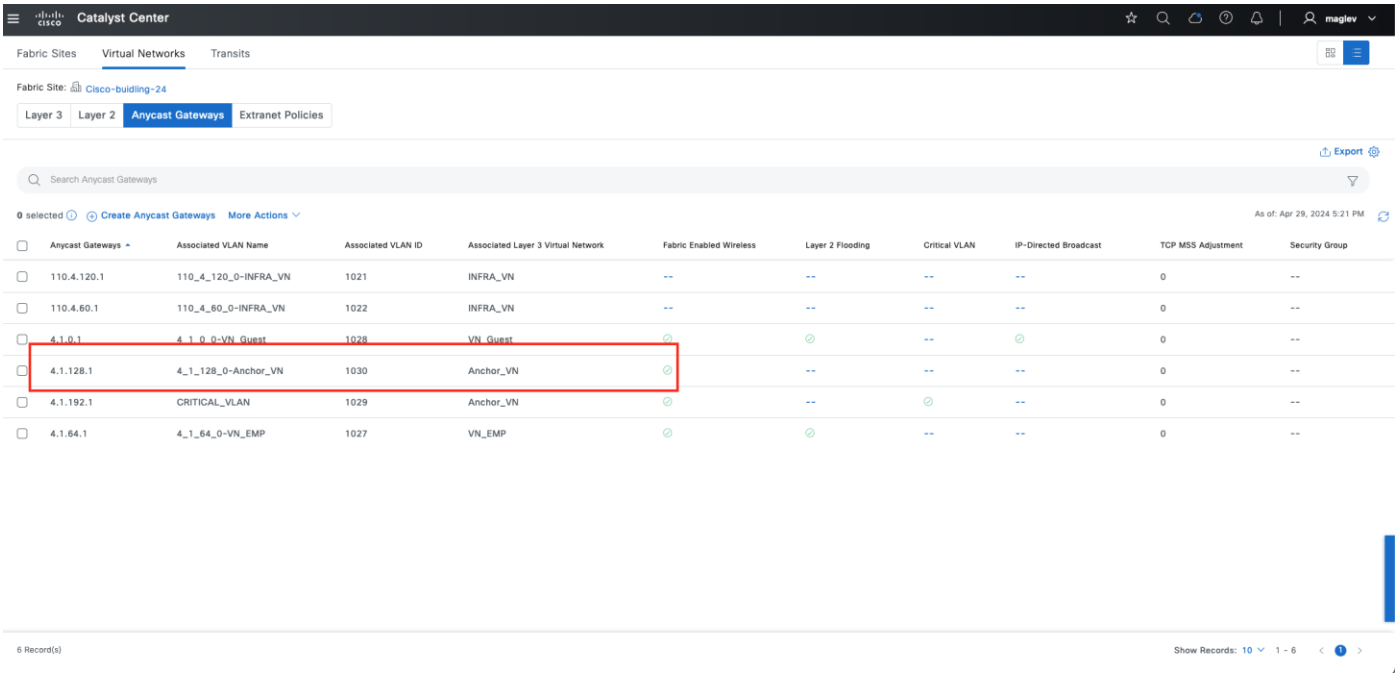
VN がアンカー VN として設定されると、関連付けられたすべての IP プールもアンカーされ、アンカーリングサイトから選択して使用できます。

エニーキャストゲートウェイの作成のセクションを参照し、**Anchor_VN** に新しいエニーキャストゲートウェイを作成します。

- 左上隅にあるメニューアイコンをクリックして [Design] > [Network Settings] の順に選択し、[IP Address Pools] タブをクリックしてから、**Building-24-Anchor** の IP プールを予約します（「手順 2：ファブリックサイト用 IP プールの予約」を参照）。




- エニーキャストゲートウェイを作成し、**Cisco-building-24** の **Anchor_VN** に追加します。

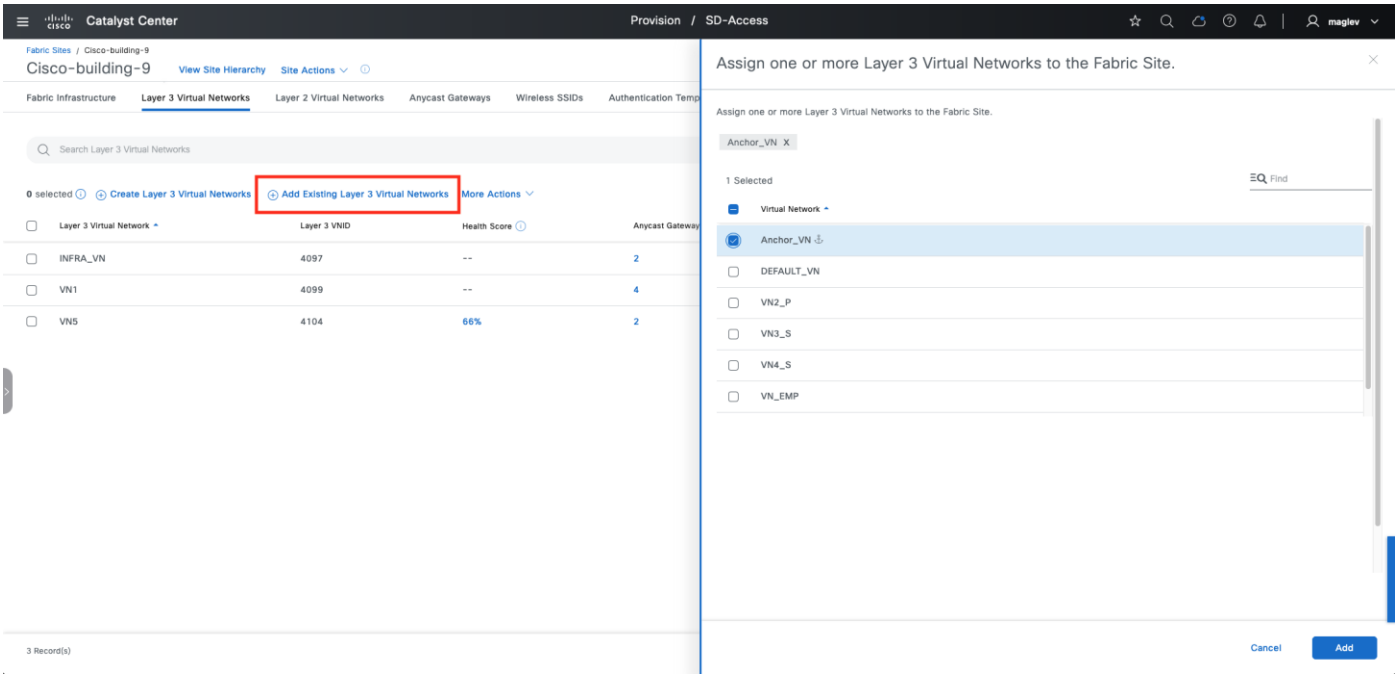



## 手順 2。 アンカーサイトへのアンカー VN とアンカープールの追加

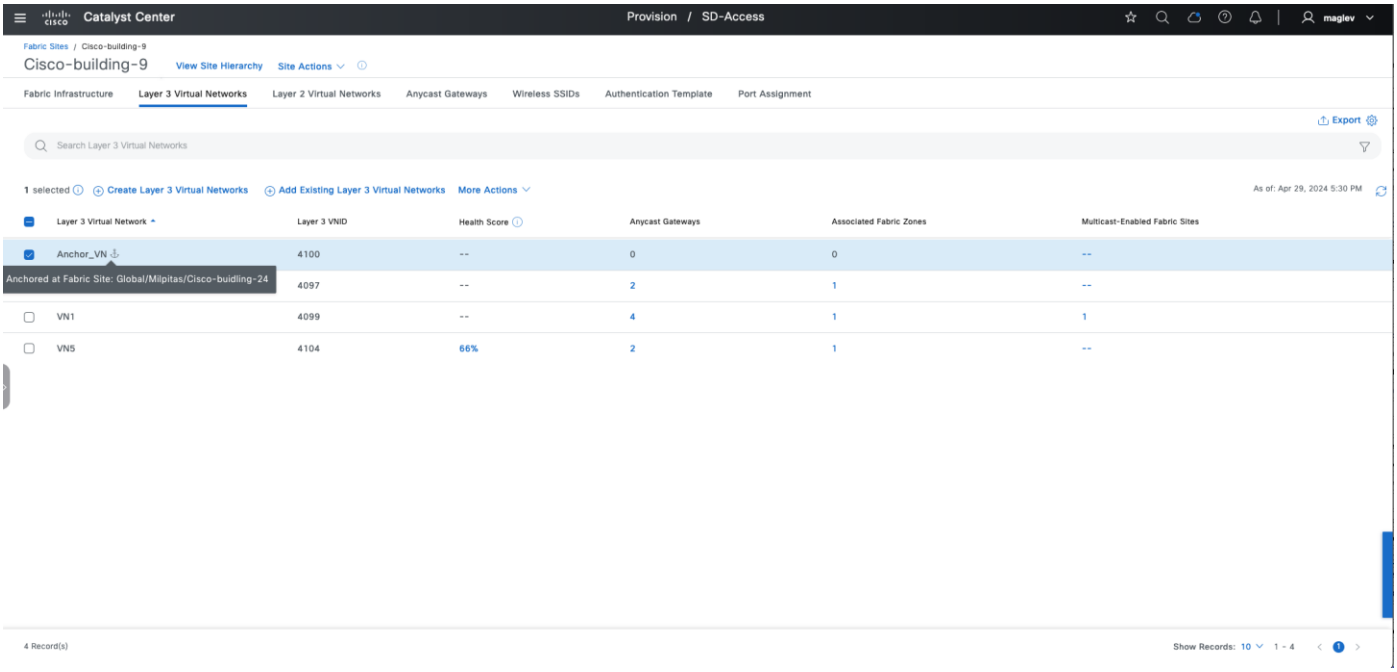
他のファブリックサイトに移動します。この例では、別のファブリックサイト **Cisco-Building-9** を使用してプロセスを説明します。**Cisco-Building-9** には、2 つのローカル コントロール プレーン ノード（IP：2.3.3.11 および 2.3.3.12）、複数のエッジノード、および 1 つのスタンドアロン C9800 ワイヤレスコントローラがあります。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックし、[Cisco- Building-9] テキストリンクをクリックしてから、[Layer 3 Virtual Networks] タブをクリックします。

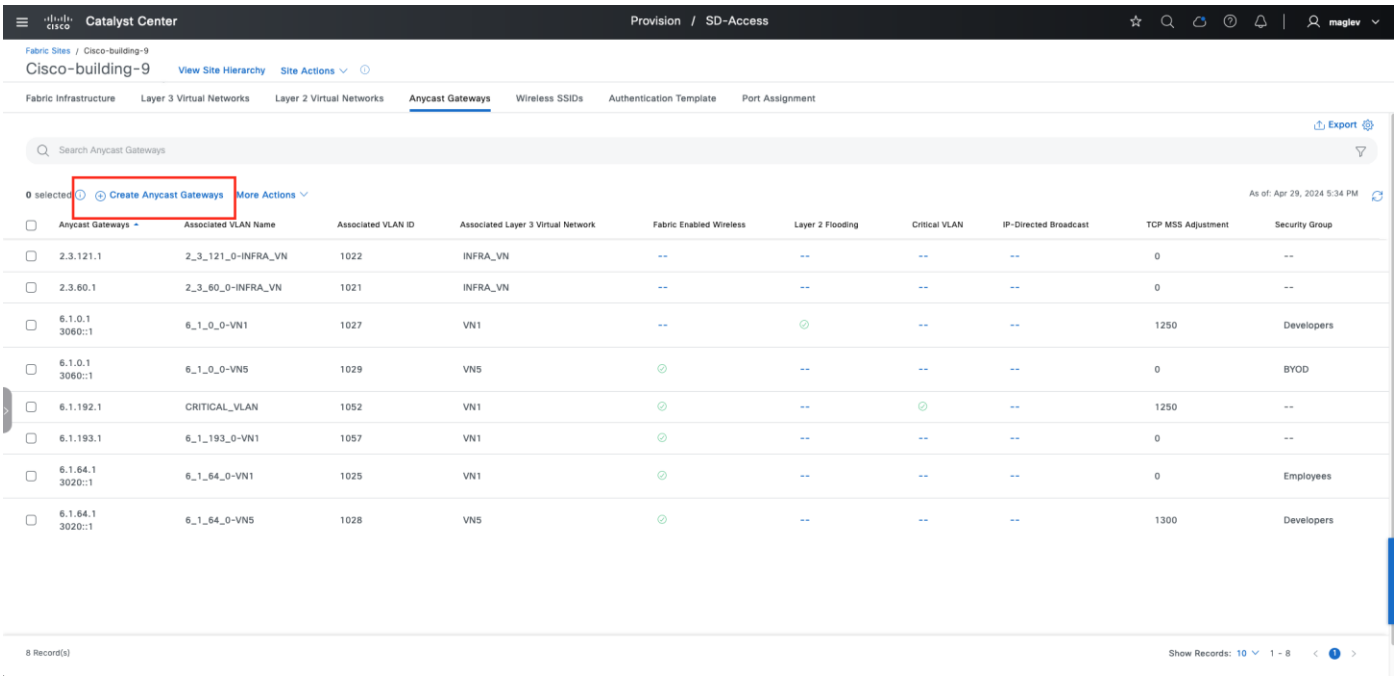
**ステップ 2.** [Add Existing Layer 3 Virtual Networks] をクリックし、スライドインペインで [Anchor_VN] をオンにして [Add] をクリックし、ワークフローを完了してタスクを展開します。



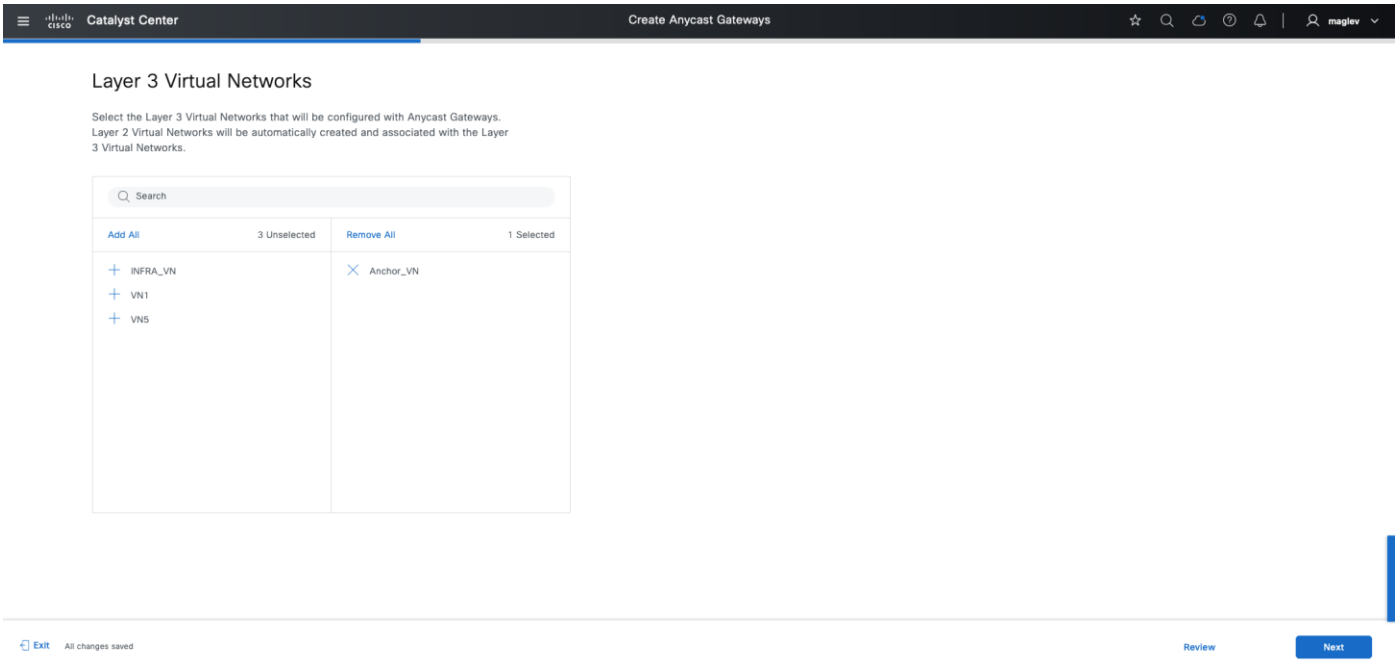

タスクが完了すると、**Anchor_VN** が、アンカーサイトとして **Cisco-building-24** を識別するアンカーアイコンとともに追加されます。



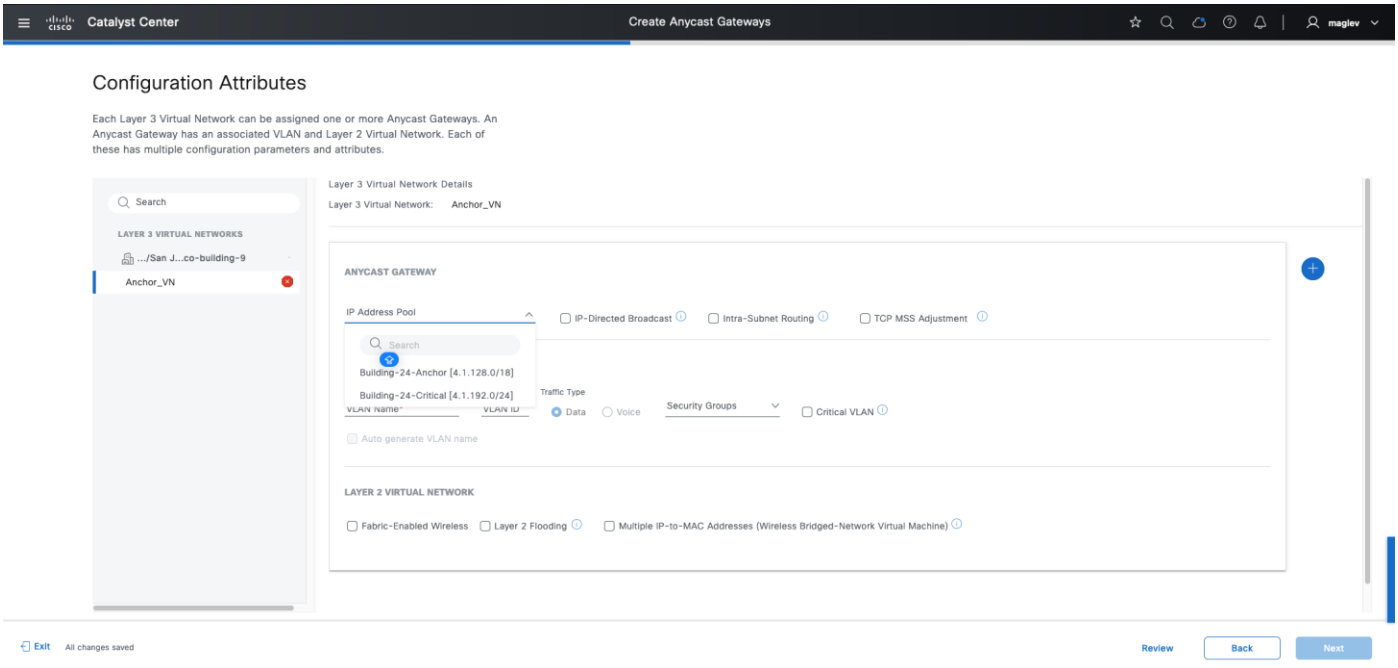
**ステップ 3.** IP アドレスプールを追加します。[Anycast Gateways] タブに移動してから、[Create Anycast Gateways] をクリックします。




**ステップ 4.** [Anchor_VN] を選択します。



[Anchor_VN] に追加できるのはアンカープールのみです。




**ステップ 5.** 優先属性を持つ **Building-24-Anchor** プールを追加し、ワークフローを完了します。

**ステップ 6.** **Cisco-Building-9** のファブリックエッジノードで、確立された 4 つの LISP セッションを確認します。最初の 2 つは **Cisco-Building-9** ローカル コントロール プレーンで確立され、残りの 2 つは **Cisco-building-24** アンカー コントロール プレーンで確立されます。

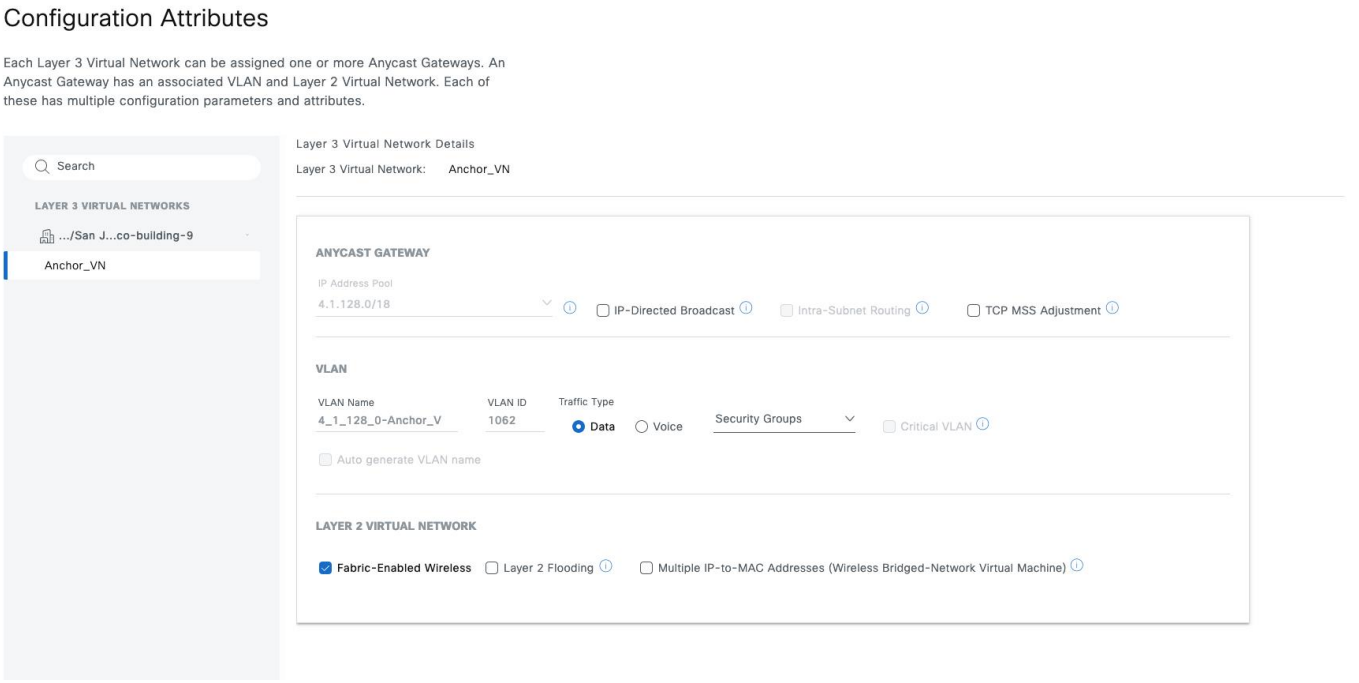
```
TB2-FE2#show lisp session

Sessions for VRF default, total: 4, established: 4
Peer              State      Up/Down        In/Out    Users
2.3.3.11:4342     Up         3d10h        1343/550    42
2.3.3.12:4342     Up         3d10h        1347/553    42
110.4.0.62:4342   Up         00:00:25       66/5      5
110.4.0.63:4342   Up         00:00:02       66/5      5
```

**技術的なヒント：** 継承されたサイトのエッジに、グローバル ルーティング テーブルのアンカーサイトにあるコントロールプレーンノードとボーダーノードの loopback0 インターフェイスアドレスへの明示的なルートがあることを確認します。アンカーサイトにあるコントロールプレーンノードとボーダーノードには、loopback0 インターフェイス アドレス エッジへの明示的なルートもあります。

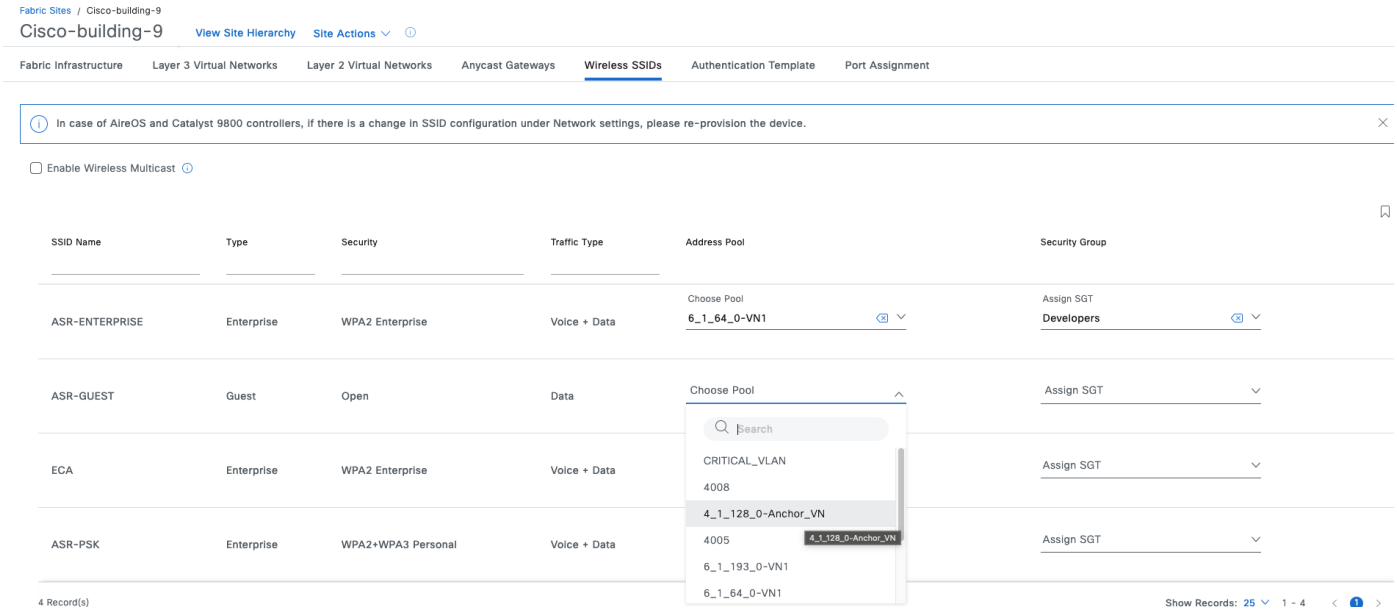
**ステップ 7.** 継承されたサイトの SSID にアンカープールを関連付けます。

アンカープールは、継承されたサイトの有線クライアントとワイヤレスクライアントの両方に使用できます。

**ステップ 8.** ワイヤレスクライアントのアンカープールを使用するには、アンカープールの [Configuration Attributes] の [Fabric-Enabled Wireless] チェックボックスをオンにします。




**ステップ 9.** メニューアイコンボタンから [Provision] > [Fabric Sites] の順に選択して右上のテーブルビューアイコンをクリックし、[Cisco-Building-9] テキストリンクをクリックして [Wireless SSIDs] タブをクリックして、アンカープールを SSID **ASR-Guest** に関連付けてタスクを展開します。




**ステップ 10.** `show wireless fabric summary` コマンドを使用して、**Cisco-Building-9** のワイヤレスコントローラを検証します。スタンドアロン ワイヤレス コントローラは、次のコントロールプレーンノードを使用します。

- **default-control-plane** はローカル コントロール プレーンであり、**Fabric-Enabled Wireless** 属性が有効になっているすべてのローカルセグメント（レイヤ 2 とレイヤ 3）によって使用されます。

- **Milpitas_Cisco-bu_e087e** は、アンカーサイト **Cisco-building-24** のコントロールプレーンノードです。アンカープールセグメントも関連付けられます。

```
katar-faniu-ewlc#show wireless fabric summary

Fabric Status      : Enabled


Control-plane:
Name                                IP-address                                Key                                       Status
-------------------------------------------------------------------------------------------------------------------------------
default-control-plane               2.3.3.11                                  2fbc7f                                    Up
default-control-plane               2.3.3.12                                  2fbc7f                                    Up
Milpitas_Cisco-bu_e087e             110.4.0.62                                cf90d4420ccb45ad                          Up
Milpitas_Cisco-bu_e087e             110.4.0.63                                cf90d4420ccb45ad                          Up


Fabric VNID Mapping:
  Name              L2-VNID       L3-VNID       IP Address                                Subnet                                    Control plane name
-------------------------------------------------------------------------------------------------------------------------------------------------------
  4004              8235          0                                                       0.0.0.0                                   default-control-plane


Fabric VNID Mapping:
  Name              L2-VNID       L3-VNID       IP Address                                Subnet                                    Control plane name
-------------------------------------------------------------------------------------------------------------------------------------------------------
  4005              8236          0                                                       0.0.0.0                                   default-control-plane
  4008              8228          0                                                       0.0.0.0                                   default-control-plane
  6_1_0_0-VN5       8195          0                                                       0.0.0.0                                   default-control-plane
  6_1_64_0-VN1      8192          0                                                       0.0.0.0                                   default-control-plane
  6_1_64_0-VN5      8194          0                                                       0.0.0.0                                   default-control-plane
  6_1_193_0-VN1     8233          0                                                       0.0.0.0                                   default-control-plane
  CRITICAL_VLAN     8210          0                                                       0.0.0.0                                   default-control-plane
  2_3_60_0-INFRA_VN    8188       0                                                       0.0.0.0                                   default-control-plane
  2_3_121_0-INFRA_VN   8189       4097          2.3.121.0                                 255.255.255.0                             default-control-plane
  4_1_128_0-Anchor_VN  16201      0                                                       0.0.0.0                                   Milpitas_Cisco-bu_e087e
```

**ステップ 11.** **ASR-Guest** という名前の WLAN のステータスを検証するには、`show fabric wlan summary` コマンドを使用します。

```
katar-faniu-ewlc#show fabric wlan summ
Number of Fabric wlan : 2

WLAN Profile Name                    SSID                          Status
-----------------------------------------------------------------------------
17   ASR-ENTERP_Global_F_eec05e51    ASR-ENTERPRISE                  UP
20   ASR-GUEST_profile               ASR-GUEST                       UP
```

## クリティカル VLAN のエニーキャストゲートウェイの作成

デフォルトでは、ネットワーク アクセス デバイス（NAD）が設定済みの RADIUS サーバーに到達できない場合、NAD に接続されている新しいホストは認証できず、ネットワークへのアクセスは提供されません。クリティカル認証、AAA 失敗ポリシー、または単にクリティカル VLAN とも呼ばれるアクセス不能認証バイパス機能は、RADIUS サーバーが使用できない（ダウンしている）場合に特定の VLAN 上でのネットワークアクセスを許可します。

NAD は、ポートに接続されているエンドポイントを認証しようとする場合、最初に、設定されている RADIUS サーバーのステータスをチェックします。利用可能なサーバーが 1 つあれば、NAD はホストを認証できます。ただし、設定済みの RADIUS サーバーのすべてが使用不可能でクリティカル VLAN 機能が有効になっている場合は、NAD はエンドポイントへのネットワークアクセスを許可して、ポートを認証ステートが特別なケースであるクリティカル認

証ステートにします。RADIUS サーバーが再度使用可能になったときに、クリティカル認証ステートのクライアントをネットワークに対して再認証する必要があります。

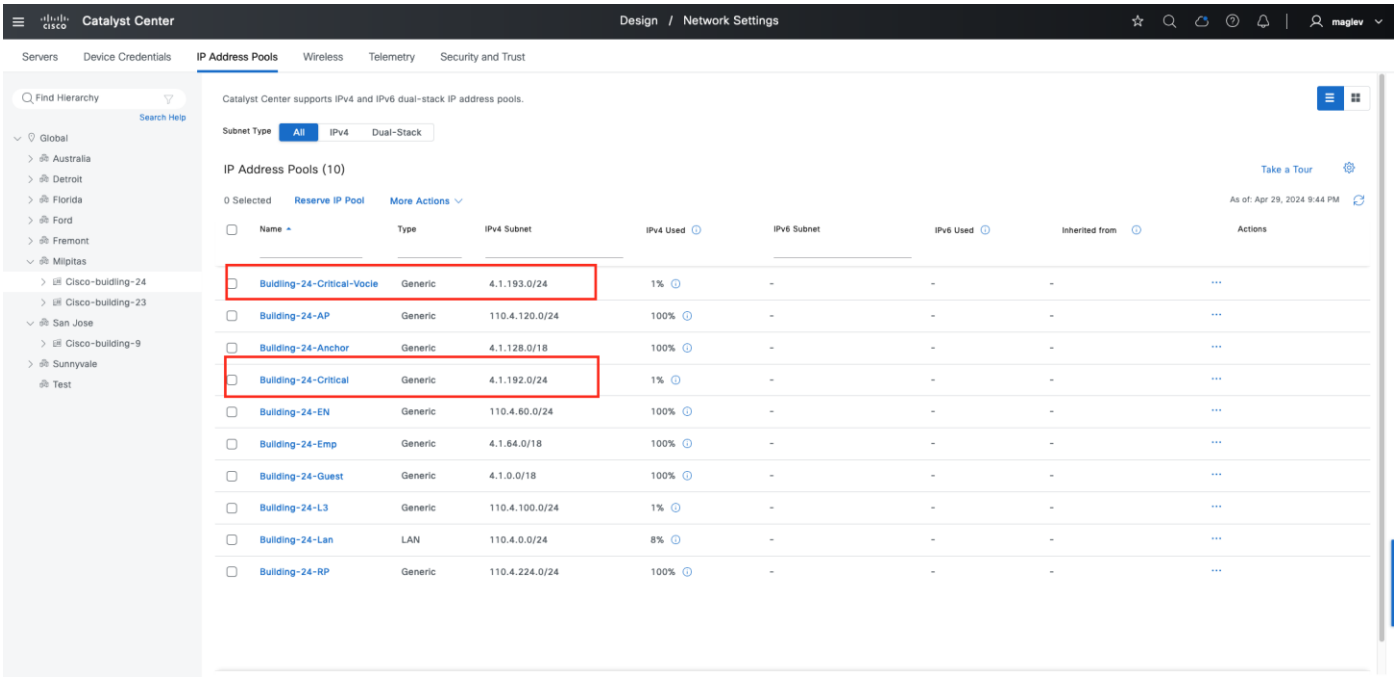
同様に、クリティカル音声 VLAN サポートは、RADIUS サーバーが到達不能になった場合、設定済みの音声 VLAN に音声トラフィックを入れることによって機能します。

Cisco SD-Access では、クリティカルデータ VLAN に VLAN 名 CRITICAL_VLAN を使用して、クリティカル音声 VLAN に VLAN ID 2046 の VIOCE_VLAN を使用します。変更することはできません。ファブリックサイトには、1 つのクリティカルデータ VLAN と 1 つのクリティカル音声 VLAN のみを含めることができます。クリティカル音声 VLAN 2046 は、デフォルトですべてのファブリックエッジに展開される音声 VLAN でもあります。したがって、クリティカル音声 VLAN を明示的に定義する必要はありません。これは、同じ VLAN が音声およびクリティカル音声 VLAN サポートの両方に使用されるためです。これにより、RADIUS サーバーが使用可能かどうかに関係なく、電話機がネットワークにアクセスできるようになります。

IP 電話が FE に接続され、ラップトップが IP 電話に接続されている別のエンドポイントである Cisco SD-Access dot1x マルチドメインケースで、Radius サーバーがダウンしている場合、IP 電話はクリティカル音声 VLAN を介して制限付きアクセスを許可され、ラップトップはクリティカルデータ VLAN を介して制限付きアクセスを許可します。

**ステップ 1.** [Network Setting] ウィンドウで、Cisco-building-24 用に 2 つの新しい IP アドレスプールを予約します。

**図 46.　重要なデータ VLAN および音声 VLAN のエニーキャストゲートウェイが、ファブリックサイト Cisco-building-24 で作成される**

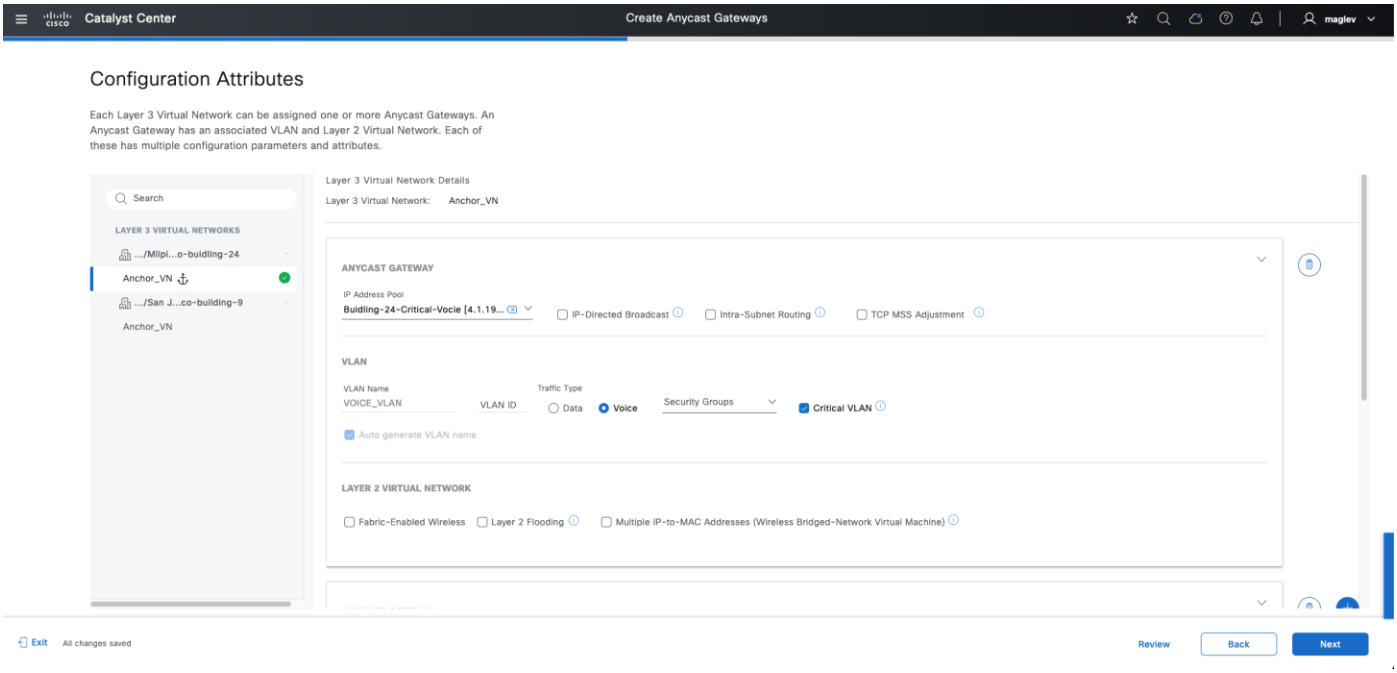



**ステップ 2.** メニューアイコンボタンから、[Provision] > [Virtual Networks] の順に選択し、右上のテーブルビューアイコンをクリックします。

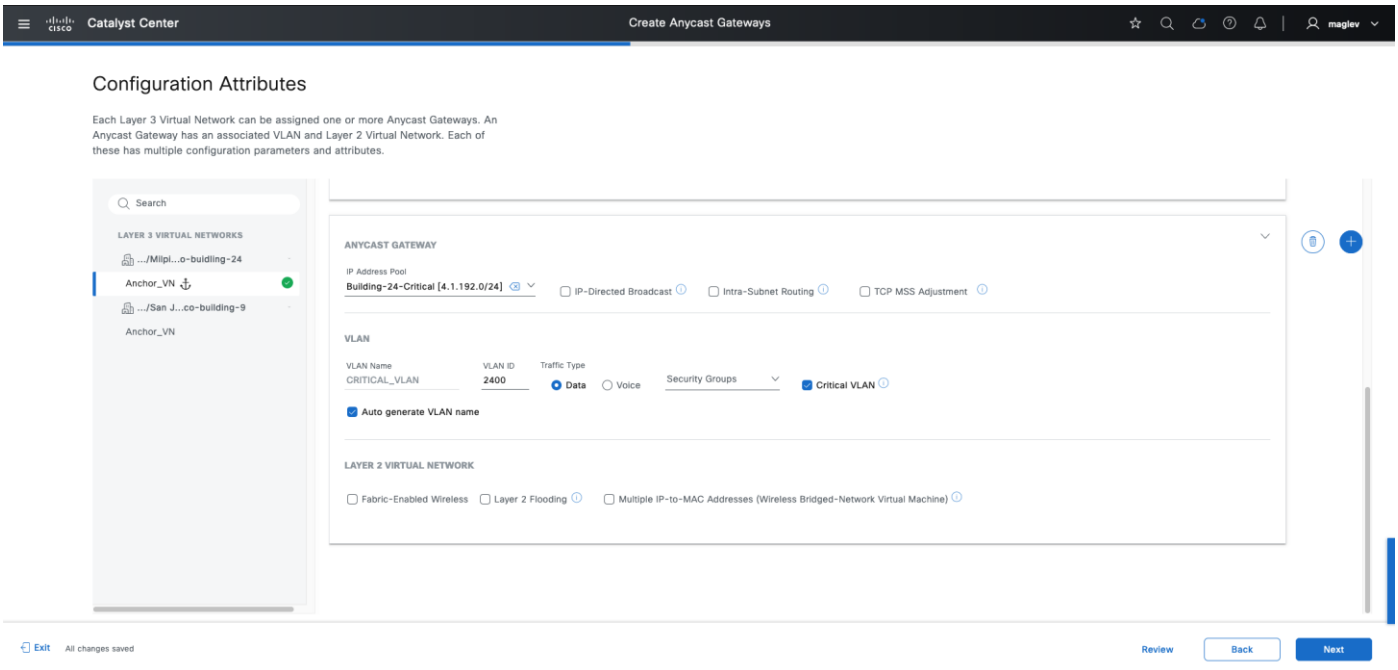
**ステップ 3.** [Anycast Gateways] タブをクリックして、[Create Anycast Gateways] をクリックして [Anchor_VN] を選択します。

**ステップ 4.** [Critical VLAN] チェックボックスをオンにして、2 つのプールを追加します。

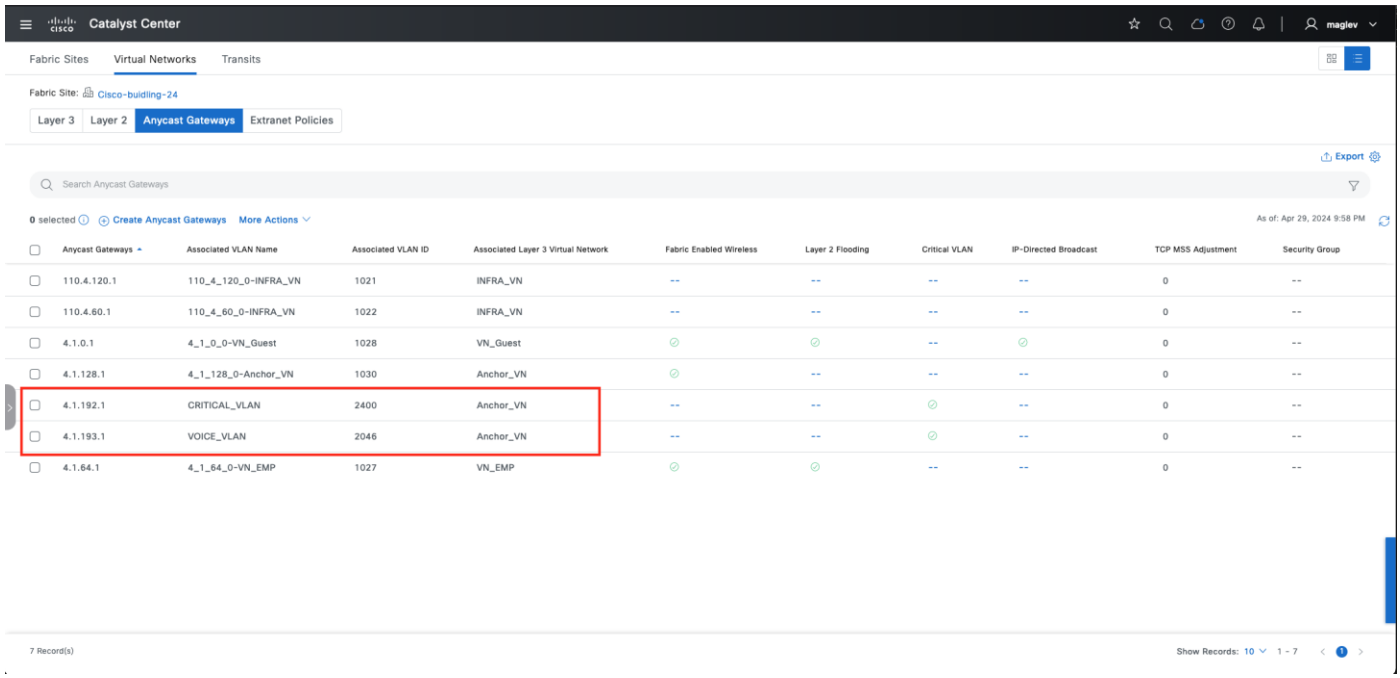
- **クリティカル VLAN**（音声トラフィック用）。**VLAN 名**と **VLAN ID** はカスタマイズできません。




- **クリティカル VLAN**（データトラフィック用）。**VLAN 名**はカスタマイズできません。**VLAN ID** は編集できます。



**ステップ 5.** [Next] をクリックしてワークフローを完了し、タスクを展開します。




## （オプション）C9800 ワイヤレスコントローラのプロビジョニング

このプロセスは、ファブリック対応ワイヤレスコントローラとして C9800 デバイスを追加することに焦点を当てています。

前のセクションで説明したように、スタンドアロンの物理 C9800 ワイヤレスコントローラは、Catalyst Center によるスケール数とアシュアランスサポートの点で優れています。Cisco SD-Access の展開でファブリック対応ワイヤレスコントローラまたは OTT ワイヤレスコントローラとして追加できます。

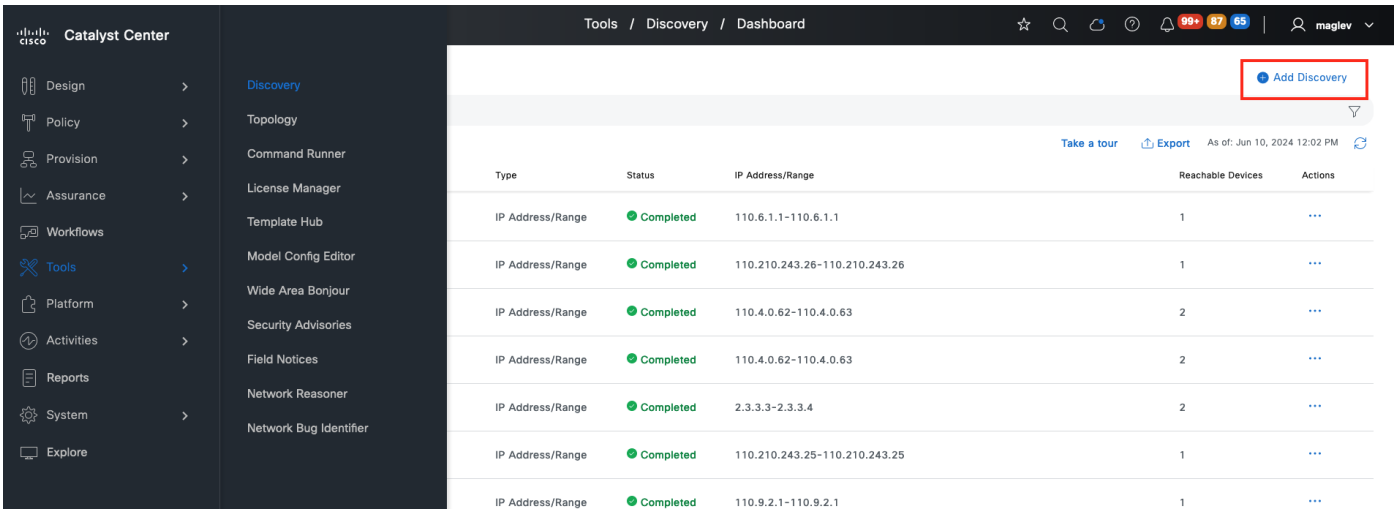
C9800 ワイヤレスコントローラを展開するための一般的なステップは次のとおりです。

1. SSID でワイヤレス ネットワーク プロファイルを作成します（「ワイヤレス SSID の設定」を参照）。
2. C9800 デバイスを検出してプロビジョニングします。
3. C9800 デバイスをファブリック（ファブリック対応ワイヤレスコントローラ）に追加します。

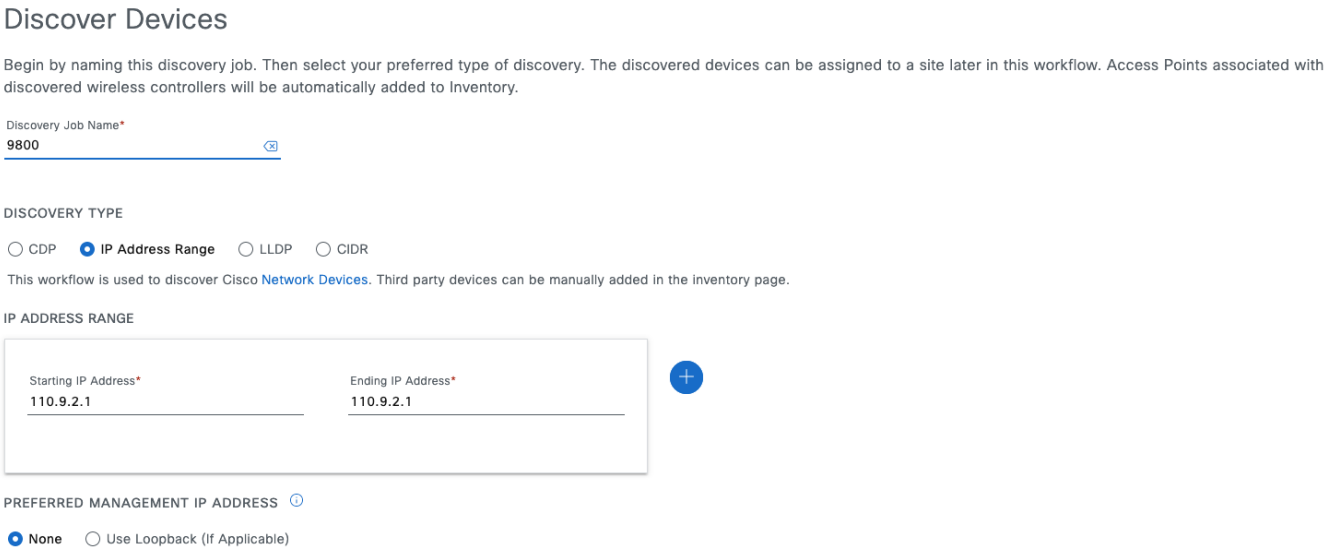
このセクションの手順では、**Floor-1** を管理するために、C9800 ワイヤレスコントローラを **Cisco-Building-9** ファブリックサイトにプロビジョニングする方法について説明します。このファブリックサイトには、**Floor-2** を管理するワイヤレスコントローラがすでにあります。SSID を持つネットワークプロファイルは、すでに追加されています。

## 手順 1。　C9800 デバイスの検出

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Tools] > [Discovery] を選択し、右上の [Add Discovery] をクリックします。

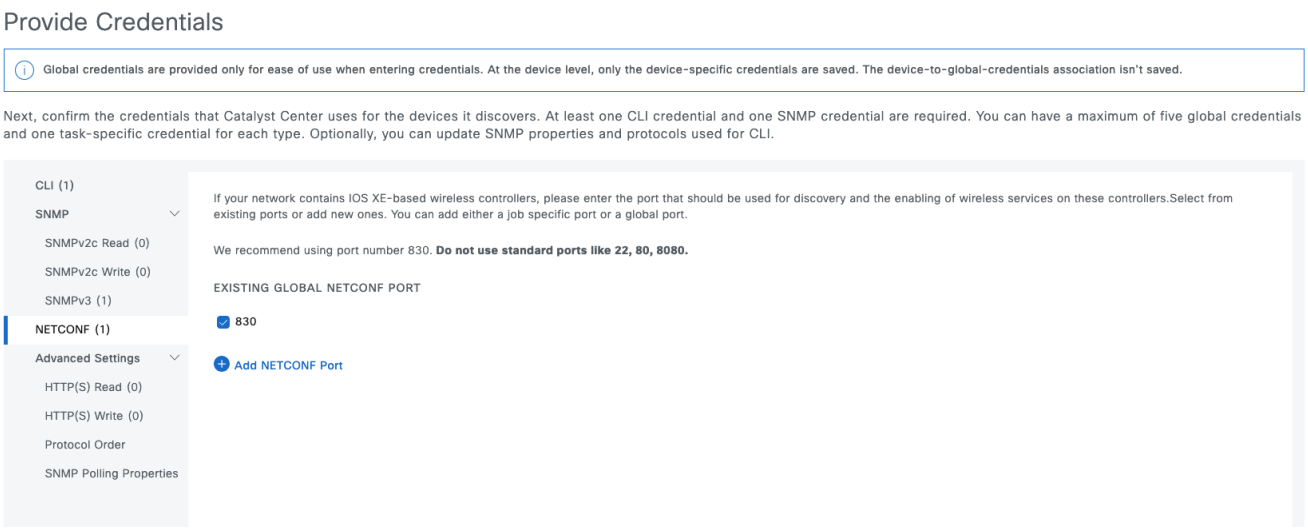



**ステップ 2.** IP 情報を入力します。

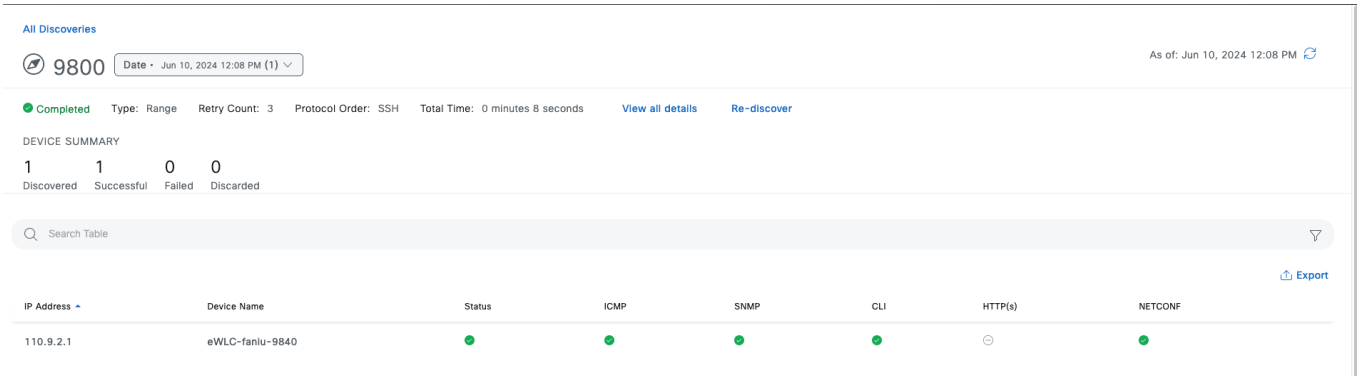



**技術的なヒント：**　ワイヤレス管理 IP は C9800 デバイスで設定する必要があり、DHCP で割り当てられた IP アドレスは使用できません。

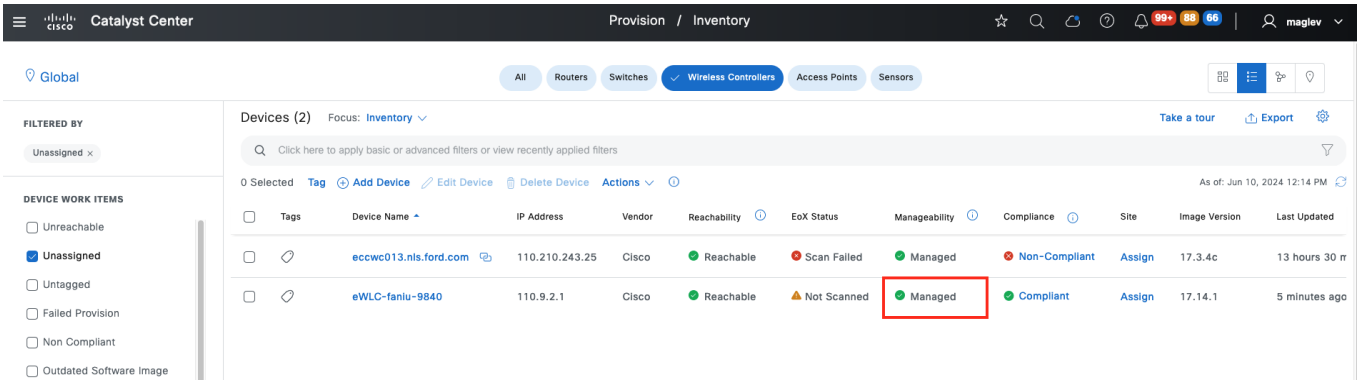
**ステップ 3.** [CLI]、[SNMP]、および [Netconf] に必須の必要な情報を入力し、検出タスクを開始します。




検出が成功すると、[Discovery] ウィンドウが開きます。




**ステップ 4.** [Inventory] ウィンドウで検証します。左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順にクリックし、デバイスが [Managed] ステータスになっていることを確認します。




**技術的なヒント：**

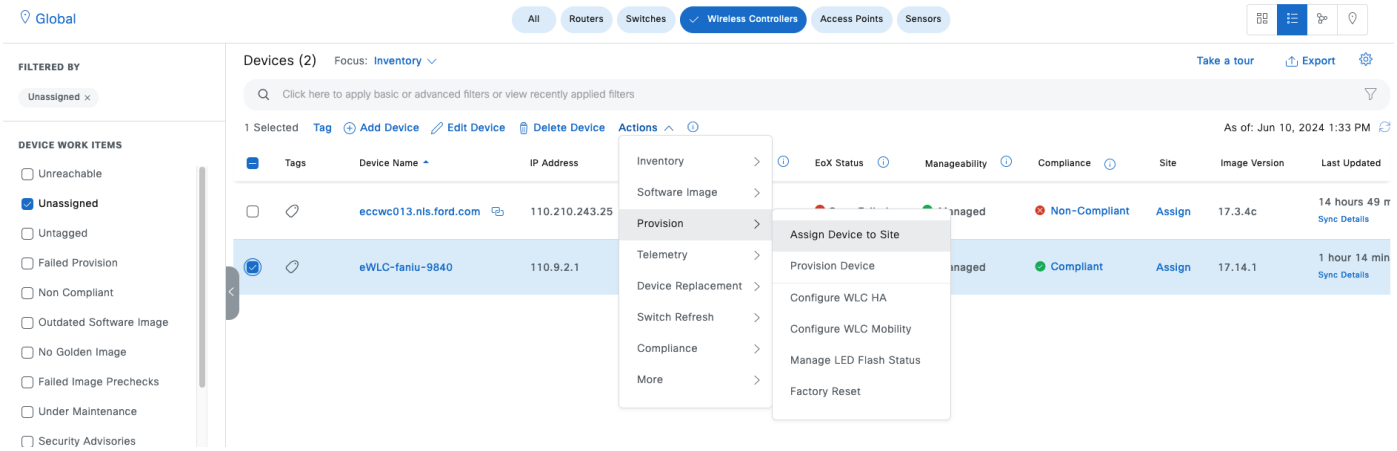
1. フィルタを適用すると、デバイスをより迅速に見つけることができます。上記の例では、上部の [Wireless Controllers] をクリックし、左側のペインで [Device Work Items] > [Unassigned] の順にクリックします。

2. **Unassigned** は、デバイスがまだサイトに割り当てられていないことを意味します。検出されたデバイスは、検出

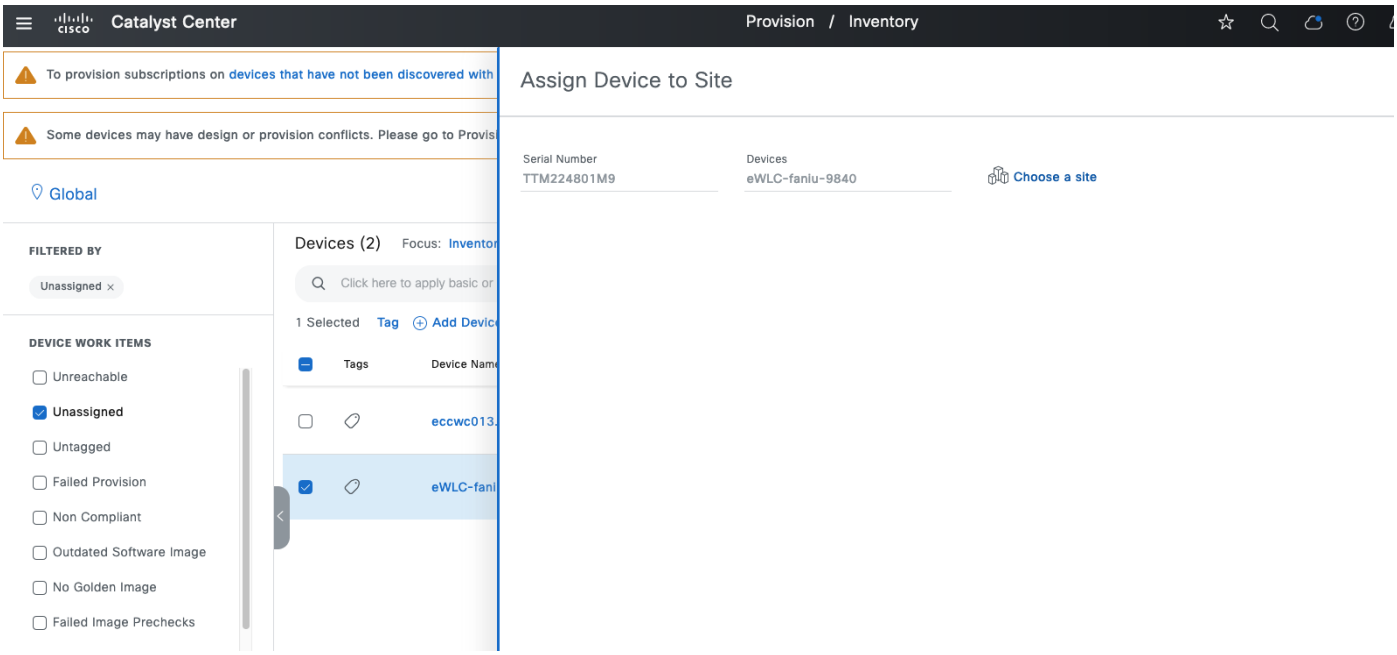
ワークフロー中にすでにサイトに割り当てられています。左上の [Global] をクリックしてサイトに切り替えます。

## 手順 2。 サイトへの C9800 の割り当てとプロビジョニング

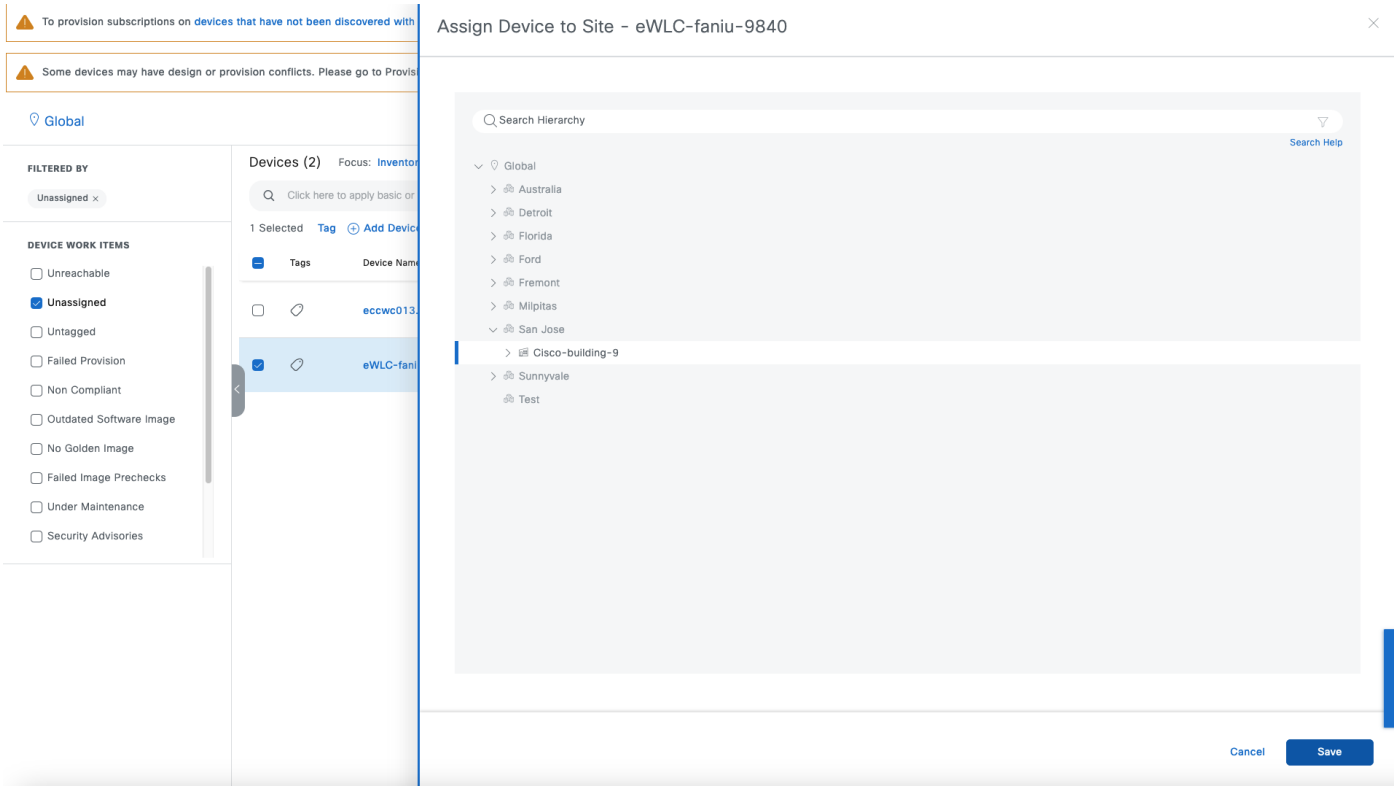
**ステップ 1.** デバイスのチェックボックスをオンにし、[Actions] > [Provision] > [Assign Device to Site] の順に選択します。



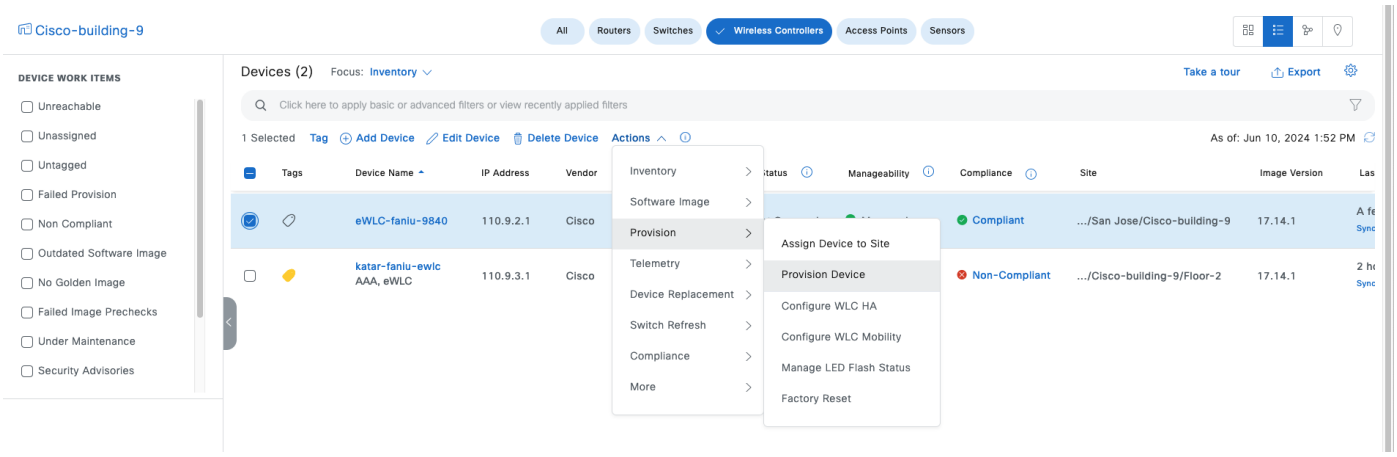

**ステップ 2.** [Choose a site] をクリックします。



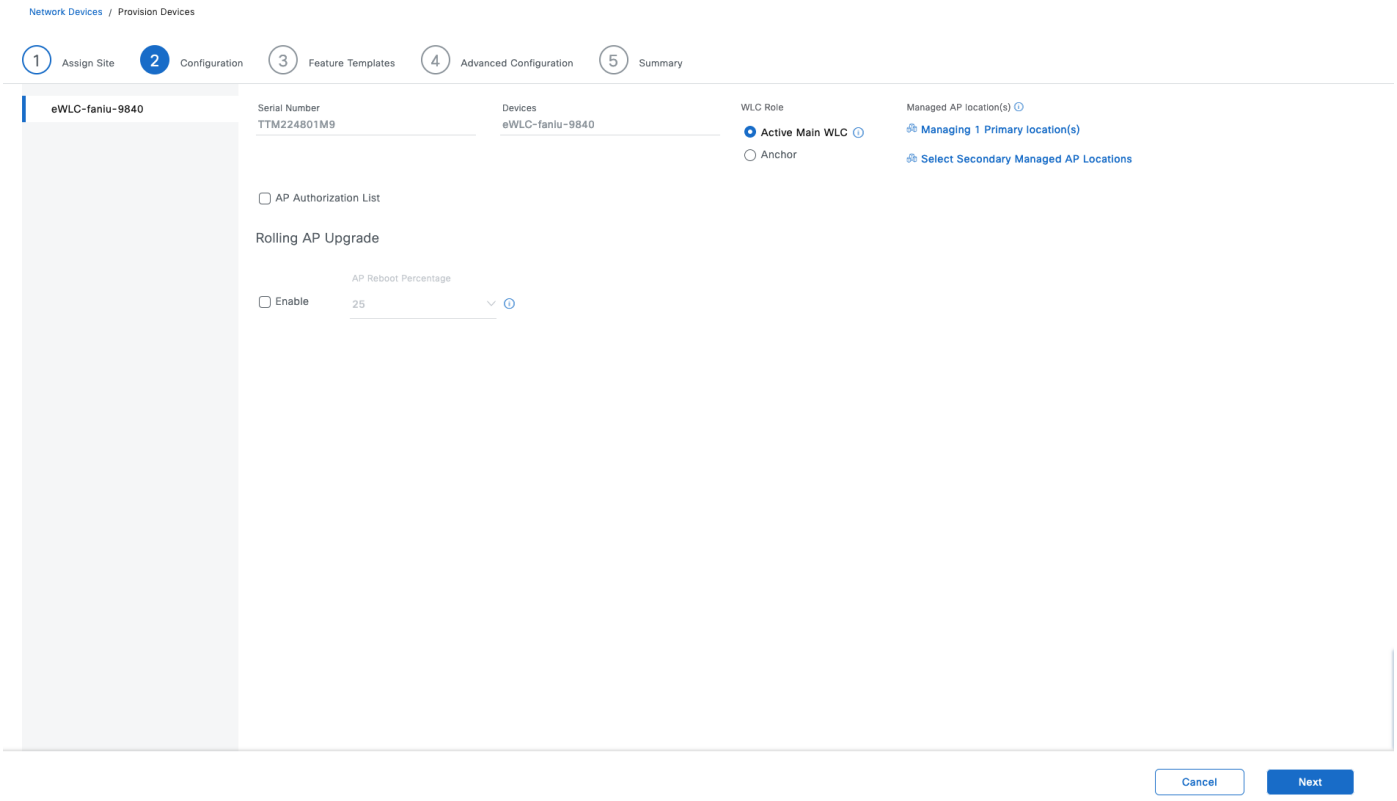
**ステップ 3.** サイト [Cisco-Building-9] を選択し、[Save] をクリックしてワークフローを完了し、タスクを展開します。



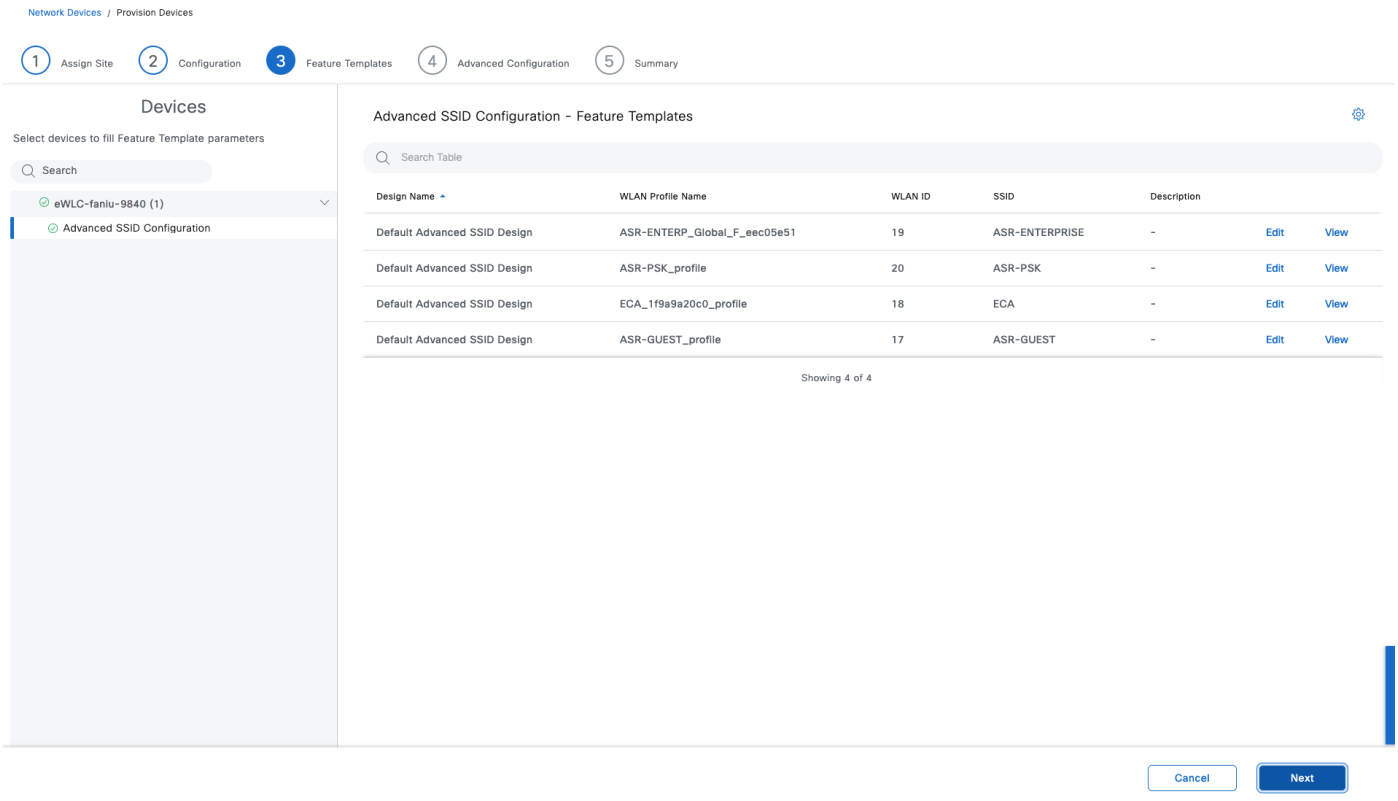

**ステップ 4.** サイトの割り当て後は、前のフィルタは適用されません。場所を [Global] から [Cisco-Building-9] に変更し、[Unassigned] チェックボックスをオフにしてデバイスを確認し、[Actions] > [Provision] > [Provision Device] の順に選択します。



**ステップ 5.** **Floor-1** という名前の AP のプライマリ管理対象場所を選択します。

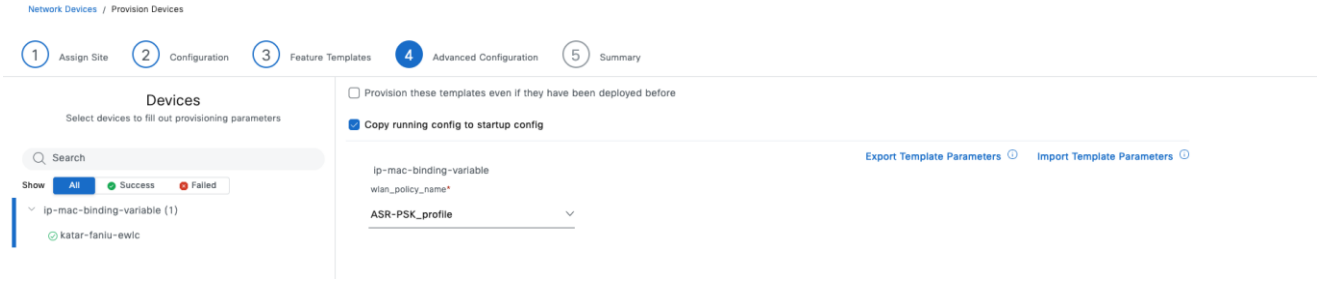



**ステップ 6.** [Advance SSID configurations] を選択して確認します（オプション）。



**ステップ 7.** [Next] をクリックして [Advanced Configuration]（オプション）に移動すると、CLI テンプレートは関連付けられているテンプレートがあるかどうかを表示します。

**図 47.　テンプレートが関連付けられている同じサイトの別のワイヤレスコントローラの例**

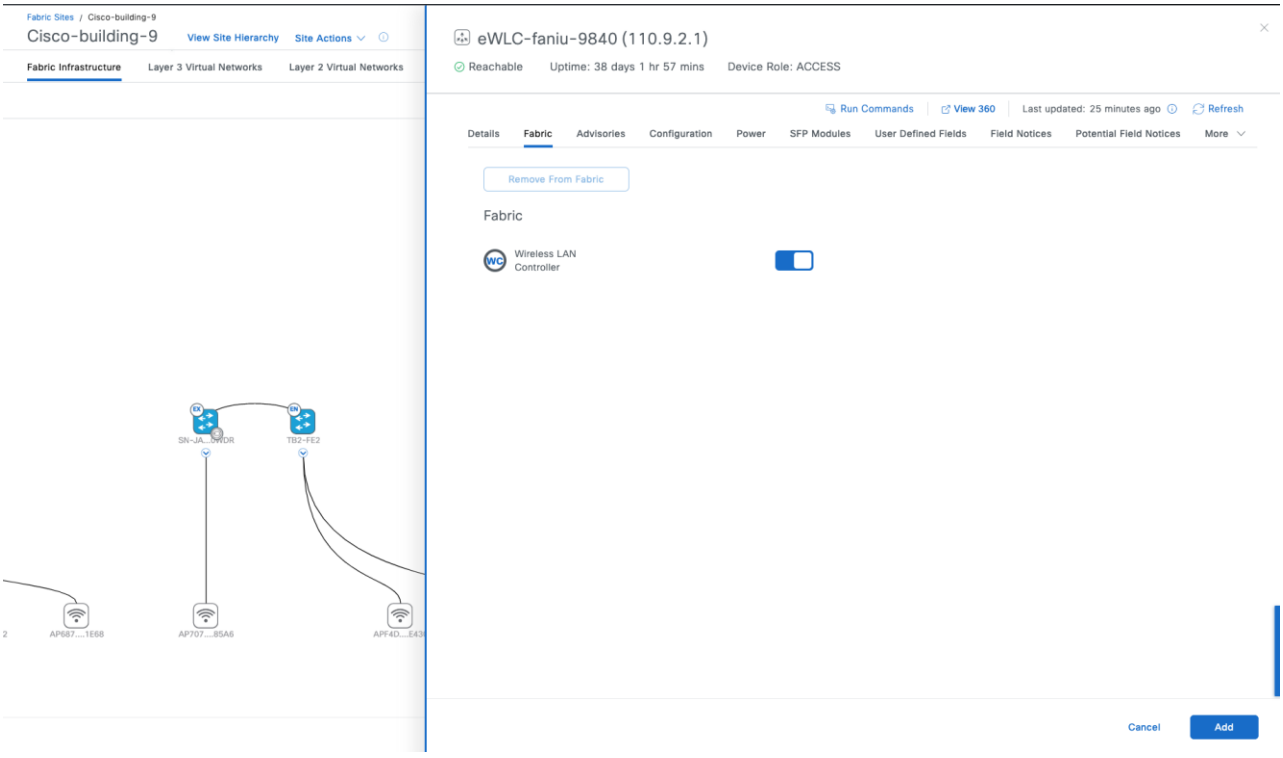



**ステップ 8.** [Next] をクリックし、[Summary] ウィンドウで設定を確認してタスクを展開します。

## 手順 3。　ファブリック対応ワイヤレスコントローラとしてのファブリックサイトへの C9800 デバイスの追加

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Site] の順に選択し、右上のテーブルビューアイコンをクリックして、[Cisco-Building-9] テキストリンクをクリックします。

**ステップ 2.** ワイヤレスコントローラを見つけて、[Wireless LAN Controller] を有効にし、[Add] をクリックしてタスクを展開します。

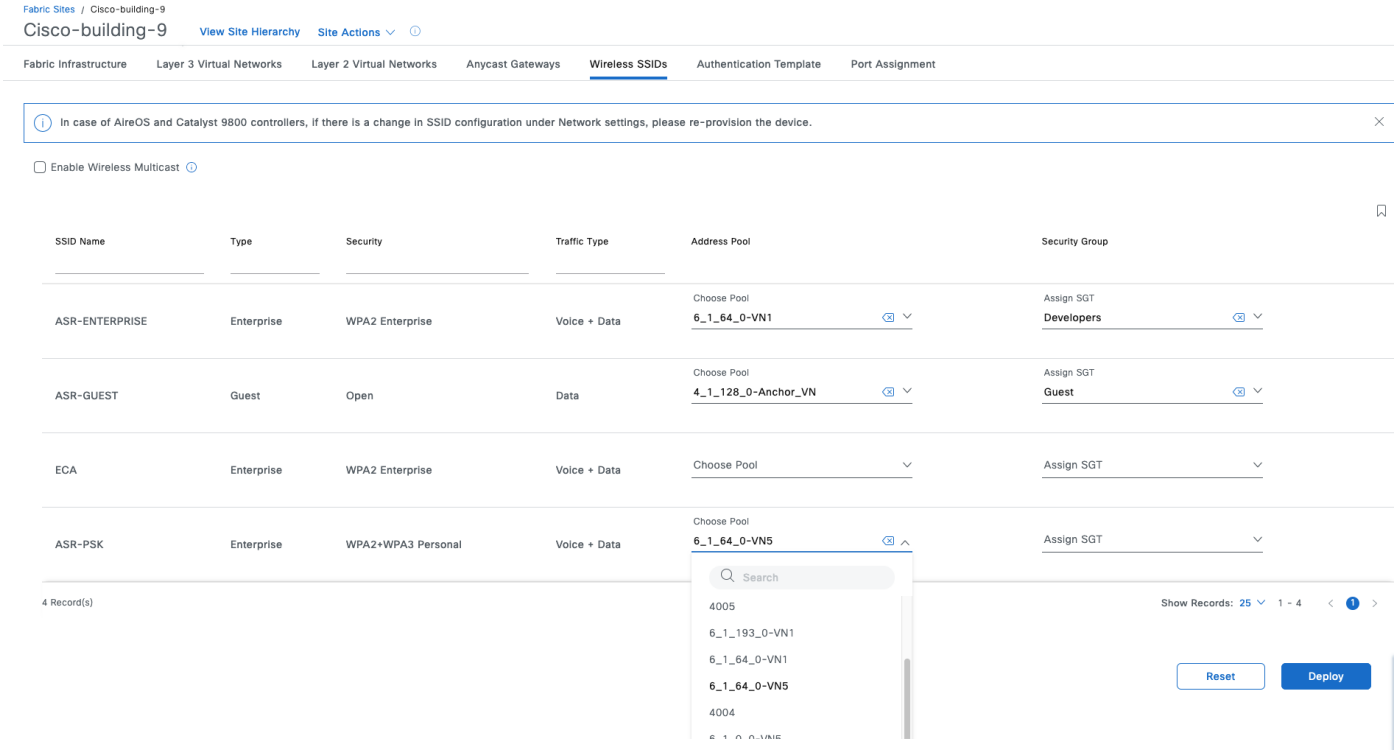



**技術的なヒント：**　ファブリック コントロール プレーン プロトコルに耐障害性を持たせるには、各ファブリック ノードのグローバル ルーティング テーブルにワイヤレスコントローラへの特定のルートが存在する必要があります。ワイヤレスコントローラの IP アドレスへのルートは、ボーダーでアンダーレイ内部ゲートウェイプロトコル（IGP）に再配布されるか、各ノードで静的に設定される必要があります。ワイヤレスコントローラは、Cisco SD-Access 内の RLOC です。LISP RLOC 到達可能性チェックでは、ワイヤレスコントローラへの特定のルートがアン

ダーレイで必要です。ワイヤレスコントローラは、デフォルトルート経由では到達できません。

## 手順 4。 ファブリックワイヤレス SSID の設定

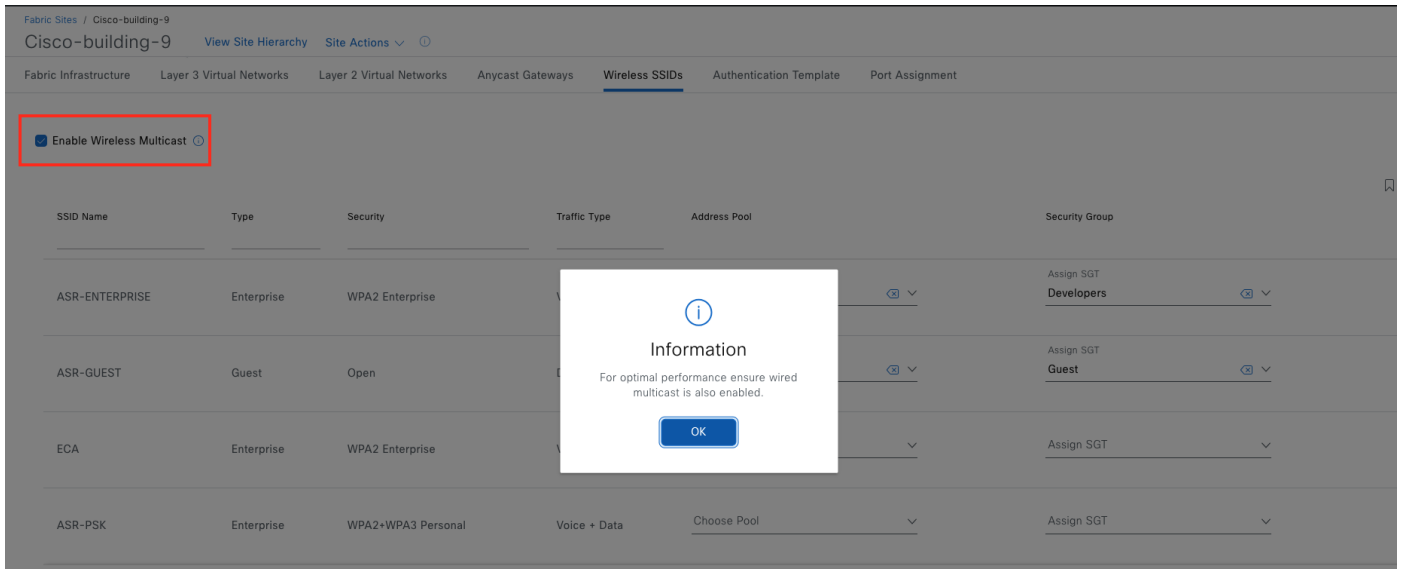
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Site] の順に選択し、右上のテーブルビューアイコンをクリックして、[Cisco-Building-9] テキストリンクをクリックし、[Wireless SSID] タブをクリックして、IP **アドレスプール**を次の図に示すように関連付けます。




**注：** ファブリック SSID は、レイヤ 3 IP プールまたはレイヤ 2 セグメントが関連付けられた後に起動します。

**ステップ 2.** [Enable Wireless Multicast] チェックボックスをオンにして、ワイヤレスコントローラでグローバル マルチキャスト モードおよび Internet Group Management Protocol（IGMP）スヌーピングを有効にします（サイトレベルのオーバーレイマルチキャスト設定が必要です）。

**ステップ 3.** [Enable Wireless Multicast] チェックボックスをオンにします。



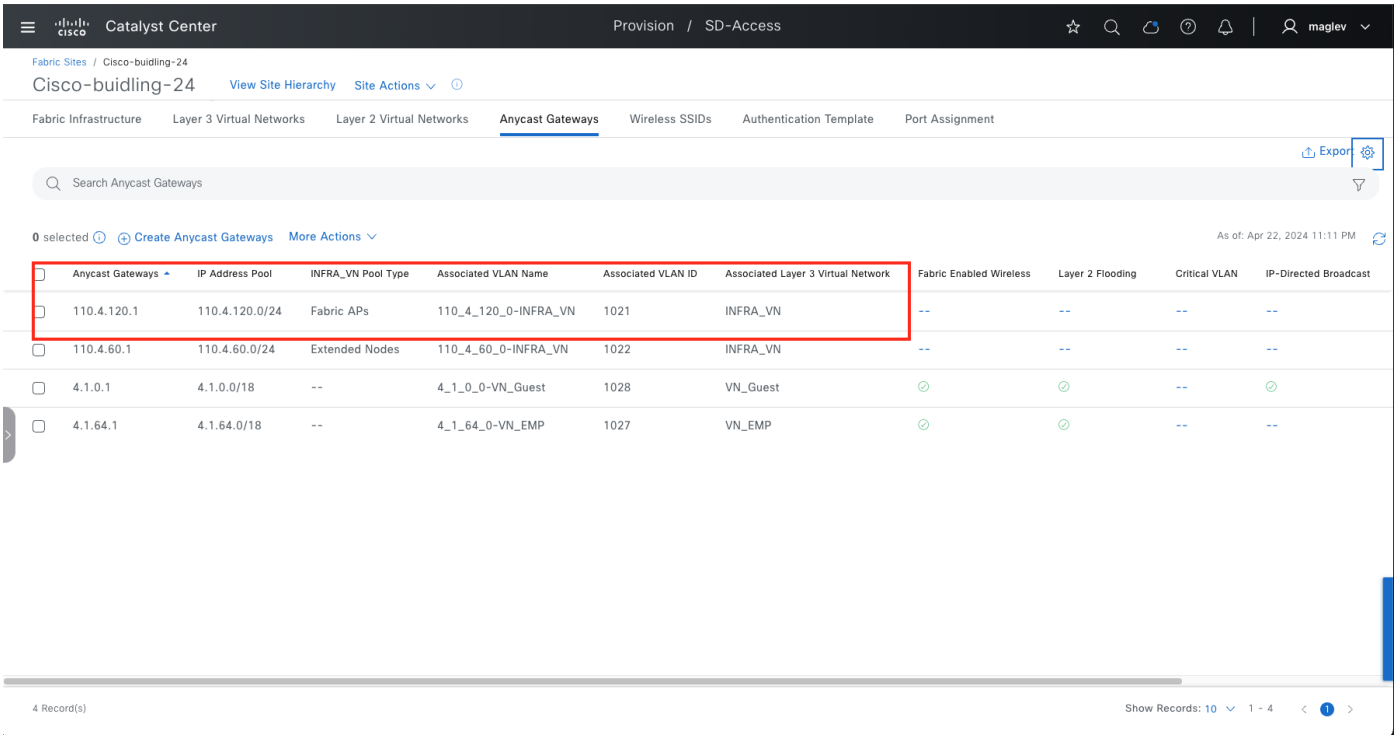
## Cisco SD-Access ネットワークの運用

このセクションでは、エンドポイントのオンボーディング、ファブリックサイトの変更、障害が発生したファブリックデバイスの交換、および Catalyst Center を使用した破棄に対する Day-*N* 運用の手順について説明します。

### AP のオンボード

AP は、ファブリックの特殊なケースです。これらはファブリック インフラストラクチャの一部ですが、エンドポイントのようにエッジノードに接続されます。このため、トラフィックパターンは一意です。AP は、オーバーレイネットワークを使用して DHCP アドレスを受信し、アンダーレイネットワークを使用してワイヤレスコントローラに関連付けます。ワイヤレスコントローラに関連付けられると、オーバーレイネットワークを介してワイヤレスコントローラによって Catalyst Center に登録されます。このトラフィックフローに対応するために、グローバル ルーティング テーブル（GRT）にある AP サブネットがオーバーレイネットワークに関連付けられます。

「手順 1：INFRA_VN でのエニーキャストゲートウェイの追加」では、AP のエニーキャストゲートウェイが設定されています。




**注：** Catalyst Center と AP の間、ワイヤレスコントローラと AP の間の到達可能性を確認します。

**手順 1。** AP ポートの割り当て

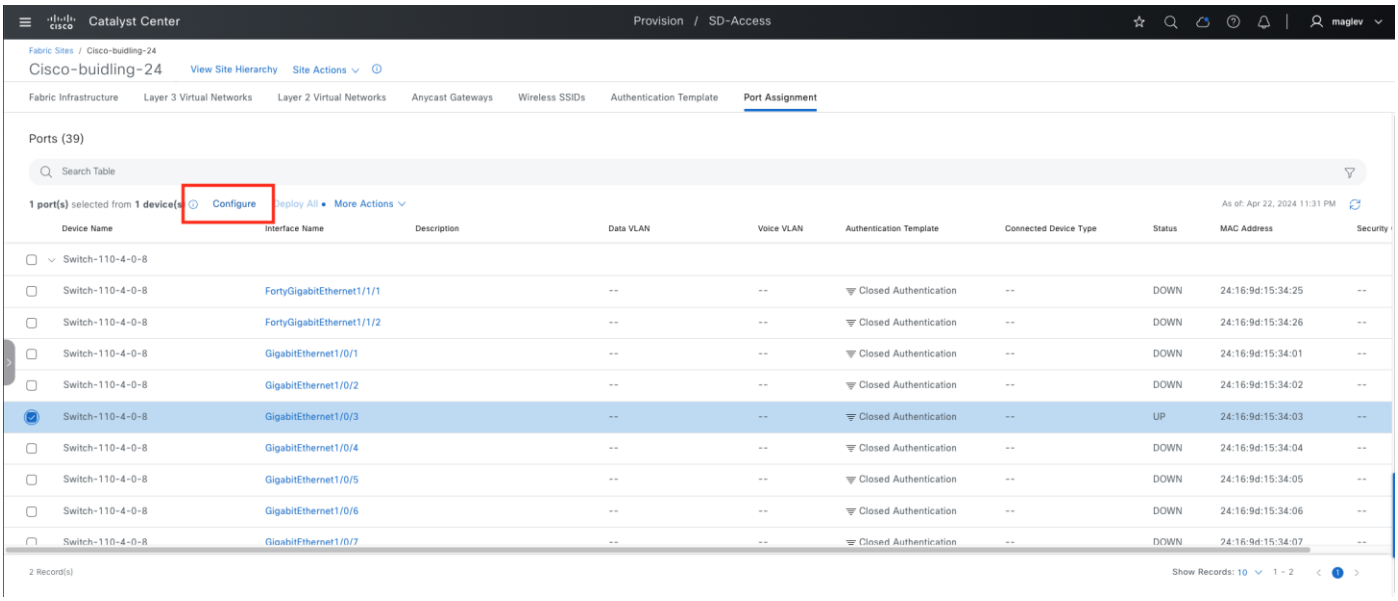
この手順では、AP を **Cisco-building-24** にオンボーディングし、組み込みワイヤレスコントローラ N+1 ピア **Common-A** および **Common-B** に参加します。

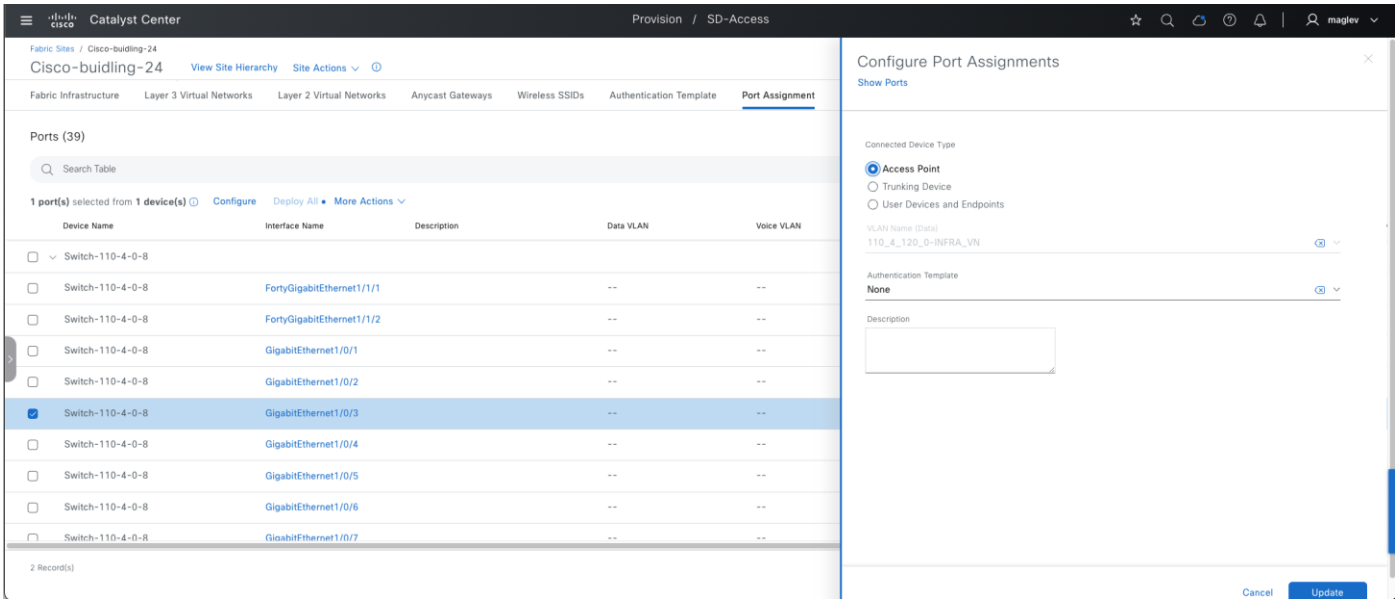
Catalyst Center により、AP の自動オンボーディングが可能になります。認証テンプレートが [No Authentication] に設定されている場合、Autoconf はデバイスを Cisco AP として識別するために使用され、接続されたエッジポー

トは正しく設定されます。別の認証テンプレート（**クローズド認証**など）がグローバルに使用されている場合は、セキュアな AP オンボーディングが必要でない限り、エッジノードのスイッチポート設定を変更する必要があります。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Site] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Port Assignment] タブをクリックします。

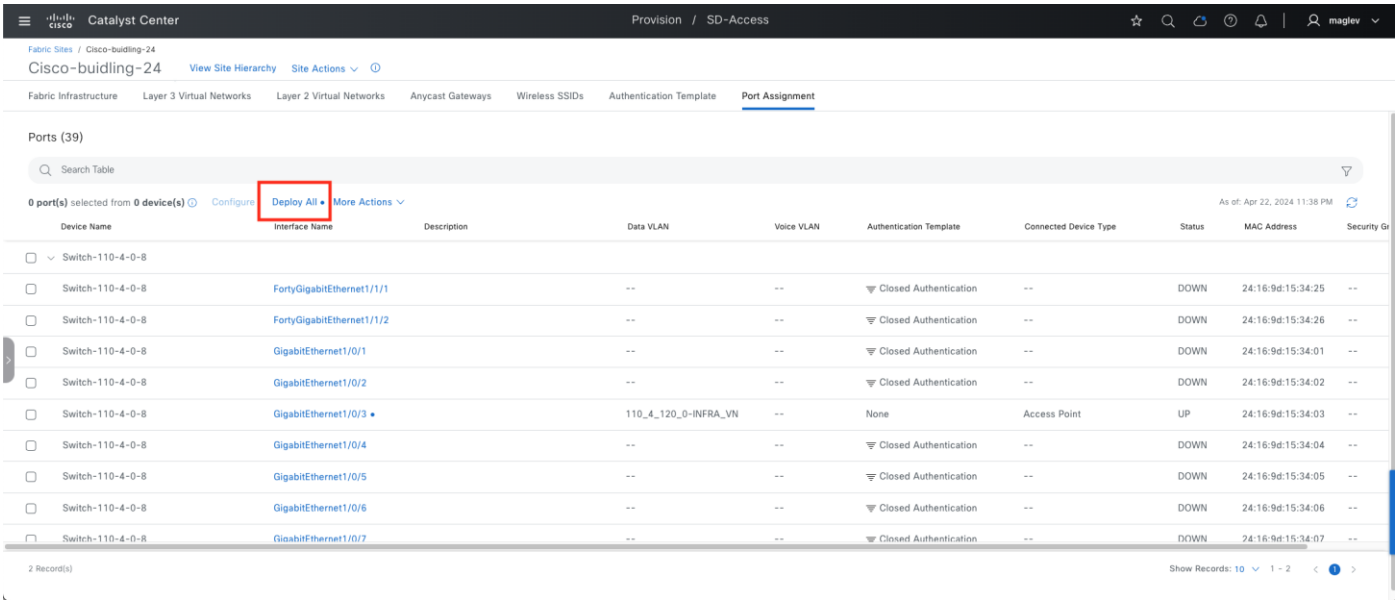
**ステップ 2.** ファブリックエッジ **Switch-110-4-8** と**インターフェイス名**のポート [GigabitEthernet1/0/3] のチェックボックスを見つけてオンにします。スライドインペインで [Access Point] と [Authentication Template] のタイプ [None] を選択し、[Update] をクリックします。



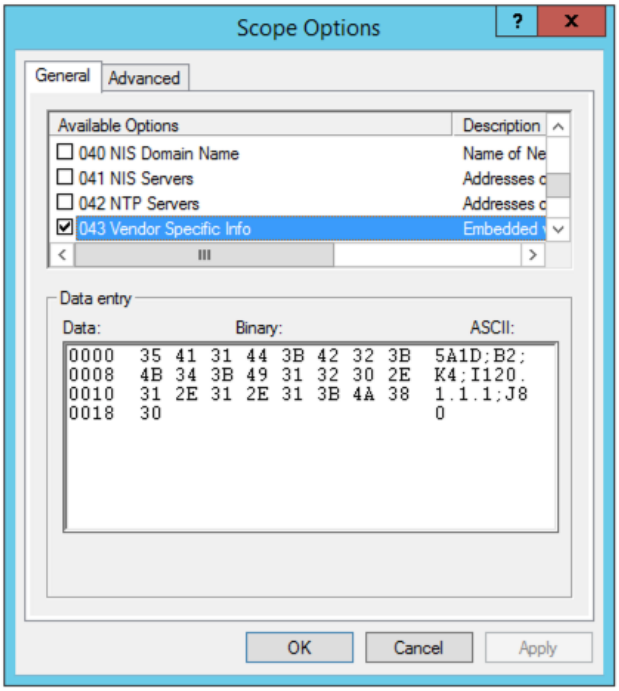

**ステップ 3.** （オプション）さらにポートを設定します。

**ステップ 4.** [Deploy All] をクリックし、ポートに設定をプッシュします。

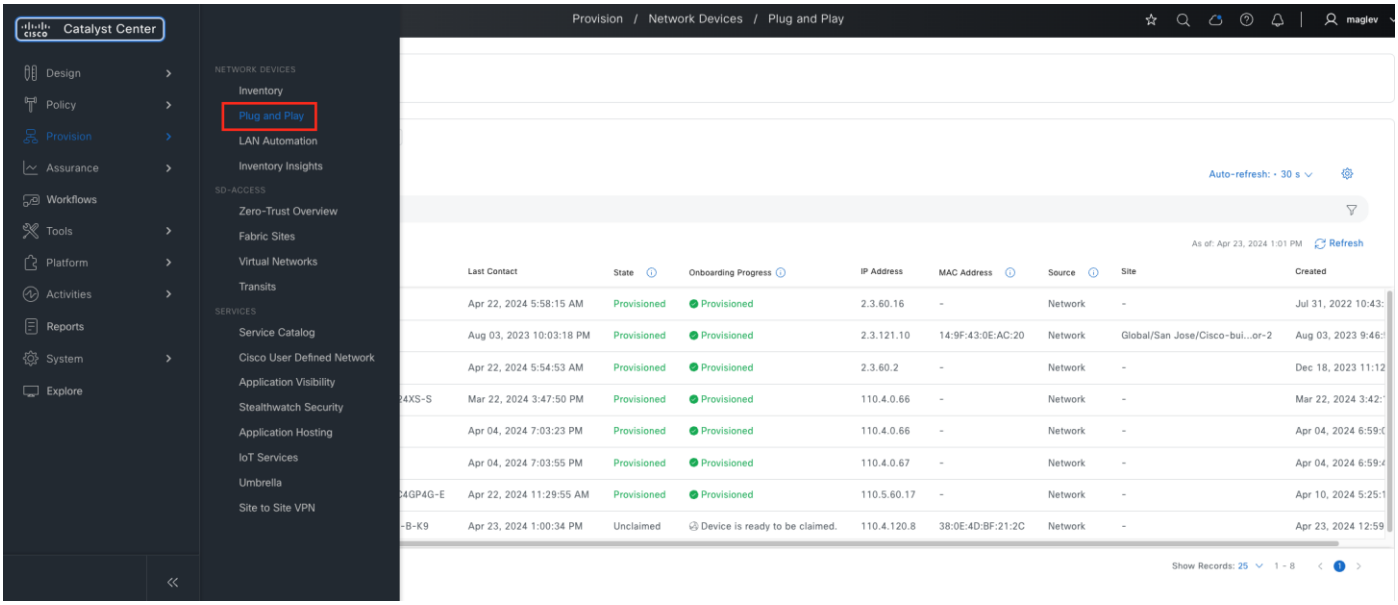



## 手順 2。 Catalyst Center PnP プロセスによる AP

**ステップ 1.** Catalyst Center IP ファブリック インターフェイス IP を指す DHCP サーバーで AP DHCP スコープのオプション 43 を ACSII 値 **5A1D; B2;K4;I120.1.1.1;J80** で設定します。120.1.1.1 は、例で示すように Catalyst Center の IP アドレスです。

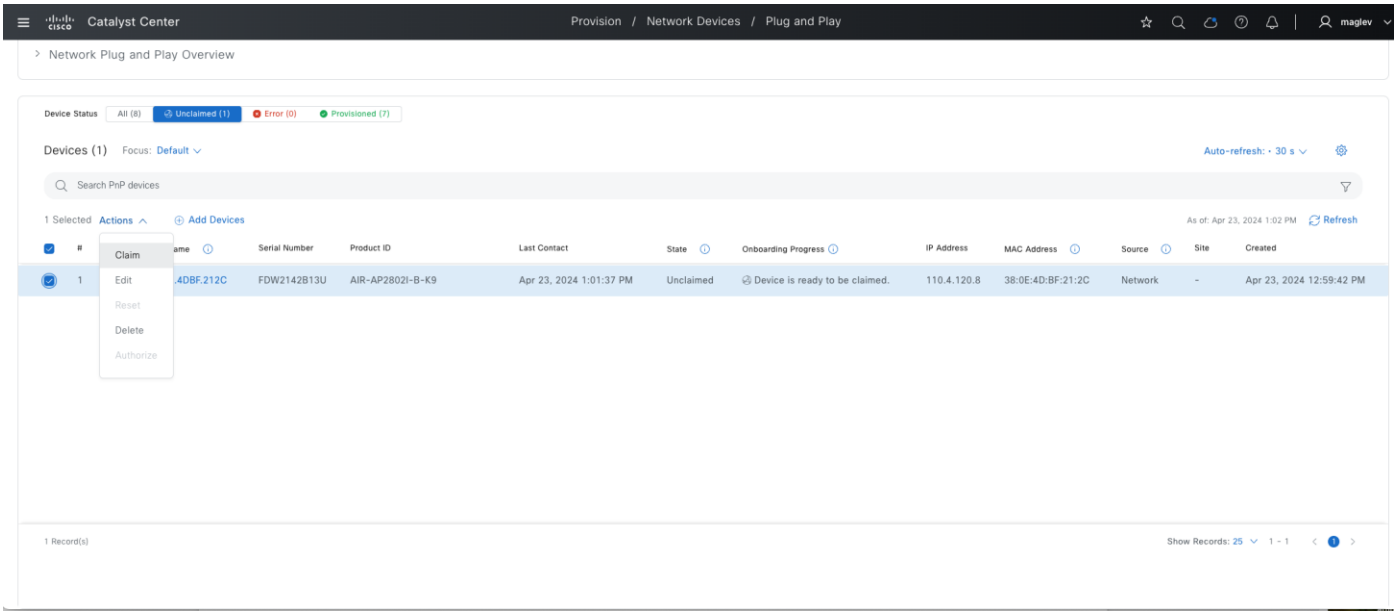


**ステップ 2.** AP デバイスを GI1/0/3 に接続します。メニューアイコンボタンから、[Provision] > [Plug and Play] の順に選択します。




**ステップ 3.** [Unclaimed] ステータスカテゴリから新しい AP を見つけます。

**ステップ 4.** 新しい AP のチェックボックスをオンにし、[Actions] > [Claim] の順に選択します。

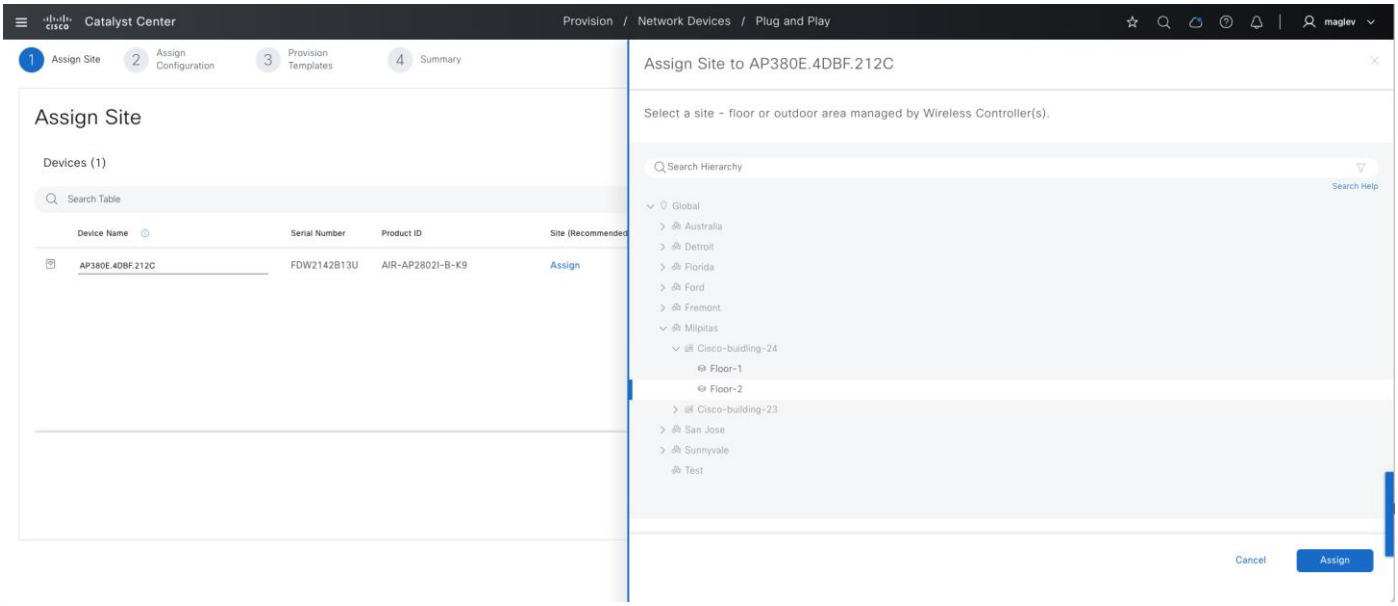


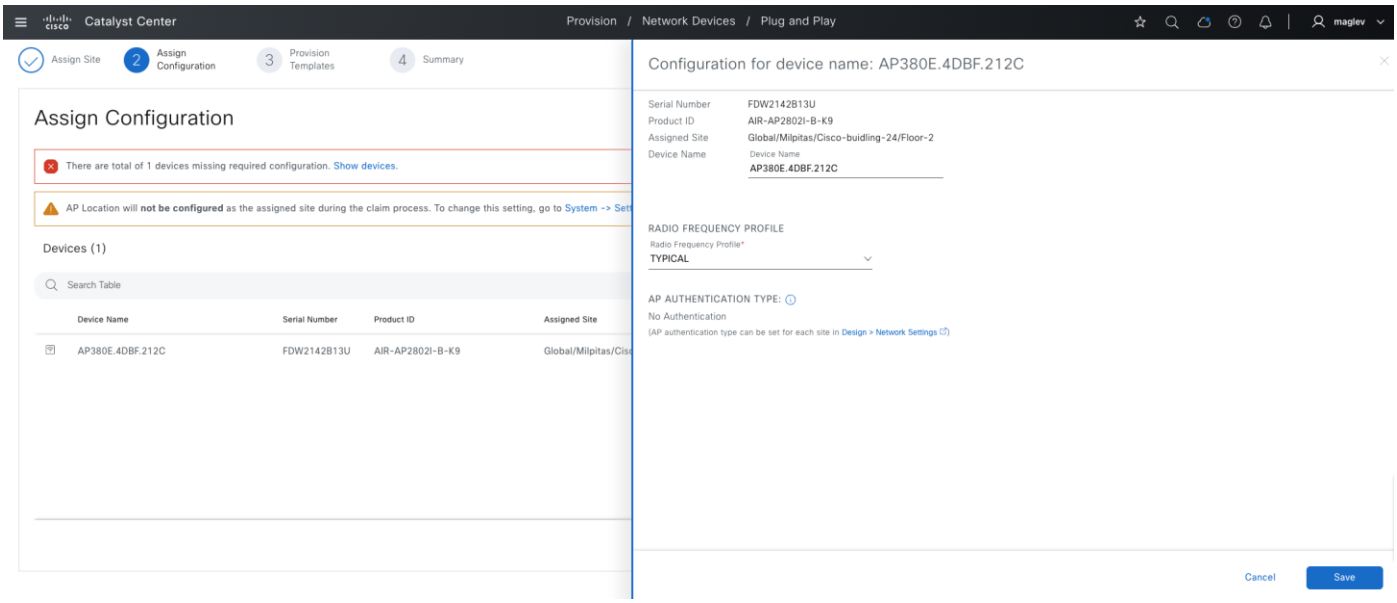
**ステップ 5.** **Claim** ワークフローでは、次の設定を使用します。

[Assign Site]：[Cisco-building-24] と [Floor-2] を選択します

[Assign Configuration] > [Radio Frequency Profile]：[Typical] を選択します

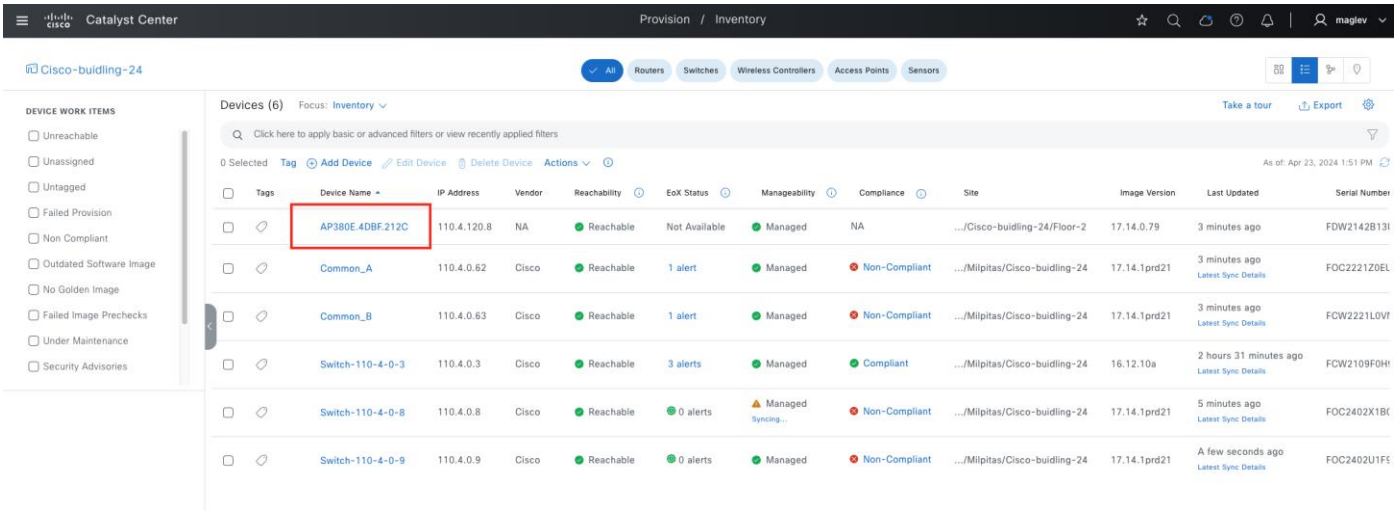
[Provision Templates]：オプション




**ステップ 6.** [Save] をクリックし、[Claim] プロセスを完了します。

**ステップ 7.** 左上隅にあるメニューアイコンをクリックし、[Provision] > [Inventory] の順に選択して確認します。




**ステップ 8.** 組み込みワイヤレスコントローラで `show ap summary` コマンドを使用して **Common-B** を確認します。

```
Common_B#show ap summ
Number of APs: 1

CC = Country Code
RD = Regulatory Domain

AP Name                  Slots AP Model          Ethernet MAC   Radio MAC      CC   RD   IP Address                                  State       Location
-------------------------------------------------------------------------------------------------------------------------------------------------------
AP380E.4DBF.212C         2     AIR-AP2802I-B-K9  380e.4dbf.212c 005d.7315.d300 US   -B   110.4.120.8                                 Registered  default location
```

## 手順 3。 OTT 展開での AP のオンボード

Catalyst Center による AP オンボーディングは CUWN OTT 展開でサポートされており、これはファブリック AP オンボーディングと同じです。これには、AP プール、接続されたファブリックエッジでのポート割り当て（サイトレベルの認証がない場合は Autoconf）、および PnP プロセスが必要です。ただし、FlexConnect OTT では、ポート割り当てを手動で設定する必要があります。

AP に接続するファブリックエッジポートは、FlexConnect VLAN トラフィックを許可するようにネイティブ VLAN を定義してトランクポートとして設定する必要があります。

設定を展開するには、Catalyst Center CLI テンプレートを使用することをお勧めします。この設計および導入ガイドでは、テンプレートについては取り上げていません。「Cisco Catalyst Center User Guide」の「Create Templates to Automate Device configuration Changes」セクションを参照してください。

テンプレートの設定例：

- `ap_interface`：AP に接続されたインターフェイス
- `native_VLAN`：ワイヤレスコントローラへの AP 接続に使用される VLAN
- `allowed VLAN range`：ローカル Flex 接続に使用される VLAN

```
interface $ap_interface
no switchport mode access
no marco auto processing
switchport mode trunk
switchport trunk native vlan $native_vlan
switchport trunk allowed vlan $allowed_vlan_range
```

## 拡張ノードとポリシー拡張ノードのオンボード

AP と同様に、拡張ノードはファブリックエッジまたは別の拡張ノードに接続されます。拡張ノードの IP プールは、INFRA_VN に必要です。

拡張ノードは、次のノードです。

- 拡張ノード
- ポリシー拡張ノード
- サプリカントベースの拡張ノード（SBEN）

ポリシー拡張ノードは、VN 内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードデバイスには、Cisco IOS XE リリース 17.1.1s 以降を実行している Cisco Catalyst Industrial Ethernet（IE）3400、IE 3400H、IE9300 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチがあります。シスコ デジタル ビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチは、ポリシー拡張ノードとして設定することはできません。

Catalyst Center は、拡張ノードまたはポリシー拡張ノードとそのアップストリームデバイスのポートチャネルを自動的に設定します。SBEN とそのアップストリームデバイスは、単一の物理リンクを使用して設定されます。

SBEN は、IEEE 802.1x（Dot1x）サプリカント設定を受け取り、完全な認証と承認の後にのみ Cisco SD-Access ネットワークにオンボードされるポリシー拡張ノードデバイスです。サプリカントベースの拡張ノードデバイスをオンボードするには、ファブリックエッジのオーセンティケータポートをクローズド認証テンプレートで設定する必要があります。

SBEN オンボーディングをサポートするプラットフォームは次のとおりです。

**ファブリックエッジまたは FiaB**

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9300、C9400、C9500、および C9500H スイッチ。

**SBEN**

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9200、C9300、C9400、C9500、および C9500H スイッチ。

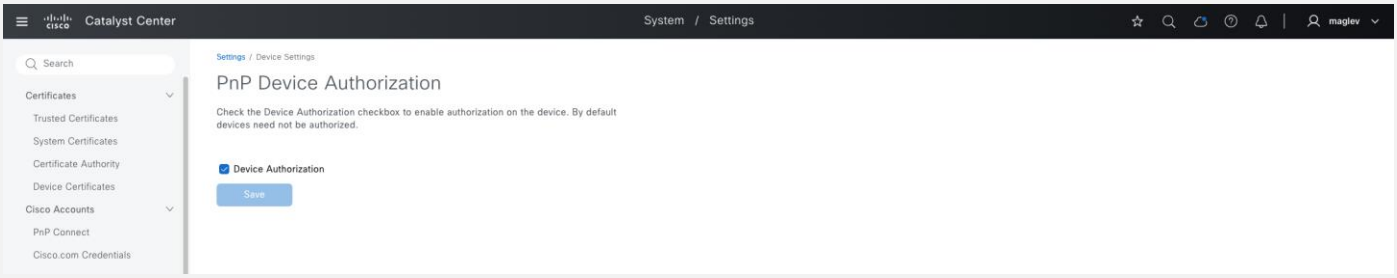
デバイスは、拡張ノードネイバーのライセンスとデバイス自体のライセンスに従ってオンボードされます。

- ネイバーが Essentials ライセンスで動作している場合、デバイスのライセンスに関係なく、そのデバイスは標準の拡張ノードとしてオンボードされます。
- ネイバーが Advantage ライセンスで動作していて、デバイスに Essentials ライセンスがある場合、そのデバイスは標準の拡張ノードとしてオンボードされます。
- ネイバーが Advantage ライセンスで動作していて、デバイスに Advantage ライセンスがある場合、そのデバイスはポリシー拡張ノードとしてオンボードされます。
- デバイスに複数のネイバーがあり、各ネイバーのライセンスレベルが異なる場合、デバイスのライセンスに関係なく、そのデバイスは標準の拡張ノードとしてオンボードされます。

このセクションの手順は、ファブリックサイト **Cisco-building-24** でのポリシー拡張ノードと SBEN のオンボーディングを説明しています。

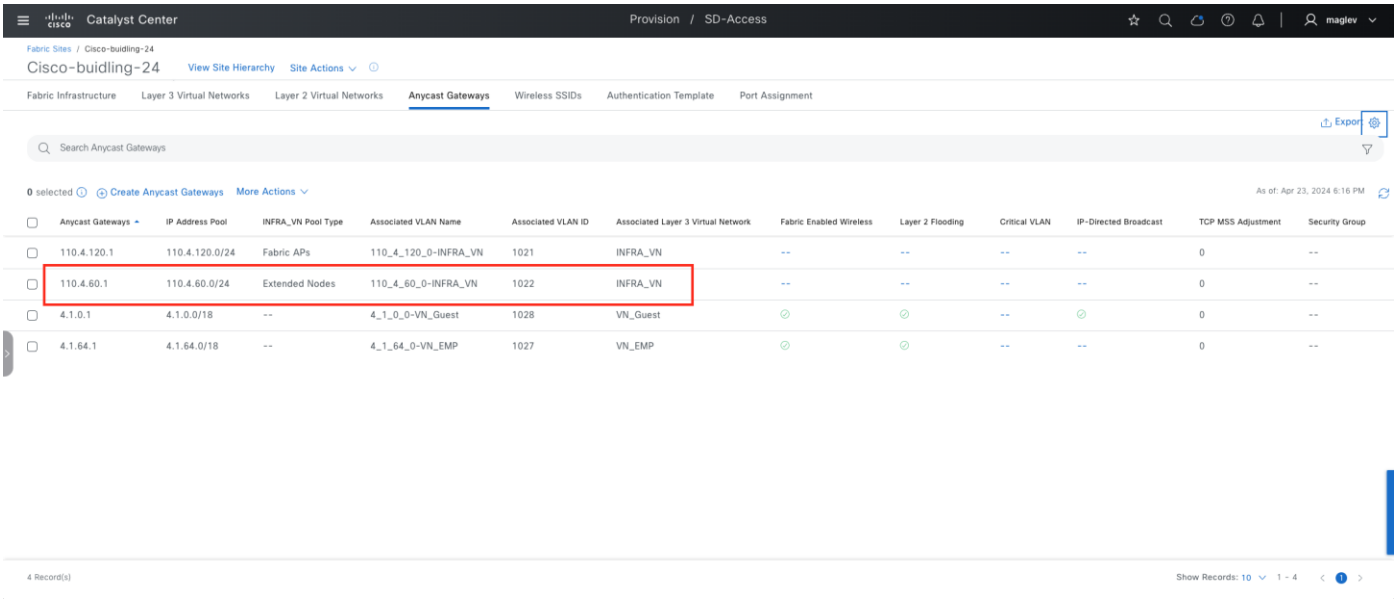
**注：　PnP デバイス認証**により、Catalyst Center でデバイス認証が有効になります。有効にすると、拡張ノードのオンボーディングプロセス、または LAN 自動化ワークフローの PnP デバイスが [Plug and Play] ウィンドウで承認される必要があります。

左上隅にあるメニューアイコンをクリックして [System] > [Settings] を選択し、左側のペインで [PnP Device Authorization] をクリックして、この機能を有効または無効にします。




## 手順 1。　拡張ノードプールの設定

拡張ノードプールは、「手順 1：INFRA_VN でのエニーキャストゲートウェイの追加」で設定されています。

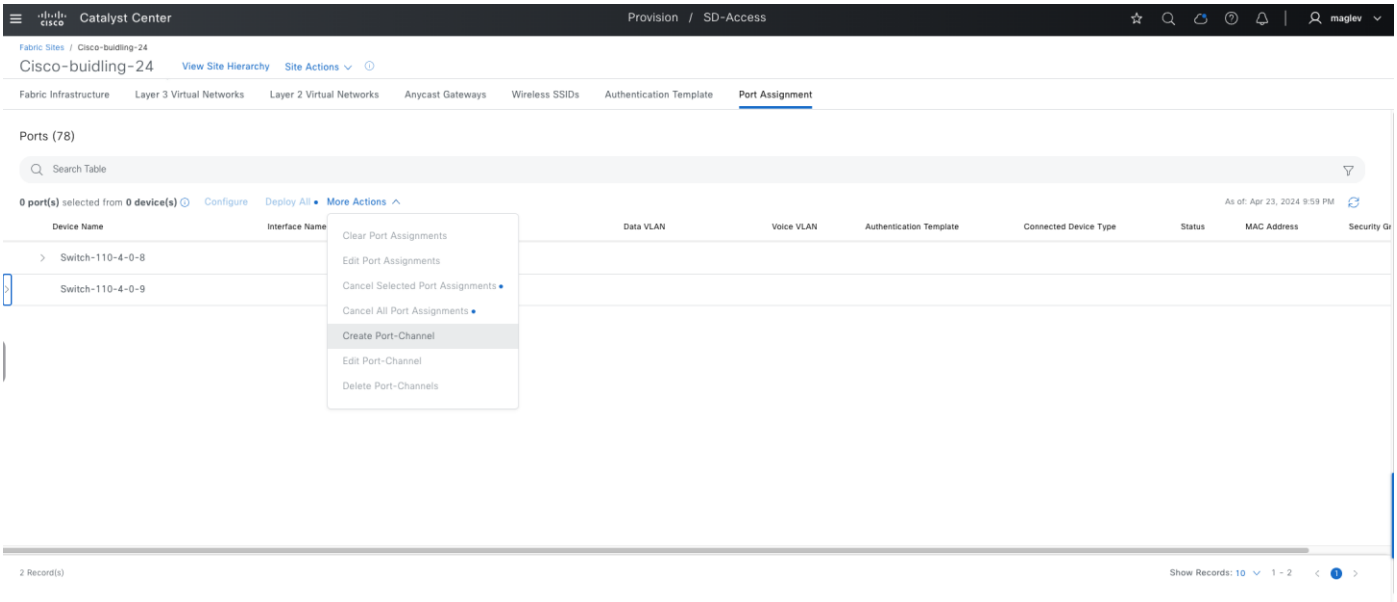



## 手順 2。 ポリシー拡張ノードのオンボード

**Cisco-buidling-24** は、サイトレベルの**クローズ認証**テンプレートを使用します。拡張ノードまたはポリシー拡張ノードをオンボードするには、オンボードする前にポートチャネルを手動で設定します。サイトレベルの認証テンプレートが [No Authentication] に設定されている場合、Catalyst Center はポートチャネルを自動的に設定します。

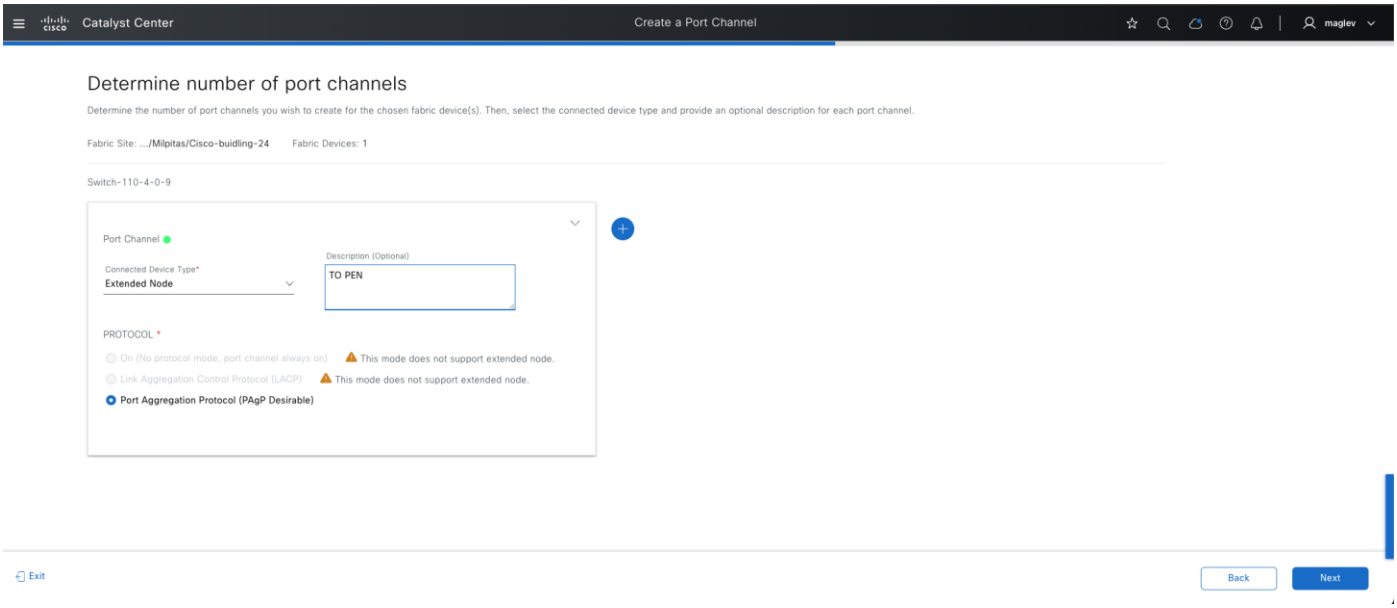
この手順例では、PnP デバイス承認が無効になっています。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fiber Sites] の順に選択し、右上のテーブルビューアイコンをクリックし、[Port Assignment] タブをクリックして [More Actions] > [Create Port-Channel] を選択します。

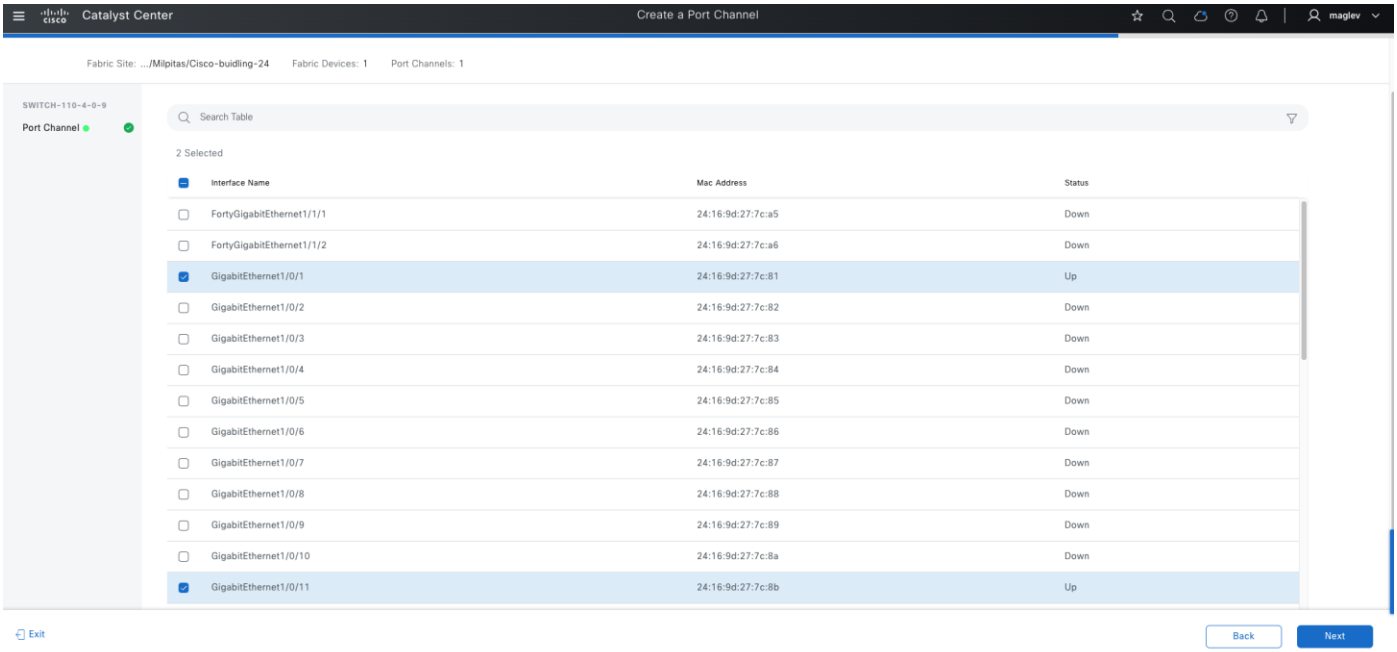



**ステップ 2.** この例のファブリックエッジとして [Switch-110-4-0-9] を選択します。

**ステップ 3.** [Create a Port Channel] ウィンドウで、[Connected Device Type] > [Extended Node] を選択し、[Protocol] > [Port Aggregation Protocol] を選択して、[Next] をクリックします。



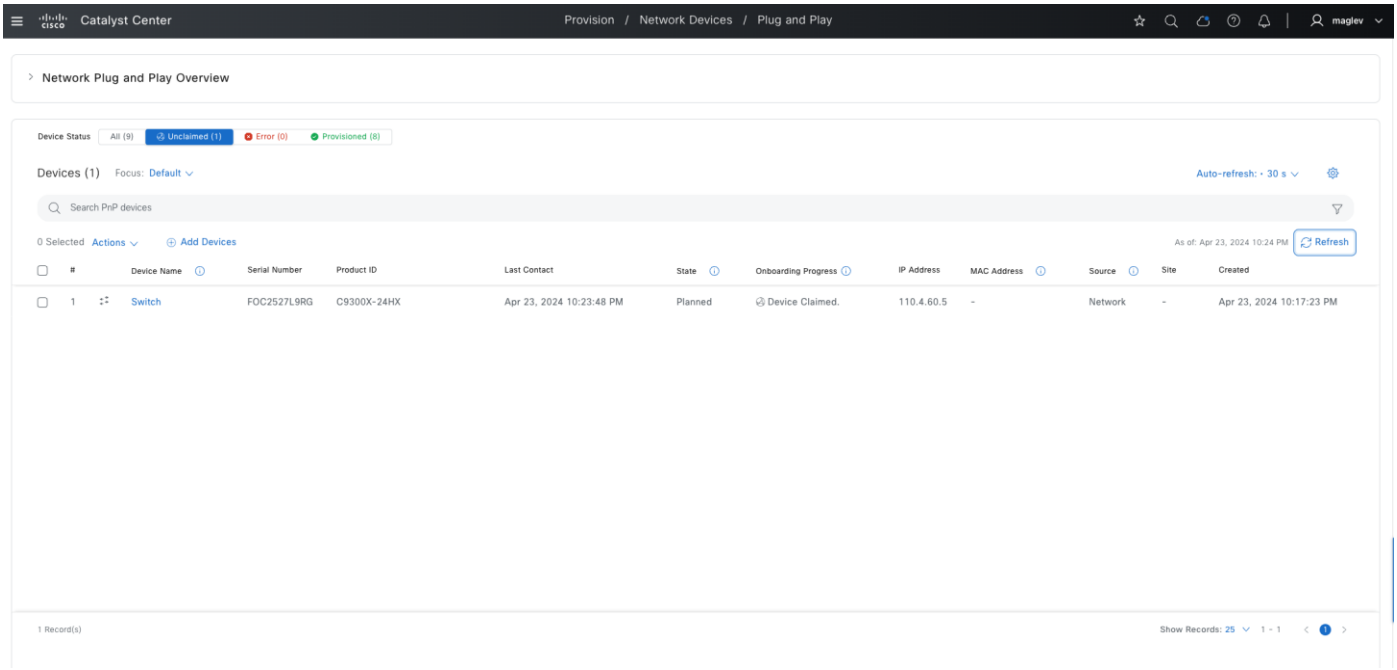

**ステップ 4.** デバイスをプロビジョニングするには、拡張ノードに接続するポートを選択し、[Next] をクリックしてワークフローを完了します。



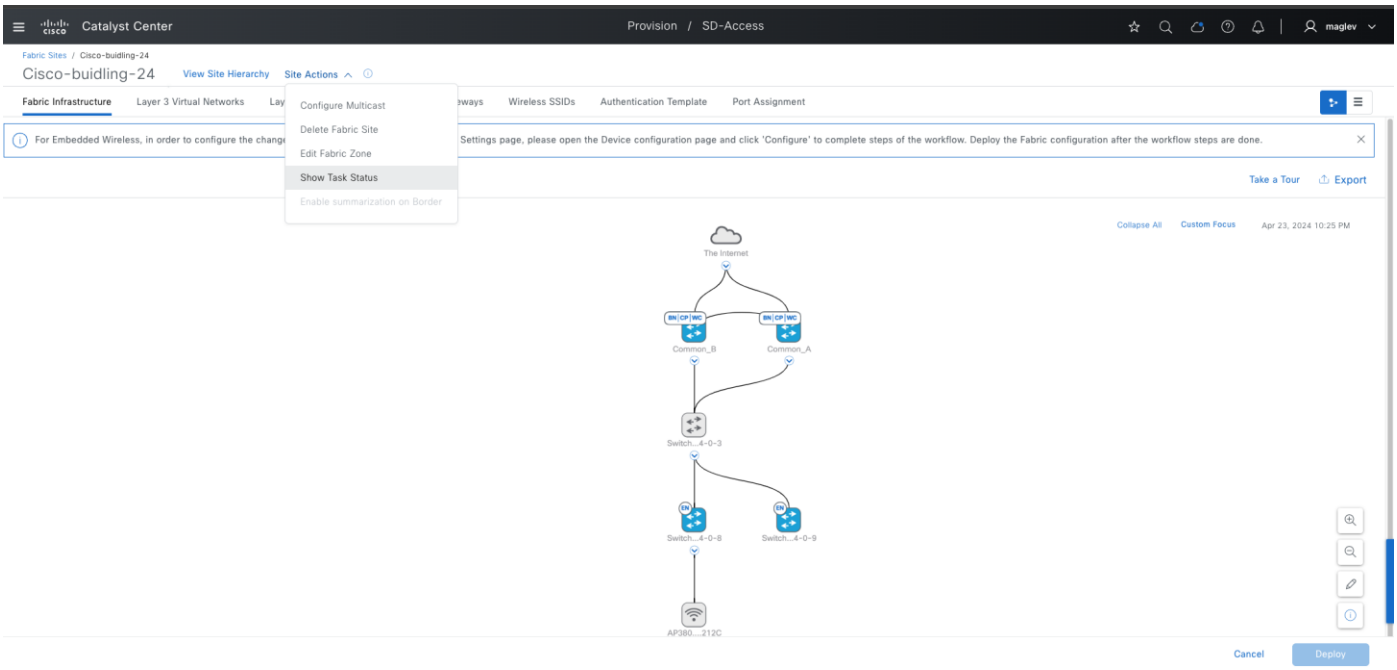

**ステップ 5.** Catalyst Center IP ファブリック インターフェイス IP を指す DHCP サーバーで AP DHCP スコープのオプション 43 を ACSII 値 **5A1D; B2;K4;I120.1.1.1;J80** で設定します。120.1.1.1 は、Catalyst Center アドレス（AP プールと同じ設定）です。

**ステップ 6.** デバイスをファブリックエッジに接続し、オンボーディングが完了するまで待ちます。AP オンボーディングとは異なり、要求プロセスの要件はありません。Catalyst Center は、デバイスを自動的に要求してファブリックサイトにオンボードします。

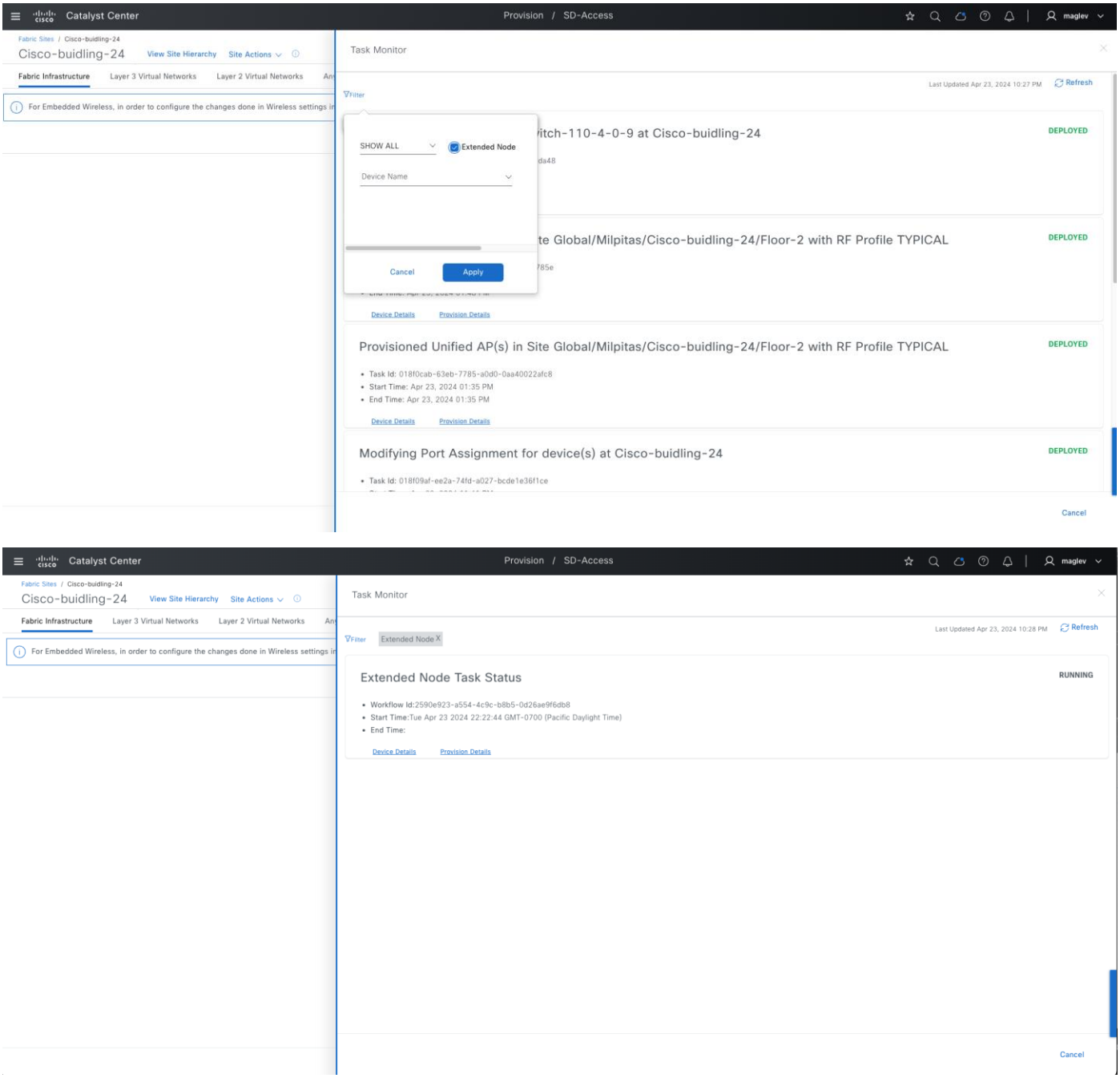
**ステップ 7.** [Plug and Play] ウィンドウから監視します。左上隅にあるメニューアイコンをクリックして [Provision] > [Plug and Play] の順に選択し、[Unclaimed] をクリックします。




**ステップ 8.** ファブリック サイト ウィンドウから監視します。左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックし、[Cisco-building-24] テキストリンクをクリックして [Site Actions] > [Show Task Status] の順に選択します。



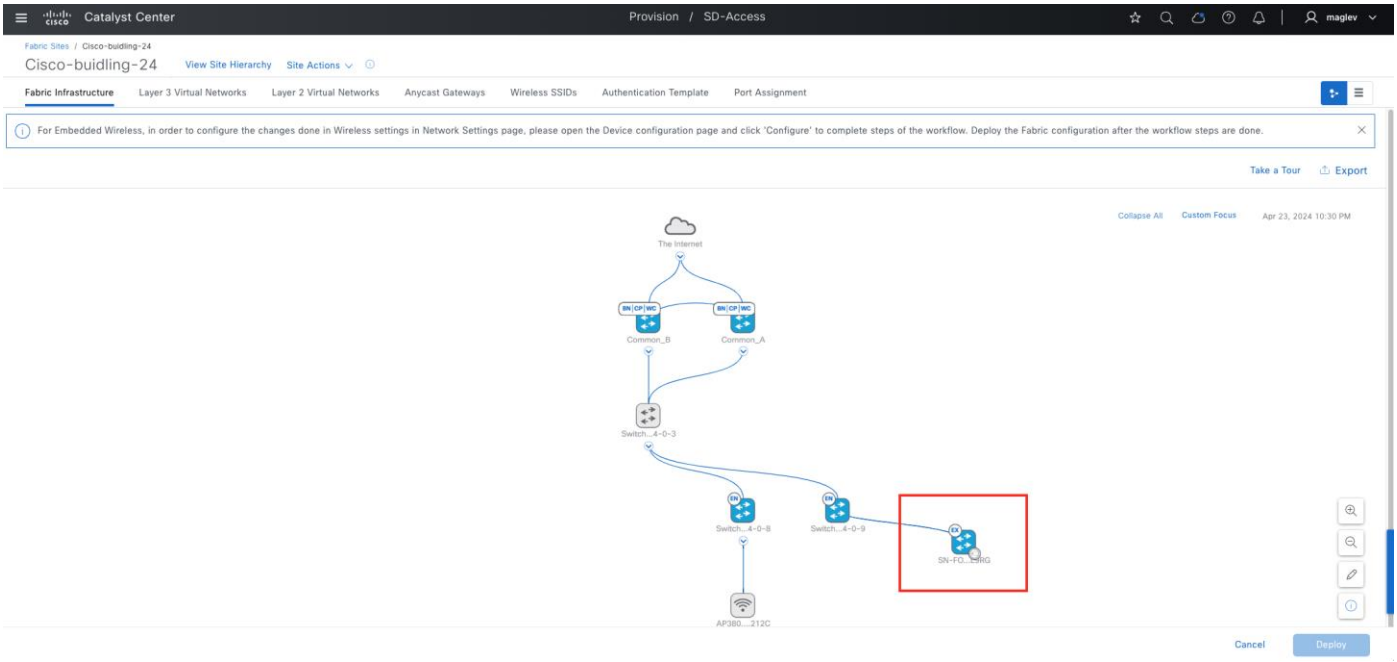

**ステップ 9.** オンボーディングの進行状況を監視するには、[Task Monitor] スライドインペインで、[Filter] > [Extended Node] の順にクリックします。







オンボーディングが完了すると、デバイスは [Fabric Infrastructure] タブに青色で表示され、ファブリックロールが **EX** とマーク付けされます。




**ステップ 10.** 必要に応じてこの手順を繰り返して、さらにポリシー拡張ノードをオンボードします。複数の拡張ノードを同時にオンボードできます。

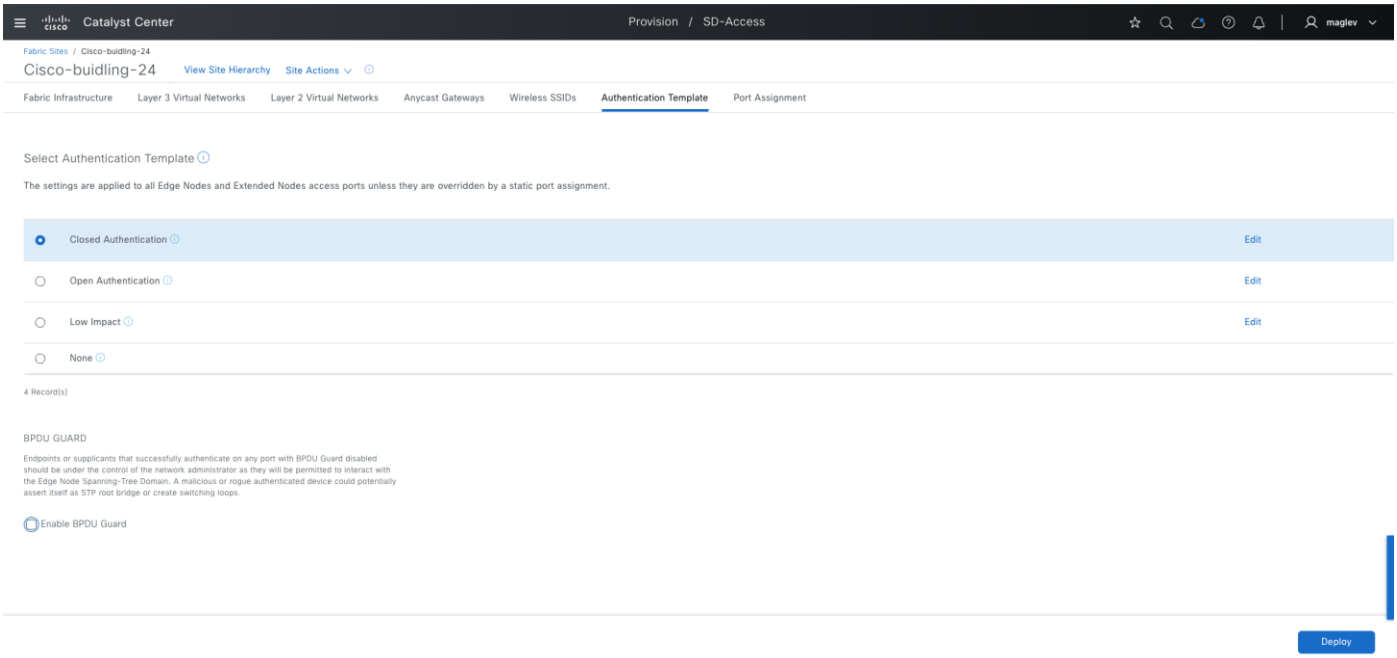
## SBEN のオンボード

SBEN のオンボードには、SBEN プールと Cisco ISE が必要です。

### 手順 1。 SBEN プールの設定

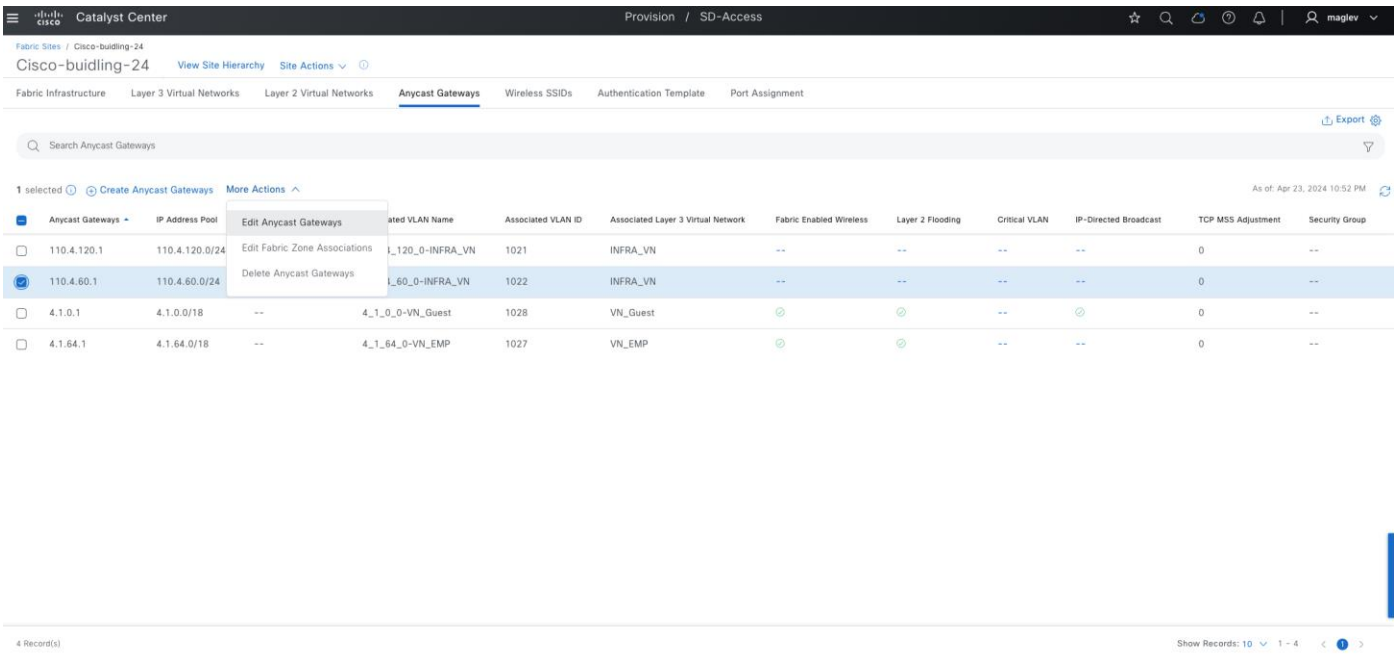
INFRA_VN は、1 つの AP プールと 1 つの拡張ノードプールのみをサポートします。SBEN をオンボードするには、拡張ノードプールを SBEN プールキャパシティで有効にする必要があります。

**ステップ 1.** ファブリックサイトでブリッジ プロトコル データ ユニット（BPDU）ガードを無効にします。[Authentication Template] タブをクリックし、[Enable BPDU Guard] オプションを非アクティブにしてから、[Deploy] をクリックします。

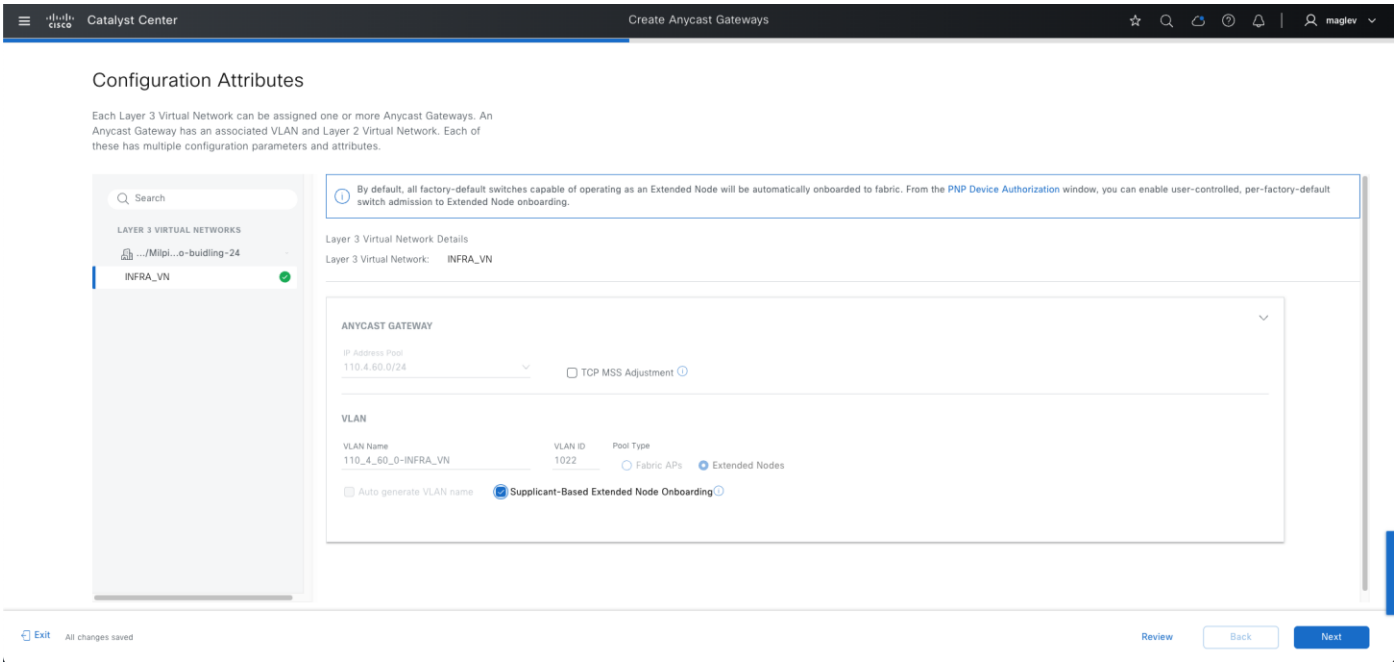



**注：** 拡張ノードプールがファブリックゾーンでも使用されている場合は、ゾーンに対して同じ手順を繰り返します。

**ステップ 2.** [Anycast Gateways] タブをクリックします。拡張プールを選択し、[More Actions] > [Edit Anycast Gateways] の順にクリックします。



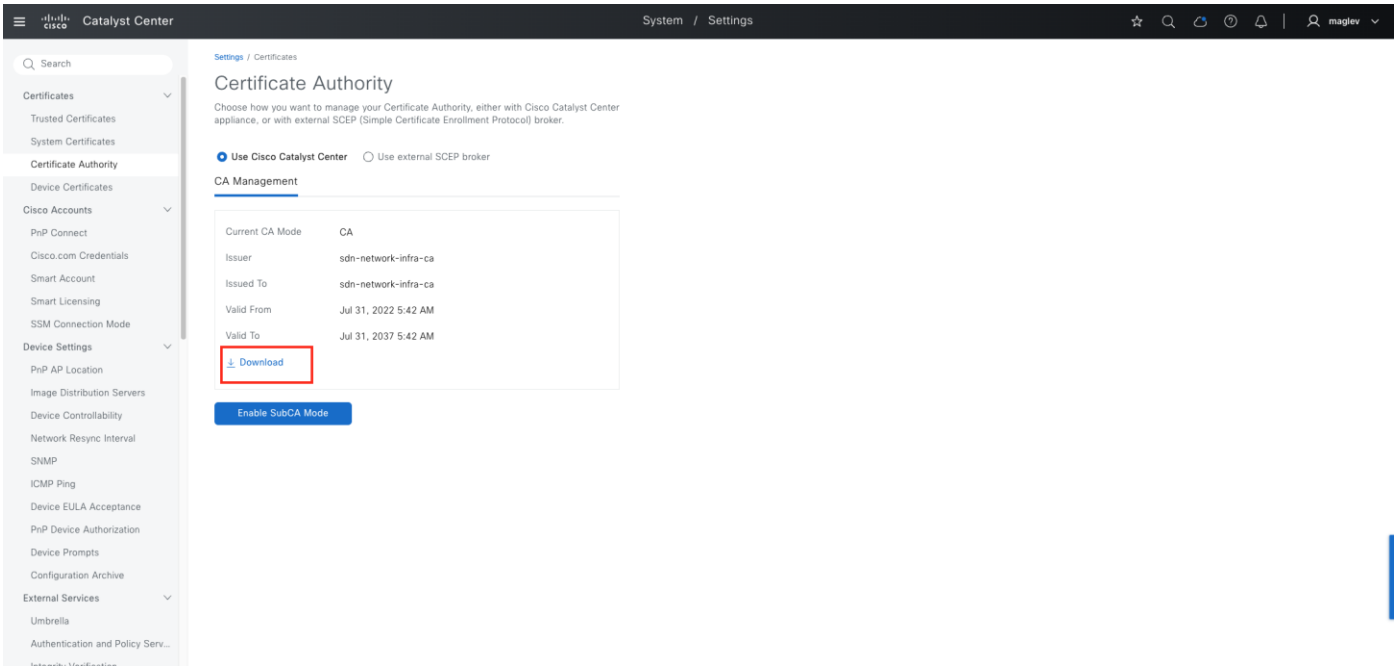
**ステップ 3.** [Supplicant-Based Extended Node Onboarding] チェックボックスをオンにしてから、ワークフローを完了します。




## 手順 2。 Cisco ISE でのポリシーの設定

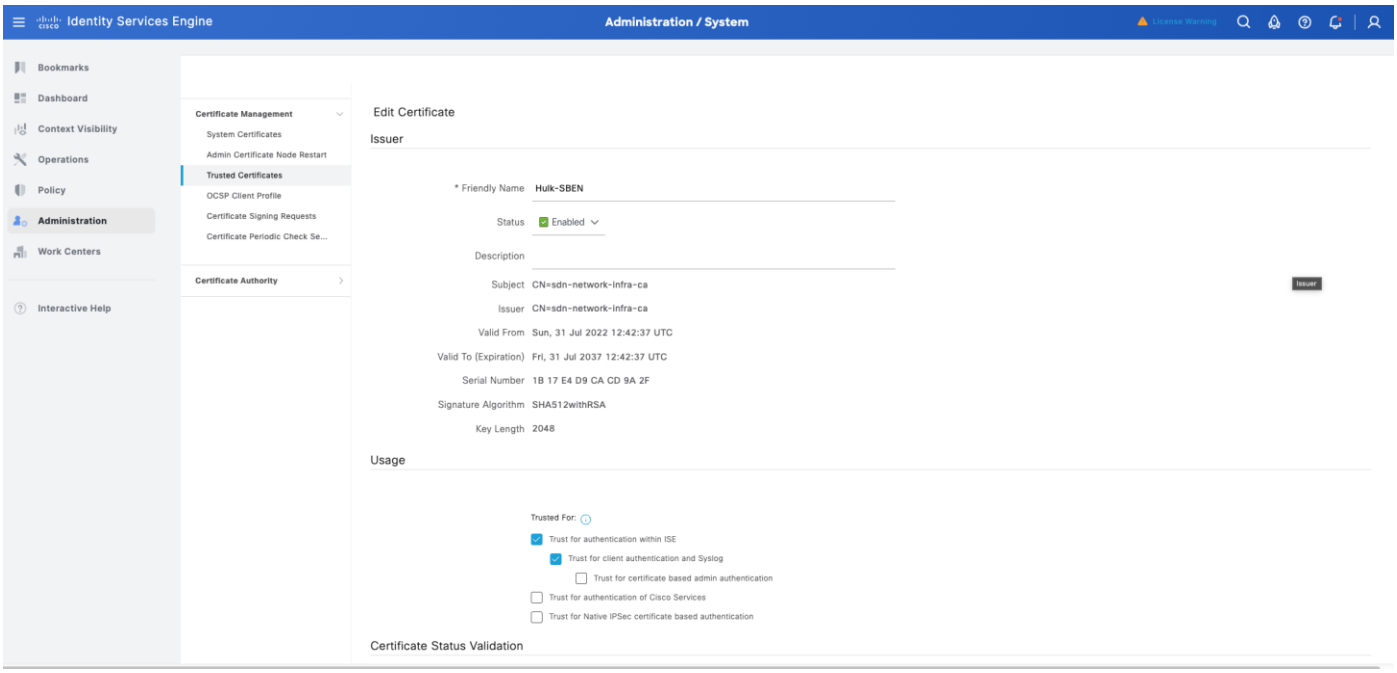
Cisco ISE を設定して、ソフトウェアリリース 3.1 以降で動作することを確認します。

**ステップ 1.** Catalyst Center から CA 証明書をダウンロードします。[System] > [Settings] > [Certificate Authority] > [Download] の順にクリックします。




**ステップ 2.** CA 証明書を Cisco ISE にインポートします。Cisco ISE のホームウィンドウで、[Administration] > [System] > [Certificates] > [Trusted Certificates] > [Import] の順にクリックします。

**ステップ 3.** インポートウィンドウで、[Trust for client authentication and Syslog] チェックボックスをオンにします。




**ステップ 4.** ポリシーを設定します。[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] の順にクリックし、表 25 に示されているそれぞれの radius 属性を使用して 3 つのプロファイルを設定します。

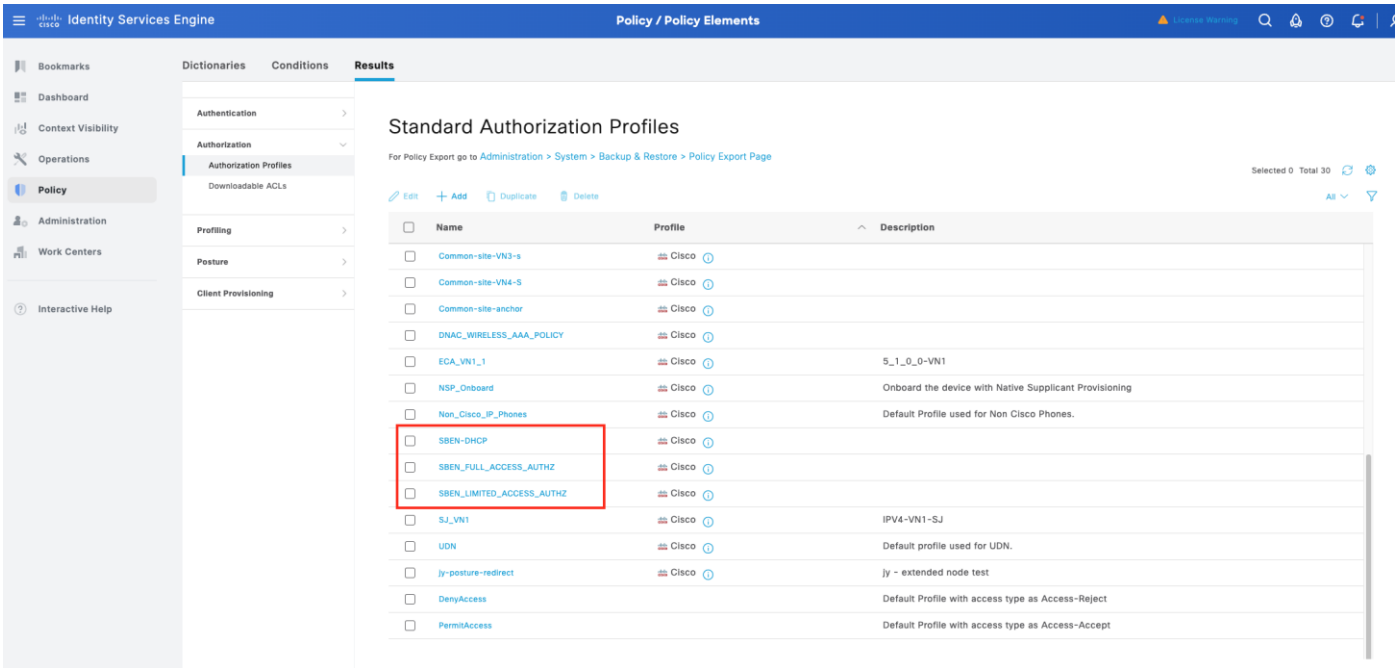
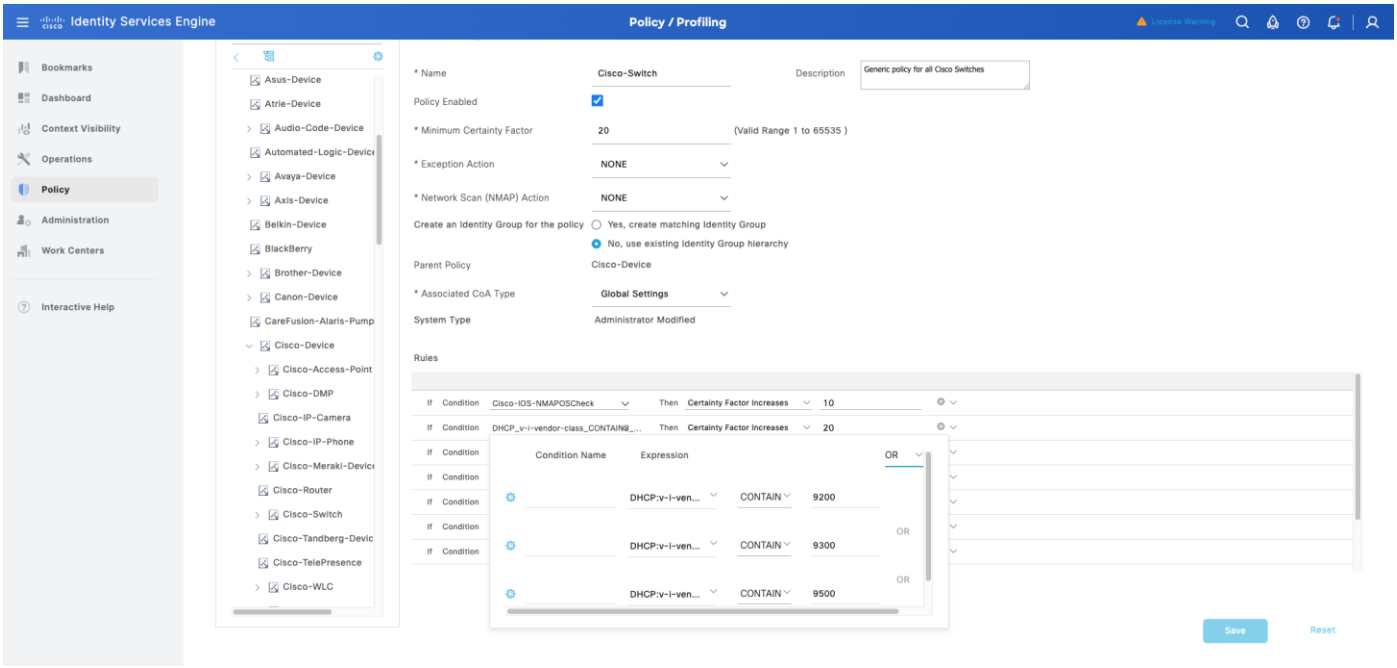


**表 25.** プロファイルの設定

| 名前 | アクセスタイプ | フィルタ ID | cisco-av-pair = interface-template-name |
|---|---|---|---|
| SBEN-DHCP | ACCESS_ACCEPT | SBEN_DHCP_ACL.in | |
| SBEN_LIMITED_ACCESS_AUTHZ | ACCESS_ACCEPT | SBEN_MAB_ACL.in | SWITCH_SBEN_MAB_TEMPLATE |
| SBEN_FULL_ACCESS_AUTHZ | ACCESS_ACCEPT | | SWITCH_SBEN_FULL_ACCESS_TEMPLATE |

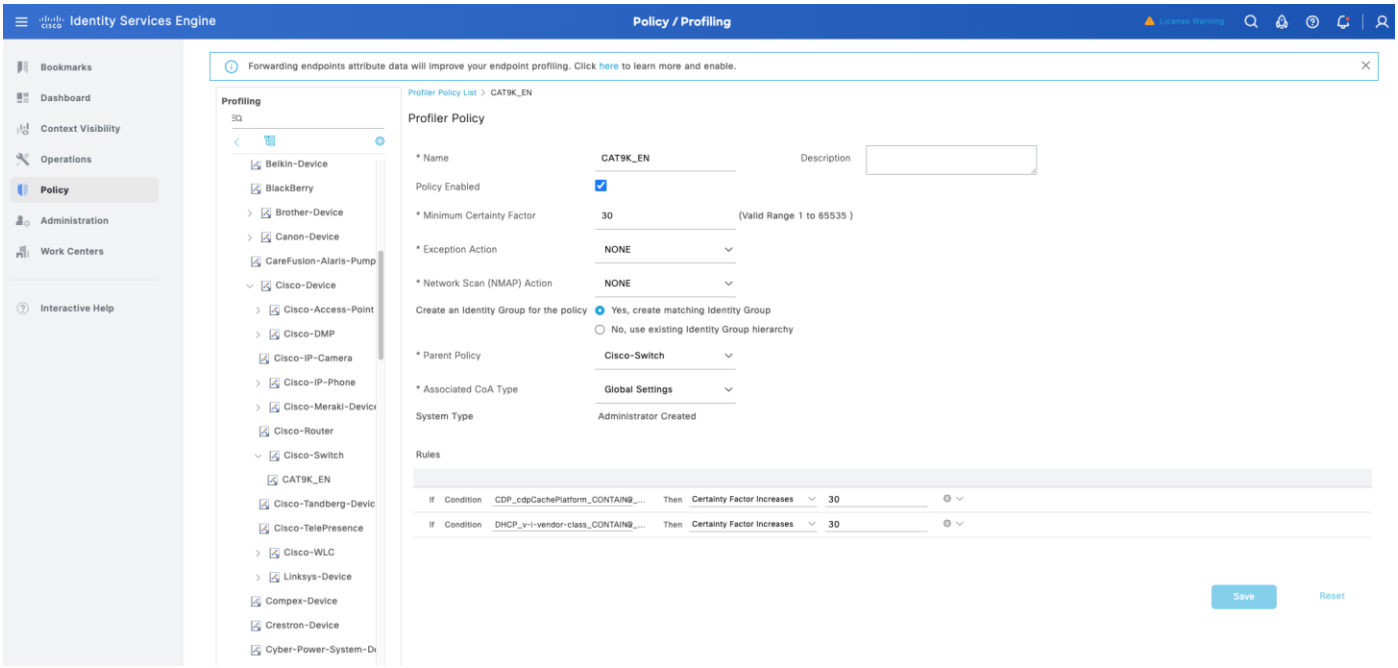
**ステップ 5.** デバイス プロファイリング ポリシーを定義します。[Policy] > [Profiling] > [Profiling Policies] の順にクリックします。

a. [Policy / Profiling] ウィンドウで、[Cisco-Device] : [Cisco-Switch] ポリシーの新しい [DHCP-v-i-vendor-class] 条件を追加します。[Associated COA type] > [Global Settings] の順に選択します。

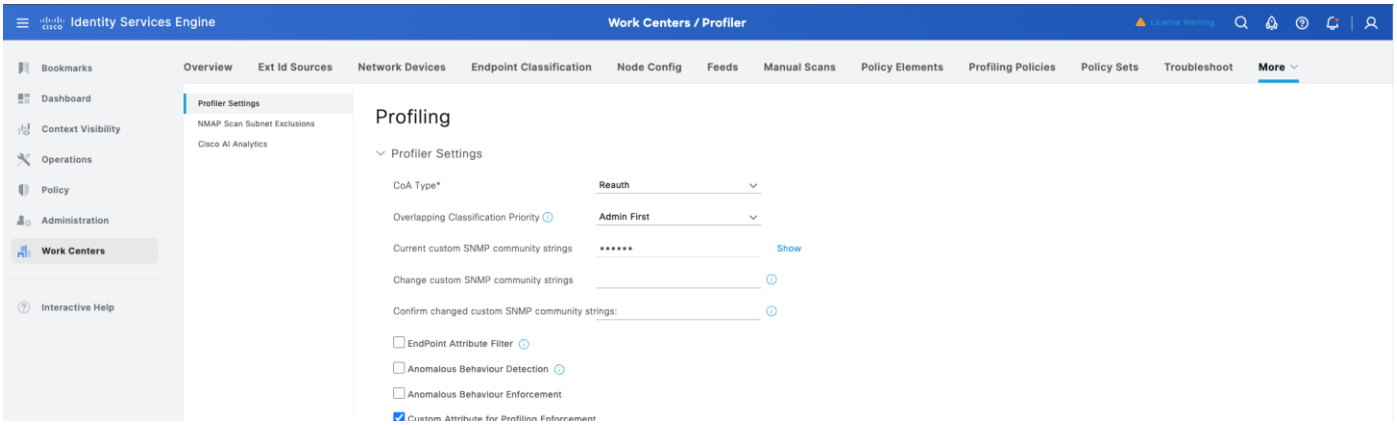


b. [Cisco-Switch] の下に、**サプリカントデバイスの新しい子ポリシー**を作成し、[CdpCachePlatform] および [V-I-Vendor-Class] 条件を適用します。

子ポリシーの [Minimum Certainty Factor] の値が親ポリシーの値よりも高いことを確認してください。

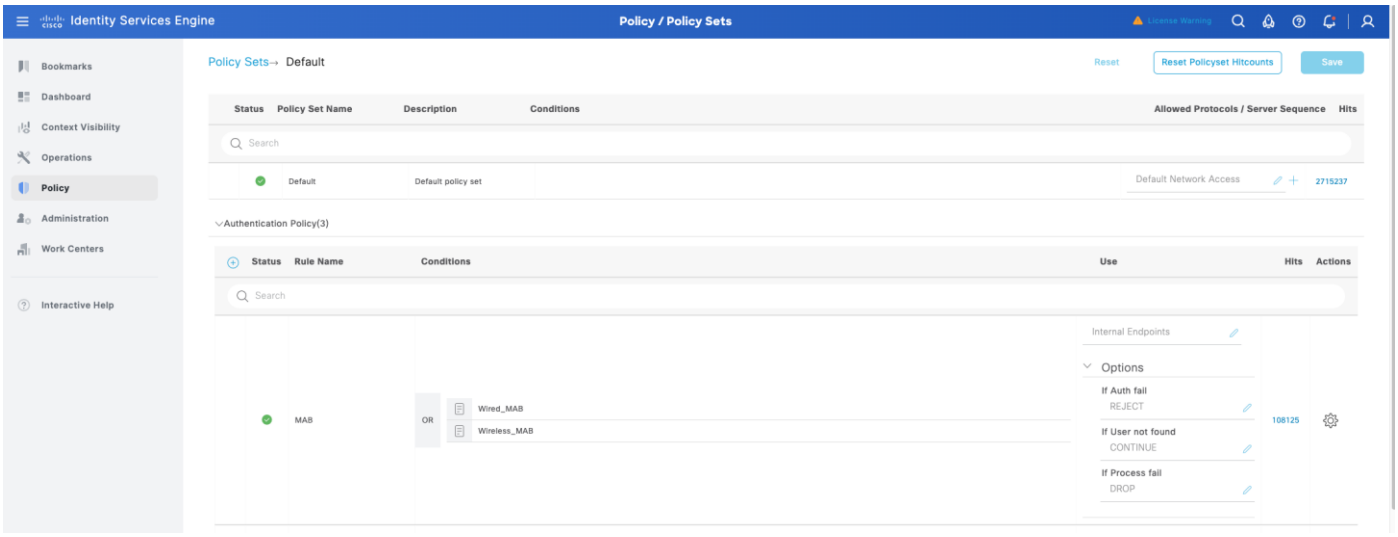



**ステップ 6.** グローバル認可変更（CoA）タイプを設定します。Cisco ISE のホームウィンドウで、[Work Centers] > [Profiler Settings] の順にクリックし、[CoA Type] で [Reauth] を選択します。

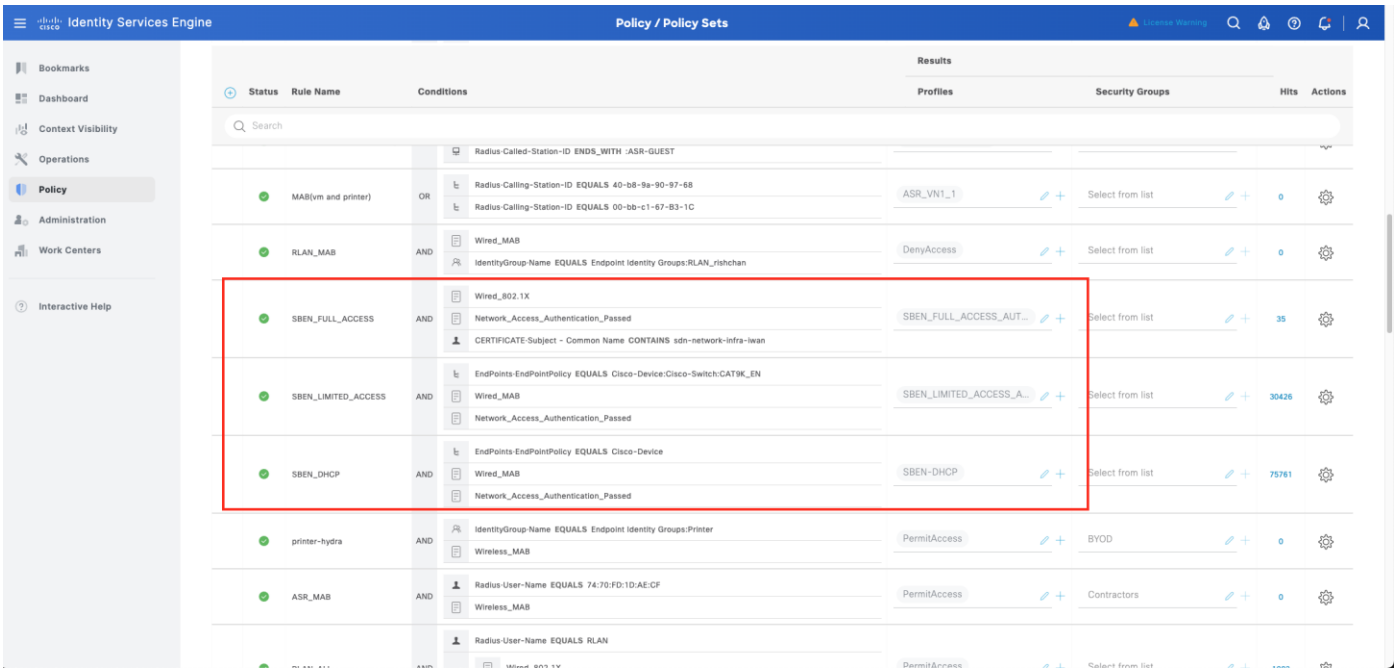


**ステップ 7.** 認証ポリシーを設定します。[Policy] > [Policy Sets] > [Default] > [Authentication Policy] の順に選択します。

a. [If User not found] フィールドの場合、デフォルトの MAB ポリシーが [CONTINUE] に設定されていることを確認します。




b. [Policy Sets] ウィンドウで、サプリカントデバイスの認証ポリシーを設定し、ポリシーを以前に作成した認証プロファイル（SBEN-DHCP、SBEN_LIMITED_ACCESS_AUTHZ、SBEN_FULL_ACCESS_AUTHZ）に関連付けます。

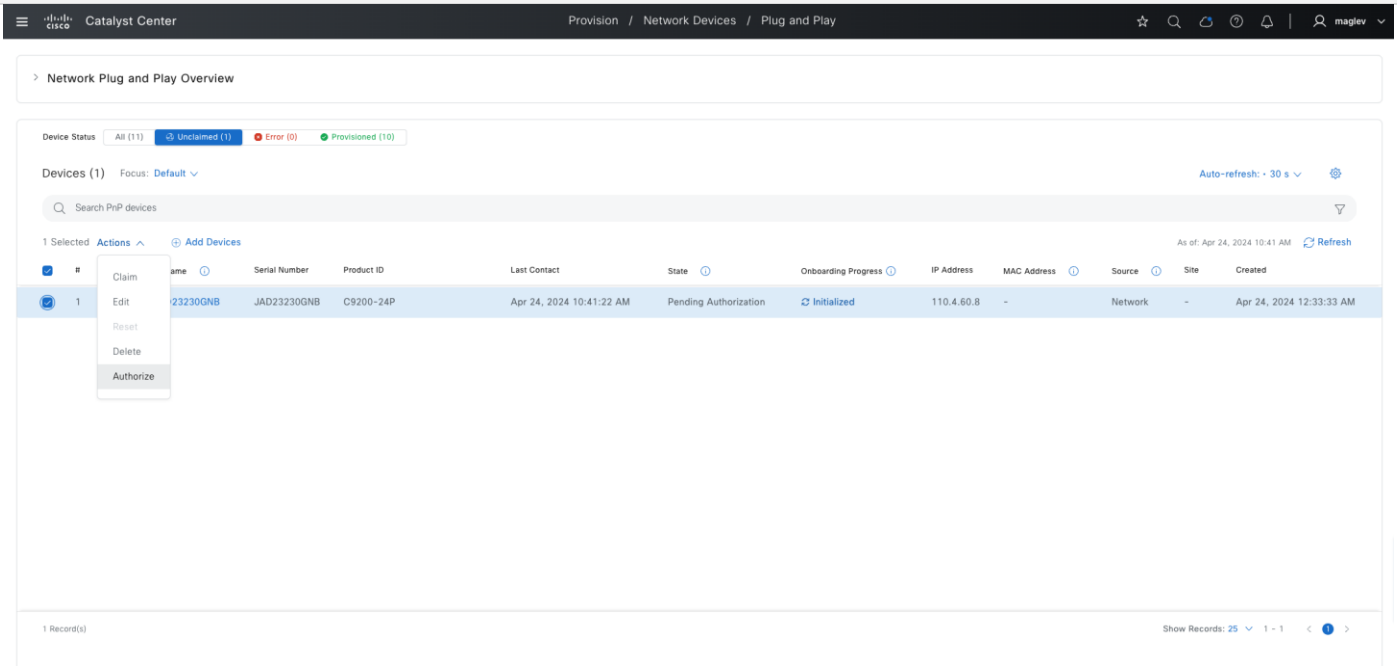


## 手順 3。　サプリカントベースの拡張ノードのオンボード

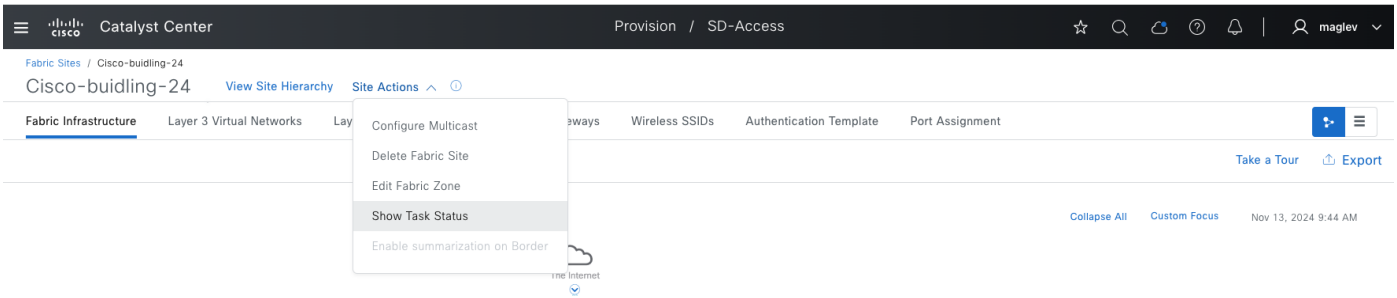
単一リンク接続でオンボードされたポリシー拡張ノードの 1 つに新しいデバイスを接続します。この例では、PnP デバイス許可が有効になっています。

**ステップ 1.** [Plug and Play] ウィンドウから監視します。デバイスのステータスが [Pending Authorization] の場合、[Actions] > [Authorize] の順にクリックします。

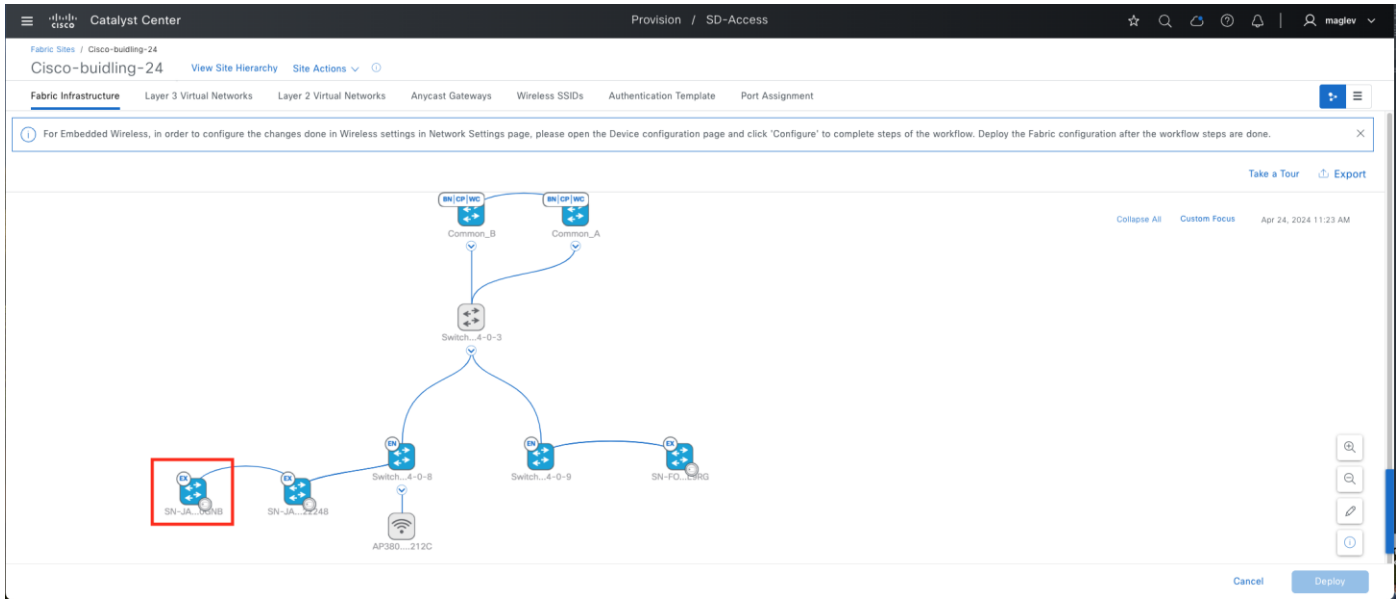
**注：**　ステップ 1 は、PnP デバイス許可が有効になっている場合にのみ必要です。




**ステップ 2.** ファブリックサイトから [Show Task Status] を監視します。




オンボーディングが終了し、デバイスがファブリックに追加されます。

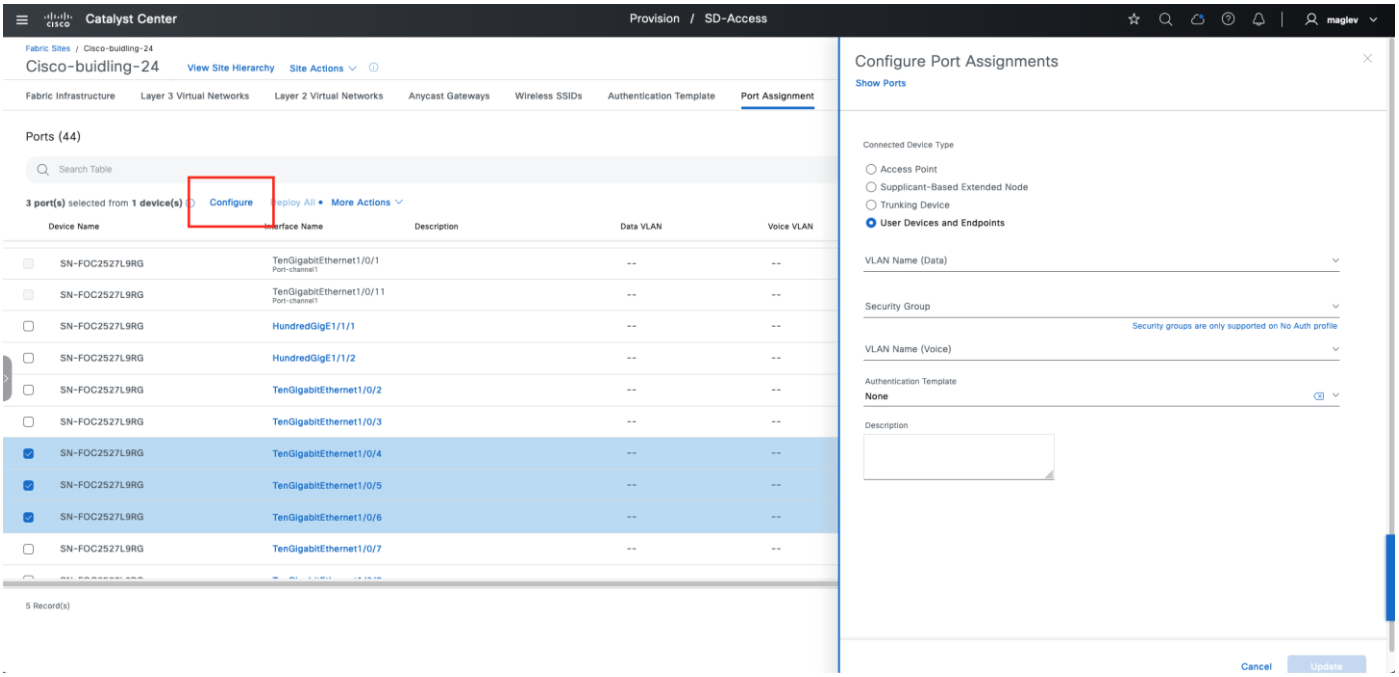



**注：** オンボーディング時に、新しい SBEN デバイスは別の SBEN デバイスに接続されます。これは、デイジーチェーンと呼ばれます。

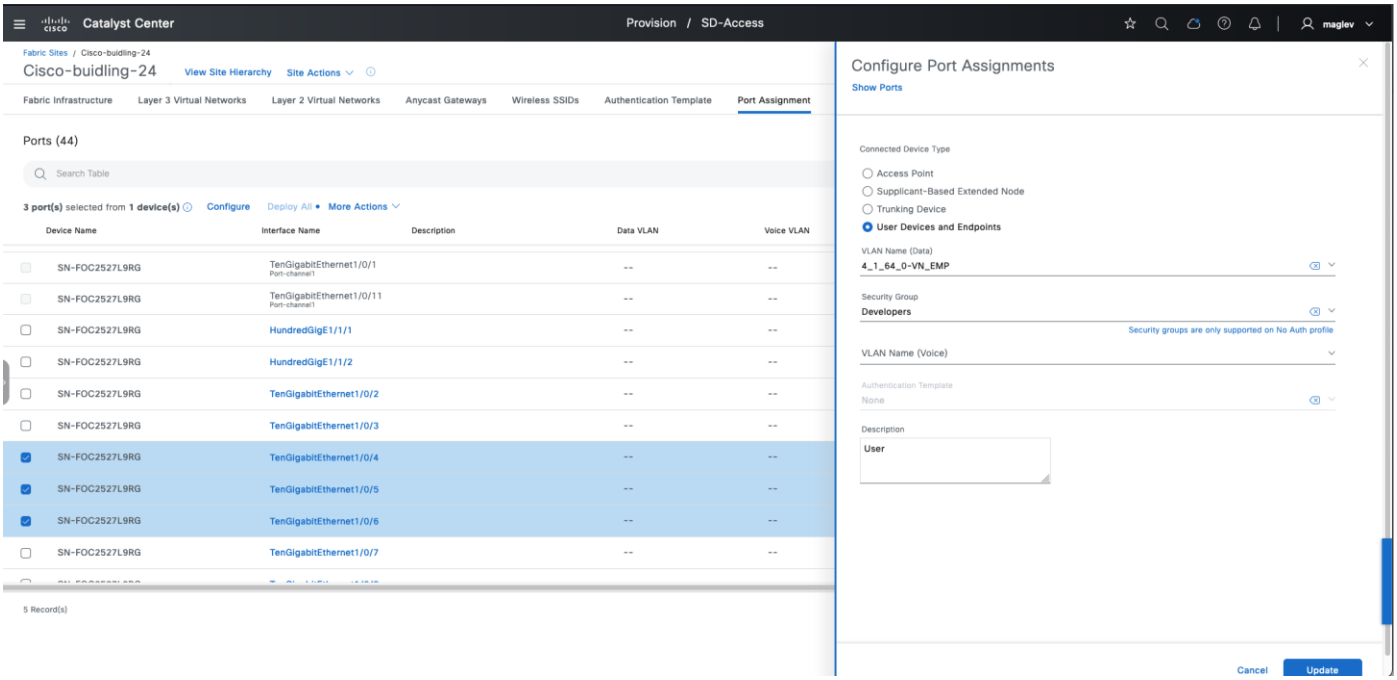
## クライアントのオンボード

AP と拡張ノードに加えて、ポート割り当てでは、エンドポイントにトランクポートとアクセスポートを必要とするサーバーデバイスの物理ポートを指定および設定することもできます。次の例は、ユーザーデバイスおよびエンドポイント、トランキングデバイスとして、接続済みデバイスタイプに対して複数の個別のポートを設定する方法を示しています。

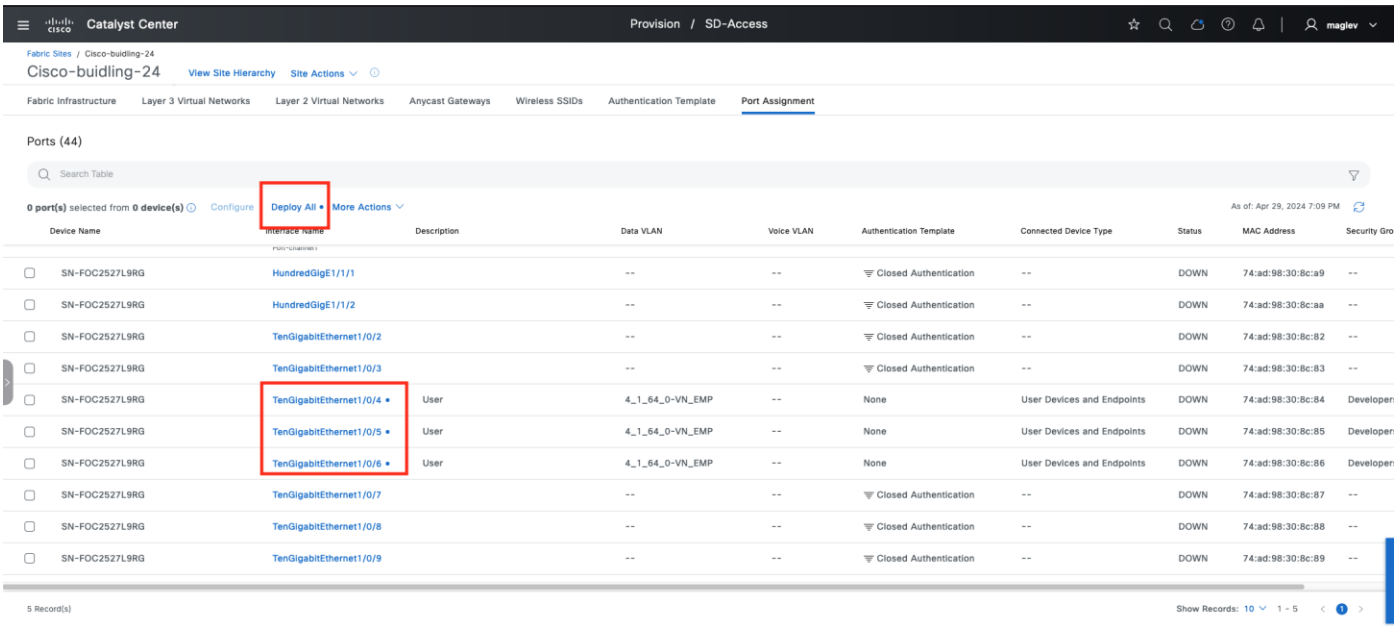
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Port Assignment] タブをクリックして物理ポートのチェックボックスをオンにし、[Configure] をクリックします。



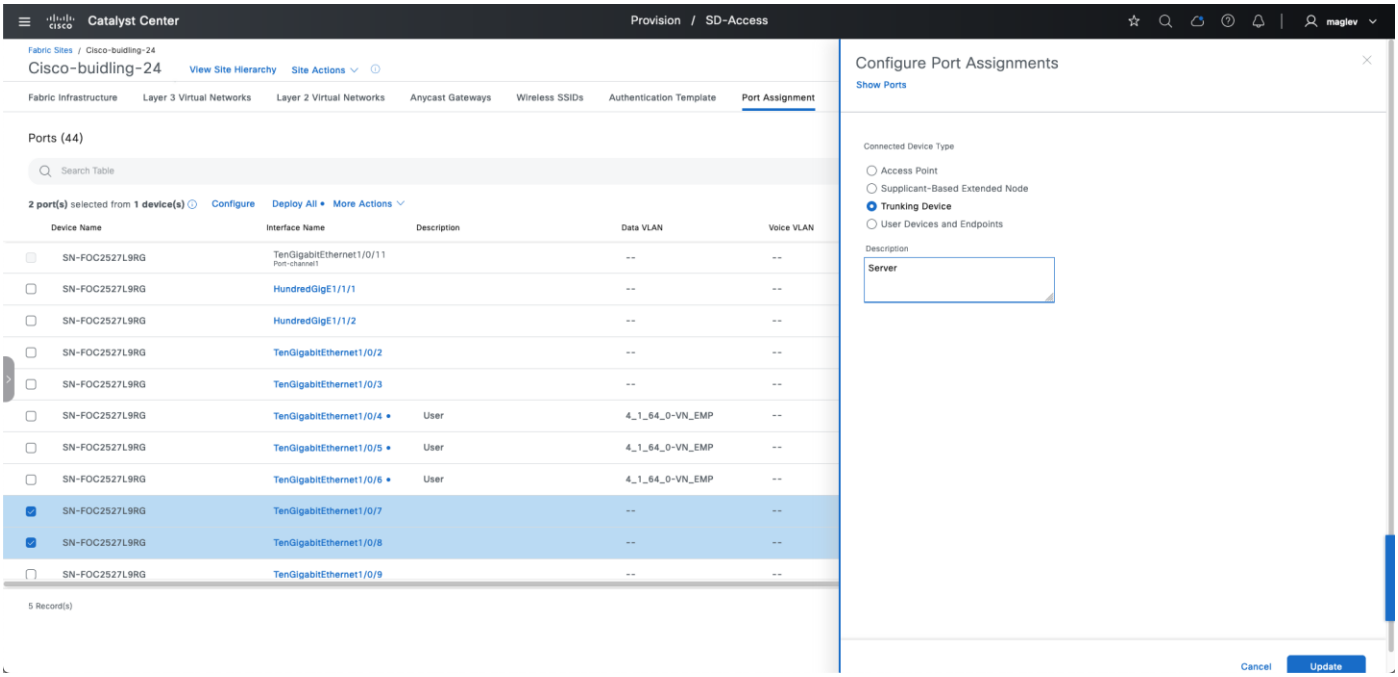

**ステップ 2.** 必要な情報を設定してから、[Update] をクリックします。



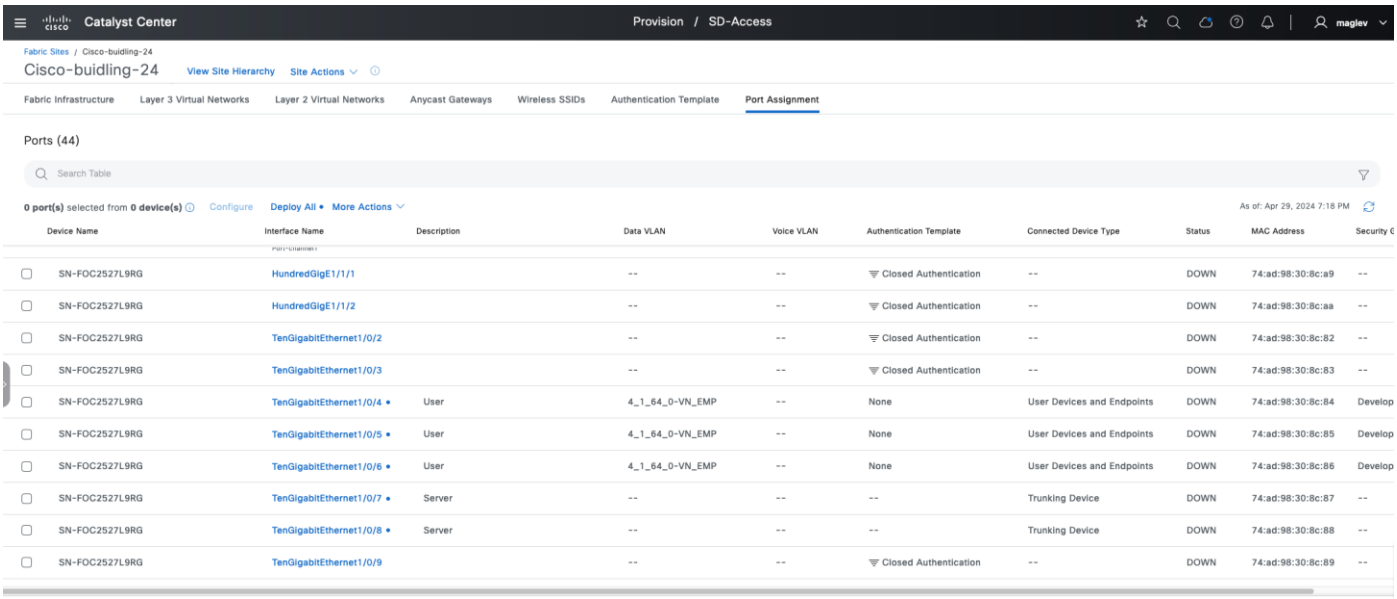

**ステップ 3.** [Deploy All] は、プロビジョニングが必要な、いくつかの変更があることを示すドットでマーク付けされます。保留中の変更がある物理ポートにも、ドットがマーク付けされます。




**ステップ 4.** 引き続き他のポートを**トランキングデバイス**として設定してから、[Update] をクリックします。




**ステップ 5.** [Deploy All] をクリックして、デバイスに変更を展開します。




**ステップ 6.** デバイスでクライアント情報を確認します。

ホストは、エッジノードまたは PEN ノードに接続されます。認証でオンボードされている場合は、`show access-session interface xx detail` コマンドを使用します。

```
            Interface:  GigabitEthernet1/0/17
                IIF-ID:  0x1475166D
          MAC Address:  76b3.c249.0100
         IPv6 Address:  Unknown
         IPv4 Address:  4.1.64.10
            User-Name:  common
          Device-type:  Un-Classified Device
          Device-name:  Unknown Device
                  VRF:  VN_EMP
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
  Acct update timeout:  172800s (local), Remaining: 151704s
    Common Session ID:  0700046E00005D67D104EA2B
     Acct Session ID:  0x00005d1a
              Handle:  0x97000d2b
      Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Local Policies:

Server Policies:
          Vlan Group:  Vlan: 1027
           SGT Value:  6


Method status list:
       Method           State
        dot1x           Authc Success
```

ワイヤレスコントローラでワイヤレスクライアントを確認する必要があります。`show wireless client summary` コマンドを使用します。

```
katar-faniu-ewlc#show wireless client summ
Number of Clients: 1

MAC Address    AP Name                                          Type ID   State            Protocol Method     Role
-------------------------------------------------------------------------------------------------------------------
782b.469b.4290 AP707D.B9B4.85A6                                 WLAN 17   Run              11ac     Dot1x      Local

Number of Excluded Clients: 0
```

また、`show wireless client mac-address xx detail` コマンドを使用して、詳細を確認します。

**図 48.　　切り捨てられた出力例（情報が多すぎるため）**

```
katar-faniu-ewlc#show wireless client mac-address 782b.469b.4290 detail

Client MAC Address : 782b.469b.4290
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 6.1.64.12
Client IPv6 Addresses : fe80::268a:bbea:b04c:6b42
                        3020::1756:9007:8e46:bea5
Client Username : lily
AP MAC Address : 6cb2.aedc.1940
AP Name: AP707D.B9B4.85A6
AP slot : 1
Client State : Associated
Policy Profile : ASR-ENTERP_Global_F_eec05e51
Flex Profile : default-flex-profile
Wireless LAN Id: 17
WLAN Profile Name: ASR-ENTERP_Global_F_eec05e51
Wireless LAN Network Name (SSID): ASR-ENTERPRISE
BSSID : 6cb2.aedc.194e
Connected For : 39 seconds
Protocol : 802.11ac
Channel : 104
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 86400 sec (Remaining time: 86362 sec)
```

## ファブリック機能の変更

エニーキャストゲートウェイとファブリックボーダーでの新しいファブリック機能の有効化、サイトレベルの認証テンプレートの変更、ファブリックサイトへのエニーキャストゲートウェイの追加、ポート割り当ての実行、ファブリック SSID の変更または追加など、特定のファブリック操作は、Cisco SD-Access ワークフローで許可されています。通常、変更不可能な機能と属性は、GUI でグレー表示されます。たとえば、次の操作は許可されません。

- ファブリックロールの変更：

  デバイスのファブリックロールを変更するには、まずこのデバイスをファブリックから削除し、新しいロールを使用して再度追加する必要があります。

- Cisco SD-Access タイプの変更：

  ファブリックサイトが LISP Pub/Sub または LISP/BGP として設定されている場合、LISP/BGP または LISP Pub/Sub への変更はサポートされていません。ファブリックサイトを切断し、ファブリックを再構築します。

- ファブリックデバイスの別のサイトへの移動：

デバイスがサイトにプロビジョニングされている場合、別のサイトに変更することはできません。ファブリックサイトとインベントリからデバイスを削除し、デバイスを再追加または再検出して、新しいサイトにプロビジョニングします。

- VN アンカーの設定：

  使用中の VN をアンカーすることはできません。すべてのエニーキャストゲートウェイを削除し、ファブリックゾーンから VN の関連付けを解除して、アンカー VN として設定します。

- ファブリックゾーンの無効化：

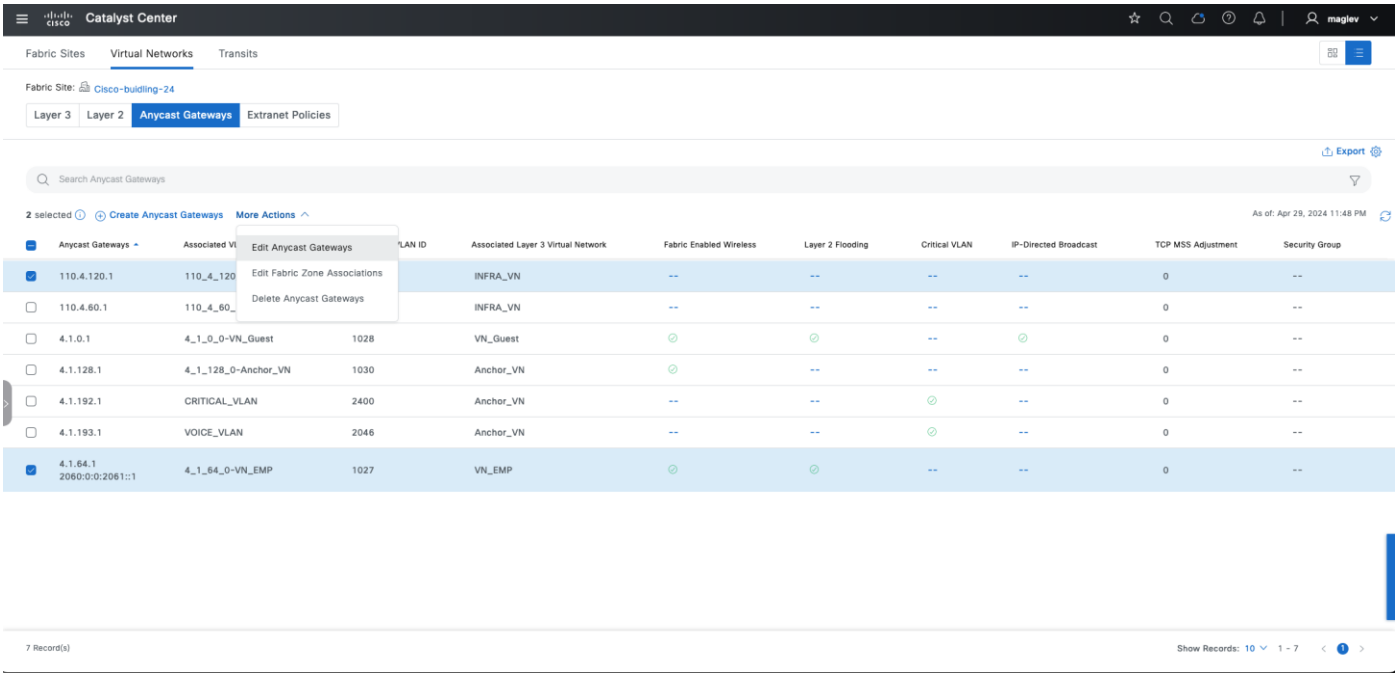
  ファブリックゾーンにアクティブなエッジデバイスとエニーキャストゲートウェイが関連付けられている場合、ファブリックゾーンを無効にすることはできません。ゾーンからすべてのエッジを削除し、マルチキャストが存在する場合は削除し、エニーキャストゲートウェイを削除してから、ファブリックゾーンを無効にします。

このセクションのプロセスでは、エニーキャストゲートウェイと許可されたサイトレベルの認証の変更について説明します。

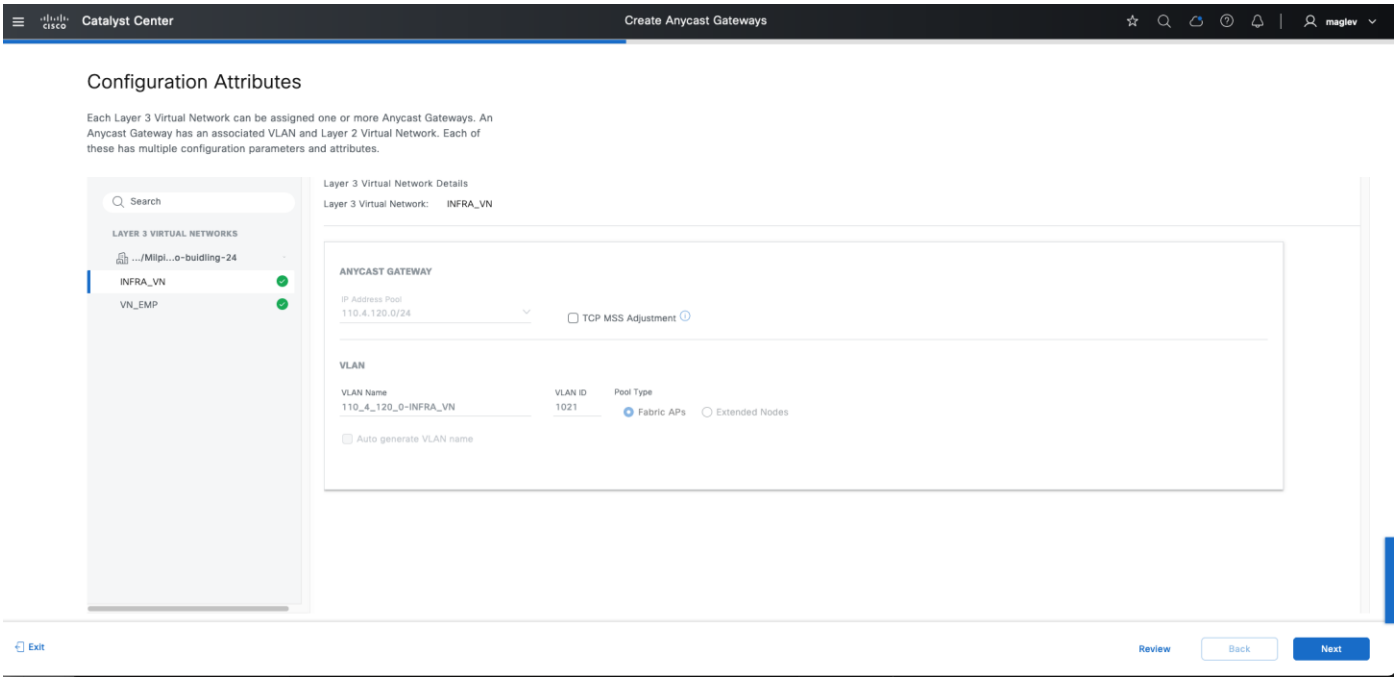
### エニーキャストゲートウェイの更新

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Anycast Gateways] タブをクリックして複数のプールのチェックボックスをオンにします。

**ステップ 2.** [More Actions] > [Edit Anycast Gateways] を選択します。

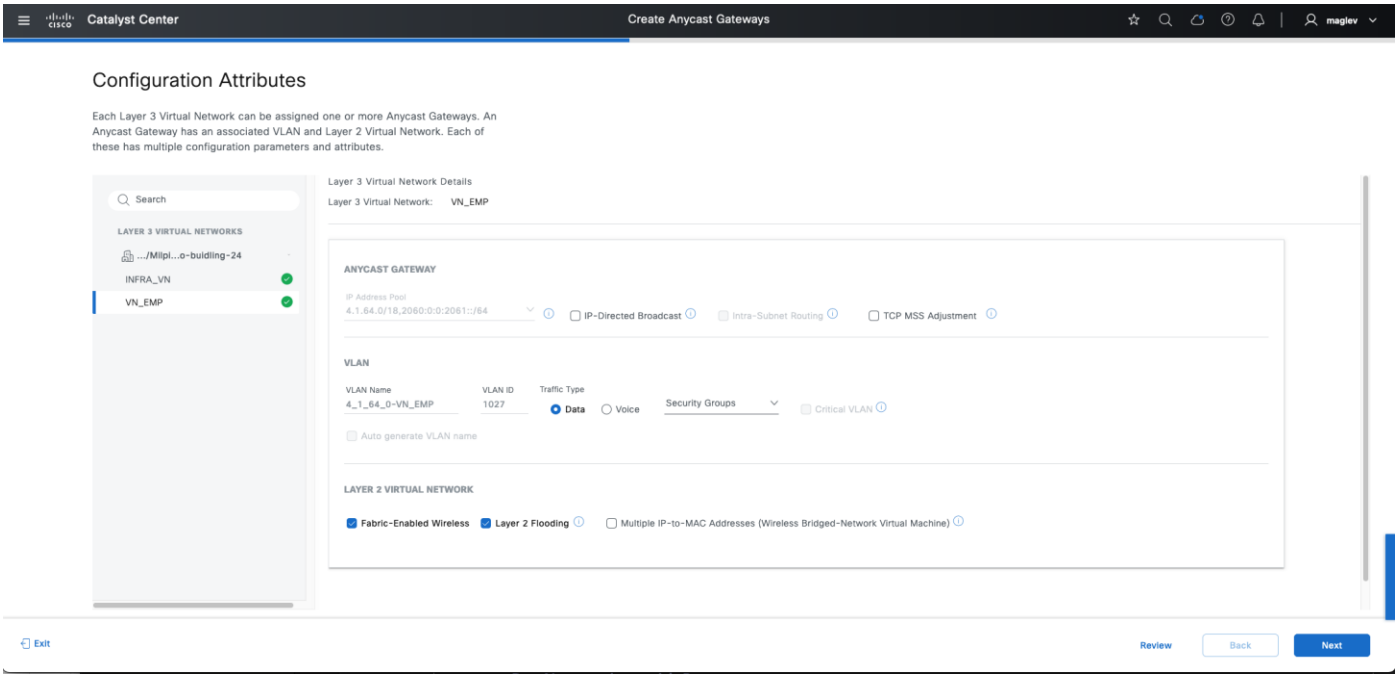


**INFRA_VN** には AP プールと拡張ノードプールがあり、[TCP MSS Adjustment] のみ変更可能です。




**技術的なヒント：** 「手順 3：サプリカントベースの拡張ノードのオンボード」セクションで説明したように、拡張ノードプールを SBEN プールに変更できます。

カスタマー VN の場合、**VLAN 名**、**VLAN ID**、**クリティカル VLAN** は変更できません。

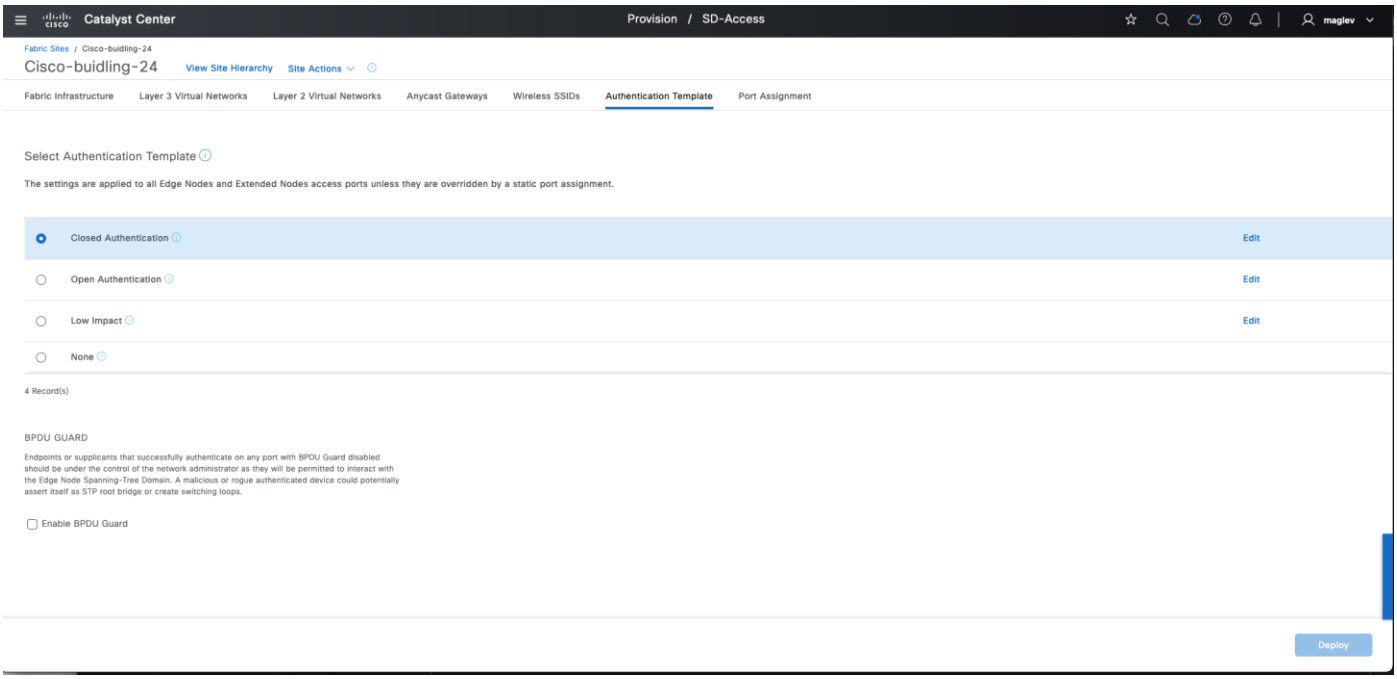


### サイトレベル認証の変更

サイトレベルの認証は直接変更できます。新しい認証テンプレート設定は、ポート割り当て設定がないすべての Catalyst Center 管理対象アクセスポートにプッシュされます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Authentication Template] タブをクリックします。

**ステップ 2.** 新しい**認証テンプレート**を選択し、[Deploy] をクリックします。




**注：** SBEN プールが設定されている場合、**認証テンプレート**を [Closed Authentication] から別の**認証テンプレート**または [Enable BPDU Guard] に変更することはできません。すべての SBEN ノードを削除し、SBEN プールを無効にしてから、**認証テンプレート**と **BPDU ガード**の設定を変更します。

## バナーサポートの使用

Catalyst Center は、サイトレベルで Day-*N* の変更を適用するためのバナーサポートも提供します。Day-*N* 運用には、次のものが含まれます。

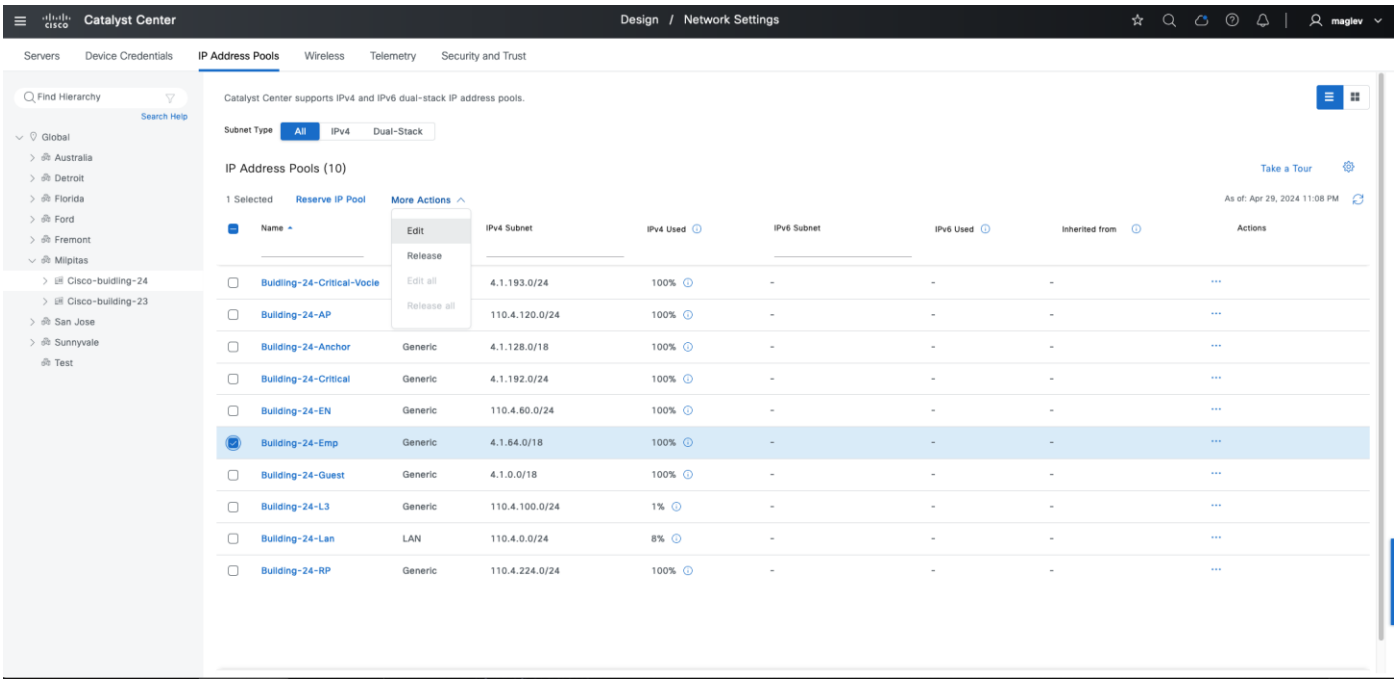
- IPv4 アドレスプールの IPv4 および IPv6 デュアルスタックプールへの移行
- DHCH サーバーと DNS IP アドレスの更新
- 新しいラインカードまたはスタックメンバーの追加

### IPv4 アドレスプールのデュアルスタックプールへの移行

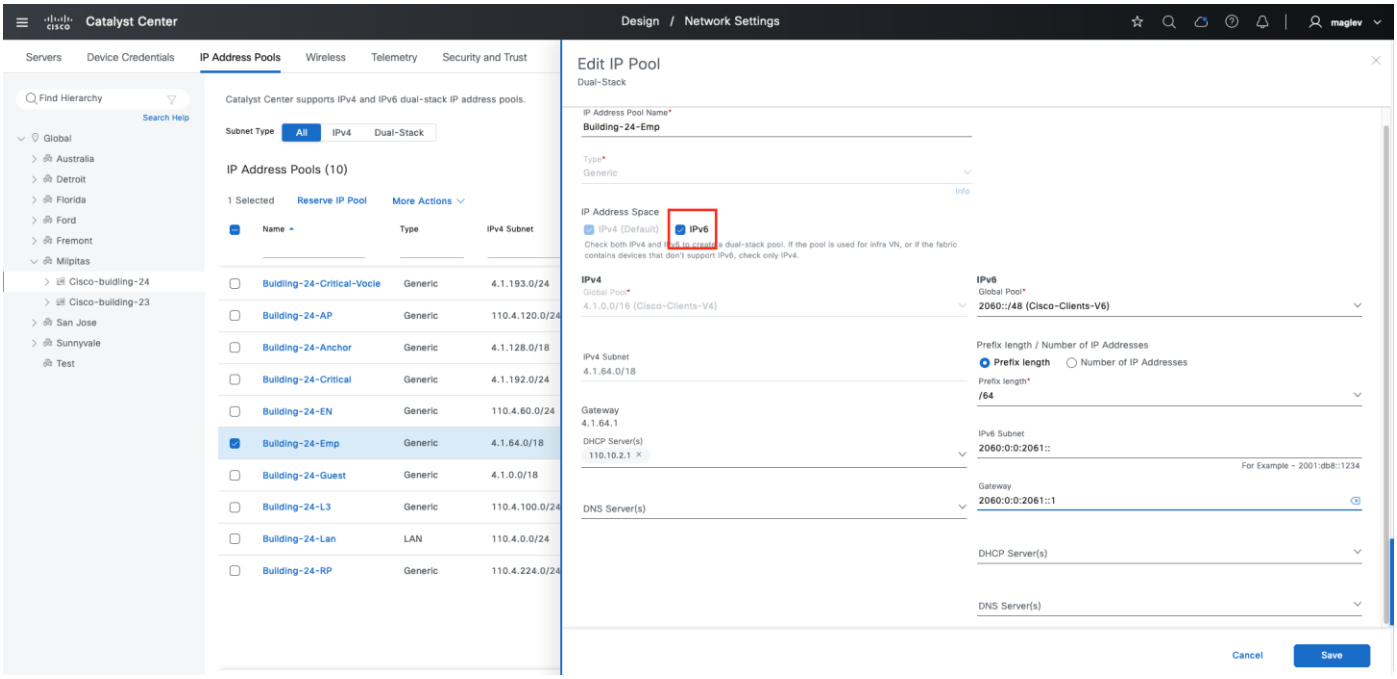
このプロセス例は、IPv4 クライアントプール **Building-24-Emp** を **Cisco-building-24** のデュアルスタックプールに移行する方法を示しています。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Design] > [Networking Setting] の順に選択し、[IP Address Pools] タブをクリックします。

**ステップ 2.** [Global] から [Cisco-Buidling-24] に切り替えます。[Building-24-Emp] チェックボックスをオンにして、[More Actions] > [Edit] の順に選択します。

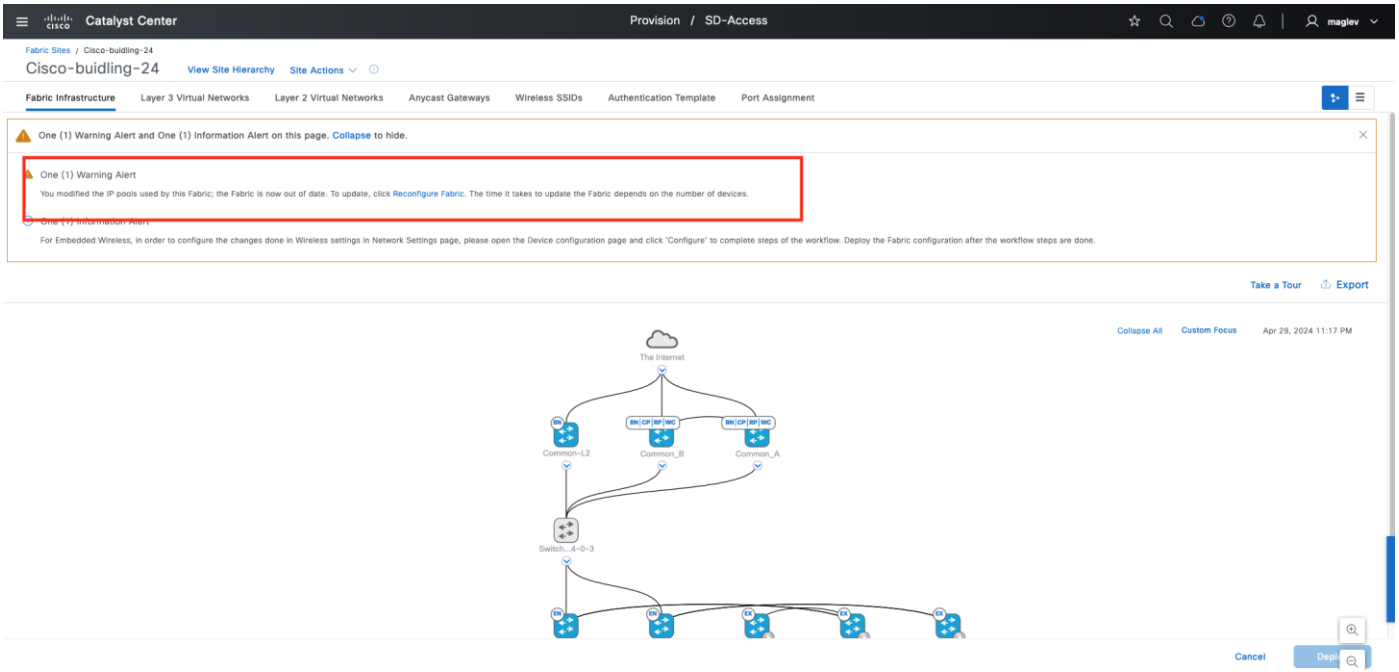



**ステップ 3.** [IPv6] チェックボックスをオンにして、[Global Pool]、[Prefix Length]、[IPv6 subnet]、および [Gateway] フィールドに必要な情報を入力し、[Save] をクリックします。




**ステップ 4.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Fabric Infrastructure] タブをクリックします。

**図 49.　　ファブリックバナー表示の再設定**

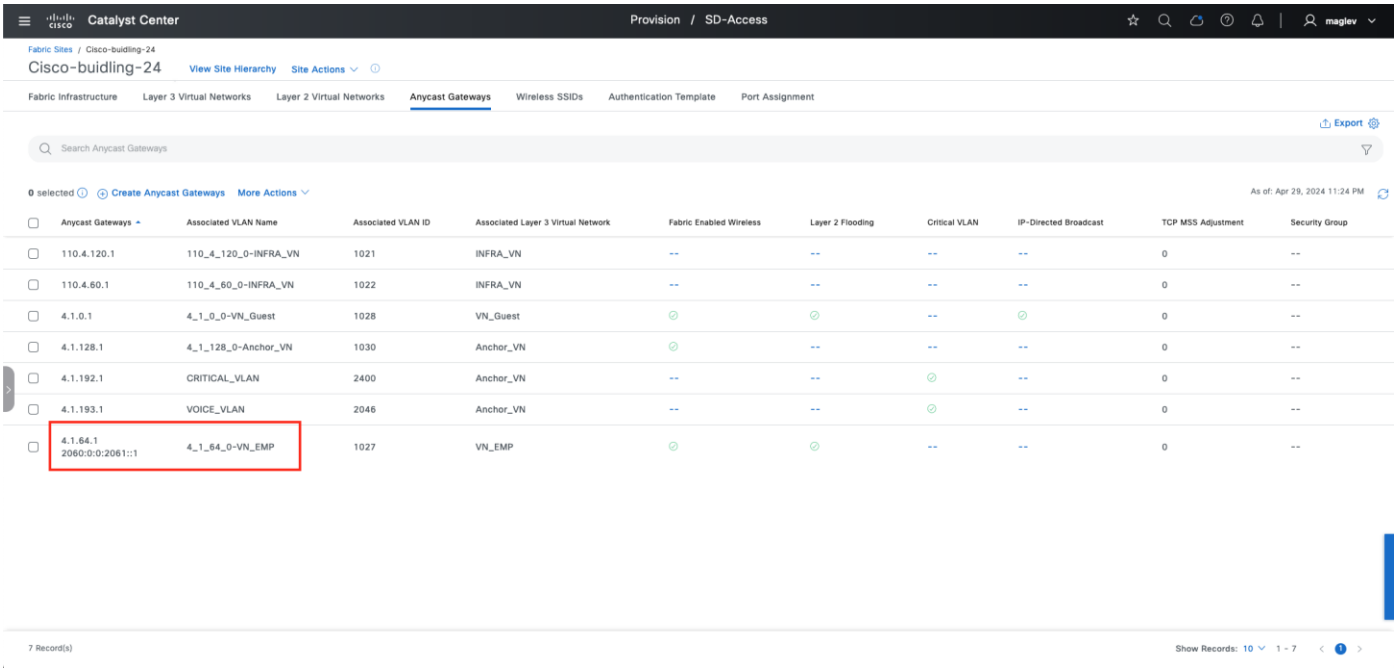



**ステップ 5.**　バナーの [Reconfigure Fabric] をクリックし、[Deploy] をクリックします。

**注：**
1. [Reconfigure Fabric] バナーが表示されると、このサイトでのすべてのファブリック操作がブロックされます。

2. ファブリックゾーンがあり、IP アドレスプールがゾーンで使用されている場合、サイトとゾーンの両方にバナーが表示されます。

**ステップ 6.**　[Anycast Gateway] タブをクリックします。プールはデュアルスタックプールに変換されます。

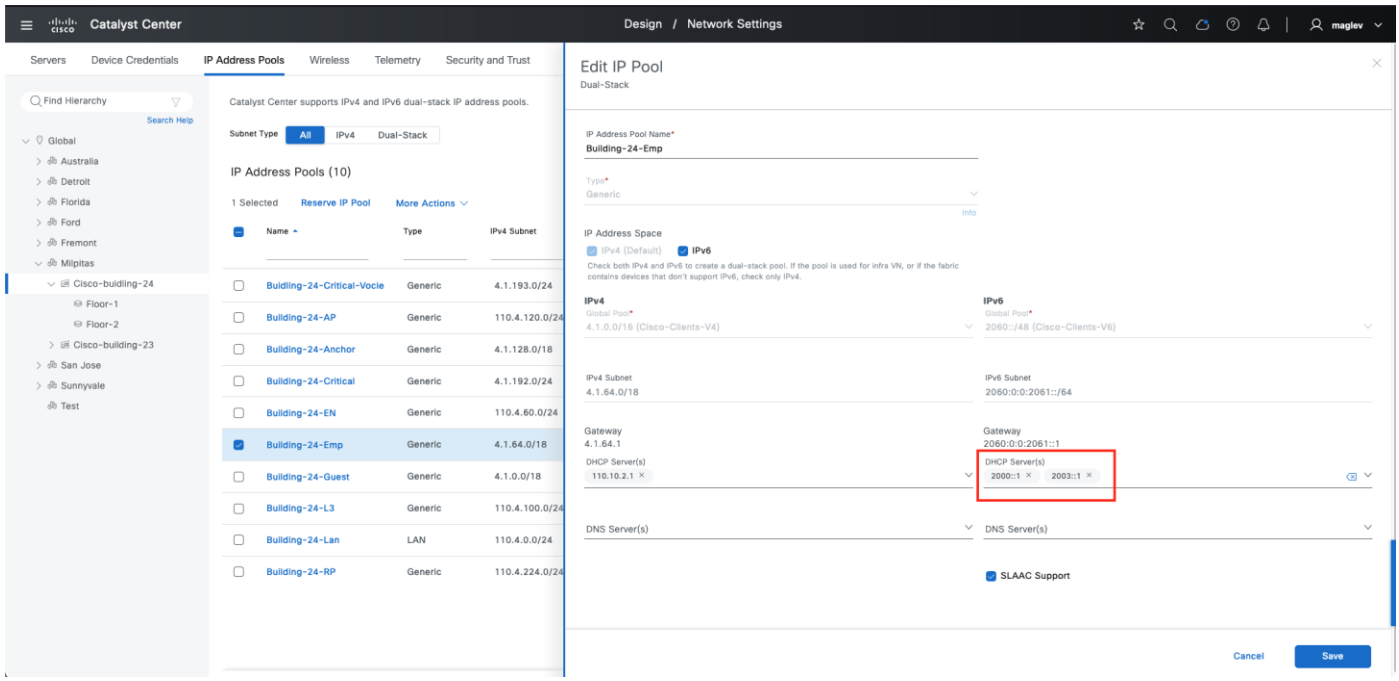


## IP アドレスプール内の DHCP または DNS サーバーの更新

IP アドレスプールの DHCP または DNS を更新すると、同じ再設定バナーが使用されます。

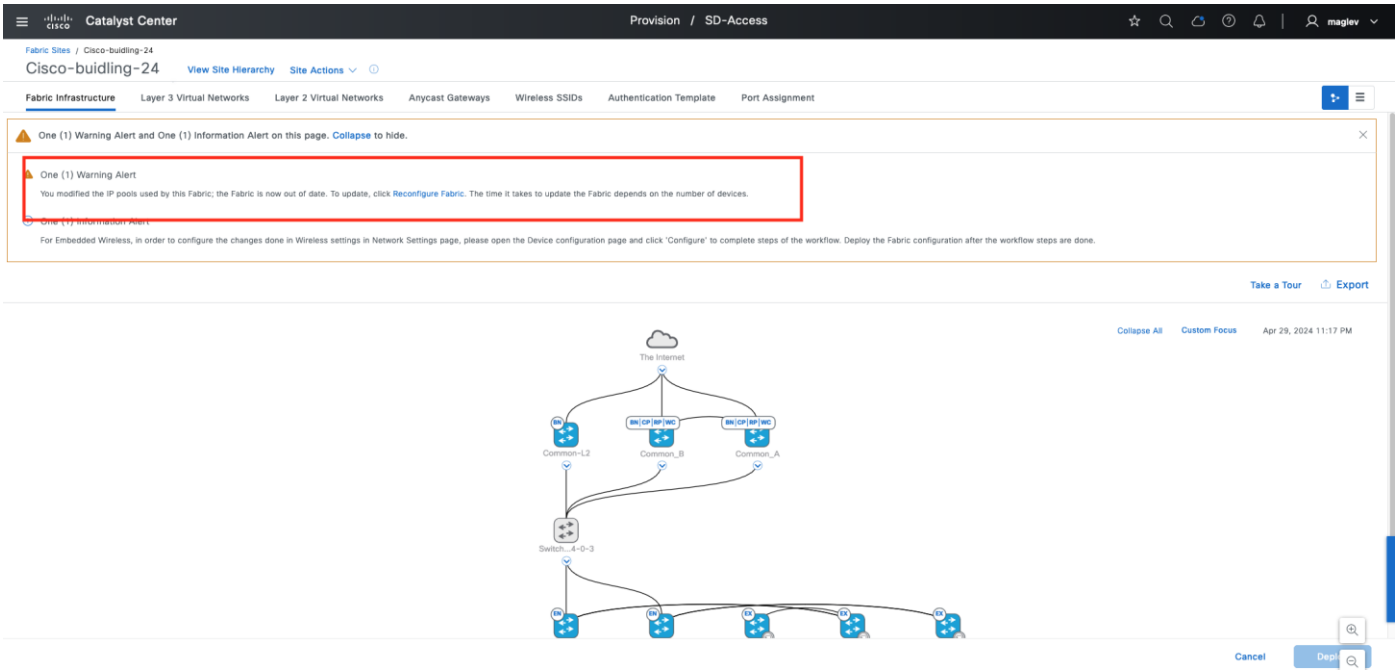
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Design] > [Networking Setting] の順に選択し、[IP Address Pools] タブをクリックします。

**ステップ 2.** [Global] から [Cisco-Buidling-24] に切り替えます。[Building 24-Emp] チェックボックスをオンにして [More Actions] > [Edit] の順に選択し、[DHCP Server(s)] を関連付け、[Save] をクリックします。




**ステップ 3.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、左上のテーブルビューアイコンをクリックして [Cisco-building-24] テキストリンクをクリックし、[Fabric Infrastructure] タブをクリックします。

**図 50.　　ファブリックバナー表示の再設定**

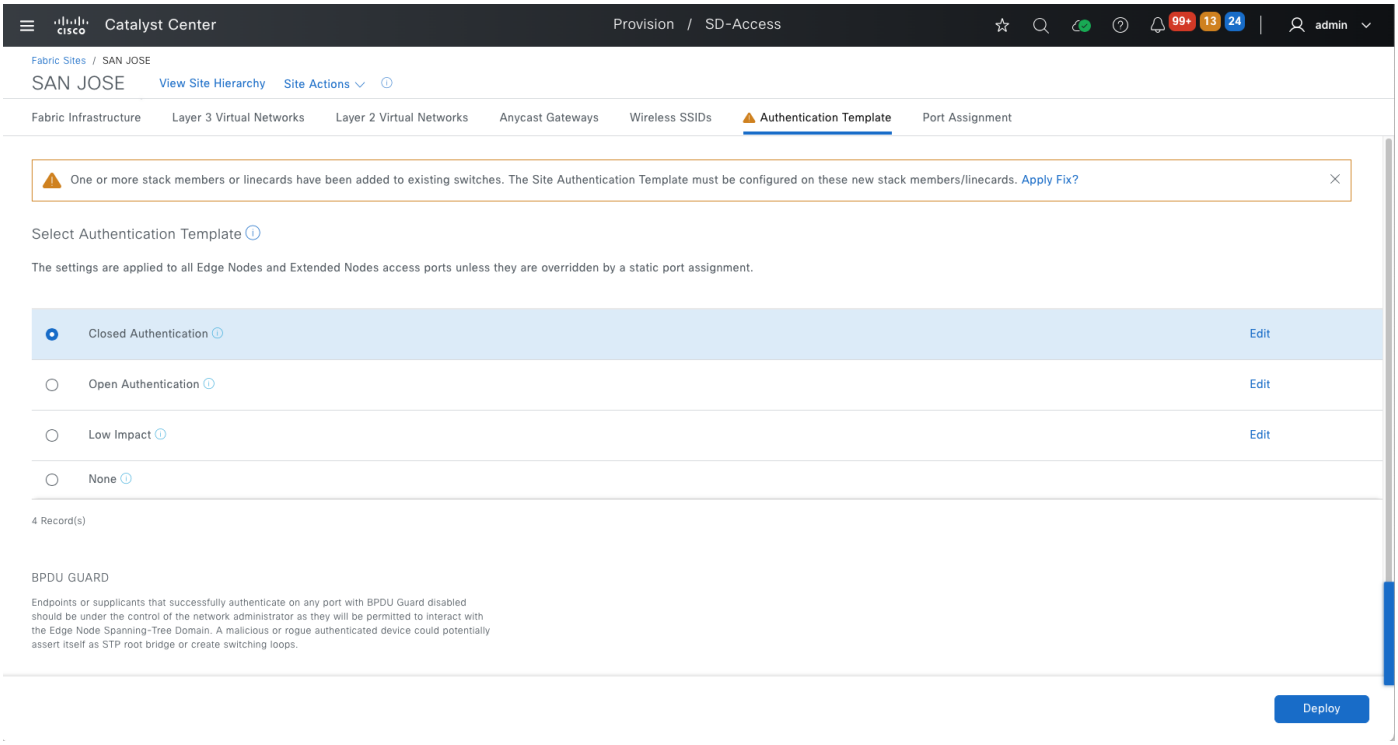



**ステップ 4.** バナーの [Reconfigure Fabric] をクリックし、[Deploy] をクリックします。

### 新しいラインカードのファブリックエッジへの追加

ファブリックエッジデバイスまたは拡張ノードに新しいラインカードまたは新しいスタックメンバーを追加すると、その新しいラインカードまたはスタックメンバーにはアクセスポートへのサイトレベルの認証テンプレートは適用されません（サイトレベルの認証テンプレートの設定が [None] を除くすべての場合）。図 48 に示すように、バナーを適用して、新しいラインカードまたは新しいスタックメンバーのすべてのアクセスポートに認証テンプレートを設定します。

**図 51.　　Catalyst Center に、認証テンプレートを適用するためのバナーが表示される**




**注：**　　このバナーは、ファブリックの動作をブロックすることはありません。

## アップグレードされたクラスタでの移行バナーの使用

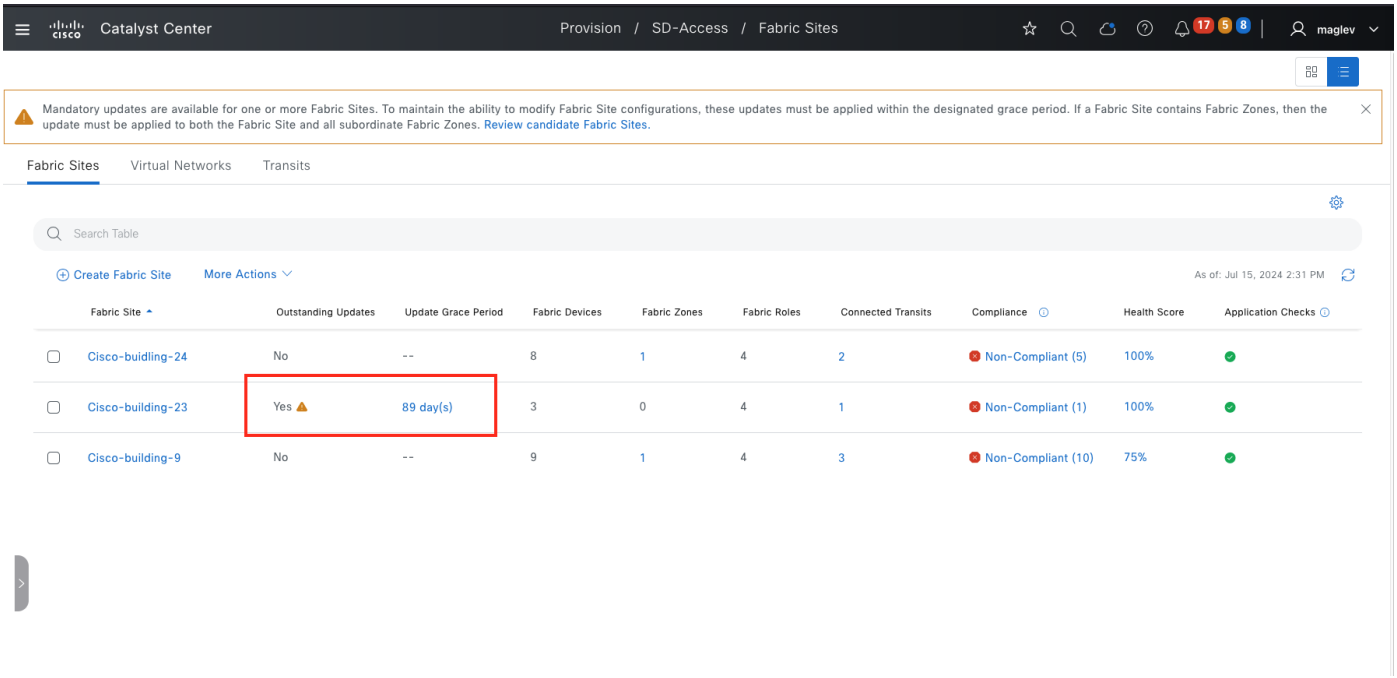
クラスタを新しいリリースにアップグレードすると、Cisco SD-Access ネットワークで重要な修正、動作の変更など、新しい必須の変更が発生する可能性があります。

Catalyst Center では、変更を適用するための移行バナーが用意されています。できるだけ早期に、メンテナンス ウィンドウ アクティビティで変更を適用することをお勧めします。

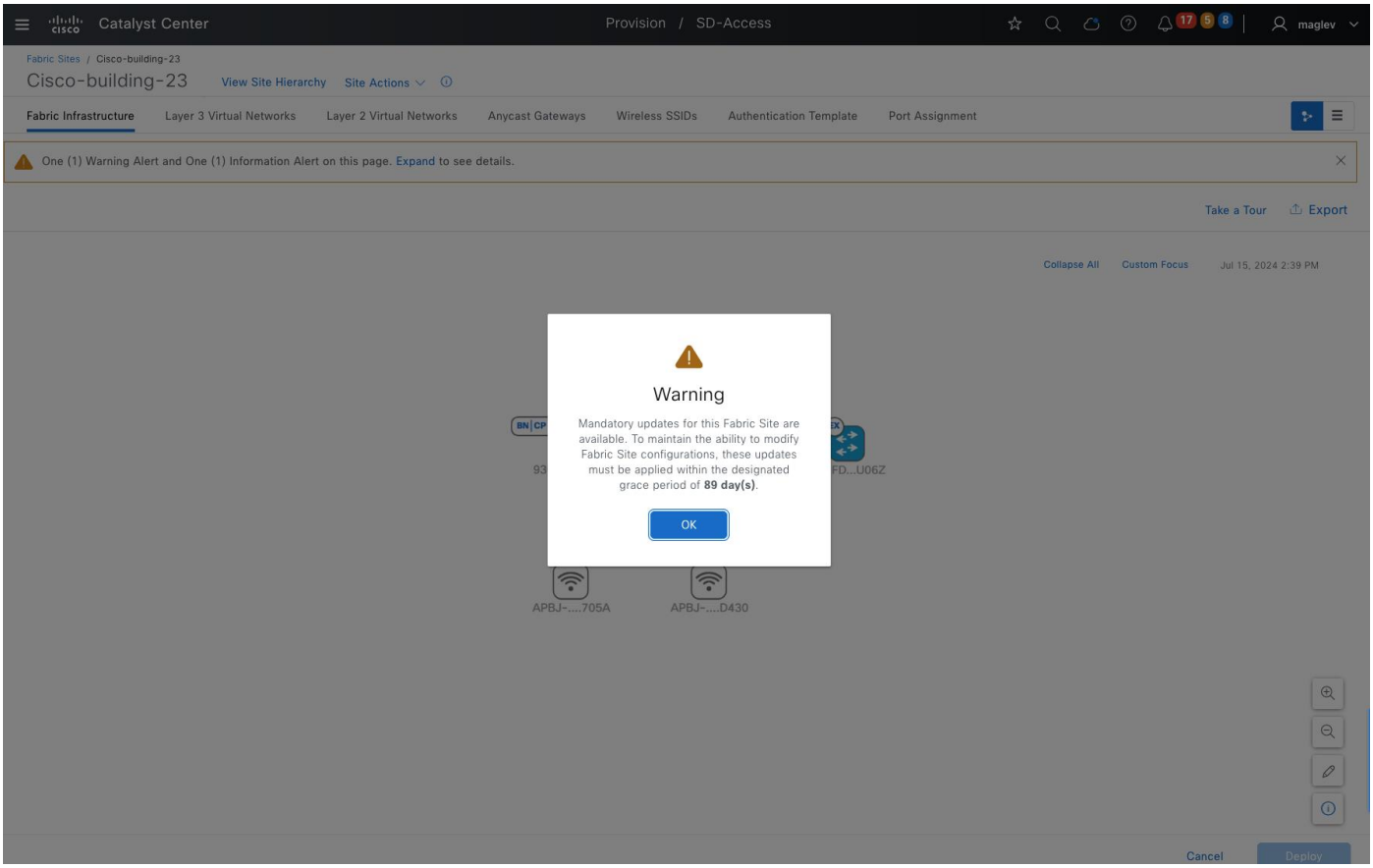
2.3.7.6 以降、移行バナーの適用は必須であり、ネットワーク管理者は 180 日間バナーを適用することができます。180 日が経過すると、すべてのファブリックの動作がブロックされます。

図 49 に示すように、[Fabric Sites] タブのテーブルビューから、必須の更新があり、[Fabric Site]、[Outstanding Updates] と [Update Grace Period] のそれぞれの情報が追加されていることを示すバナーが表示されます。

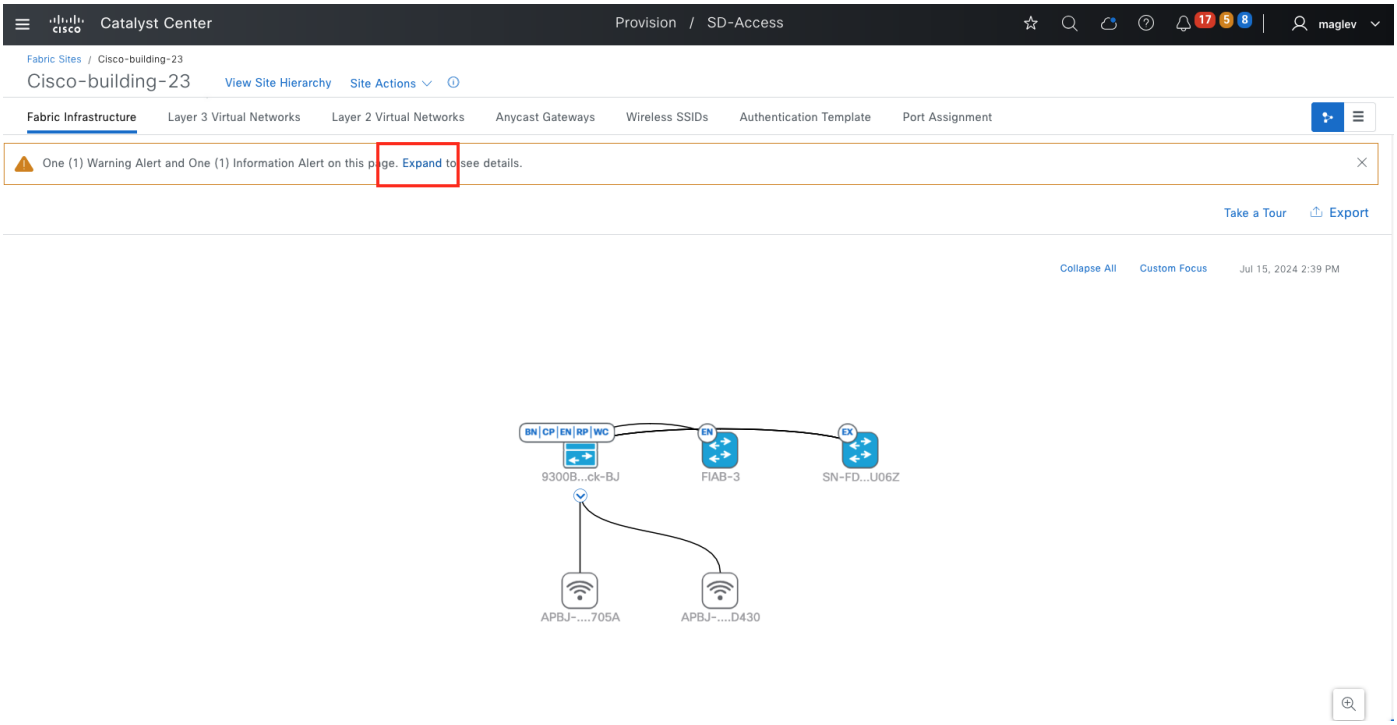
**図 52.　　Cisco-Building-23 に、ファブリックの動作がブロックされる 89 日以内に適用する必要がある必須の変更がある**



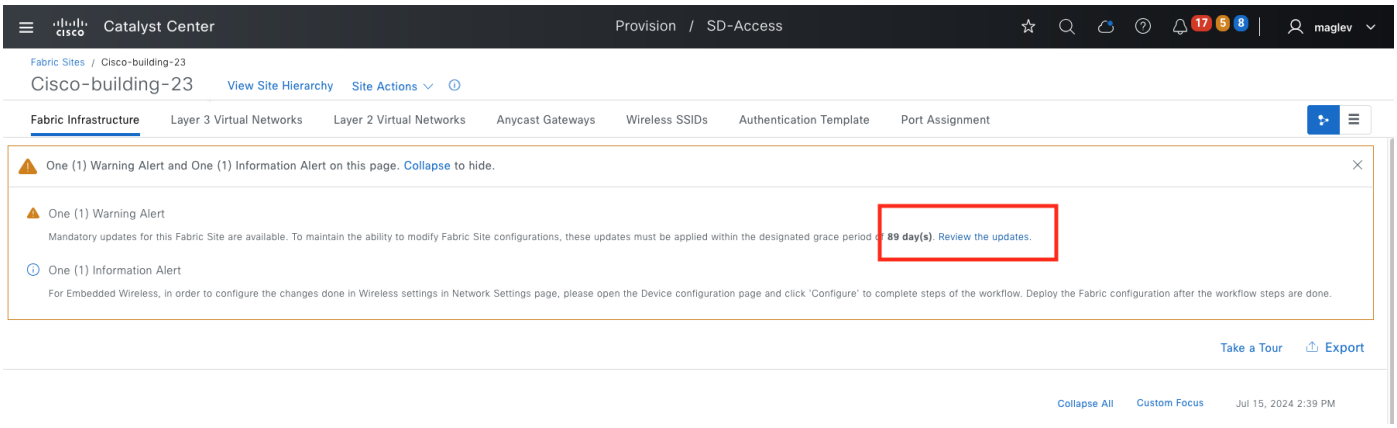

**ステップ 1.** 必須の更新を適用するには、[Cisco-Building-23] をクリックしてから、情報ウィンドウで [OK] をクリックします。



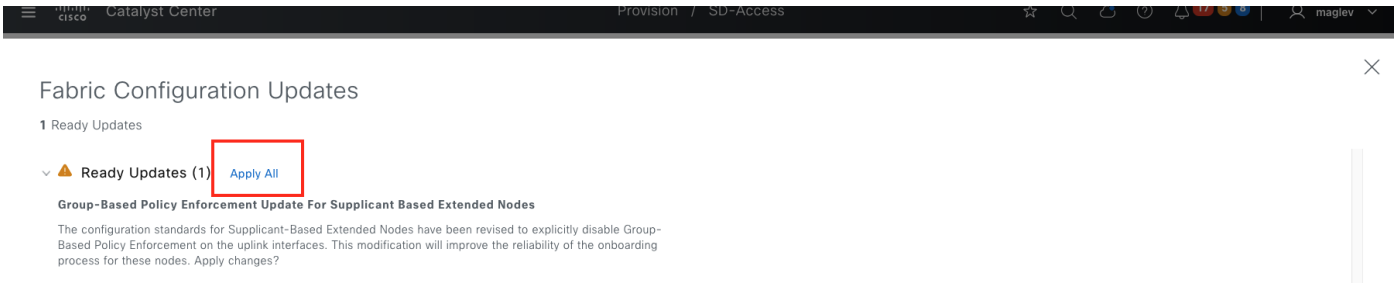
**ステップ 2.** [Expand] をクリックします。




**ステップ 3.** [Review the updates] をクリックします。




**ステップ 4.** このファブリックサイトには更新が 1 つしかないため、[Apply All] をクリックして更新を適用します。



## 障害が発生したデバイスの交換（RMA ワークフロー）

RMA では、ルータ、スイッチ、および AP を共通のワークフローに従って交換できます。ファブリック展開では、RMA ワークフローは次を除くすべてのファブリックデバイスでサポートされます。

- ワイヤレスコントローラが組み込まれたデバイス
- シスコ ワイヤレス コントローラ
- シャーシベース Nexus 7700 シリーズ スイッチ
- スイッチスタック（SVL スタッキング）
- REP リング内のプラットフォーム

Catalyst Center を使用して、障害が発生したデバイスで次の RMA のステップを実行します。

**ステップ 1.** 障害が発生したデバイスを交換対象としてマーク付けします。

**ステップ 2.** デバイスの交換を開始します。

**ステップ 3.** 交換用デバイスを割り当てます。

障害が発生したデバイスと交換用デバイスは、同じ PID と同じモジュールである必要があります。障害が発生したデバイスにアップリンク ネットワーク モジュールがある場合、交換用デバイスにも同じアップリンク ネットワーク モジュールが必要です。

交換用デバイスは、次の 2 つの方法でオンボードできます。

- ワンタッチ方式では、検出またはインベントリインポートを介して交換用デバイスがインベントリに追加されます。
- ゼロタッチ方式では、PnP を介して交換用デバイスをオンボードします。

RMA のステップ 1 の間に、障害が発生したデバイスを交換対象としてマーク付けすると、一時的な DHCP サーバー設定が、Catalyst Center が管理するネイバーデバイスの 1 つにプッシュされます。他のネイバーに接続されたインターフェイスは、これらのネイバー上でシャットダウンされます。交換用デバイスは、PnP を使用してゼロタッチオンボーディングを実行し、この DHCP サーバーから IP を取得できます。

DHCP サーバーの設定は削除され、RMA プロセスが完了すると、Catalyst Center によってインターフェイスが自動的に復元されます。

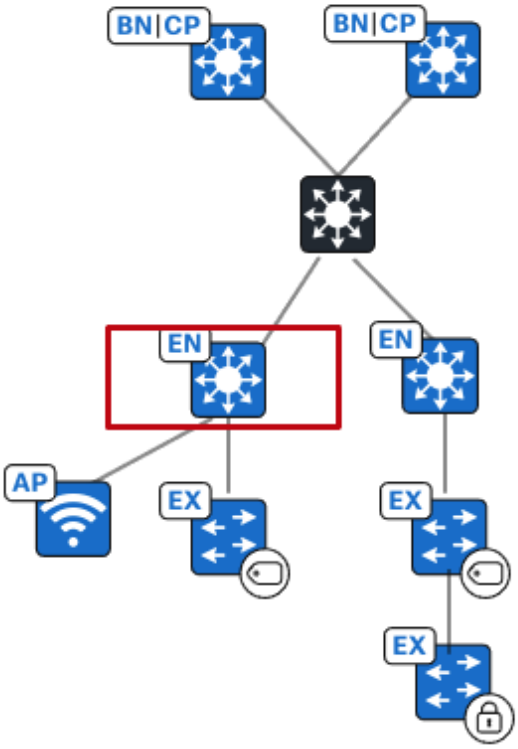
障害が発生した AP または拡張ノードに RMA が必要な場合、一時的な DHCP サーバー設定は必要ありません。交換用 AP と拡張ノードは、AP プールと拡張ノードプールに設定されているのと同じ DHCP サーバーから IP アドレスを受け取ります。その後、PnP プロセスによってオンボーディングされるため、ゼロタッチオンボーディングが可能になります。

交換用デバイスが検出によって追加された場合、またはインベントリに直接インポートされた場合は、そのソフトウェアバージョンが、障害が発生したデバイスと同じであることを確認してください。PnP でオンボードされ、障害が発生したデバイスでゴールデンイメージが実行されている場合、Catalyst Center は SWIM を使用して交換用デバイスをゴールデンイメージにアップグレードします。

このセクションでは、ゼロタッチを使用した RMA 手順に焦点を当てています。ファブリックエッジデバイスの RMA と、コロケーションされたボーダーおよびコントロール プレーン デバイスの RMA は、図 53 に示すトポロジで示されています。ファブリック AP の RMA 手順は、非ファブリック AP の RMA と同じです。「Wireless Automation with Cisco Catalyst Center (CVD)」ガイドを参照してください。

### 交換用デバイスのゼロタッチオンボーディングによるファブリックエッジの RMA

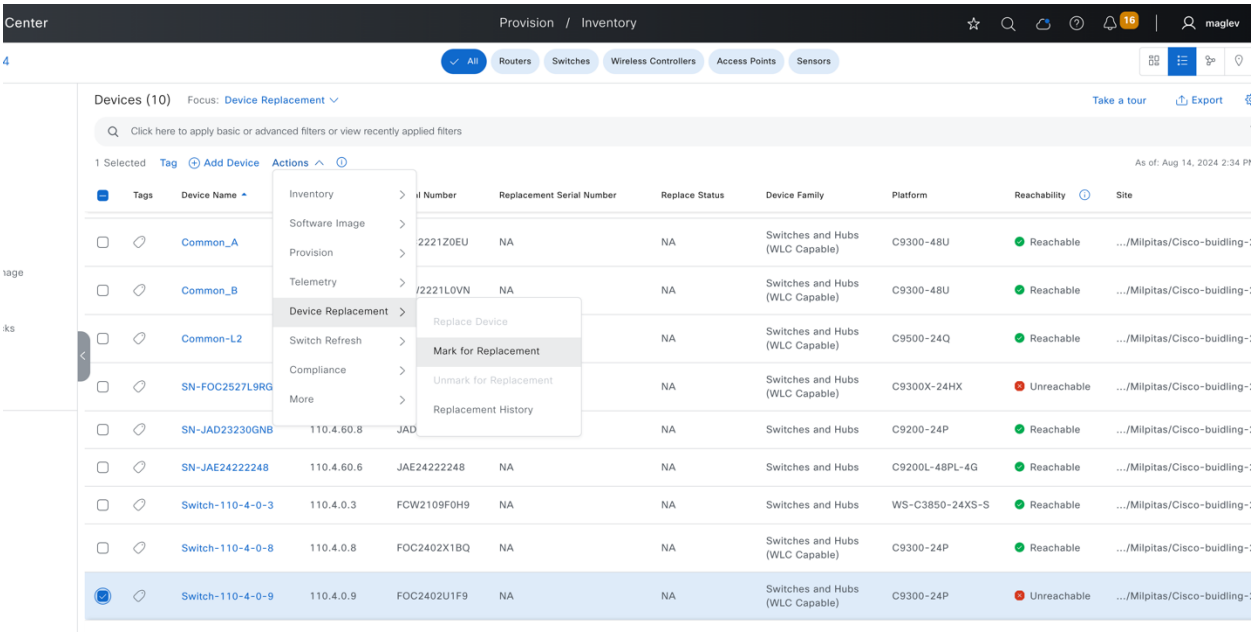
**図 53.　障害が発生したファブリックエッジ（Switch-110-4-0-9）は、アップリンクの中間スイッチ（Switch-110-4-0-3）とダウンリンクの AP およびポリシー拡張ノードに接続されています。**




**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順に選択し、右上のリストビューアイコンをクリックします。

**ステップ 2.** [Focus] を [Device Replacement] に変更します。

**ステップ 3.** [Switch-110-4-0-9] チェックボックスをオンにして、[Actions] > [Device Replacement] > [Mark for Replacement] の順に選択します。



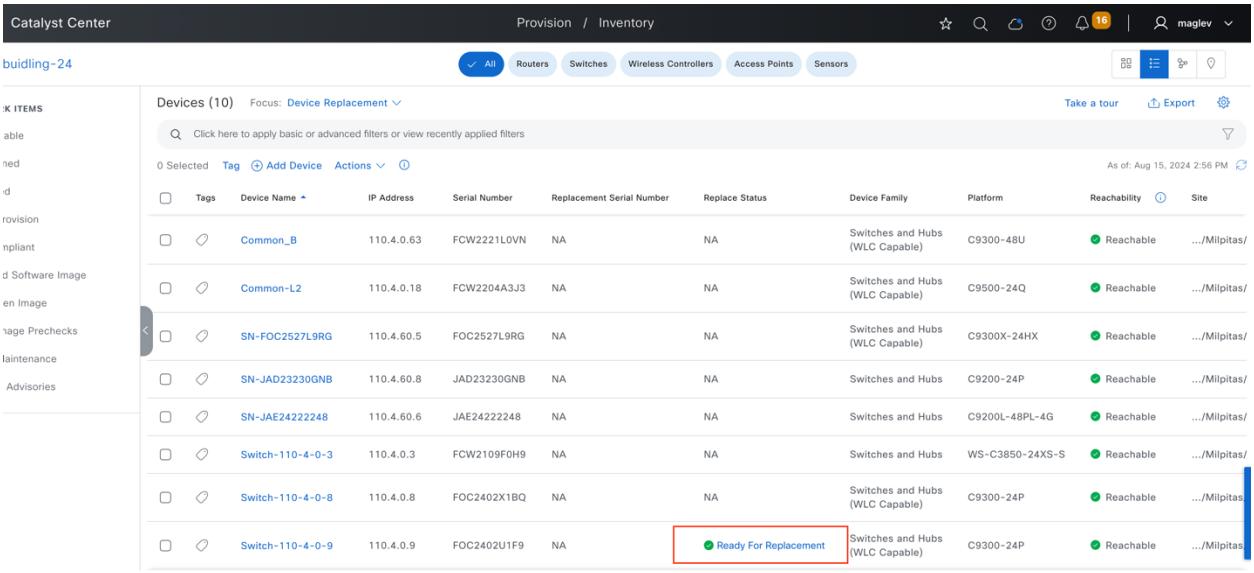

**注：**

1. 障害が発生したデバイスが拡張ノード、AP、または非ファブリックデバイスの場合、ネットワークの準備はスキップされ、[Replace] ステータスが [Ready For Replacement] に変わります。

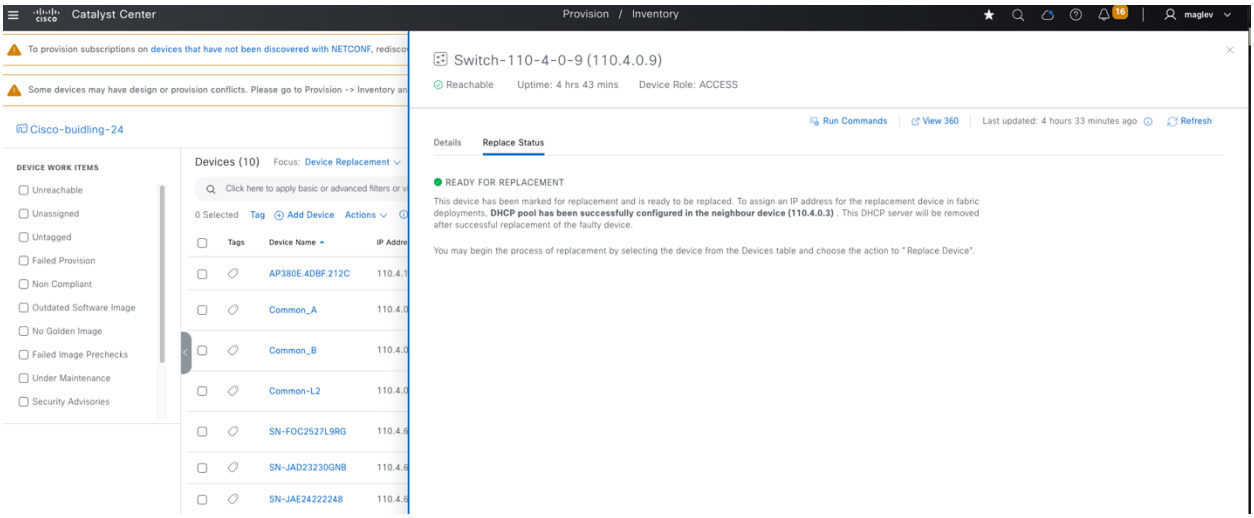
2. ネイバーデバイスが別のファブリックエッジであり、障害が発生したデバイスが拡張ノードでも AP でもない場合、Catalyst Center は DHCP サーバー設定を追加するだけでなく、ネイバーデバイスから PnP VLAN も削除します（PnP VLAN は、拡張ノードプールがアクティブであり、拡張ノードのオンボーディングに使用されるときを設定します）。

3. Catalyst Center 2.3.7.9 以降、障害が発生したデバイスを交換対象としてマーク付けするには、障害が発生したデバイスを [Unreachable] にする必要があります。

ネットワークの準備は、[Mark for Replacement] の操作が完了した後にトリガーされます。DHCP サーバー設定が、ネイバーデバイスにプッシュされます。設定が正常に完了すると、[Replace Status] が [NA] から [Ready For Replacement] に変わります。




**ステップ 4.** [Ready For Replacement] をクリックします。DHCP 設定がネイバー 110.4.0.3 にプッシュされたことを説明するメッセージが表示されます。




**ステップ 5.** ネイバーデバイスからのコンソール出力を確認します。

**図 54.　　Switch-110-4-0-3 DHCP サーバー設定がプッシュされる**

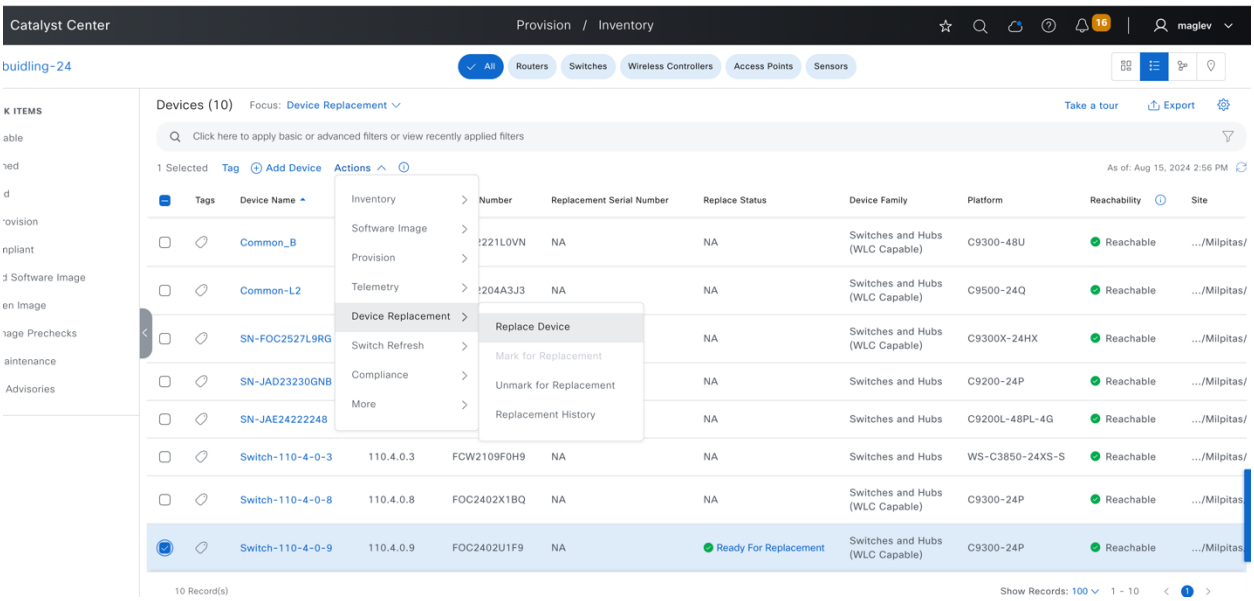
```
Switch-110-4-0-3#
004386: *Aug 15 21:59:40.074: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: solution] [Source: 120.1.1.1] [localport: 22] at 21:59:40 UTC Thu Aug 15 2024
004387: *Aug 15 21:59:40.091: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:!exec: enable
004388: *Aug 15 21:59:40.214: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp excluded-address 110.4.0.1 110.4.0.14
004389: *Aug 15 21:59:40.263: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp excluded-address 110.4.0.16 110.4.0.255
004390: *Aug 15 21:59:40.311: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp pool TenGigabitEthernet1/0/5
004391: *Aug 15 21:59:40.353: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:network 110.4.0.0 255.255.255.0
004392: *Aug 15 21:59:40.399: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:option 43 ascii 5A1D;B2;K4;I120.1.1.1;J80;
004393: *Aug 15 21:59:40.429: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:default-router 110.4.0.14
004394: *Aug 15 21:59:40.446: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:class ciscopnp
004395: *Aug 15 21:59:40.482: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:address range 110.4.0.1 110.4.0.254
004396: *Aug 15 21:59:40.526: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp class ciscopnp
004397: *Aug 15 21:59:40.550: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:option 60 ^ciscopnp
004398: *Aug 15 21:59:40.558: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:exit
```

**ステップ 6.** 交換用スイッチを中間スイッチの同じポートに接続します。交換用デバイスが、PnP オンボーディングを開始します。

**ステップ 7.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Plug and Play] の順に選択し、[Unclaimed] タブをクリックします。

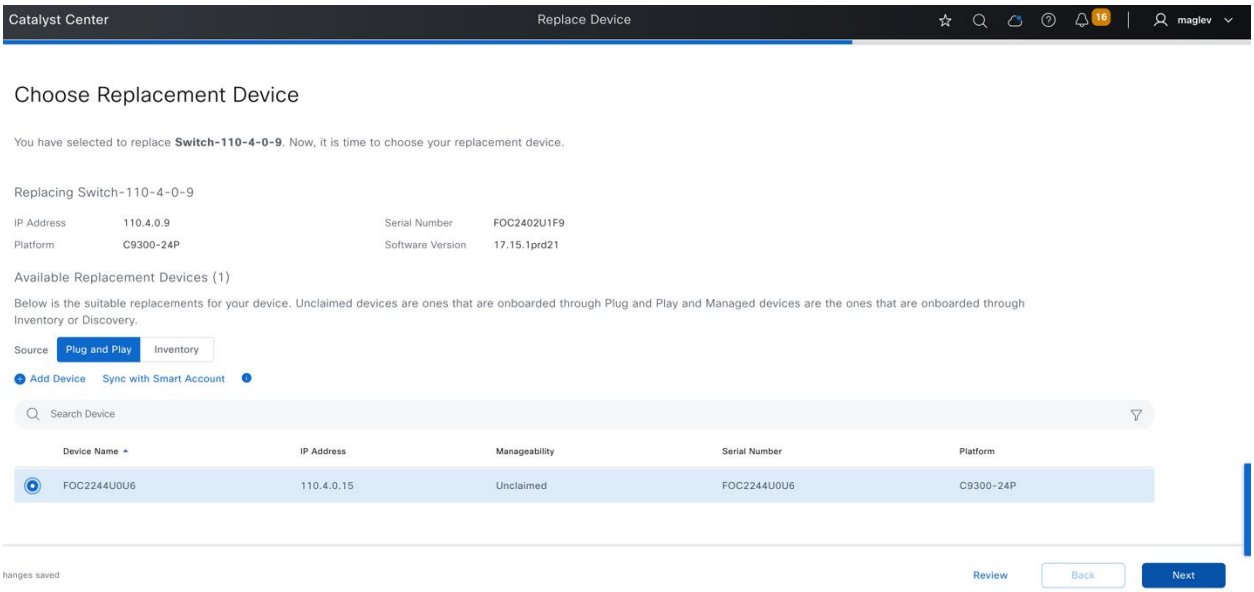
**ステップ 8.** 新しいデバイスが表示され、オンボーディングステータスに [Device is ready to be claimed] と表示されたら、[Inventory] ウィンドウに戻って、RMA を開始します。左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順に選択し、右上のリストビューアイコンをクリックして [Focus] を [Device Replacement] に変更します。

**ステップ 9.** [Switch-110-4-0-9] チェックボックスをオンにし、[Actions] > [Device Replacement] > [Replace Device] の順に選択します。

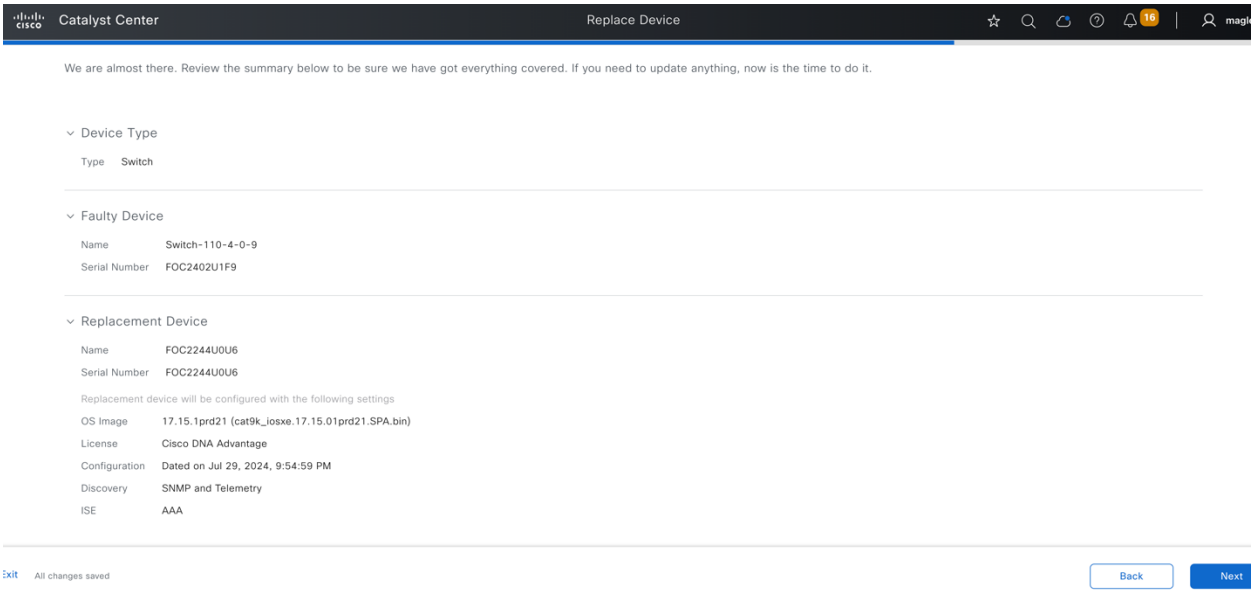



**ステップ 10.** ゼロタッチオンボーディングを実行するワークフローで、[Plug and Play] タブをクリックします。交換用デバイスは、Catalyst Center に接続すると表示されます。

**ステップ 11.** デバイスを選択して [Next] をクリックします。




**ステップ 12.** タスクの概要を確認して [Next] をクリックします。




**ステップ 13.** 設定のプレビューはサポートされます。交換用デバイスにプッシュする設定を確認し、[Deploy] をクリックして設定をプッシュします。

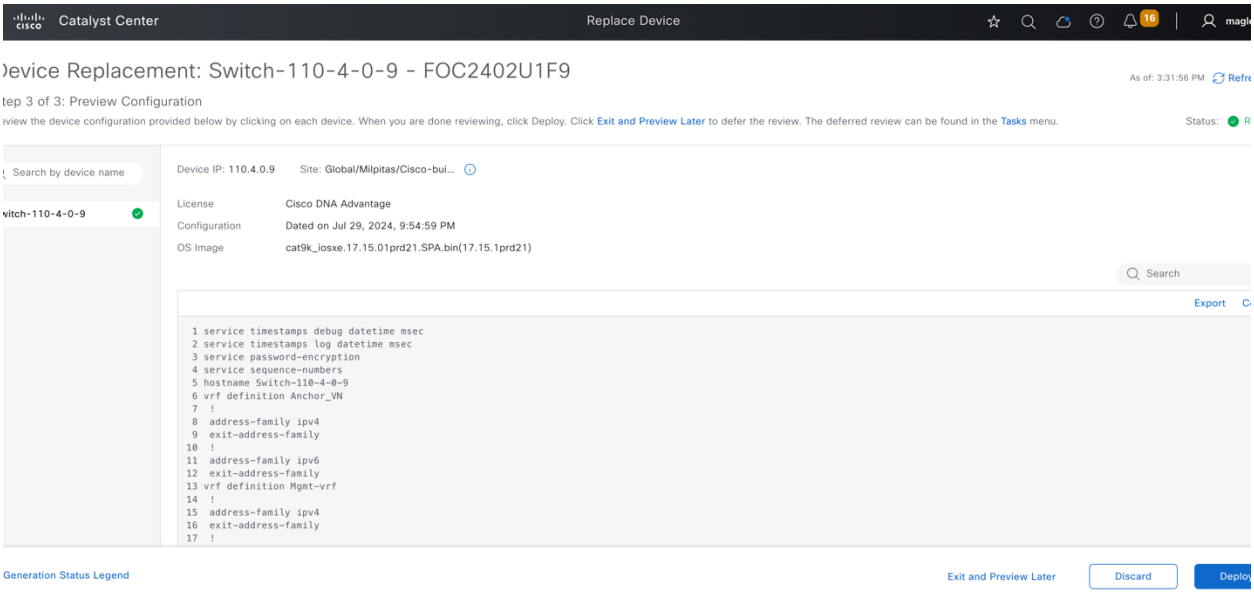
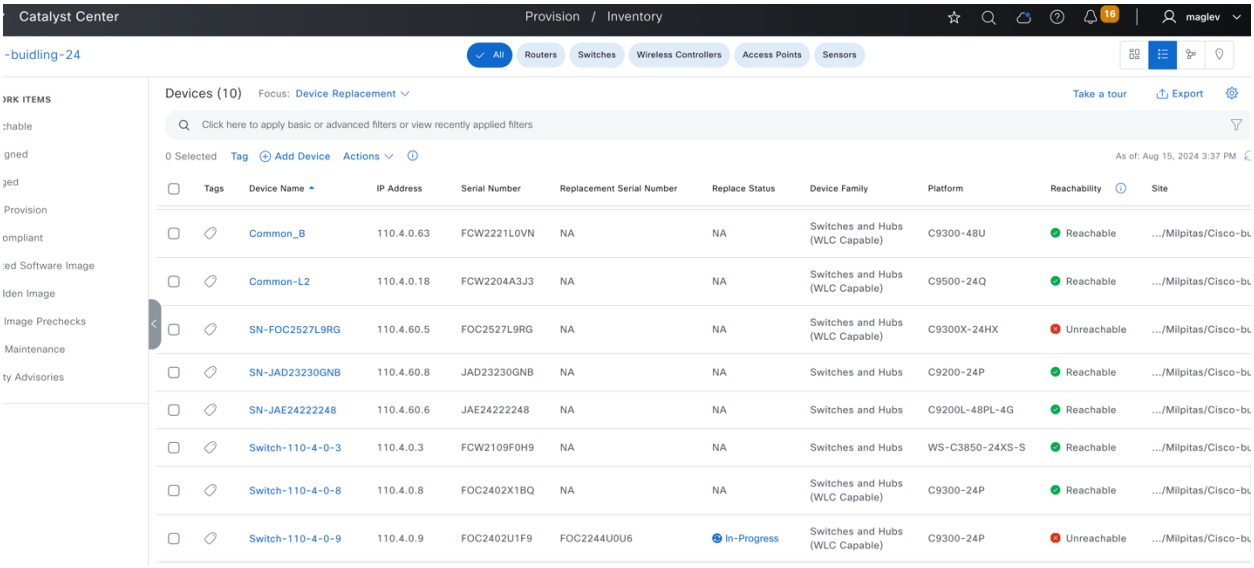
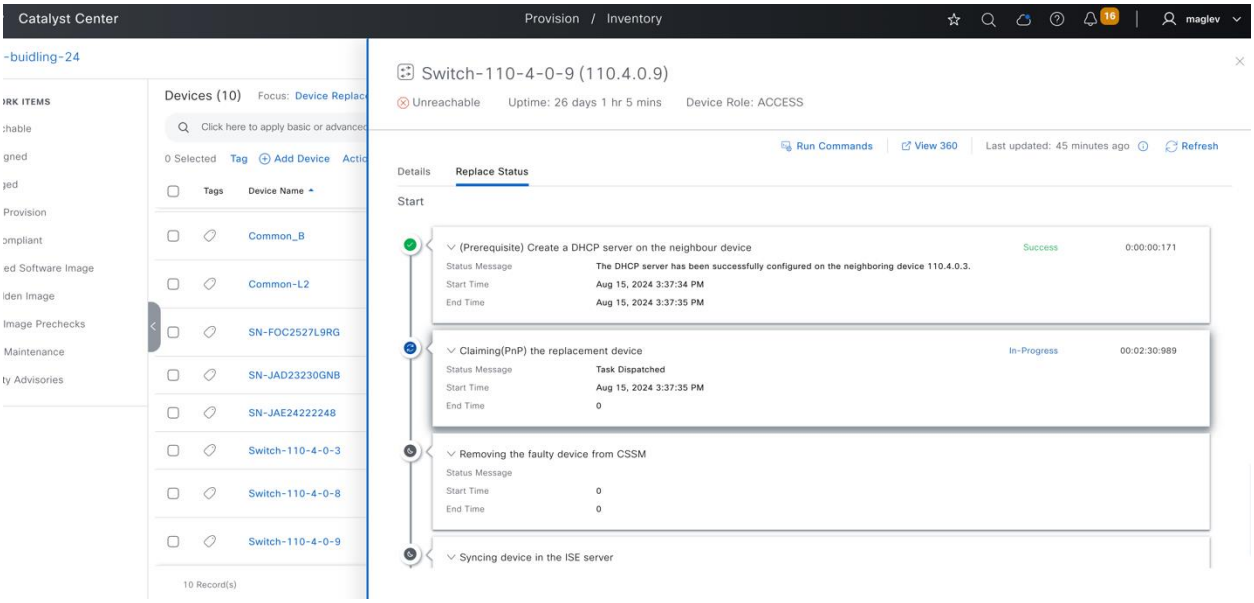


**図 55.　　[Replace Status] に [In-progress] と表示される**

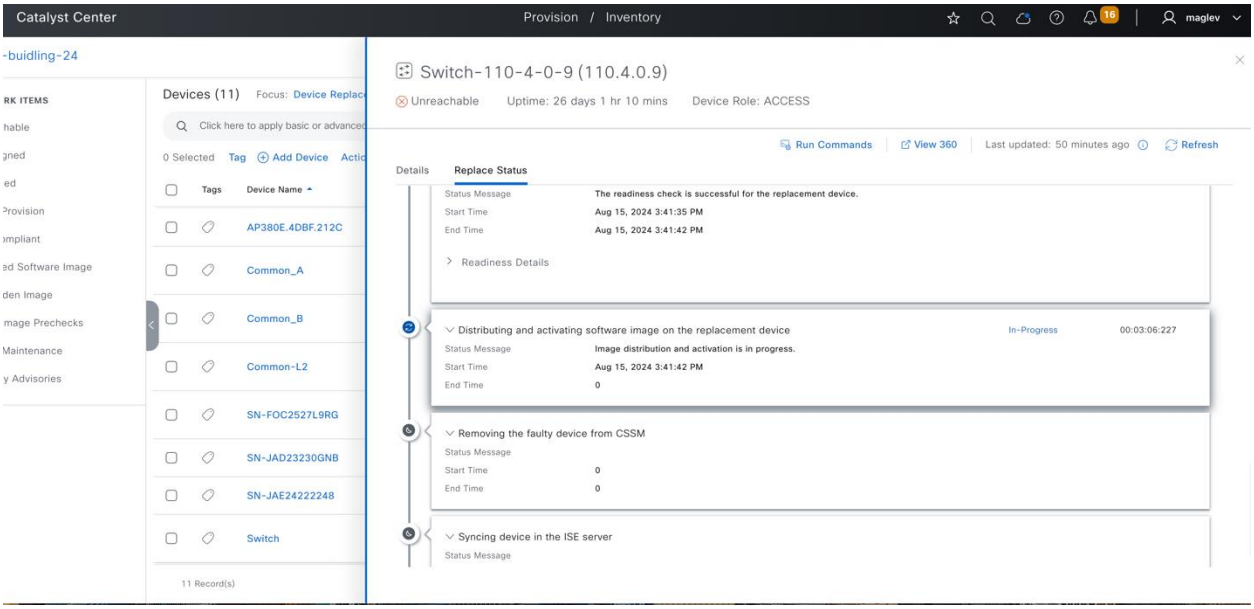



**ステップ 14.** RMA の進捗を監視するには、[In-Progress] をクリックし、スライドインペインでタスクのステータスを確認します。




**ステップ 15.** 交換用デバイスが障害が発生したデバイスと同じイメージを実行していない場合、Catalyst Center は交換用デバイスをゴールデンイメージにアップグレードします。障害が発生したデバイスのイメージが**ゴールデン**としてマーク付けされていることを確認します。

**図 56.　　ステータスに、進行中のイメージのアップグレードが表示される**




**ステップ 16.** RMA が完了するまで待ちます。[Replace Status] が [NA] に変わります。

**ステップ 17.** [Actions] > [Device Replacement] > [Replacement History] の順に選択します。

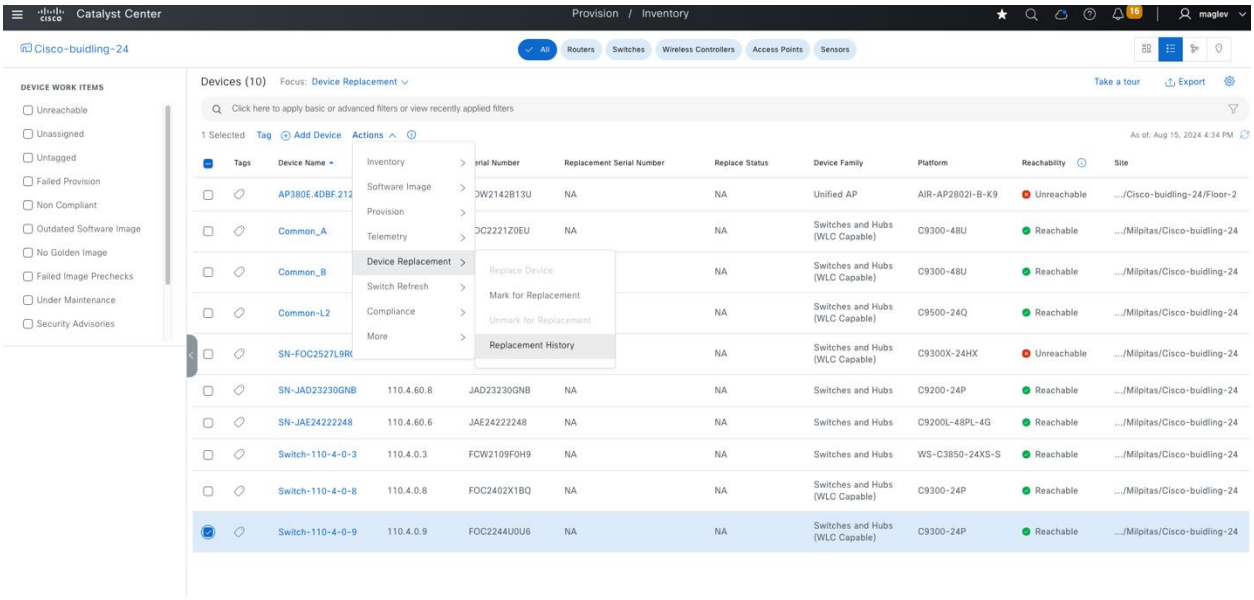
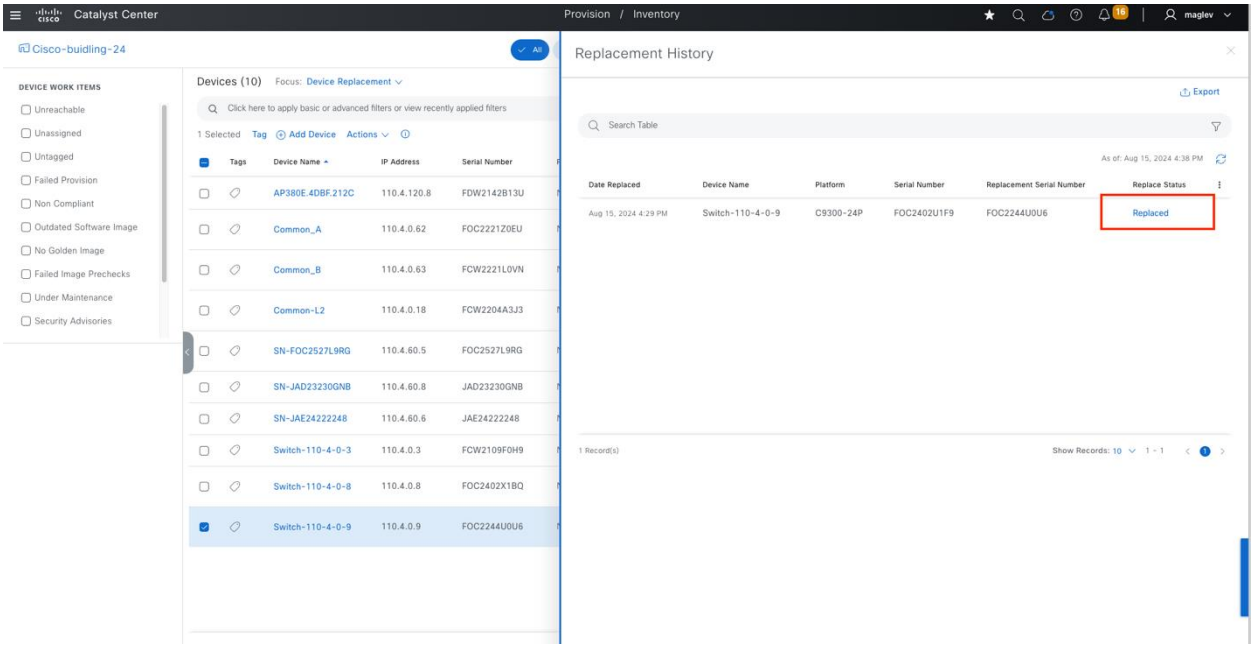


**図 57.　　[Replace Status] に [Replaced] と表示される**



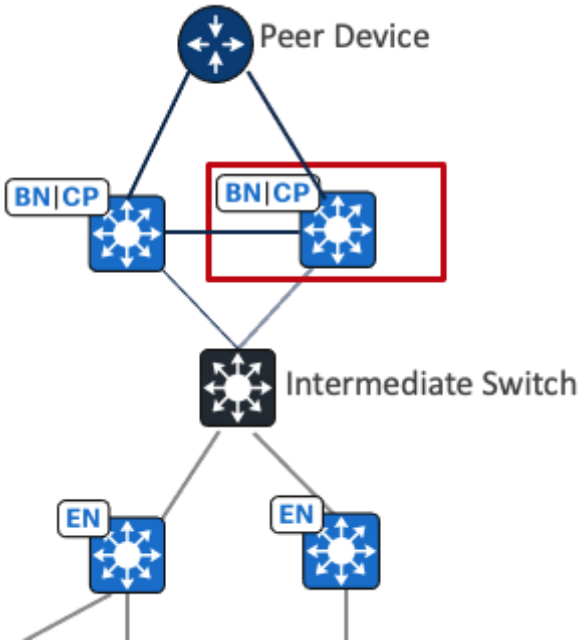

**ステップ 18.** ネイバーデバイスで、DHCP サーバーの設定が削除されたことを確認します。

```
004551: *Aug 15 23:30:47.014: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp excluded-address 110.4.0.1 110.4.0.14
004552: *Aug 15 23:30:47.062: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp excluded-address 110.4.0.16 110.4.0.255
004554: *Aug 15 23:30:49.106: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp pool TenGigabitEthernet1/0/5
004555: *Aug 15 23:30:49.159: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp class ciscopnp
```

**ステップ 19.** 障害が発生したデバイスと同じポートを使用して、すべての拡張ノード、すべての AP、クライアントなど、他の接続を再開します。

### ゼロタッチオンボーディングでコロケーションしたボーダーおよびコントロール プレーン デバイスの RMA

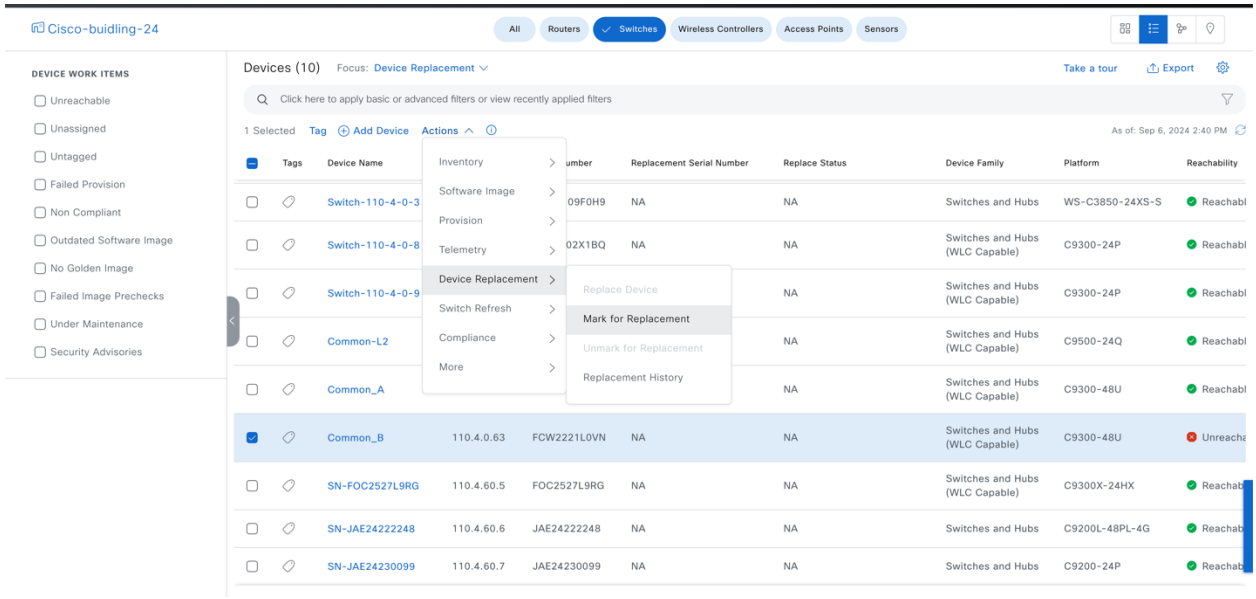
コントロールプレーンとコロケーションしたボーダーの RMA は、ファブリックエッジデバイスの RMA に似ています。コントロールプレーン（**Common_B**）で障害が発生したファブリックボーダーは、中間スイッチ（**Switch-110-4-0-3**）、**Common_A**、およびピアデバイスに接続されています。




**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順に選択し、右上のリストビューアイコンをクリックします。

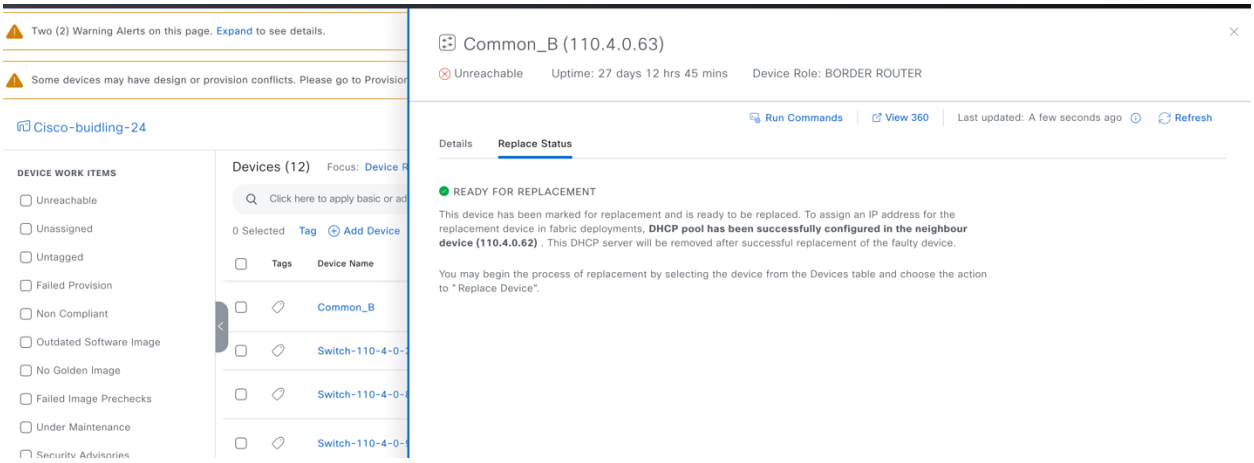
**ステップ 2.** [Focus] を [Device Replacement] に変更します。

**ステップ 3.** [Common_B] チェックボックスをオンにしてから、[Actions] > [Device Replacement] > [Mark for Replacement] の順に選択します。




ネットワークの準備は、DHCP サーバー設定をアップリンク ネイバー デバイスにプッシュします。

**図 58.　DHCP 設定が 110.4.0.62 Common_A にプッシュされる例**



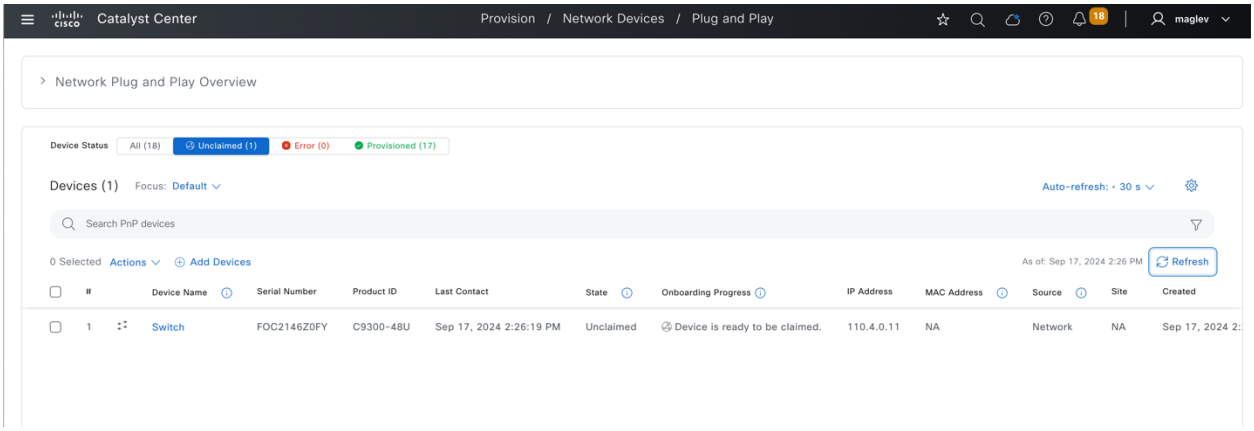

**ステップ 4.**　**Common_A** デバイスで確認します。

```
047919: Sep 17 23:14:50.906: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:!exec: enable
047920: Sep 17 23:14:50.997: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp excluded-address 110.4.0.1 110.4.0.10
047921: Sep 17 23:14:51.037: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp excluded-address 110.4.0.12 110.4.0.255
047922: Sep 17 23:14:51.064: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp pool GigabitEthernet1/0/25
047923: Sep 17 23:14:51.088: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:network 110.4.0.0 255.255.255.0
047924: Sep 17 23:14:51.122: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:option 43 ascii 5A1D;B2;K4;I120.1.1.1;J80;
047925: Sep 17 23:14:51.144: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:default-router 110.4.0.10
047926: Sep 17 23:14:51.156: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:class ciscopnp
047927: Sep 17 23:14:51.182: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:address range 110.4.0.1 110.4.0.254
047928: Sep 17 23:14:51.198: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:ip dhcp class ciscopnp
047929: Sep 17 23:14:51.219: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:option 60 ^ciscopnp
047930: Sep 17 23:14:51.224: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:exit
```

**ステップ 5.**　交換用スイッチを **Common_A** の同じポート、ピアデバイス、および中間スイッチに接続します。新しいスイッチで PnP オンボーディングが開始します。

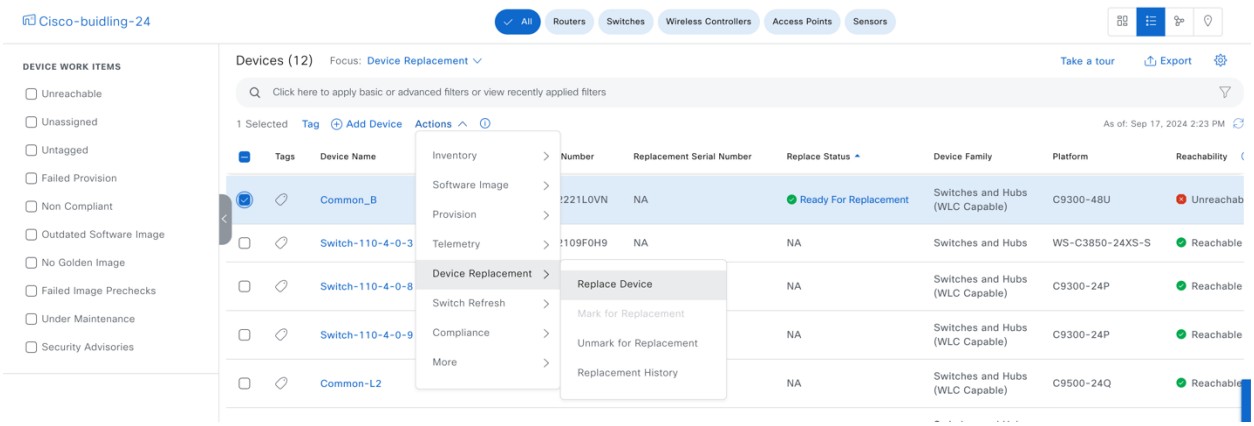
**ステップ 6.**　[Plug and Play] ウィンドウを監視します。

**ステップ 7.**　左上隅にあるメニューアイコンをクリックして [Provision] > [Plug and Play] の順に選択し、[Unclaimed] をクリックします。

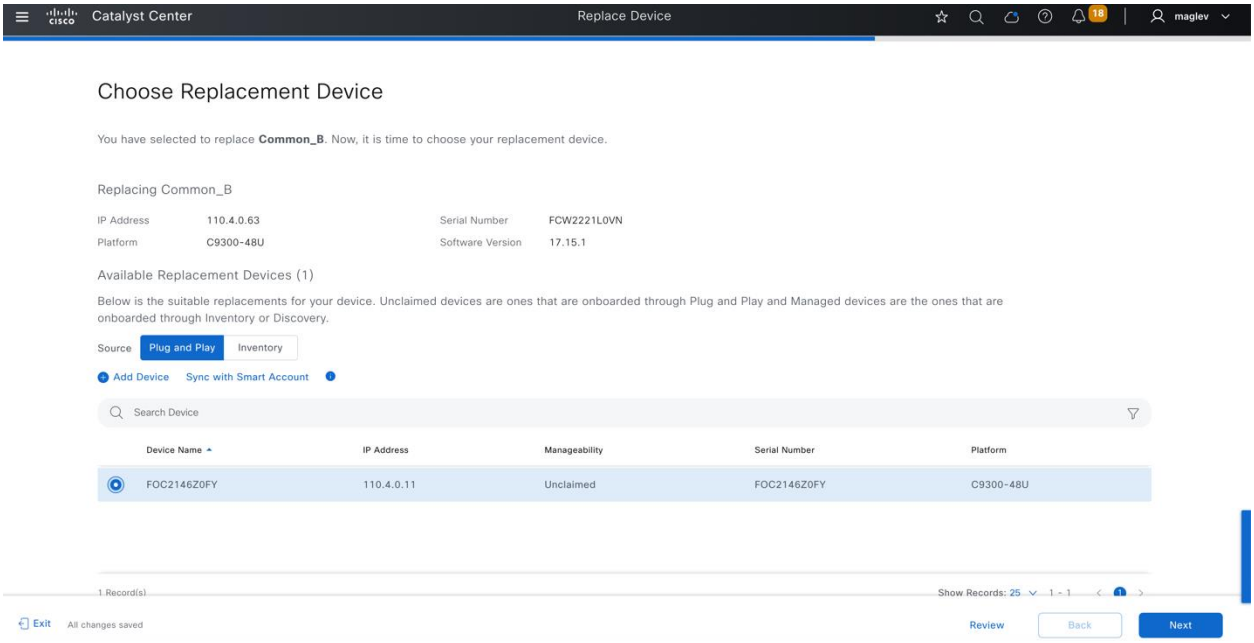



**ステップ 8.**　新しいデバイスが表示され、オンボーディングステータスに [Device is ready to be claimed] と表示されたら、戻って RMA を開始します。左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順に選択し、右上のリストビューアイコンをクリックして [Focus] を [Device Replacement] に変更します。

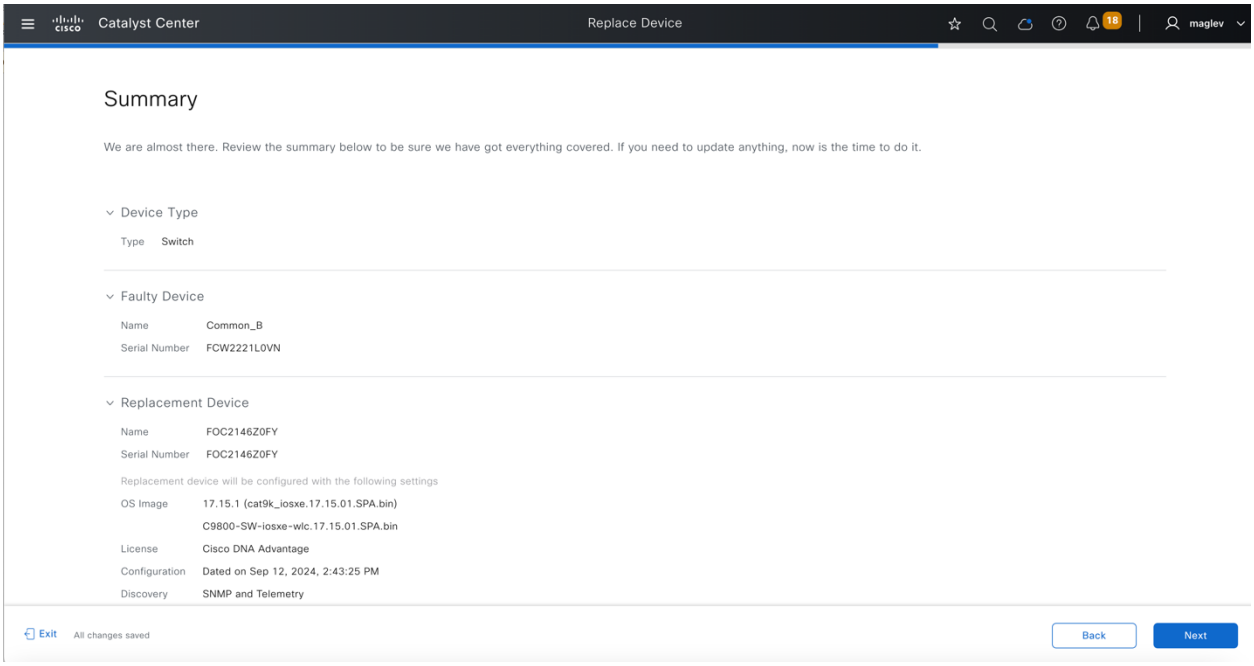
**ステップ 9.** [Common_B] チェックボックスをオンにしてから、[Actions] > [Device Replacement] > [Replace Device] の順に選択します。




**ステップ 10.** ゼロタッチ オンボーディング ワークフローで、[Plug and Play] タブをクリックし、交換用デバイスのオプションボタンをクリックしてから、[Next] をクリックします。



**ステップ 11.** タスクの概要を確認して [Next] をクリックします。




**ステップ 12.** 交換用デバイスにプッシュする設定を確認し、[Deploy] をクリックして設定をプッシュします。

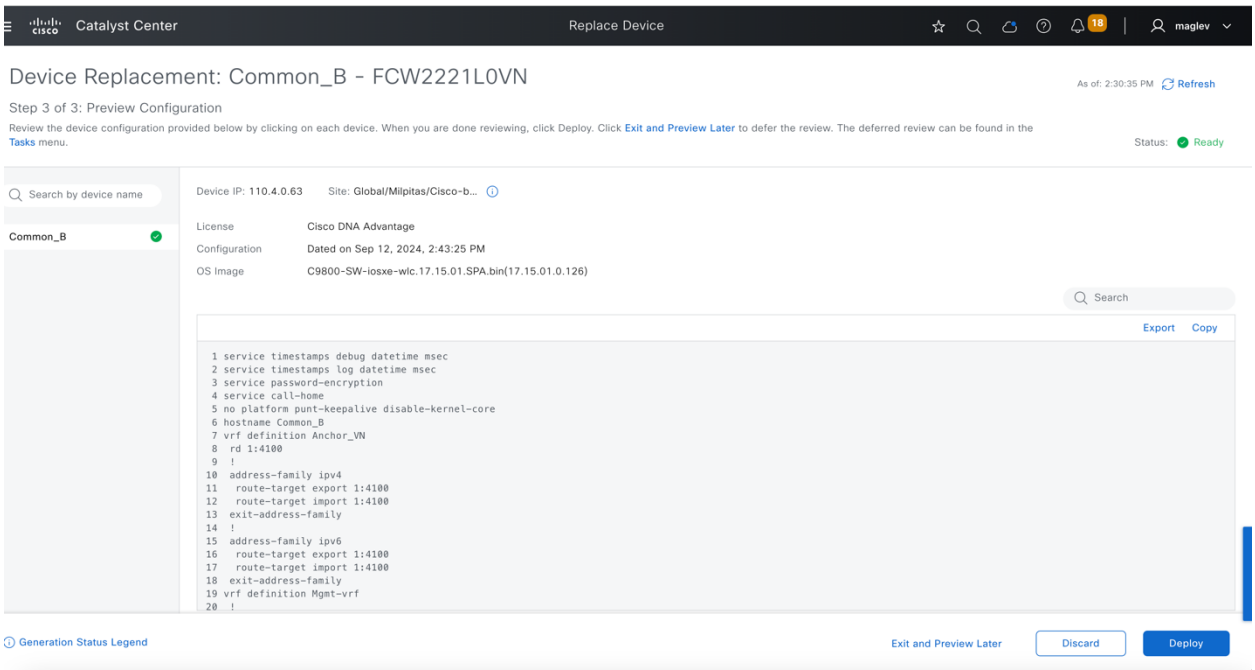
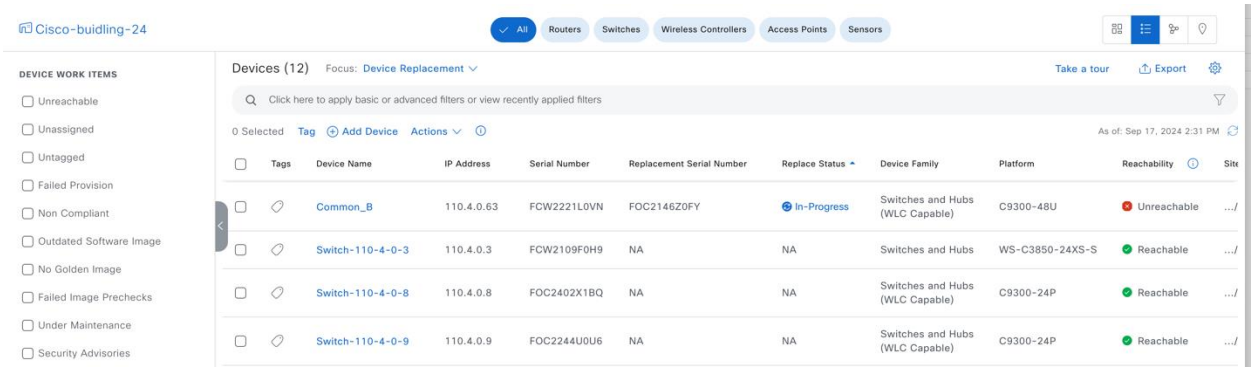
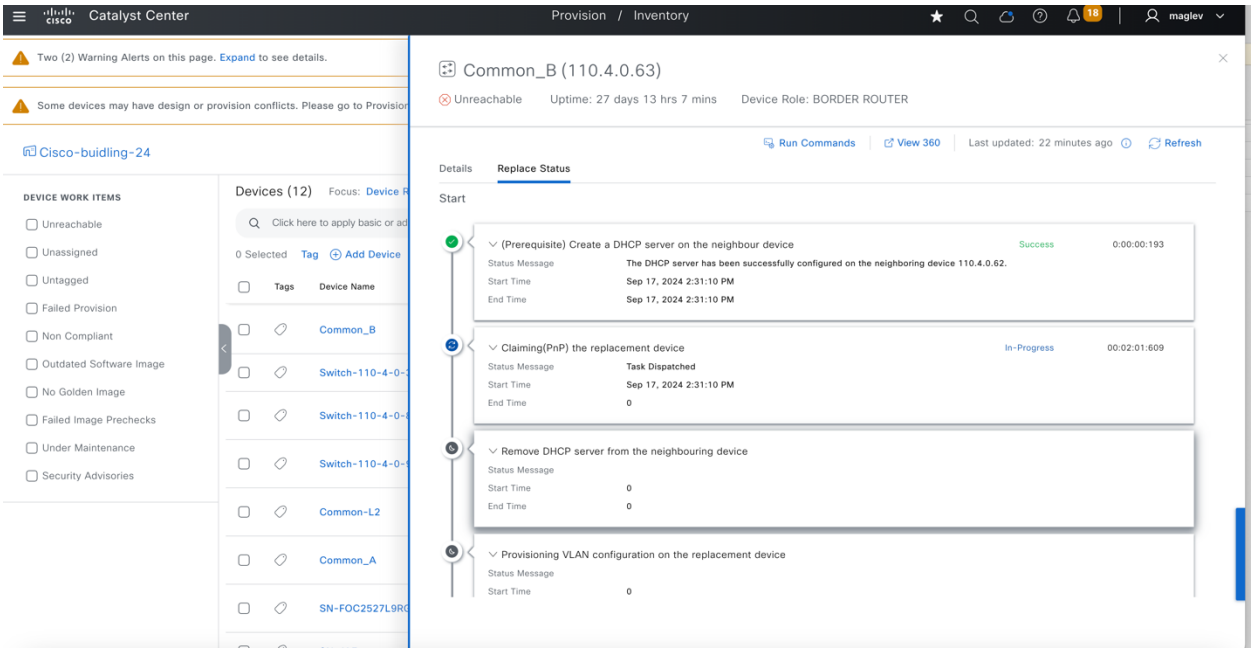


**図 59.　[Replace Status] に [In-progress] と表示される**

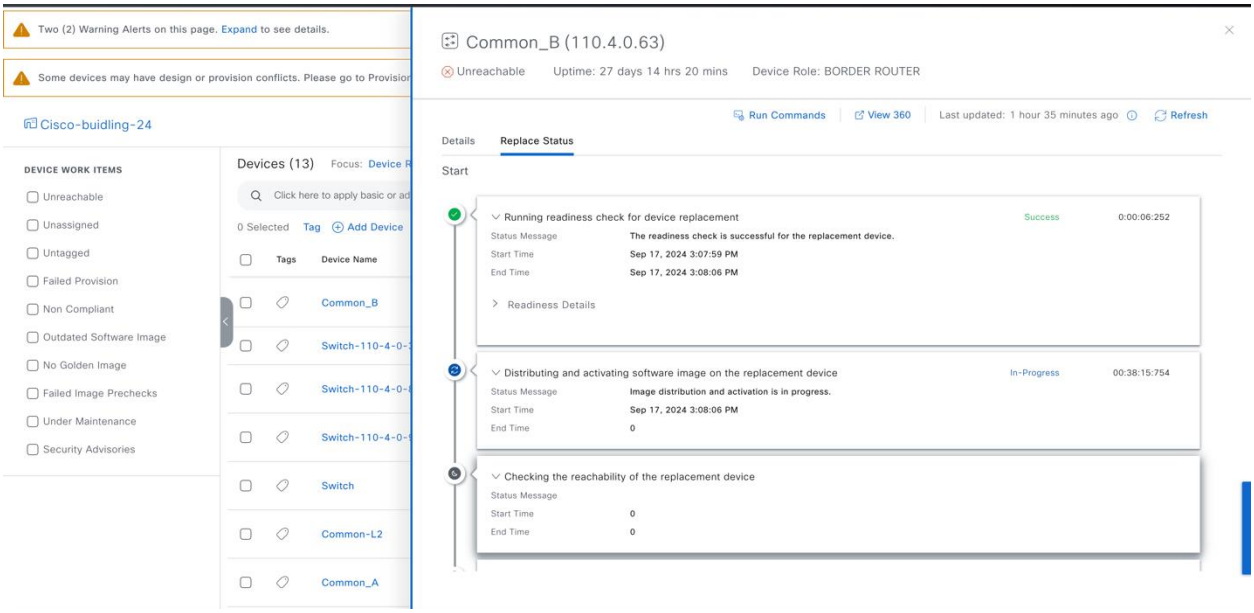



**ステップ 13.** RMA の進捗を監視するには、[In-Progress] をクリックし、スライドインペインでタスクのステータスを確認します。




**ステップ 14.** 交換用デバイスが障害が発生したデバイスと同じイメージを実行していない場合、Catalyst Center は交換用デバイスをゴールデンイメージにアップグレードします。障害が発生したデバイスのイメージが**ゴールデン**としてマーク付けされていることを確認します。

**図 60.　　[Replace Status] に、進行中のイメージのアップグレードが表示される**




**ステップ 15.**　RMA が完了するまで待ちます。[Replace Status] が [NA] に戻ります。[Actions] > [Replacement History] の順にクリックします。

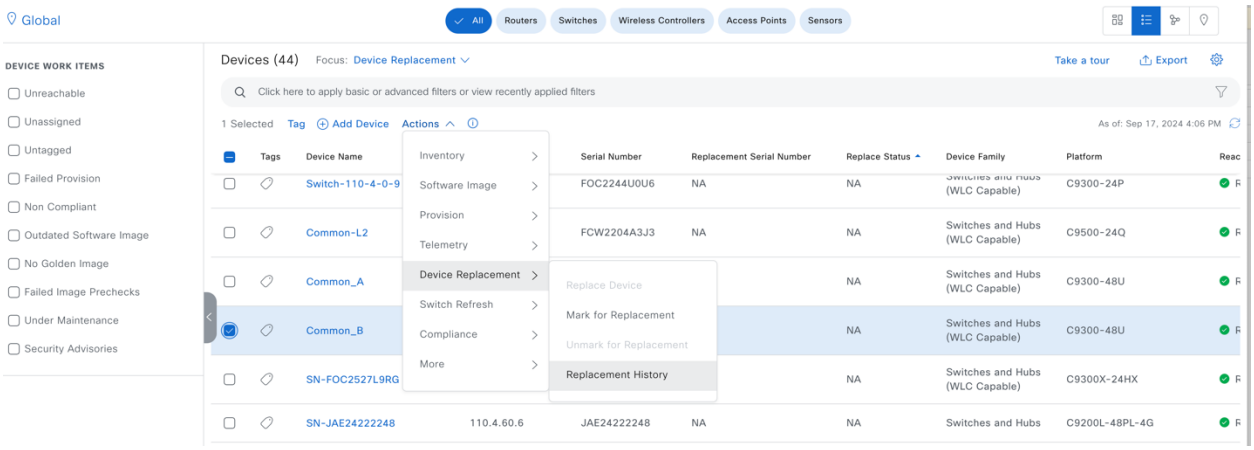
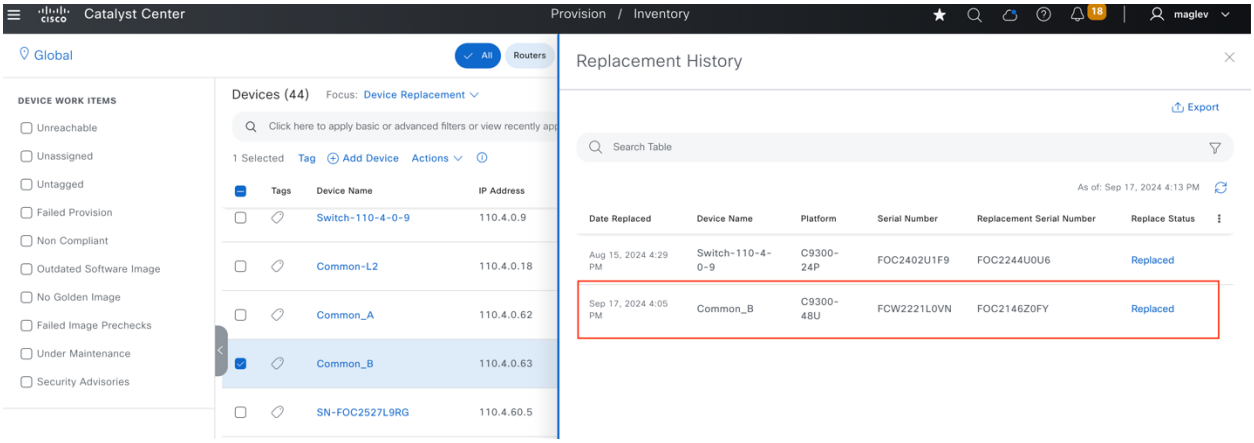



**図 61.　　以前に障害が発生したデバイスのレポートの [Replace Status] が [Replaced] になる**



**ステップ 16.** **Common_A** デバイスで、DHCP 設定が削除されたことを確認します。

```
047952: Sep 18 02:17:33.864: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp excluded-address 110.4.0.1 110.4.0.10
047953: Sep 18 02:17:33.897: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp excluded-address 110.4.0.12 110.4.0.255
047954: Sep 18 02:17:33.921: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp pool GigabitEthernet1/0/25
047955: Sep 18 02:17:33.944: %PARSER-5-CFGLOG_LOGGEDCMD: User:solution  logged command:no ip dhcp class ciscopnp
```

**ステップ 17.** 他の物理的な接続がある場合は、再開します。

**技術的なヒント：** RMA を実行する場合：
1. 障害が発生したデバイスを切断し、デバイスがインベントリで到達不能として表示されるまで待ちます。デバイスに交換のマーク付けをします。

2. 交換用デバイスに電源が入っている場合は、障害が発生したデバイスに交換のマーク付けをする前に、アップストリームデバイスに交換用デバイスを接続しないでください。

3. 交換用デバイスで PnP オンボーディングが完了するまでは、拡張ノードなどのダウンストリームデバイスを接続しないでください。

4. 障害が発生したデバイスが拡張ノードでも AP でもない場合は、ゼロタッチ RMA を実行するために少なくとも 1 台のアップストリームデバイスが Catalyst Center によって管理されていることを確認してください。

5. ゼロタッチ RMA ワークフローでは、障害が発生したデバイスにソフトウェアサブパッケージがある場合は、交換用デバイスが「バンドル」モードではなく「インストール」モードで実行されていることを確認してください。

## ファブリックサイトの切断

このセクションでは、ファブリックサイトを切断するプロセスを説明します。

1. ファブリックサイトからすべてのファブリックデバイスを削除します。
2. ファブリックゾーンを無効にします。
3. ファブリックサイトを削除します。

### デバイスの削除

Catalyst Center からデバイスを削除するには、ファブリックサイトからファブリックロールを無効にしてインベントリからデバイスを削除します。

**手順 1。** A. ファブリックからのファブリックエッジまたは拡張ノード、ポリシー拡張ノード、SBEN の削除

**パート 1**：ポート割り当てのクリーンアップが必要な拡張ノードやファブリックエッジなどの、アクセスロールを持つデバイスを削除します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックし、[Cisco-Building-23] テキストリンクをクリックして [Port Assignment] タブをクリックします。

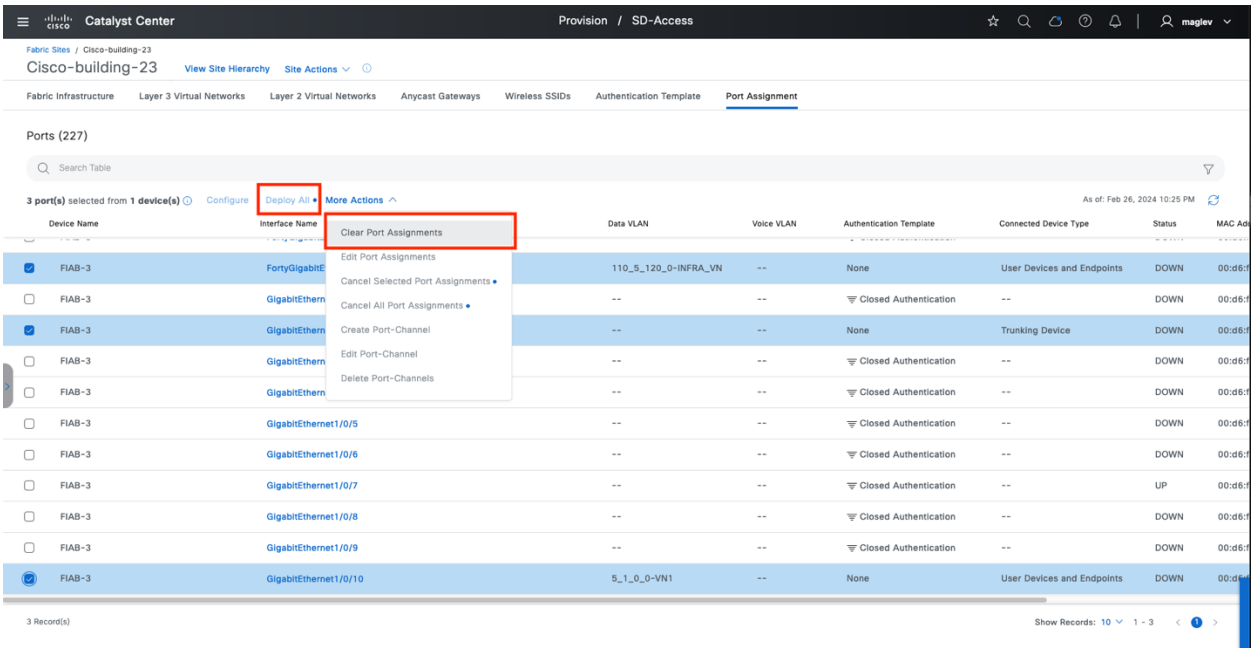
**ステップ 2.** カスタマイズされた [Port Assignment] 設定がある、すべての物理ポートのチェックボックス（[Port Channel] を除く）をオンにします。

**ステップ 3.** [More Actions] > [Clear Port Assignment] の順に選択します。

**ステップ 4.** [Deploy All] をクリックし、展開を続行します。

**ステップ 5.** [Port Channel] が設定されている場合は、[Port Channel] をクリックし、[More Actions] > [Delete Port-Channels] の順に選択して、展開を続行します。

**図 62.　　[Clear Port Assignment] の実行後に [Deploy All] が有効になる**




**パート 2**：ポート割り当てをクリーンアップした後、ファブリックサイトからファブリックロールを無効にします。

**ステップ 1.** [Fabric Infrastructure] ウィンドウに移動し、ターゲットデバイスをクリックします。

**ステップ 2.** 右側のペインで [Remove from Fabric] をクリックし、展開に進みます。

## 手順 1。　　B. ファブリックサイトからのファブリックボーダーノード、コントロールプレーンノード、ワイヤレスコントローラの削除

**ステップ 1.** [Fabric Infrastructure] ウィンドウに移動し、ターゲットデバイスをクリックします。

**ステップ 2.** 右側のペインで [Remove from Fabric] をクリックし、展開に進みます。

**注：**　ファブリックサイトには、少なくとも 1 つのコントロールプレーンノードが必要です。ファブリックサイトに、他のファブリックロールが有効になっているデバイスがまだある場合は、すべてのコントロールプレーンノードを削除することはできません。最初に、コントロールプレーンロールのないデバイスを削除します。

**技術的なヒント：**　デバイスが到達不可能な場合、ポート割り当てをクリーンアップしてファブリックからデバイスを削除するタスクは [Fail] として報告されますが、これらのデバイスのファブリックロールは削除されます。**インベントリ**からの削除が許可されます。

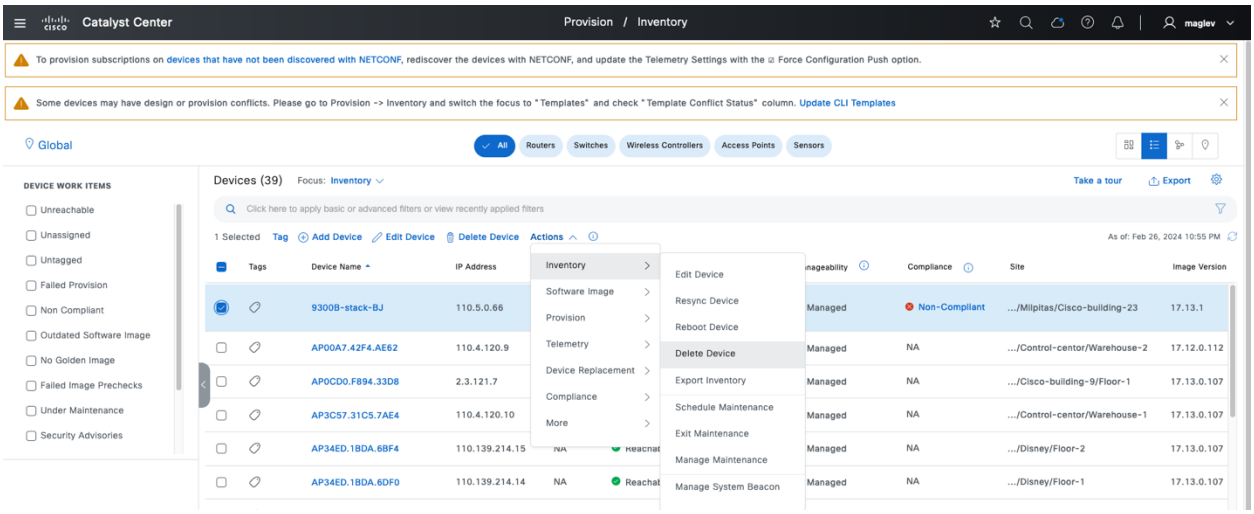
## 手順 2。　　インベントリからのデバイスの削除

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

**ステップ 2.** ターゲットデバイスのチェックボックスを見つけてチェックボックスをオンにします。

**ステップ 3.** [Actions] > [Inventory] > [Delete Device] の順に選択し、削除ワークフローを続行します。

**図 63.　　インベントリからのデバイスの削除**




拡張ノード、ポリシー拡張ノード、または SBEN を削除する場合は、インベントリから削除した後、アップリンクデバイスのポート設定をクリーンアップします。次に例を示します。

**図 64.　　拡張ノードまたはポリシー拡張ノードがインベントリから削除された後のアップリンクデバイスでのポートチャネル設定の削除**

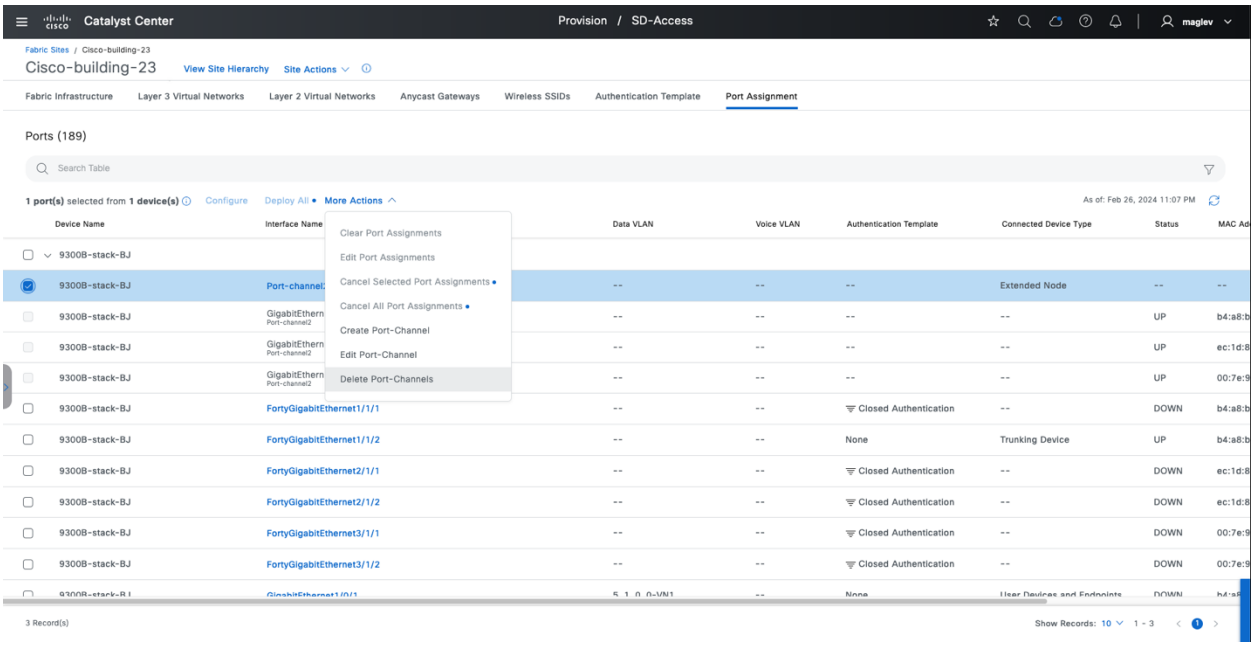
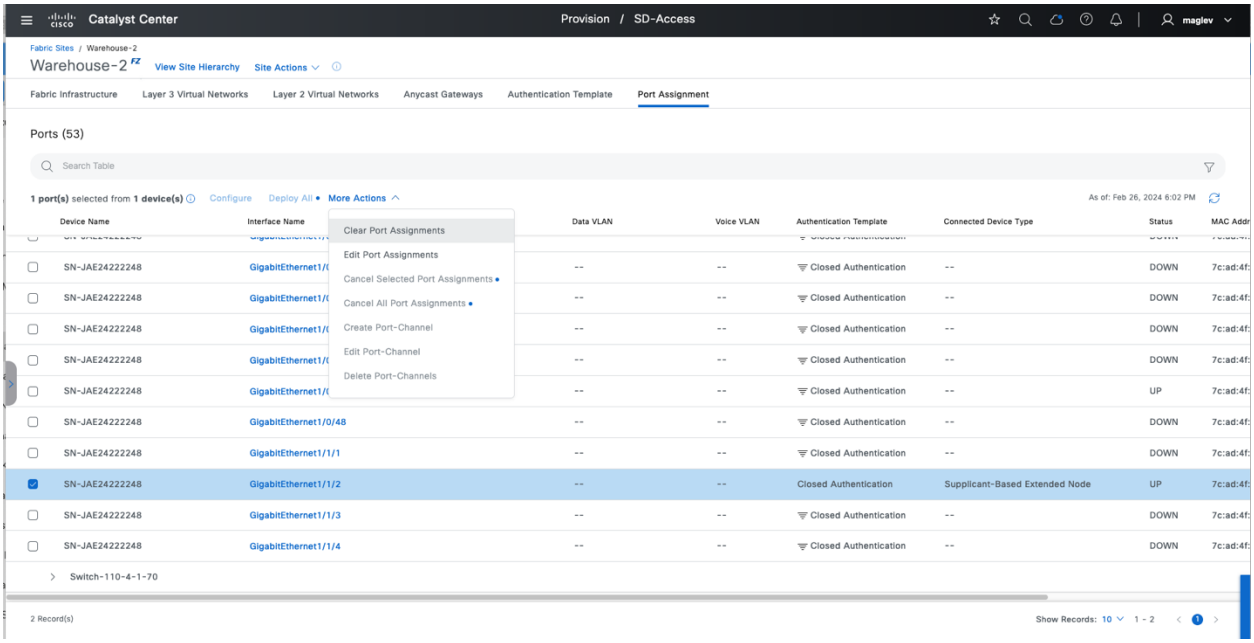


**図 65.　　SBEN がインベントリから削除された後のアップリンクデバイス上での物理ポート設定の削除**




## エニーキャストゲートウェイの削除

エニーキャストゲートウェイは、ファブリックサイトに関連付けた後に、ファブリックゾーンおよび継承されたサイトに追加できます。ファブリックサイトからエニーキャストゲートウェイを削除するには、まずファブリックゾーンとすべての継承されたサイトからエニーキャストゲートウェイを削除する必要があります。

エニーキャストゲートウェイ **4.1.0.1** は、**Control-center** のアンカー VN GUEST で設定され、ファブリックゾーン **Floor-1** および継承されたサイト **Cisco-Building-9** に追加されます。

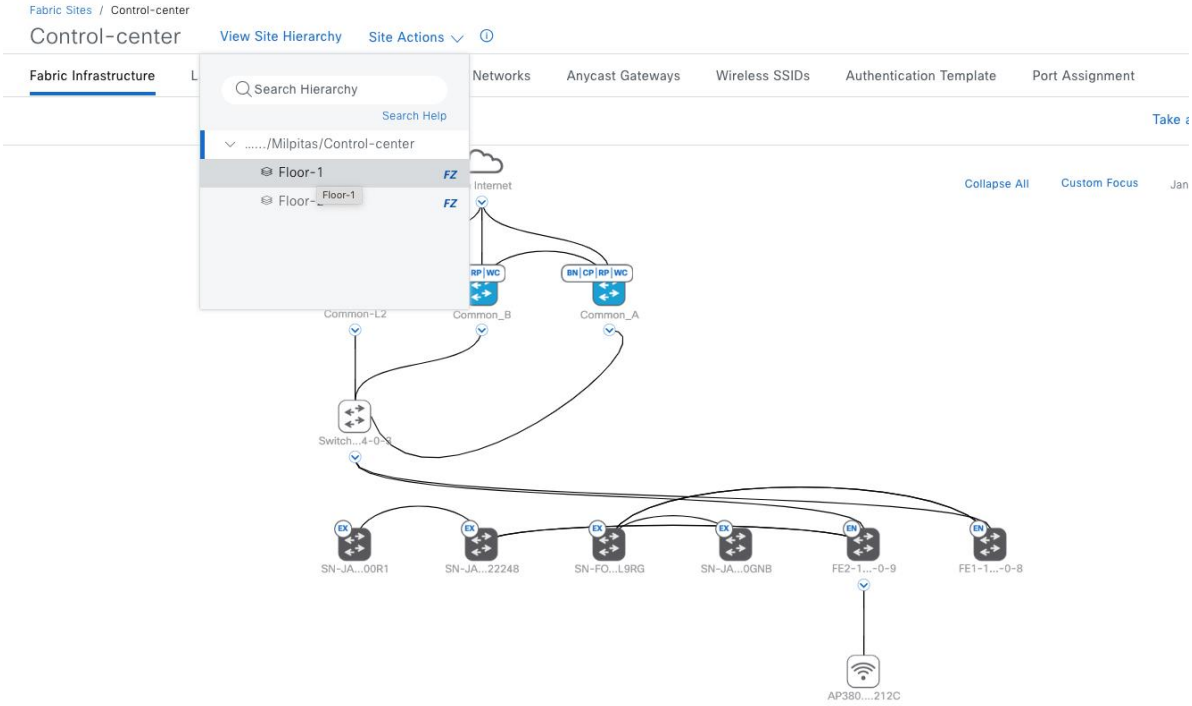
手順 1 に従って、ファブリックゾーン、継承されたサイト、および control-center からエニーキャストゲートウェイ **4.1.0.1** を削除します。

### 手順 1。　　ファブリックゾーンからのエニーキャストゲートウェイの削除

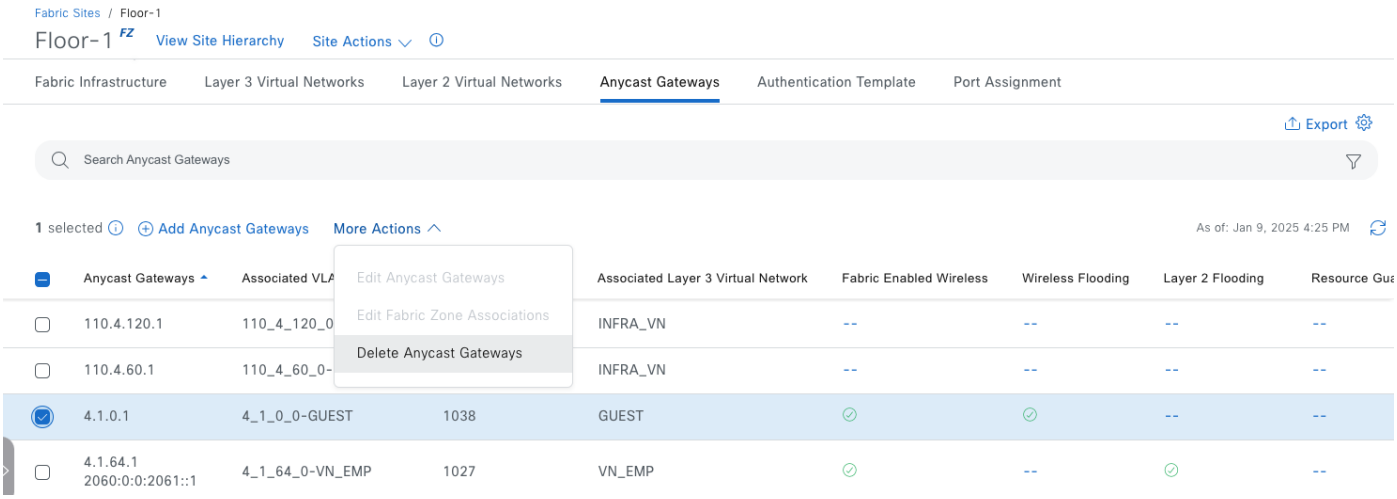
ファブリックゾーン内のエニーキャストゲートウェイは、ファブリックゾーンレベルまたはファブリックサイトレベルで削除できます。

**方法 1**：**4.1.0.1** をゾーンレベルの **Floor-1** から削除します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] > [Control-center] の順に選択し、[View Site Hierarchy] > [Floor-1] の順に選択します。




**ステップ 2.** [Anycast Gateways] タブをクリックして [4.1.0.1] チェックボックスをオンにし、[More Actions] > [Delete Anycast Gateways] の順に選択します。

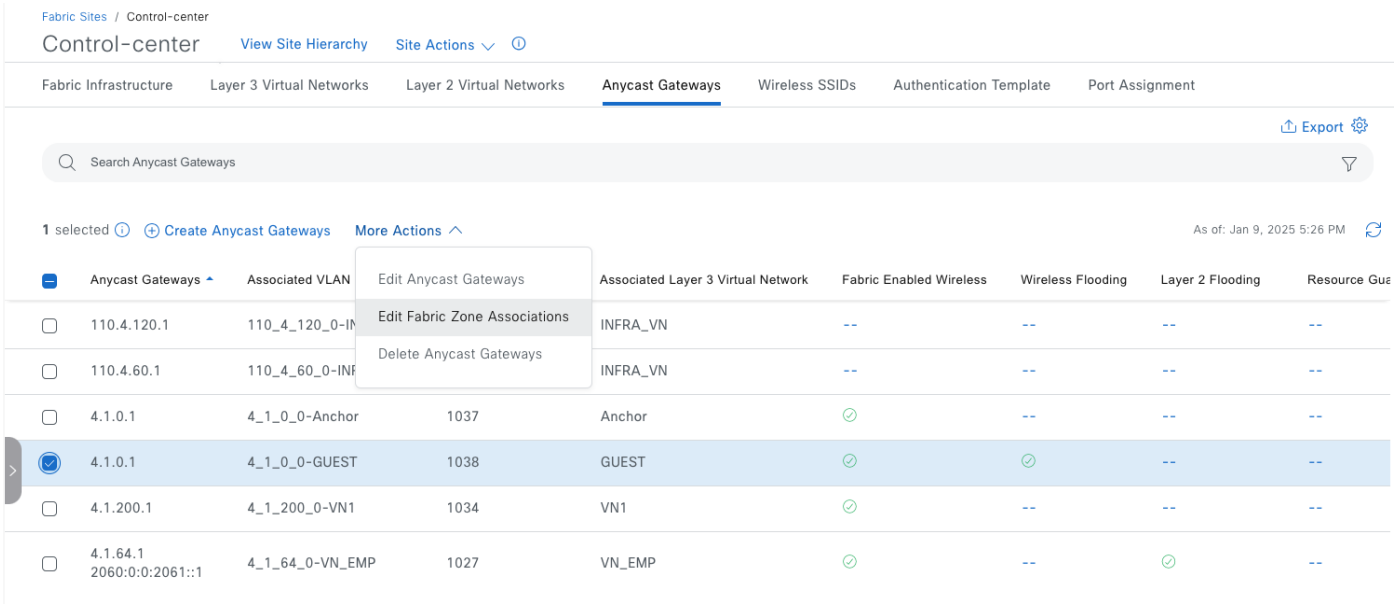



**ステップ 3.** 変更を適用してタスクを展開します。

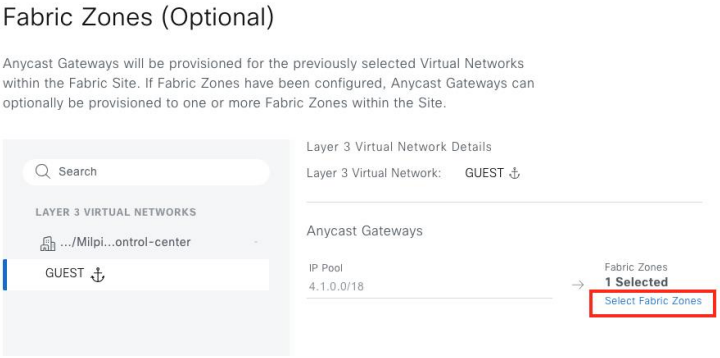
**方法 2**：**4.1.0.1** をサイトレベルの **Floor-1** から削除します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Fabric Sites] > [Control-center] の順に選択します。

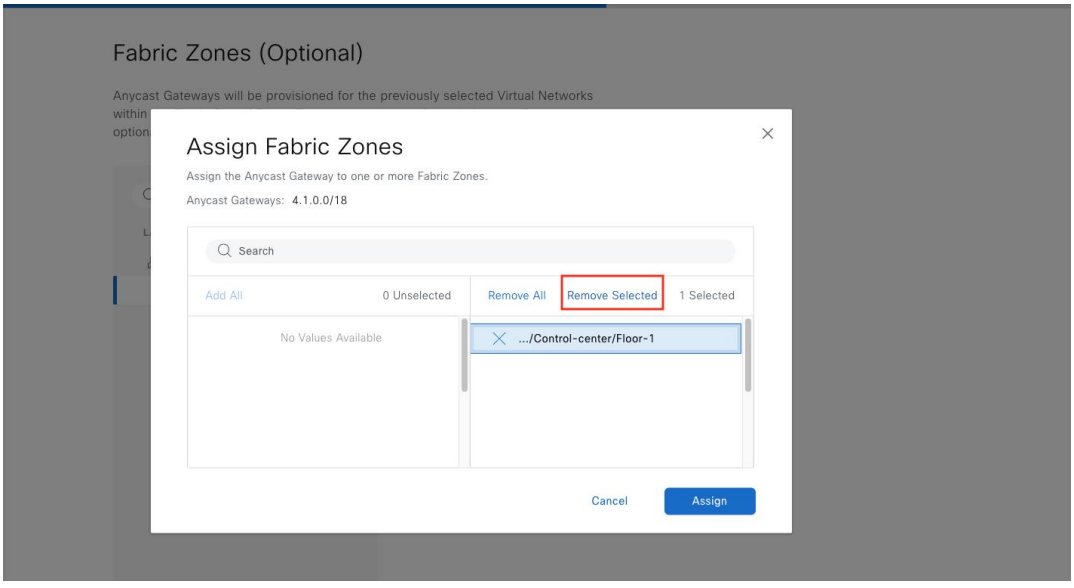
**ステップ 2.** [Anycast Gateways] タブをクリックして [4.1.0.1] チェックボックスをオンにし、[More Actions] > [Edit Fabric Zone Associations] の順に選択します。




**ステップ 3.** ワークフローで、[Select Fabric Zones] をクリックします。




**ステップ 4.** ゾーンを選択し、[Remove Selected] をクリックしてから、[Assign] をクリックします。



**ステップ 5.** ワークフローを完了し、タスクを展開します。

## 手順 2。 継承されたサイトからのエニーキャストゲートウェイの削除

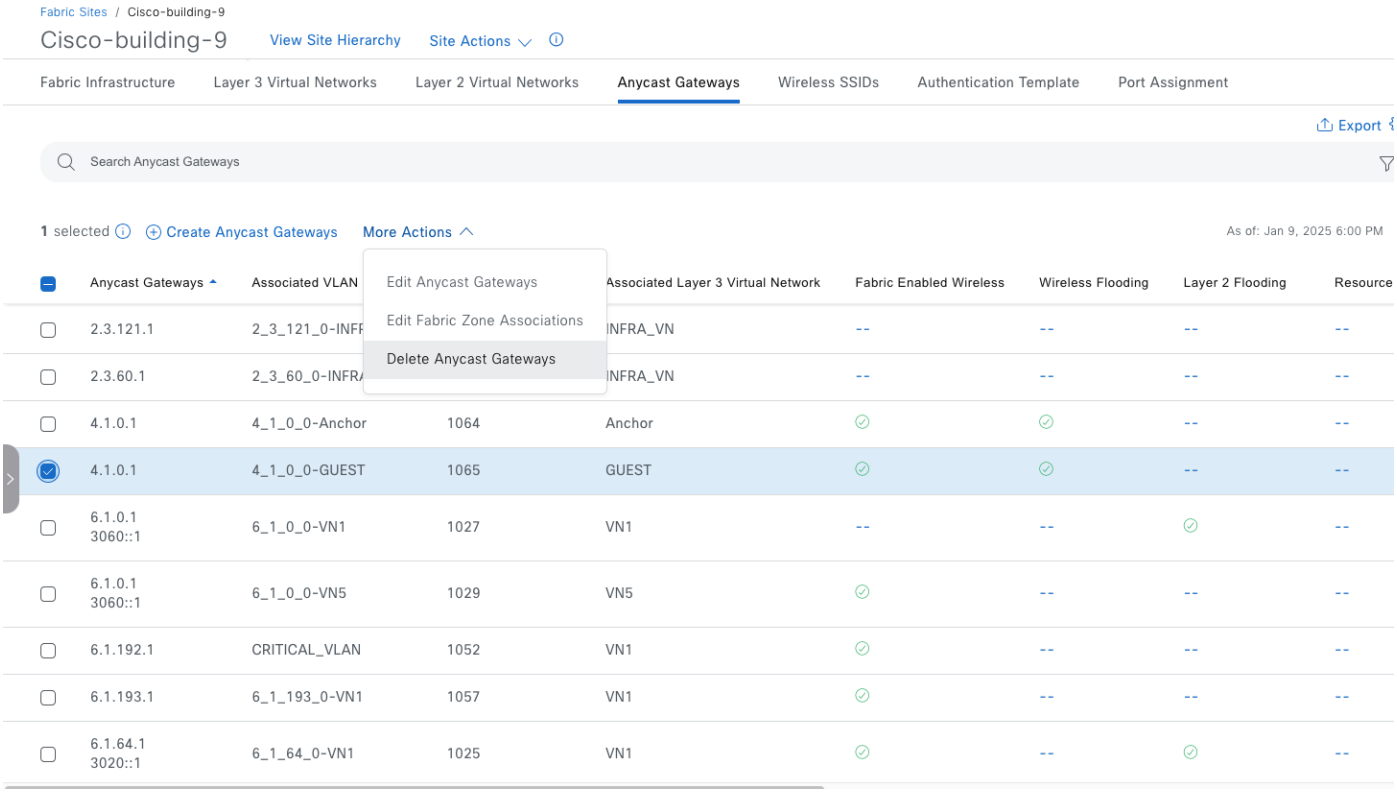
エニーキャストゲートウェイ **4.1.0.1** が、継承されたサイト **Cisco-Building-9** に追加されます。

エニーキャストゲートウェイ **4.1.0.1** を削除するには、次の手順を実行します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] の順に選択し、右上のテーブルビューアイコンをクリックして、[Cisco-Building-9] テキストリンクをクリックします。

**ステップ 2.** [Anycast Gateways] タブをクリックして [4.1.0.1] チェックボックスをオンにし、[More Actions] > [Delete Anycast Gateways] の順に選択します。

**ステップ 3.** 変更を適用してタスクを展開します。

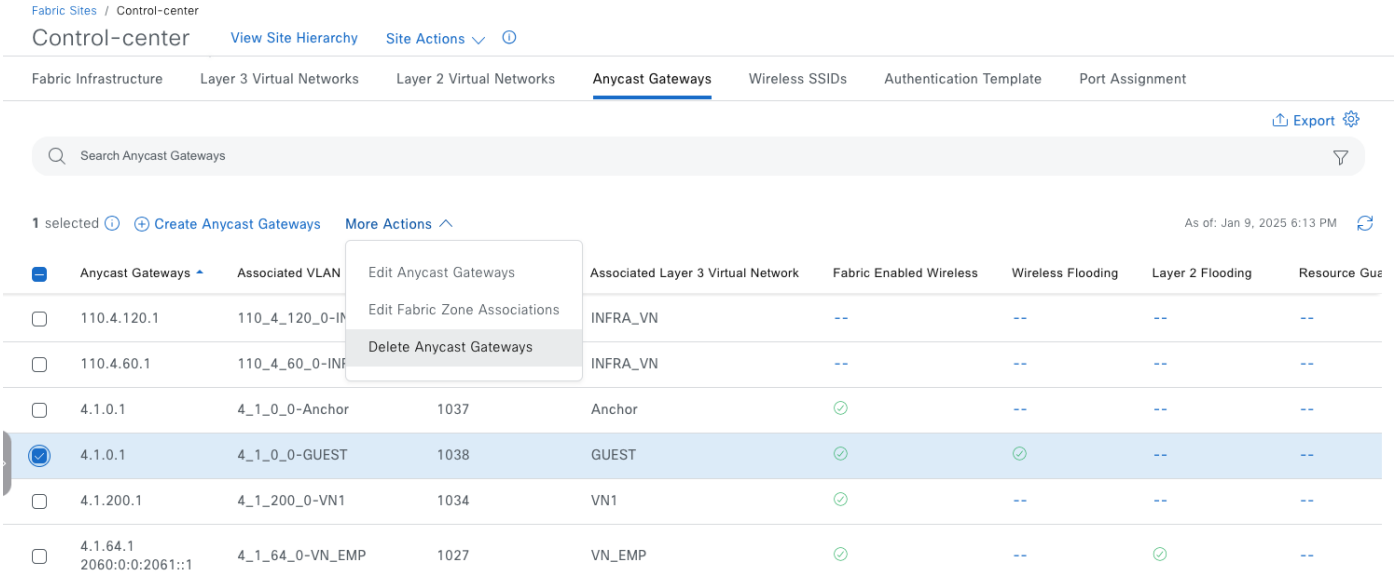



## 手順 3。 ファブリックサイトからのエニーキャストゲートウェイの削除

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[Provision] > [Fabric Sites] > [Control-center] の順に選択します。

**ステップ 2.** [Anycast Gateways] タブをクリックして [4.1.0.1] チェックボックスをオンにし、[More Actions] > [Delete Anycast Gateways] の順に選択します。

**ステップ 3.** 変更を適用してタスクを展開します。




## ファブリックゾーンの無効化

ファブリックゾーンは、ファブリックエッジ、拡張ノード、ポリシー拡張ノード、または SBEN などのデバイスがゾーンに割り当てられておらず、ゾーンにエニーキャストゲートウェイが割り当てられていない場合にのみ無効にできます。

**ステップ 1.** デバイスを削除する。「デバイスの削除」の手順 1a に従います。

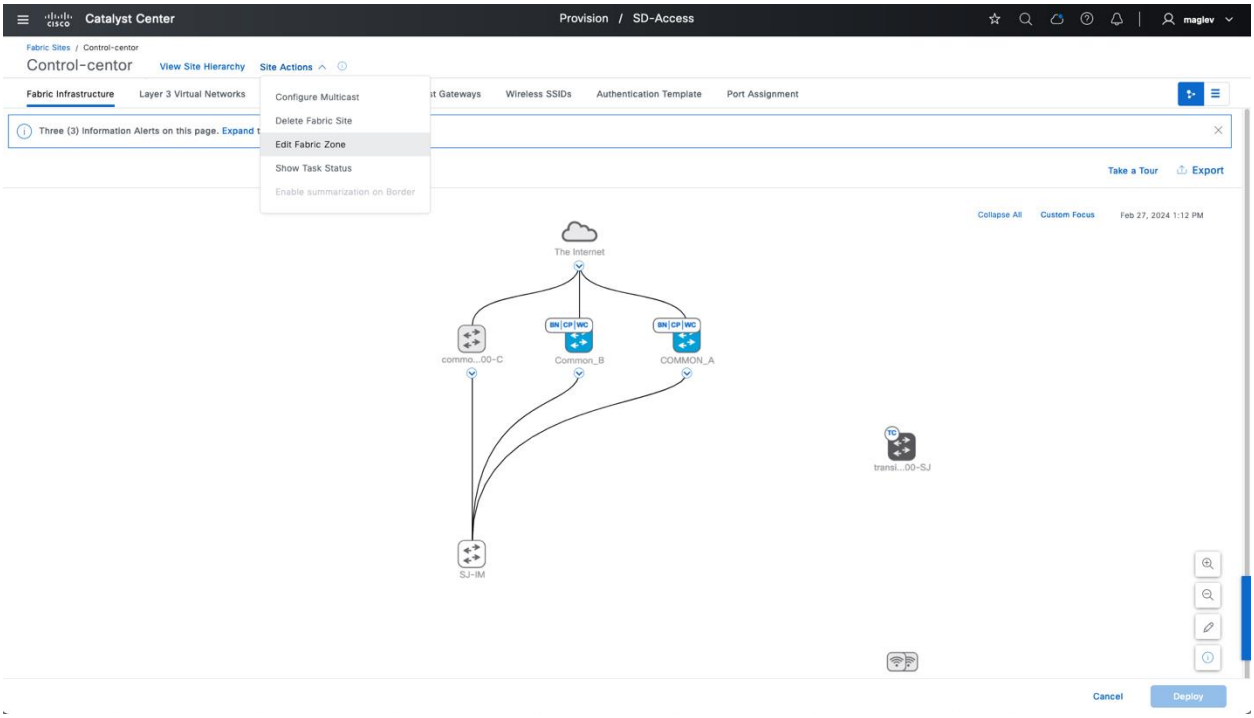
**ステップ 2.** エニーキャストゲートウェイを削除します。「エニーキャストゲートウェイの削除」に従います。

**技術的なヒント：** 最初にステップ 2、次にステップ 1 を行うこともできます。

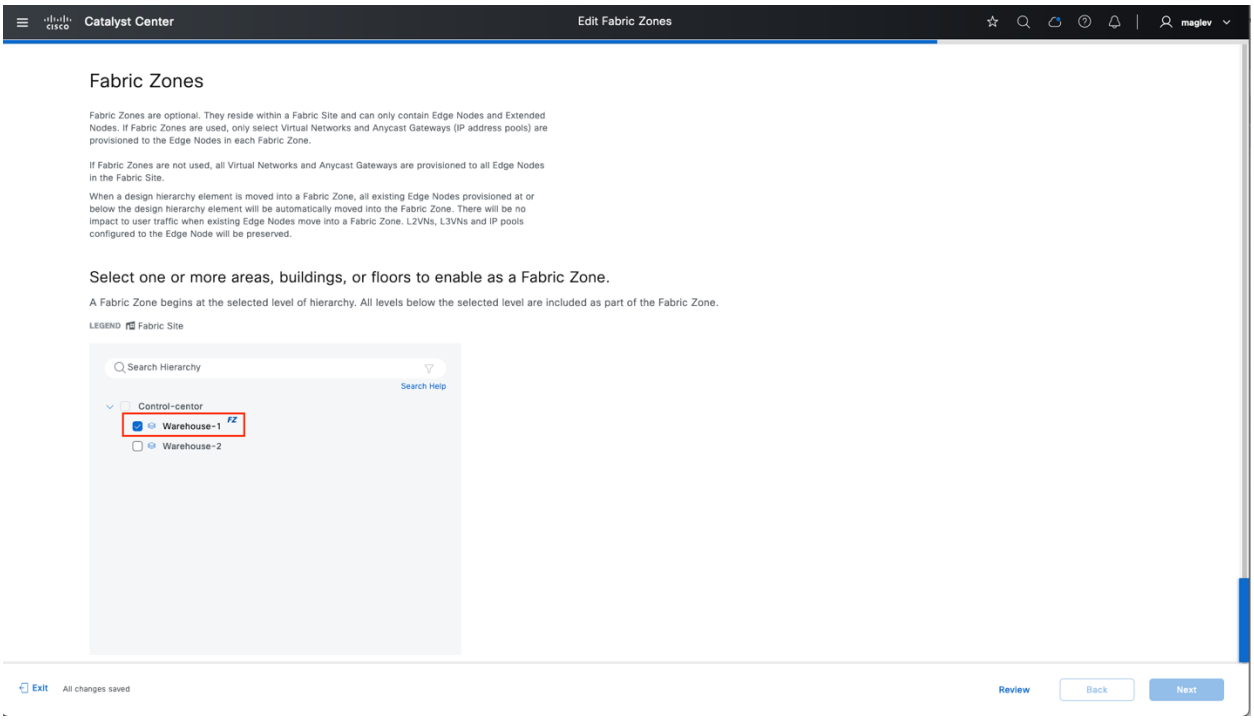
**ステップ 3.** サイトレベルまたはゾーンレベルのいずれかでファブリックゾーンを無効にします。

**方法 1**：サイトレベルでファブリックゾーンを無効にします。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Fabric Sites] > [Control-center] の順に選択し、[Site Actions] > [Edit Fabric Zone] の順に選択します。



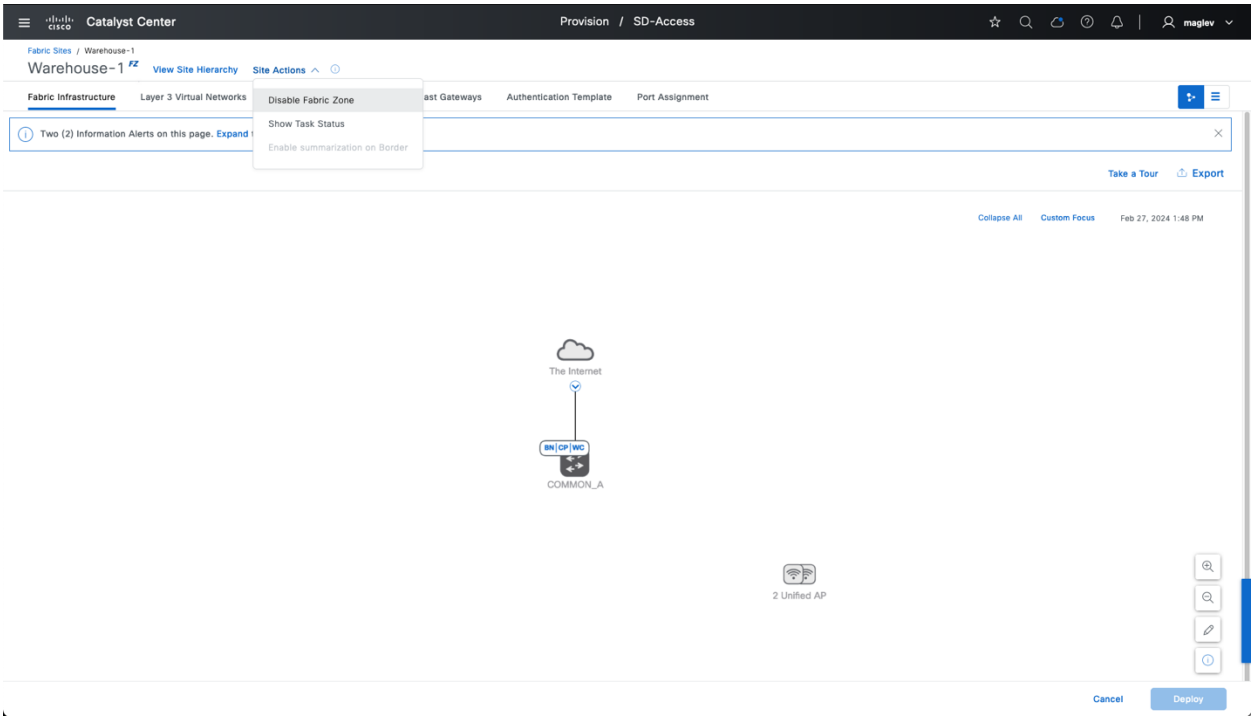

**ステップ 2.** フロアのチェックボックスをオフにして、ゾーンを無効にします。



**方法 2：**ゾーンレベルでファブリックゾーンを無効にします。

**ステップ 1.** ファブリックゾーンに移動します。

**ステップ 2.** [Site Actions] > [Disable Fabric Zone] の順に選択します。




## ファブリックサイトの削除

ファブリックサイトは、ファブリックデバイス、エニーキャストゲートウェイ、レイヤ VN、アンカー VN、ファブリックゾーン、マルチキャストがない場合にのみ削除できます。マルチキャストが有効になっている場合は、まずマルチキャストを削除します。

マルチキャストグループを削除するには、次の手順を実行します。

**ステップ 1.** ファブリックサイトに移動し、[Site Actions] > [Remove Multicast Configuration] の順に選択します。

**ステップ 2.** エニーキャストゲートウェイを削除します。「エニーキャストゲートウェイの削除」に従います。

**ステップ 3.** アンカー VN が設定されている場合は、継承されたサイトからアンカーされたエニーキャストゲートウェイとアンカー VN を削除し、次のいずれかを実行します。

- これらの VN でアンカーを無効にします。ファブリックサイトから VN を削除する必要はありません。
- ファブリックサイトから直接削除します。これらの VN でレイヤ 3 ハンドオフが設定されている場合は、レイヤ 3 ハンドオフをファブリックボーダーから削除する必要があります。

**図 66.　　VN 「GUEST」および「GUEST_P」でのアンカーの削除**

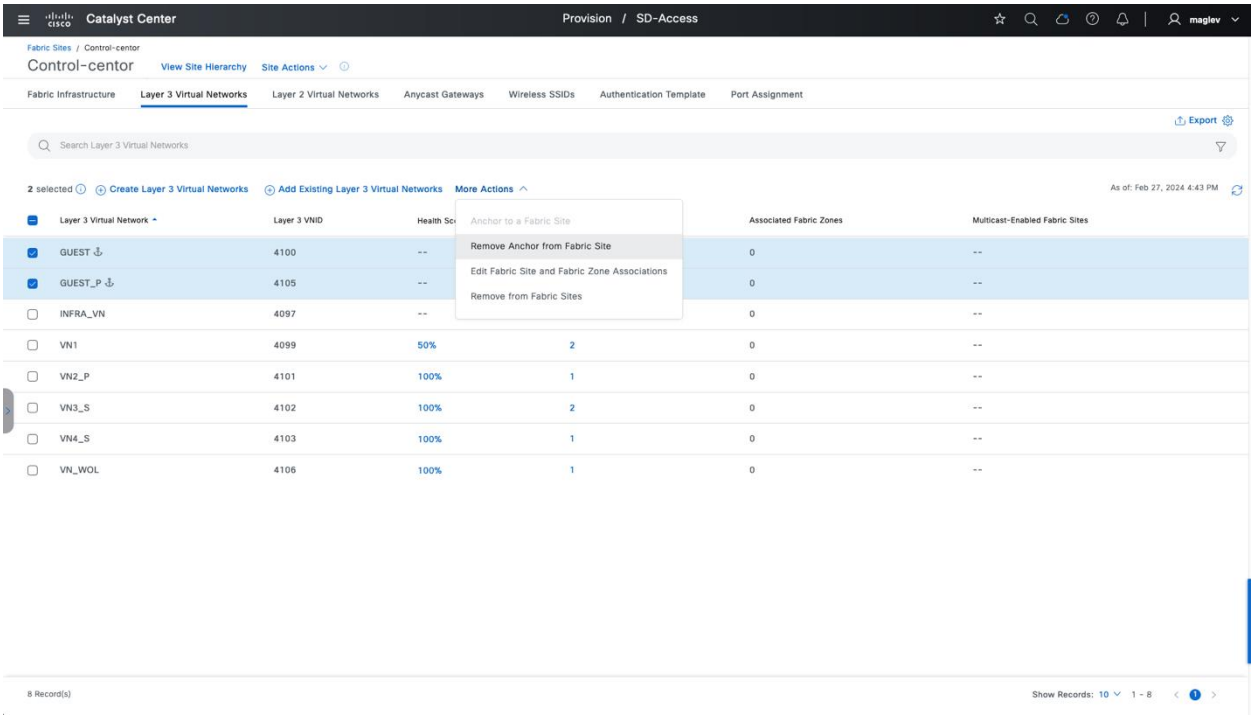
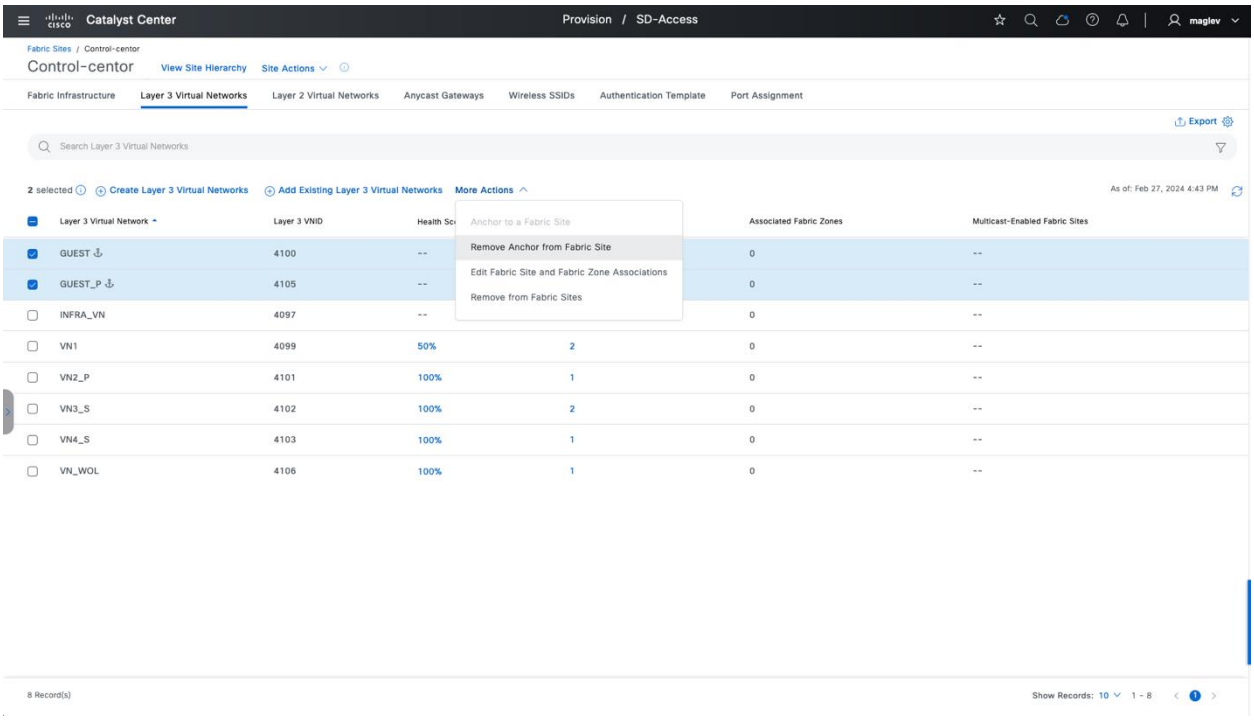



**図 67.　　ファブリックサイトからアンカー VN 「GUEST」および「GUEST_P」の直接削除**




**ステップ 4.** ファブリックデバイスを削除します。「デバイスの削除」の手順 1 に従います。手順に従って、拡張ノード、ポリシー拡張ノード、SBEN、ファブリックエッジ、ワイヤレスコントローラ、ファブリックボーダー、コントロールプレーンノードなどのファブリックデバイスを削除します。

**ステップ 5.** ファブリックゾーンを無効にします。「ファブリックゾーンの無効化」のステップ 3 に従います。

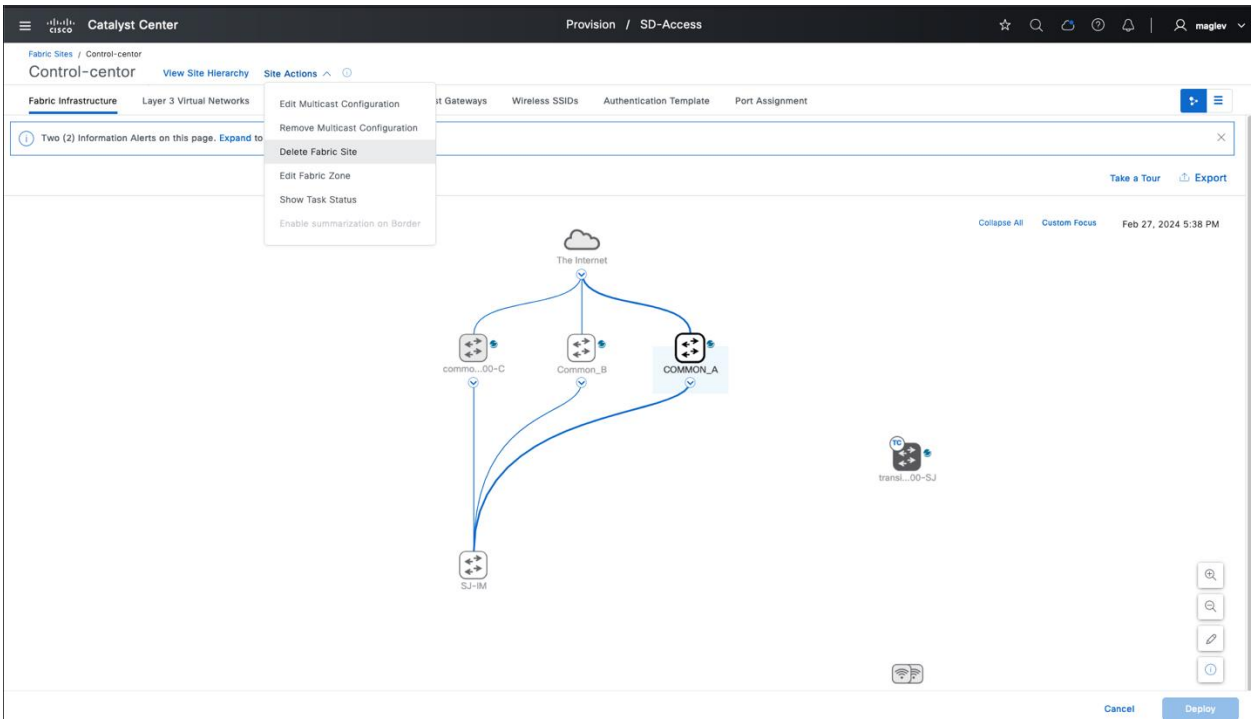
**ステップ 6.** ファブリックサイトに移動し、[Site Actions] > [Delete Fabric Site] を選択して、展開を続行します。

**注：**　サイトにトランジット コントロール プレーン デバイスがある場合は、ファブリックサイトを削除する前に削除してください。

トランジット コントロール プレーン デバイスを削除するには、次の手順を実行します。

**ステップ 1**. [Provision] > [SD-Access] > [Transits] の順に移動します。

**ステップ 2**. 該当するトランジットを選択して削除します。



## Cisco SD-Access ネットワークと Cisco SD-Access アプリケーションの監視

このセクションでは、Catalyst Center Assurance アプリケーションを使用した Cisco SD-Access ネットワークの日常的な正常性チェック、システムヘルスツールを使用した Cisco SD-Access アプリケーションの正常性の監視、および Cisco SD-Access 互換性マトリックスを使用してファブリックサイトにデバイスを追加したときのデバイス資格の検証について説明します。

Catalyst Center Assurance は、増え続けるビジネスニーズに対応するために、優れた一貫性のあるサービスレベルでの包括的なソリューションを提供します。リアクティブなネットワーク監視およびトラブルシューティング、ネットワーク実行のプロアクティブかつ予測的側面に対応し、クライアント、アプリケーション、およびサービスの最適なパフォーマンスを確保します。

アシュアランスには、次のようなメリットがあります。

- ネットワーク、クライアント、およびアプリケーション関連の問題へ実用的な情報を提供します。これらの問題は、複数の情報の基本的および高度な相関関係から成り立っているため、ホワイトノイズと誤検出は除外されます。
- システムガイド付きおよびガイドなしの両方のトラブルシューティングを提供します。アシュアランスでは、複数の重要業績評価指標（KPI）を関連付けるシステムガイド付きの方法を提供します。テストとセンサーの結果に基づいて、問題の根本原因を特定し、解決のために可能なアクションを提案します。データの監視ではなく、問題点を浮き彫りにすることに重点が置かれています。アシュアランスでは、レベル 3 サポートエンジニアに相当する作業が行われることもしばしばあります。
- ネットワークとネットワークデバイス、クライアント、アプリケーション、およびサービスに関する詳細な正常性スコアを提供します。アクセス（オンボーディング）と接続の両方のクライアント エクスペリエンスが保証されます。

Catalyst Center システム正常性ツールは、アプリケーションの正常性、システムステータス、およびアップグレードの準備状況を検証するのに役立ちます。

Catalyst Center は、動作中の Cisco SD-Access ファブリックノードのハードウェアおよびソフトウェア属性を Cisco SD-Access 互換性マトリックスの情報と定期的に比較し、互換性の問題が検出された場合は新しいデバイスがファブリックサイトに追加されないようにブロックします。

### 全体的な正常性のアシュアランス

[Overall Health Dashboard] には、ネットワークおよびクライアントデバイスの稼働状況の概要と、注意が必要な上位 10 件の問題のビューが表示されます。ここから、ネットワークの正常性またはクライアントの正常性にドリルダウンして、次の手順例に示すように、ネットワーク インフラストラクチャとクライアントがどの程度正常に実行されているかをより詳細に確認できます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Assurance] > [Health] の順に選択し、[Overall] タブをクリックします。

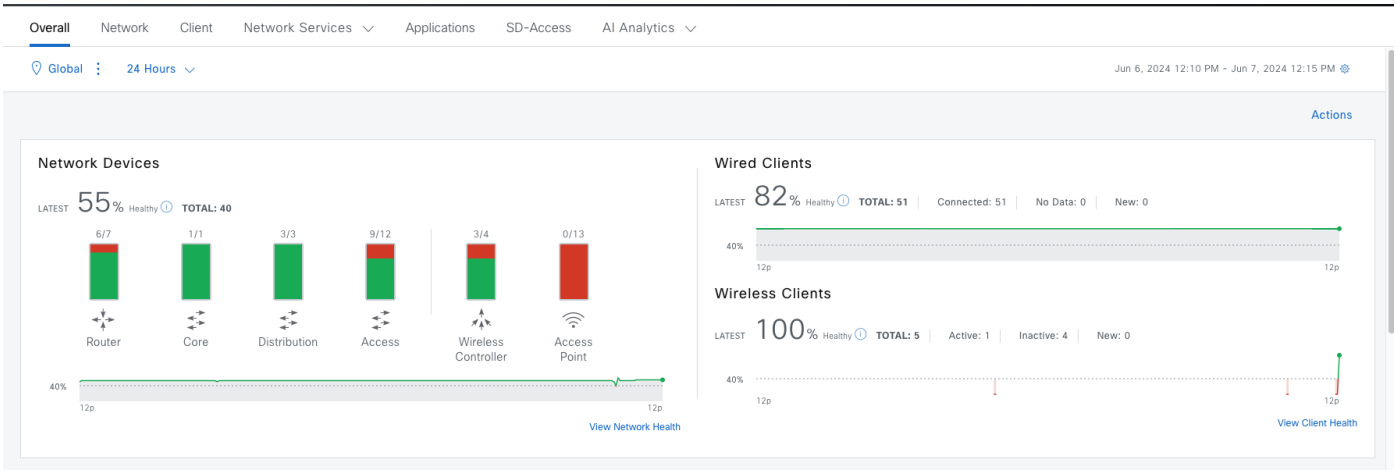
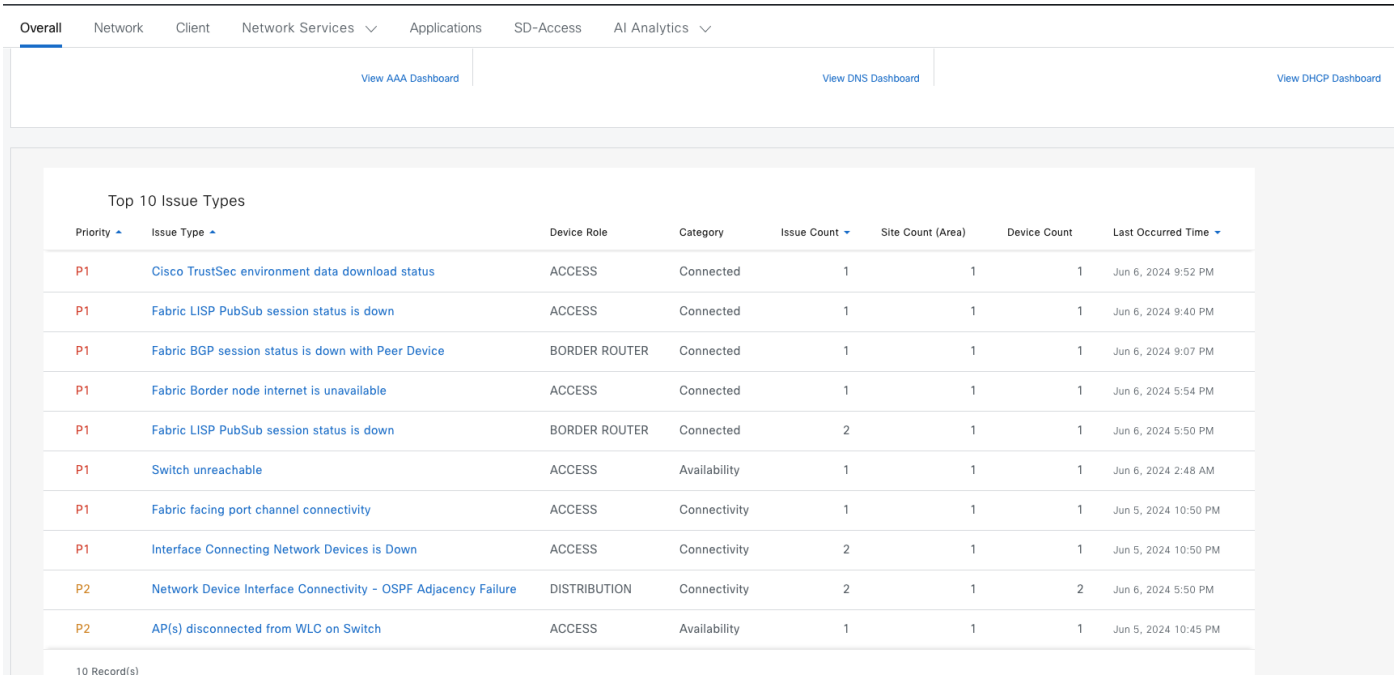
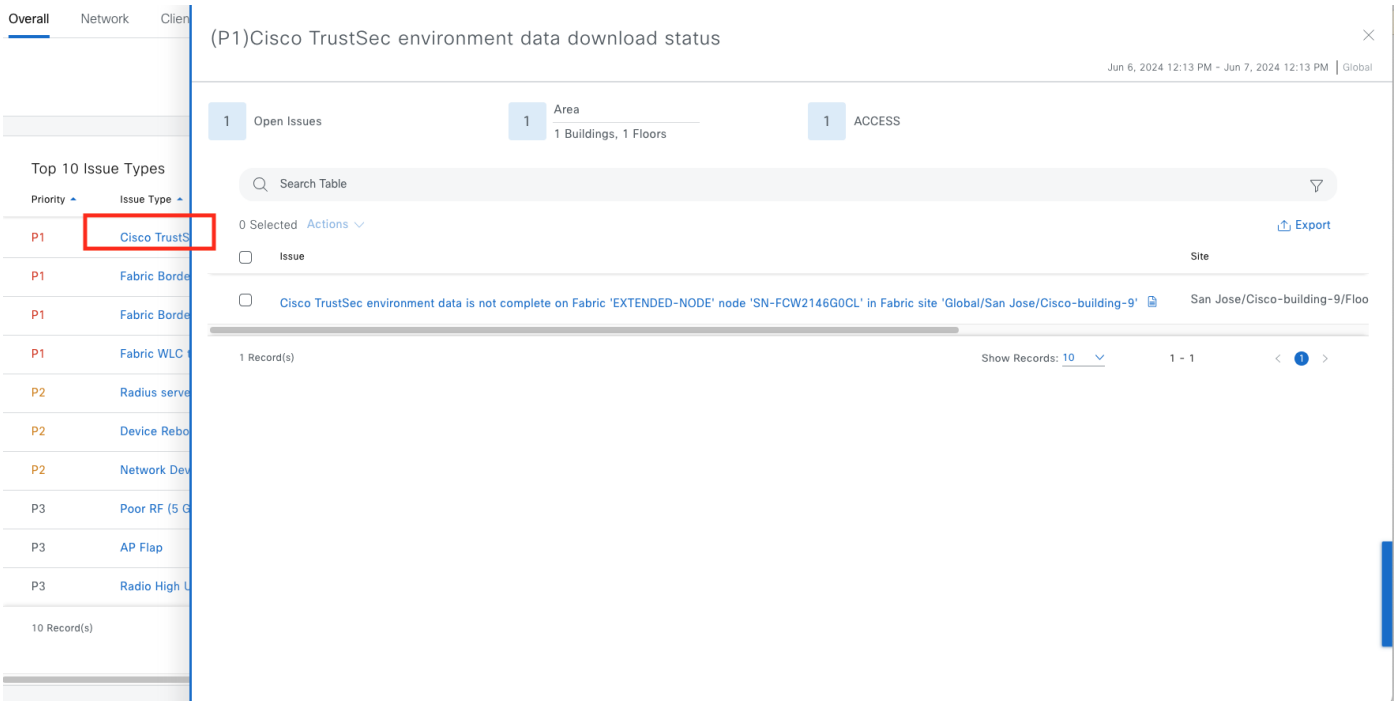


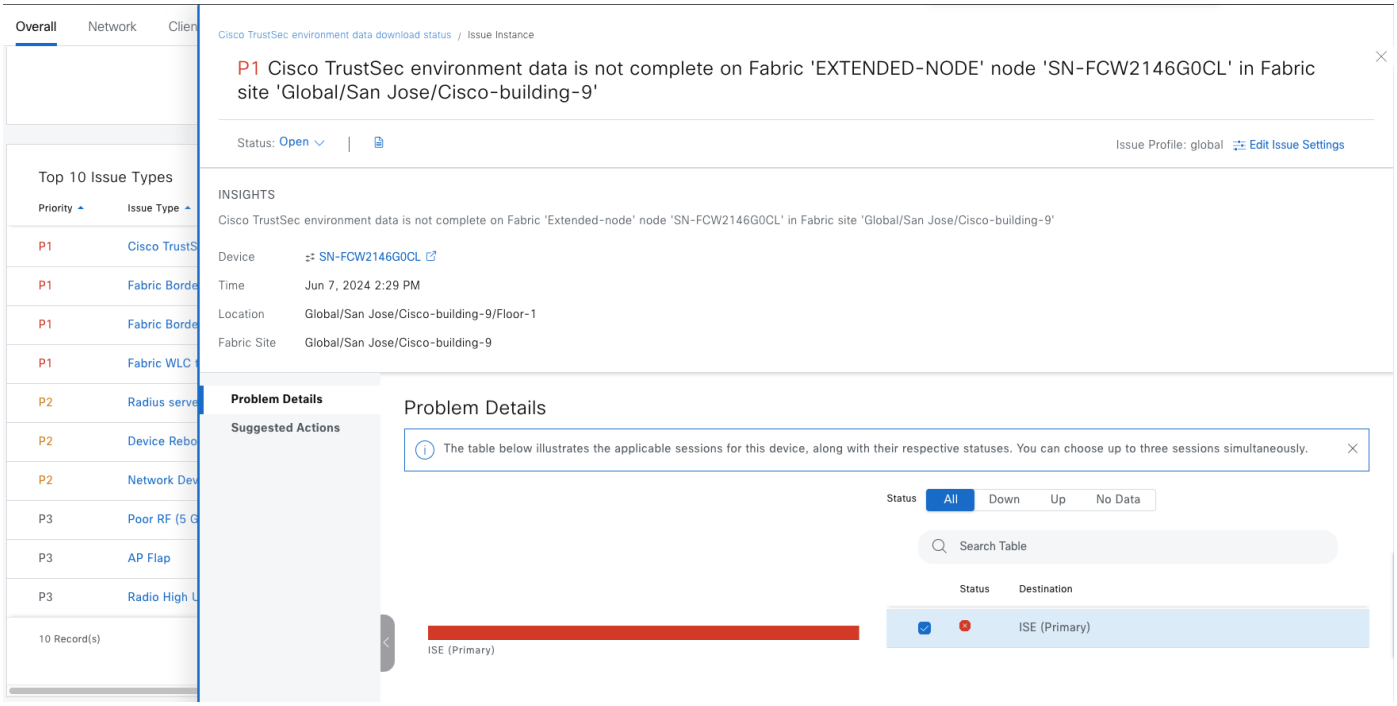

**図 68.　　上位 10 件の問題のタイプ**



**ステップ 2.** 個々の問題をクリックして詳細を表示し、推奨されるアクションに従います。

**図 69.　　Cisco TrustSec 環境データのダウンロードステータスの問題を示す例**



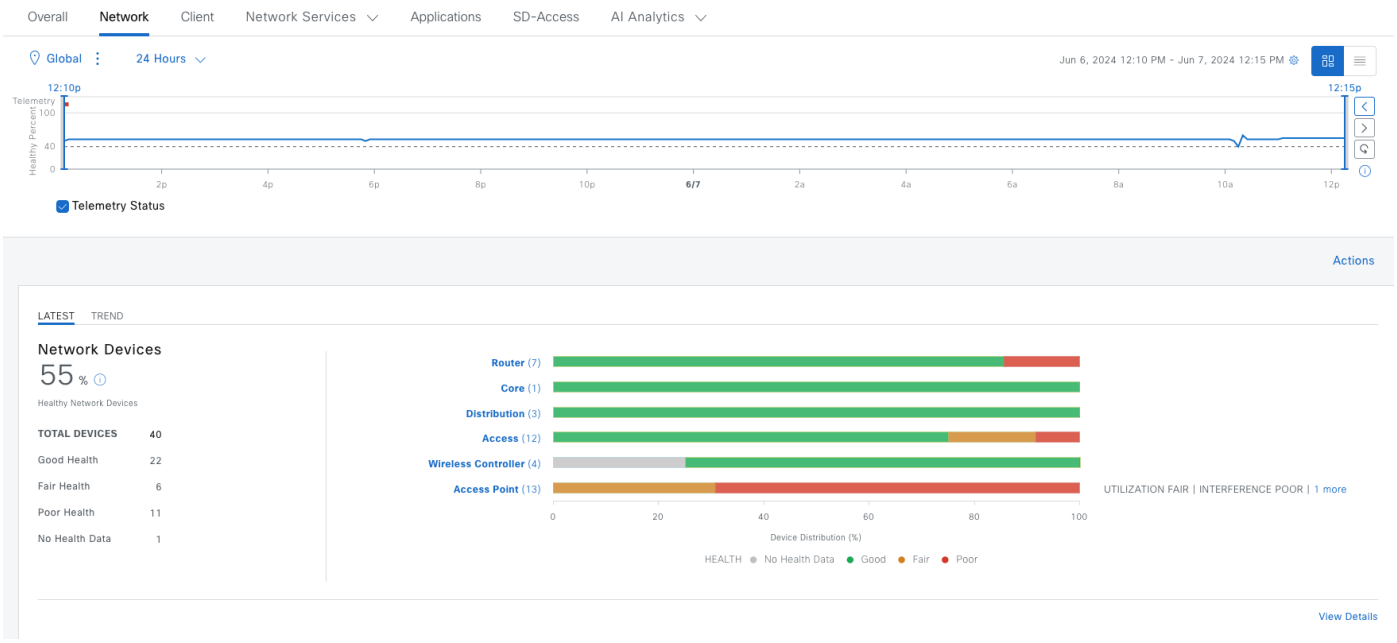



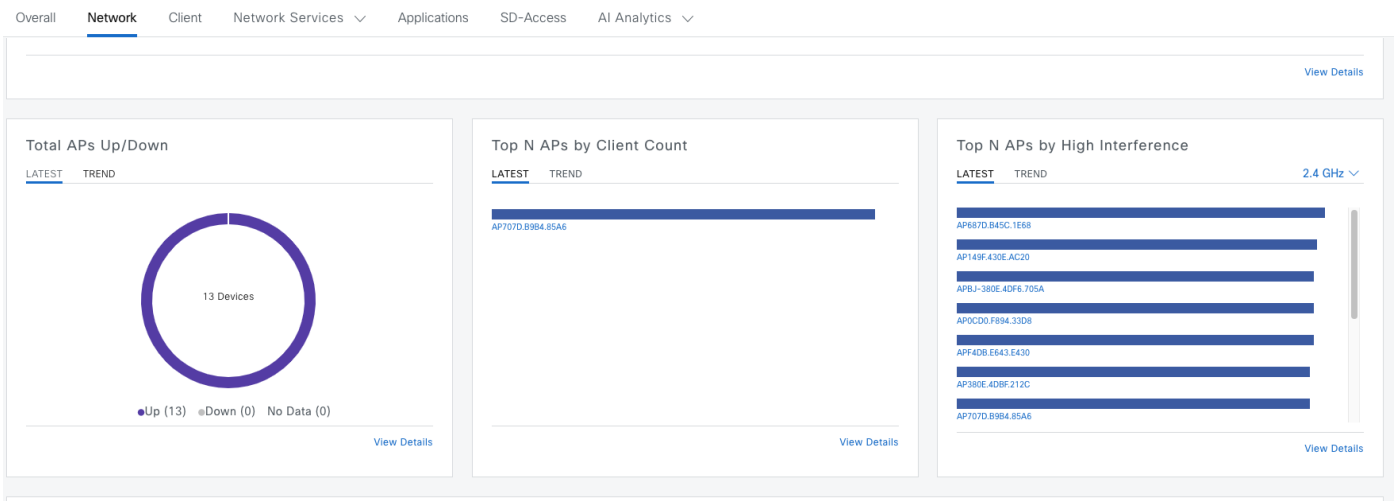
## ネットワークの正常性のアシュアランス

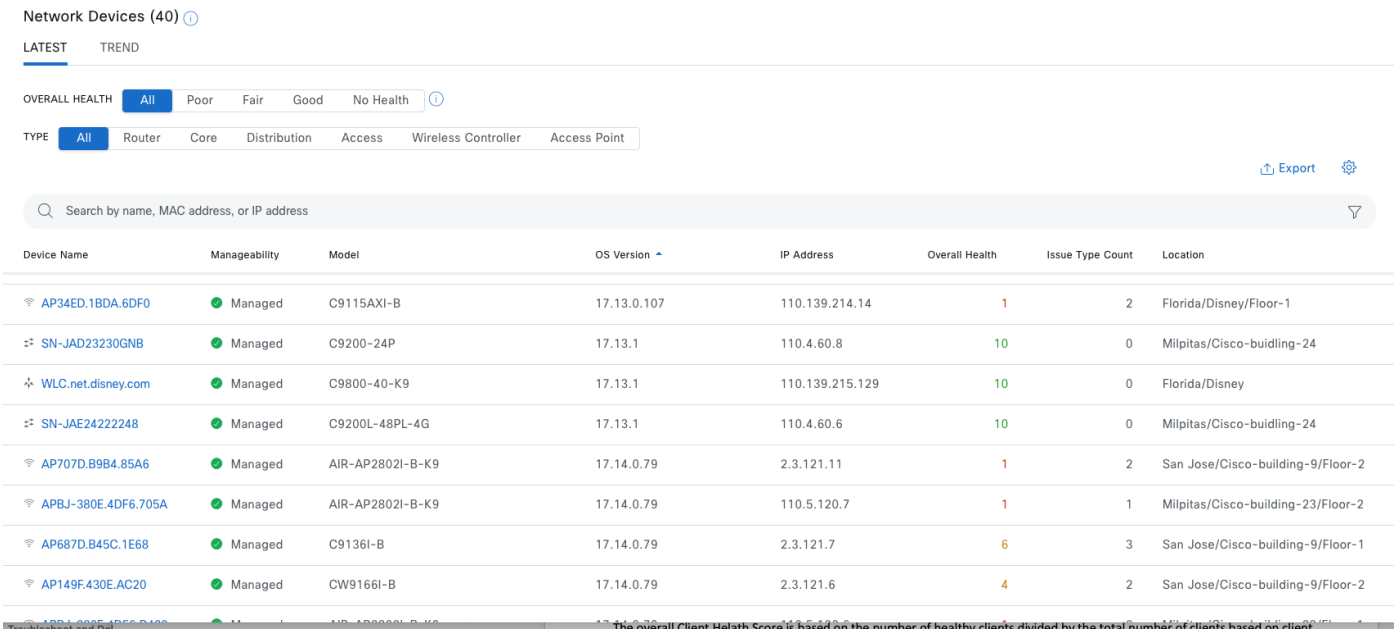
個々のネットワークデバイスの正常性スコアは、システム、データプレーン、およびコントロールプレーンの正常性に基づいて計算されます。ネットワークデバイスには、ルータ、スイッチ、ワイヤレスコントローラ、および AP が含まれます。メンテナンスモードのクライアントとデバイスは、ネットワークの正常性スコアに含まれません。

全体的なネットワークの正常性は、手順の図に示されているように、正常なデバイスを、Catalyst Center によって監視されているタイプごとのデバイスの総数で割った割合の計算で示されます。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Assurance] > [Health] の順に選択し、[Network] タブをクリックします。

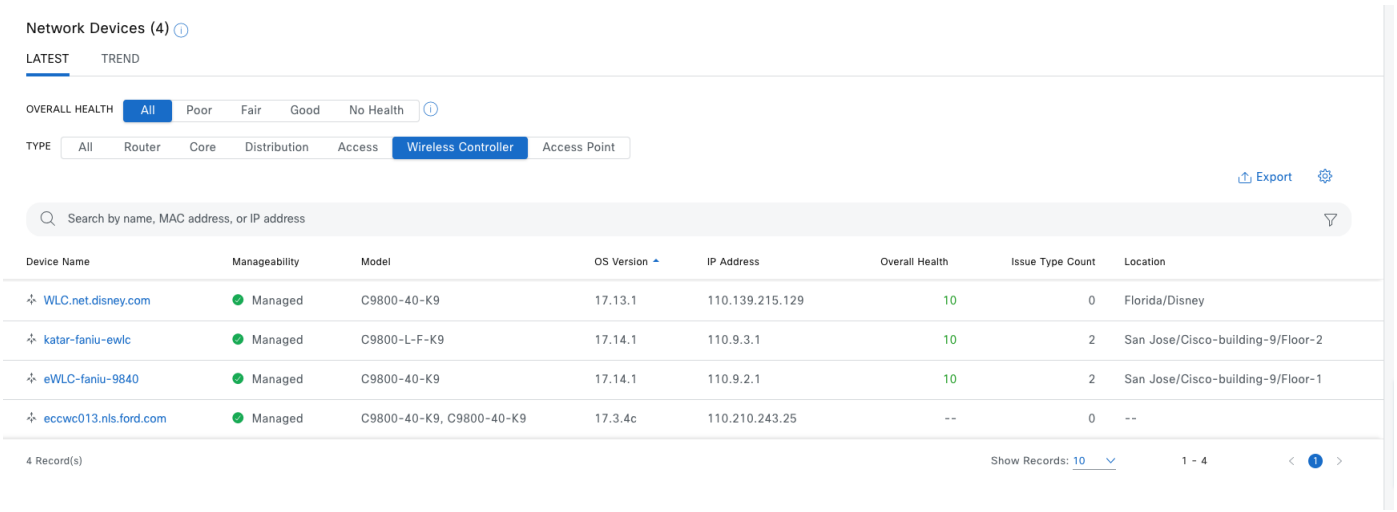




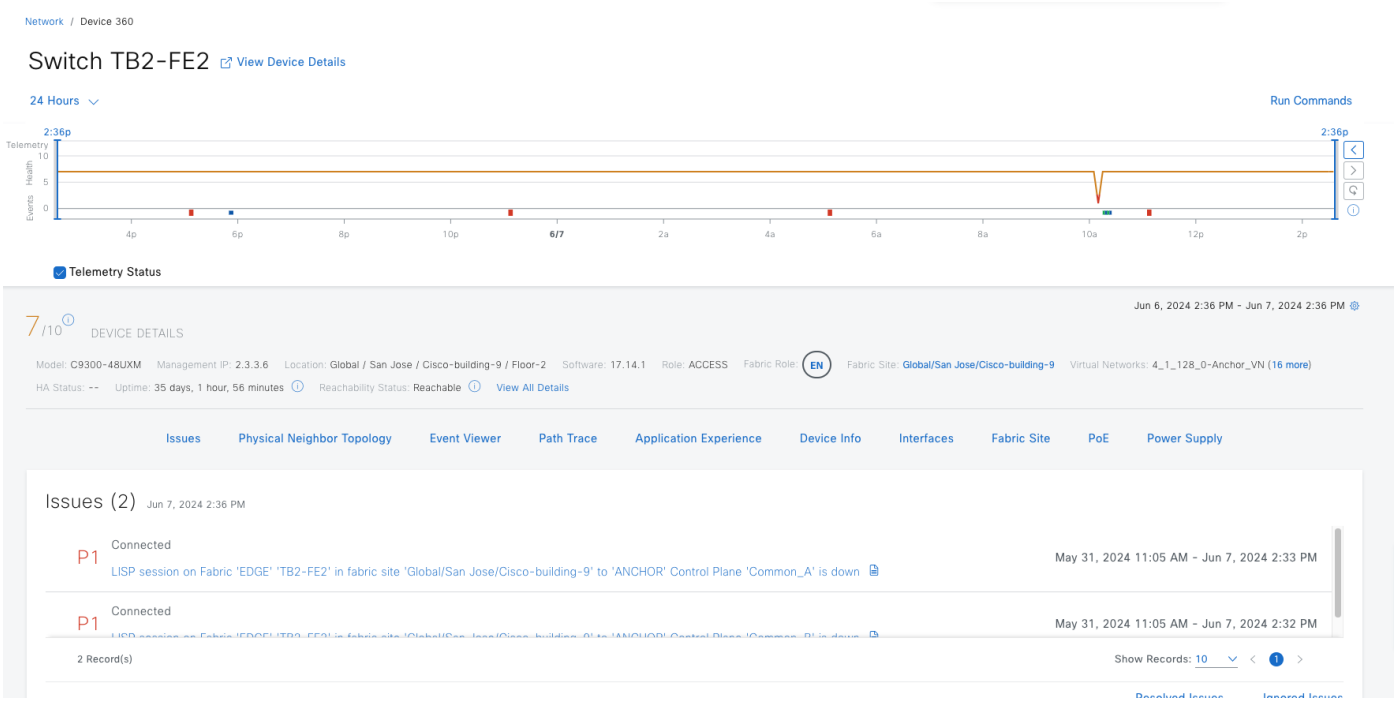

**ステップ 2.** フィルタを使用して、正常性ステータスまたはデバイスタイプでデバイスをフィルタ処理します。特定のデバイスセットの [Search] を使用します。

**図 70.　　[All] > [Wireless Controllers] の確認に適用されたフィルタの表示**




**注：**　ネットワークの正常性スコアは、場所のみに基づいて計算されます。デバイスの場所が不明な場合、そのデバイスはネットワーク ヘルス スコアに考慮されません。デバイスがプロビジョニングされていない場合、その正常性は監視されません。図中の最後のワイヤレスコントローラを参照してください。正常性スコアはありません。

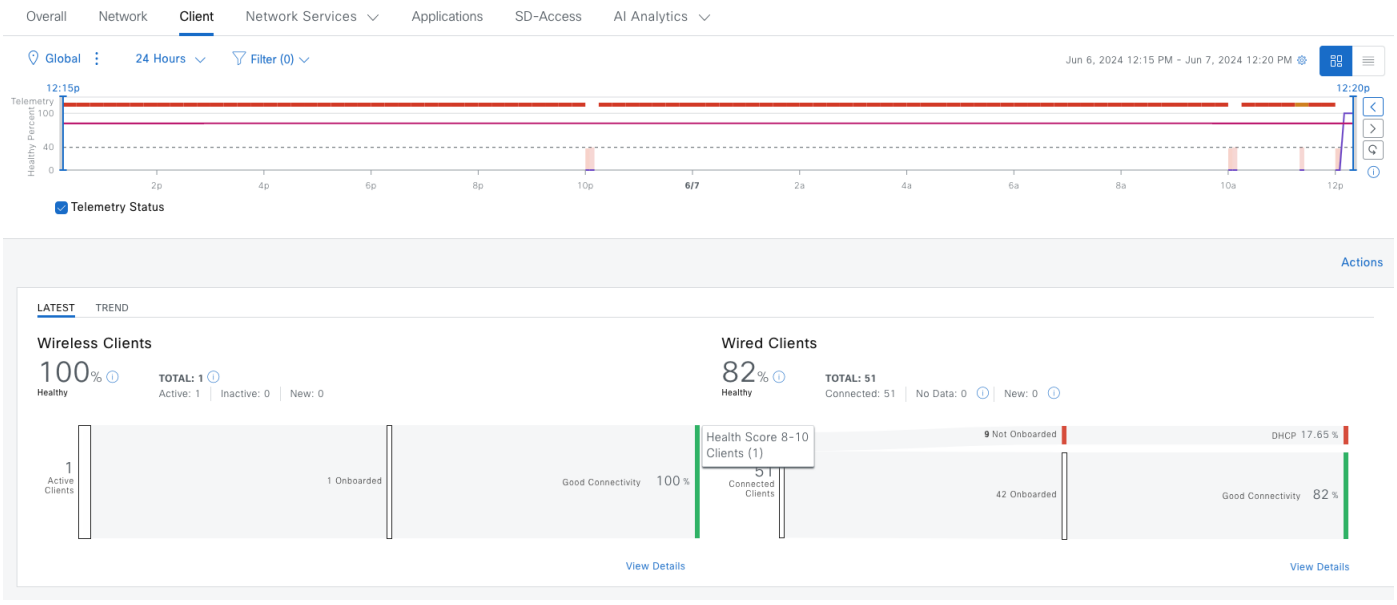
**ステップ 3.** [Device 360] ウィンドウにリダイレクトしたいデバイスをクリックして、詳細な正常性情報を確認します。

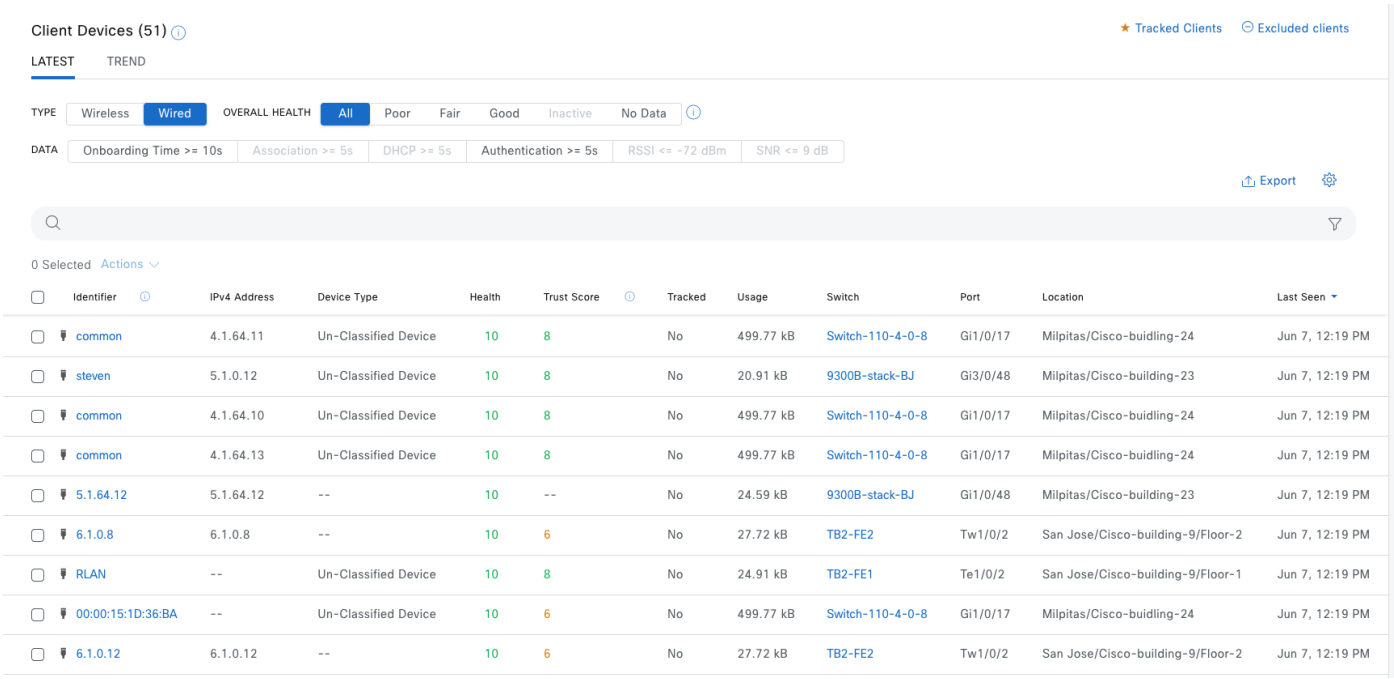



## クライアントの正常性のアシュアランス

個々のクライアントの正常性スコアは、最初のオンボーディングと、永続的な接続エクスペリエンスに基づいて計算されます。クライアントの正常性ダッシュボードは、クライアントがネットワークにどの程度接続できるかについての分析概要を示します。クライアントが接続されると、ダッシュボードにはクライアント接続エクスペリエンスの詳細が表示されます。

全体的なクライアントの正常性スコアは、正常なクライアント数を、クライアントのタイプ（有線またはワイヤレス）に基づいたクライアントの合計数で割った数値に基づきます。






**ステップ 1.** [Network Health] ウィンドウと同様に、フィルタと**検索**機能を使用してクライアントを見つけます。

**ステップ 2.** [Client 360] ウィンドウにリダイレクトするクライアントをクリックして、詳細を確認します。

例の図 69 と図 70 は、[Client 360] ウィンドウでのクライアントの詳細を示しています。

**図 71.　　ワイヤレスクライアント「lily」**

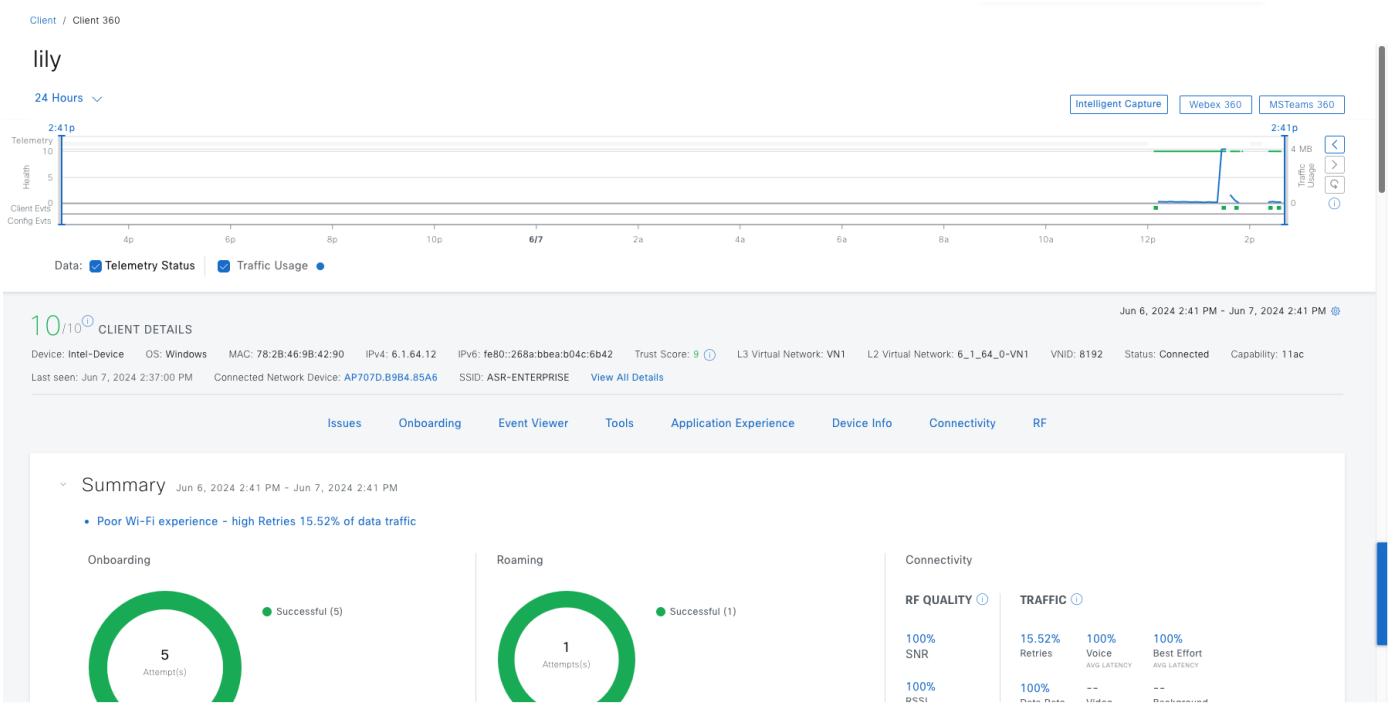
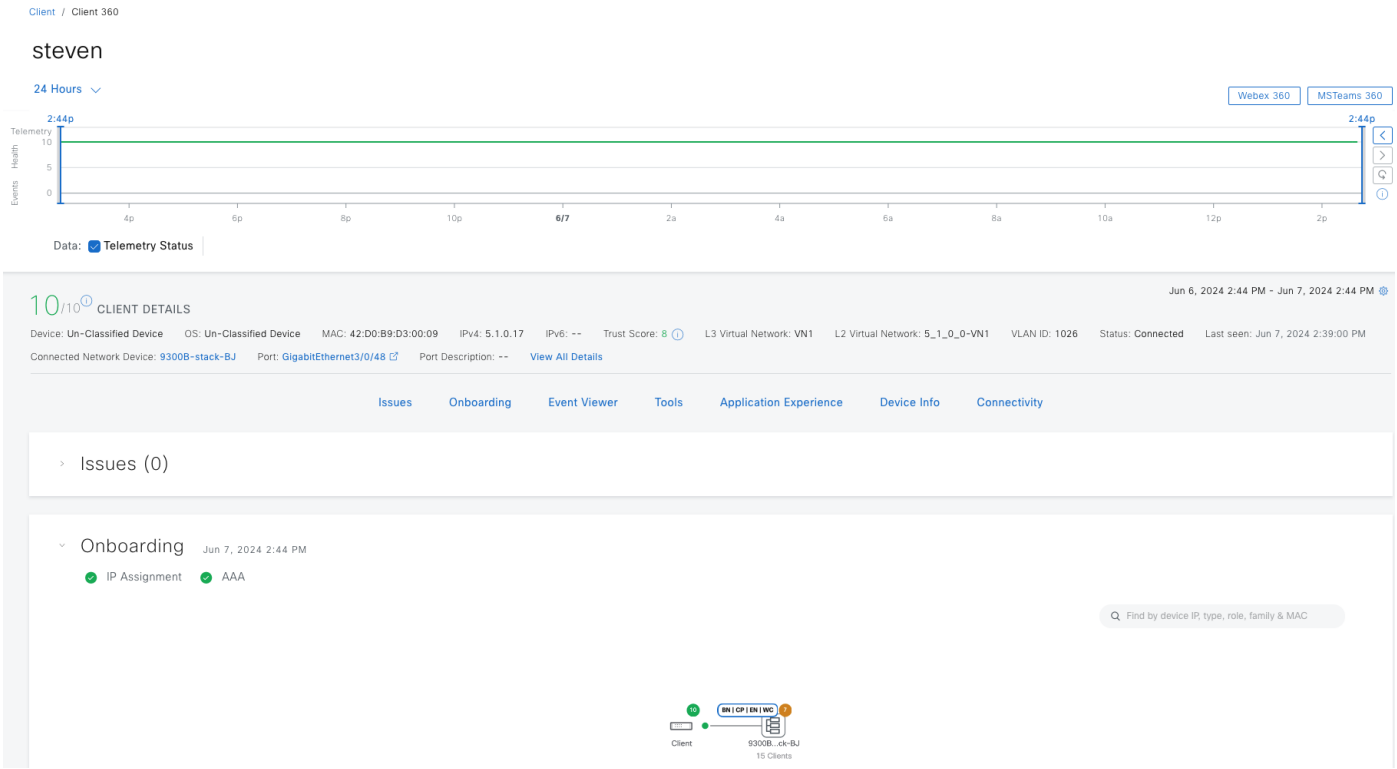


**図 72.　　有線クライアント「steven」**



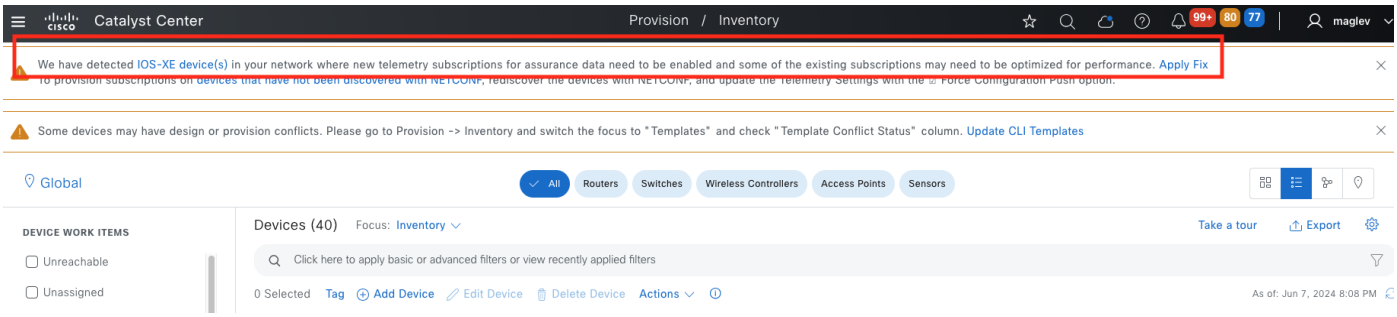

## Cisco SD-Access のアシュアランス

SD-Access アシュアランスは、ファブリックロールで動作するデバイスでテレメトリ サブスクリプションをプロビジョニングして、ほぼリアルタイムのアシュアランスデータを収集します。この機能を使用するには、ファブリックデバイスを NETCONF 用に設定して、NETCONF で検出されるようにし、Catalyst Center テレメトリを有効にする必要があります。

Catalyst Center のアップグレード後、デバイスで新しいテレメトリ サブスクリプションをプロビジョニングします。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Provision] > [Inventory] の順に選択します。新しいテレメトリ サブスクリプションがある場合、[Inventory] ウィンドウの上部にバナーが表示されます。

**ステップ 2.** [Apply Fix] をクリックして、新しいテレメトリ サブスクリプションをプッシュします。Catalyst Center は、更新が必要なデバイスを自動的に選択します。




アシュアランスで Cisco SD-Access の正常性を確認するには、次の手順を実行します。

**ステップ 1.** 左上隅にあるメニューアイコンをクリックして [Assurance] > [Health] の順に選択し、[SD-Access] タブをクリックします。

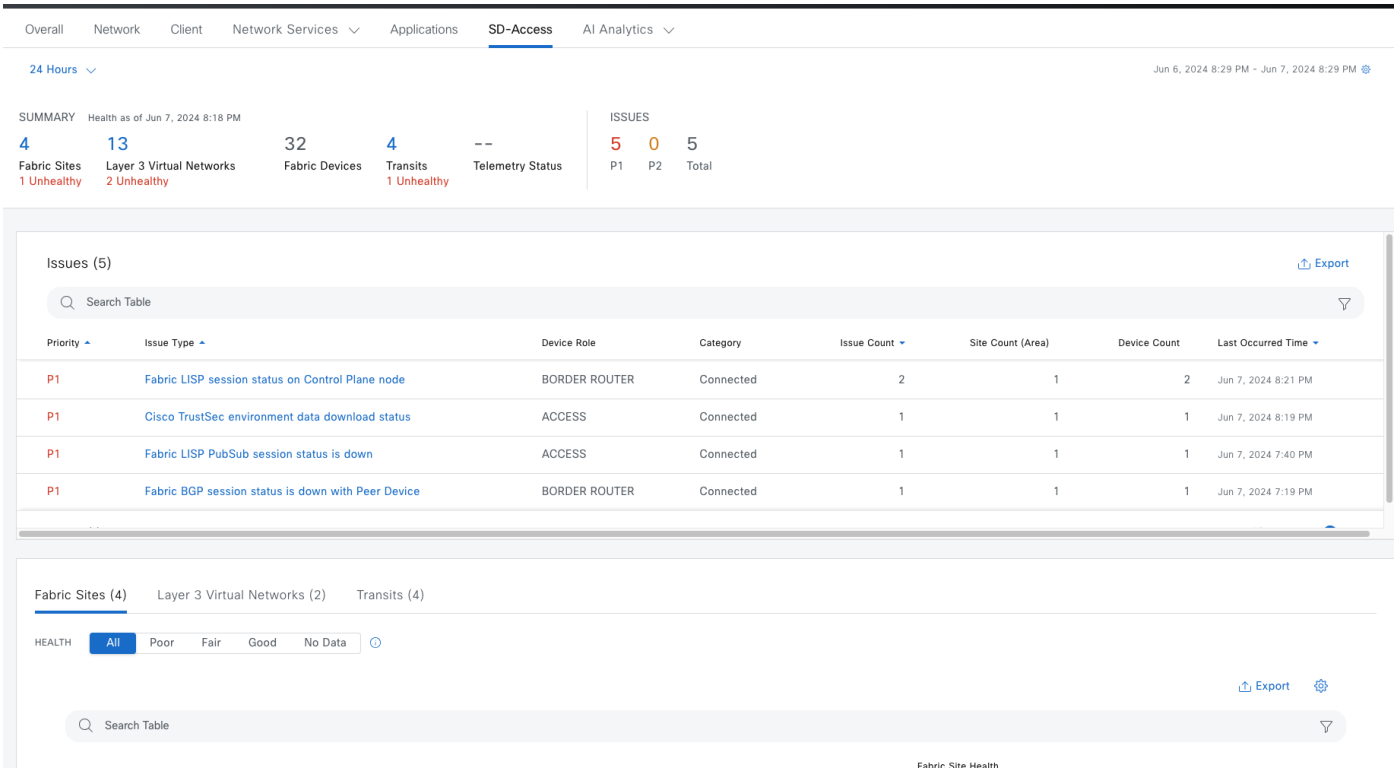
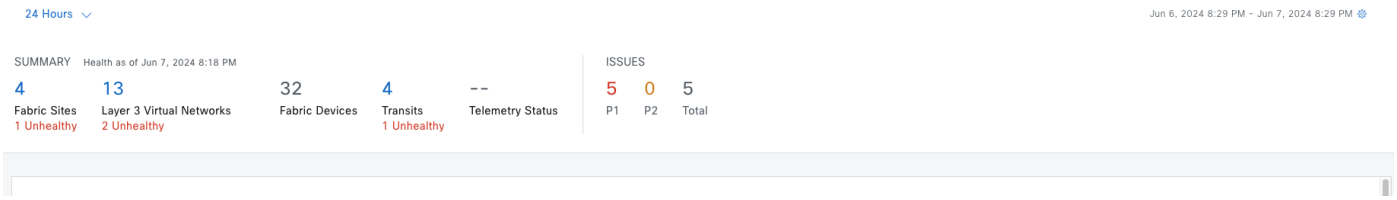
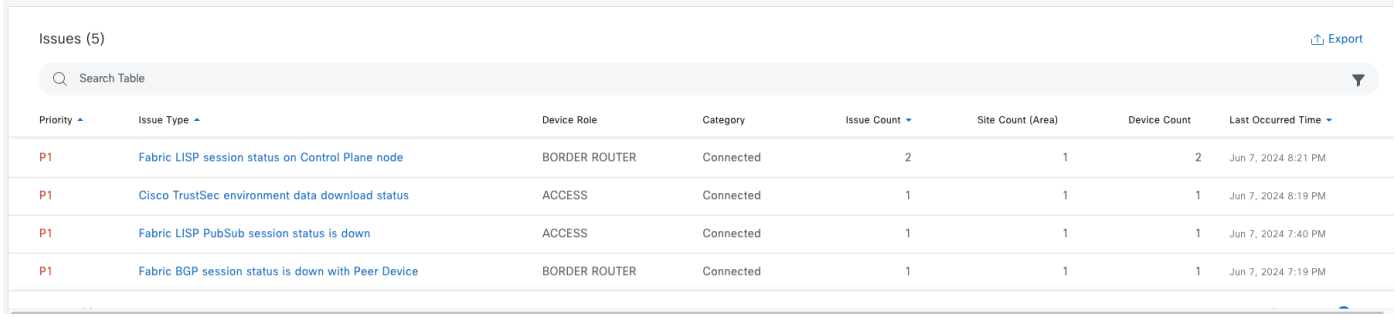



**図 73.　[Summary] ダッシュレット**




| アイテム | 説明 |
|---|---|
| SUMMARY | ◦ [Fabric Sites]：ファブリックサイトの数。<br>◦ [Layer 3 Virtual Networks]：レイヤ 3 仮想ネットワークの数。<br>◦ [Fabric Devices]：ファブリックデバイスの数。<br>◦ [Transits]：トランジットネットワークとピアネットワークの数。<br>◦ [Telemetry Status]：ファブリックサイトのテレメトリステータスを表示します。 |
| ISSUES | ◦ [P1]：優先度 1 の問題の数。<br>◦ [P2]：優先度 2 の問題の数。<br>◦ [Total]：P1、P2、および P3 の問題の合計数。 |

**図 74.　　[Issues] ダッシュレット**

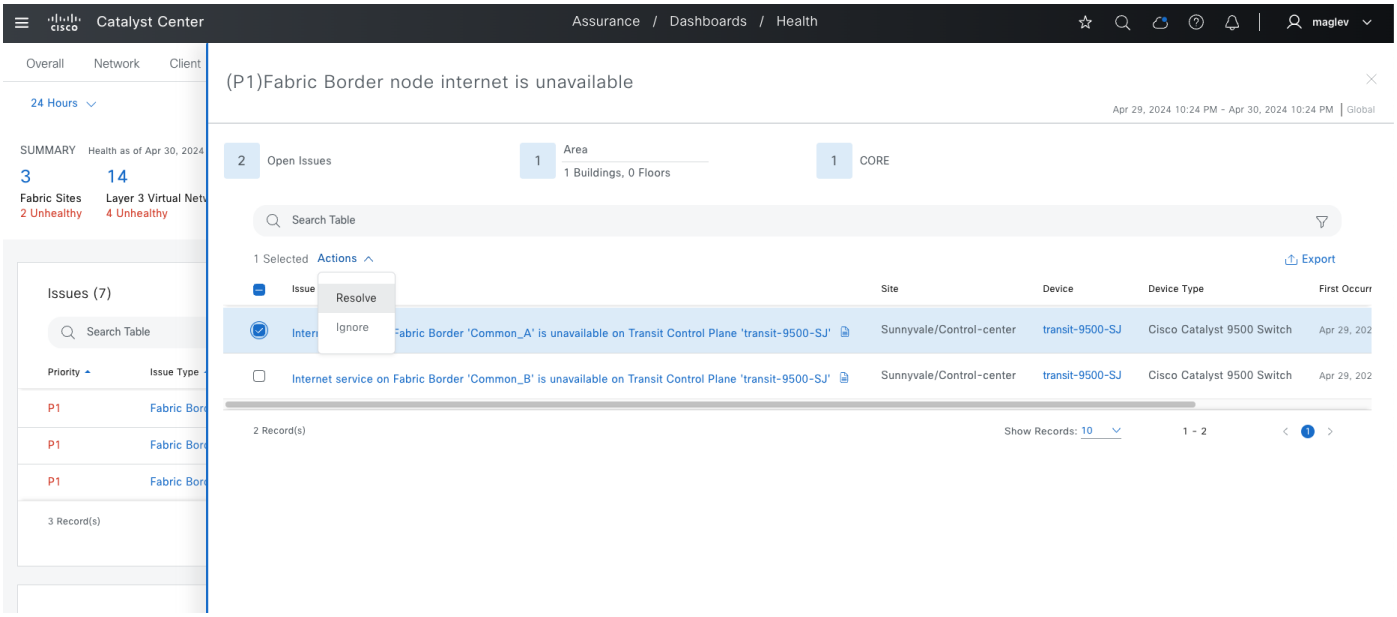



対処する必要がある場合、上位 10 件の問題が表示されます。問題は色分けされ、事前割り当てされた **P1** から始まる優先度レベルで並び替えられます。

**ステップ 2.**　問題をクリックすると、スライドインペインが開き、問題のタイプに関する追加の詳細が表示されます。

**ステップ 3.**　スライドインペインで問題のインスタンスをクリックします。必要に応じて、次の操作を実行できます。

- 問題のインスタンスを解決するには、[Status] > [Resolve] の順に選択します。
- 問題のインスタンスを無視するには、次の手順を実行します。
  a. [Status] > [Ignore] の順に選択します。
  b. スライダで問題を無視する時間数を設定して、確認します。
- 問題の詳細を確認するには、その問題をクリックします。



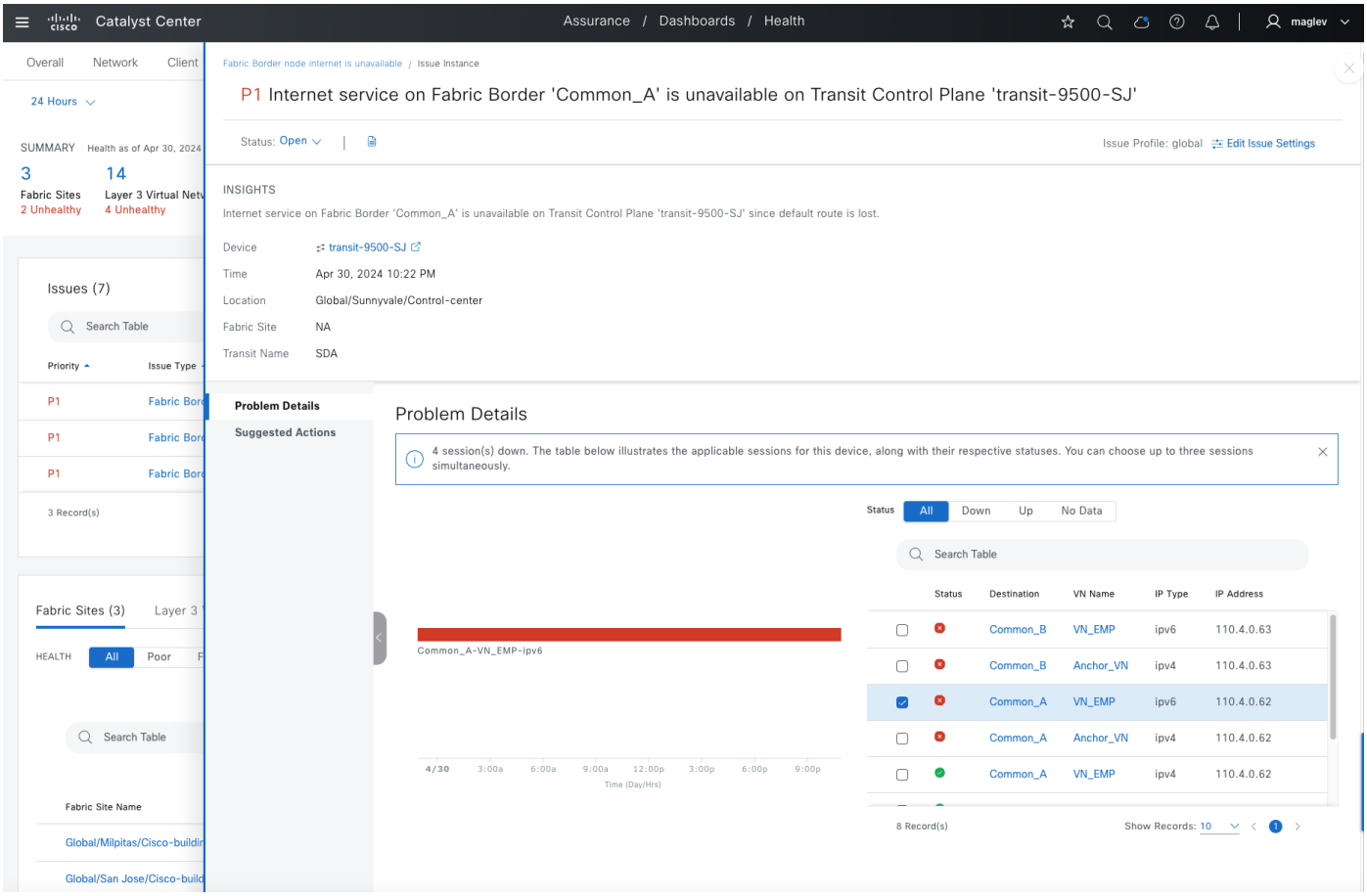
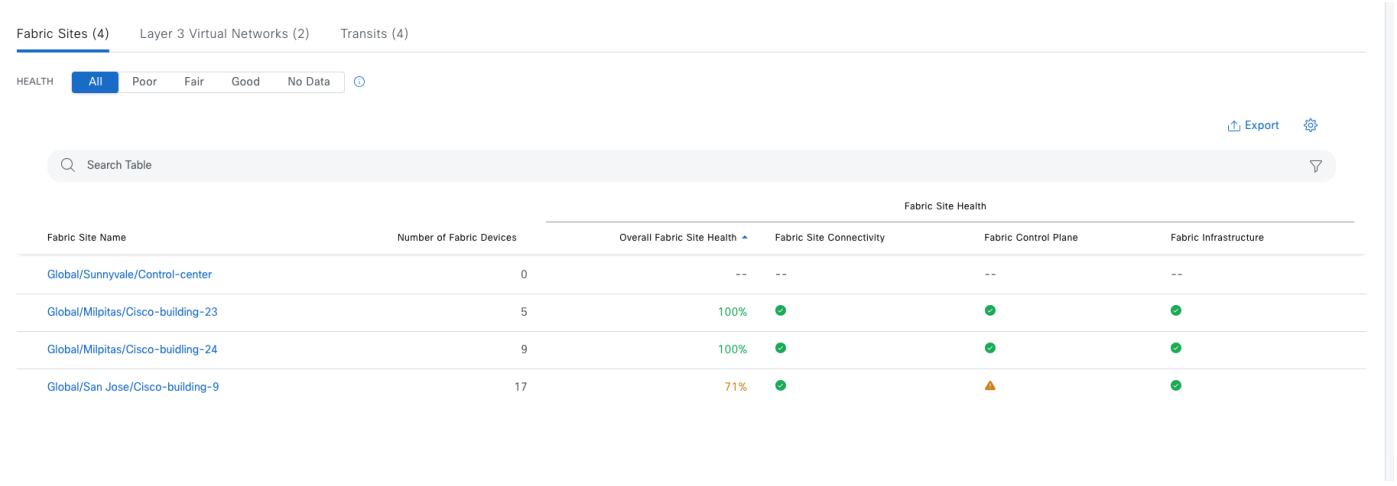



**図 75. [Fabric Sites] ダッシュレット**



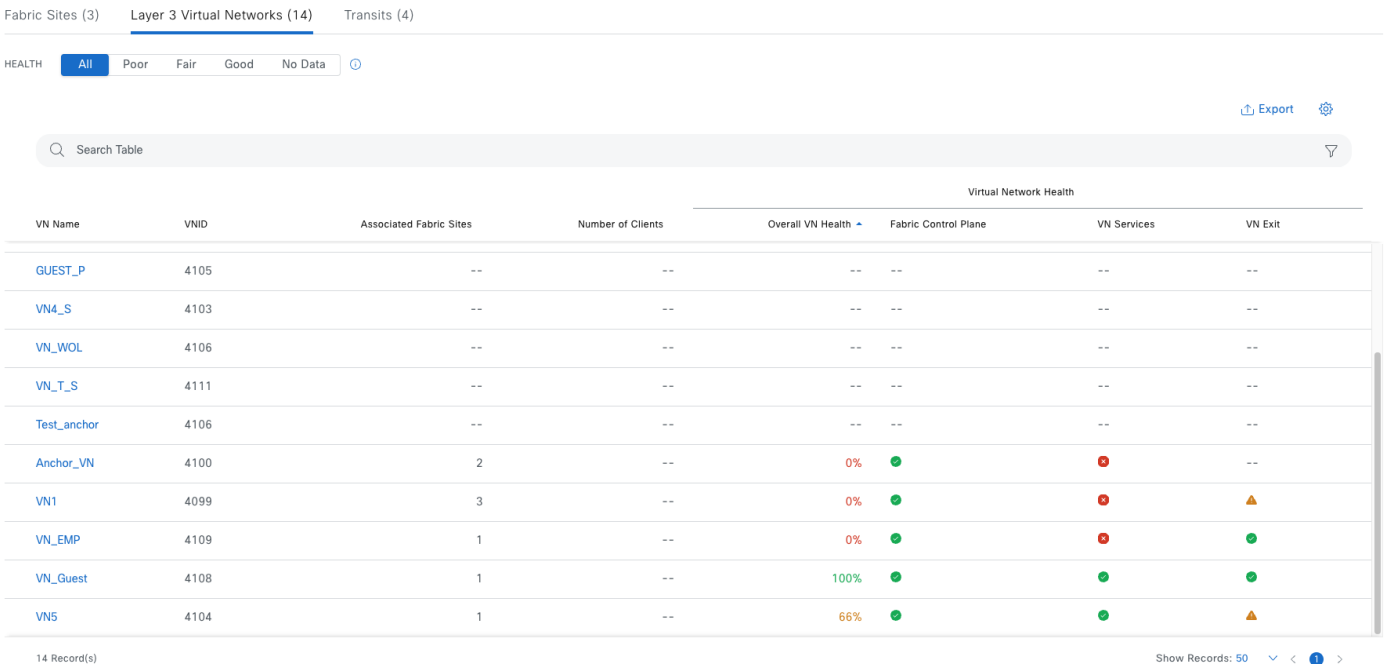
ファブリックサイトの詳細情報を表形式で表示します。デフォルトでは、[Fabric Site] テーブルには次の情報が表示されます。

- [Fabric Site Name]：ファブリックサイトの名前
- [Number of Fabric Devices]：ファブリックサイト内のファブリックデバイスの数
- [Fabric Site Health]：
  - [Overall]：ファブリックサイトの全体的な正常性。名前をクリックして、[Fabric Site 360] ウィンドウにリダイレクトします。ファブリックサイトの正常性の監視を参照してください。
  - [Fabric Site Connectivity]：ファブリックサイトとの接続の正常性
  - [Fabric Control Plane]：ファブリックサイトのコントロールプレーンの正常性
  - [Fabric Infrastructure]：ファブリックサイトを構成するデバイスの正常性

次のオプションを使用して、クライアントの正常性を基にテーブルをフィルタリングします。

- **All**
- [Poor]：正常性スコアが 1 ～ 3 のファブリックサイト
- [Fair]：正常性スコアが 4 ～ 7 のファブリックサイト
- [Good]：正常性スコアが 8 ～ 10 のファブリックサイト
- [No Data]：データのないファブリックサイト

**図 76.　[Layer 3 Virtual Networks] ダッシュレット**

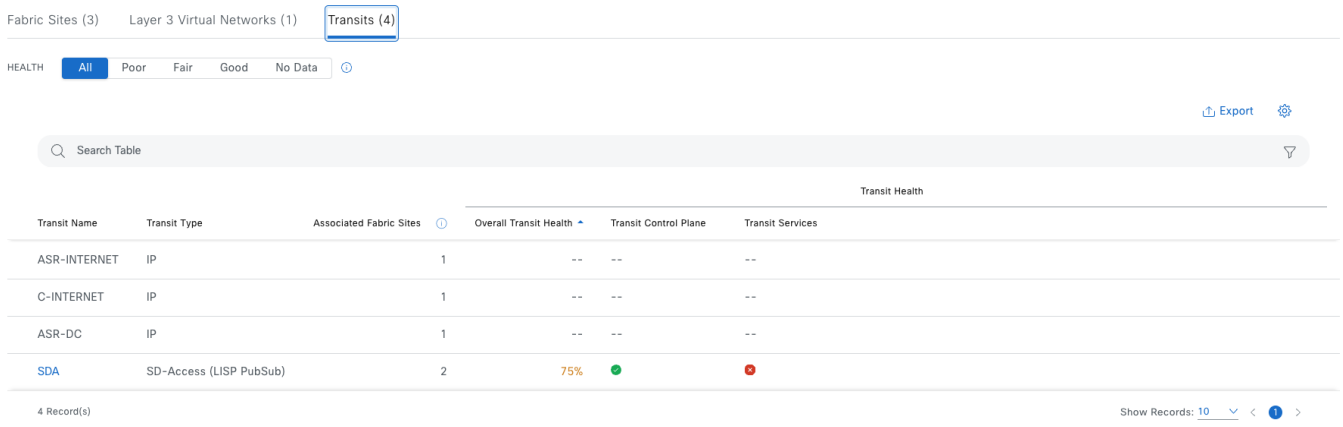


詳細な VN テーブル情報を表示します。デフォルトでは、VN テーブルには次の情報が表示されます。

- [VN Name]：VN の名前。名前をクリックして、VN360 ウィンドウにリダイレクトします。「VN 360 を使用したレイヤ 3 VN の正常性の監視」を参照してください。
- [Associated Fabric Sites]：VN 内の関連サイトの数
- [Number of Clients]：VN 内のエンドポイントの数
- [Virtual Network Health]：
  - [Overall VN Health]：VN の全体的な正常性
  - [Fabric Control Plane]：VN のコントロールプレーンの正常性
  - [VN Services]：VN サービスの正常性
  - [VN Exit]：ピアデバイスへの BGP セッションの正常性

**注：　レイヤ 3 仮想ネットワーク**は **INFRA_VN** を監視せず、カスタマイズされた VN と **Default_VN**（使用している場合）のみを監視します。

**図 77.　[Transits] ダッシュレット**




トランジットネットワークおよびピアネットワークの詳細情報を表形式で表示します。デフォルトでは、トランジットネットワークおよびピアネットワークのテーブルには次の情報が表示されます。

- [Transit Name]：トランジットネットワークまたはピアネットワークの名前。「VN 360 を使用したレイヤ 3 VN の正常性の監視」を参照してください。
- [Transit Type]：IP または SD-Access
- [Associated Fabric Sites]：関連付けられているサイトの数
- [Transit Health]：
  - [Overall]：トランジットネットワークおよびピアネットワークの全体的な正常性

- [Transit Control Plane]：トランジット コントロール プレーンの正常性
- [Transit Services]：インターネットの可用性の正常性

## Fabric Site 360 を使用したファブリックサイトの正常性の監視

[Fabric Dashlet] セクションに示されているように、ファブリックサイトをクリックしてサイトの詳細な正常性情報を表示します。

正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

- [Fabric Site Health]：正常性は、このサイトの正常なファブリックノードの割合です。

チャート内のハイパーリンクされたファブリックカテゴリをクリックしてサイドペインを開き、それぞれの KPI サブカテゴリを表示できます。

| KPI 名 | KPI のサブカテゴリ | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| AAA Server Status | Fabric Infrastructure | あり | 10 分/10 分 | エッジノードと拡張ノードから各 AAA サーバーのサーバーステータスを監視します |
| CTS Environment Data Download | Fabric Infrastructure | あり | 10 分/10 分 | Cisco ISE サーバーのエッジ、PEN、および SBEN での Cisco TrustSec 環境データのダウンロードを監視します。AAA サーバーのステータスがダウンした場合、Cisco TrustSec の正常性も自動的に停止します。<br><br>デバイスイメージ（> = 17.9）が必要 |
| Extended Node Connectivity | Fabric Site Connectivity | なし | 5 分/5 分 | 設定されたポートチャネル上の拡張ノードとエッジノード間のリンクステータスを監視します |
| Control plane reachability | Fabric Site Connectivity | なし | 10 分/10 分 | ファブリック ワイヤレス コントローラ ノードからローカル コントロール プレーン ノードへの IPSLA 到達可能性ステータスを監視します |
| LISP Session Status | Fabric Control Plane | あり | 10 分/10 分 | ボーダーノードとエッジノードからローカル コントロール プレーン ノードへの LISP プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| Pub/Sub Session Status for INFRA_VN | Fabric Infrastructure | あり | 10 分/10 分 | INFRA_VN のボーダーノードからローカル コントロール プレーン ノードへの Pub/Sub プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| BGP session from Border to Control Plane | Fabric Site Connectivity | あり | 10 分/10 分 | INFRA_VN についてのみ、特定のボーダーノードからローカル コントロール プレーン ノードへの BGP セッションステータ |

| KPI 名 | KPI のサブカテゴリ | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| | | | | スを監視します。<br><br>デバイスイメージ（> = 17.10）が必要 |
| BGP session from Border to Peer Node for Infra_VN | Fabric Site Connectivity | あり | 10 分/10 分 | 特定のボーダーノードとその非ファブリックピアから BGP セッションステータスを監視します。セッションは、INFRA_VN のみ、および LISP/BGP と、Pub/Sub プロトコルサイトを使用した LISP の両方で追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |

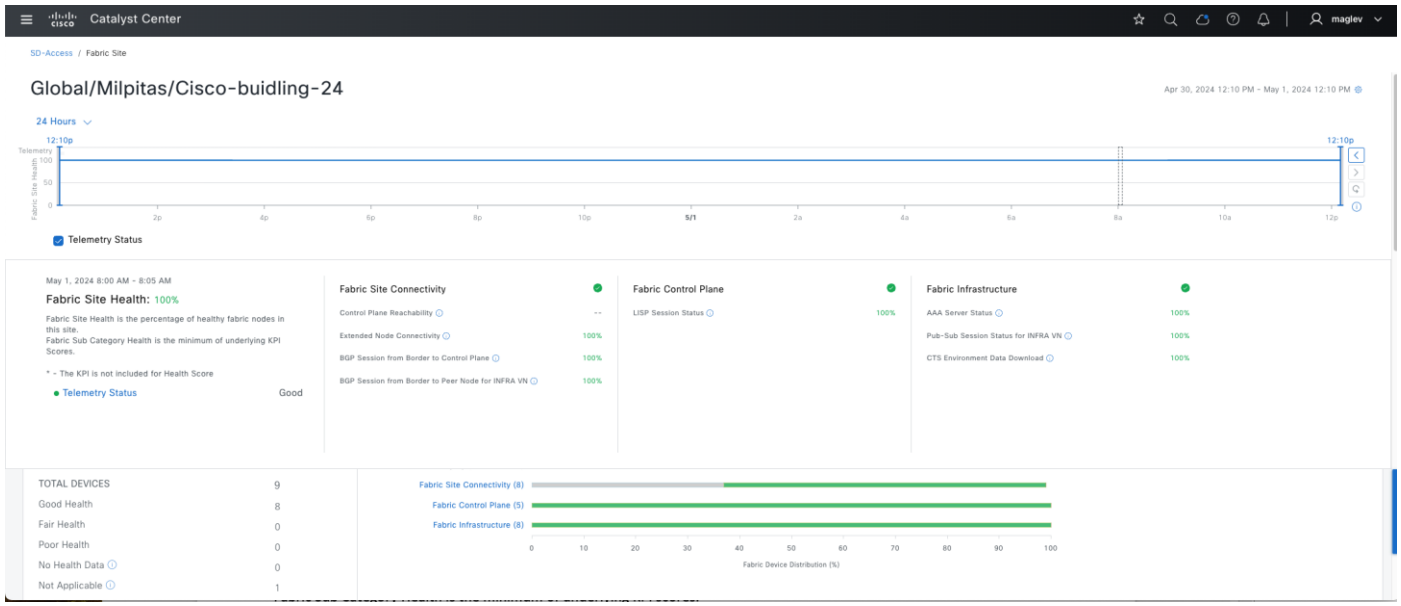
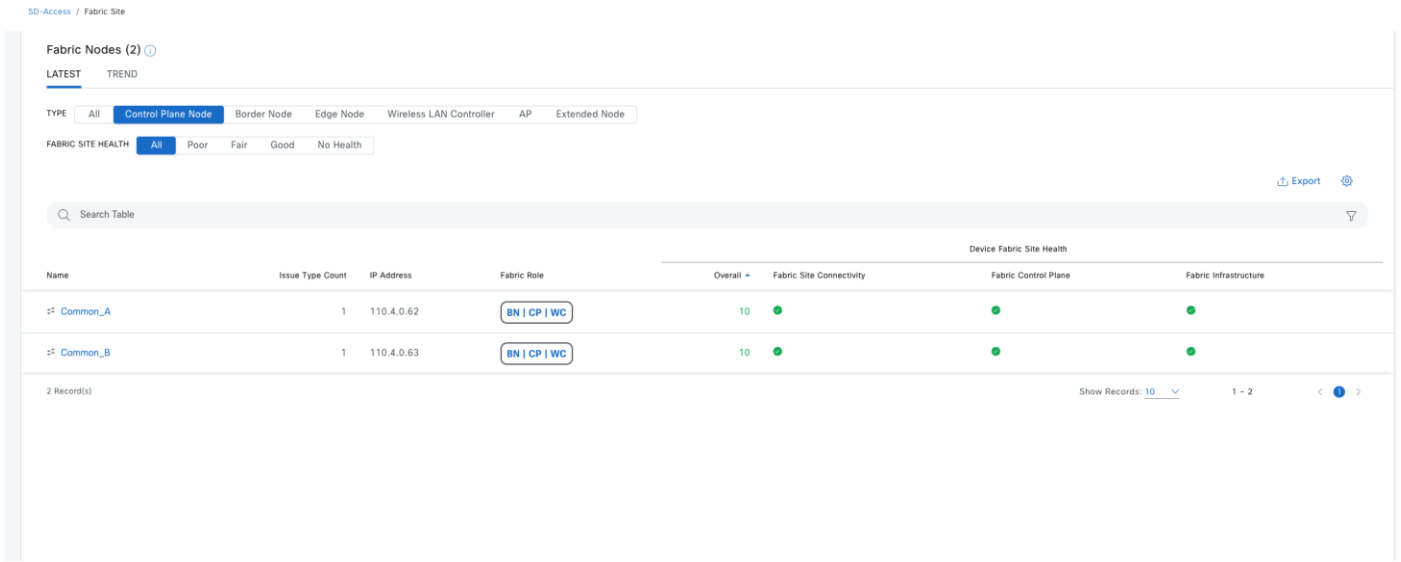



**図 78.　　[Fabric Nodes] ダッシュレット**



| アイテム | 説明 |
| --- | --- |
| TYPE | オプション（[All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric wireless controller]、[Fabric AP]、[Extended Node]）を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。 |
| FABRIC SITE HEALTH | 次の使用可能なオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。<br>• All<br>• [Poor]：正常性スコアが 1 ～ 3 のデバイス。<br>• [Fair]：正常性スコアが 4 ～ 7 のデバイス。<br>• [Good]：正常性スコアが 8 ～ 10 のデバイス。<br>• [No Health]：正常性データのないデバイス。 |
| [Fabric Node] テーブル | 選択したサイトのすべてのファブリックノードのデバイス情報を表形式で表示します。<br>**注：**全体的な正常性スコアは、ファブリックサイト接続とファブリック インフラストラクチャの KPI メトリック正常性スコアの最小サブスコアです。<br>[Name]、[Issue Type Count]、および [Fabric Role] 列には、ファブリック名、問題数、およびファブリックロール（エッジ、ボーダー、マップサーバーなど）が表示されます。<br>[Device Fabric Site Health] の [Overall] 列で、正常性スコアの上にマウスカーソルを合わせます。全体の [Device Fabric Site Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。<br>カーソルを [Fabric Site Connectivity]、[Fabric Control Plane]、および [Fabric Infrastructure] アイコンに合わせると、正常性スコアが表示されます。 |

## VN 360 を使用したレイヤ 3 VN の正常性の監視

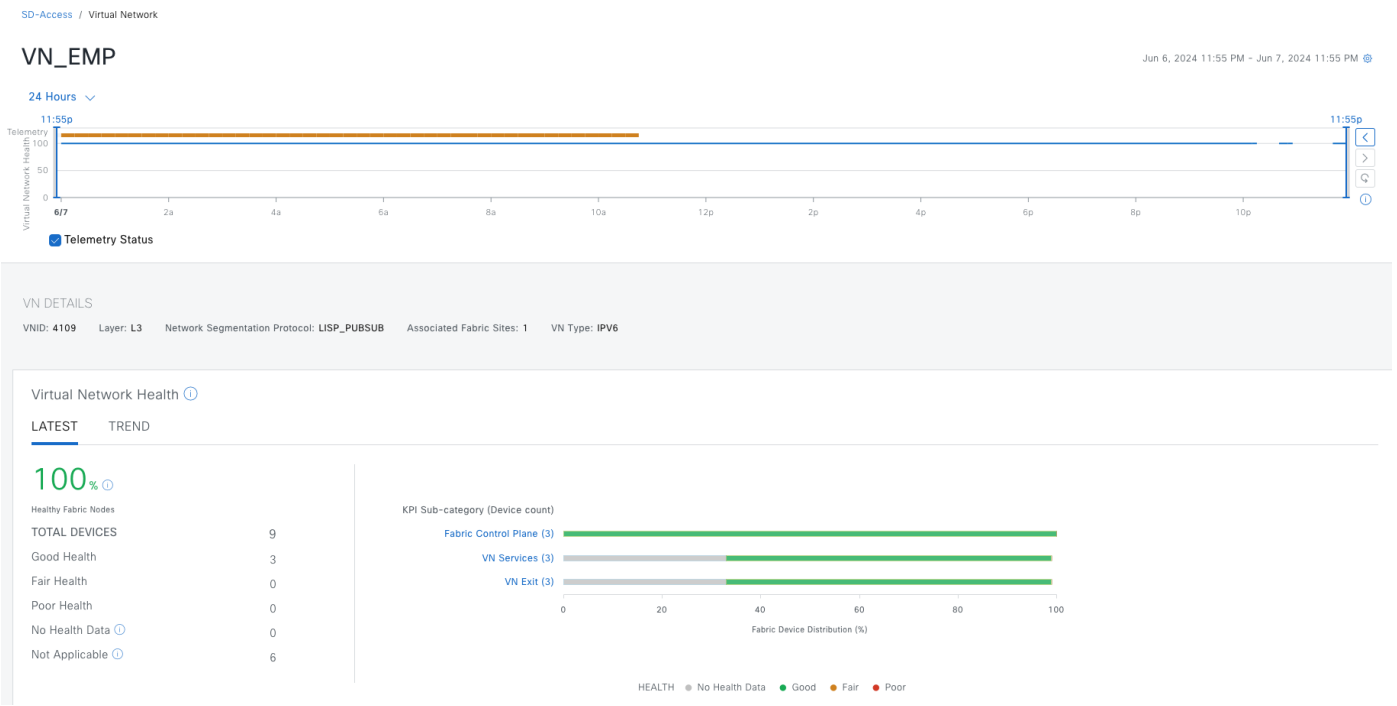
前のセクションで示したように、VN をクリックして、特定の VN の詳細な正常性情報を表示します。

VN の正常性スコアは、VN における正常なデバイスの割合です。VN のカテゴリ正常性は、対応するサブカテゴリの KPI スコアの最小値です。VN シリーズには、ボーダーからピアノード、マルチキャスト（外部 RP）、デフォルトのルート登録、および VN コントロールプレーンまでの BGP セッションが含まれます。

デフォルトで表示されます。左側のペインには、VN の正常性の概要スコアと、デバイスの合計数が表示されます。右側のペインには、チャートが表示されます。

- [Healthy Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。
- [Total Devices]：ファブリックデバイスの合計数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] 状態のデバイスの数。
- [Charts]：この色分けされたスナップショットビュー チャートには、KPI サブカテゴリが表示されます。

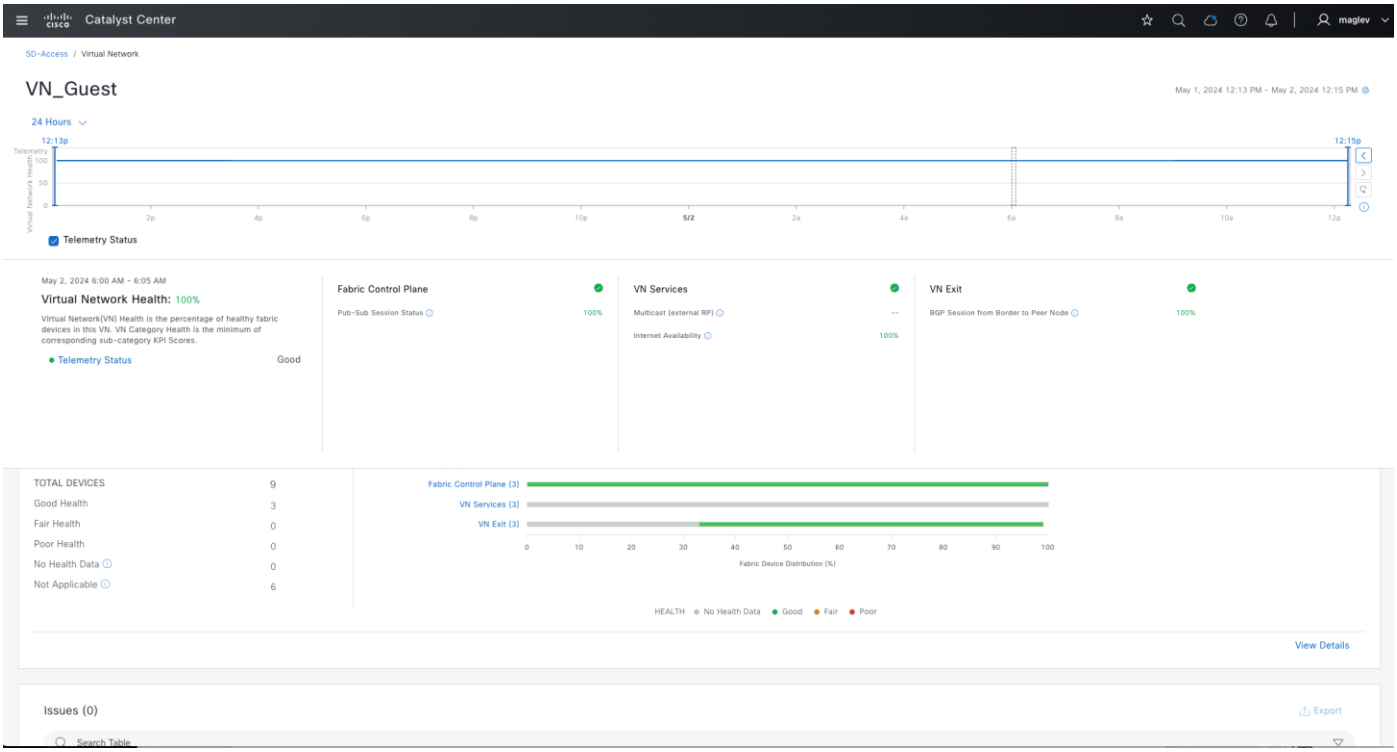
| KPI 名 | サブカテゴリ | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| Pub/Sub Session Status | Fabric Control Plane | あり | 10 分/10 分 | FiaB ノードの INFRA_VN および継承された VN を除くすべての VN について、ボーダーノードから、接続されたローカル コントロール プレーン ノードへの Pub/Sub プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| Internet Availability | VN service | あり | 10 分/10 分 | 外部ボーダーのデフォルトルートを監視し、それを Pub/Sub サイトを使用した LISP 内のコントロールプレーンノードで登録します。<br><br>外部ボーダーのデフォルトルートを監視し、それを Pub/Sub サイトを使用した LISP 内のトランジットプレーンノードで登録します。<br><br>デバイスイメージ（> =17.8）が必要 |
| Multicast (External RP) | VN service | なし | 10 分/10 分 | 外部マルチキャスト RP への到達可能性ステータスを監視します。 |
| BGP Session from Border to Peer Node | VN exist | あり | 10 分/10 分 | 特定のボーダーノードとその非ファブリックピアから BGP セッションステータスを監視します。セッションは、INFRA_VN を除くすべての設定済み VN、および Pub/Sub プロトコルサイトを使用した LISP/BGP と LISP の両方で追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |



いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。

チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。

ハイパーリンクされたカテゴリをクリックして、より詳しいサイドペインを開きます。




## トランジットの正常性の監視：Transit 360

前のセクションで示したように、トランジット（Cisco SD-Access タイプ）をクリックして、Cisco SD-Access トランジットの詳細な正常性情報を表示します。

正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

- [Transit Network Health]：正常性スコアは、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスの正常性は含まれません。[Fabric Category Health] は、基礎となる KPI スコアの最小値です。
- [Transit Site Control Plane]：トランジットの LISP セッションや Pub/Sub セッションなどの KPI サブカテゴリが一覧表示されます。トランジット正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイス、および関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。

デフォルトで表示されます。2 つのペインがあります。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。

- [Health Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。
- [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] 状態のデバイスの数。
- [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間のトランジット コントロール プレーンを示します。

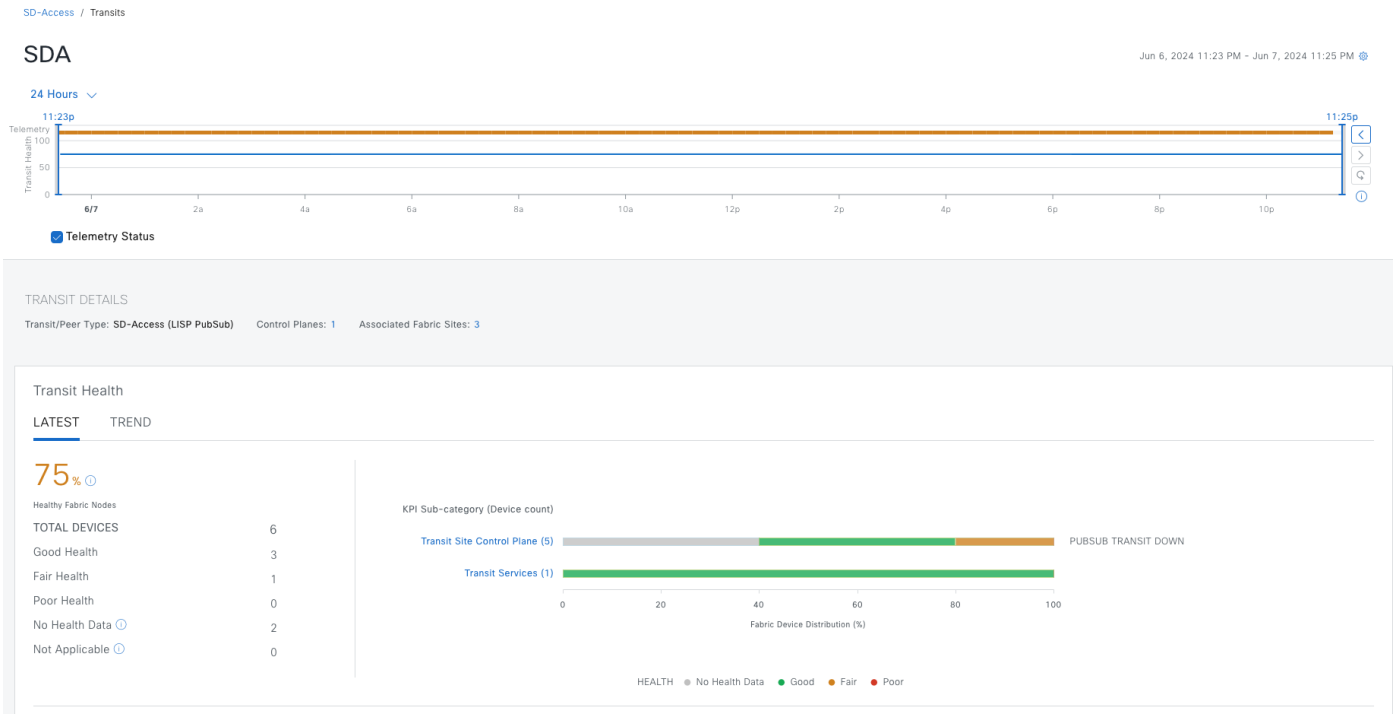
**ステップ 1.** いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。

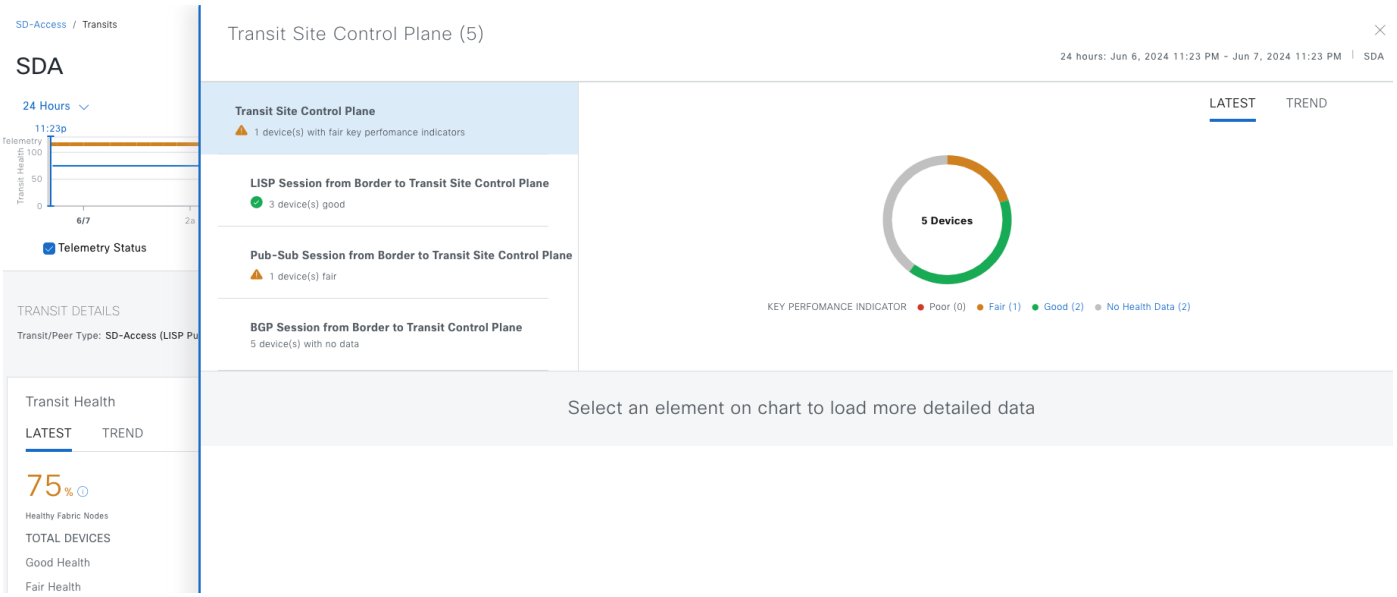
**ステップ 2.** チャート内のハイパーリンクされた [Transit Control Plane] をクリックしてサイドペインを開き、トランジット コントロール プレーンの次の KPI サブカテゴリを表示します。

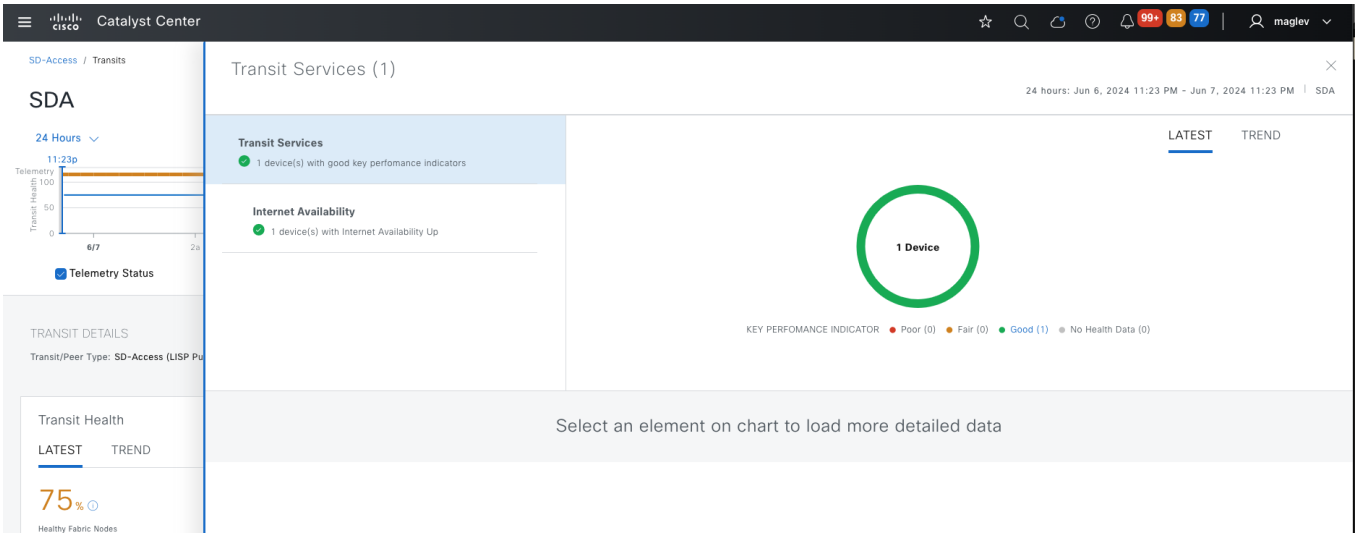
| KPI | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|
| Pub/Sub Session from Border to Transit Site Control Plane | あり | 10 分/10 分 | INFRA_VN のボーダーノードからローカル コントロール プレーン ノードへの Pub/Sub プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| LISP Session from Border to Transit Site Control Plane | あり | 10 分/10 分 | ボーダーノードから、接続されたトランジット コントロール プレーン ノードへの LISP プロトコルのセッションを監視します。<br><br>デバイスイメージ（> =17.6.2）が必要 |
| BGP Session from Border to Transit Control Plane | あり | 10 分/10 分 | 特定の外部ボーダーノードおよび接続されているトランジット コントロール プレーン ノードから BGP セッションのステータスを監視します。セッションは、LISP/BGP プロトコルサイト内の INFRA_VN が追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |

**ステップ 3.** チャート内のハイパーリンクされた [Transit Service] をクリックしてサイドペインを開き、トランジットサービスの次の KPI サブカテゴリを表示します。

| KPI | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|
| Internet Availability | あり | 10 分/10 分 | 外部ボーダーのデフォルトルートを監視し、Pub/Sub サイトを使用して LISP 内のトランジットプレーンノードに登録します。<br><br>デバイスイメージ（> = 17.8）が必要 |






**ステップ 4.** 上位 10 件の問題まで下にスクロールして、このトランジットおよび**関連するファブリックサイト**に対する**問題**を表示します。

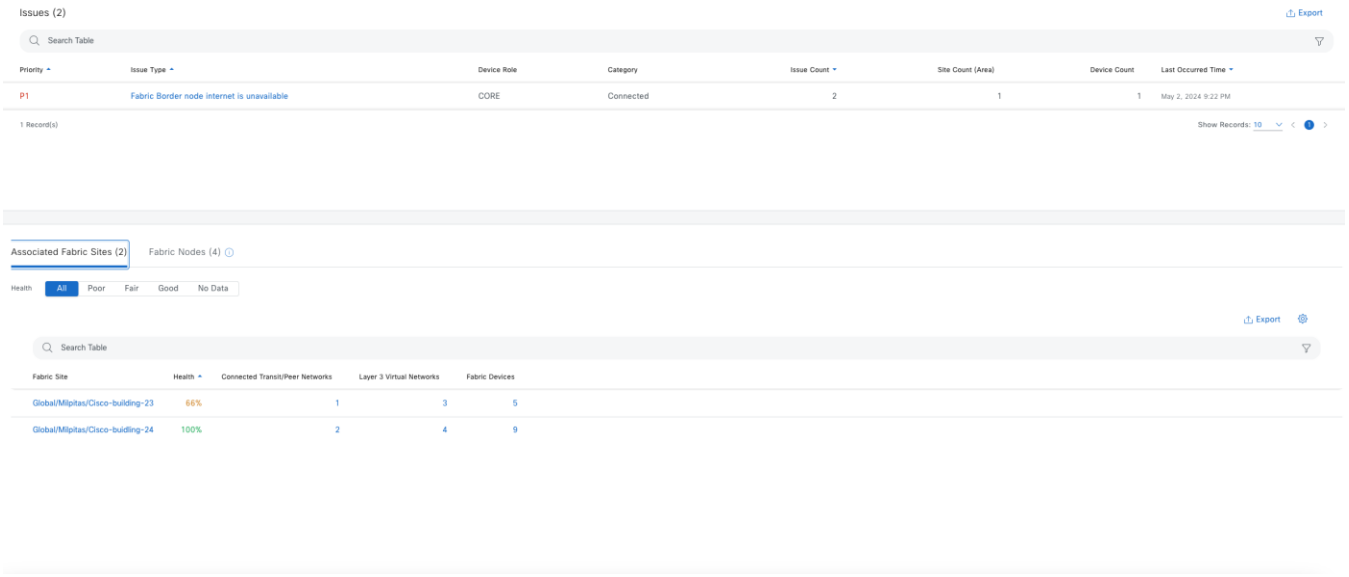
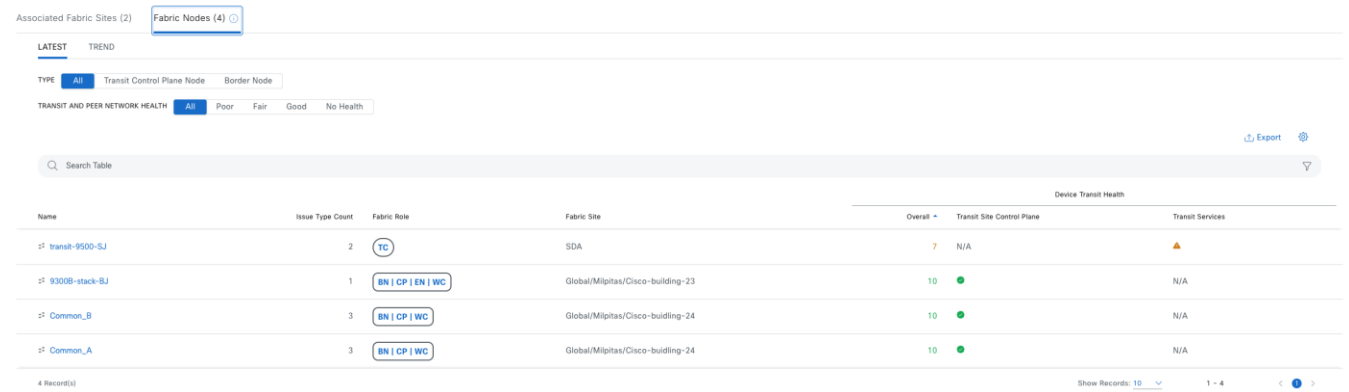



**図 79.** **ボーダーとトランジット コントロール プレーンの正常性を表示するファブリックノード**



## デバイス 360 を使用したデバイスの正常性の監視

[Device 360] ウィンドウを使用して、特定のデバイスの詳細なデバイス正常性情報を表示します。Catalyst Center によってプロビジョニングおよび管理されるすべてのファブリックデバイスが監視されます。Catalyst Center は、さまざまな KPI と、さまざまなファブリックロールに基づいた情報を提供します。

**図 80.　　ファブリックエッジ**

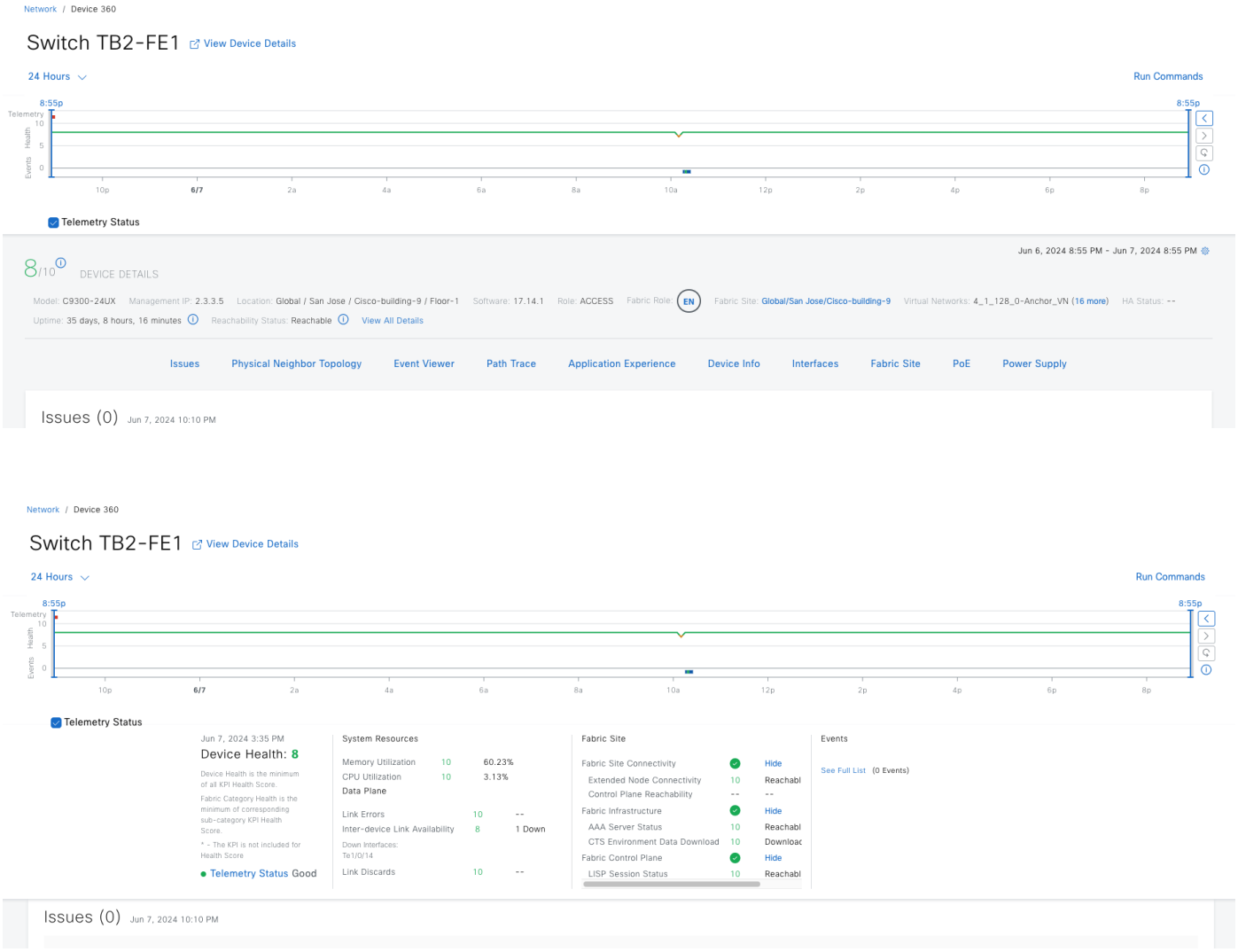


**図 81.　　コントロールプレーンと組み込みワイヤレスコントローラを使用したファブリックボーダー**

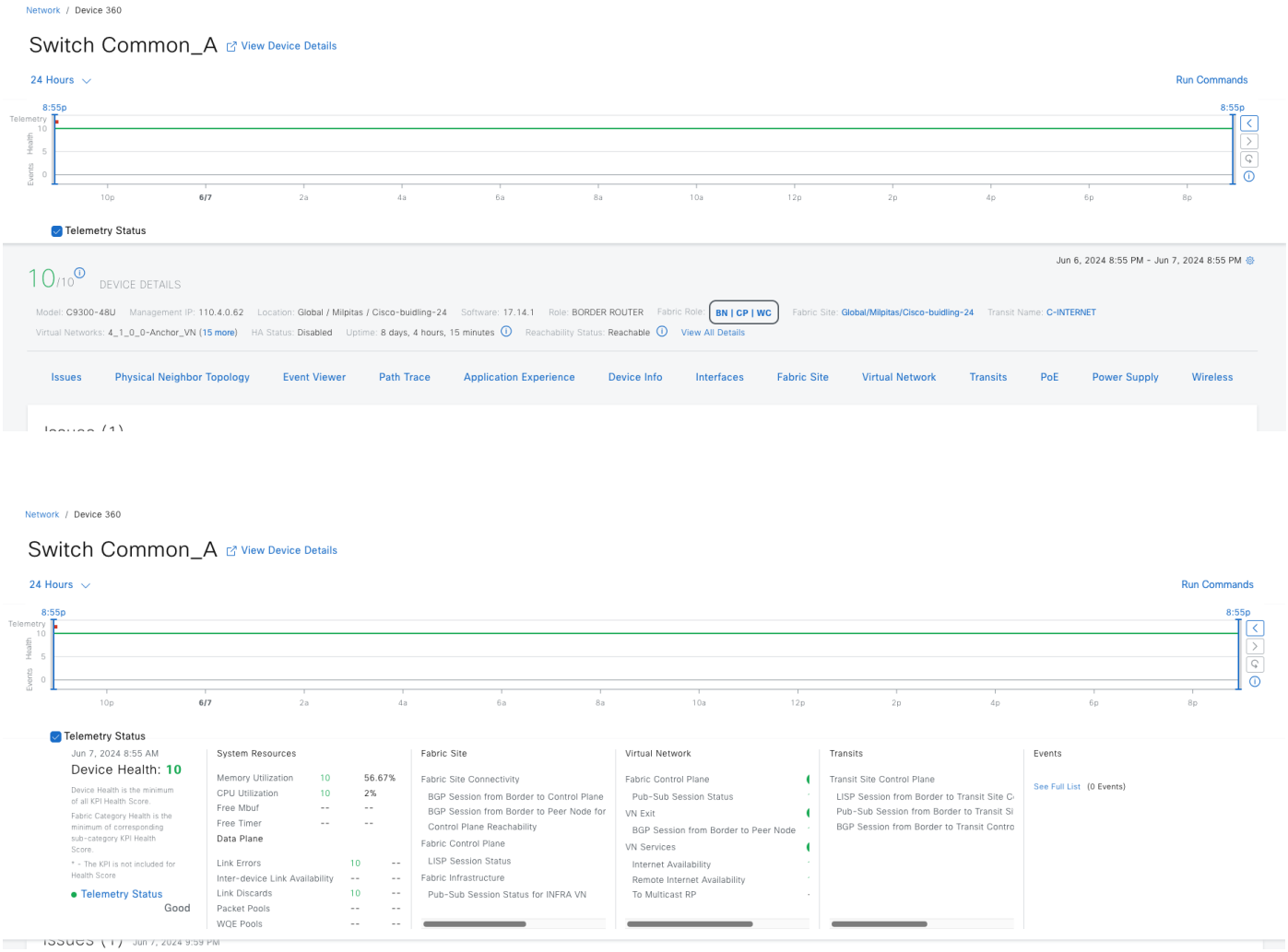
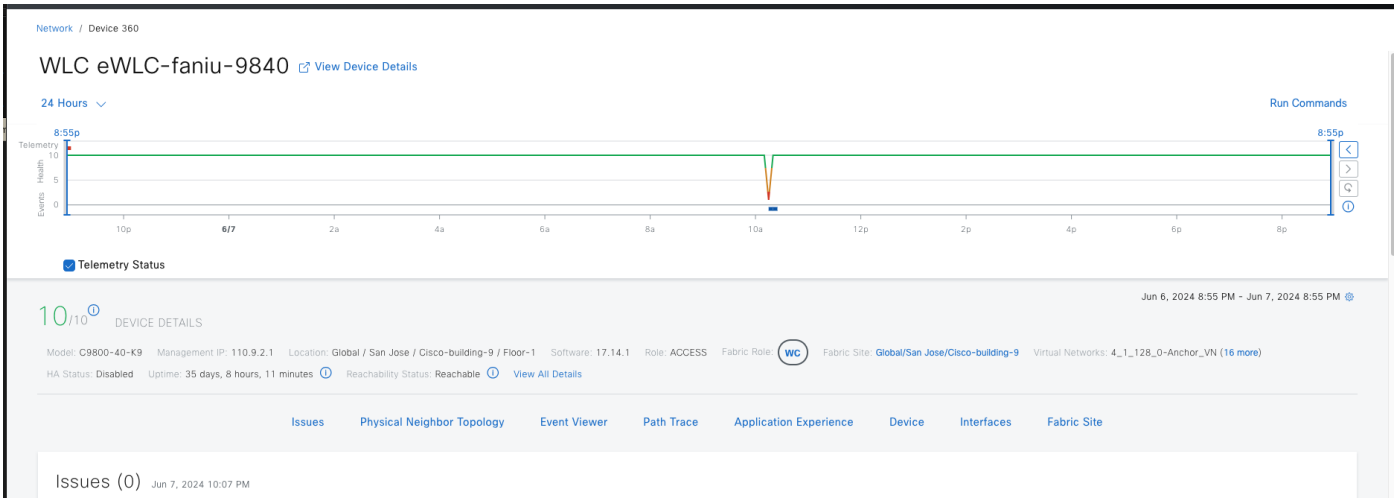



**図 82.　　ファブリック ワイヤレス コントローラ**



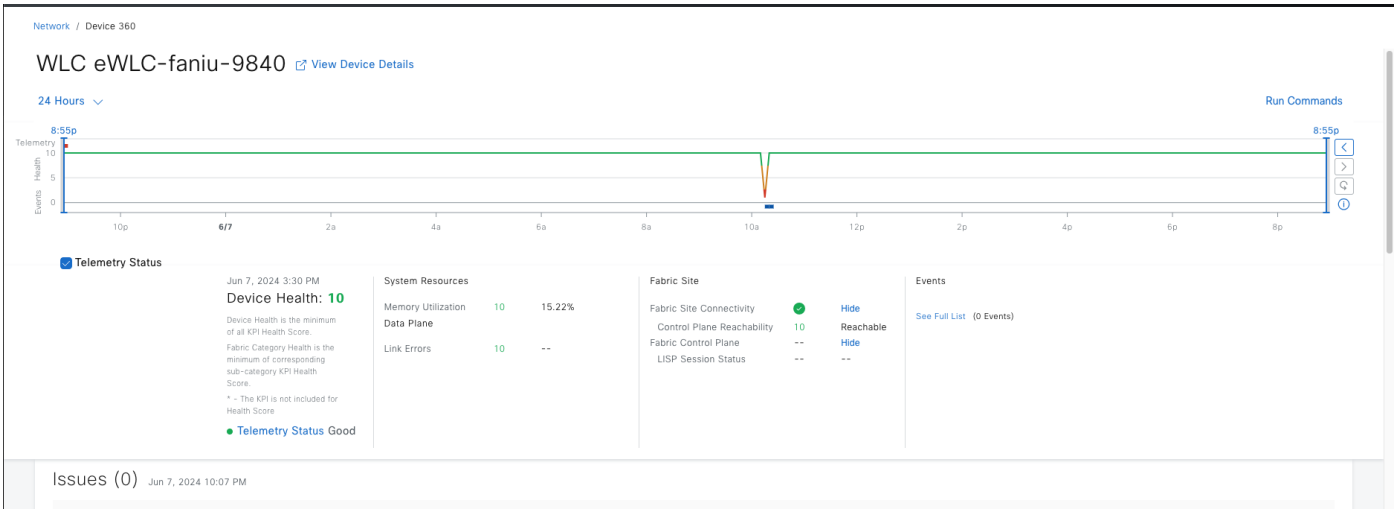
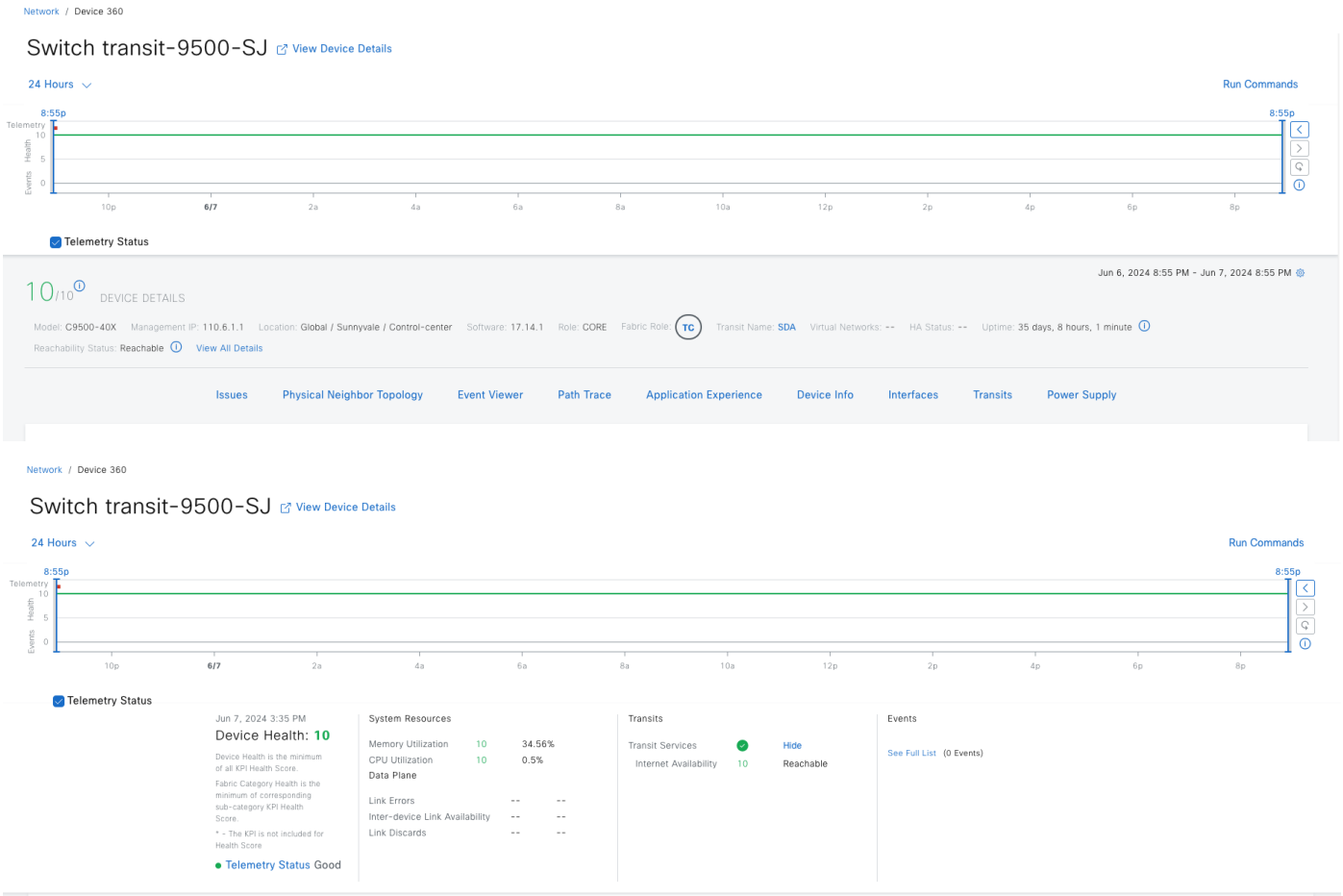
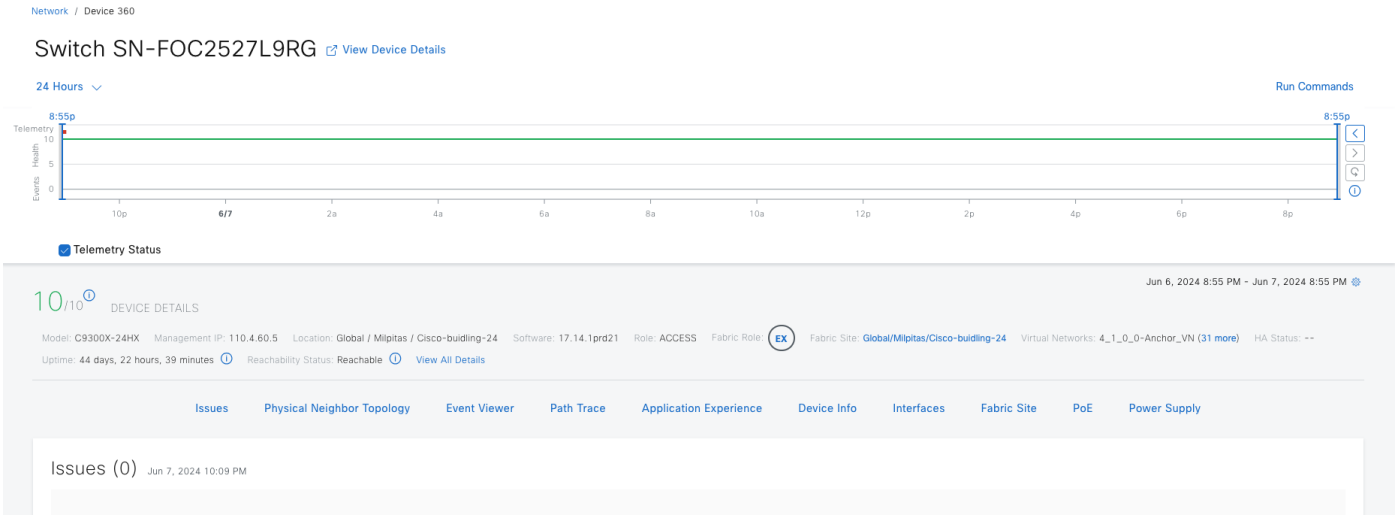
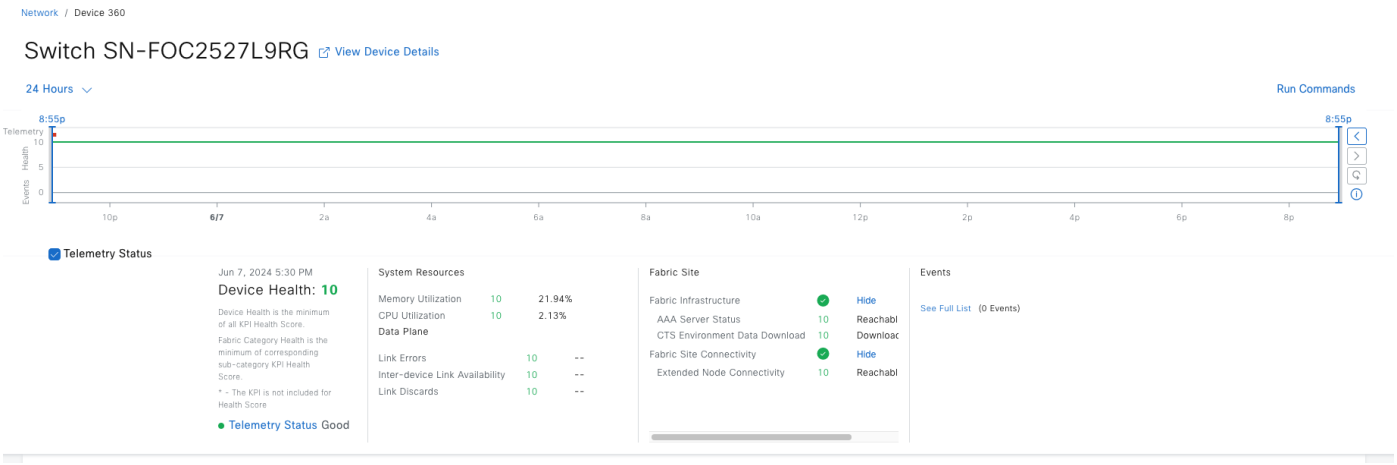



**図 83.　　トランジット コントロール プレーン**



## 図 84.　　ポリシー拡張ノード




## 図 85.　　AP：正常性スコアの計算にファブリック KPI がない

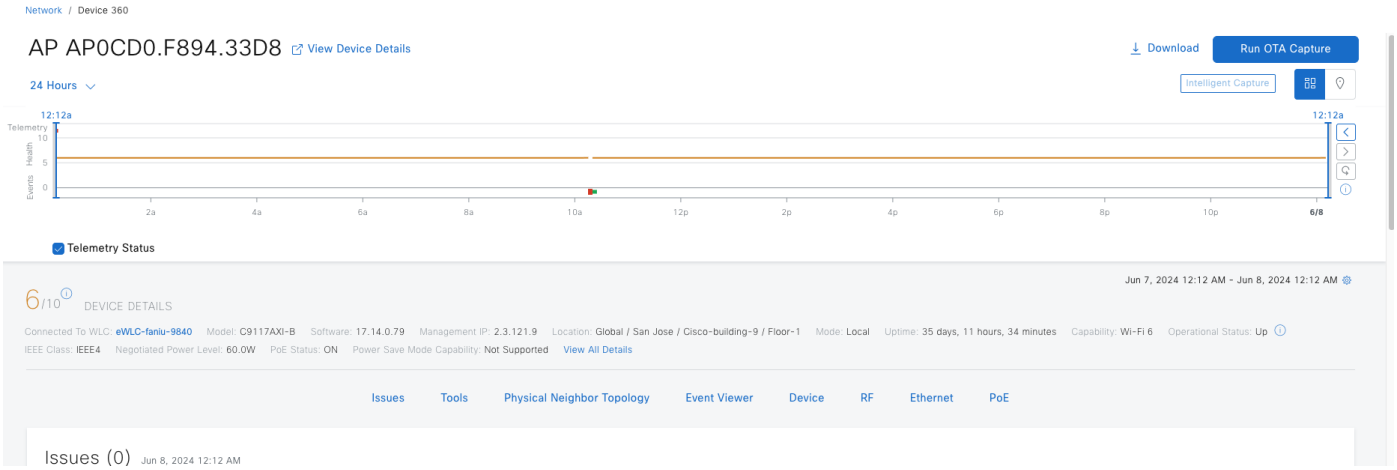


**表 26.** デバイスの正常性スコアに含まれるファブリック KPI

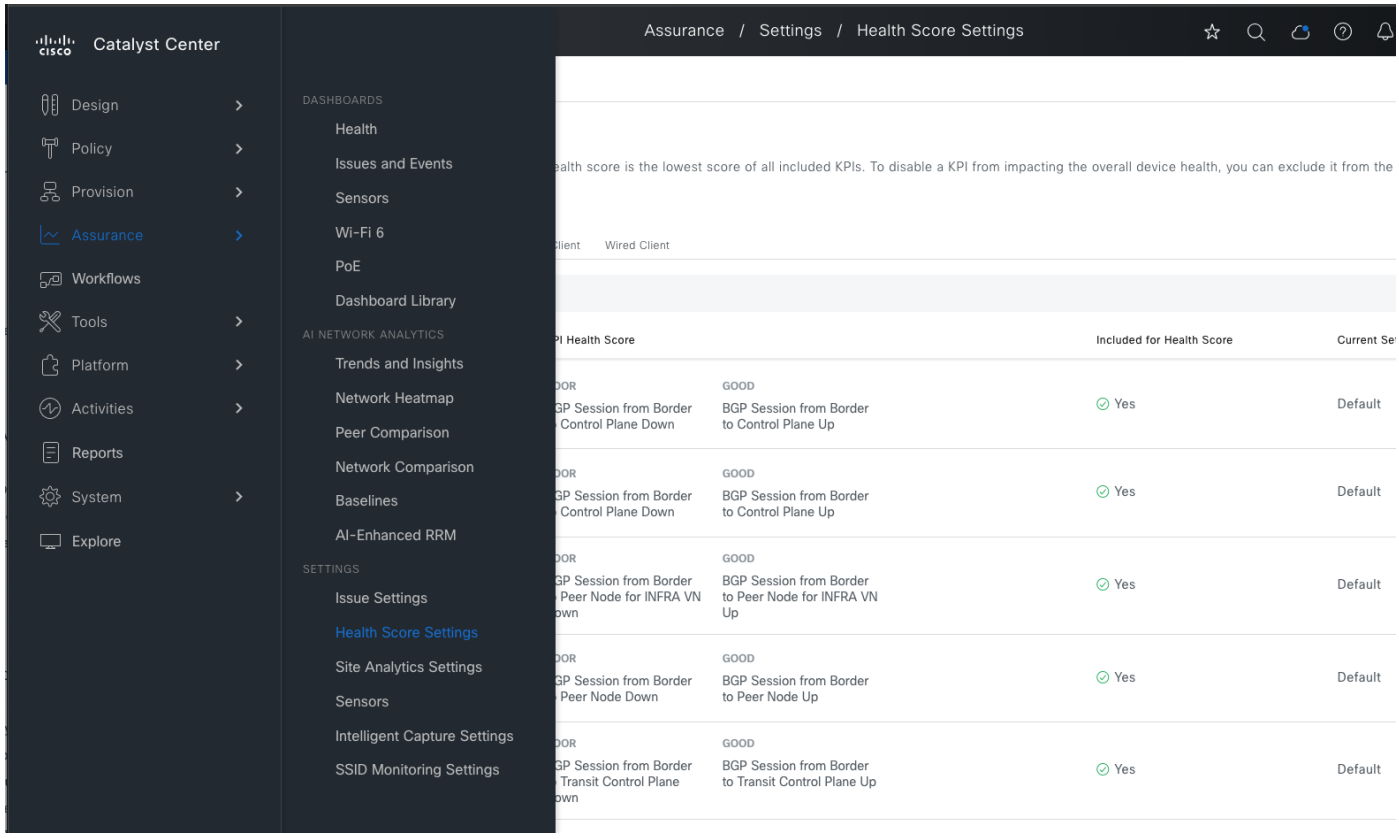
| KPI 名 | 該当するファブリック ロール | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| AAA Server Status | エッジ/EN/PEN/SBEN | あり | 10 分/10 分 | エッジノードと拡張ノードから各 AAA サーバーのサーバーステータスを監視します。 |
| [CTS Environment Data Download] | エッジ/PEN/SBEN | あり | 10 分/10 分 | Cisco ISE サーバーのエッジ、PEN、および SBEN での CTS 環境データのダウンロードを監視します。AAA サーバーのステータスがダウンした場合、CTS 正常性も自動的にダウンします。<br><br>デバイスイメージ（> = 17.9）が必要 |
| Extended Node Connectivity | エッジ/EN/PEN | なし | 5 分/5 分 | 設定されたポートチャネル上の拡張ノードとエッジノード間のリンクステータスを監視します。 |
| Multicast RP | ボーダー | なし | 10 分/10 分 | 外部マルチキャスト RP への到達可能性ステータスを監視します。 |
| Control plane reachability | ワイヤレスコントローラ | なし | 10 分/10 分 | ファブリック ワイヤレス コントローラ ノードからローカル コントロール プレーン ノードへの IPSLA 到達可能性ステータスを監視します。 |
| LISP Session Status | エッジ/ボーダー | あり | 10 分/10 分 | ボーダーノードとエッジノードからローカル コントロール プレーン ノードへの LISP プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| LISP Session from Border to Transit Site Control Plane | ボーダー | あり | 10 分/10 分 | ボーダーノードから、接続されたトランジット コントロール プレーン ノードへの LISP プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| Pub/Sub Session Status | ボーダー | あり | 10 分/10 分 | FiaB ノードの INFRA_VN および継承された VN を除く、すべての VN のボーダーノードから、接続されたローカル コントロール プレーン ノードへの Pub/Sub プロトコル セッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| Pub/Sub Session Status for INFRA_VN | ボーダー | あり | 10 分/10 分 | INFRA_VN のボーダーノードからローカル コントロール プレーン ノードへの Pub/Sub プロトコル セッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |

| KPI 名 | 該当するファブリック ロール | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| Pub/Sub Session from Border to Transit Site Control Plane | ボーダー | あり | 10 分/10 分 | すべての VN のボーダーノードから、接続されたトランジット コントロール プレーン ノードへの Pub/Sub プロトコルセッションを監視します。<br><br>デバイスイメージ（> = 17.6.2）が必要 |
| Internet Availability | コントロールプレーン<br><br>トランジット コントロール プレーン | あり | 10 分/10 分 | 外部ボーダーのデフォルトルートを監視し、それを Pub/Sub サイトを使用した LISP 内のコントロールプレーンノードで登録します。<br><br>外部ボーダーのデフォルトルートを監視し、それを Pub/Sub サイトを使用した LISP 内のトランジットプレーンノードで登録します。<br><br>デバイスイメージ（> = 17.8）が必要 |
| [Remote Internet Availability] | コントロール プレーン | あり | 10 分/10 分 | リモートファブリックサイトが、Pub/Sub サイトで LISP 内の SD-Access トランジット接続ボーダーを介してバックアップインターネットを提供できるかどうかを監視します。KPI インターネット可用性がすでに停止している場合、この KPI は監視されません。<br><br>デバイスイメージ（> = 17.8）が必要 |
| BGP Session from Border to Peer Node | ボーダー | あり | 10 分/10 分 | 特定のボーダーノードとその非ファブリックピアから BGP セッション ステータスを監視します。セッションは、INFRA_VN を除くすべての設定済み VN、および Pub/Sub プロトコルサイトを使用した LISP/BGP と LISP の両方で追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |
| BGP session from Border to Control Plane | ボーダー | あり | 10 分/10 分 | INFRA_VN についてのみ、特定のボーダーノードからローカル コントロール プレーン ノードへの BGP セッションステータスを監視します。<br><br>デバイスイメージ（> = 17.10）が必要 |

| KPI 名 | 該当するファブリック ロール | 問題の自動解決 | 最大遅延（問題/正常性スコア） | 使用目的 |
|---|---|---|---|---|
| BGP session from Border to Peer Node for Infra_VN | ボーダー | あり | 10 分/10 分 | 特定のボーダーノードとその非ファブリックピアから BGP セッション ステータスを監視します。セッションは、INFRA_VN のみ、および LISP/BGP と、Pub/Sub プロトコル サイトを使用した LISP の両方で追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |
| BGP session from Border to Transit Control Plane | ボーダー | あり | 10 分/10 分 | 特定の外部ボーダーノードおよび接続されているトランジット コントロール プレーン ノードから BGP セッションのステータスを監視します。セッションは、LISP/BGP プロトコルサイト内の INFRA_VN が追跡されます。<br><br>デバイスイメージ（> = 17.10）が必要 |

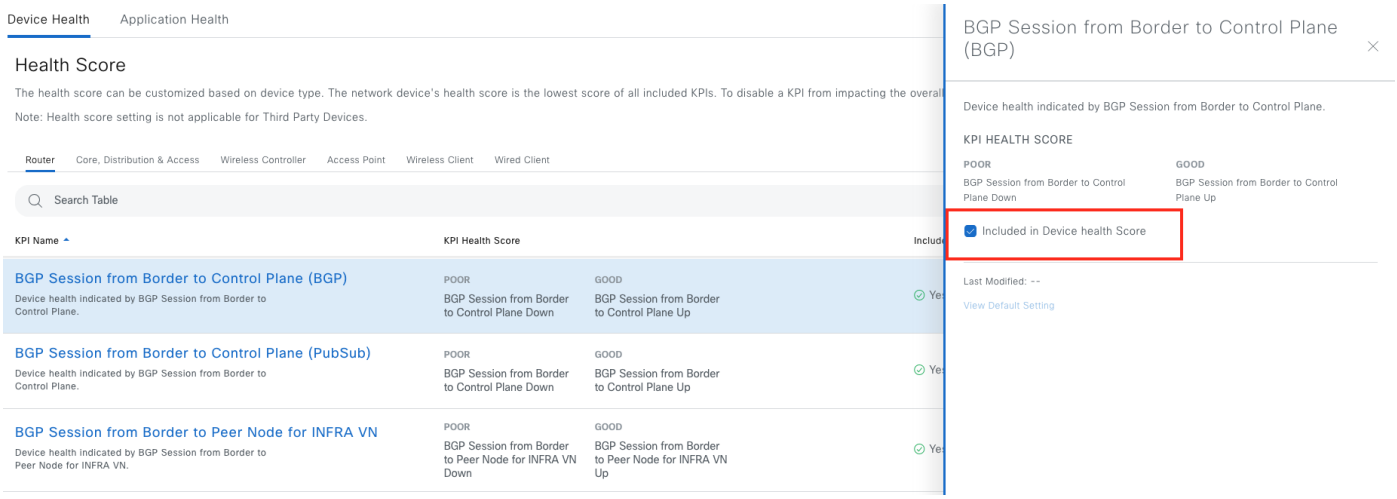
正常性スコアの計算で特定の KPI を除外するには、次の手順を実行します。

**ステップ 1.** [Assurance] > [Setting] > [Health Score Settings] に移動します。



**ステップ 2.** KPI を見つけてクリックし、[Included in Device health Score] チェックボックスをオフにします。

**図 86.　　デバイスタイプルータのボーダーからコントロールプレーンへの BGP セッションを除外した例**




## パストレース

ネットワーク管理者は、ネットワーク内の 2 つのノード（指定された送信元デバイスと指定された接続先デバイス）間でパストレースを実行できます。2 つのノードは、有線ホストまたはワイヤレスホスト、レイヤ 3 インターフェイスの組み合わせ、あるいは両方で構成できます。

パストレースを開始すると、Catalyst Center は、検出されたデバイスのネットワークトポロジとルーティングデータを確認して収集します。このデータを使用して、2 つのホストまたはレイヤ 3 インターフェイス間のパスを計算し、パストレーストポロジにパスを表示します。このトポロジには、パスの方向とパスに沿ったデバイスが含まれ、デバイスの IP アドレスも表示されます。ディスプレイには、パスに沿ったデバイスのプロトコル（Switched、STP、ECMP、Routed、Trace Route）や、その他のソース タイプも表示されます。

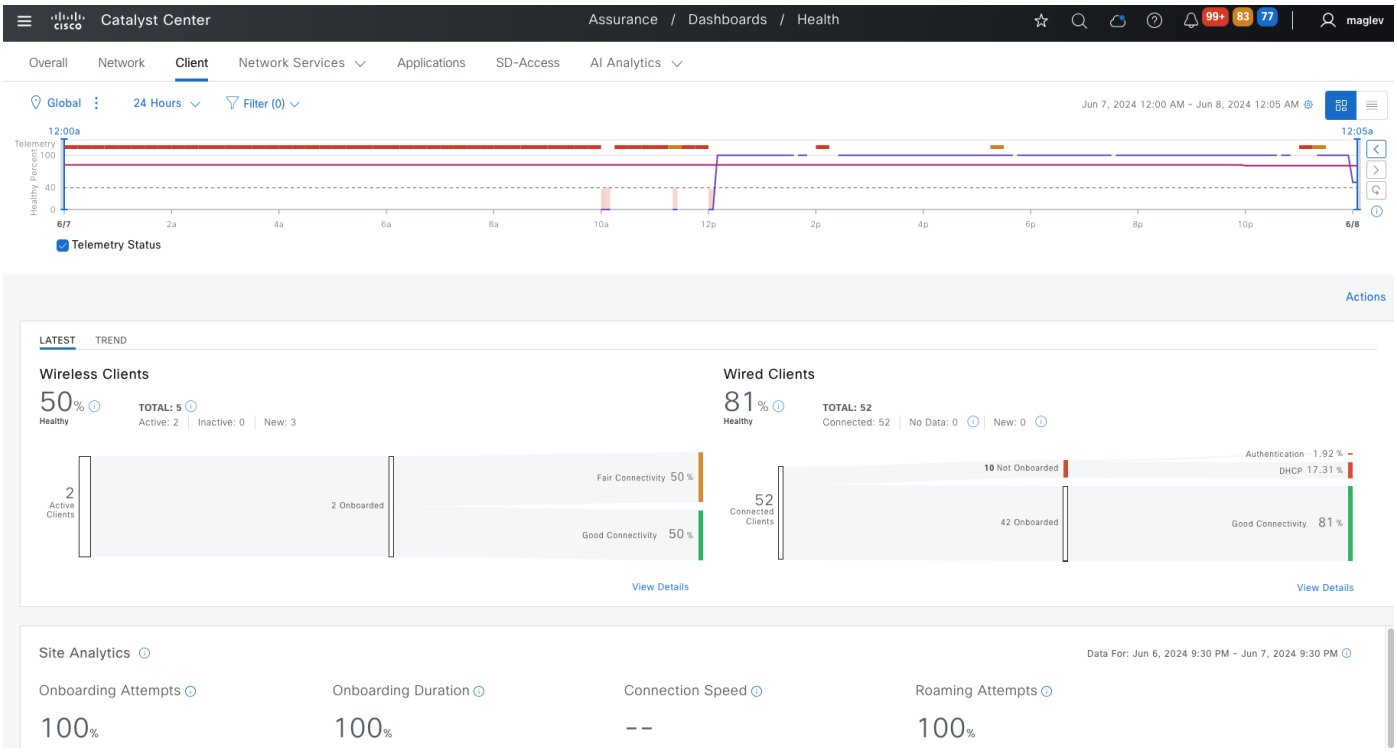
パストレースには、次の制限事項と制約があります。

- ファブリッククライアントと非ファブリッククライアントの間のパストレースは、サポートされていません。
- デバイスで CDP プロトコルを有効にする必要があります。
- 複数の仮想ルーティングおよび転送（VRF）仮想ネットワーク（VN）上にある 2 つのファブリッククライアント間のパストレースは、サポートされていません。
- ルータのループバック インターフェイスからのパストレースは、サポートされていません。
- 重複する IP アドレスは、ファブリックの有無にかかわらずサポートされていません。
- Locator ID/Separation Protocol（LISP）ファブリック機能のパストレースは、トラフィックが実行されていて、エッジスイッチでキャッシュを利用できることが必要です。
- Cisco 適応型セキュリティアプライアンス（ASA）は CDP をサポートしていないため、Cisco ASA のパストレースはサポートされていません。Cisco ASA アプライアンスを通るパスを識別することはできません。
- タグなしモードのワイヤレスコントローラの管理インターフェイスでは、パストレースはサポートされていません。

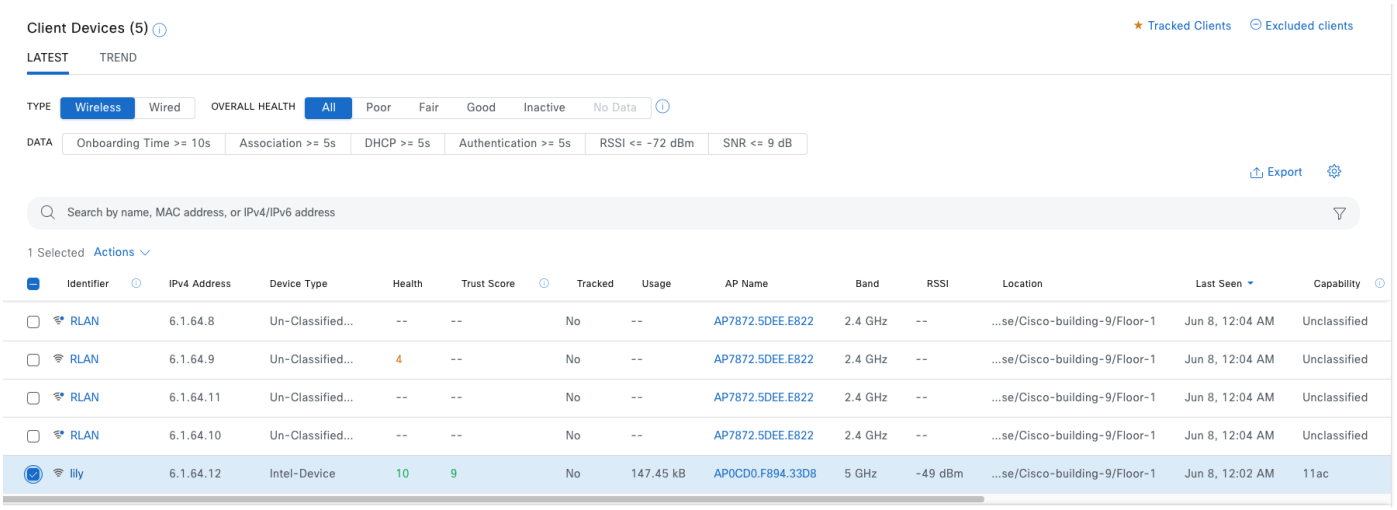
- 仮想スイッチングシステム（VSS）、マルチリンク集約制御プロトコル（MLACP）、または仮想ポートチャネル（vPC）のパストレースはサポートされていません。
- スイッチ仮想インターフェイス（SVI）上の等コスト マルチパス ルーティング（ECMP）のパストレースは、サポートされていません。
- NAT またはファイアウォールを使用するデバイスでのパストレースはサポートされていません。
- Hot Standby Router Protocol（HSRP）VLAN のホストから任意の HSRP ルータに接続されている 非 HSRP VLAN のホストへのパストレースは、サポートされていません。
- ポートチャネルの Port Aggregation Protocol（PAgP）モードは、サポートされていません。LACP モードのみがサポートされています。
- Cisco SD-Access ファブリックで OTT を使用するワイヤレスクライアントのパストレースはサポートされていません。
- レイヤ 2 スイッチからのパストレースはサポートされていません。
- シスコの産業用イーサネット（IE）スイッチは、Cisco SD-Access ソリューションの一部として拡張されたノードです。現在、パストレースは拡張ノードを認識していないため、トポロジに拡張ノードが含まれている場合は、エラーメッセージが表示されます。
- デバイス用に IPv4 アドレスと IPv6 アドレスの両方を使用するデュアルスタックはサポートされていません。この状況になると、指定されたアドレスが不明であることを示すエラーメッセージが表示されます。

[Client 360] または [Device 360] ウィンドウからパストレースを実行できます。次の例は、**lily** という名前のクライアントからの開始パストレースを示しています。

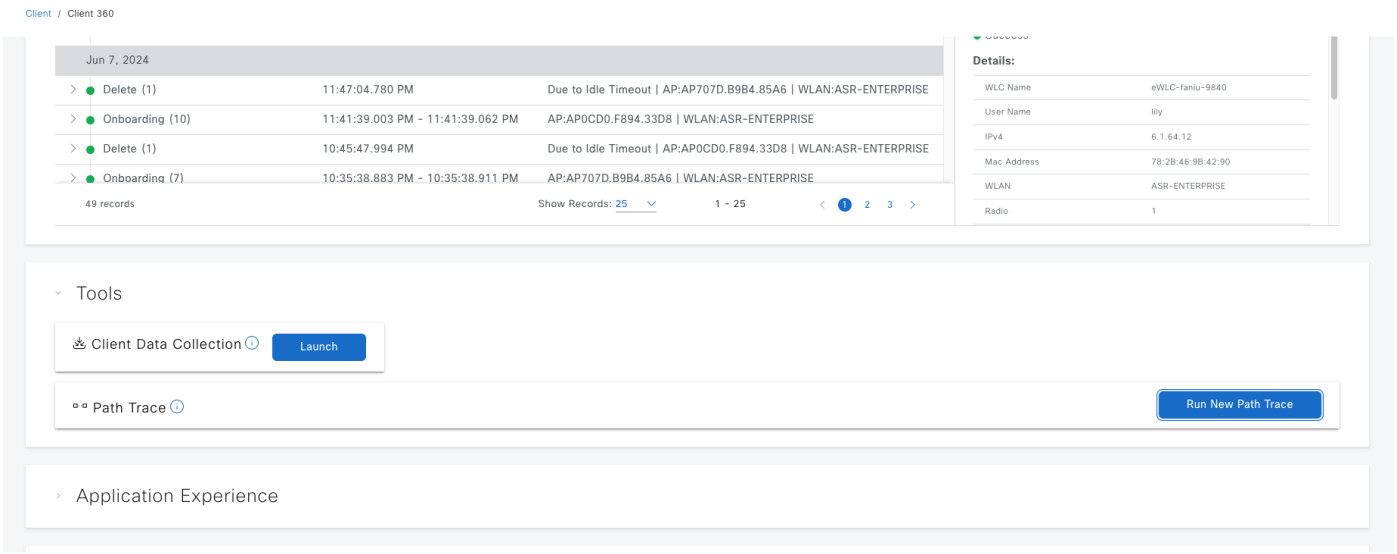
**ステップ 1.** メニューアイコンボタンから [Assurance] > [Health] の順に選択し、[Client] タブをクリックします。




**ステップ 2.** クライアント [lily] のチェックボックスを見つけてオンにします。



**ステップ 3.** リダイレクトされた [Client 360] ウィンドウで [Tools] セクションまで下にスクロールし、[Run New Path Trace] をクリックします。



**ステップ 4.** 必須フィールドに入力します。[Destination] フィールドが IP **6.1.0.9** の有線クライアント用であれば、[Start] をクリックします。

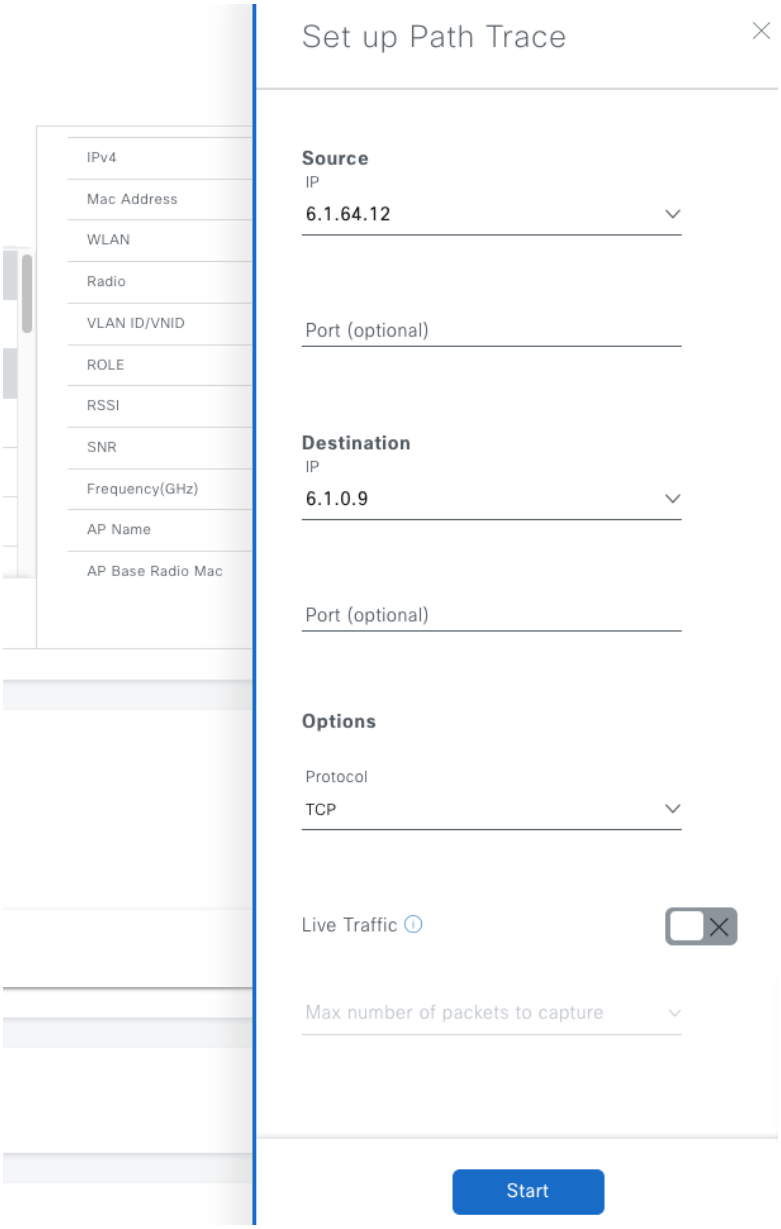



**図 87.　　パストレースが開始されて「Loading Trace」が表示される**

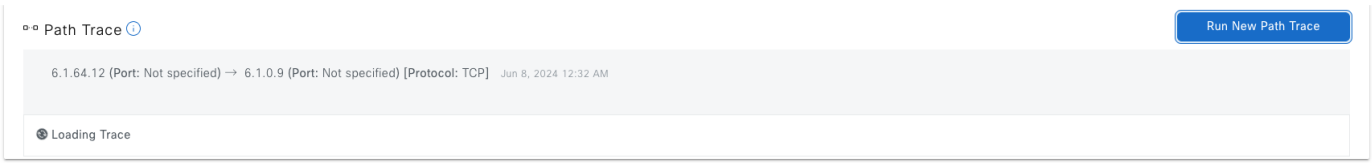


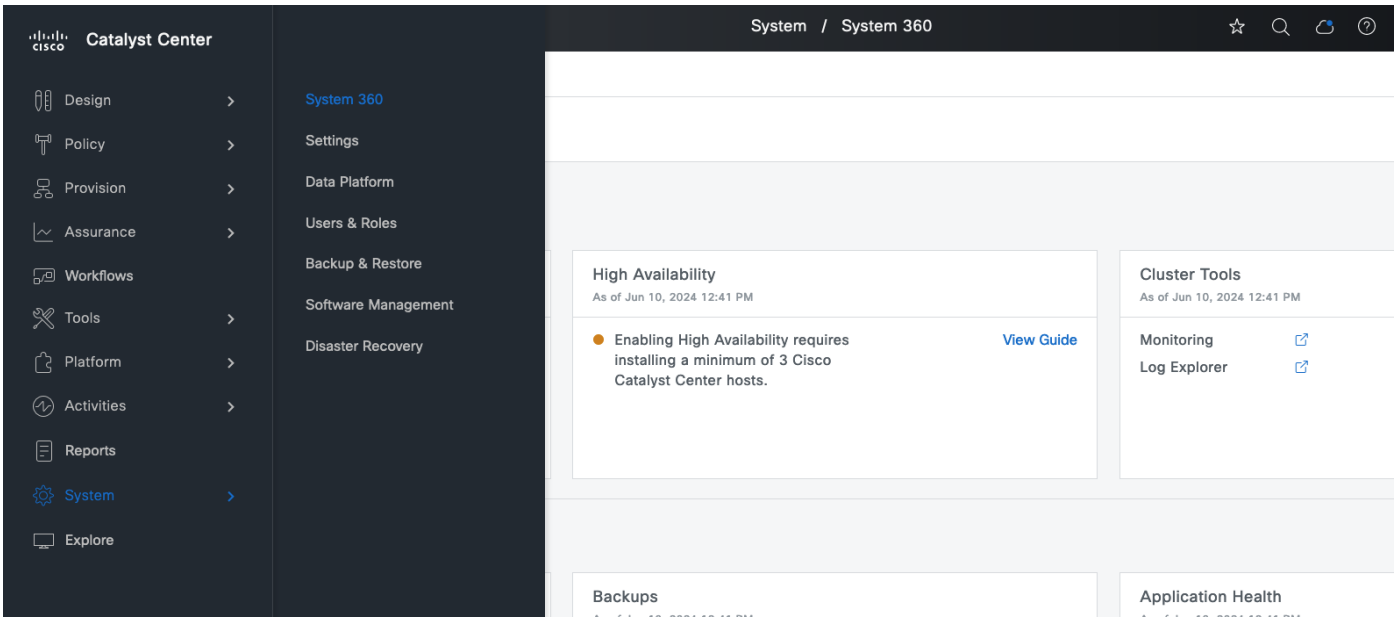
**図 88.　　終了すると、これら 2 つのクライアント間の各ホップのデバイスを持つトポロジが表示される**


## Cisco SD-Access アプリケーションの正常性の監視

Catalyst Center は、ネットワーク管理者が Cisco SD-Access アプリケーションの正常性を監視するのに役立つシステム検証ツールを提供します。このツールは、Cisco SD-Access アプリケーションのデータベースデータの不整合を 15 分ごとに自動的にチェックします。チェックは、手動で実行することもできます。

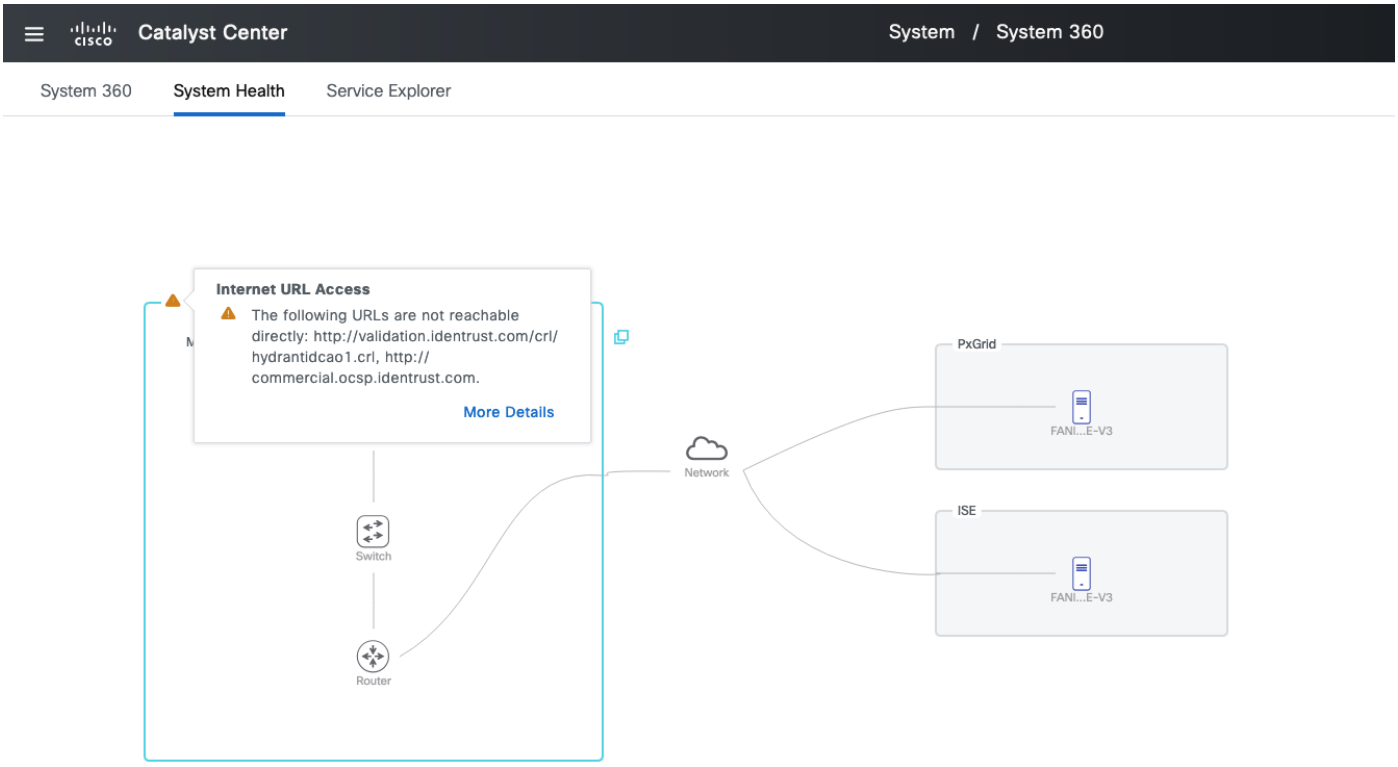
結果を確認するには、次の手順を実行します。

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



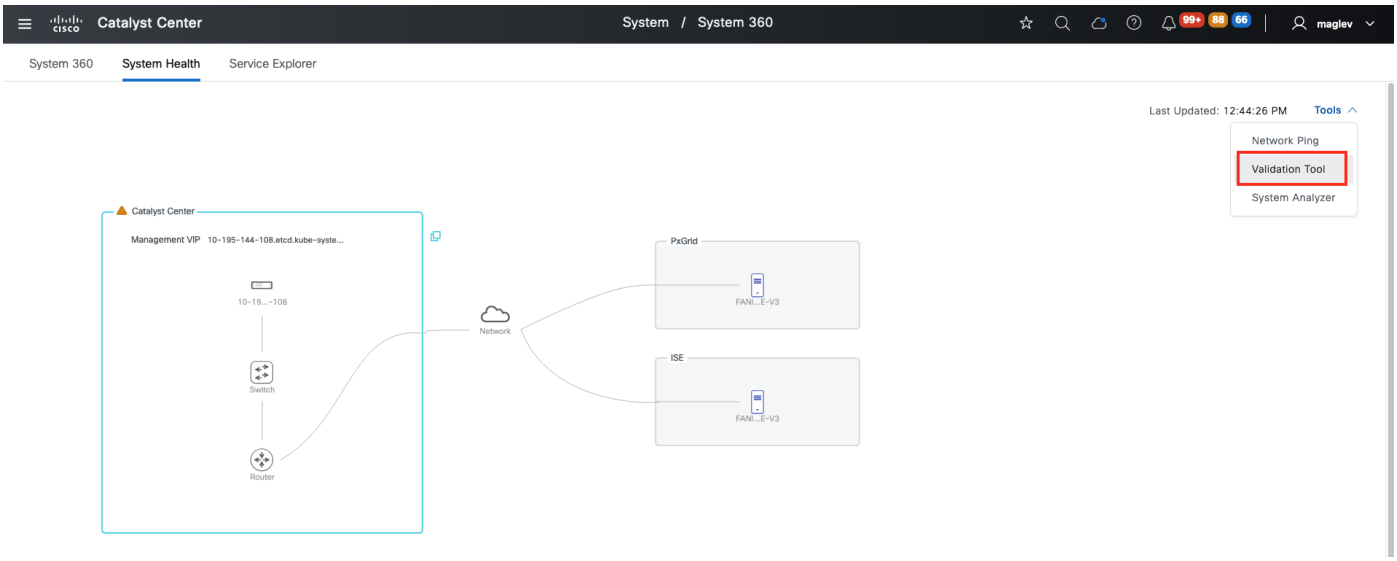

**ステップ 2.** ランディングウィンドウで、[System Health] タブをクリックします。このウィンドウには、システムレベルの障害または警告があるかどうかが表示されます。

**図 89.　　Catalyst Center に警告のみが表示されている例**

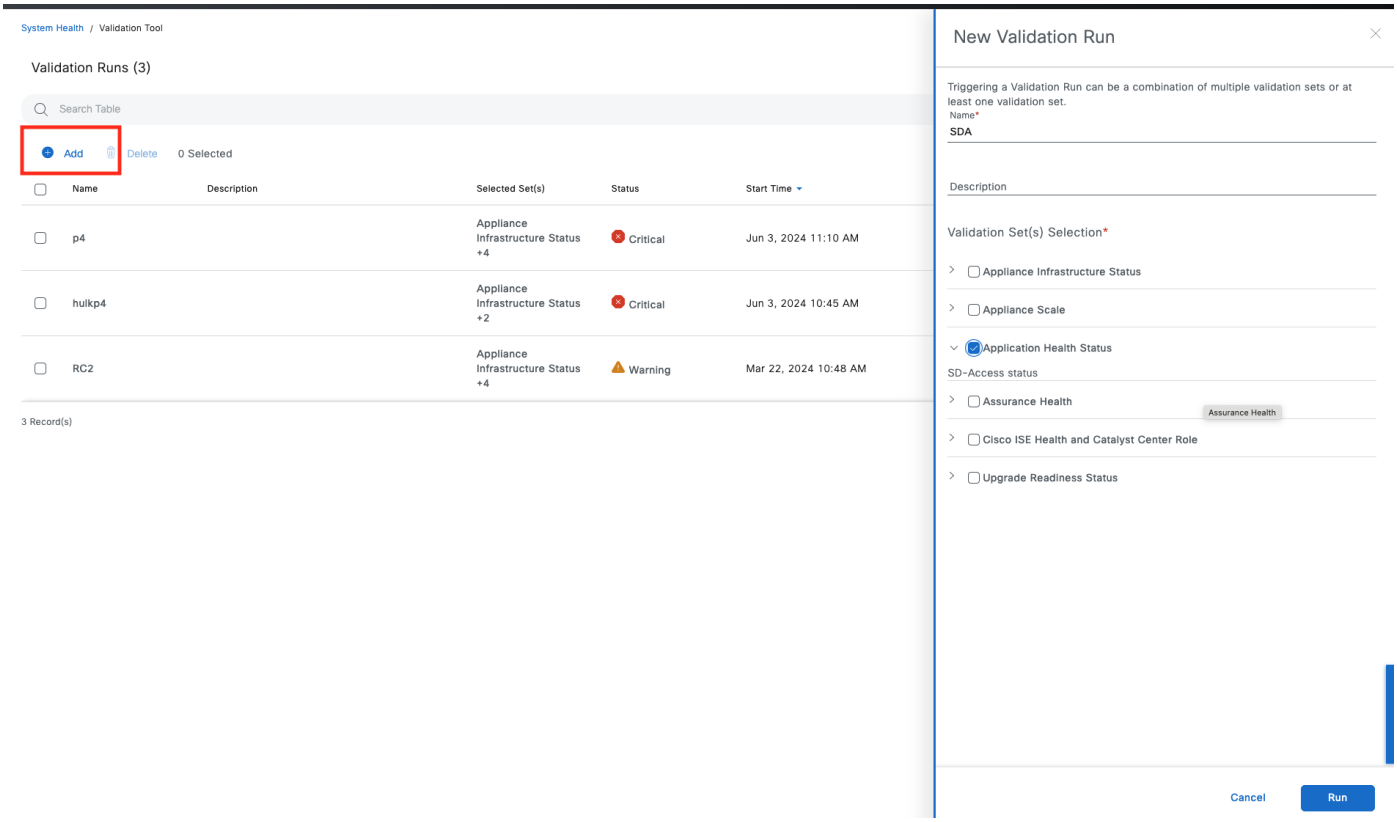



チェックを手動で実行するには、次の手順を実行します。

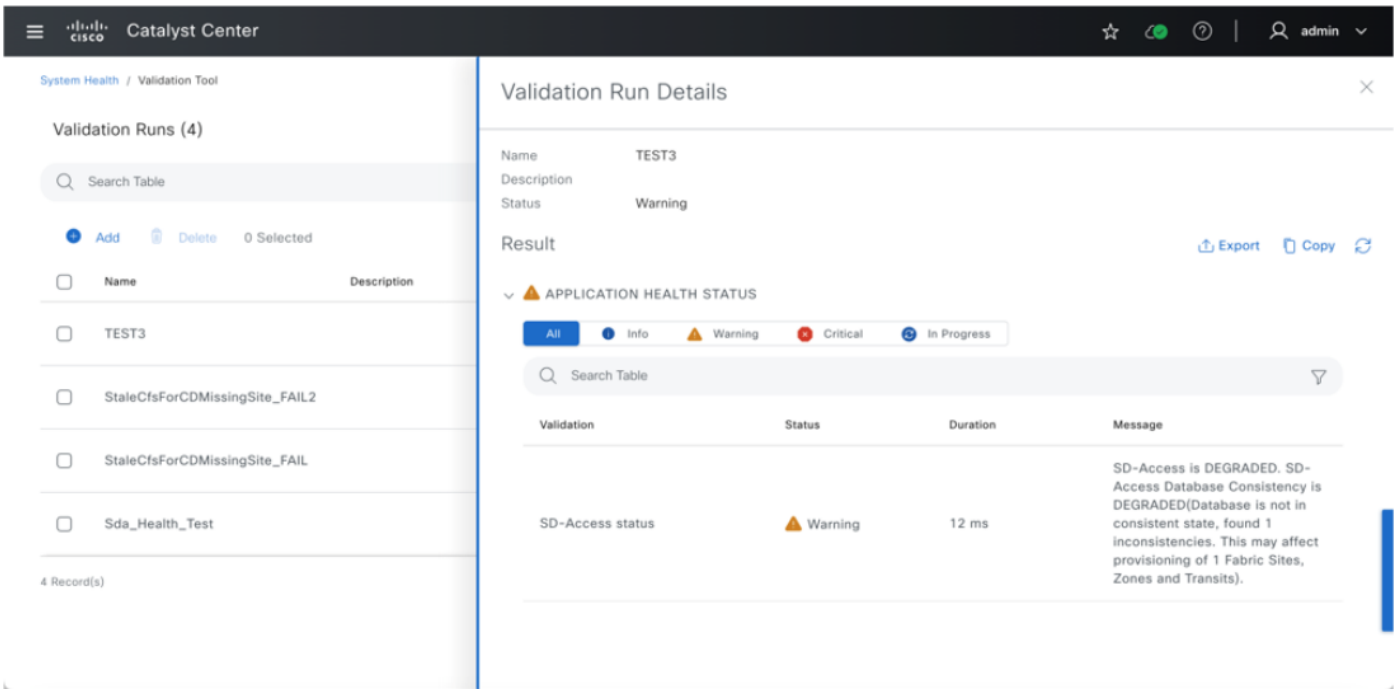
**ステップ 1.**　[Tools] > [Validation Tool] の順にクリックします。

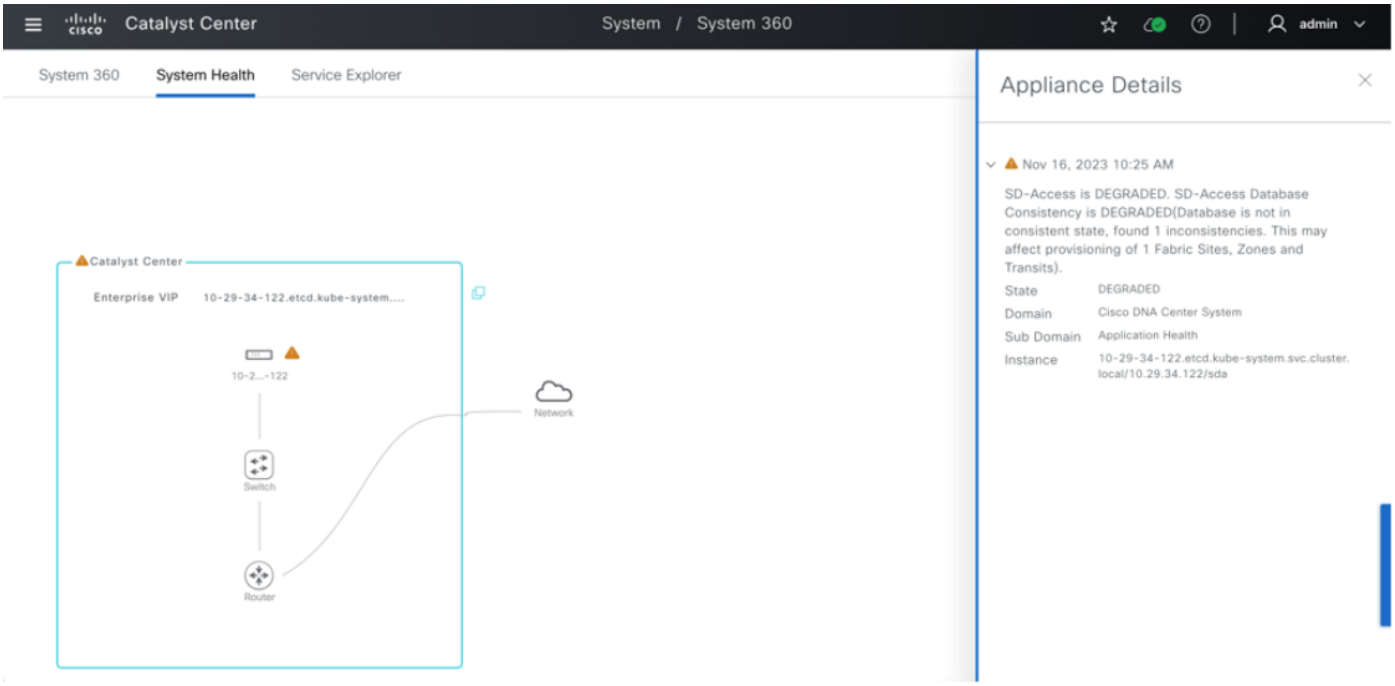


**ステップ 2.** [Validation Tool] ウィンドウで [Add] をクリックし、スライドインペインで Cisco SD-Access の [Application Health Status] チェックボックスをオンにします。




障害がある場合、[SD-Access status] で DEGRADED メッセージを報告します。






**ステップ 3.** アップグレード後および毎日の操作で、[System Health] ウィンドウを確認します。Cisco SD-Access が DEGRADED メッセージを報告した場合、Cisco TAC サポートに連絡してください。

## Cisco SD-Access 互換性マトリックス

Catalyst Center では、Cisco SD-Access ロールのプロビジョニング中に、管理対象デバイスのソフトウェア イメージ バージョンにおける Cisco SD-Access 互換性マトリックスのコンプライアンスを維持します。

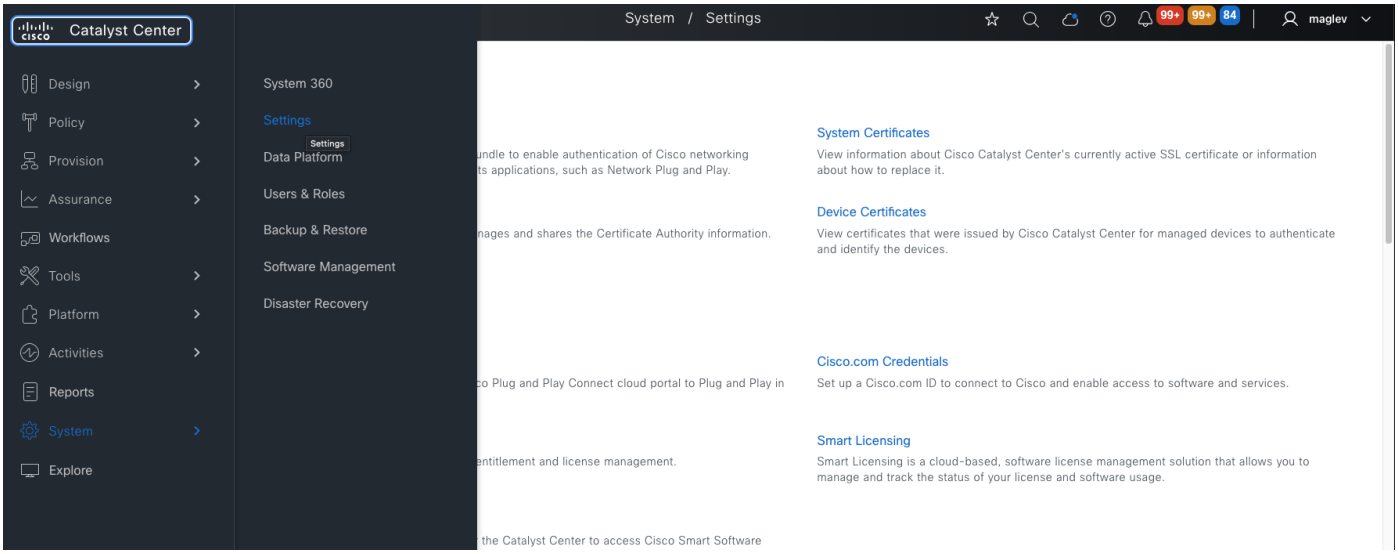
Catalyst Center Provision サービスが起動すると、スケジューラが 24 時間ごとに実行されるように設定され、事前定義されたリンクを使用してシスコから入手可能な最新のファイルをダウンロードするタスクがトリガーされます。新しいファイルがない場合、ダウンロードタスクはスキップされます。リリースされているバージョンがある場合に、ダウンロードタスクをトリガーできます。

エアギャップのお客様の場合、ダウンロードタスクは常に失敗します。最新のファイルをダウンロードし、新しいファイルを UI からアップロードする必要があります。シスコに到達できないクラスタの場合も、同じ手動アップロードが必要です。

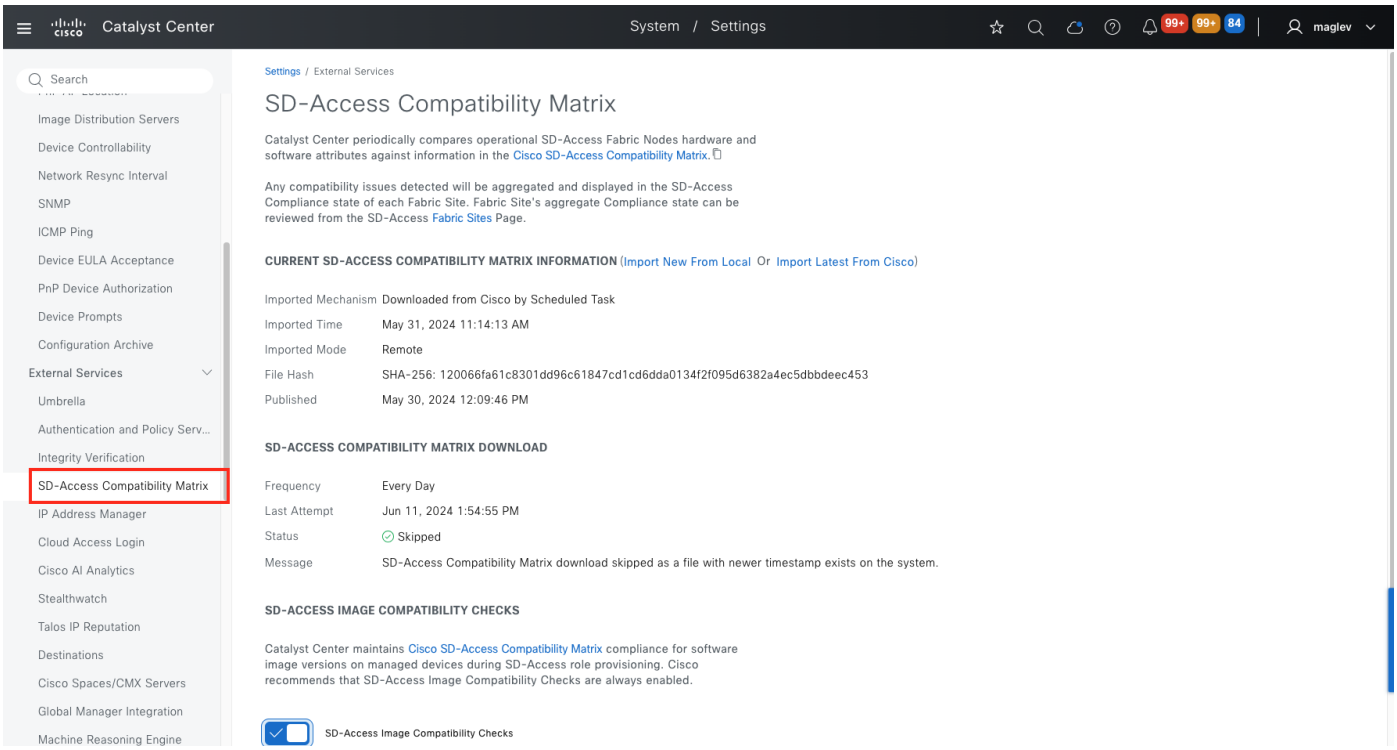
デバイスが互換性のないソフトウェアを実行している場合、またはデバイスが Cisco SD-Access でサポートされていない場合、Catalyst Center は、ボーダー、コントロールプレーン、エッジ、拡張ノード（PnP 自動オンボーディング）、およびワイヤレスコントローラのロールを使用してこのデバイスをファブリックに追加する機能をブロックします。2.3.7.5 以降のリリースの Catalyst Center では適用がデフォルトで有効になっていますが、無効にすることができます。

新しい互換性マトリックスファイルをアップロードするか、適用を無効にするには、次の手順を実行します。

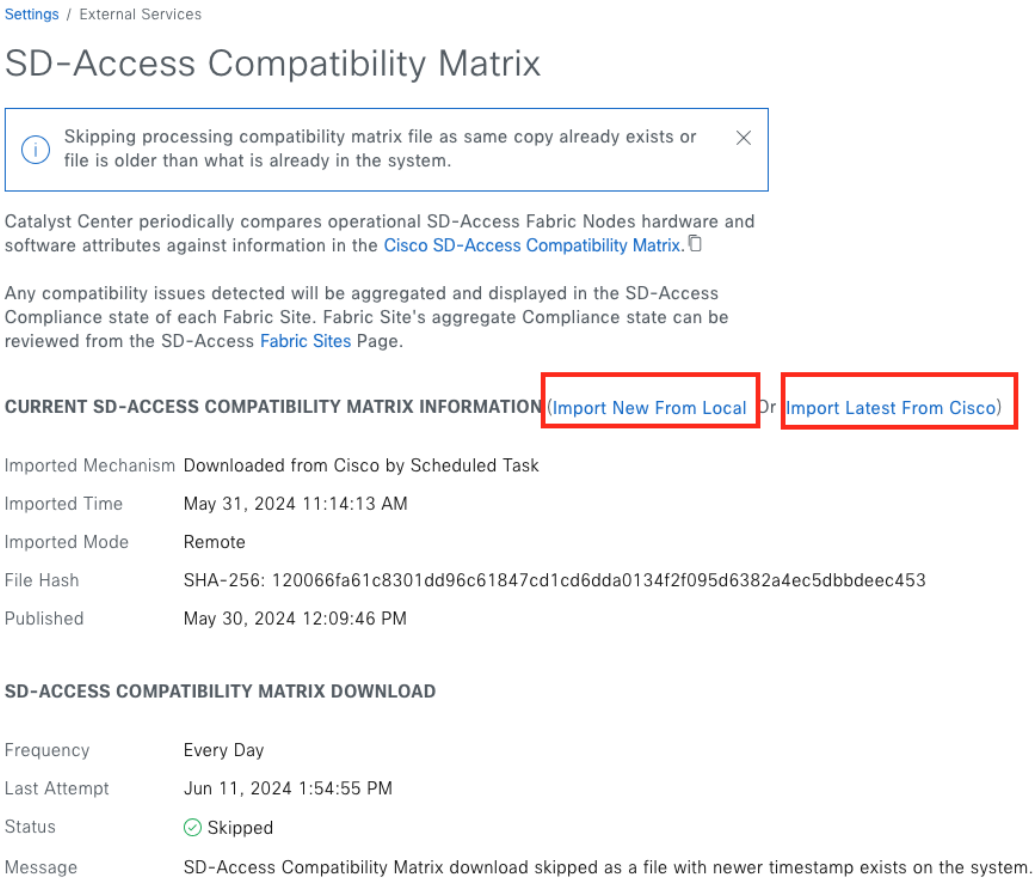
**ステップ 1.** 左上隅にあるメニューアイコンをクリックして、[System] > [Settings] の順にクリックします。



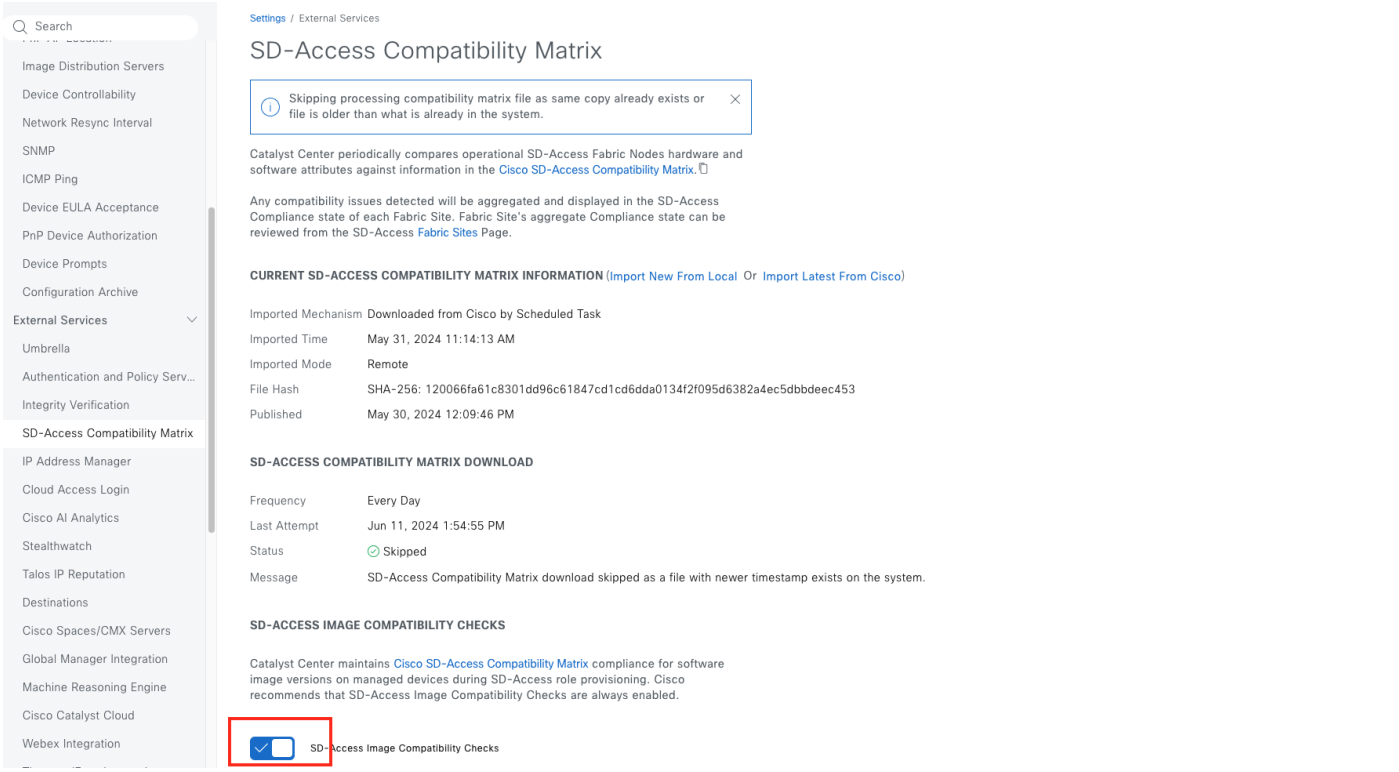

**ステップ 2.** [External Services] > [SD-Access Compatibility Matrix] をクリックして、ランディングウィンドウに移動します。




- 新しい互換性マトリックスファイルをアップロードするには、[Import New From Local] をクリックします。
- 新規にダウンロードする場合は、[Import Latest from Cisco] をクリックします。

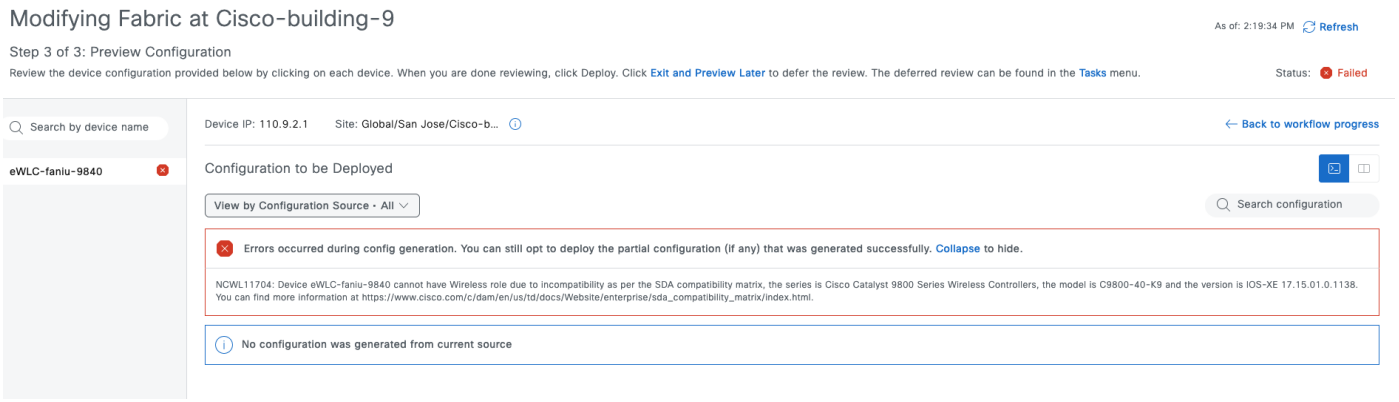



- 適用を無効にするには、ウィンドウの一番下までスクロールして、[SD-Access Image Compatibility Checks] を無効にします。




**技術的なヒント：** [SD-Access Image Compatibility Checks] は有効のままにします。

**図 90.　互換性マトリックスでサポートされていないデバイスイメージを実行しているため、どのように eWL Catalyst 9800 コントローラをファブリックに追加できなかったかを示す例**



# 付録

## 付録 A：検証に使用するハードウェアとソフトウェア

この設計および導入ガイドは、次の表にリストされているハードウェアとソフトウェアを使用して作成されています。

**表 27.** ハードウェアおよびソフトウェア

| 機能エリア | 製品 | ソフトウェアのバージョン |
|---|---|---|
| スタンドアロンワイヤレス LAN コントローラ | Cisco Catalyst 9800-40 ワイヤレスコントローラ | 17.15.1 |
| Catalyst 9000 の組み込みワイヤレスコントローラ | Cisco Catalyst 9300 の組み込みワイヤレスコントローラ | 17.15.1 |
| コロケーションされたファブリックボーダーとコントロールプレーン | Cisco Catalyst 9300 | 17.15.1 |
| ファブリックエッジ | Cisco Catalyst 9300 | 17.15.1 |
| ポリシー拡張ノードとサプリカントベースの拡張ノード | Catalyst 9300 と Catalyst 9200 | 17.15.1 |
| エンタープライズ SDN コントローラ | Catalyst Center | 2.3.7.x |
| AAA サーバー | Cisco ISE（Identity Services Engine） | 3.3 |

## 付録 B：用語集

**AP** アクセスポイント

**Cisco ISE** Cisco Identity Services Engine

**CDP** Cisco Discovery Protocol

**CMD** Cisco メタデータ

**CTS** Cisco TrustSec

**CUWN** Cisco Unified Wireless Network

**DS** 分散システム

**EID** エンドポイントのアイデンティティ

**GRT** グローバル ルーティング テーブル

**HA** 高可用性

**MSRB** マルチサイト リモート ボーダー

**PSN** ポリシーサービスノード

**RF** 無線周波数

**OTT** オーバーザトップ

**pxGrid** Platform Exchange Grid

**REST API** Representational State Transfer アプリケーション プログラミング インターフェイス

**RLOC** ルーティングロケータ

**SD-Access** Cisco Software Defined Access

**SGACL** セキュリティ グループ アクセス コントロール リスト

**SGT** セキュリティグループタグ

**SSID** サービスセット識別子

**SSO** ステートフル スイッチオーバー

**SXP** SGT 交換プロトコル

**SVI** スイッチ仮想インターフェイス

**VN** 仮想ネットワーク

**VNI** VXLAN ネットワーク識別子

**VRF** 仮想ルーティングおよび転送

**VXLAN** Virtual Extensible Local Area Network

**WLAN** ワイヤレス ローカル エリア ネットワーク

**WLC** ワイヤレス LAN コントローラ

## 付録 C：参考資料

Catalyst Center 2.3.7.x Third-Generation Installation Guide

Cisco ISE installation Guide

Cisco Software-Defined Access Compatibility Matrix

Catalyst Center 2.3.7.x Data Sheet

Policy Platform Capability Matrix

Catalyst Center 2.3.7.x User Guide

Catalyst Center SD-Access LAN Automation Deployment Guide

SD-Access Solution Design Guide

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。