AD-キャンパス6.2

グループベースポリシーコンフィギュレーションガイド

内容

制限事項およびガイドライン

1. サポートされるモデルの詳細については、ソリューションの仕様を参照してください。
2. S5560X-EI および S6520X-EI シリーズは、マイクロセグメンテーションをサポートしていません。
3. S5560X/S6520X シリーズスイッチでは、VXLAN トンネルインターフェイスで受信した特定のプロトコルパケット(ARP パケットおよび MLD パケットを含む)を、CPU に配信せずに直接転送できるようにする必要があります。これにより、パケットが CPU に与える影響を回避できます。設定手順は次のとおりです。
   a. **undo mac-address static source-check enable** コマンドをグローバルに設定します。
   b. VSI ビューで **flooding disable all all-direction** コマンドまたは **flooding disable broadcast all-direction** コマンドが設定されている場合は、VSI ビューで **undo flooding disable** コマンドを実行して設定を削除する必要があります。次に、**flooding disable all** コマンドまたは **flooding disable broadcast** コマンドを再度実行します。
   c. **forwarding vxlan-packet inner-protocol** { **ipv4** | **ipv6** }コマンドをグローバルに設定します。IPv4 サービスと ipv6 サービスの両方が使用可能な場合は、IPv4 と ipv6 の両方のパラメーターを設定します。
   d. ポート分離グループをグローバルに設定します。すべてのリーフのダウンリンクインターフェイスでポート分離を設定します。リーフダウンリンクインターフェイス間で従来の VLAN サービスにアクセスする必要がある場合は、ポート分離グループに追加する必要はありません。これにより、これらのリーフダウンリンクインターフェイス間でブロードキャスト、不明なマルチキャスト、および不明なユニキャストのトラフィックを分離できなくなる可能性があります。
4. S5560X-EI/S5560X-HI/S6520X-EI/S6520X-HI デバイスは、Edge Device(ED)として動作できません。
5. S5560X-HI/S6520X-HI デバイスがゲートウェイ共有モードでボーダーデバイスとして動作する場合、インターフェイス上でリターントラフィックを許可するように PBR を設定する必要があります。
6. BYOD セキュリティグループを設定するには、最初に vDHCP サーバーを設定する必要があります。
7. シングルリーフのシナリオでは、コントローラはループバックインターフェイスに IP アドレスを自動的に割り当てません。ファブリック相互接続サービスをサポートするために、Web インターフェイスでファブリックの VTEP IP を編集できます。
8. アクセスデバイスをルータに接続するには、WAN インターフェイスではなく LAN インターフェイスを使用し、ルータ上で DHCP および NAT をディセーブルにする必要があります。
9. パブリックホストのシナリオでは、名前/アドレスバインディング機能は、802.1X+iNode 認証モードのみをサポートします。複数のユーザーカウントで共有されるパブリックホストでの MAC ポータル認証はサポートしません。

10. Microsoft DHCP サーバーは、スタンドアロン展開の疎結合モードでのみ IPv6 アドレスの割り当てをサポートします。

11. Microsoft DHCP サーバーの 1 つのアドレスプールに含まれる MAC-IP バインディングの数は、2000 未満である必要があります。

12. Microsoft DHCP サーバーに障害が発生すると、スタンバイサーバーはバインディングエントリーを生成できず、IP アドレスの割り当てのみが可能になります。障害が回復した後、エンドポイントはオフラインになった後にのみバインドされ、再認証のために再びオンラインになります。

13. グループポリシーの既定の操作が **Deny** として構成されている場合、ベストプラクティスとして、IT リソースグループの物理サーバーをスパインデバイス経由で接続し、**vpn-default** という名前のプライベートネットワークに展開します。IT リソースグループが **vpn-default** という名前のプライベートネットワークに展開されている場合、既定では、すべてのプライベートネットワークがすべての IT リソースグループへのアクセスを許可されます。各プライベートネットワークでアクセスが許可されていない IT リソースグループを構成し、拒否操作を含むグループポリシーを展開することで、リソースへのアクセスを禁止できます。IT リソースグループがサービス VPN に展開されている場合、サービスプライベートネットワーク内のユーザーは既定で IT リソースグループにアクセスできません。IT リソースグループにアクセスするには、許可操作を含むポリシーを構成する必要があります。

14. サーバーに接続されたレイヤー3 スイッチでは、PVST ではなく MSTP を設定する必要があります。

15. SeerBlade モジュールのネットワークポートとスパインデバイスの間にスイッチを配置する必要があります。

16. 非標準ネットワーク、特にファイアウォールを含むネットワークでは、ソリューションのポートマトリックスドキュメントの説明に従って、対応するポートを有効にします。

17. セカンダリサブネットがレイヤー2 ネットワークドメイン用に設定されている場合、ユーザーIP バインディング機能はアクセスポリシーで許可されません。

18. IP セグメントベース認証およびユーザーIP アドレスバインディング認証がアクセスポリシーで設定されている場合を除き、**mac-authentication carry user-ip** コマンドは使用しないでください。認証用のスタティック IP アドレスを使用してエンドポイントを設定する必要がある場合は、コントローラを介して **arp snooping** コマンドを展開し、スタティック IP アドレスを EIA に配信できます。

19. ユーザー認証では、802.1X 認証モードと MAC/MAC ポータル認証モードがサポートされています。実際のネットワークでは、1 つの認証モードのみを設定する必要があります。必要に応じて認証モードを選択できます。必要でない限り、両方の認証モードを設定しないことをお勧めします。ただし、キャンパスネットワークでは両方の認証モードの設定がサポートされています。

20. spine/leaf/access/AC デバイスの IRF ファブリックを手動で設定する場合は、最初に **irf mac-address persistent always** コマンドを実行して、マスター/下位デバイスのスイッチオーバー時に IRF ファブリックのブリッジ MAC アドレスが変更されないようにする必要があります。

21. コントローラは、同じファブリック内の同じ VPN 内でだけレイヤー2 およびレイヤー3 マルチキャスト

をサポートします。

22. マルチキャスト送信元が VLAN モードでデバイスにアクセスする場合、S12500G-AF および S10500/S10500X スイッチシリーズの*SH カード、ならびに S6550XE および S6525XE デバイスがサポートされます。
23. ユーザーがオンラインのときに DHCP サーバーを変更することはできません。
24. デバイスのグループを複数のコントローラに同時に組み込むことはできません。
25. DHCP サーバーのセットは、複数のコントローラに同時に組み込むことはできません。
26. S5130-EI/HI スイッチは **qos priority dscp 0** コマンドをサポートしておらず、エンドポイントによる DSCP 値の不正な変更を防ぐことができません。
27. 一部のスイッチチップは、レートをネゴシエートできません。たとえば、S6525XE-HI スイッチは、レートを Gbps にネゴシエートできません。
28. ARP フラッディングの場合は、製品の推奨に従って攻撃防御コマンドを設定します。
29. 環境内に複数のセキュリティグループが存在する場合は、AC のオンデマンド展開機能をイネーブルにすることを推奨します。
30. ベストプラクティスとして、スパインデバイスの VSI インターフェイス 4094 に対して **arp send-gratuitous-arp interval** コマンドを設定し、間隔を 30 秒に設定します。
31. **Automation** > **Campus Network** > **Network Parameter**s > **vDHCP** パスの DDI ページにあるエンドポイント IP コリジョン検出機能では、syslog 機能との連携が必要です。手動でオンボードされたリーフデバイスの場合は、**info-center loghost vpn-instance vpn-default 100.1.0.100** 設定を追加します。
32. デバイスをモニタリングリストに追加し、**snmp trap** コマンドを発行する場合は、VPN を設定する必要があります。
33. ファブリックに手動オンボードデバイスと自動オンボードデバイスの両方が含まれている場合(このハイブリッドデバイスのオンボードシナリオは推奨されません)、両方のオンボード方式の VSI/VLAN 4094 の IP アドレスが異なることを確認します。さらに、手動でオンボードしたデバイスのアンダーレイ IP アドレスとアンダーレイ VLAN が、自動化テンプレートのアンダーレイ IP アドレスと遅延解除 VLAN の範囲内にないことを確認します。
34. コントローラでデバイス間集約グループが追加または削除されると、リーフデバイスは一時的に切断されます。この状況は、管理ネットワークに非対称 IRB 転送機能を設定する(**evpn irb asymmetric** コマンドを使用)ことで回避できます。安定した状況では、非対称 IRB 転送機能を無効にする必要があります(**undo evpn irb asymmetric** コマンドを使用)。
35. 名前/アドレスバインディングと IP ソースガード(IPv4 インターフェイスバインディング)または ARP 検出の両方を設定することはできません。
36. 外部展開の場合、ベストプラクティスとして、リーフデバイスに IP ソースガード(IPv4 インターフェイス

バインディング)を展開しないでください。

37. DRNI ネットワーキングでは、DR デバイスごとに一意のルータ ID を手動で指定する必要があります。

概要

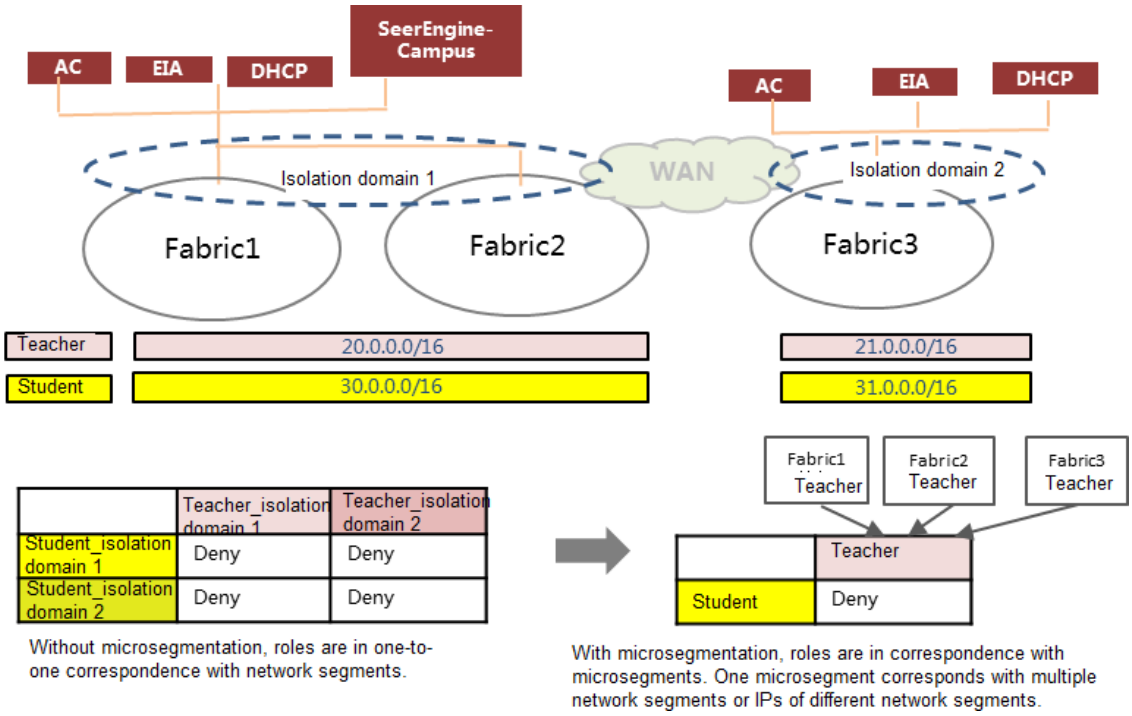
この文書では、AD-Campus 6.2 ソリューションの基本的な導入について、次の手順に従って説明します。

- 関連ソフトウェアのインストールと展開
- アンダーレイを手動で設定します。
- 物理デバイスの手動による組み込み。
- SeerEngine キャンパスコントローラの基本的なサービス設定とユーザー設定
- 有線ユーザー認証とオンボーディング。

AD-Campus 6.2 ソリューションは、マイクロセグメントをユーザーロールまたはセキュリティグループとして定義するマイクロセグメンテーションに基づいて実装され、分離ドメイン間でセキュリティグループをサポートします。セキュリティグループに指定されたセキュリティグループ ID は、マイクロセグメント ID です。セキュリティグループは、複数の分離ドメイン内のレイヤー2 ネットワークドメインにバインドでき、異なる VXLAN ID が異なる分離ドメインのセキュリティグループに展開されます。

マイクロセグメンテーションベースのソリューションは、ユーザーをセキュリティグループに関連付け、ユーザーを IP アドレス範囲から分離し、ユーザーロールからセキュリティグループへのバインディングを通じて、異なる分離ドメイン内の同じユーザーの認証とオンボーディングを実装する。このソリューションは、ユーザーが分離ドメイン間を移動するときに、ユーザーロールとグローバルな統一ポリシーの実施に基づいてサービス分割を実装する。

マイクロセグメンテーションでは、分離ドメイン間のセキュリティグループがサポートされるため、各 IP アドレス範囲に基づいてセキュリティグループのグループ間ポリシーを構成する必要はありません。また、マイクロセグメンテーションでは、サブセキュリティグループもサポートされます。サブセキュリティグループは、親グループから権限を継承できます。また、サブグループの権限を個別に構成して、きめ細かい権限制御とユーザーロールの割当てを実現することもできます。



サービス機能については、表 1 に示す関連資料で説明されています。

表 1 機能と関連ドキュメント

任意管理項目	説明	ドキュメント
自動化	デバイス導入の自動化	*AD-Campus 6.2 Automation設定ガイド* *AD-Campus 6.2 Optimized Automation Configuration Guide*
セミオートメーション	スパイン/リーフデバイスの手動組み込み、およびアクセスデバイスの自動組み込み	*AD-Campus 6.2 Semi-Automation設定ガイド*
ワイヤレス	AC組み込み、ワイヤレスユーザー認証、およびオンボーディング	*AD-Campus 6.2 ワイヤレスサービスコンフィギュレーションガイド*
IPv6(IPv6	IPv6デバイスの組み込みとユーザーのIPv6アドレス取得	*AD-Campus 6.2 IPv6 サービスコンフィギュレーションガイド*
複数キャンパスの相互接続	分離ドメイン相互接続、および分離ドメインと複数のファブリック間の相互接続	*AD-Campus 6.2 Multi-Campus Multi-Fabric コンフィギュレーションガイド*
MicrosoftのDHCP	Microsoft DHCP密結合環境のセットアップと構成	*AD-Campus 6.2 Tight Microsoft DHCP Management Configuration Guide(Microsoft*

任意管理項目	説明	ドキュメント
		DHCP 管理設定ガイド)
セキュリティの集約	ユーザー機器組み込みサービス	*AD-Campus 6.2 Security Convergenceコンフィギュレーションガイド*
EPON	EPONのネットワーク設定とサービス設定	*AD-Campus 6.2 EPON設定ガイド*
故障したデバイスの交換	故障したデバイスの正確な交換と異種の交換	*AD-Campus 6.2デバイス交換コンフィギュレーションガイド*

単一ファブリックのネットワーク方式

AD-Campus ネットワークソリューションでサポートされるネットワークモデルには、デュアルスパインネットワークと IRF ネットワークがあります。デュアルスパインネットワークでは、2 つのスパインが DR システムを形成するか、冗長性と負荷分散のためにアップリンクでデュアルホーム接続されます。IRF ネットワークでは、2 つのデバイスを 1 つのデバイスに仮想化して、複数のデバイスの共同運用、統合管理、および中断のないメンテナンスを実現します。デバイスアーキテクチャに従って、2 つのモデルには次のネットワークスキームが含まれます。

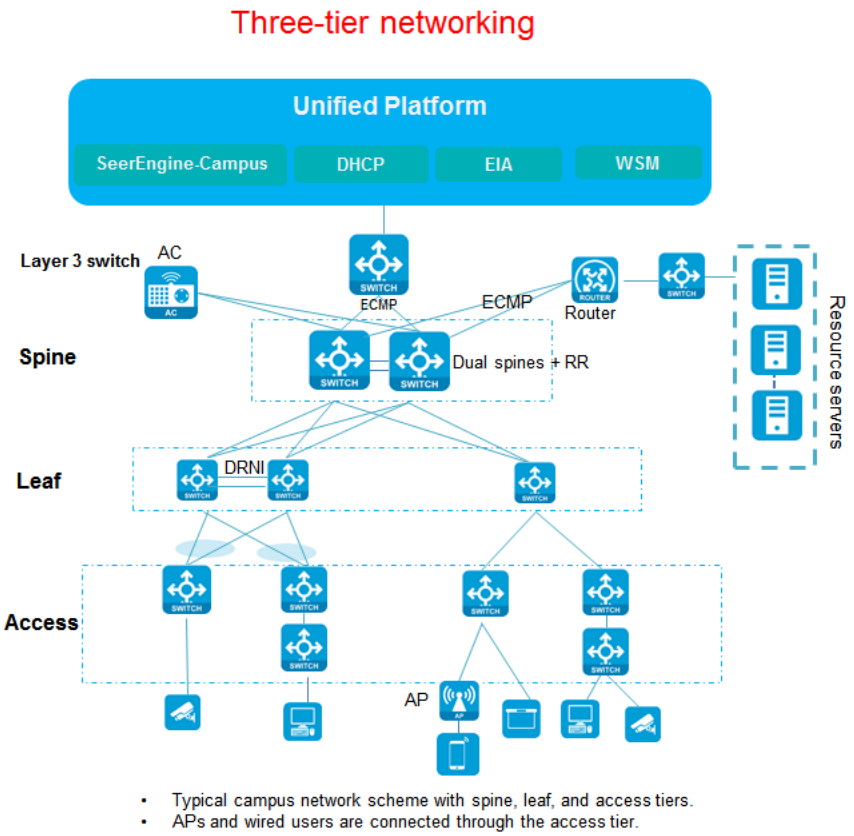
- **3 層ネットワークスキーム**: スパイン層、リーフ層およびアクセス層を含みます。これは、キャンパスネットワークの典型的なネットワークスキームです。スパイン、リーフおよびアクセスデバイスは IRF ファブリックをサポートします。さらに、アクセスデバイスはマルチレベルカスケード接続をサポートします。
- **2 層ネットワークスキーム**: アクセスデバイスのない、スパイン層とリーフ層を含みます。ワイヤレス AP と有線ユーザーは、リーフデバイスに直接接続されます。
- **シングルリーフネットワークスキーム**: リーフ層とアクセス層が含まれ、スパインデバイスは含まれません。通常、小規模なネットワークで使用されます。ネットワークには、IRF ファブリック内に 1 つのリーフデバイスまたは 2 つのリーフデバイスを含めることができます。アクセスデバイスは、IRF ファブリックとマルチレベルカスケード接続をサポートします。

このドキュメントで紹介する 3 層、2 層、およびシングルリーフのネットワーク方式は、単一ファブリック用です。マルチファブリックネットワーク構成の詳細については、「AD-Campus 6.2 Multi-Campus Multi-Fabric Configuration Guide」を参照してください。

デュアルスパインネットワーク

3 層ネットワーク方式

図 1 3 層ネットワーク方式



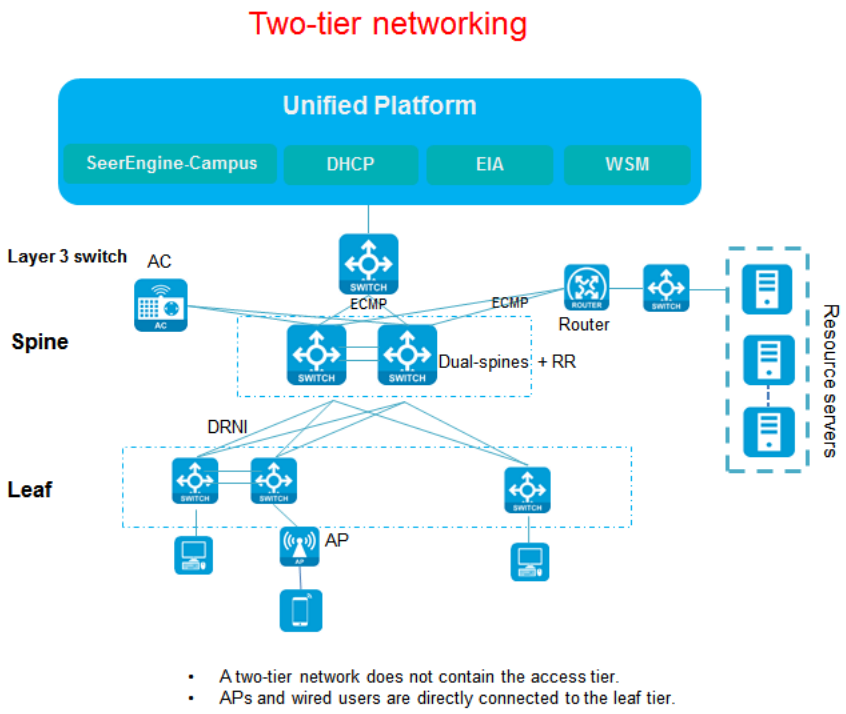
3 層ネットワーク方式には、スパイン、リーフ、およびアクセスデバイスが含まれます。これは、AD-Campus ソリューションの一般的なネットワークです。

スパインデバイスは、VXLAN をサポートする必要があり、通常、ルートリフレクタ(RR)およびルーティングデバイスとして動作して、異なるリーフデバイス間でルートを転送します。また、さまざまなタイプのサーバーと通信するための境界デバイスとしても動作します。デュアルスパインデバイスには、DRNI ネットワーキングと非 DRNI ネットワーキングの 2 つのモードがあります。デュアルスパインデバイスの場合、有線シナリオで DRNI を設定する必要はありません。AC がヘアピンモードでスパインデバイスに接続されている場合、2 つのスパインデバイスは DR システムを形成し、DR インターフェイスを介して AC と通信する必要があります。リーフデバイスは、ユーザー認証およびルート転送のために VXLAN をサポートする必要があります。アクセスデバイスは、AP およびエンドポイントに接続し、マルチレベルカスケード接続をサポートします。

デュアルスパインのシナリオでは、スパインデバイスを手動で組み込みます。詳しくは、または「Configure dual spine uplink または Configure DRNI for dual spine devices (manual)」を参照してください。

2 層ネットワーク方式

図 2 2 層ネットワーク方式

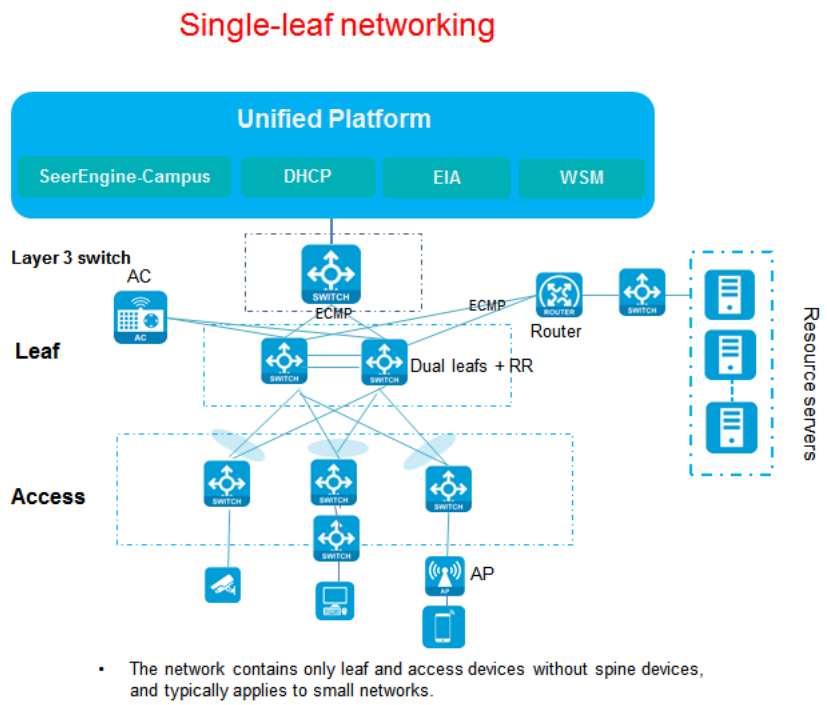


AD-Campus ソリューションの 2 層ネットワーキングスキームには、アクセスデバイスのないスパインデバイスとリーフデバイスのみが含まれます。ワイヤレス AP と有線ユーザーは、リーフデバイスに直接接続されます。リーフデバイスを AP とユーザーに接続するインターフェイスは、手動で設定する必要があります。

スパインデバイスは、VXLAN をサポートする必要があり、通常、異なるリーフデバイス間でルートを転送するための RR およびルーティングデバイスとして機能します。また、さまざまなタイプのサーバーと通信するための境界デバイスとしても機能します。デュアルスパインデバイスには、DRNI ネットワーキングと非 DRNI ネットワーキングの 2 つのモードがあります。デュアルスパインデバイスの場合、有線シナリオで DRNI を設定する必要はありません。AC がヘアピンモードでスパインデバイスに接続されている場合、2 つのスパインデバイスは DR システムを形成し、DR インターフェイスを介して AC と通信する必要があります。

シングルリーフネットワーク方式

図 3 シングルリーフネットワーク方式

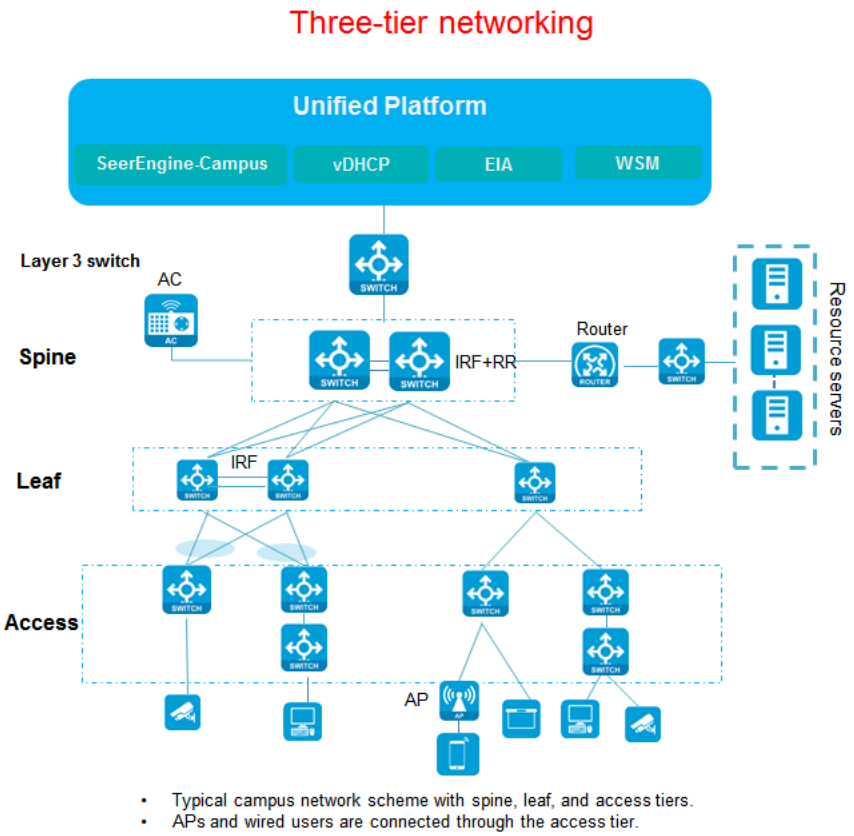


シングルリーフネットワーキングスキームには、1 つのリーフデバイス(または IRF ファブリックを形成する 2 つのリーフ)のみが含まれ、スパインデバイスは含まれません。複数のアクセスデバイスがリーフデバイスまたはリーフ IRF ファブリックに接続されます。ネットワーク展開は簡単です。このスキームは、通常、小規模なネットワークに適用できます。リーフデバイス(またはリーフ IRF ファブリック)は、境界デバイスとさまざまなサーバー間のインターワーキングを実装します。ベストプラクティスとして、デュアルリーフデバイスに DRNI を設定します。AC がヘアピンモードでリーフデバイスに接続されている場合、2 つのリーフデバイスは DR システムを形成し、DR インターフェイスを介して AC と通信する必要があります。

IRF ネットワーキング

3 層ネットワーク方式

図 4 3 層ネットワーク方式



3 層ネットワーク方式には、スパイン、リーフ、およびアクセスデバイスが含まれます。これは、AD-Campus ソリューションの一般的なネットワークです。

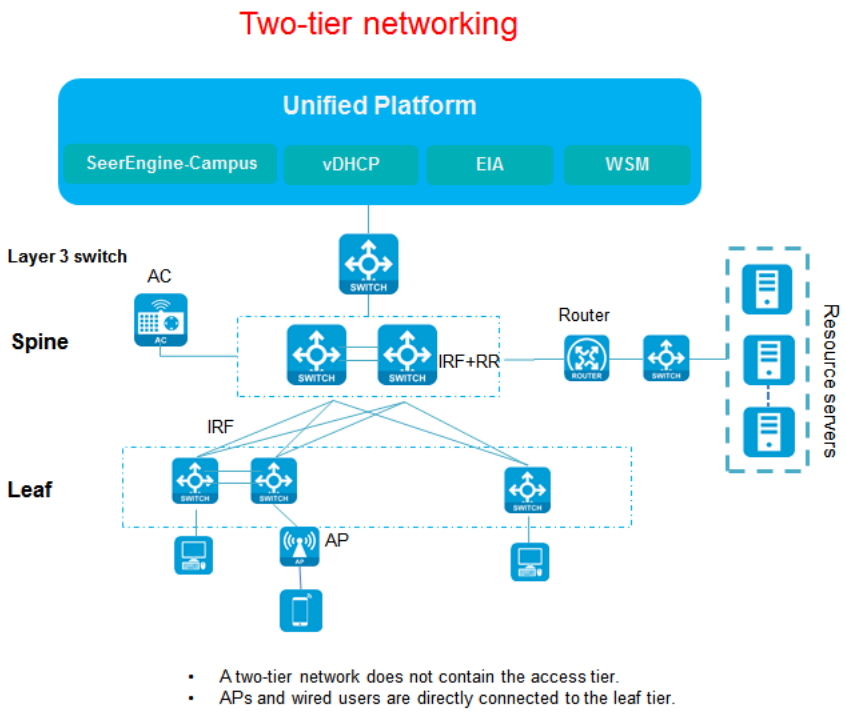
スパインデバイスは VXLAN をサポートする必要があり、通常は RR およびルーティングデバイスとして動作して、異なるリーフデバイス間でルートを転送します。また、さまざまなタイプのサーバーと通信するための境界デバイスとしても動作します。スパインデバイスは、スタンドアロンモードおよび IRF モードでの展開をサポートします。

リーフデバイスは、ユーザー認証とルート転送のために VXLAN をサポートする必要があります。

アクセスデバイスは AP とエンドポイントに接続し、マルチレベルのカスケード接続をサポートします。

2 層ネットワーク方式

図 5 2 層ネットワーク方式

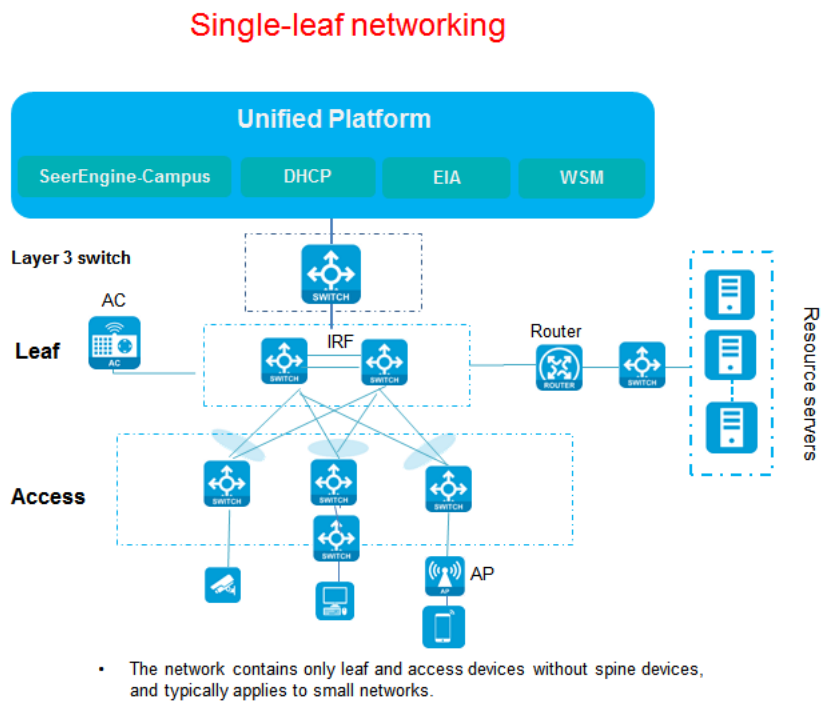


2 層ネットワーク方式には、アクセスデバイスのないスパインデバイスとリーフデバイスのみが含まれます。ワイヤレス AP と有線ユーザーは、リーフデバイスに直接接続されます。リーフデバイスを AP とユーザーに接続するインターフェイスは、手動で設定する必要があります。

スパインデバイスは VXLAN をサポートする必要があり、通常は RR およびルーティングデバイスとして動作して、異なるリーフデバイス間でルートを転送します。また、さまざまなタイプのサーバーと通信するための境界デバイスとしても動作します。スパインデバイスは、スタンドアロンモードおよび IRF モードでの展開をサポートします。

シングルリーフネットワーク方式

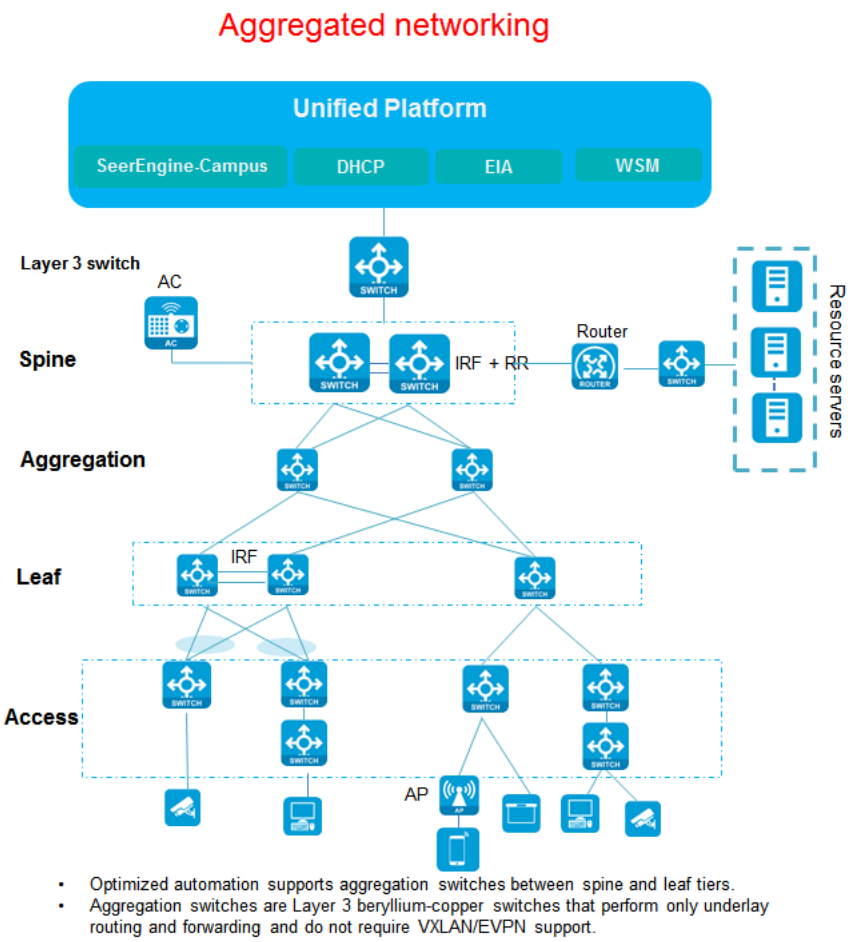
図 6 シングルリーフネットワーク方式



シングルリーフネットワーキングスキームには、スパインデバイスを使用せずに、1 つのリーフデバイス(または IRF ファブリックを形成する 2 つのリーフ)のみが含まれます。複数のアクセスデバイスがリーフデバイスまたはリーフ IRF ファブリックに接続されます。ネットワーク展開は簡単です。このスキームは通常、小規模なネットワークに適用できます。リーフデバイスは、さまざまなタイプのサーバーと通信するための境界デバイスとして機能し、スタンドアロンモードおよび IRF モードでの展開をサポートします。

集約された 3 層/2 層ネットワーク

図 7 集約された 3 層のネットワーク図



集約された 3 層/2 層ネットワーキングには、次の機能があります。

- 一般的な 3 層/2 層ネットワーキングと比較して、集約ネットワークでは、スパイン層とリーフ層の間にレイヤー3 集約スイッチが追加されるため、VXLAN/EVPN が不要になります。
- Spine/leaf/access は、スタンドアロンまたは IRF アーキテクチャをサポートします。
- スパイン/リーフ層とアグリゲーション層は、複数のリンクを介して接続され、等コストマルチパス(ECMP)ルーティングを形成する。
- リーフ層とアクセス層は、複数のリンクを介して接続され、リンク集約を実装します。

サーバーとデバイス間の接続

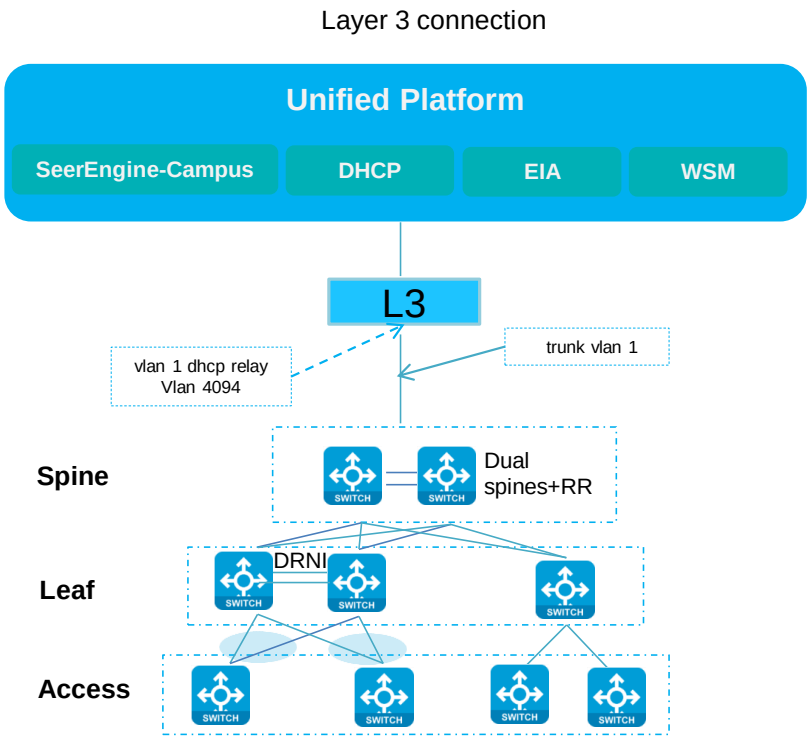
前述の 3 つのネットワーキングスキームは、スパイン、リーフ、およびアクセスデバイスの接続モードに基づいており、AD-Campus ソリューションの単一ファブリック内の基本的なネットワーキングスキームです。

この項では、Unified Platform とそのコンポーネント(SeerEngine キャンパス、vDHCP サーバー、EIA など)およびスイッチ間の接続、つまりレイヤー3 ネットワーク接続について説明します。

コントローラとスイッチの管理 IP アドレスは、異なるネットワークセグメントに属し、レイヤー3 ルーティングを介して相互に到達します。コントローラは、リモートエンドまたはローカルエンドに展開できます(コントローラとデバイスは、同じレイヤー2 ネットワークドメインにある必要はなく、レイヤー3 接続だけが必要です)。展開には、1 つまたは 2 つの NIC が必要です。展開に 1 つの NIC を使用する場合、SeerEngine キャンパスと統合プラットフォームはそれぞれ 1 つの NIC を共有します。展開に 2 つの NIC を使用する場合、SeerEngine キャンパスと統合プラットフォームはそれぞれ 1 つの NIC を個別に使用します。

デュアルスパインネットワーク

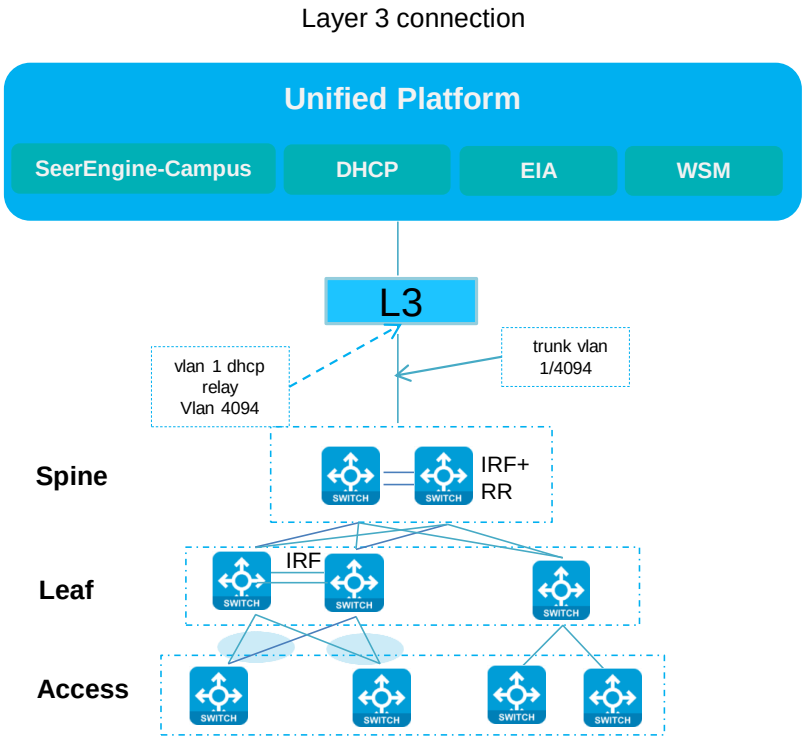
図 8 デュアルスパインデバイスを介したサーバーとデバイスの接続



スパインデバイスの IRF ネットワーキング

図 9 スパインデバイスの IRF ファブリックを介したサーバーとデバイスの接続

Connections between servers and devices



ネットワーク構成

1. AD-Campus ネットワークでは、SeerEngine キャンパス、DHCP サーバー、およびネットワークデバイスがレイヤー3 で相互接続されています。スパインデバイスとサーバーの間に必要なアップリンクは 1 つだけで、リンクに対して **port trunk permit vlan1 4094** コマンドを実行する必要があります。
2. スパインデバイスは、VXLAN をサポートし、異なるリーフデバイス間でルートを転送するための RR およびルーティングデバイスとして機能する必要があります。また、さまざまなタイプのサーバーと通信するための境界デバイスとしても機能します。スパインデバイスとリーフデバイス間のリンクは、アンダーレイリンクです。スパインデバイスとリーフデバイス間のルートが到達可能であることを確認するだけで済みます。
3. リーフデバイスは、ダウンリンクインターフェイスを使用してアクセスデバイスに接続します。リーフダウンリンクインターフェイスは、ユーザー認証を実行します。ユーザーがオンラインになると、リーフデバイスは **downlink interface + VLAN ID** によってさまざまなアクセスインターフェイスを識別し、ログインアカウントに基づいてさまざまなユーザーセキュリティグループにユーザーを割り当てます。
4. アクセスデバイスはレイヤー2 で動作し、通常はエンドポイントに接続されます。アクセスデバイスと

リーフデバイス間のリンクは、アクセスアップリンクインターフェイスを介して接続され、アップリンクインターフェイスは、**port trunk permit vlan all** コマンドを使用して、すべての VLAN を許可するトランクポートとして設定されます。アクセスデバイスは、最大 3 レベルのカスケード接続をサポートします。自動展開時には、アクセスデバイス間のカスケード接続に GE インターフェイスを使用する必要があります。

5. SeerEngine キャンパスコントローラは、アクセスデバイスの各ダウンリンクインターフェイスに VLAN ID(VLAN 101 から開始)を割り当て、各エンドポイントの場所をマークします。マルチレベルカスケード接続のアクセスデバイスの場合、コントローラは VLAN ID を段階的に割り当てます。たとえば、2 レベルのカスケード接続のアクセスデバイスの場合、コントローラは第 1 レベルのアクセスデバイスに VLAN 101 から VLAN 152 を割り当て、第 2 レベルのアクセスデバイスに VLAN 153 から開始する VLAN ID を割り当てます。同じリーフの異なるダウンリンクインターフェイスに接続されたアクセスデバイスの場合、コントローラは VLAN 101 から開始する VLAN ID を各アクセスデバイスに割り当てます。
6. stp edged-port コマンドを使用して、ユーザーエンドポイントに接続されたアクセスデバイス上のインターフェイスをエッジポートとして設定します。

```
#
 Interface GigabitEthernet1/0/31
 port link-mode bridge
 port access vlan 130
 stp edged-port
#
```

重要:

stp edged-port コマンドは、アクセスデバイスが組み込まれた後に、エンドポイントに接続されたアクセスデバイスインターフェイスに対して発行されます。アクセスデバイスとリーフデバイス間のリンクが後で追加された場合、stp edged-port コマンドは自動的に削除されません。コマンドは手動で削除する必要があります。

設定ワークフロー

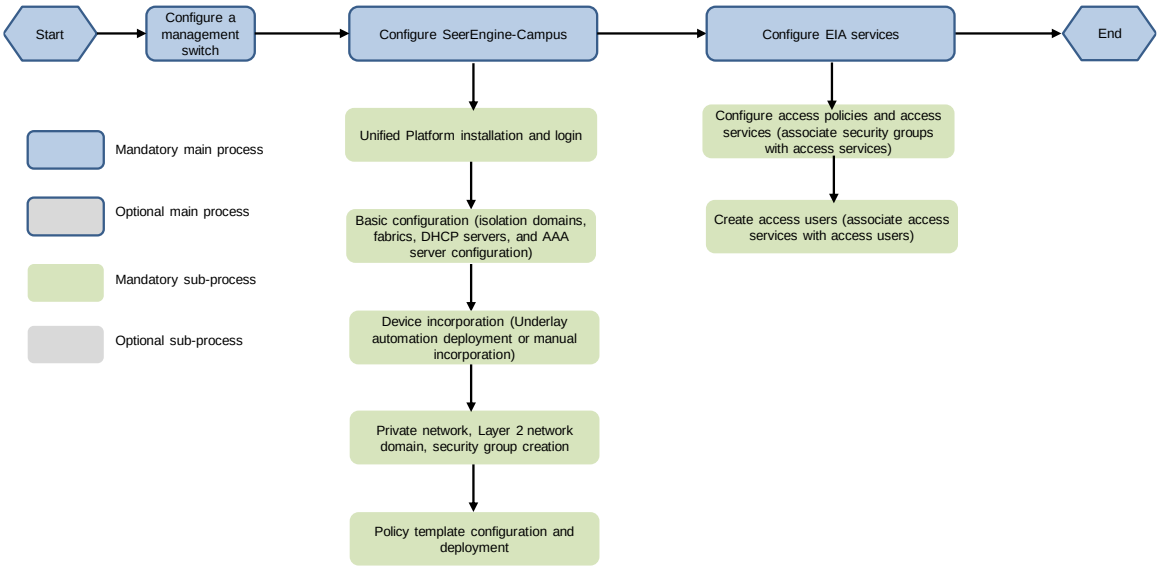
AD-Campus 6.2 ソリューションには、アンダーレイ設定、デバイスの組み込み、オーバーレイ設定、およびユーザー認証設定が必要です。

- アンダーレイ構成は、デバイスを組み込む前の基本であり、通常は、自動オンボード構成または手動構成を通じて、デバイスの物理的な接続構成に関連しています。
- オーバーレイ設定は、プライベートネットワーク、レイヤー2 ネットワークドメイン、セキュリティグループの作成、およびグループ間ポリシーとサービスチェーンの設定など、ユーザーサービスに関連しています。

- ユーザー認証設定には、ユーザー管理、アクセスポリシー、およびアクセスサービスが含まれます。ユーザー認証設定は、EIA 認証サーバーを介して実装されます。

SeerEngine キャンパス環境と EIA 環境はどちらも、スタンドアロン配置とクラスタ配置をサポートしています。詳細については、『AD-Campus 6.2 Unified Platform and Deployment Guide』を参照してください。

図 10 設定ワークフロー



重要:

自動デバイス展開または手動設定によって、アンダーレイ設定を実行します。

- 自動デバイス展開の詳細については、「AD-Campus 6.2 Automation Configuration Guide」を参照してください。
- 0 手動設定の詳細については、「Manually incorporating a device」を参照してください。

ソフトウェアとハードウェアの要件

アプリケーション要件

表 2 アプリケーション要件

製品	名前	説明	備考
統合プラットフォーム	GlusterFS	製品内でローカル共有ストレージ機能を提供	必須
	ポータル	ポータル、統合認証、ユーザー管理、サービスゲートウェイ、ヘルプセンター	必須
	カーネル	権限、リソースID、ライセンス、構成センター、リソースグループ、およびログサービス	必須
	カーネルベース	アラーム、アクセスパラメーターテンプレート、監視テンプレート、レポート、EメールおよびSMS転送サービス	必須
	ネットワーク	基本的なネットワーク管理(ネットワークリソース、ネットワークパフォーマンス、ネットワークトポロジー、iCC)	必須
	カーネル領域	階層型管理	オプション
	ダッシュボード	ダッシュボードフレームを提供します	必須
	ウィジェット	ダッシュボード用のウィジェットを提供します	必須
	Syslog	syslog機能とログセンターを提供	オプション
	Websocket	レガシーデバイスの自動化機能と最適化された自動化機能を提供	必須
キャンパスのシナリオに必要なコンポーネント	SeerEngineキャンパス	基本的なキャンパスサービス設定を提供する、キャンパスネットワーク管理コントローラ	必須
	vDHCP	DHCPサーバー、デバイスの自動オンボード、およびエンドユーザーへのアドレスの割り当て	必須
	EIA	ユーザー認証サービス構成を提供する、エンドユーザーのインテリジェントなアクセス	必須

製品	名前	説明	備考
	WSM	ワイヤレスアクセスサービスを提供するワイヤレス管理プラットフォーム	オプション
	EAD	エンドポイントアクセスコントロールプラットフォーム、エンドポイントアクセスの制御	オプション
	EPS	エンドポイントをアクティブに識別し、エンドポイントアクセスを検出するエンドポイントプロファイリングシステム	オプション
	SeerAnalyzer	ネットワークデータの収集と分析	オプション
	SMP	ファイアウォール管理機能を提供する	オプション
密結合をサポートするDHCPサーバー	vDHCPサーバー	H3C DHCPサーバー	必須
	Microsoft DHCPサーバー	密結合と疎結合をサポート	*該当なし*

ハードウェア要件

表 3 サポートされるデバイスのモデルと役割

デバイスモデル	デフォルトの役割	サポートされるその他の役割
S12500G-AF	スパイン	リーフ/アクセス
S 10500 X/S 10500	スパイン	リーフ/アクセス
S7500X	リーフ	スパイス/アクセス
S6550XE-HI	リーフ	アクセス
S6525XE-HI	リーフ	アクセス
S 6520 X-HI	リーフ	アクセス
S 5560 X-HI	リーフ	アクセス
S6520X-EI(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)	リーフ	アクセス
S5560X-EI(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)	リーフ	アクセス

S6520X-SIの場合	アクセス	該当なし
S5130-EI S 5130-HI S5130S-E S5130S-HI	アクセス	該当なし

リソースと IP アドレスの計画

サービスリソースプランニング

サーバーとデバイス間の中間スイッチは、L3 スイッチと呼ばれます。デバイスが自動または手動のどちらでオンボードされる場合でも、デバイスとコントローラ間の接続を確保するために、中間 L3 スイッチに手動設定が必要です。

設定の前に、ネットワークを準備します。SeerEngine キャンパスコントローラと統合プラットフォームは、1 つのネットワークアダプタを共有することも、異なるネットワークアダプタを使用することもできます。

重要:

ベストプラクティスとして、EIA と VLAN 4094 には異なるサブネットの IP アドレスを使用してください。

デュアルホームスパイン

SeerEngine キャンパスのコントローラと統合プラットフォームは、1 つのネットワークアダプタを共有します。

図 11 SeerEngine キャンパスのコントローラと統合プラットフォームは、1 つのネットワークアダプタを共有します。

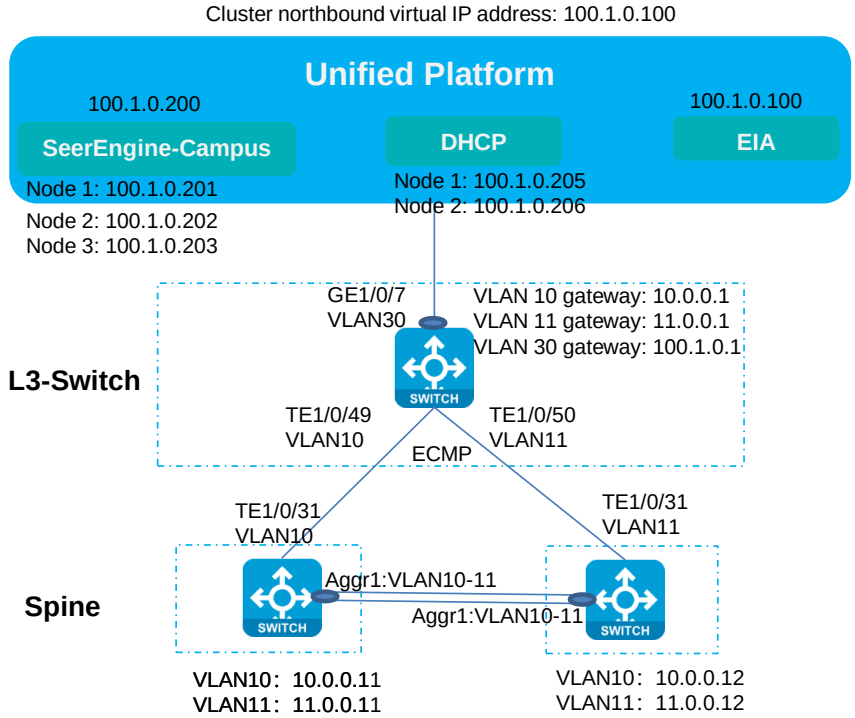


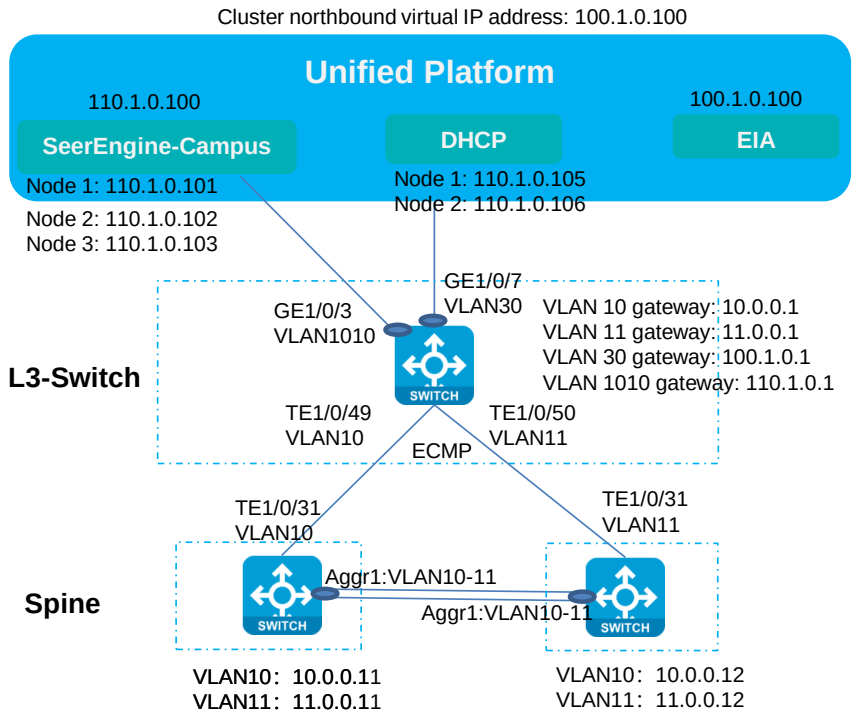
表 4 サーバーの IP アドレスとレイヤー3 スイッチのネットワーク計画のリスト

項目(Item)	例:	備考
VLAN 1ネットワークセグメント(ゲートウェイ)	120.1.0.0/24(120.1.0.1)	導入を自動化するVLAN 1ネットワーク
VLAN 4094ネットワークセグメント(ゲートウェイ)	130.1.0.0/24(130.1.0.1)	コントローラとデバイス間の通信用のVLAN 4094ネットワーク
VLAN 10ネットワークセグメント(ゲートウェイ)	10.0.0.0/24(10.0.0.1)	レイヤー3でのスパインデバイスとの相互接続用のVLAN 10
VLAN 11ネットワークセグメント(ゲートウェイ)	11.0.0.0/24(11.0.0.1)	レイヤー3でのスパインデバイスとの相互接続用のVLAN 11
VLAN 30ネットワークセグメント(ゲートウェイ)	100.1.0.0/24(100.1.0.1)	統合プラットフォーム、SeerEngineキャンパス、およびvDHCPで使用されるネットワークセグメント
アンダーレイIPアドレスのネットワークセグメント	200.1.1.0/24	スパインおよびリーフデバイス上のループバックインターフェイスIPアドレスのネットワークセグメント
Unified Platformノースバウンドサービスの IPアドレス	100.1.0.100	Unified Platformへのログインに使用されるアドレス
EIA	100.1.0.100	コンバージドデプロイメント中のUnified PlatformのノースバウンドサービスIPアドレスであるEIAサーバーIPアドレス
SeerEngineキャンパスクラスタのIPアドレス	100.1.0.200	SeerEngineキャンパスクラスタのIPアドレス
SeerEngineキャンパスノードのIPアドレス	ノード1:100.1.0.201 ノード2:100.1.0.202	SeerEngineキャンパスノードのIPアドレス

項目(Item)	例:	備考
	ノード3:100.1.0.203	
vDHCPクラスタのIPアドレス	100.1.0.204	vDHCPサーバーのクラスタIPアドレス(実際には使用されません)
vDHCPノードのIPアドレス	ノード1:100.1.0.205 ノード2:100.1.0.206	vDHCPサーバーの2つのノードのIPアドレス
Microsoft DHCPのIPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス

SeerEngine キャンパスのコントローラと統合プラットフォームでは、異なるネットワークアダプタを使用します。

図 12 SeerEngine キャンパスのコントローラと統合プラットフォームでは、異なるネットワークアダプタを使用します。



この例では、SeerEngine キャンパスコントローラと統合プラットフォームがそれぞれ 1 つの NIC を使用しています。表 5 に、アドレスプランニングを示します。

表 5 サーバーの IP アドレスとレイヤー3 スイッチのネットワーク計画のリスト

項目	例:	備考
VLAN 1ネットワークセグメント(ゲートウェイ)	120.1.0.0/24(120.1.0.1)	導入を自動化するVLAN 1ネットワーク
VLAN 4094ネットワークセグメント(ゲートウェイ)	130.1.0.0/24(130.1.0.1)	コントローラとデバイス間の通信用のVLAN 4094ネットワーク
VLAN 10ネットワークセグメント(ゲートウェイ)	10.0.0.0/24(10.0.0.1)	レイヤー3でのスパインデバイスとの相互接続用のVLAN 10
VLAN 11ネットワークセグメント(ゲートウェイ)	11.0.0.0/24(11.0.0.1)	レイヤー3でのスパインデバイスとの相互接続用のVLAN 11
VLAN 30ネットワークセグメント(ゲートウェイ)	100.1.0.0/24(100.1.0.1)	Unified PlatformでPCとの通信に使用されるネットワークセグメント
VLAN 1010(ゲートウェイ)	110.1.0.0/24(110.1.0.1)	SeerEngineキャンパスとvDHCPがコントローラとPC間の通信に使用するネットワークセグメント(SeerEngineキャンパスが独立したネットワークアダプタを使用する場合に設定)
アンダーレイIPアドレスのネットワークセグメント	200.1.1.0/24	スパインおよびリーフデバイス上のループバックインターフェイスIPアドレスのネットワークセグメント
Unified Platformノースバウンドサービスの IPアドレス	100.1.0.100	Unified Platformへのログインに使用されるアドレス
EIA	100.1.0.100	EIAサーバーのIPアドレス
SeerEngineキャンパスクラスタのIPアドレス	110.1.0.100	SeerEngineキャンパスクラスタのIPアドレス
SeerEngineキャンパ	ノード1:110.1.0.101	SeerEngineキャンパスノードのIPアドレス

項目	例:	備考
スノードのIPアドレス	ノード2:110.1.0.102 ノード3:110.1.0.103	
vDHCPクラスタのIPアドレス	110.1.0.104	vDHCPサーバーのクラスタIPアドレス(実際には使用されません)
vDHCPノードのIPアドレス	ノード1:110.1.0.105 ノード2:110.1.0.106	vDHCPサーバーの2つのノードのIPアドレス
Microsoft DHCPのIPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス

IRF ファブリック内のデュアルホームスパイン

SeerEngine キャンパスのコントローラと統合プラットフォームは、1 つのネットワークアダプタを共有します。

SeerEngine キャンパスコントローラと統合プラットフォームは、1 つの NIC を共有できます。この場合、統合プラットフォーム、SeerEngine キャンパス、vDHCP、および EIA は、同じネットワークセグメント内の IP アドレスを使用します。

図 13 SeerEngine キャンパスのコントローラと統合プラットフォームは、1 つのネットワークアダプタを共有します。

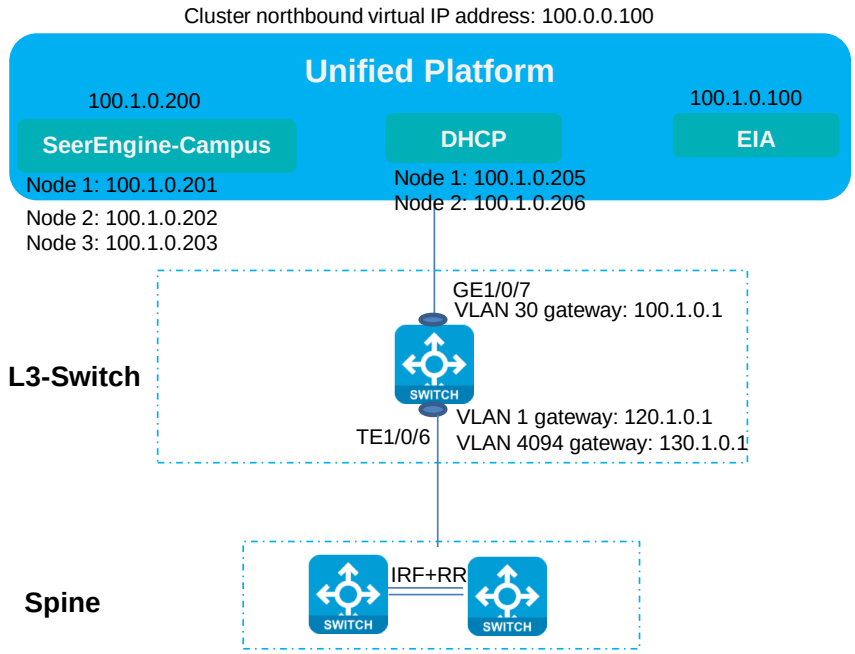


表 6 サーバーの IP アドレス

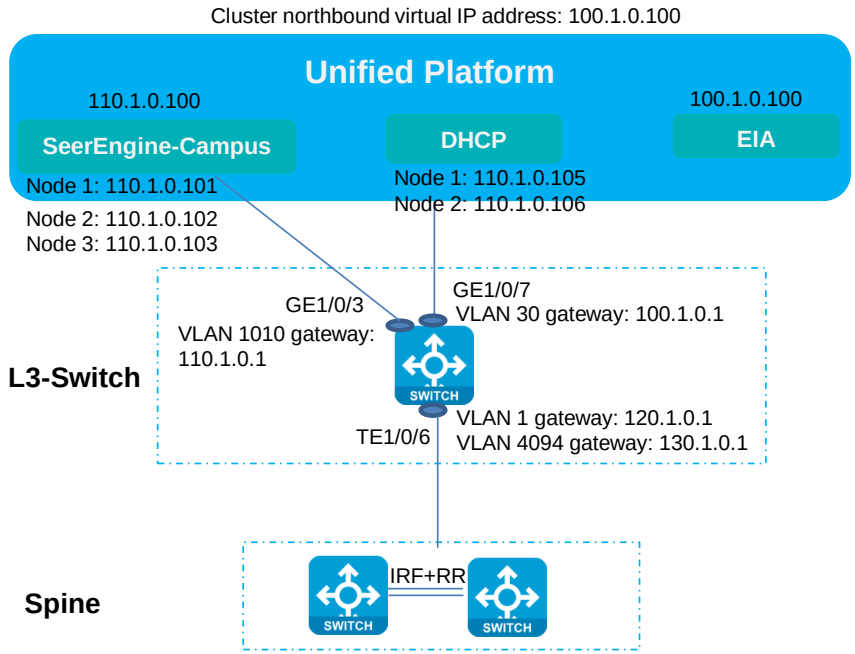
項目	例:	備考
VLAN 1ネットワークセグメント(ゲートウェイ)	120.1.0.0/24(120.1.0.1)	導入を自動化するVLAN 1ネットワーク
VLAN 4094ネットワークセグメント(ゲートウェイ)	130.1.0.0/24(130.1.0.1)	コントローラとデバイス間の通信用のVLAN 4094ネットワーク
VLAN 30ネットワークセグメント(ゲートウェイ)	100.1.0.0/24(100.1.0.1)	統合プラットフォーム、SeerEngineキャンパス、およびvDHCPで使用されるネットワークセグメント
VLAN 91ネットワークセグメント	91.1.0.0/24	手動取り込み時のスパインデバイスとリーフデバイス間の通信用VLAN
アンダーレイIPアドレスのネットワークセグメント	200.1.1.0/24	スパインおよびリーフデバイス上のループバックインターフェイスIPアドレスのネットワークセグメント
Unified Platformノースバウンドサービスの IPアドレス	100.1.0.100	Unified Platformへのログインに使用されるアドレス
EIA	100.1.0.100	コンバージドデプロイメント中にEIAサーバーによって使用されるUnified Platformのノースバウンドサービス IP
SeerEngineキャンパスクラスタのIPアドレス	100.1.0.200	SeerEngineキャンパスクラスタのIPアドレス
SeerEngineキャンパスノードのIPアドレス	ノード1:100.1.0.201 ノード2:100.1.0.202 ノード3:100.1.0.203	SeerEngineキャンパスノードのIPアドレス
vDHCPクラスタのIPアドレス	100.1.0.204	vDHCPサーバーのクラスタIPアドレス(実際には使用されません)
vDHCPノードのIPアドレス	ノード1:100.1.0.205 ノード2:100.1.0.206	vDHCPサーバーの2つのノードのIPアドレス
Microsoft DHCPのIPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアド

項目	例:	備考
		レス

SeerEngine キャンパスのコントローラと統合プラットフォームでは、異なるネットワークアダプタを使用します。

SeerEngine キャンパスのコントローラと Unified Platform は、それぞれ 1 つの NIC と 2 つのネットワークセグメントの IP アドレスを使用できます。この場合、EIA と Unified Platform クラスタは一方のネットワークセグメントの IP アドレスを使用し、SeerEngine キャンパスと vDHCP はもう一方のセグメントの IP アドレスを使用します。

図 14 SeerEngine キャンパスのコントローラと統合プラットフォームでは、異なるネットワークアダプタを使用します。



この例では、SeerEngine キャンパスコントローラと統合プラットフォームがそれぞれ 1 つの NIC を使用しています。表 7 に、アドレスプランニングを示します。

表 7 サーバーの IP アドレス

項目	例:	備考
VLAN 1ネットワークセグメント(ゲートウェイ)	120.1.0.0/24(120.1.0.1)	導入を自動化するVLAN 1ネットワーク
VLAN 4094ネットワークセグメント(ゲートウェイ)	130.1.0.0/24(130.1.0.1)	コントローラとデバイス間の通信用のVLAN 4094ネットワーク

項目	例:	備考
VLAN 30ネットワークセグメント(ゲートウェイ)	100.1.0.0/24(100.1.0.1)	Unified PlatformでPCとの通信に使用されるネットワークセグメント
VLAN 1010ネットワークセグメント(ゲートウェイ)	110.1.0.0/24(110.1.0.1)	SeerEngineキャンパスとvDHCPがコントローラとPC間の通信に使用するネットワークセグメント(SeerEngineキャンパスが独立したネットワークアダプタを使用する場合に設定)
VLAN 91ネットワークセグメント	91.1.0.0/24	手動で組み込む場合のスパインデバイスとリーフデバイス間の通信用VLAN
アンダーレイIPアドレスのネットワークセグメント	200.1.1.0/24 201.1.1.0/24	スパインおよびリーフデバイス上のループバックインターフェイスIPアドレスのネットワークセグメント
Unified Platformノースバウンドサービスの IPアドレス	100.1.0.100	Unified Platformへのログインに使用されるアドレス
環境アセスメント	100.1.0.100	EIAサーバーのIPアドレス
SeerEngineキャンパスクラスタのIPアドレス	110.1.0.100	SeerEngineキャンパスクラスタのIPアドレス
SeerEngine-キャンパスノードのIPアドレス	ノード1:110.1.0.101 ノード2:110.1.0.102 ノード3:110.1.0.103	SeerEngineキャンパスノードのIPアドレス
vDHCPクラスタのIPアドレス	110.1.0.104	vDHCPサーバーのクラスタIPアドレス(実際には使用されません)
vDHCPノードのIPアドレス	ノード1:110.1.0.105 ノード2:110.1.0.106	vDHCPサーバーの2つのノードのIPアドレス
Microsoft DHCPのIPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス

ユーザーリソースプランニング

表 8 に、このマニュアルでのユーザーサービスのリソースプランニングを示します。

表 8 ユーザーサービスの資源計画

項目(Item)	例:	備考
教師セキュリティグループのネットワークセグメント(ゲートウェイ)	20.0.0.0/16(20.0.0.1)	教師セキュリティグループユーザーのためのネットワーク
学生セキュリティグループ(ゲートウェイ)のネットワークセグメント	30.0.0.0/16(30.0.0.1)	学生セキュリティグループユーザーのためのネットワーク
BYODセキュリティグループ(ゲートウェイ)のネットワークセグメント	50.0.0.0/16(50.0.0.1)	BYODユーザーのネットワーク
ゲストネットワークセグメント(ゲートウェイ)	22.2.2.0/24(22.2.2.1)	ゲストユーザー用のネットワーク
認証失敗ネットワークセグメント(ゲートウェイ)	33.3.3.0/24(33.3.3.1)	認証に失敗したユーザーのネットワーク
Fail-permitネットワークセグメント(ゲートウェイ)	52.0.0.0/24(52.0.0.1)	fail-permitユーザーのネットワーク
Web PortalシナリオのIPアドレスグループ	104.0.0.1から104.0.0.254	Web Portalがユーザーに接続するネットワークセグメント
ITリソースグループ	41.0.0.0/8	ITリソースグループ
キャンパス出力アドレスプール	192.168.10.10から192.168.10.100	キャンパス出力アドレスプール
Microsoftの密結合DHCPアドレス	8.0.0.171	Microsoftの密結合DHCPアドレス
Microsoftの疎結合DHCPアドレス	8.0.0.173	Microsoftの疎結合DHCPアドレス
Web Portalシナリオでのサードパーティー AAAアドレス	10.99.12.189	Web Portalシナリオでのサードパーティー AAAアドレス
Web PortalシナリオのEIAアドレス	110.0.0.100	個別のEIAを使用できるWeb Portalシナリオの EIAアドレス。このセクションでは、個別のEIAをWeb Portalサ

項目(Item)	例:	備考
		ーバーとして使用します。
Web Portalシナリオのリーフデバイスの4094ネットワークセグメントのIPアドレス	130.1.0.34	Web Portalシナリオのリーフデバイスの4094ネットワークセグメントの IPアドレス

ユーザーVLAN プランニング

SeerEngine キャンパスには、4 つの VLAN プールがあらかじめ設定されています。**Automation**> **Campus Network**> **Network Devices**. を選択します。右上隅にある **VNID Pools** リンクをクリックして、VNID pool configuration ページを開きます。VLANs タブをクリックして、システムの現在の VLAN プール情報をすべて表示できる VLAN pool ページを開きます。

セキュリティグループのタイプは次のとおりです。デフォルトで作成される Campus アクセス VLAN プール(default_access)、セキュリティグループ VLAN プール(default_security_group)、およびキャンパス認証フリーVLAN プール(default_auth_free)のリソースプール名は編集できません。

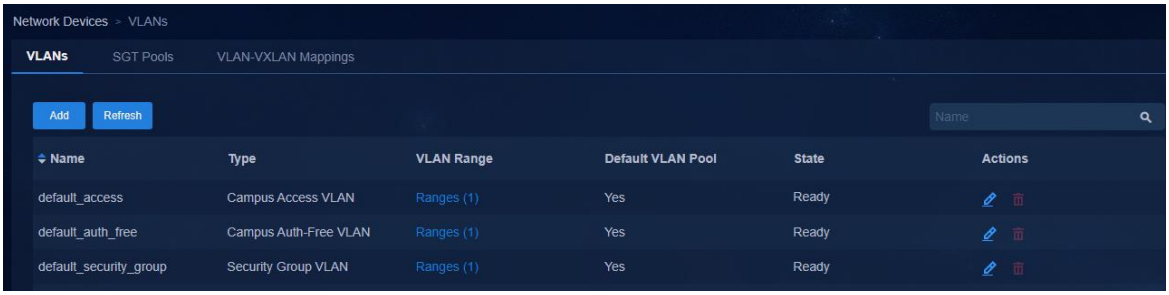
重要:

- VLAN プールは、バインディングで指定された後は変更できません。VLAN プールを編集するには、たとえば、新しい VLAN 範囲を追加または削除し、VLAN 範囲を予約するには、事前に計画を立てる必要があります。
- 異なる VLAN プールをオーバーラップさせることはできません。
- アクセス VLAN プールは、予約された VLAN 範囲の設定をサポートします。
- SeerEngine キャンパスでは、デバイスオートメーションスタックの BFD 検出用に、デフォルトで VLAN 100 が割り当てられています。VLAN 4090～4094 は予約済み VLAN です。
- DRNI が設定されている場合、コントローラは、DR システムの 2 つのデバイス間のアンダーレイのルート同期のために、デフォルトで VLAN 2 を発行します。
- ユーザー環境を以前のバージョンから 6.0 バージョンにアップグレードする場合、VLAN 監査の違いが存在する可能性があります。この問題は、データの同期によって解決できます。

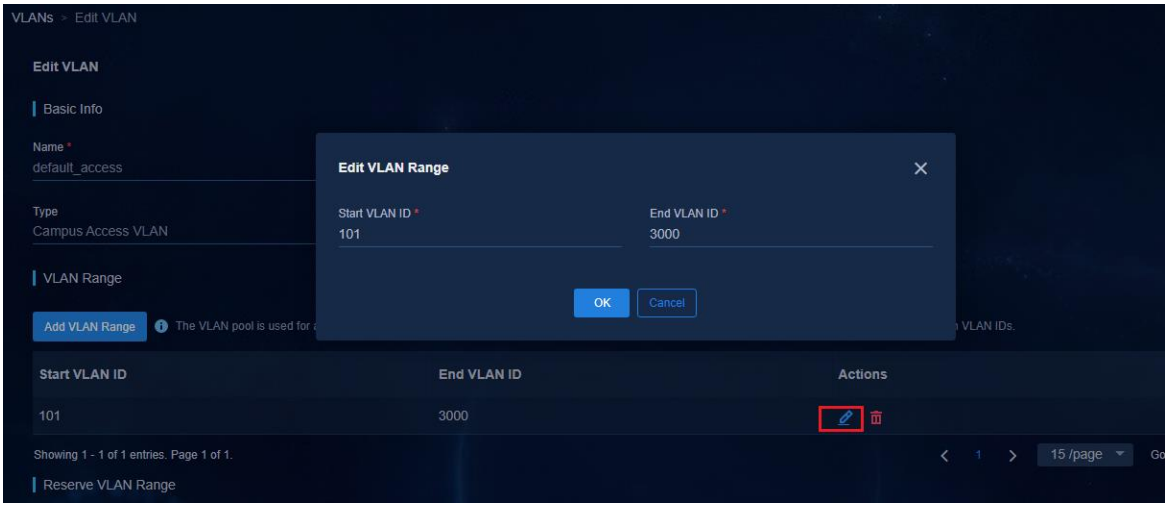
- キャンパスアクセス VLAN プール:アクセスデバイスがオンラインになった後、アクセスデバイスの VLAN 設定を発行するために使用されます。デフォルトの VLAN 範囲は 101～3000 です。
- セキュリティグループ VLAN プール:隔離されたドメイン内のセキュリティグループに VLAN ID を割り当て、ユーザーアクセスを可能にするために使用されます。デフォルトの VLAN 範囲は 3501～4000 です。
- キャンパス認証不要 VLAN プール:隔離されたドメインで認証不要 VLAN ID を割り当て、認証不要

バインディングのアクセスデバイスで VLAN 設定を発行するために使用されます。デフォルトの VLAN 範囲は 4051～4060 です。

- キャンパススタティックアクセス VLAN プール:スタティックキャンパスアクセス VLAN には、2801～3000 の VLAN 範囲を使用することをお勧めします。アクセス VLAN プールの範囲は、VLAN 101～VLAN 2800 に変更する必要があります。実際のネットワーク要件に従って値を設定します。



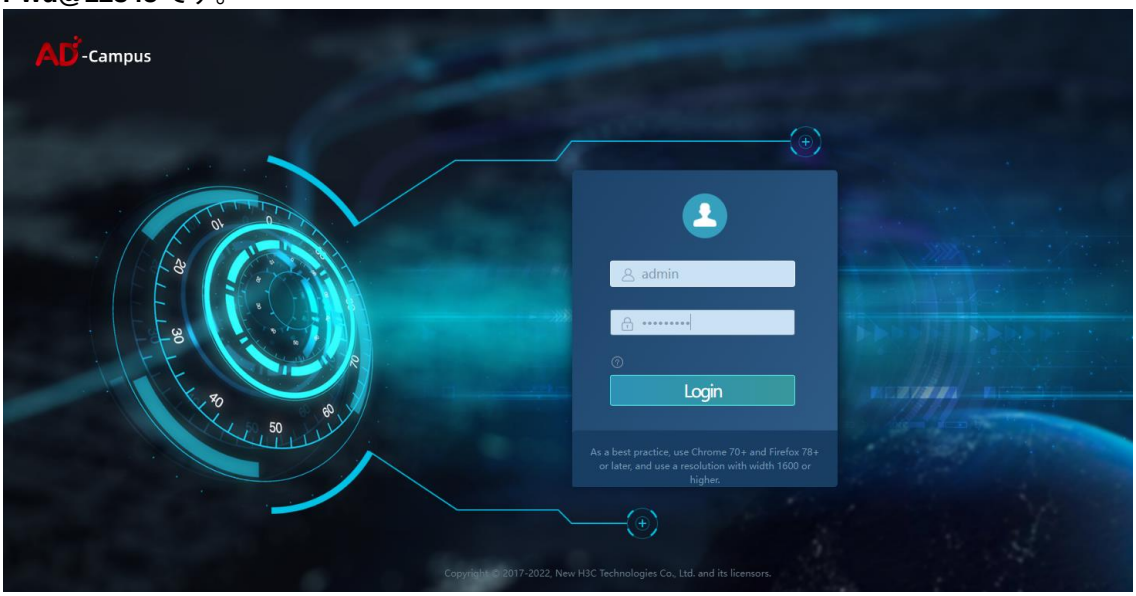
各リソースの VLAN プール範囲を調整する必要がある場合は、図に示すように、**Actions** 列をクリックして、VLAN プールを編集するためのページを開きます。**VLAN Range** 領域で、Actions 列をクリックして **Edit VLAN Range** ページを開き、VLAN 範囲を計画どおりに変更します。



AD-Campus コンフィギュレーション

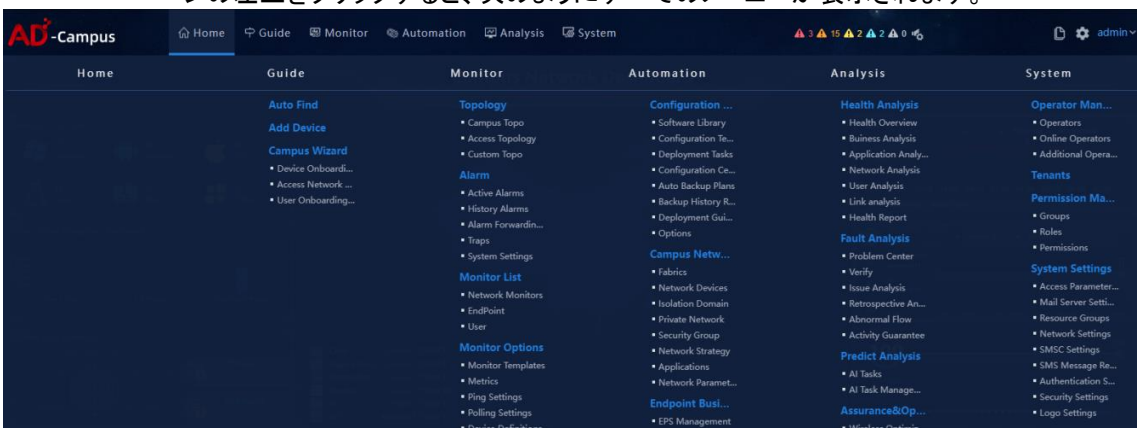
AD-Campus設定ページにログインします。

1. インストールおよび展開後、次の図に示すように、ブラウザのアドレスバーに AD-Campus コントローラのログインアドレスを入力して、ログインページを開きます。ログインアドレスの形式は http://100.1.0.100:30000/です。ログイン IP アドレスは、Unified Platform クラスタのノースバウンドサービス IP です。デフォルトのログインユーザー名とパスワードは、それぞれ **admin** と **Pwd@12345** です。



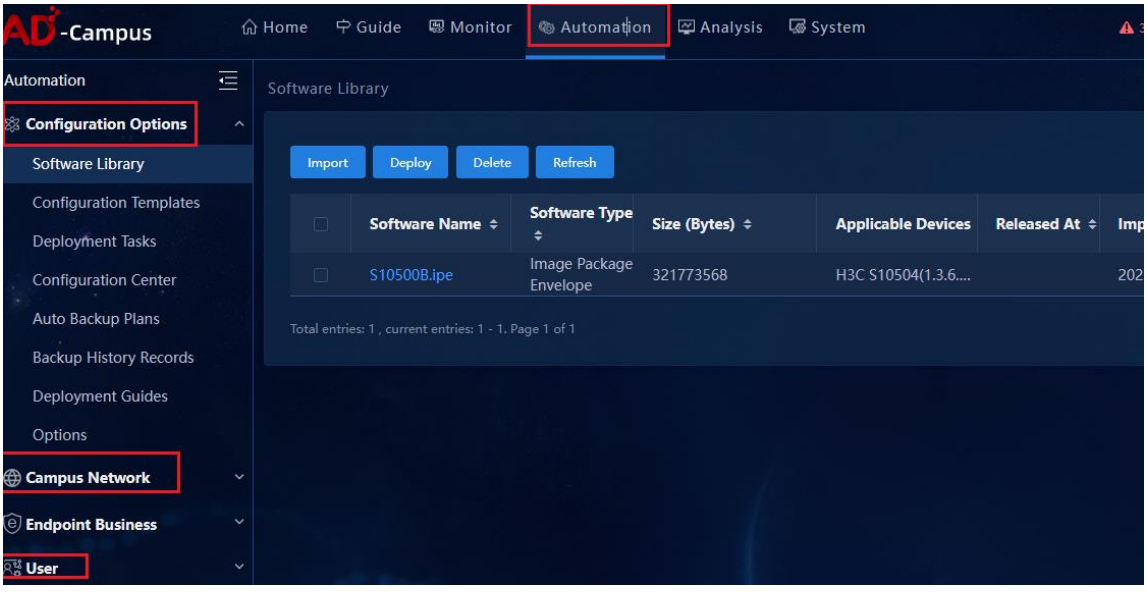
2. ユーザー名とパスワードを入力したら、**Login** をクリックして、AD-Campus コントローラの設定ページを開きます。

3. AD-Campusページの左上をクリックすると、次のようにすべてのメニューが表示されます。



4. 自動化機能モジュールは、AD-Campus サービスの構成に使用されます。ページの Automation タブをクリックして、左側のナビゲーションペインのメニューを次のように展開します。

   - **Configuration Options**: デバイスバックアップ、構成リカバリ、ソフトウェアライブラリなどのサービスを構成できます。
   - **Campus Network**: SeerEngine キャンパスコントローラに関連するサービスを設定できます。これには、デバイスオンボーディング、分離ドメイン、ファブリック、セキュリティグループ、グループ間ユーザーポリシー、およびサービスチェーンの自動テンプレート作成が含まれます。
   - **User**: アクセスサービス、アクセスポリシー、アクセスユーザーなど、EIA 認証サーバーのサービスを設定できます。

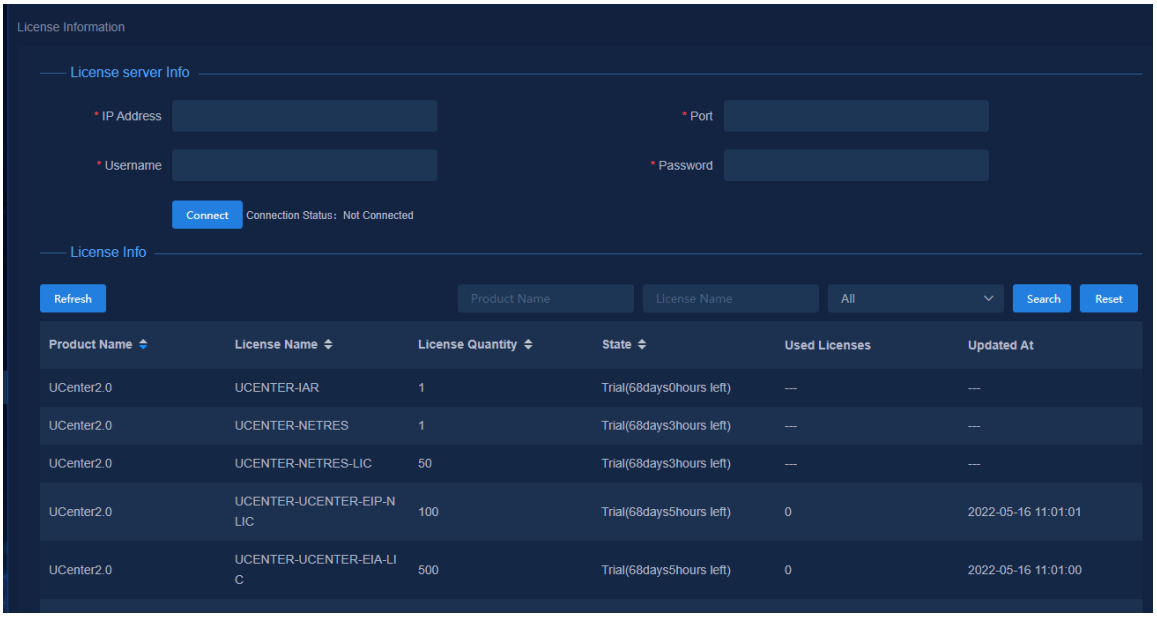


ライセンスの登録

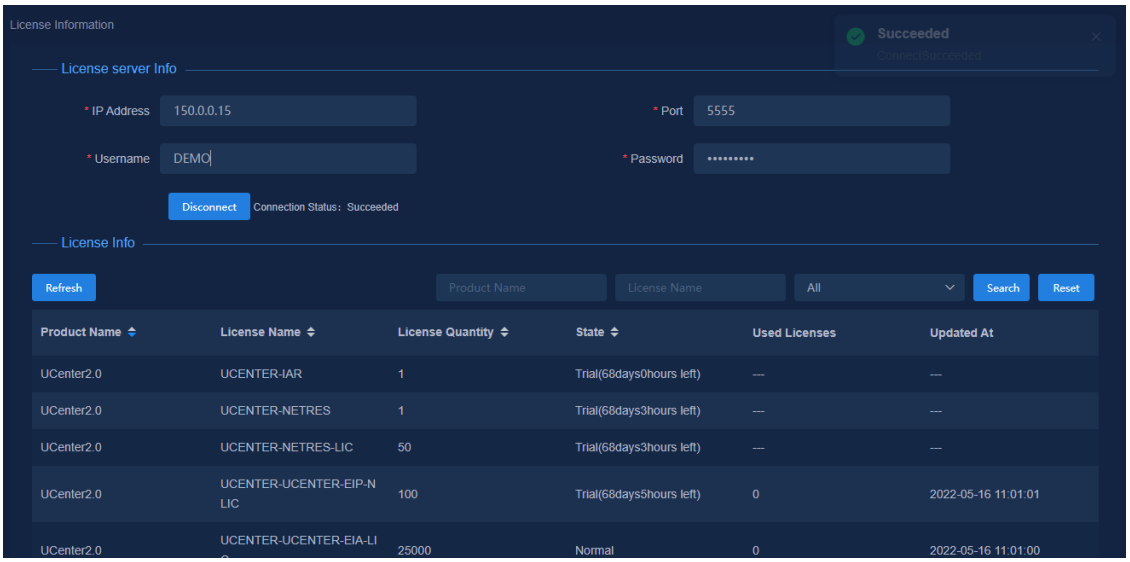
注:

- コントローラのインストールと展開が完了したら、SeerEngine キャンパス、EIA、vDHCP、および統合プラットフォームのコンバージェンス用のライセンスを登録する必要があります。ライセンスを登録する前に、ライセンスサーバーを設定し、ライセンスを購入してください。
- 現在のソフトウェアバージョンでは、ライセンスを登録することも、一時ライセンスを使用することもできます。
- ここでは、AD-Campus インターフェイスでライセンスを登録する方法についてのみ説明します。ライセンスサーバーの設定については、ライセンスサーバーのマニュアルを参照してください。

1. **System** > **License**> **License Information** を選択して、ライセンス登録ページを開きます。
2. システムがインストールおよび展開されると、デフォルトで一時ライセンスが使用可能になります。



3. ライセンス情報ページで、次のライセンスサーバーパラメーターを設定します。次に、接続をクリックしてライセンスサーバーに接続します。
   - **IP アドレス**: ライセンスサーバーの IP アドレスを入力します。Unified Platform クラスタのノースバウンド IP とライセンスサーバーが相互に到達できることを確認します。
   - **Port**: 5555。
   - **Username/Password**: ユーザー名 admin とパスワード admin@123 を入力します。アカウントとパスワードは、クライアント構成ページで構成されます。構成されたアカウントとパスワードを入力します。
4. ライセンスの登録後、ライセンス情報ページにライセンスが表示されます。



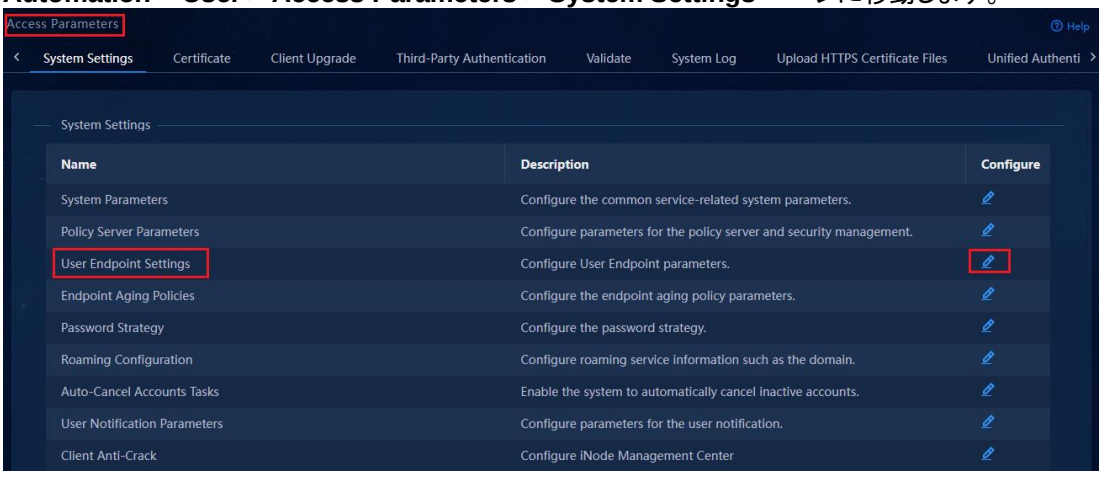
前提条件

コンフィギュレーションガイドを使用してサービスを設定する前に、エンドポイント設定、システムパラメーター、認証サーバー設定、および DHCP サーバー設定を設定する必要があります。

ユーザーエンドポイント設定の構成

認証サーバーで VXLAN ネットワーキングをイネーブルにするには、次のタスクを実行します。

1. **Automation > User > Access Parameters > System Settings** ページに移動します。

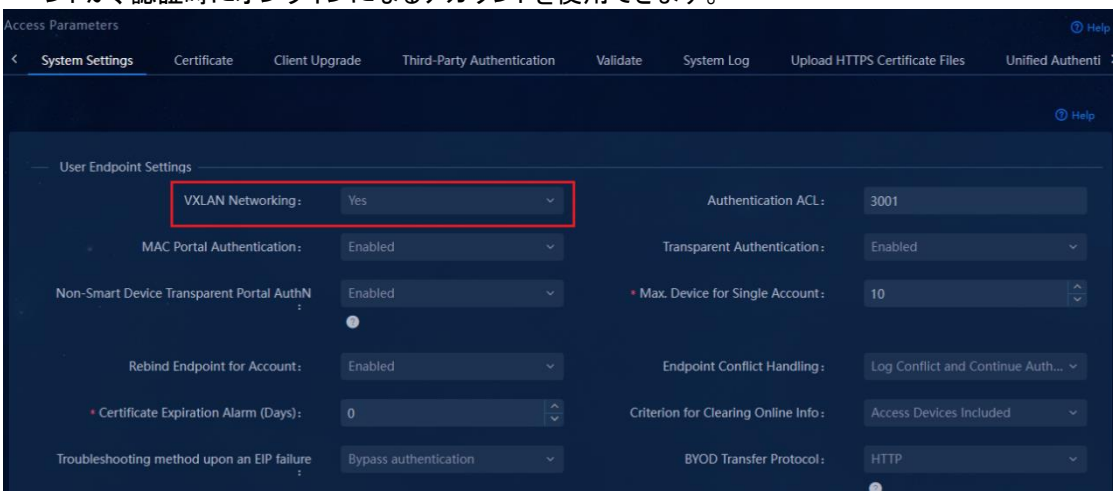


2. リストの User Endpoint Settings の Configure 列をクリックして、**User Endpoint Settings** ページを開きます。**User Endpoint Setting**s および構成 **Director Controller Configuration** のパラメーターを構成します。

   ユーザーエンドポイント設定のパラメーター:

   - **VXLAN Networking**: **Yes** を選択します。

  - **System** > **License**> **License Information**: **Enabled** を選択します。
- **Transparent Authentication**: **Enable**d を選択します。
- 同じ名前のアカウントの IP アドレスを強制的にバインド解除します。既定の設定はいいえです。
  - **No**: No を選択すると、IP アドレスはプリエンプトされず、生成された IP バインディングは再利用されません。
  - **Yes**: Yes を選択すると、IP バインディングが IP アドレスをプリエンプトできます。IP アドレスにバインドされているエンドポイントがオフラインになると、別のエンドポイントがオンラインになったときに、オフラインのエンドポイントの IP バインディングを再利用します。
- アカウントごとのエンドポイントの最大数は、アカウントがサポートできる認証エンドポイントの最大数を制限するために使用されます。デフォルトの数は 10 です。たとえば、「≪単一アカウントの最大デバイス **Max. Device for Single Account** を 10 に設定した場合、最大 10 のエンドポイントが、認証時にオンラインになるアカウントを使用できます。



ダイレクタコントローラ構成のパラメーター:

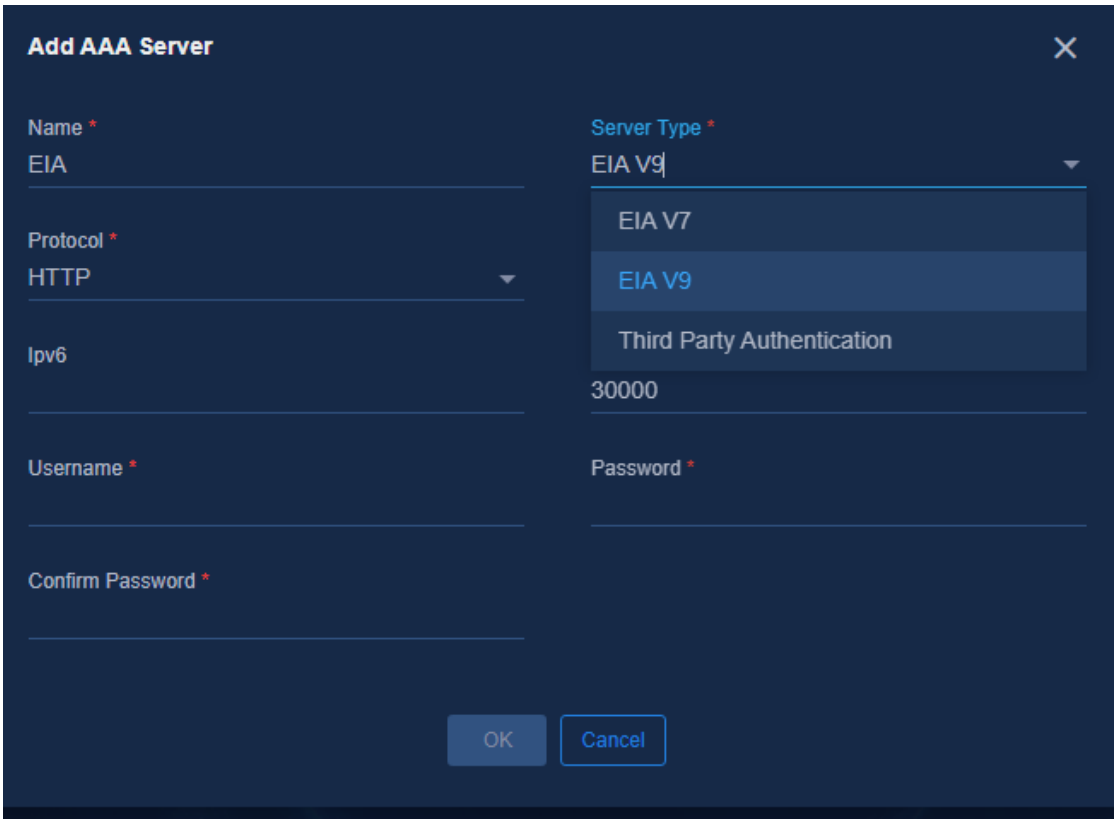
- **埋込みコントローラ**: SeerEngine キャンパスと EIA が同じプラットフォームに配置されている場合、**Yes** を選択すると、パラメーターを手動で指定する必要がないことを示します。**No** を選択すると、次のパラメーターを指定する必要があることを示します。
- **IP Address**: SeerEngine キャンパスコントローラへのログインに使用する IP アドレスを入力します。
- **Port**: 30000(Unified Platform にログインするためのポート番号)
- **Username/Password**: デフォルト設定の **admin** と **Pwd@12345** をそれぞれ入力します。
- **Protocol**: HTTP(または HTTPS)。デフォルトのプロトコルは HTTP です。Unified Platform の導入時に使用するプロトコルを選択します。

AAA

AAA サーバーは、H3C EIA V7(iMC EIA)、EIA V9(コンテナ化された EIA)、およびサードパーティーの認証サーバーをサポートします。

Automation> Campus Network> Network Parameters> AAA ページに移動し、Add をクリックして EIA サーバーを追加します。

- **Name**: AAA サーバーの名前を入力します。現在の環境の既存の AAA サーバーの名前と同じにすることはできません。
- **Server Type**: サーバータイプを選択します。
  - **EIA V9**: Unified Platform に配置された EIA サーバー。
  - **EIA V7**: iMC プラットフォームにデプロイされた EIA サーバー。階層 EIA をサポートするのは EIA V7 のみです。
  - **Third-Party Authentication**: サードパーティーの AAA サーバー。
- **Protocol**: EIA サーバーへのログインに使用するプロトコルを選択します。デフォルト設定は HTTP です。
- **IPv4 Address**: EIA サーバーの IP アドレスを入力します。
- **IPv6 Address**: EIA サーバーの IPv6 アドレスを入力します。このパラメーターはオプションです。
- **GUI Port**: 選択したサーバータイプに基づいて、システムによって自動的に設定されます。
- **User Name**: EIA サーバーへのログインに使用するユーザー名を入力します。
- **Password**: EIA サーバーへのログインに使用するパスワードを入力します。



EIA V9

EIA コンポーネントが Unified Platform クラスタ環境で設定されると、EIA V9 のコンテナ化された配置によって、EIA コンポーネントが **Default EIA** として AAA リストに自動的に追加されます。

EIA V7

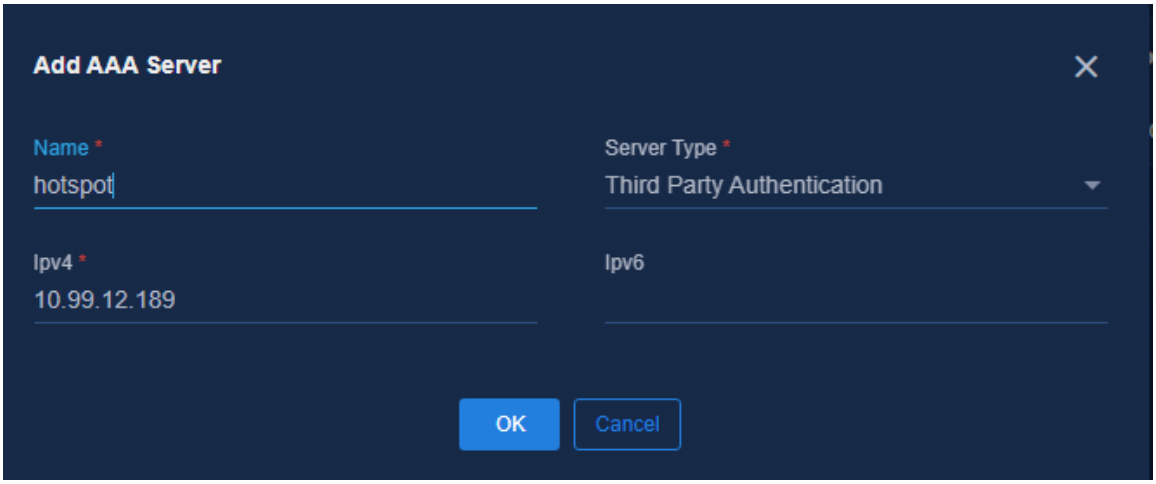
EIA V7 サーバーは、Windows または Linux オペレーティングシステム(iMC プラットフォーム)に展開され、シングルホストモード、クラスタモード、および階層展開モードをサポートします。

- **シングルホストモード**: Windows または Linux オペレーティングシステムをサポートする物理サーバーまたは VM が必要です。
- **クラスタモード**: Windows または Linux オペレーティングシステムを使用する 2 台の物理サーバーが必要です。2 台のサーバーがクラスタを形成します。
- **階層型配置モード**: 1 つの上位 EIA ノードと複数の下位 EIA ノードが必要です。最大 20 のノードがサポートされます。ユーザーおよびポリシーを含む認証設定は、上位 EIA ノードで構成されます。下位 EIA ノードは、上位ノードからの設定を同期します。このモードは、マルチキャンパスのシナリオに適しています。これらの EIA ノードは、サービスの可用性を向上させるために相互のバックアップとして機能します。EIA V7 のみが階層型 EIA 配置をサポートしています。EIA V9 は階層型 EIA 配置をサポートしていません。現在のソフトウェアバージョンでは、Windows+MySQL または Linux+MySQL アーキテクチャのみがサポートされています。Windows+SQLServer はサポートされていません。MySQL データベースバージョン 5.5 から 5.8 がサポートされています。ベストプラクティ

スとして、バージョン 5.7 を使用してください。

サードパーティー認証

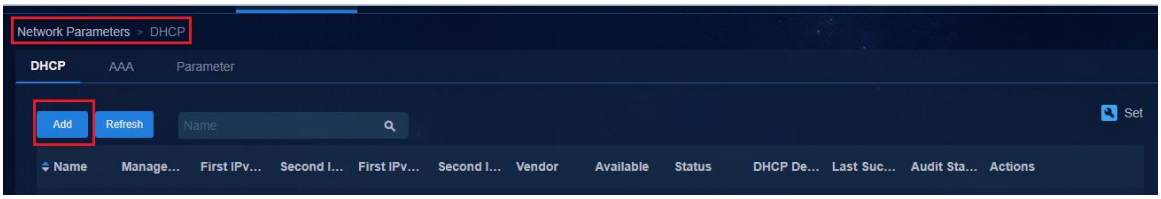
Web Portal 認証には、サードパーティー認証サーバーが使用されます。SeerEngine キャンパスコントローラ上でサードパーティーサーバーの IP アドレスを設定し、相互に到達できることを確認するだけです。



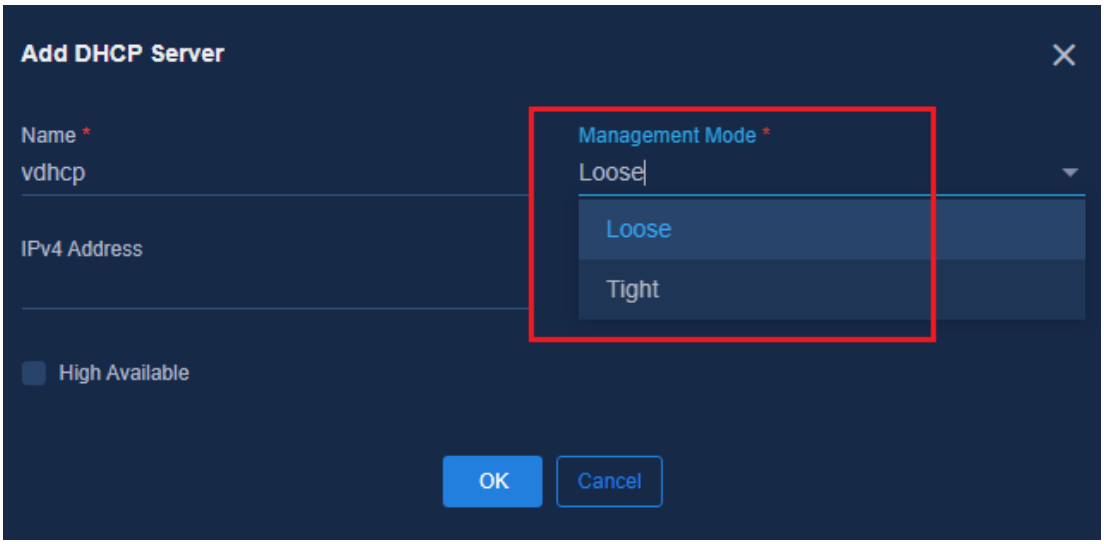
DHCP サーバー

Automation> Campus Network> Network Parameters> DHCP ページに移動します。

Add をクリックして、**Add DHCP Server** ページを開きます。



Add DHCP Server ページでは, 2 つの管理モードが利用可能: tight coupling と loose coupling を使用できます。



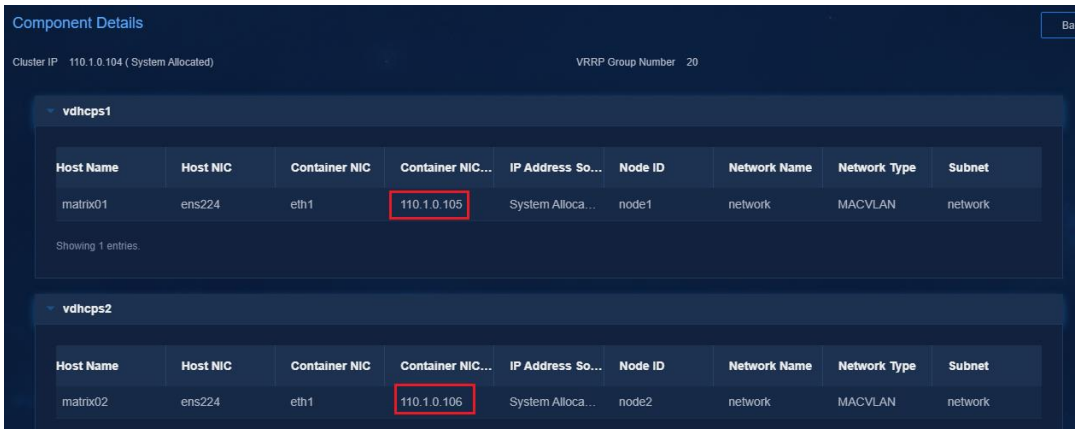
Tight coupling

注:

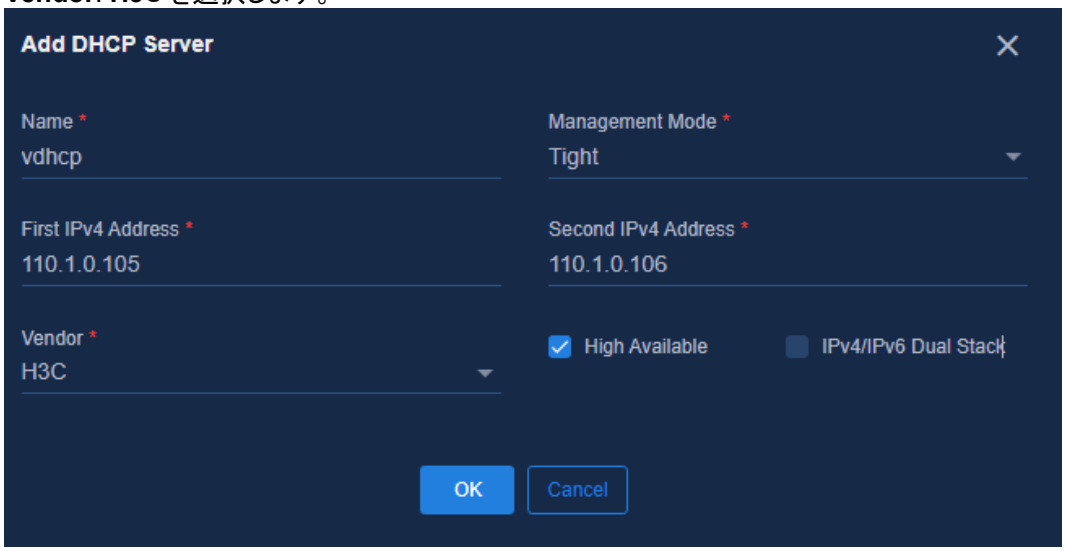
- H3C が独自に開発した vDHCP サーバーと Microsoft DHCP サーバーは、密結合をサポートしています。
- 密結合モードでは、SeerEngine キャンパスコントローラは、ページで設定された IP アドレスセグメントに従って、DHCP サーバーとの IP アドレスプールの作成を要求します。IP アドレスバインディングはサポートされています。
- 自動デバイス展開用の DHCP サーバーは、H3C vDHCP サーバーである必要があります。

vDHCP サーバー

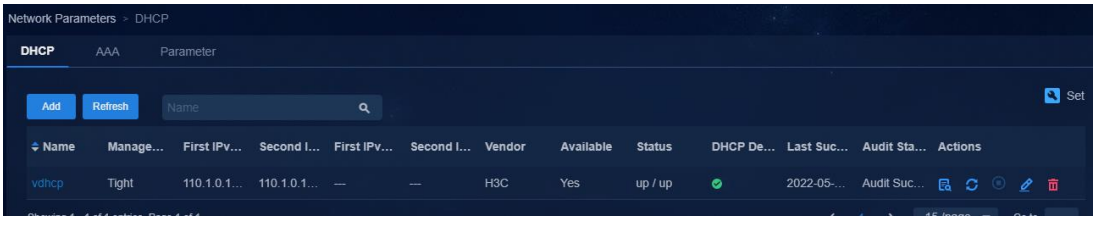
1. **Add DHCP Server** ページで、次のパラメーターを指定し、**OK** をクリックして設定を完了します。
   - **Management Mode**: vDHCP サーバーはこのモードのみをサポートしているため、**Tight** を選択します。
   - **High Available**: クラスタ環境では選択する必要がありますが、スタンドアロン環境では不要です。
   - **IPv4/IPv6 デュアルスタック**: IPv6 オートメーションサービスまたはユーザーIPv6 サービスに対してデュアルスタックデバイスを有効にします。設定については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。
   - **IP Address**: vDHCP でのデプロイ時に割り当てられた IP アドレスを入力します。vDHCP のデプロイページで IP アドレスを表示できます。**System > Deployment Management** にナビゲートし、**Public Service** オプションを展開し、をクリックして詳細を表示します。



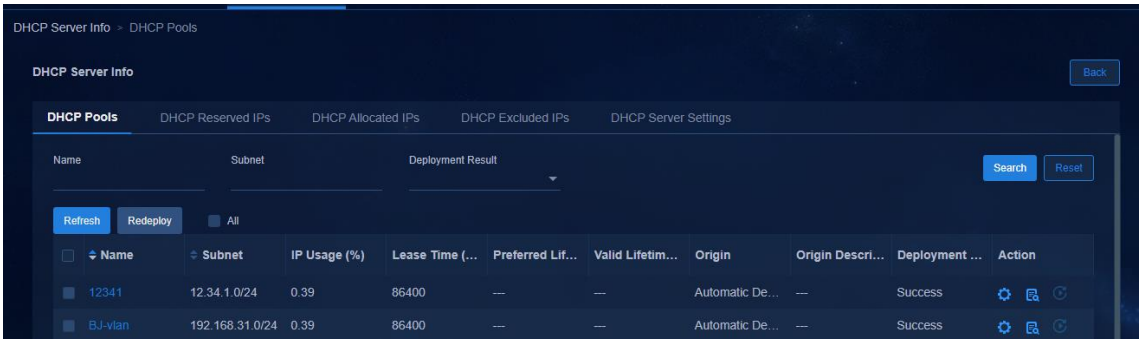
- **Vendor**: **H3C** を選択します。



2. DHCP サーバーを追加した後、DHCP サーバーの **Actions** 列 をクリックして、DHCP サーバーを同期化します。同期が完了すると、Audit Status 列に **Audit Successful** と表示されます。



3. DHCP サーバーのアドレスプールおよび IP アドレス割り当て情報を表示するには、DHCP サーバーの名前をクリックします。

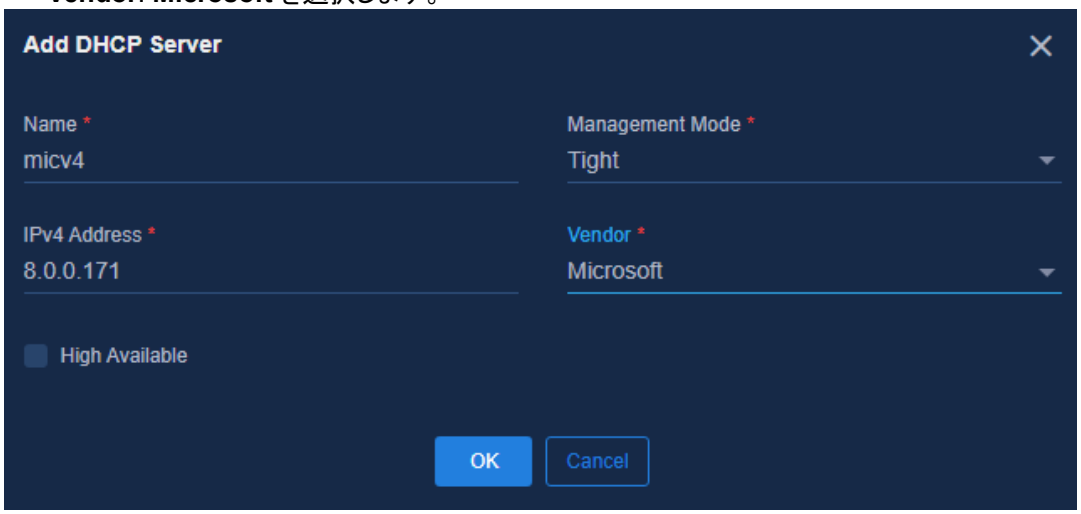


Microsoft DHCP サーバーを追加する

1. DHCP サーバーを追加する

   a. **Add DHCP Server** ページで、**ベンダー**に Microsoft を選択し、次のパラメーターを構成して、OK をクリックします。

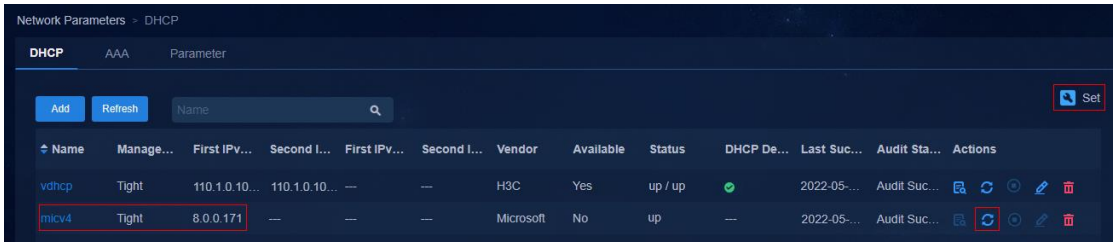
   - **Management Mode**: Tight を選択します。
   - **High Availability**: DHCP HA モードでこのオプションを選択します。スタンドアロンモードでは、このオプションを選択する必要はありません。
   - **IPv4**: Microsoft DHCP サーバーの IP アドレスを入力します。クラスタモードでは、両方の DHCP サーバーの IP アドレスを入力します。
   - **Vendor**: **Microsoft** を選択します。



   b. DHCP サーバーを追加した後、DHCP サーバーの **Actions** 列 をクリックして、DHCP サーバーを同期化します。同期が完了すると、**Audit Status** 列に **Audit Successful** と表示されます。

   c. Microsoft DHCP HA ステータスを監視するには、DHCP リストページの右上隅にある Set をクリックします。デフォルトでは、HA モニタはイネーブルです。SeerEngine キャンパスコントローラは、DHCP HA ステータスを定期的に監視します。コントローラは、プライマリ Microsoft DHCP サー

バーの障害を検出すると、バックアップ Microsoft DHCP サーバーを自動的にイネーブルにします。

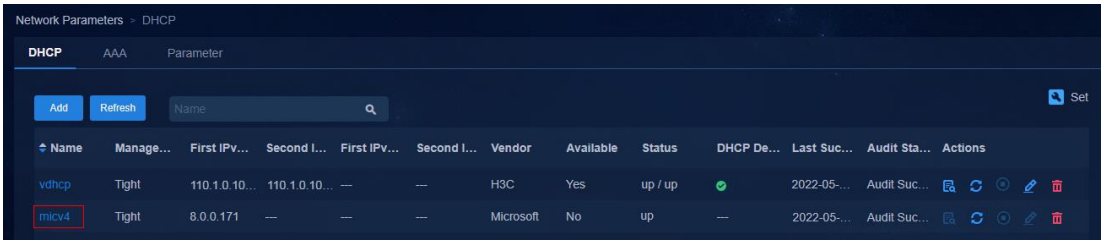


2. VXLAN 4094 アドレスプールを設定します。

重要:

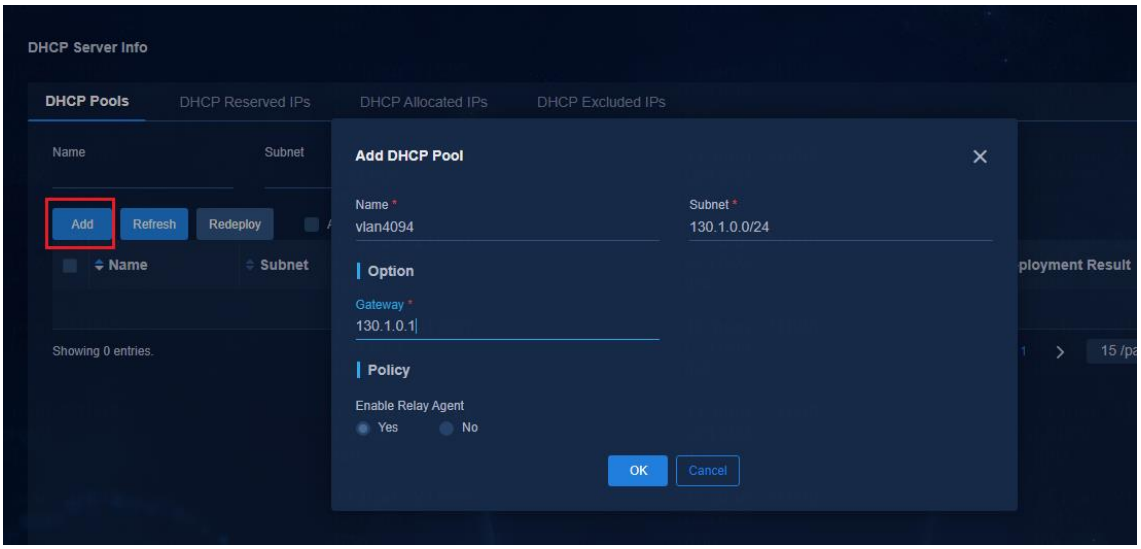
Microsoft DHCP サーバーを追加した後、SeerEngine キャンパスコントローラ上にアドレスプールを手動で作成し、アドレスプールがデバイス上の VXLAN 4094 と同じネットワーク上にあることを確認する必要があります。アドレスプールを作成しない場合、Microsoft DHCP サーバーはリーフデバイスから送信された DHCP 要求に応答できません。

DHCP タブで、Microsoft DHCP サーバーの名前をクリックします。

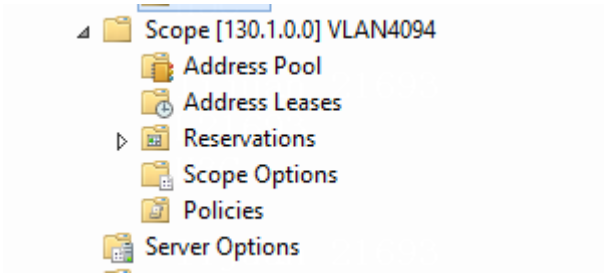


DHCP Pools タブで、**Add** をクリックしてアドレスプールを追加します。

- **Subnet**: アドレスプールがデバイス上の VXLAN 4094 と同じネットワーク上にあることを確認します。このアドレスプールはユーザーサービスには使用されません。
- **Gateway**: VXLAN 4094 と同じネットワークセグメントの IP アドレスを入力します。
- その他のパラメーターには、デフォルト値を使用します。



Microsoft DHCP サーバーが正常に作成および展開されると、作成されたスコープが Microsoft DHCP サーバーに表示されます。



Loose coupling

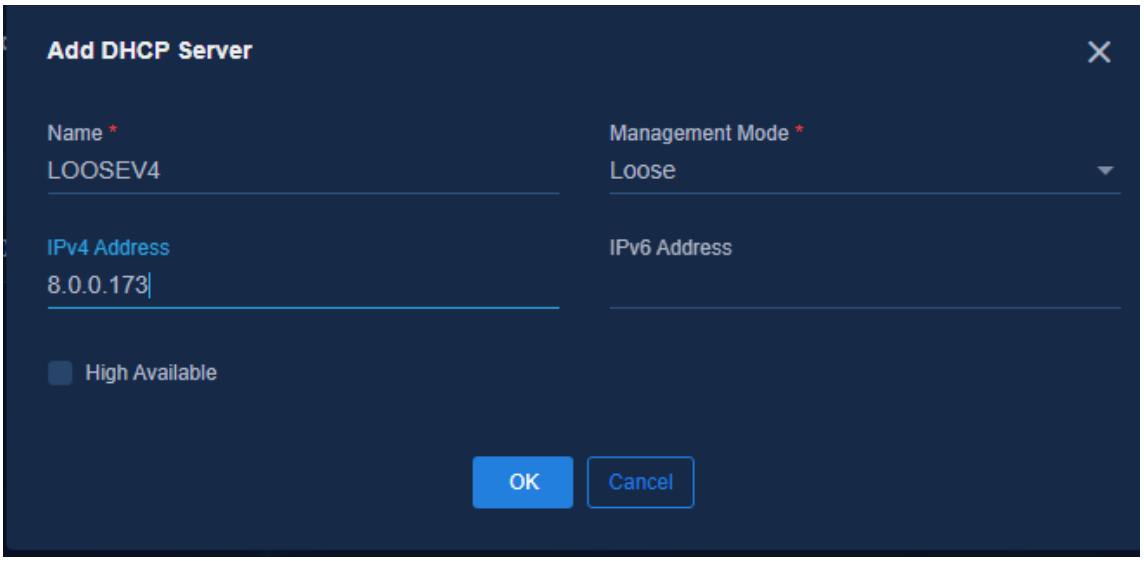
注:

- Microsoft DHCP サーバーおよび WRD DHCP サーバー(Option 82 をサポート)は、疎結合をサポートします。
- 疎結合モードでは、SeerEngine キャンパスコントローラは DHCP サーバーにアドレスプールを作成せず、DHCP サーバーからのアドレスプール情報を同期化しません。
- リーフデバイスによって送信される DHCP リレーパケットで伝送される Option 82 情報を照合するために、すべてのアドレスプールとアドレスプールのポリシーを手動で作成する必要があります。

疎結合モードの DHCP サーバーは同期できません。DHCP サーバーに使用できる ボタンがなく、**Audit Status** は「--」です。

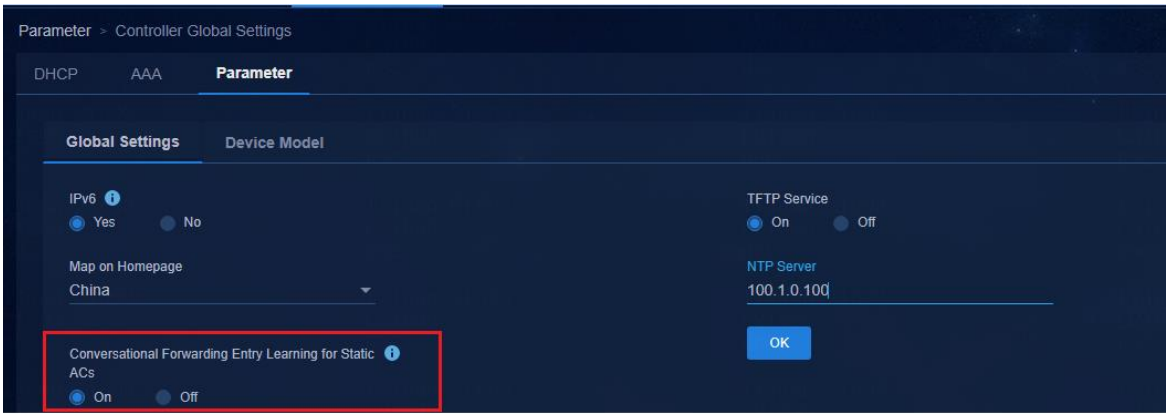
疎結合モードでは、SeerEngine キャンパスコントローラは DHCP サーバーに設定を発行したり、DHCP サーバーのアドレスプール情報を同期したりしません。したがって、fail-permit セキュリティグループ内のサブネットのアドレスプールと、DHCP サーバー上のアドレスプールポリシーを手動で作成する必要があります。

アドレスプールポリシーを構成するには、サードパーティーの DHCP サーバーが VXLAN ID を Option 82 値に設定し、DHCP パケットで Option 82 を識別する必要があります。構成方法は DHCP サーバーによって異なります。詳細については、各 DHCP サーバーベンダーの構成情報を参照してください。



スタティック AC のための会話型転送エントリー学習

S6520X シリーズまたは S5560X シリーズのデバイスがネットワークに存在する場合は、ベストプラクティスとして、**Automation**> **Campus Network**> **Network Parameters**> **Parameters** ページに移動して、スタティック AC のカンバセーション転送エントリーラーニングをイネーブルにします。



機能を有効にした後、サービスインスタンスがサービストラフィックを受信した場合に限り、デバイスはサービスインスタンスの転送エントリー情報をドライバに発行して、設定を有効にします。リーフデバイス上の静的サービスインスタンスに次の設定を展開します。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 link-aggregation mode dynamic
```

```
 stp tc-restriction
 mac-based ac
dot1x
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x critical vsi vsi9
 dot1x critical eapol
 mac-authentication
 mac-authentication hz1
 port-security free-vlan 1 3501 to 3505 4094
 #
 service-instance 3501
  encapsulation s-vid 3501
  xconnect vsi vsi3 on-demand
  arp detection trust
#
```

デバイスのオンボード

従来の自動デバイスオンボーディング

レガシー自動デバイスオンボーディングは、自動化を実装するコントローラおよびデバイスのプロセスです。設定の詳細については、『AD-Campus 6.2 Automation Configuration Guide』を参照してください。

最適化された自動デバイスオンボーディング

最適化された自動デバイスオンボーディングにより、コントローラはデバイスのサポートなしで自動化を実装できます。設定の詳細については、『AD-Campus 6.2 Optimized Automation Configuration Guide』を参照してください。

半自動オンボーディング

半自動オンボーディングは、スパインデバイスとリーフデバイスを手動で組み込むことです。自動アクセスデバイスのオンボーディングと、スパインデバイスとリーフデバイスを手動で組み込むシナリオについては、「Manually incorporating a device」を参照してください。自動アクセスデバイスのオンボーディングおよびその他の半自動設定については、『AD-Campus 6.2 Semi-Automation Configuration Guide』を参照してください。

デバイスを手動で組み込む

この項では、自動展開されないスパインデバイス、リーフデバイスおよびアクセスデバイスを手動で構成するための基本的な構成手順について説明します。次の構成は、デバイスロール別のアンダーレイ構成と、デバイスを組み込むためにコントローラが必要とする構成のみに基づいています。構成後、SeerEngine キャンパスコントローラはデバイスを組み込むことができます。

重要:

- このドキュメントでは、アンダーレイの手動設定について説明しています。アンダーレイの自動化設定については、『AD-Campus 6.2 Automation Configuration Guide』を参照してください。
- L3 スイッチまたは VLAN 4094 セグメントのないゲートウェイがスパインデバイス上にある場合、リーフデバイス上のコントローラネットワークセグメントへのスタティックルートを設定する必要はありません。

レイヤー3 スイッチを設定する

レイヤー3 スイッチを設定するには:

1. DHCP と STP をグローバルにイネーブルにします。

DHCPを有効にする.
dhcp enable
#
STPを有効にします。
stp global enable
#
VLAN 4094 インターフェイスを構成する.
#
Vlan 4094
#
#
interface Vlan-interface4094
ip address 130.1.0.1 255.255.255.0
#
#VLAN 1 設定は、自動デバイスオンボードに使用されます。ネットワーク内のすべてのデバイスが手動でオンボードされている場合、VLAN 1 設定は必要ありません。
interface Vlan-interface1
ip address 120.1.0.1 255.255.255.0
dhcp select relay // DHCP リレー エージェント関連の構成は、自動デバイス オンボーディングに使用されます。 スパイン/リーフ/アクセス デバイスが手動で設定されて組み込まれている場合、DHCP リレー エージェント関連の設定は必要ありません。
dhcp relay server-address 110.1.0.105 // vDHCPサーバーノードのIPアドレス.
dhcp relay server-address 110.1.0.106
#
VLAN 30 および VLAN 1010 の VLAN インターフェイスを作成する.
#
Vlan 30
Vlan 1010
#
interface Vlan-interface 30
ip address 100.1.0.1 255.255.255.0
#
interface Vlan-interface 1010
ip address 110.1.0.1 255.255.255.0
#
スパインデバイスに接続されたインターフェイスを設定します。
#
interface Ten-GigabitEthernet1/0/6
description to_spine
port link-type trunk
port trunk permit vlan 1 4094 //スパイン/リーフ/アクセス デバイスがネットワークに手動で導入およびオンボードされている場合は、undo allowed vlan1 コマンドを実行します。
#
ユニファイド プラットフォームに接続するインターフェイスを VLAN 30 に追加します。
#
interface GigabitEthernet1/0/7
port access vlan 30
stp edged-port //サーバーを接続するレイヤー 3 スイッチ ポートを STP エッジ ポートとして指定します。
#
SeerEngine-Campus と vDHCP に接続するインターフェイスを VLAN 1010 に追加し

ます。
#
interface GigabitEthernet1/0/3
port access vlan 1010
stp edged-port //サーバーを接続するレイヤー 3 スイッチ ポートを STP エッジ ポートとして指定します。
#
デフォルトルートを追加する.
#認証ユーザーと EIA 間の相互接続のために、スパインデバイス上の VSI インターフェイス 4094 の IP アドレスにネクストホップを設定します。
ip route-static 0.0.0.0 0 130.1.0.2 //ネクストホップがスパインデバイス上の VSI インターフェイス 4094 のインターフェイスアドレスであるデフォルトルートを設定します。
#

スパインデバイスを設定する

Spine デバイスを SeerEngine キャンパスに組み込む前に、次の操作を手動で実行します。

1. スパインのロールとシステム名を設定します。
   #デフォルトで役割が spine であるデバイスの場合、spine 役割を設定する必要はありません。そうでない場合は、最初に spine 役割を設定してからデバイスを再起動して、設定を有効にします。
   vcf-fabric role spine
   #
   sysname Spine
   #
2. トポロジを決定するように LLDP を設定します。
   #
   lldp global enable
   #
3. STP を設定します。
   stp ignored vlan 2 to 4094
   stp global enable
   stp root primary //スパインデバイスを STP ルートとして指定します。
   #
4. SNMP、NETCONF、Telnet、および SSH を設定します。
   #SNMP を設定します。次に、デフォルトの設定を示します。SNMP コミュニティストリングは、実際の設定に基づいて調整できます。
   snmp-agent
   snmp-agent community write private
   snmp-agent community read public
   snmp-agent sys-info version all
   snmp-agent packet max-size 4096
   #
   #NETCONF を設定します。
   netconf soap http enable
   netconf soap https enable
   netconf ssh server enable
   restful https enable
   #
   #Telnet を設定します。
   telnet server enable //Configure Telnet when using Telnet functions

#

#SSH を設定します。

ssh server enable

#

5. Telnet および SSH のユーザー名とパスワードを設定します。

#ユーザー名を admin に、パスワードを H3C1234567 に設定します。

local-user admin class manage

password simple H3C1234567//パスワードが複雑度の要件を満たしていることを確認します。パスワードの長さは 10～63 文字で、数字、大文字、小文字および特殊文字の少なくとも 2 種類の文字が含まれている必要があります。漢字はサポートされておらず、パスワードに疑問符(?)、スペース、ユーザー名またはユーザー名の逆順を含めることはできません。

service-type telnet http https ssh

authorization-attribute user-role network-admin

authorization-attribute user-role network-operator

#

line vty 0 63

authentication-mode scheme

user-role network-admin

user-role network-operator

#

6. VLAN 4094 を作成します。

#VLAN 4094 を作成します。

VLAN 4094

#

7. OSPF を設定します。

#

ospf 1 router-id 200.1.1.254

non-stop-routing

area 0.0.0.0

#

8. ループバックインターフェイスを設定します。

#

interface LoopBack0

ip address 200.1.1.254 255,255,255,255

ospf 1 area 0.0.0.0 //OSPF を設定します。

#

9. スパインデバイスのダウンリンクインターフェイスを設定します。複数のダウンリンクインターフェイスが存在する場合は、複数の VLAN インターフェイスを作成します。

#VLAN を作成します。

VLAN 91

#

#VLAN インターフェイスを作成します。

interface Vlan-interface91

ip address 91.1.0.1 24 //未使用のネットワークアドレスを使用します。

ospf network-type p2p

ospf 1 area 0.0.0.0

#

#スパインデバイスのダウンリンクインターフェイスで port trunk permit コマンドを実行します。

#

```
interface Ten-GigabitEthernet3/0/16
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 91 // spine/leaf/access デバイスがネットワークに手動で展開され、オンボードされている場合は、undo permit vlan1 コマンドを実行します。
```

#

デフォルトでは、SeerEngine キャンパスは次の VLAN を自動的に割り当てます。

- DRNI の 2 つのデバイス間でアンダーレイのルートを同期するための VLAN 2。
- 自動スタックデバイスの BFD 用の VLAN 100。
- アクセススイッチの VLAN 101 から VLAN 2800。
- VLAN 2801 から VLAN 3000(AC へのスタティックアクセス用)
- セキュリティグループの VLAN 3501 から VLAN 4000。
- 自動オンボーディングにおけるスパインデバイスとリーフデバイス間の相互接続リンク用の VLAN 3001 から VLAN 3500。
- VLAN 4090～VLAN 4094 は予約されています。
- VLAN 1 から VLAN 99、および VLAN 4001 から VLAN 4089 は、コントローラによって自動的に割り当てられません。
- デフォルトでは、VLAN 4051～VLAN 4060 が認証フリーVLAN として使用されます。
- VLAN インターフェイスをルーティング用に設定する場合は、VLAN 3 から VLAN 99、VLAN 4001 から VLAN 4050、および VLAN 4061 から VLAN 4089 を使用することをお勧めします。

スパインデバイスとリーフデバイスの間の複数のリンクは ECMP リンクです。VLAN 1 に対して STP がイネーブルになっているため、スパインデバイスとリーフデバイスの間のリンクが破棄状態になっている場合は正常です。

10. L2VPN をイネーブルにします。

#

```
l2vpn enable
```

#

11. VPN-Target、VSI VXLAN 4094 および VSI インターフェイスの IP アドレス、およびコントローラとデバイス間のトンネル接続用の L3VNI を設定します。

#VPN-Default を作成し、RD と RT をグローバルに 1:1 に設定します。

#

```
ip vpn-instance vpn-default
route-distinguisher 1:1
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#
address-family ipv4
```

vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#
address-family evpn
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#

#VSI インターフェイス 4094 の IP アドレスを設定します。

interface Vsi-interface4094
ip binding vpn-instance vpn-default
ip address 130.1.0.2 255.255.255.0
local-proxy-arp enable
arp proxy-send enable // ARP プロキシをイネーブルにして、ネットワーク例外またはタイムアウトが原因で、エンドポイント装置がサーバーARP 情報なしではサーバーに接続できない問題を解決します。
#

#レイヤー3 転送用に VSI インターフェイスと L3VNI を設定します。

#インターフェイスが特定のインターフェイスの IP アドレスを借用できるようにするには、ip address unnumbered コマンドを使用します。VPN-Default に対してセキュリティグループが作成されると、レイヤー3 フォワーディングによって送信されるパケットの送信元 IP アドレスは、VSI インターフェイス 4094 の IP アドレスとして指定されます。

#VSI-interface 4092 を作成して、VPN-Default の L3VNI を設定します。

interface Vsi-interface4092
ip binding vpn-instance vpn-default
ip address unnumbered interface Vsi-interface4094
l3-vni 4092
#

#VSI VXLAN 4094 インスタンスを設定します。

vsi vxlan4094
gateway vsi-interface 4094
vxlan 4094
evpn encapsulation vxlan
mac-advertising disable
arp mac-learning disable
nd mac-learning disable
route-distinguisher auto
vpn-target auto export-extcommunity
vpn-target auto import-extcommunity
#

12. BGP EVPN を設定します。

#BGP を設定します。複数のリーフデバイスがある場合は、複数のピアを設定します。

#手動で設定した BGP AS 番号は、SeerEngine キャンパスのファブリックで設定された AS 番号と一致している必要があります。

#

bgp 100
non-stop-routing
router-id 200.1.1.254　//各デバイスには異なるルータ ID があります。
peer 200.1.1.252 as-number 100 //BGP ピアを設定します。BGP ピアの IP アドレスは、リーフデバイス上のループバックインターフェイスの IP アドレスです。
peer 200.1.1.252 connect-interface LoopBack0
#
address-family l2vpn evpn
reflector cluster-id 200.1.1.254　// デュアルスパイン環境でリフレクタクラスタを設定します。

2 つのデバイスが同じクラスタ ID を持ちます。
undo policy vpn-target　// undo policy vpn-target を設定し、受信した VPNv4 ルートをフィルタリングしません。
peer 200.1.1.252 enable // 複数のリーフノードが存在する場合は、複数のリーフエントリーを設定します。
peer 200.1.1.252 reflect-client　//異なる Leaf デバイス間でルートを転送するためのルートリフレクタを設定します。
#
ip vpn-instance vpn-default
#
address-family ipv4 unicast
 import-route direct　// リーフデバイスで IPv4 アドレスのオンデマンド展開が有効になっている場合は、直接ルートをインポートします。
 import-route static　//スタティックルートをインポートします。
#

13. スパインデバイスのアップリンクインターフェイス(レイヤー3 スイッチに接続)を AC インターフェイスとして設定し、VSI VXLAN 4094 にバインドします。

#
 interface Ten-GigabitEthernet3/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4094　// spine/leaf/access デバイスがネットワークに手動で展開され、オンボードされている場合は、undo permit vlan1 コマンドを実行します。
service-instance 4094　// サービスインスタンス 4094 を作成します。
encapsulation s-vid 4094　// VLAN タグ 4094 を照合します。
xconnect vsi vxlan4094　// VSI vxlan4094 をバインドします。
#

14. スタティックルートを設定します。

#スパインデバイスがレイヤー3 で SeerEngine キャンパスおよび EIA に接続されている場合、ネクストホップとしてレイヤー3 スイッチの VLAN 4094 の IP アドレスを使用して、サーバーへのスタティックルートを設定します。
ip route-static vpn-instance vpn-default 110.1.0.0 24 130.1.0.1　//宛先 IP アドレスは、コントローラのサブネット上にあります。
#
ip route-static vpn-instance vpn-default 100.1.0.0 24 130.1.0.1　// 宛先 IP アドレスは、サーバーのサブネット上にあります。
#
#DHCP サーバーの IP アドレスが別のネットワーク上にある場合は、DHCP サーバーにスタティックルートを追加する必要があります。
ip route-static vpn-instance vpn-default 132.0.0.0 24 130.1.0.1　// DHCP サーバーのネットワーク IP アドレス。
#

15. VXLAN トンネルの MAC アドレス学習および ARP/ND 学習をディセーブルにします。

#VXLAN トンネルの ARP 学習を無効にして、リモートパケットの ARP 学習を禁止します。
vxlan tunnel arp-learning disable
#
#IPv6 サービスを設定するには、ND ラーニングを無効にする必要があります。
vxlan tunnel arp-learning disable
#

#VXLAN トンネルの MAC アドレス学習を無効にして、リモートパケットの MAC アドレス学習を禁止します。
vxlan tunnel mac-learning disable
#

16. NTP を設定します。
#
clock timezone beijing add 08:00:00
#
#IP アドレスは、NTP サーバーの IP アドレスです。統合プラットフォームは、組み込みの NTP サーバーで構成されます。IP アドレスは、クラスタノースバウンドサービス IP です。
ntp-service enable
ntp-service unicast-server 100.1.0.100 vpn-instance vpn-default
#

17. スパインデバイスの IRF ファブリックのブリッジ MAC アドレスを変更されていない状態に設定します。スパインデバイスが IRF ファブリック内にある場合は、次のコマンドを使用して、マスター/バックアップスイッチオーバー中にデバイスのブリッジ MAC アドレスが変更されないようにします。
#
irf mac-address persistent always
#

リーフデバイスの構成

重要:

S5560X スイッチまたは S6520X スイッチをリーフデバイスとして使用する場合は、スイッチモードを VXLAN に設定し、設定を有効にするためにデバイスを再起動します。

リーフデバイスを SeerEngine キャンパスに組み込む前に、次の操作を手動で実行します。
#スイッチモードを表示し、VXLAN モードであることを確認します。
dis switch-mode status
Switch-mode in use: VXLAN MODE.
Switch-mode for next reboot: VXLAN MODE.
#
#スイッチモードを表示するには、次のコマンドを使用します。
switch-mode ?
0 NORMAL MODE (default)
1 VXLAN MODE
2 802.1BR MODE
3 MPLS MODE
4 MPLS-IRF MODE
#
#設定を有効にするには、モードを VXLAN モードに設定し、デバイスを再起動します。
switch-mode 1
#

1. リーフロールとシステム名を設定します。
#デバイスのロールがデフォルトで leaf の場合、leaf ロールを設定する必要はありません。そうでない場合は、まず leaf ロールを設定してからデバイスを再起動し、設定を有効にします。
vcf-fabric role leaf

```
#
#sysname を設定します。
sysname leaf1
#
```

2. トポロジを決定するように LLDP を設定します。

```
#
Lldp global enable
#
```

3. STP を設定します。

```
#
stp ignored vlan 2 to 4094
stp global enable
#
```

4. Leaf デバイスのダウンリンクインターフェイスで stp tc-restriction コマンドを実行します。

```
int Ten-GigabitEthernet1/3/0/16
#
stp tc-restriction
#
```

⚠ 警告!

リーフデバイスのダウンリンクインターフェイスで stp tc-restriction コマンドを実行します。エンドポイントデバイスに直接接続されている場合は、stp edged-port コマンドを実行します。

5. SNMP、NETCONF、Telnet、および SSH を設定します。

#SNMP を設定します。次に、デフォルトの設定を示します。SNMP コミュニティストリングは、実際の設定に基づいて調整できます。

```
snmp-agent
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent packet max-size 4096
#
#NETCONF を設定します。
#
netconf soap http enable
netconf soap https enable
netconf ssh server enable
restful https enable
#
#Telnet を設定します。
telnet server enable
#
#SSH を設定します。
ssh server enable
#
```

6. Telnet および SSH のユーザー名とパスワードを設定します。

#ユーザー名を admin に、パスワードを H3C1234567 に設定します。
local-user admin class manage
password simple H3C1234567　// パスワードが複雑度の要件を満たしていることを確認します。パスワードの長さは 10～63 文字で、数字、大文字、小文字および特殊文字の少なくとも 2 種類の文字が含まれている必要があります。漢字はサポートされておらず、パスワードに疑問符(?)、スペース、ユーザー名またはユーザー名の逆順を含めることはできません。
 service-type telnet http https ssh
 authorization-attribute user: role network-admin
 authorization-attribute user-role network-operator
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
#

7. VLAN 4094 を作成します。
#VLAN 4094 を作成します。
VLAN 4094
#

8. OSPF を設定します。
#
ospf 1 router-id 200.1.1.252
non-stop routing
area 0.0.0.0
#

9. ループバックインターフェイスを設定します。
#
Interface LoopBack0
ip address 200.1.1.252 255.255.255.255　// スパインデバイスで BGP ピアを確立します。
ospf 1 area 0.0.0.0
#

10. スパインデバイスと相互接続するための L3 VLAN インターフェイスを設定します。
#VLAN を作成します。
vlan 91　//VLAN がスパインデバイス上の VLAN と同じであることを確認します。
#
#VLAN インターフェイスを作成します。
 interface Vlan-interface91
 ip address 91.1.0.2 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
#リーフデバイスのアップリンクインターフェイスで、port trunk permit vlan コマンドを実行します。
#
 interface Ten-GigabitEthernet1/2/0/13
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 91

#

デフォルトでは、SeerEngine キャンパスは次の VLAN を自動的に割り当てます。

- DRNI の 2 つのデバイス間でアンダーレイのルートを同期するための VLAN 2。
- 自動スタックデバイスの BFD 用の VLAN 100。
- アクセススイッチの VLAN 101 から VLAN 2800。
- AC へのスタティック接続の場合は VLAN 2801 から VLAN 3000。
- セキュリティグループ用の VLAN 3501 から VLAN 4000、自動オンボーディングでのスパインデバイスとリーフデバイス間の相互接続リンク用の VLAN 3001 から VLAN 3500。
- VLAN 4090～VLAN 4094 は予約されています。
- VLAN 3 から VLAN 99、および VLAN 4001 から VLAN 4089 は、コントローラによって自動的に割り当てられません。
- デフォルトでは、VLAN 4051～VLAN 4060 が認証フリーVLAN として使用されます。
- VLAN インターフェイスをルーティング用に設定する場合は、VLAN 3 から VLAN 99、VLAN 4001 から VLAN 4050、および VLAN 4061 から VLAN 4089 を使用することをお勧めします。

スパインデバイスとリーフデバイスの間の複数のリンクは ECMP リンクです。VLAN 1 に対して STP が有効になっているため、スパインデバイスとリーフデバイスの間のリンクが破棄状態になっている場合は正常です。

11. L2VPN をイネーブルにします。
#L2VPN を有効にします。
l2vpn enable
#

12. VPN-Default、VSI VXLAN 4094 および VSI インターフェイスの IP アドレス、および L3VNI を設定し、コントローラとデバイス間のトンネル接続用のダウンリンク AC インターフェイス(アクセスデバイスへの接続)にサービスインスタンス(バインディング VXLAN 4094)を設定します。
#VPN-Default を作成し、RD と RT をグローバルに 1:1 に手動で設定します。

```
#
ip vpn-instance vpn-default
route-distinguisher 1:1
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#
address-family ipv4
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#
address-family evpn
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
#
#VSI インターフェイス 4094 の IP アドレスを設定します。
#
```

```
interface Vsi-interface4094
ip binding vpn-instance vpn-default
ip address 130.1.0.3 255.255.255.0
local-proxy-arp enable
arp proxy-send enable   // ARP プロキシをイネーブルにして、ネットワーク例外またはタイムアウトのために、サーバー上の ARP 情報がないとエンドポイントデバイスがサーバーに接続できないという問題を解決します。
#
#レイヤー3 転送用に VSI インターフェイスと L3VNI を設定します。
#インターフェイスが特定のインターフェイスの IP アドレスを借用できるようにするには、ip address unnumbered コマンドを使用します。VPN-Default に対してセキュリティグループが作成されると、レイヤー3 フォワーディングによって送信されるパケットの送信元 IP アドレスは、VSI インターフェイス 4094 の IP アドレスとして指定されます。
#
interface Vsi-interface4092
ip binding vpn-instance vpn-default
ip address unnumbered interface Vsi-interface4094
l3-vni 4092
#
#VSI VXLAN 4094 インスタンスを設定します。
#
vsi vxlan4094
gateway vsi-interface 4094
vxlan 4094
evpn encapsulation vxlan
  mac-advertising disable
  arp mac-learning disable
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
dhcp snooping trust tunnel
#
#アクセスデバイスに接続しているリーフデバイスのダウンリンクインターフェイスを AC インターフェイスとして設定します。
interface Ten-GigabitEthernet1/2/0/9
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 4094
stp tc-restriction
#
service-instance 4094
encapsulation s-vid 4094
xconnect vsi vxlan4094
#
```

13. BGP EVPN を設定します。

```
#BGP 100 を設定し、スパインデバイスを BGP ピアとして指定します。
bgp 100
  non-stop-routing
  router-id 200.1.1.252   //  各デバイスには異なるルータ ID があります。ベストプラクティスとして、ID をループバックインターフェイスの IP アドレスとして設定します。
  Peer 200.1.1.254 as-number 100
  peer 200.1.1.254 connect-interface LoopBack0
#
  address-family l2vpn evpn
```

```
  peer 200.1.1.254 enable
 #
 ip vpn-instance vpn-default
 #
  address-family ipv4 unicast
 #
```

14. スタティックルートを設定します。

#スパインデバイスとサーバーがレイヤー3 で接続されている場合、ネクストホップとしてレイヤー3 スイッチの VLAN 4094 の IP アドレスを使用して、サーバーへのスタティックルートを設定します。

ip route-static vpn-instance vpn-default 110.1.0.0 24 130.1.0.1　// 宛先 IP アドレスは、コントローラのサブネット上にあります。

#

ip route-static vpn-instance vpn-default 100.1.0.0 24 130.1.0.1　// 宛先 IP アドレスは、サーバーのサブネット上にあります。

#

#DHCP サーバーが別のネットワーク上にある場合は、DHCP サーバーにスタティックルートを追加する必要があります。

ip route-static vpn-instance vpn-default 132.0.0.0 24 130.1.0.1　// DHCP サーバーのネットワーク IP アドレス。

#

15. DHCP スヌーピングを設定します。

#

dhcp snooping enable vlan 2 to 4094

#

16. VLAN 1 および VLAN 4094 に対して、IP ソースガードをフィルタフリーとして設定します。

#この設定は、リーフダウンリンクインターフェイスに IP ソースガードが設定されている場合に必要です。IP ソースガードが設定されていない場合、サービスは影響を受けません。

ip verify source exclude vlan 1

ip verify source exclude vlan 4094

#

17. VXLAN トンネルの MAC アドレス学習および ARP 学習をディセーブルにします。

#VXLAN トンネルの ARP 学習を無効にします。

vxlan tunnel arp-learning disable

#

#VXLAN トンネルの MAC アドレス学習を無効にします。

vxlan tunnel mac-learning disable

#

18. 会話型学習を使用可能にします。(この機能はオプションで、デフォルトでは使用不可になっています。必要に応じて使用可能にできます。)

リーフデバイスで会話型学習がイネーブルになっている場合は、スパインデバイスで BGP vpn-default の直接ルートをインポートする必要があります。この操作により、エンドポイントのすべてのプライベートサブネットルートがリーフデバイスおよびスパインデバイスにインポートされ、エンドポイントとサーバーおよび外部ネットワーク間の相互運用性が確保されます。

#ハードウェアリソースを節約するために、EVPN を介して同期されたリモート ARP エントリーは、デフォルトではハードウェアに配信されませんが、トラフィック要求の場合には配信されます。

ip forwarding-conversational-learning　// 会話型学習を有効にします。

#トラフィックが停止した後、ハードウェアテーブルエントリーを削除するためのデフォルトのエージングタイムは 60 分です。次のコマンドを使用してエージングタイムを設定できます。

[leaf1] ip forwarding-conversational-learning aging ?

INTEGER<60-1440> Aging time in (minutes)

#

重要:

- S5560X-HI および S6520X-HI のオンデマンド展開機能を設定することをお勧めします。
- リーフデバイスが同時にボーダーデバイスとして動作する場合は、オンデマンド展開機能を設定しないことをお勧めします。

19. NTP を設定します。

#

clock timezone beijing add 08:00:00

#

#NTP サーバーの IP アドレスを指定します。

ntp-service enable

ntp-service unicast-server 100.1.0.100 vpn-instance vpn-default

#

20. 設定を確認します。

上記の設定タスクを完了したら、これらのタスクが正常に設定されているかどうかを確認します。次の情報は、スパインデバイスとリーフデバイスの両方から表示できます。

[leaf1] display interface Vsi-interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface Link Protocol Primary IP Description
Vsi4092 UP UP 130.1.0.3 //VSI-interfaces 4094 and 4092 are created successfully.
Vsi4094 UP UP 130.1.0.3
[leaf1]
[leaf1]dis l2vpn vsi
Total number of VSIs: 2, 1 up, 1 down, 0 admin down
VSI Name VSI Index MTU State
Auto_L3VNI4092_4092 0 1500 Down //Automatically generated.
vxlan4094 1 1500 Up
[leaf1]
[leaf1] display interface Tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface Link Protocol Primary IP Description
Tun1 UP UP -- //Tunnel is up.
[leaf1]
[leaf1] display interface Tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface

Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 200.1.1.252, destination 200.1.1.254
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 29 packets, 2064 bytes, 0 drops
Output: 8 packets, 720 bytes, 0 drops
[leaf1]
[leaf1]ping -vpn-instance vpn-default 100.1.0.100 //Ping the server.
Ping 100.1.0.100 (100.1.0.100): 56 data bytes, press CTRL+C to break
56 bytes from 100.1.0.100: icmp_seq=0 ttl=63 time=3.646 ms
56 bytes from 100.1.0.100: icmp_seq=1 ttl=63 time=1.699 ms
56 bytes from 100.1.0.100: icmp_seq=2 ttl=63 time=2.058 ms
56 bytes from 100.1.0.100: icmp_seq=3 ttl=63 time=7.078 ms
56 bytes from 100.1.0.100: icmp_seq=4 ttl=63 time=1.680 ms
--- Ping statistics for 100.1.0.100 in VPN instance vpn-default ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.483/1.620/1.991/0.189 ms
[leaf1]

21. リーフ IRF ファブリックのブリッジ MAC アドレスを変更されていない状態に設定します。

リーフデバイスが IRF ファブリック内にある場合は、次のコマンドを使用して、マスター/下位スイッチオーバー中にデバイスのブリッジ MAC アドレスが変更されないようにします。

#
irf mac-address persistent always
#

アクセスデバイスの設定

1. デバイスのアクセスロールとシステム名を設定します。

#デフォルトの役割は access です。デフォルト以外の役割を有効にするには、再起動が必要です。

#
vcf-fabric role access
#
#
sysname access1
#

2. トポロジを決定するように LLDP を設定します。

#
lldp global enable
#

3. STP を設定します。

#
stp global enable
#

4. SNMP、NETCONF、Telnet、および SSH を設定します。

#SNMP を設定します。次に、デフォルトの設定を示します。SNMP コミュニティストリングは、実際の設定に基づいて

調整できます。

#

snmp-agent

snmp-agent community write private

snmp-agent community read public

snmp-agent sys-info version all

snmp-agent packet max-size 4096

#

#NETCONF を設定します。

netconf soap http enable

netconf soap https enable

netconf ssh server enable

restful https enable

#

#Telnet を設定します。

telnet server enable

#

#SSH を設定します。

ssh server enable

#

5. Telnet および SSH のユーザー名とパスワードを設定します。

#ユーザー名を admin に、パスワードを H3C1234567 に設定します。

local-user admin class manage

password simple H3C1234567//パスワードが複雑度の要件を満たしていることを確認します。パスワードの長さは 10～63 文字で、数字、大文字、小文字および特殊文字の少なくとも 2 種類の文字が含まれている必要があります。漢字はサポートされておらず、パスワードに疑問符(?)、スペース、ユーザー名またはユーザー名の逆順を含めることはできません。

service-type telnet http https ssh

authorization-attribute user-role network-admin

authorization-attribute user-role network-operator

#

line vty 0 63

authentication-mode scheme　// ユーザー名とパスワードを使用しない場合は、none に設定します。

user-role network-admin

user-role network-operator

#

6. アクセスデバイスをリーフデバイスに接続するアップリンクインターフェイスで、permit vlan all コマンドを実行します。

#アクセスアップリンクポートで permit vlan all コマンドを実行します。

interface Ten-GigabitEthernet1/0/52

port link-mode bridge

port link-type trunk

port trunk permit vlan all

#

7. VLAN を作成します。

#

vlan 4093 to 4094

#

8. (任意)VLAN 1 の L3 インターフェイスを設定します。

#(任意)アクセスデバイスに VLAN-interface 1 を設定しないでください。

```
interface Vlan-interface1
ip address 120.1.0.4 255.255.255.0
#
```

9. VLAN 4094 の L3 インターフェイスを設定します。これにより、SeerEngine キャンパスはアクセスデバイスを管理できます。

```
#
interface Vlan-interface4094
ip address 130.1.0.4 255.255.255.0
#
```

10. VLAN 4094 のスタティック IP アドレスを設定します。

#スパインデバイスとサーバーがレイヤー3 で接続されている場合、ネクストホップとしてレイヤー3 スイッチの VLAN 4094 の IP アドレスを使用して、サーバーへのスタティックルートを設定します。

```
ip route-static 110.1.0.0 24 130.1.0.1    // 宛先 IP アドレスは、コントローラのネットワークセグメントに存在します。
ip route-static 100.1.0.0 24 130.1.0.1    // 宛先 IP アドレスは、サーバーのネットワークセグメントにあります。
```

11. NTP サーバーを設定します。

```
#
clock timezone beijing add 08:00:00
#
#NTP サーバーの IP アドレスを指定します。
ntp-service enable
ntp-service unicast-server 100.1.0.100
#
```

12. STP エッジポートを設定します。

アクセスデバイスが SeerEngine キャンパスコントローラに組み込まれると、コントローラは、ユーザーに接続されているアクセスデバイスのポートを STP エッジポートとして自動的に設定し、各ポートに VLAN ID を自動的に割り当てます。コントローラがエッジポートの自動展開に失敗した場合は、手動で設定できます。

```
#
interface GigabitEthernet1/0/22
port access vlan 115
stp edged-port
#
```

13. アクセスデバイスの IRF ファブリックのブリッジ MAC アドレスを変更されていない状態に設定します。

アクセスデバイスが IRF ファブリック内にある場合は、次のコマンドを使用して、マスター/下位スイッチオーバー中にデバイスのブリッジ MAC アドレスが変更されないようにします。

```
#
irf mac-address persistent always
```

#

集約デバイスの構成

スパインデバイスとリーフデバイスの間に接続されたデバイスとして、集約デバイスを手動で組み込む場合、集約デバイスはデバイスロール情報を判断しないため、デバイスロールを設定する必要はありません。集約デバイスの手動設定は次のとおりです。

1. デバイスのシステム名を設定します。

   #集約デバイスを手動で組み込む場合、デバイスロール情報は判断されないため、デバイスロールを設定する必要はありません。

   #

   sysname aggr1

   #

2. トポロジを決定するように LLDP を設定します。

   #

   lldp global enable

   #

3. STP を設定します。

   #

   stp global enable

   #

4. SNMP、NETCONF、および SSH を設定します。

   #SNMP を設定します。次に、デフォルトの設定を示します。SNMP コミュニティストリングは、実際の設定に基づいて調整できます。

   #

   snmp-agent

   snmp-agent community write private

   snmp-agent community read public

   snmp-agent sys-info version all

   snmp-agent packet max-size 4096

   #

   #NETCONF を設定します。

   netconf soap http enable

   netconf soap https enable

   netconf ssh server enable

   restful https enable

   #

   #SSH を設定します。

   ssh server enable

   #

5. Telnet および SSH のユーザー名とパスワードを設定します。

   #ユーザー名を admin に、パスワードを H3C1234567 に設定します。

   local-user admin class manage

   password simple H3C1234567//パスワードが複雑度の要件を満たしていることを確認します。パスワードの長さは 10～63 文字で、数字、大文字、小文字および特殊文字の少なくとも 2 種類の文字が含まれている必要があります。漢字はサポートされておらず、パスワードに疑問符(?)、スペース、ユーザー名またはユーザー名の逆順を含めることはできません。

```
 service-type http https ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
 #
 line vty 0 63
authentication-mode scheme    // ユーザー名とパスワードを使用しない場合は、none に設定します。
 user-role network-admin
 user-role network-operator
 #
```

6. OSPF を設定します。

```
#
ospf 1
 non-stop-routing
 area 0.0.0.0
#
```

7. ループバックインターフェイスを設定します。

```
#
interface LoopBack0
ip address200.1.1.200 255.255.255.0
ospf 1 area 0.0.0.0
```

8. スパインデバイスと相互接続するための L3 VLAN インターフェイスを設定します。

```
#VLAN を作成します。
vlan 92    // スパインデバイスには、対応する VLAN 設定が必要です。VLAN 設定は、スパインデバイスの設定と一致している必要があります。
#
#VLAN インターフェイスを作成します。
interface Vlan-interface92
ip address 91.2.0.2 255.255.255.0    // スパインデバイスの IP アドレスを指定します。
ospf network-type p2p
ospf 1 area 0.0.0.0
#
#集約デバイスのアップリンクインターフェイスで、port trunk permit vlan コマンドを実行します。
#
 interface Ten-GigabitEthernet1/1/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 92
```

9. リーフデバイスと相互接続するための L3 VLAN インターフェイスを設定します。

```
#VLAN を作成します。
vlan 93    // リーフデバイスには、対応する VLAN 設定が必要です。VLAN 設定は、リーフデバイスの設定と一致している必要があります。
#VLAN インターフェイスを作成します。
interface Vlan-interface93
ip address 91.3.0.2 255.255.255.0    / /リーフデバイスの IP アドレスを指定します。
ospf network-type p2p
ospf 1 ares 0.0.0.0
#
```

#集約デバイスのアップリンクインターフェイスで、port trunk permit vlan コマンドを実行します。
#
interface Ten-GigabitEthernet1/1/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 93

10. VLAN 1 のレイヤー3 インターフェイスを設定します。コントローラは、VLAN 1 を介して集約デバイスを組み込みます。VLAN 1 がサーバーに到達できることを確認します。
#
interface Vlan-interface1
ip address 120.1.0.20 255.255.255.0
#

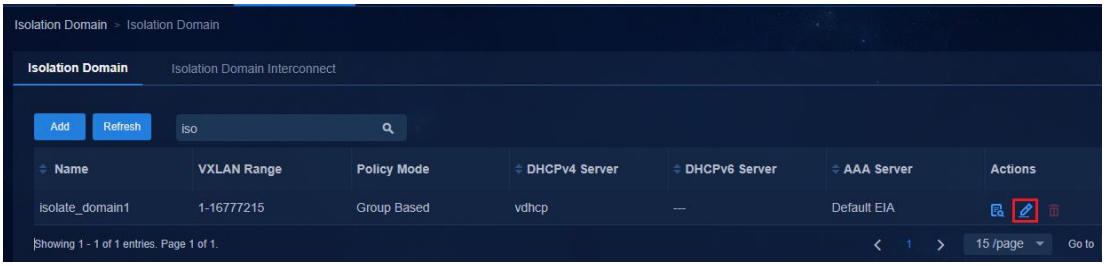
11. NTP サーバーを設定します。
#
clock timezone beijing add 08:00:00
#
#NTP サーバーの IP アドレスを指定します。
ntp-service enable
ntp-service unicast-server 100.1.0.100
#

分離ドメインの構成

Automation>Campus Network>Isolation Domain ページに移動し、Add をクリックして、隔離ドメインの設定ページを開きます。

分離ドメインの設定については、「Configure isolation domain」を参照してください。

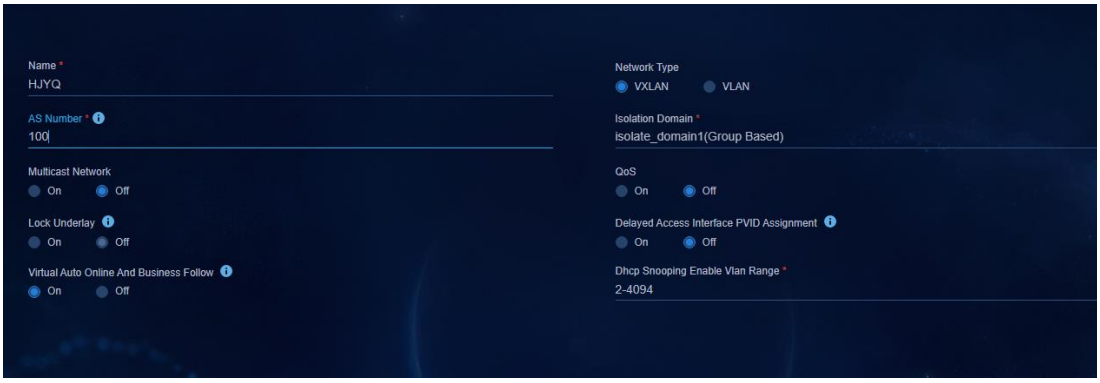
システムは、**isolate_domain1** という名前のデフォルトの分離ドメインを定義しました。分離ドメインのデフォルトのポリシーモードは IP ベースです。**Actions** 列をクリックすると、分離ドメインを編集できます。



ファブリックの構成

1. **Automation** > **Campus Network** > **Fabrics** ページに移動し、**Add** をクリックしてファブリック設定ページを開きます。

2. ファブリック設定ページで、次のようにファブリックを設定します。
   - **Name**: 名前を無制限で入力します。
   - **AS Number**: 値は 1～4294967295 の範囲の整数です。デバイスを手動で展開および管理する場合は、ファブリックに設定された AS 番号が、デバイスに手動で設定された BGP AS 番号と同じであることを確認します。
   - **Isolation Domain**: ファブリックが属する分離ドメインを選択します。
   - **Multicast Network**: デフォルトでは「≪オフ Off です。必要に応じて「≪オン On を選択できます。
   - **QoS policy**: デフォルトでは「オフ」になっています。必要に応じて「オン」を選択できます。
   - **Lock Underlay**: 既定ではオフになっており、ファブリックを追加するときに編集することはできません。自動デバイス展開中は無効にし、自動デバイス展開の完了後は必要に応じて有効にします。
   - **Delayed Access Interface PVID Assignment**: デフォルトではオフになっており、デバイスがアクティブになったときにコントローラが自動的に PVID を割り当てます。On を選択すると、デバイスがアクティブになったときにコントローラが PVID を割り当てないため、デバイスのアクティブ化後に PVID を手動で設定できます。
   - **Virtual Auto Online And Business Follow**: デフォルト設定はオンです。これは、VXLAN ネットワーキングの認可と、セキュリティグループ間のアクセスポリシーの認可を制御するために使用されます。操作する前に、設定のプロンプト情報を読んでください。



3. **OK** をクリックして、ファブリックの作成を完了します。追加されたファブリックが Fabrics ページに表示されます。デフォルトでは、各ファブリックに対して 11 の汎用デバイスグループが作成されます。

デバイスの組み込み

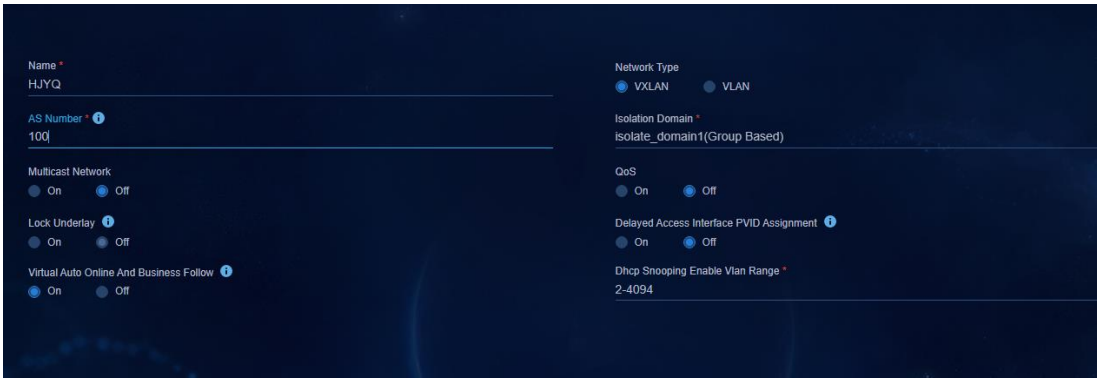
デバイスを手動で組み込むことも、デバイスの自動組み込みを有効にすることもできます。

手動による組み込み

スパインデバイスとリーフデバイスを設定するには、**Guide**> **Add Device** ページに移動し、次のパラメー

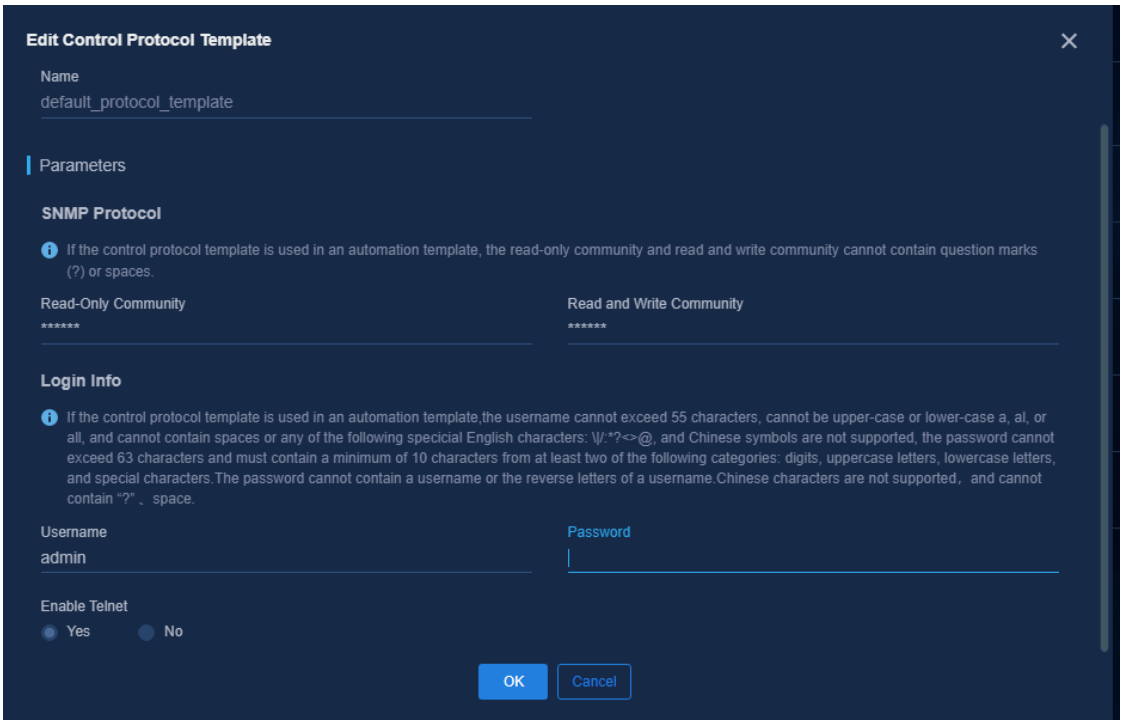
ターを設定します。

- **Host Fabric**: ファブリックはグループベースのポリシーモードを使用する必要があります。
- **Device Role**: オプションには、Spine、Leaf、Access、および Aggregation があります。選択したロールが、デバイスに設定されている実際のロールと一致していることを確認します。
- **Management IP**: VXLAN-interface 4094/VLAN-interface 4094 の IP アドレスを入力します。
- **Underlay IP**: デバイスのループバックインターフェイスの IP アドレスを入力します。
- **Device Series**: 追加したデバイスタイプを選択します。
- **Device Control Protocol Template**: テンプレートを設定するか、デフォルトのプロトコルテンプレートを選択します。

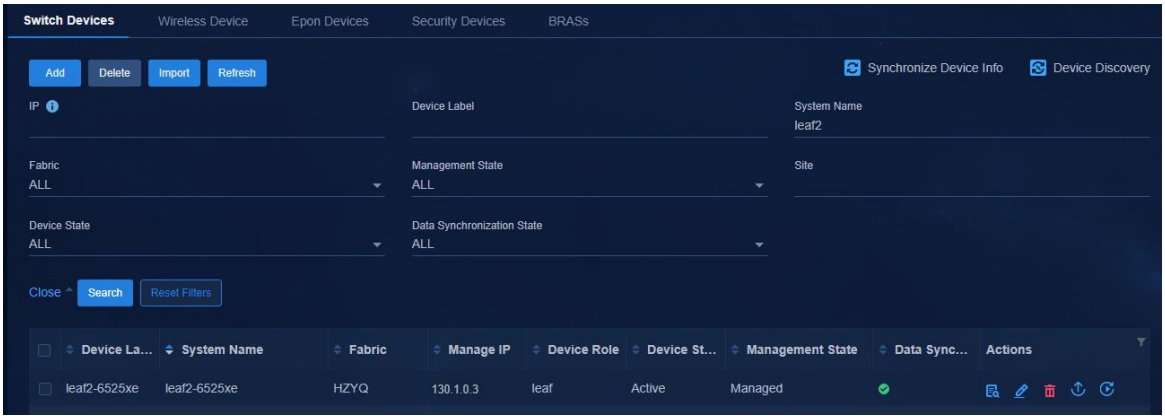


Edit Control Protocol Template をクリックして、テンプレートを編集します。

- **Control Protocol** タブで、次の手順を実行します。
  - **Read and Write Community**: アンダーレイ設定で設定された SNMP パラメーターに基づいて、SNMP 読み取りおよび書き込みコミュニティ名を設定します。
  - **Read Only Community**: アンダーレイ設定で設定された SNMP パラメーターに基づいて、SNMP 読み取り専用コミュニティ名を設定します。
  - **Username**: アンダーレイ設定で設定されているローカルユーザー名を NETCONF ユーザー名として指定します。
  - **Password**: NETCONF ユーザーのパスワードを入力します。パスワードは 10 から 63 文字の文字列で、数字、大文字、小文字および特殊文字の少なくとも 2 種類の文字を含む必要があります。パスワードには、漢字、疑問符(?)、スペース、ユーザー名またはユーザー名の逆順を含めることはできません。



デバイスが追加されると、初期状態は **Inactive** になります。データの同期が完了したら、Refresh をクリックします。デバイスの状態が **Active** に変わり、デバイスが接続されたことを示します。



spine または leaf デバイスを組み込んだ後、dis openflow instance 1 controller コマンドを実行して、SeerEngine キャンパスコントローラに接続されたデバイスに関する詳細情報を表示できます。

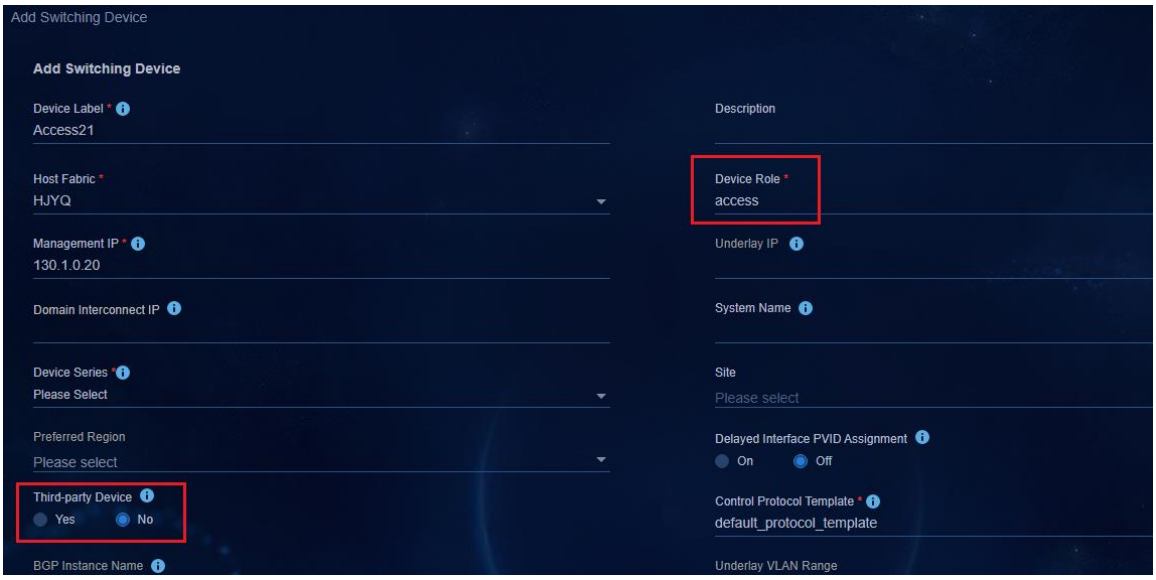
```
#
[SpineA]dis openflow instance 1 controller
Instance 1 controller information:
Reconnect interval: 60 (s)
Echo interval : 5 (s)
Controller ID : 1
Controller IP address : 110.1.0.103
Controller port : 6633
Local IP address : 130.1.0.101
Controller role : Slave
Connect type : TCP
```

```
Connect state : Established
Packets sent : 76
Packets received : 182
SSL policy : --
Control SSL policy : --
VRF name : vpn-default
Controller ID : 2
Controller IP address : 110.1.0.104
Controller port : 6633
Local IP address : 130.1.0.101
Controller role : Master
Connect type : TCP
Connect state : Established
Packets sent : 18
Packets received : 115
SSL policy : --
Control SSL policy : --
VRF name : vpn-default
[SpineA]
#
```

アクセスデバイスの組み込み:

アクセスデバイスを組み込む場合、**Third-party Device** はデフォルトで **No** に設定されています。サードパーティーデバイスまたは H3C がサポートしないロールを持つデバイスに対しては、**Yes** を選択します。

AD-Campus ソリューションでアクセスロールをサポートするデバイスモデルについては、「Hardware information」を参照してください。



重要:

アクセスデバイスは OpenFlow を介して組み込まれません。アクセスデバイス上の OpenFlow 接続情報を表示することはできません。

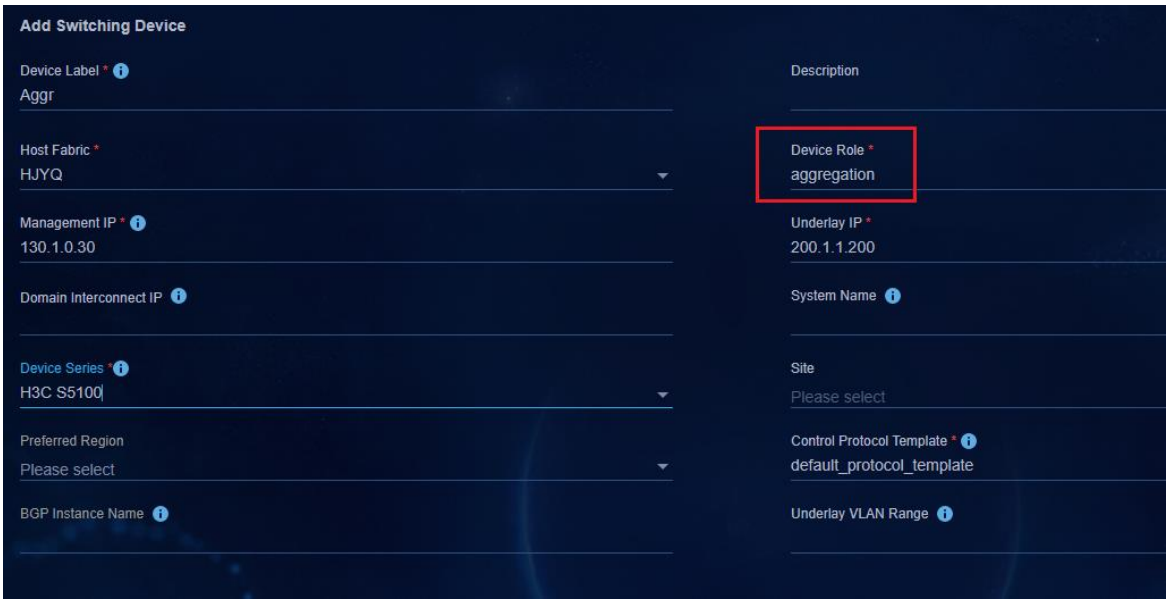
集約デバイスの組み込み:

スパインデバイスとリーフデバイスの間では、デバイスを組み込む前に、集約デバイスにコントローラを組み込むための基本設定が必要です。集約デバイスの基本設定については、「Configure aggregation devices」を参照してください。

集約デバイスを接続するリーフデバイスの基本設定は、AD-Campus ソリューションの標準ネットワーキングと同じです。設定については、「Configure leaf devices」を参照してください。

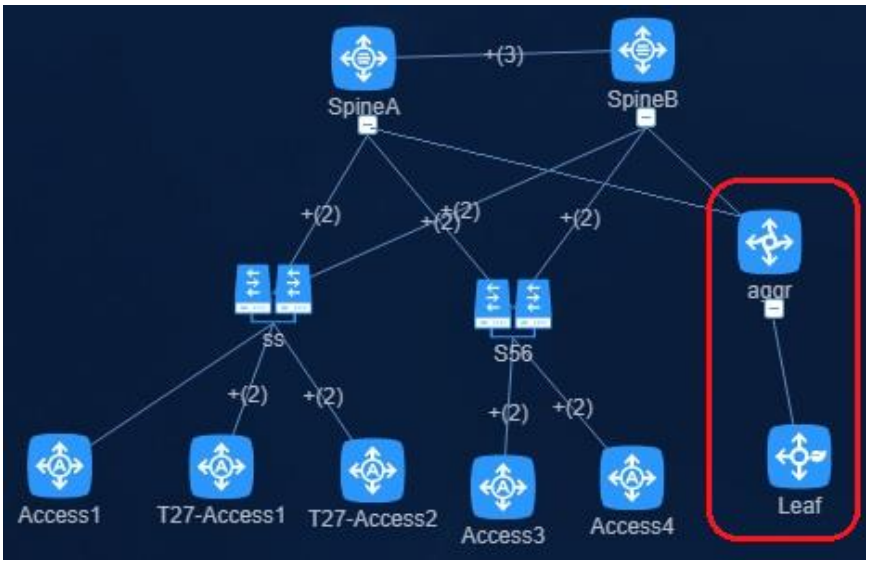
次のようにデバイス設定を構成します。

- **Device Role**: **aggregation** を選択します。集約デバイスを手動で組み込む場合、コントローラは実際のデバイスロールを確認しません。
- **Management IP**: VLAN インターフェイス 1 の IP アドレスを入力します。
- **Underlay IP**: デバイスのループバックインターフェイスの IP アドレスを入力します。
- **Device Series**: 追加したデバイスタイプを選択します。
- **Control Protocol Template**: テンプレートを設定するか、デフォルトのプロトコルテンプレートを選択します。



集約デバイスが手動で組み込まれた後、デバイスの状態は **Active** になり、デバイスの役割は **aggregation** になります。

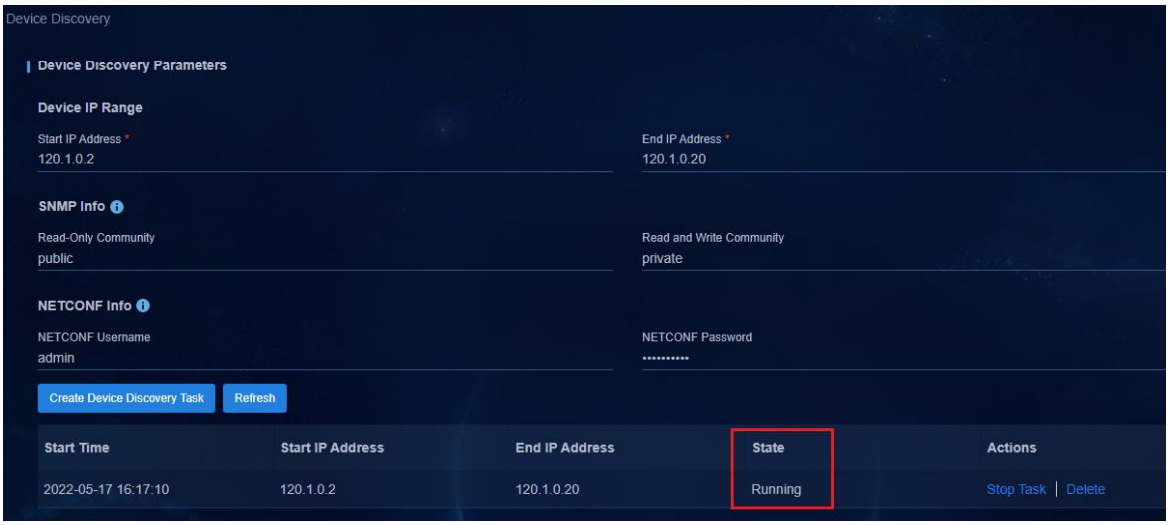
Monitor> Topology View> Network Topology ページに移動して、集約トポロジビューを表示します。



AP の自動検出

Wizard> **Device Discovery** ページに移動します。

IP アドレス範囲と SNMP パラメーターを設定し、**Create Device Discovery Task** をクリックして、組み込まれていないデバイスをスキャンします。デバイスリストで検出される、組み込まれていないデバイスは、次のとおりです。



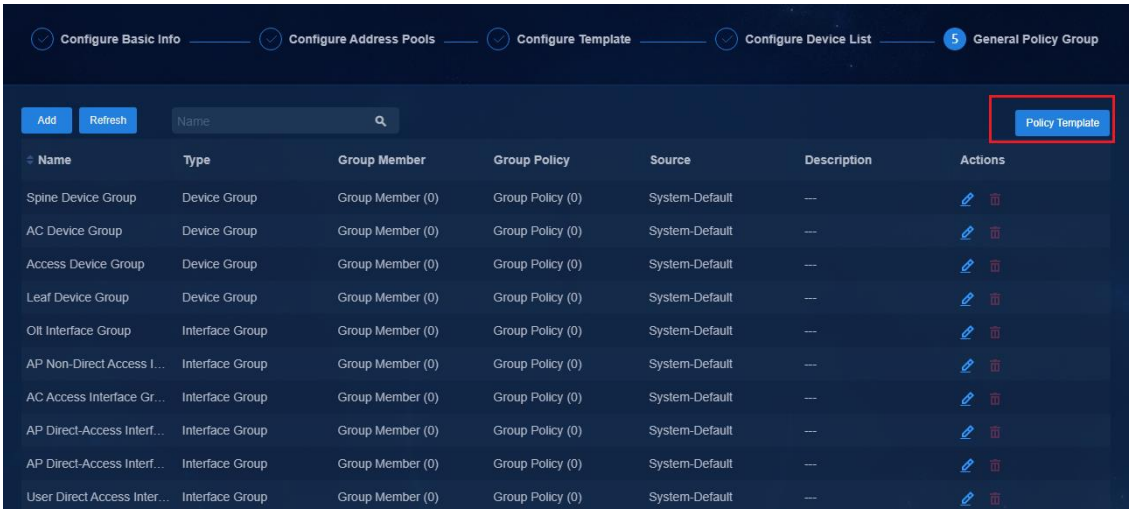
SNMP パラメーターと NETCONF パラメーターの両方を設定する場合、システムは最初に NETCONF を介してデバイスを検出します。デバイスを組み込むには、デバイスの **Actions** カラム をクリックします。パラメーターの説明については、「Manual incorporation」を参照してください。

ポリシーテンプレートを構成する

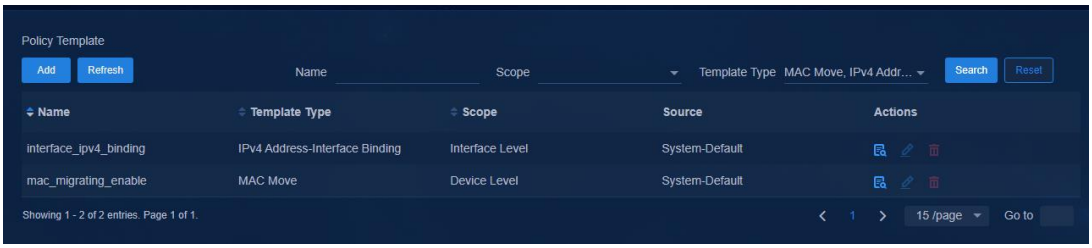
ポリシーテンプレートは、次の方法で設定できます。このマニュアルでは、例として Campus ウィザードについて説明します。

- キャンパスウィザードモード。**Wizard > Campus Wizard > Device Onboarding Planning** に移動します。手順 5 で **Policy Template** を設定します。
- 非キャンパスウィザードモード。**Automation > Campus Network > Device Groups > General Policy Group** に移動し、ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートページを開きます。

1. ページの右上隅にある **Policy Template** をクリックして、次のようにポリシーテンプレート設定ページを開きます。



2. 次のデフォルトポリシーが定義されています。
   - **interface_ipv4_binding**: 設定は、ポートセキュリティのリーフインターフェイスグループに適用されます。ip verify source ip-address mac-address コマンドは、ポリシーの設定後に発行されます。ベストプラクティスとして、現在の設定は使用しないでください。
   - **mac_migrating_enable**: 設定は、MAC 移行のリーフデバイスグループに適用されます。ユーザーは、同じリーフデバイスの同じダウンリンクポート間、または異なるダウンリンクポート間で移行されます。つまり、エンドポイントが同じアクセスデバイス上の異なるポート(異なる VLAN)間、または異なるアクセスデバイス間で移行する場合は、この設定を行う必要があります。ポリシーが設定された後、port-security mac-move permit コマンドが発行されます。現在のソリューションには、設定が必要です。

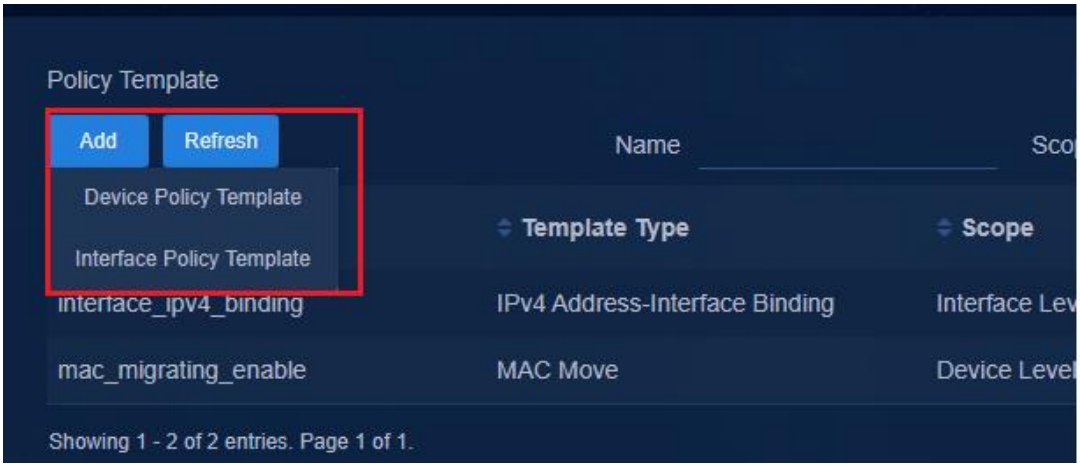


3. **Add** をクリックし、ドロップダウンリストから **Device Policy Template** または **Interface Policy Template** を選択します。

   - **Device Policy Template**: デバイスポリシーテンプレートは、AAA 認証、802.1X 認証、MAC 認証、および MAC 移行設定のリーフデバイスグループに適用できます。
   - **Interface Policy Template**: インターフェイスポリシーテンプレートは、802.1X 認証および MAC 認証設定用のリーフインターフェイスグループ(主に、リーフダウンリンクインターフェイスグループ)に適用できます。

重要:

ユーザー認証は、802.1X 認証モードと MAC/MAC ポータル認証モードをサポートしています。実際のネットワークでは、1 つの認証モードのみを構成する必要があります。必要に応じて認証モードを選択できます。両方の認証モードを構成しないことをお薦めします。



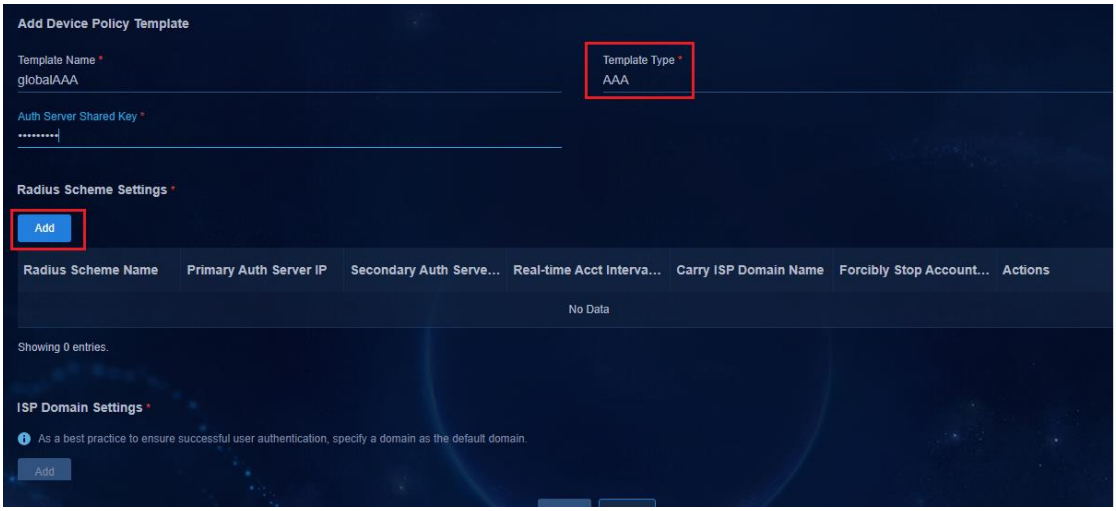
次のように、デバイスポリシーテンプレートおよびインターフェイスポリシーテンプレートを設定、カスタマイズ、および表示します。

デバイスポリシーテンプレート:AAA

1. テンプレート名、テンプレートタイプ、および認証サーバーキーを次のように設定します。

   - **Template Name**: 一意のテンプレート名を指定します。
   - **Template Type**: AAA を選択します。
   - **Auth Server Shared Key**: 必要に応じてキーを構成します。キー情報はデバイスに配布され、

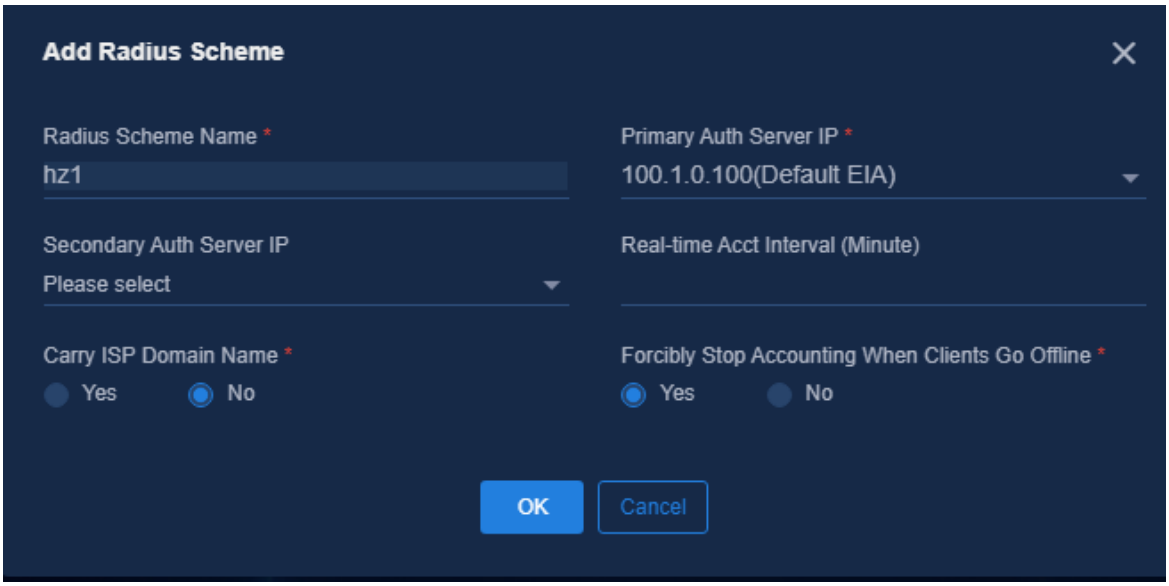
EIA に同期化されます。EIA では、この構成は必要ありません。キーは最大 64 文字をサポートし、大文字と小文字が区別されます。漢字、スペースおよび特殊文字<>&?はサポートされていません。



2. RADIUS スキームの設定:

Radius Scheme Settings 領域の **Add** をクリックして、RADIUS スキーム設定を追加するためのページを開きます。次のようにパラメーターを設定します。

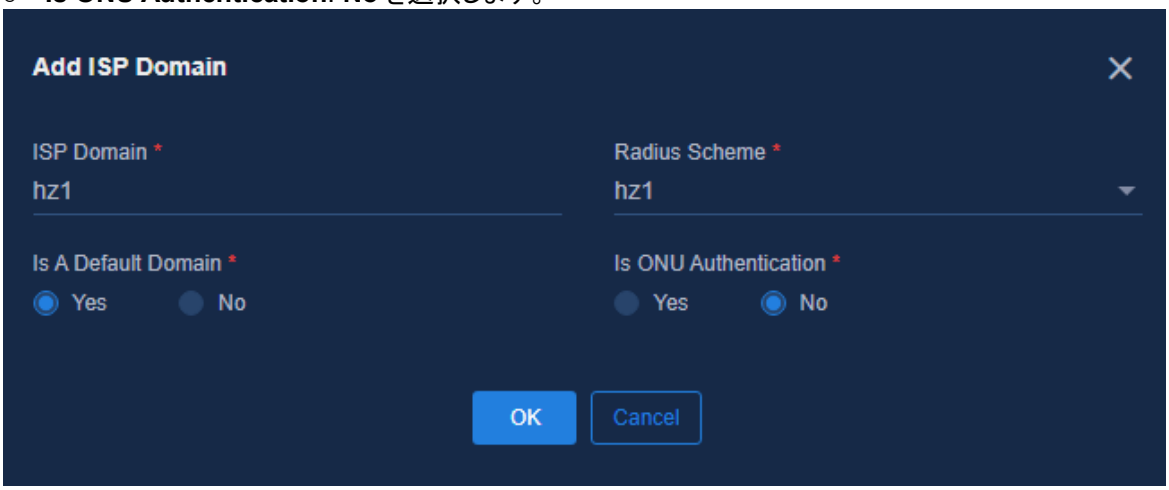
- **Primary Auth Server IP**: EIA サーバーがユーザー認証を実行するために使用する EIA V9 または EIA V7 の IP アドレスを指定します。
- **Real-time Acct Interval(Minute)**: デフォルト設定は 15 分です。
- **Carry ISP Domain Name**: デフォルト設定は **No** です。
  - **Carry ISP Domain Name** が **No** に設定されている場合、RADIUS 認証パケットで使用されるユーザー名はドメイン名を伝送しません。デフォルトでは、EIA はドメイン名サフィックスを伝送しません。
  - **Carry ISP Domain Name** が **Yes** に設定されている場合、RADIUS 認証パケット内のユーザー名はドメイン名を伝送し、ユーザーがオンラインになったときには、ユーザー名の後に @domain name を続ける必要があります。
- **Forcibly Stop Accounting When Clients Go Offline**: Yes を選択すると、クライアントがオフラインになった直後にアカウンティングが停止します。**No** を選択すると、クライアントがオフラインになった直後にアカウンティングが停止しません。



3. ISP ドメイン設定:

   ISP Domain Settings 領域の **Add** をクリックして、**Add ISP Domain** ページを開きます。パラメーターは、次のとおりです。

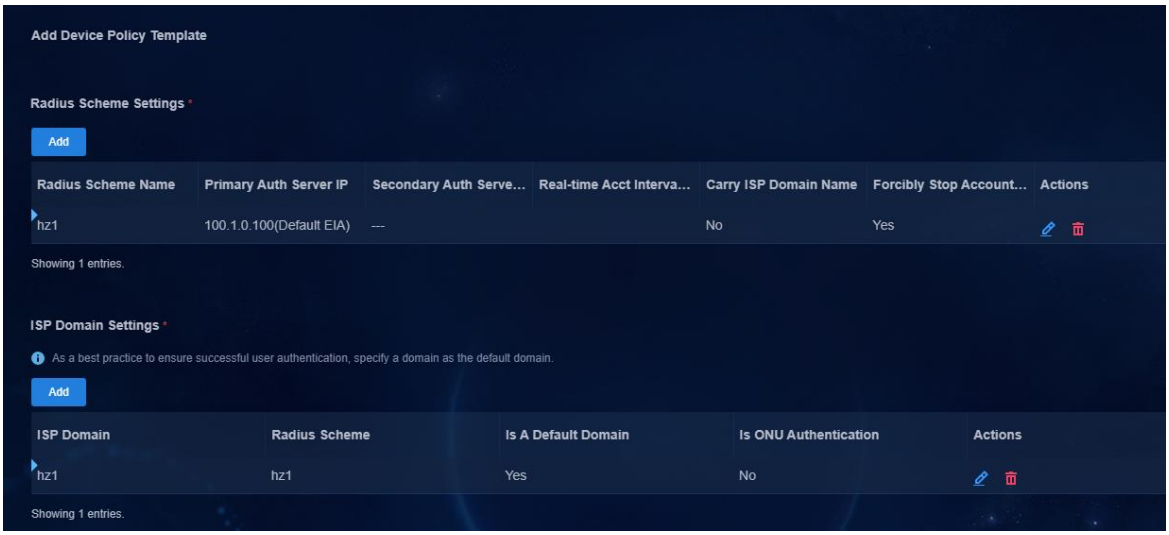
   - **ISP Domain**: **Radius Scheme** 設定を指定すると、RADIUS ドメイン名がここに表示されます。
   - **Is A Default Domain**: **Yes** を選択します。
   - **Is ONU Authentication**: **No** を選択します。



⚠ 警告!

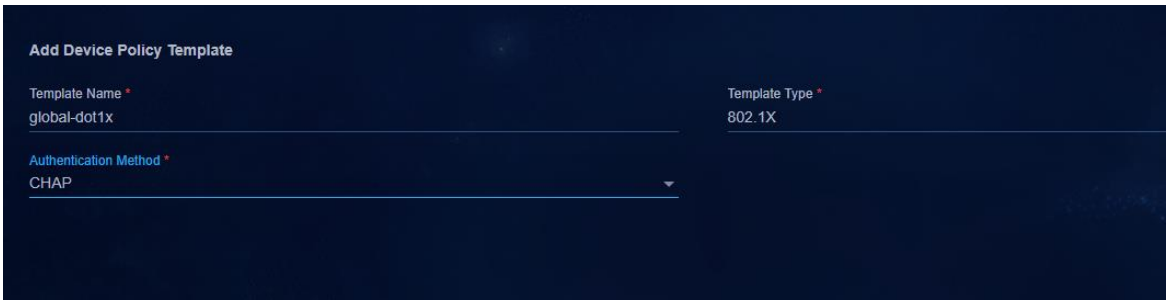
複数の ISP ドメイン名を追加できますが、使用できる既定のドメイン名は 1 つだけです。一般に、RADIUS ドメイン名と ISP ドメイン名を 1 つずつ追加できます。

AAA テンプレートが設定されると、次のように表示されます。



デバイスポリシーテンプレート:802.1X 認証

- **Template Type**: **802.1X** 認証。
- **Authentication Method**: オプションには、**EAP**、**CHAP**、および **PAP** があります。有線認証には **CHAP** を選択し、ワイヤレス認証には **EAP** を選択することをお勧めします。

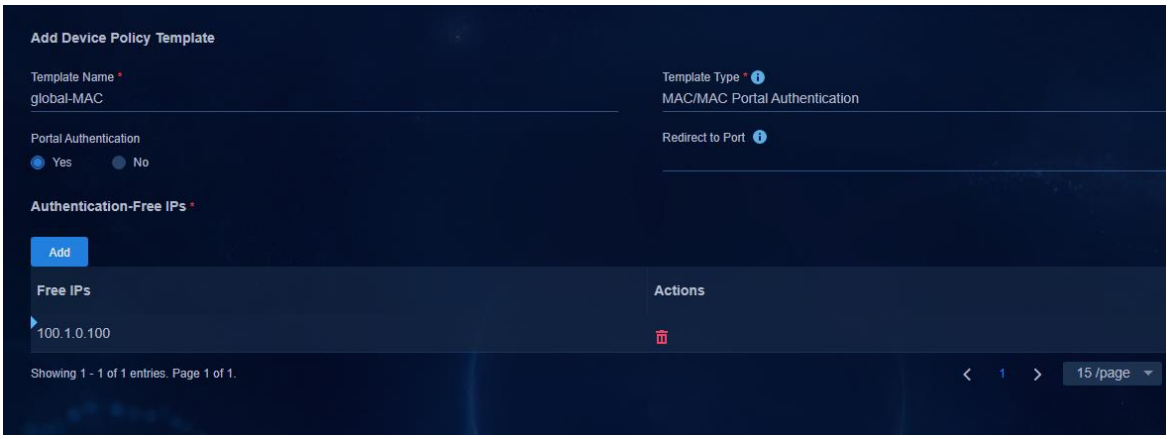


デバイスポリシーテンプレート:MAC/MAC Portal 認証

- **Template Type**: **MAC/MAC Portal authentication**。
- **Portal Authentication**: **Yes** を選択します。
- **Authentication Free IPs**: ポータル認証が有効になっている場合は、EIA サーバーの IP アドレスを認証不要 IP として指定する必要があります。EIA がアクティブ/スタンバイ環境の場合は、2 つの EIA サーバーのアドレスを追加する必要があります。

重要:

AAA テンプレートがプライマリ認証サーバーとバックアップ認証サーバーで設定されている場合、プライマリ認証サーバーとセカンダリ認証サーバーの IP アドレスを認証フリーIP として設定する必要があります。設定された認証フリーIP アドレスの場合、ポリシーテンプレートがリーフデバイスに展開された後、コントローラは、リーフが EIA に到達できるように、認証フリーIP のスーパーネット再帰ルートをリーフデバイスに展開します。



インターフェイスポリシーテンプレート:802.1X 認証

- **Template Type**: **802.1X** 認証。
- **Enable The Escape Function**: デフォルト設定は **Yes** です。必要に応じて、この機能を無効にできます。
- **Unicast Trigger**: デフォルト設定は **Yes** です。デフォルト設定を使用します。
- **Guest Access**: **No** を選択します。802.1X ゲスト機能、認証失敗機能、および MAC ポータル認証は、同じインターフェイスでは使用できません。必要に応じて、このパラメーターを設定します。
- **Access on Authentication Failure**: デフォルト設定は **Yes** です。802.1X ゲスト機能、認証失敗機能および MAC ポータル認証は、同じインターフェイスでは使用できません。必要に応じて、このパラメーターを構成します。

インターフェイスポリシーテンプレート:MAC/MAC ポータル認証

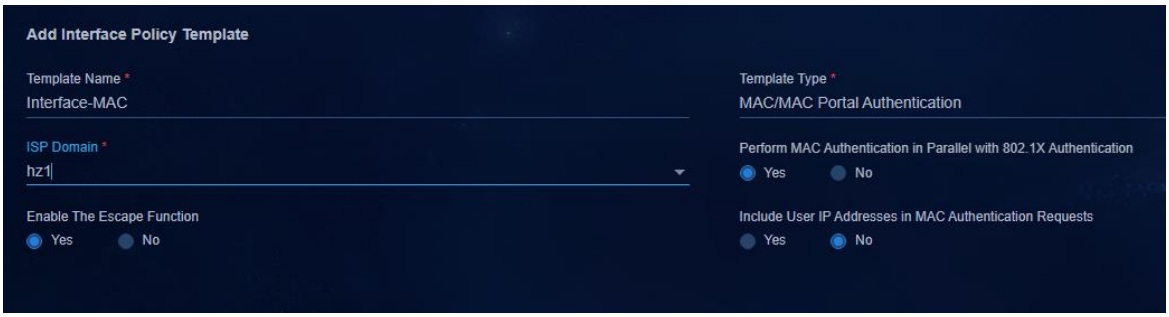
- **Template Type**: **MAC/MAC Portal authentication**。
- **Domain Name**: 以前の AAA 設定のドメイン名が、**Domain Name** ドロップダウンボックスに表示されます。設定されていない場合は、AAA に設定されているグローバルデフォルトドメイン名が使用されます。
- **Enable The Escape Function**: デフォルト設定は、**Yes** です。必要に応じて、この機能を無効にで

きます。

- **Perform MAC Authentication in Parallel with 802.1X Authentication**: デフォルト設定は **Yes** です。デフォルト設定を使用します。
- **Include User IP Addresses in MAC Authentication Requests**: デフォルト設定は **No** です。**Yes** を選択すると、スタティック IP としてエンドポイント設定のユーザー認証を行うために、インターフェイスに mac-authentication carry user-ip コマンドが発行されます。

重要:

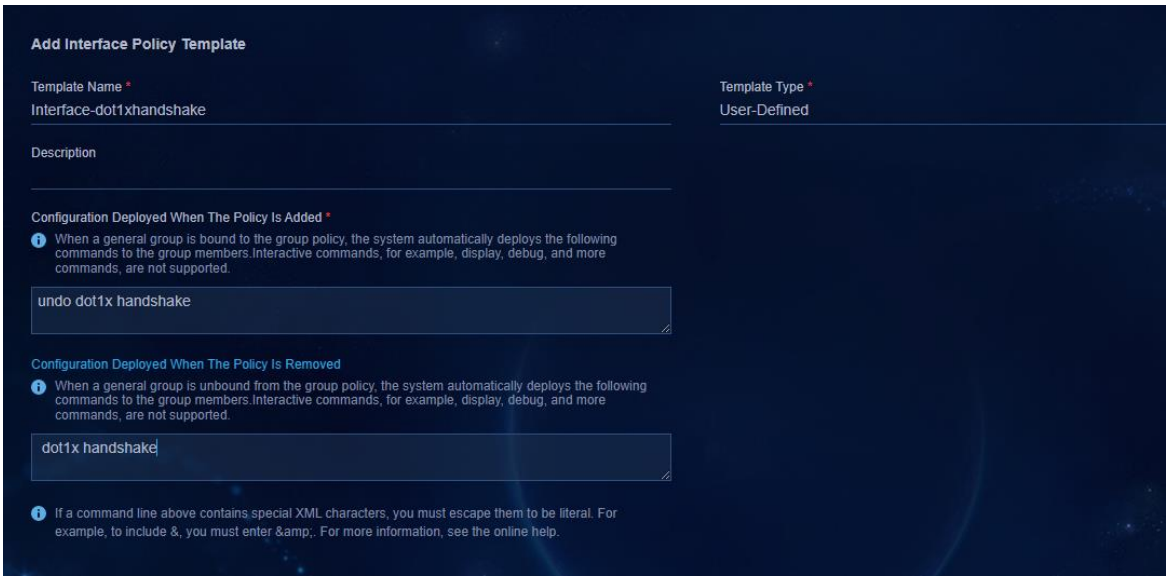
- mac-authentication carry user-ip コマンドの制約事項:このコマンドは、**By IP Range** authentication および **Bind User IP Address** authentication がアクセスポリシーで設定されている場合にだけ設定します。それ以外の場合は、このコマンドを設定しないでください。エンドポイント装置に認証用のスタティック IP アドレスを設定する必要がある場合、コントローラは ARP snooping コマンドを発行して、スタティック IP アドレスを EIA に配信します。
- mac-authentication carry user-ip コマンドの特別な制限事項については、「Fast online based on IP address ranges」を参照してください。



ポリシーテンプレートをカスタマイズする

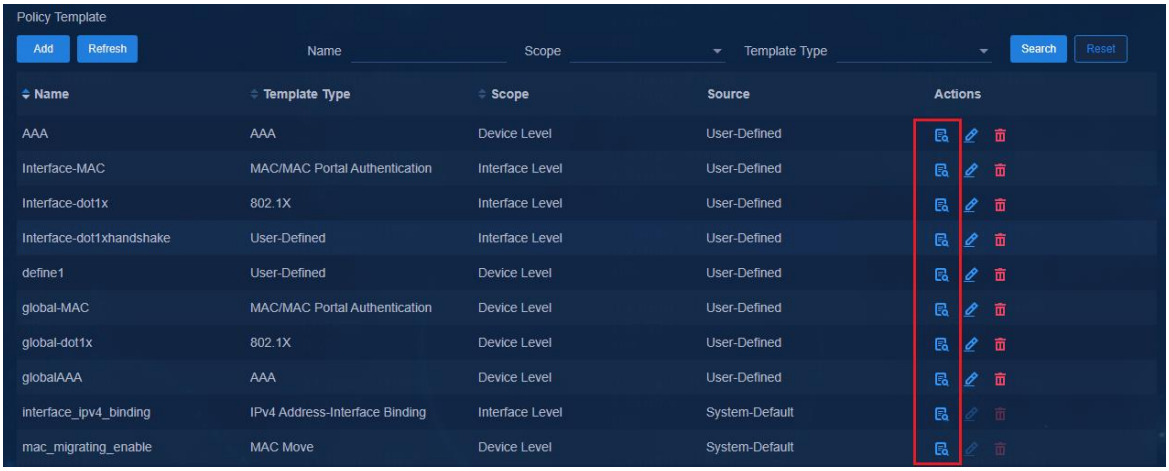
デフォルトのポリシーテンプレートに加えて、デバイスポリシーテンプレートおよびインターフェイスポリシーテンプレートを設定することもできます。次の例では、インターフェイスグループ設定のユーザー定義テンプレートを使用します。

- **Template Type**: **User-Defined** を選択します。
- **Configuration Deployed When The Policy Is Added**: グループがポリシーにバインドされたときにグループ内のメンバーに展開されるコマンドを指定します。
- **Configuration Deployed When The Policy Is Remove**: グループがポリシーからバインド解除されるときに、グループ内のメンバーにデプロイされるコマンドを指定します。このパラメーターは構成する必要があります。構成しない場合、発行されたポリシーは削除できません。



ポリシーテンプレートの内容を表示する

ポリシーテンプレートを構成した後、テンプレートの **Actions** 列をクリックして詳細を表示し、をクリックしてテンプレートを編集できます。ユーザー定義のポリシーテンプレートは編集できません。



重要:

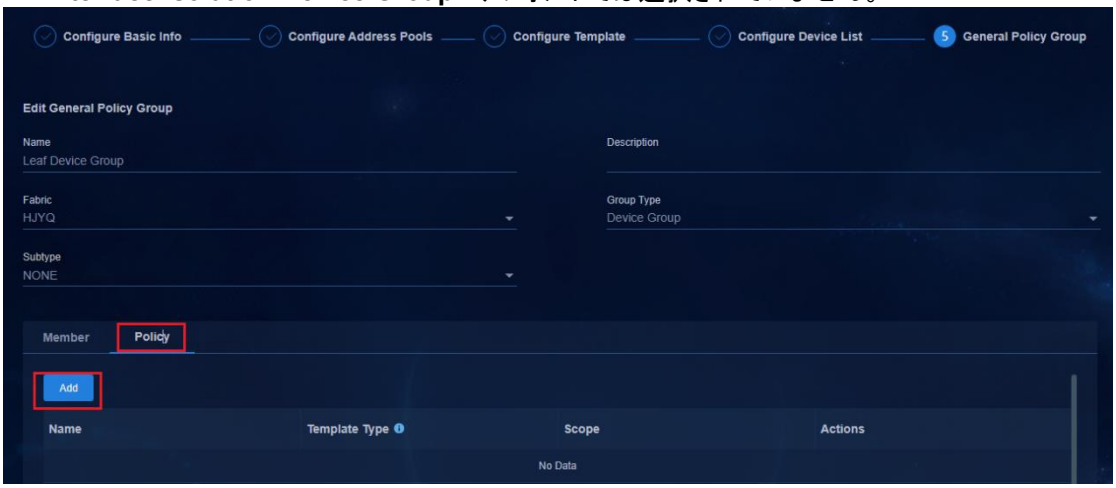
ポリシーテンプレートを設定しても、設定はデバイスに展開されません。設定をデバイスに展開するには、ポリシーテンプレートをデバイスのデバイスグループに適用する必要があります。

デバイスグループ:グループポリシー

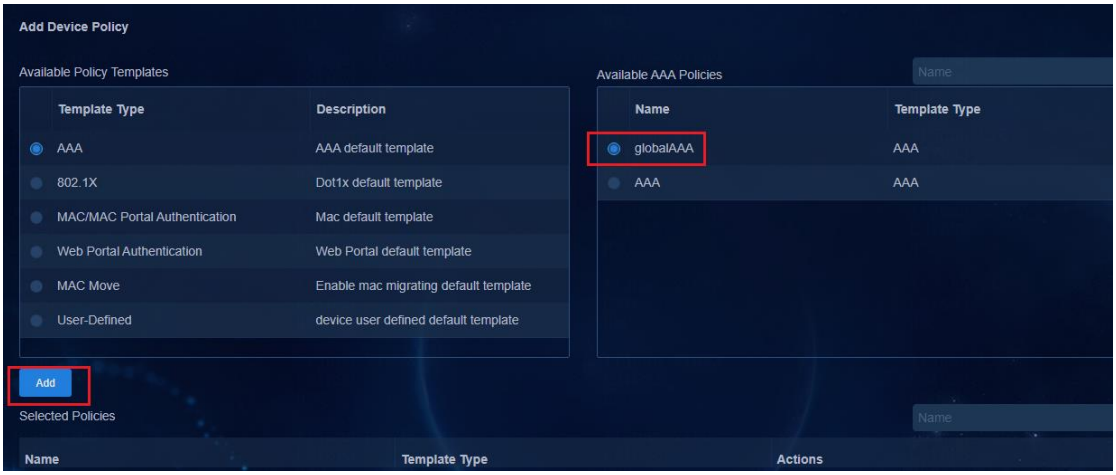
1. AAA 認証、802.1X 認証、MAC 認証、および **mac_migrating_enable** MAC 移行のデバイスポリシーテンプレートを設定します。また、ユーザー定義のポリシーテンプレートも設定できます。

   リスト内の **Leaf Device Group** に対応する **Actions** カラムをクリックします。**Policy** タブをクリックし、**Add** をクリックして、デバイスグループポリシーを追加するページを開きます。

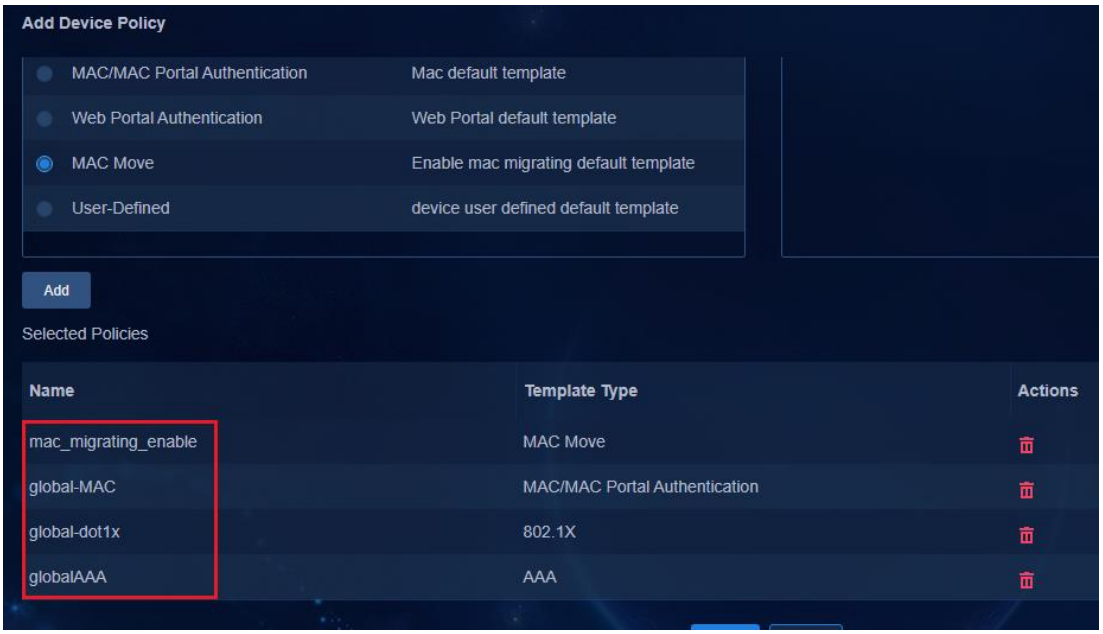
- **Interface Isolation Device Group**：デフォルトでは選択されていません。



2. **Available Policy Templates** カラムで、テンプレートタイプを選択します。テンプレートタイプを選択すると、作成されたポリシーテンプレートが右側の **Available AAA Policies** カラムに表示されます。ポリシーテンプレートを選択し、**Add** をクリックしてポリシーを追加します。



3. 同じ方法で、802.1X 認証、MAC/MAC-Portal 認証、および MAC_MOVE を追加します。**OK** をクリックして設定を保存します。



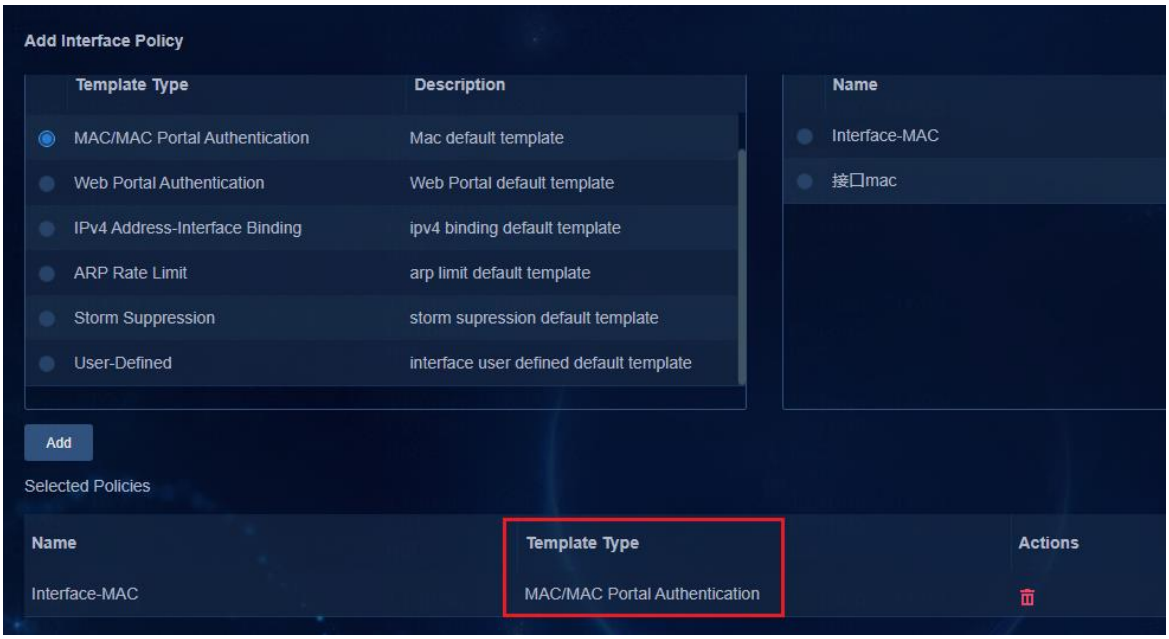
インターフェイスグループ:グループポリシー

デバイスグループポリシーの設定と同じ方法で、**Leaf Downlink Interface Group** でインターフェイスグループポリシーを設定します。**Leaf Downlink Interface Group** で、以前に設定したユーザー認証テンプレートとカスタムポリシーテンプレートを選択します。

必要に応じて、ポリシーテンプレートに 802.1X 認証または MAC 認証を選択します。この例では、次の図に示すように MAC 認証を使用します。

重要:

- 802.1X 認証と MAC/MAC ポータル認証の両方がサポートされています。必要に応じて 1 つの認証方式を構成します。両方の認証方式を構成しないことをお薦めします。
- デバイスグループのグループポリシーとインターフェイスグループのグループポリシーでは、同じ認証方式を使用する必要があります。



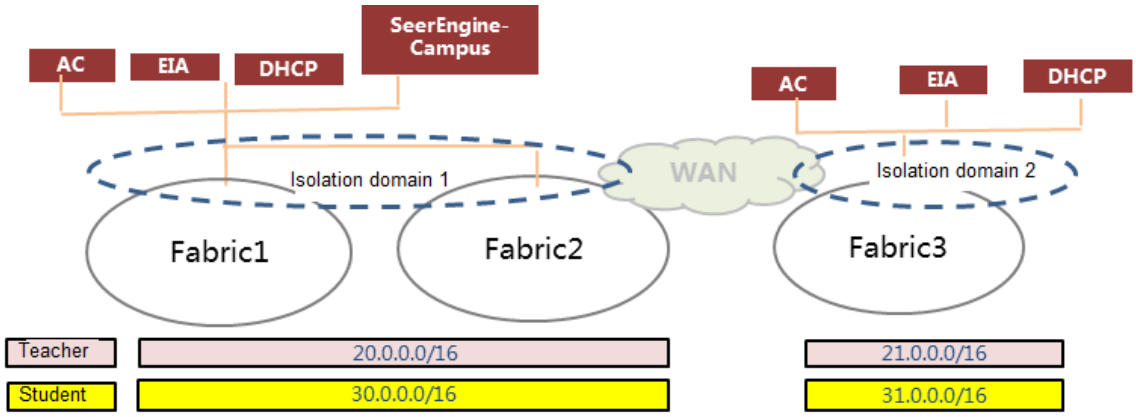
アクセスネットワーク設定の構成

このドキュメントでは、Campus ウィザードを使用してアクセスネットワークを設定します。 **Wizard > Campus Wizard > Access Network Planning** の順に選択します。アクセスネットワーク設定には、分離ドメイン、プライベートネットワーク、レイヤー2 ネットワークドメイン、およびセキュリティグループの設定が含まれます。

分離ドメインの構成

分離ドメインは、ユーザーネットワークを分離するために使用されます。分離ドメイン内の IP アドレス範囲は同じであり、異なる分離ドメイン内の IP アドレスセグメントは異なります。各分離ドメインには、DHCP システム、認証システムおよびワイヤレス AC があります。分離ドメインは通常、会社のキャンパス、病棟、学校のキャンパスなど、物理的な場所に基づいて分割されます。

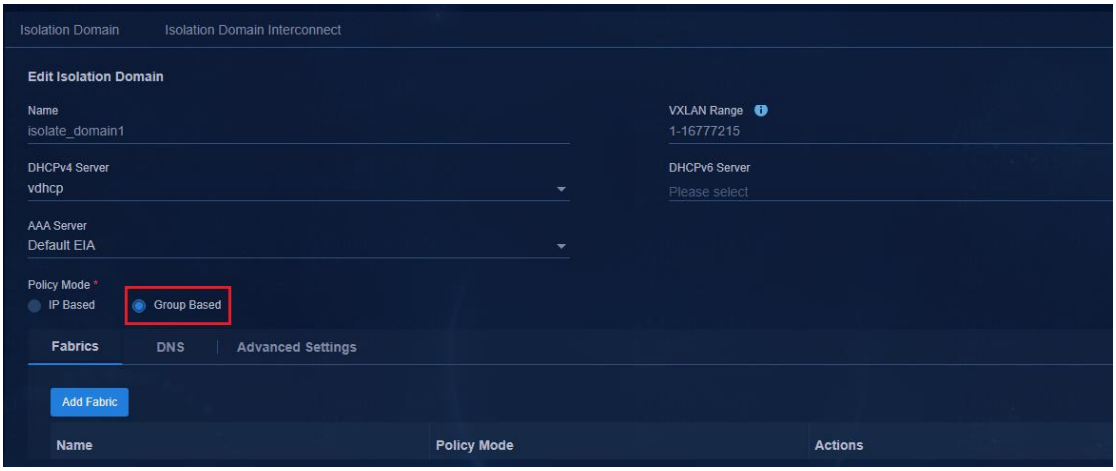
分離ドメインには複数のファブリックを含めることができますが、ファブリックは 1 つの分離ドメインにのみ属することができます。



分離ドメインを構成するには、2 つの方法があります。このドキュメントでは、Campus ウィザードを例として使用します。

- キャンパスウィザードモード。**Wizard > Campus Wizard > Access Network Planning** ページに移動し、最初のステップの **Isolation Domain** で **Isolation Domain** タブをクリックします。
- Non-Campus ウィザードモード。**Automation > Campus Network > Isolation Domain>Isolation Domain** ページに移動します。

1. システムでは、**isolate_domain1** という名前のデフォルトの分離ドメインが定義されています。分離ドメインのデフォルトのポリシーモードは **IP Based** です。分離ドメインをクリックすると、分離ドメインを編集するためのページが開きます。マイクロセグメンテーションネットワークでは、**Group Based** に設定します。

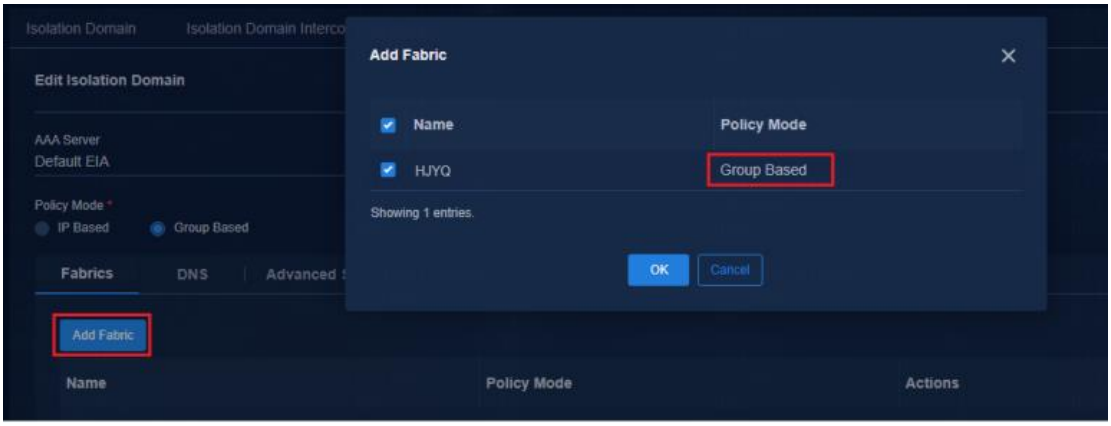


2. DHCP サーバーの指定、ポリシーモードの設定、ファブリックのバインドなど、分離ドメインを構成します。
   - **DHCP Server**: 分離ドメインで使用される DHCP サーバーを指定します。DHCP サーバーには、DHCPv4 サーバーと DHCPv6 サーバーが含まれます。実際のネットワークに応じてサーバーを選択します。
     - DHCPv4 サーバーは、密結合と疎結合の両方をサポートします。密結合では、セキュリティ

グループアドレスプールが DHCP サーバーに自動的に展開されます。疎結合では、セキュリティグループアドレスプールは DHCP サーバーに自動的に展開されません。DHCP サーバーでアドレスプールを手動で作成する必要があります。

- DHCPv6 サーバーは、疎結合のみをサポートします。DHCP サーバーでアドレスプールを手動で作成する必要があります。

- **Policy Mode**: デフォルト設定は **IP Based** です。マイクロセグメンテーションネットワークでは、**Group Based** に設定します。
- **Add Fabric**: 分離ドメインのファブリックを選択します。分離ドメインのポリシーモードは、ファブリックポリシーモードと同じである必要があります。分離ドメインと同じポリシーモードを使用するファブリックのみ選択できます。
- **Add Fabric Connection**: マルチファブリックネットワーキングに適用できます。異なるファブリックが互いに EBGP 接続を確立します。このパラメーターは、シングルファブリックネットワークでは必要ありません。
- **DNS**: 指定した分離ドメインが使用する DNS サーバー上の IP アドレス。



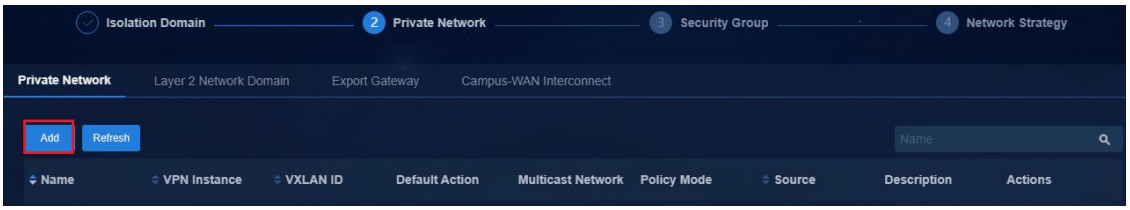
プライベートネットワークを構成する

プライベートネットワークを作成する

2 つのプライベートネットワーク設定方法があります。このドキュメントでは、Campus ウィザードを使用して設定について説明します。

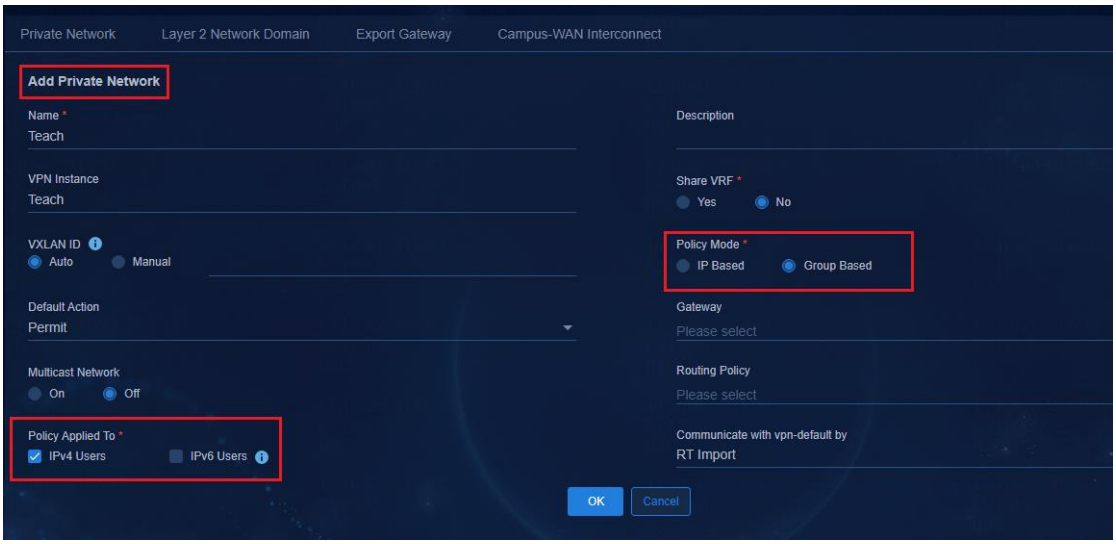
- Campus ウィザードモード。**Wizard > Campus Wizard > Access Network Planning** ページに移動し、2 番目のステップ **Private Network** で **Private Network** タブをクリックします。
- Non-Campus Wizard モード。**Automation > Campus Network > Private Network > Private Network** ページに移動します。

1. 構成が完了したら、**Next** をクリックして、プライベートネットワーク構成のページを開きます。**Add** をクリックして、プライベートネットワークを追加するページを開きます。



2. **Add Private Network** ページの入力ボックスに設定パラメーターを入力し、**OK** をクリックして設定を保存します。

   - **Share VRF**: デフォルトでは **No** に設定されています。デフォルト値を使用します。共有 VRF は共有出力ゲートウェイに使用され、共有出力ゲートウェイの作成時、および共有ゲートウェイがアクセスする IT リソースグループの作成時にだけ使用できます。
   - **XVLAN ID**: プライベートネットワークの L3 VNI を指定します。デフォルト値は **Auto** です。
   - デフォルトのアクション:
     - **Permit**: デフォルトでは、プライベートネットワーク内のすべてのユーザーが相互にアクセスできます。
     - **Deny**: プライベートネットワーク内のすべてのユーザーが相互にアクセスできません。マイクロセグメンテーションスキームでは、**Default Action** を **Deny** に設定すると、セキュリティグループ間のユーザーのみでなく、セキュリティグループ内のユーザーも相互にアクセスできなくなります。
   - **Multicast Network**: 必要に応じてこのパラメーターを設定します。
   - **Policy Mode**: マイクロセグメンテーションネットワーキングの場合、**Group Based** を選択します。
   - **Policy Applied to**: グループ間ポリシーを構成すると、IPv4 ポリシーがデプロイされます。IPv6 グループ間ポリシーをデプロイするには、**IPv6 Users** オプションを選択します。**IPv6** が選択されている場合、サービスチェーンポリシーテンプレートはこのプライベートネットワークに適用できません。
   - **Communicate with vpn default by**: オプションには、**RT Import** と **Static Route** があります。RT インポートはデフォルト設定です。ユーザーのプライベートネットワークと vpn-default は、RT インポートを介して相互接続されます。スタティックルートは新しい通信方法です。ユーザーのプライベートネットワークは vpn-default の RT をインポートし、vpn-default はユーザーのプライベートネットワークへのスタティックルートを使用して通信します。



重要:

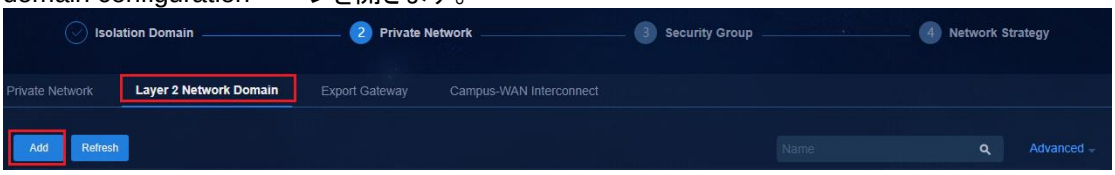
プライベートネットワークと分離ドメインは、レイヤー2 ネットワークドメインを介して相互にバインドされます。プライベートネットワークが分離ドメインにバインドされていない場合、プライベートネットワークの設定は分離ドメイン内のデバイスに展開されません。

レイヤー2 ネットワークドメインを作成する

レイヤー2 ネットワークドメインを設定するには、2 つのモードがあります。このドキュメントでは、Campus ウィザードを使用して設定について説明します。

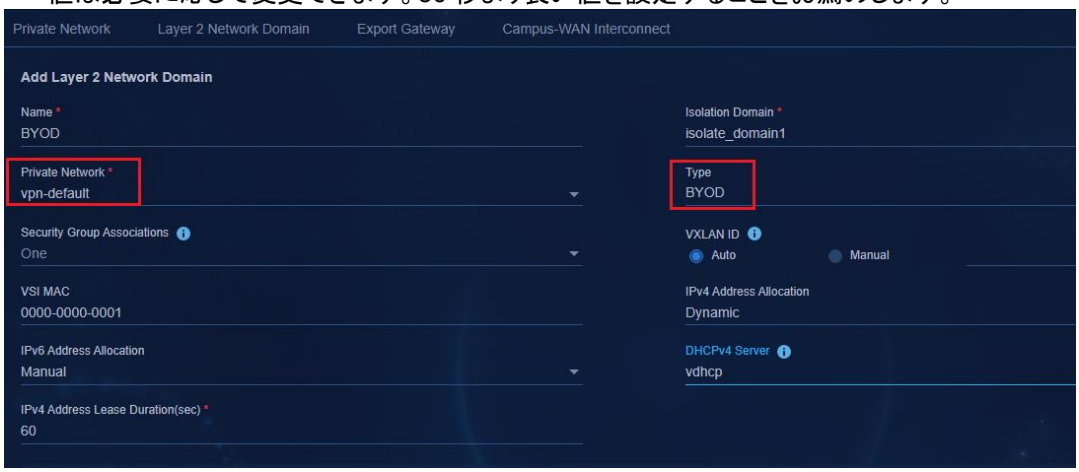
- キャンパスウィザードモード。**Wizard > Campus Wizard > Access Network Planning** ページに移動し、**Layer 2 Network Domain** タブをクリックして、2 番目のステップの **Private Network** で設定します。
- 非キャンパスウィザードモード。**Automation > Campus Network > Private Network > Layer 2 Network Domain** ページに移動します。

1. プライベートネットワークを作成したら、**Layer 2 Network Domain** をクリックして、Layer 2 network domain configuration ページを開きます。



2. **Add** をクリックして、**Add Layer 2 Network Domain** ページを開きます。BYOD 用のレイヤー2 ネットワークドメインと、プライベートネットワークユーザー用のレイヤー2 ネットワークドメインを作成する必要があります。
   - BYOD レイヤー2 ネットワークドメイン:BYOD レイヤー2 ネットワークドメインは、MAC ポータル認証に使用されます。

- **Private Network**: **vpn-default** を選択します。
- **Type**: **BYOD** を選択します。
- **DHCPv4 Server**: BYOD セキュリティグループの場合は、vDHCP を選択します。
- **IP Address Lease Duration**: BYOD アドレスプールのデフォルトリースは 60 秒です。この値は必要に応じて変更できます。30 秒より長い値を設定することをお薦めします。



- ユーザーサービスの L2 ネットワークドメイン:
  - **Private Network**: ユーザーが作成したプライベートネットワークを選択します。レイヤー2 ネットワークドメインが作成されると、プライベートネットワークの設定が、指定された分離ドメイン内のデバイスに展開されます。
  - **Type**: ユーザーサービスに対して **Normal** を選択します。
  - **Layer 2 Domain Support Types**: **Normal**、**Escape**、**Guest**、**Authentication Failed**、**Escape & Authentication Failed**.
  - **Usage**: **Exclusive, Shared,** 及び **Static access** アクセスの 3 つのオプションがあります。

    Exclusive: レイヤー2 ネットワークドメインは、1 つのセキュリティグループだけに割り当てることができます。

    Shared: 1 つのレイヤー2 ネットワークドメインを複数のセキュリティグループに割り当てることができ、同じレイヤー2 ネットワークドメインにバインドされたすべてのセキュリティグループは、同じ IP アドレスセグメントを共有します。IP アドレスセグメントは同じでも、サービスアクセス要件が異なる場合に適用されます。

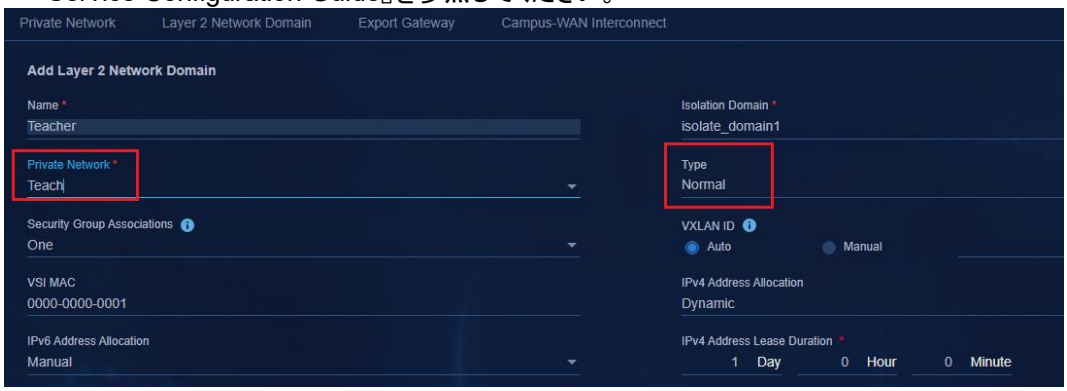
    Static Access: マイクロセグメンテーションシナリオで静的 AC 認証を使用するサービスに適用されます。
  - **IPv4 Address Allocation**: **Dynamic** は、ユーザーが IP アドレスを DHCP サーバーから取得することを意味します。**Manual** は、DHCP アドレスプールが構成されておらず、IP アドレスを手動で構成する必要があることを意味します。**Dynamic** を選択すると、アドレスリース

を設定できます。デフォルト値は 1 日です。

重要:

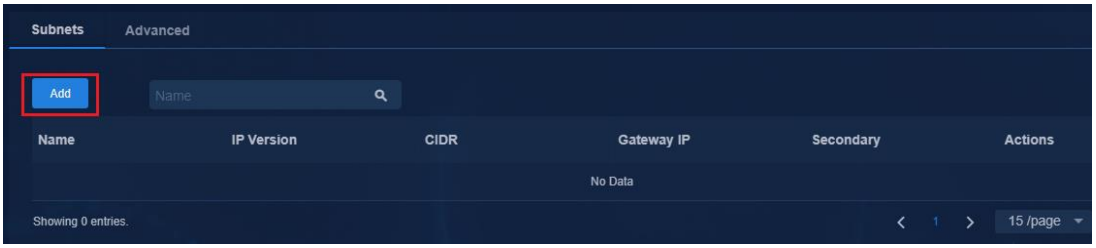
IPv4 アドレスを動的に取得するときに、一部のユーザーエンドポイントがオンボードでスタティック IP アドレスを設定している場合は、**Network Parameters > DHCP Server > IP Prohibits Assigning Addresses** ページで設定したスタティック IP アドレスを手動で追加する必要があります。

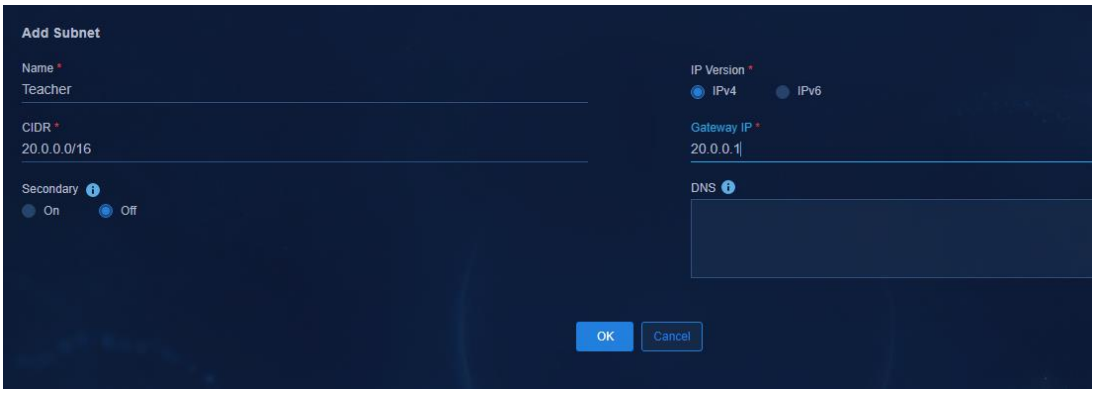
- **IPv6 Address Allocatoin**: オプションには、**Manual**、**SLACC**、**Stateful DHCPv6**、および **Stateless DHCPv6** があります。IPv6 設定の詳細については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。



3. **Subnet** タブで、**Add** をクリックして **Add Subnet** ページを開きます。サブネットパラメーターを構成し、**OK** をクリックします。**Add Subnet** ページで、**Secondary** に対して **On** または **Off** を選択します。

   - **No** を選択すると、サブネットがプライマリネットワークとして使用されます。IPv4 アドレス割り当てモードが動的である場合、システムはサブネットアドレスに基づいて DHCP サーバー上にアドレスプールを作成します。
   - **Yes** を選択すると、サブネットはセカンダリネットワークとして使用されます。システムは、サブネットアドレスに基づいて DHCP サーバーにアドレスプールを作成しません。これは、エンドポイントが静的 IP アドレスを使用する場合に適用されます。セカンダリネットワークを作成する前に、プライマリネットワークが作成されていることを確認してください。また、セカンダリネットワークが使用されている場合は、アクセスポリシーで **Bind User IP Address** 機能を使用できません。



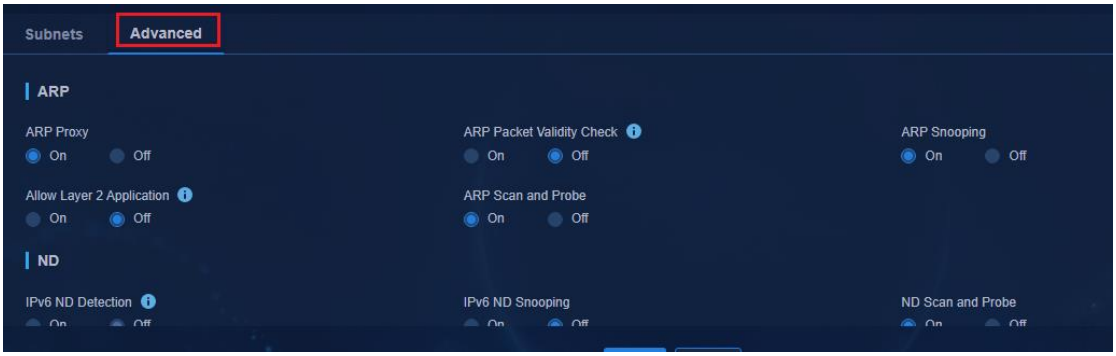


重要:

- レイヤー2 ネットワークドメインは、1 つの 1 次ネットワークセグメントと複数の 2 次ネットワークセグメントのみを持つことができます。実際のネットワーク条件に基づいて IP アドレスを計画します。セキュリティグループが異なれば、必要な IP アドレス範囲も異なります。
- セカンダリネットワークを作成する前に、プライマリネットワークが作成されていることを確認します。
- また、セカンダリネットワークが使用されている場合は、アクセスポリシーで **Bind User IP Address** 機能を使用できません。
- セカンダリネットワークをプライマリネットワークとオーバーラップさせることはできません。この機能は主に、ネットワーク変換シナリオでエンドポイント(プリンタ)のアドレスを変更せずに維持するため、複数の端末のセグメントを 1 つのセキュリティグループに割り当てるため、および ACL リソースを節約するために使用されます。
- **DNS Info**: レイヤー2 ネットワークドメインの DNS サーバーIP アドレスを指定します。

4. サブネットを構成した後、**OK** をクリックして、レイヤー2 ネットワークドメインを追加するページに戻ります。**Advanced** タブをクリックして、必要に応じてパラメーターを構成します。この例では、デフォルト設定が使用されます。
   - **ARP Proxy**: デフォルト設定は **On** です。
   - **ARP Packet Validity Check**: デフォルト設定は **Off** です。これは一般に、不正なユーザーおよびゲートウェイの ARP パケットを検出して廃棄することによって攻撃を防ぐために、アクセスデバイスで使用されます。IPv4 アドレスの取得方法が **Manual** の場合、この機能は有効にできません。
   - **ARP Snooping**: 高速な ARP 応答を提供するために ARP スヌーピングをイネーブルにするかどうかを選択します。**Broadband IoT terminals are not offline** 場合は、On を選択します。
   - **Allow Layer 2 Application**: デフォルト設定は **Off** です。**On** が選択されている場合、作成されたセキュリティグループは、セキュリティグループ内のレイヤー2 インターワーキングをサポートする **Supports Layer 2 Application** を示します。

- **ARP Scan and Probe**: デフォルト設定は **Off** です。On が選択されている場合、ARP ブロードキャストはネットワーク全体をフラッディングしません。ARP 学習は、リーフデバイスのローカルスキャンに依存します。テーブルエントリーは EVPN を介して同期されます。スイッチは ARP メッセージを転送しません。
- **IPv6 ND Detection**: この機能は、ユーザーの正当性を確認するために使用されます。
- **IPv6 ND Snooping**: デバイスは、ND パケットまたはデータパケットをリッスンすることによって ND スヌーピングエントリーを作成します。IPv6 サービスが使用できない場合は、**IPv6 ND Snooping** をイネーブルにしないでください。
- **ND Scan and Probe**: デフォルト設定は **Off** です。**On** が選択されている場合、ND ブロードキャストはネットワーク全体をフラッディングしません。ND 学習は、リーフデバイスのローカルスキャンに依存します。テーブルエントリーは EVPN を介して同期されます。スイッチは ND メッセージを転送しません。
- **DHCPv6 Snooping**: デフォルト設定は **No** です。DHCPv6 スヌーピングは、クライアントが有効なサーバーから IPv6 アドレスまたは IPv6 プレフィクスを取得し、DHCPv6 クライアントの IPv6 アドレスまたは IPv6 プレフィクスと MAC アドレスの対応関係を記録できるようにします。
- **DHCPv6 Trunk Supports Option79**: デフォルト設定 **On** です。これは、DHCPv6 サーバーがクライアントの MAC アドレスを取得できるようにするために使用されます。



注:

- **Yes** を選択すると、セキュリティグループは、ブロードキャスト、不明マルチキャスト、および不明ユニキャストのパケットを AC インターフェイスに転送し、トンネルインターフェイスにフラッディングすることを許可し、EVPN を介した VXLAN MAC 同期を許可します。SeerEngine キャンパスコントローラは、**flooding disable all all-direction** または **mac-advertising disable** コマンドをデバイスに展開しません。
- **Yes** を選択した場合は、Leaf ダウンリンクインターフェイスにブロードキャスト抑制を設定する必要があります。特定の閾値は、機器の種類およびフィールドメッセージの数に従って決定されるものとする。ベストプラクティスとして、対応する製品研究開発スタッフに相談してください。

Allow Layer 2 Application がイネーブルになっている場合、ストーム抑制は物理インターフェイス

からだけ配信でき、集約インターフェイスからは配信できません。リーフダウンリンクポートが集約ポートの場合は、次のように設定します。

a. ユーザー定義のポリシーテンプレートを構成する

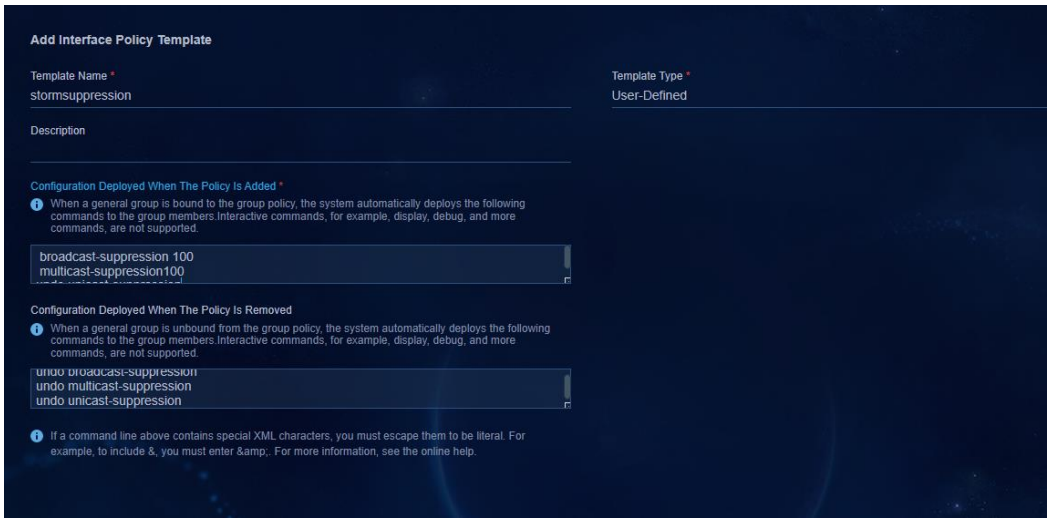
Automation > Campus Network > Device Groups > General Device Groups ページに移動し、ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートページを開きます。**Add** をクリックし、ドロップダウンリストから **Interface Policy Template** を選択します。テンプレートタイプ項目として **User-Defined** を選択し、次に示すように、対応するテキストボックスに次のコマンドを追加します。

ポリシーが追加されたときに展開される設定:

```
#
broadcast-suppression pps 100    //  デバイスモデルとメッセージ数に応じてしきい値を設定します。詳細については、該当する製品の研究開発スタッフにお問い合わせください。
  multicast-suppression pps 100
  unicast-suppression pps 100
  #
```

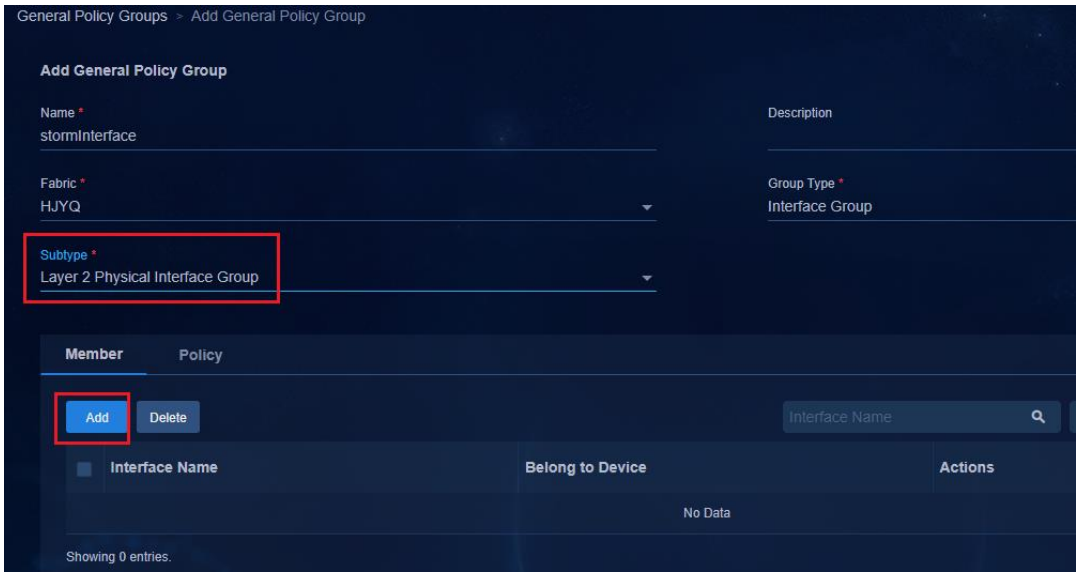
ポリシーが削除されたときに展開される設定:

```
  #
  undo broadcast-suppression
  undo multicast-suppression
  undo unicast-suppression
  #
```

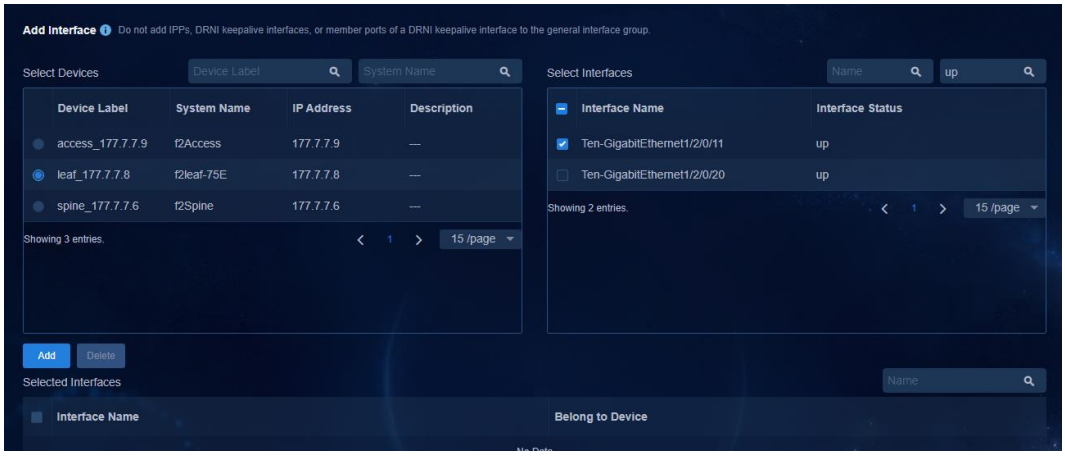


b. ユーザー定義のインターフェイスグループを設定する

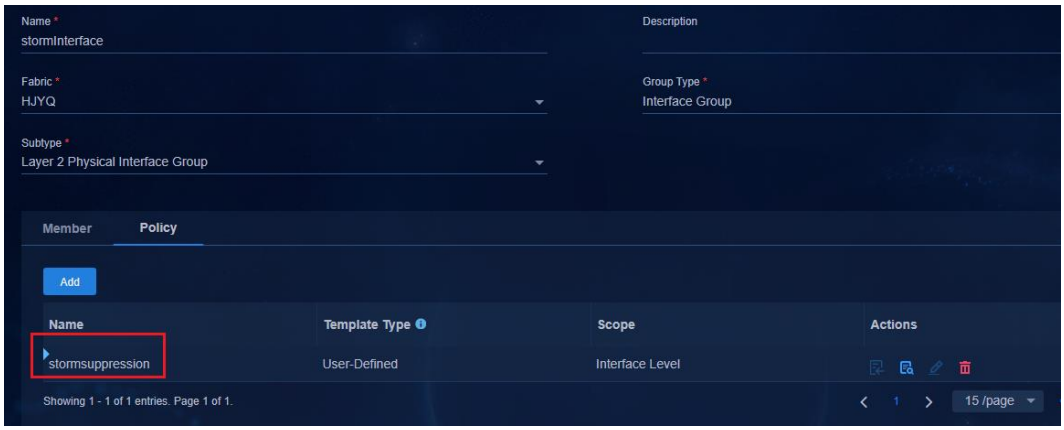
Automation > Campus Network > Device Groups > General Device Groups ページに移動し、**Add** をクリックして、汎用デバイスグループを追加するためのページを開きます。グループタイプに **Interface Group** を選択し、サブタイプに **Layer 2 Physical Interface Group** を選択します。



このページで、**Member** を選択し、**Add** をクリックして、インターフェイスを追加するページを開きます。ストーム抑制を構成するリーフダウンリンク集約ポートに含まれるメンバーインターフェイスを選択します。**Add** をクリックして、選択したインターフェイスをリストに追加します。



メンバーを選択したら、**OK** をクリックして **Add Universal Device Group** ページに戻ります。**Policy** タブをクリックし、**Add** をクリックします。インターフェイスグループポリシーを追加するページで、**User-Defined** storm suppression ポリシーを追加します。設定が完了したら、**OK** をクリックします。



設定が完了したら、メンバーインターフェイスに配信されたストーム抑制設定を表示できます。

```
#
interface Ten-GigabitEthernet0/0/8
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 101 to 3000 4093 to 4094
broadcast-suppression pps 100
multicast-suppression pps 100unicast-suppression pps 100
port link-aggregation group 1024
#
```

重要:

ARP プロキシ、ARP 検出、Allow Layer 2 Application、IPv6 ND 検出、VSI MAC アドレス、およびレイヤー2 ネットワークドメインのセグメント ID は一度だけ配信され、後で変更することはできません。そのため、設定を実行する前に、イネーブルにする機能を確認してください。

セキュリティグループを構成する

注:

- マイクロセグメンテーション機能では、セキュリティグループはマイクロセグメントとして理解できます。セキュリティグループを作成すると、コントローラはマイクロセグメンテーション設定をデバイスに展開します。セキュリティグループ ID はマイクロセグメント ID です。
- セキュリティグループは、分離ドメインを越えることができます。セキュリティグループは、複数の分離ドメインのレイヤー2 ネットワークドメインにバインドできます。複数の分離ドメイン内のデバイスに同じマイクロセグメント ID を割り当てることができます。
- マイクロセグメンテーションは、ユーザーをセキュリティグループ(マイクロセグメント)に関連付け、IP アドレスセグメントからユーザーを分離します。ユーザーは、同じアカウントとパスワードを使用して、異なる分離ドメインでオンラインになることができます。EIA は、アカウントとパスワードに基づいて同じマイクロセグメント ID をユーザーに割り当て、Uniform UX とグローバルな Uniform ポリシーの実施を

実現します。

セキュリティグループを設定するには、2 つの方法があります。このドキュメントでは、Campus ウィザードを例として使用します。

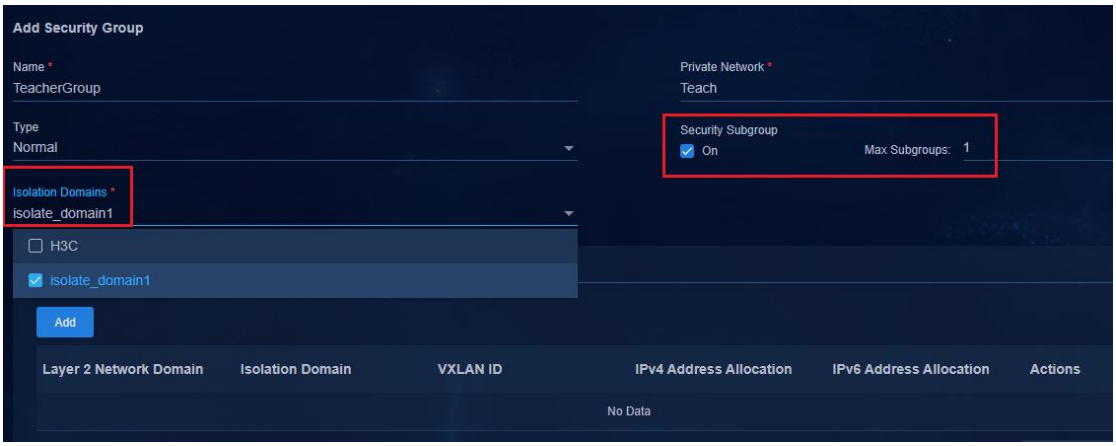
- キャンパスウィザードモード。**Wizard > Campus Wizard > Access Network Planning** ページに移動し、**User Security Group** タブをクリックして、3 番目のステップで **Security Group** を設定します。
- Non-Campus ウィザードモード。**Automation > Campus Network > Security Group > User Security Group** ページに移動します。

1. プライベートネットワークの作成後、**Next** をクリックして **Security Group** ページに移動します。**User Security Group** タブを選択し、**Add** をクリックして、セキュリティグループを追加するページに移動します。セキュリティグループの名前を入力し、プライベートネットワークを選択して、Type に Normal を選択します。

   Type: **BYOD**、**Normal**、**Authentication Failure**、および **External Network**。

   - **BYOD**: BYOD セキュリティグループは、MAC ポータル認証に使用されます。MAC 認証の前に、ユーザーは BYOD セキュリティグループに参加します。システムでは、**BYOD_Security Group** という名前のデフォルトのセキュリティグループが定義されています。グローバルにサポートされる BYOD セキュリティグループは 1 つのみです。
   - **Normal**: 標準セキュリティグループは、ユーザーサービスに使用されます。すべての基本サービスは、標準セキュリティグループを使用します。
   - **Authentication Failure**: 失敗許可セキュリティグループは、失敗許可のシナリオで使用されます。EIA サーバーに障害が発生しても、ユーザーはオンラインになり、失敗許可セキュリティグループ内のリソースにアクセスできます。1 つの分離ドメインに構成できる失敗許可セキュリティグループは 1 つのみです。
   - **External Network**: 外部ネットワークセキュリティグループは、南北サービスチェーンに使用されます。詳細については、『AD-Campus 6.2 Service Chain Configuration Guide』を参照してください。

2. **Isolation Domains** をクリックし、ドロップダウンボックスから分離ドメインをクリックします。セキュリティグループにレイヤー2 ネットワークドメインを追加する前に、分離ドメインを選択する必要があります。



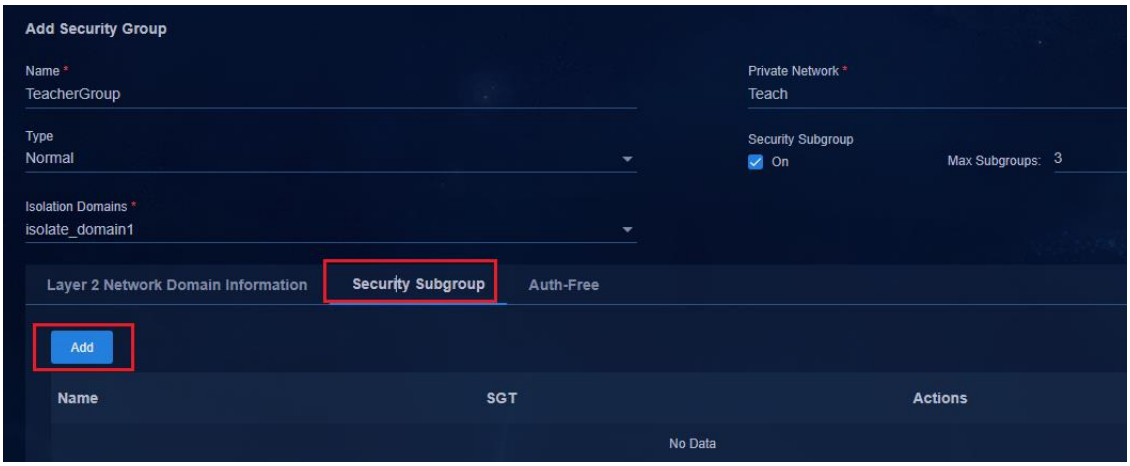
3. **Layer 2 Network Domain** タブをクリックし、**Add** をクリックして、レイヤー2 ネットワークドメインを追加するページを開きます。**Available Layer 2 Network Domain** 列でレイヤー2 ネットワークドメインを選択し、›をクリックして、選択したレイヤー2 ネットワークドメインを **Selected Layer 2 Network Domain** 列に追加します。次に、**OK** をクリックして、セキュリティグループを追加するページに戻ります。

4. Security Subgroup で **On** を選択すると、**Max Subgroups** リストと **Security Subgroups** が次のように表示されます。

   Max Subgroup リストには、1、3、7 および 15 の 4 つのオプションがあります。これにより、セキュリティグループに対して作成できるセキュリティサブグループの最大数が制限されます。最大 15 個まで作成できます。**Max Subgroups** のオプションを選択した後、**Security Subgroup** タブで選択した容量で最大のセキュリティサブグループを作成できます。

重要:

- セキュリティサブグループは、セキュリティグループに対して省略可能です。
- マイクロセグメンテーションでは、サブセキュリティグループがサポートされます。セキュリティグループは、複数のサブセキュリティグループをサポートします。サブセキュリティグループは、親グループの権限を継承できます。また、サブグループの権限を個別に構成することもできます。サブセキュリティグループは、グループ間ポリシーの例外構成に使用されます。セキュリティグループでは、詳細な権限制御のために、特定の権限を持つロールをサブセキュリティグループに割り当てることができます。



5. 作成したセキュリティグループは、User Security Group ページで表示できます。

   値 3504 はセキュリティグループ ID であり、コントローラはマイクロセグメント ID 3504 をデバイスに展開します。サブセキュリティグループ列の値 1/3 は、1 つのサブセキュリティグループが作成され、セキュリティグループに対して最大 3 つのサブセキュリティグループを作成できることを示します。

6. セキュリティグループとサブセキュリティグループを作成すると、コントローラはマイクロセグメンテーション設定をデバイスに展開します。

```
 # microsegment ID 3504 を展開します。
 microsegment 3504 name SDN_EPG_3504
 member ipv4 20.0.0.0 255.255.0.0 vpn-instance vpn1
 #
```

#サブセキュリティグループ設定を展開します。dis microsegment aggregation コマンドを実行して、サブセキュリティグループを表示できます。

#セキュリティサブグループ 3505～3507 のマイクロセグメント ID を展開します。

```
[Leaf]display microsegment aggregation
Aggregation ID Range Aggregation name
3504 3504-3507 SDN_EPGAGG_3504
[Leaf]
```

ネットワーク戦略の設定

ネットワークポリシーを設定するには、2 つの方法があります。このドキュメントでは、Campus ウィザードを使用して設定について説明します。

- キャンパスウィザードモード。**Wizard > Campus Wizard > Access Network Planning** ページに移動し、4 番目の手順の **Network Policy** でネットワークポリシーを設定します。
- 非キャンパスウィザードモード。**Automation > Campus Network > Network Policy** ページに移動します。

ネットワークポリシーページでは、グループポリシーテンプレートをドラッグすることによって、ユーザーセキュリティグループ間、およびユーザーセキュリティグループとリソースグループ間のアクセス関係を設定できます。これにより、設定が簡単になります。

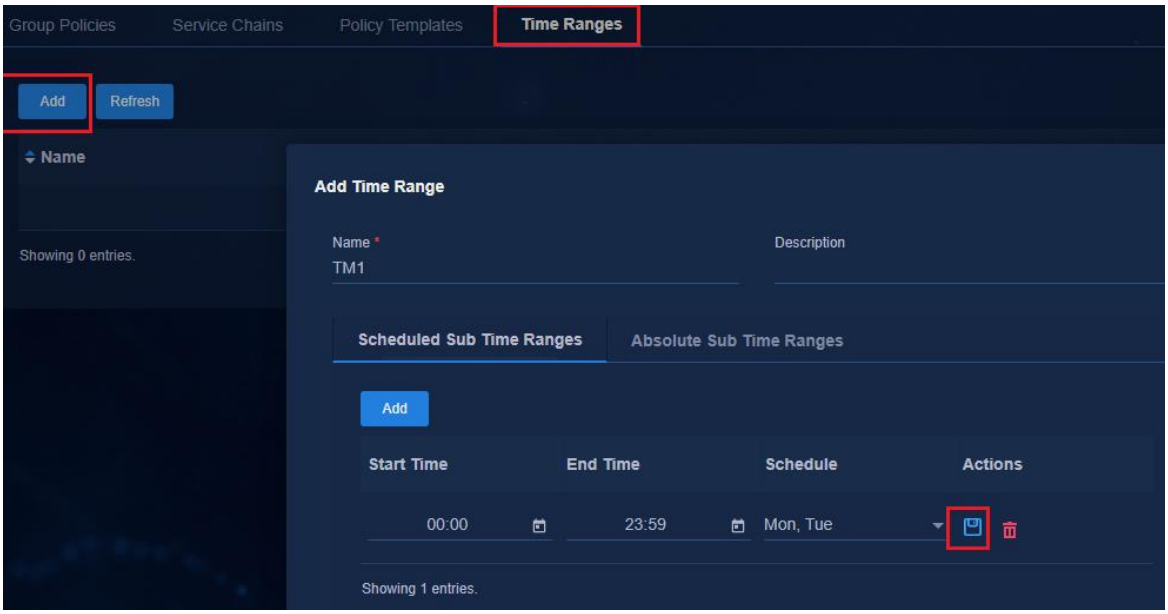
たとえば、教師セキュリティグループと生徒セキュリティグループを分離するには、**TM1** ポリシーテンプレートを対応する場所にドラッグし、**OK** をクリックします。**TM1** を右クリックして、**TM1** ポリシーテンプレートを対応する場所にドラッグします。

Table 1 セキュリティグループ間のポリシー

グループポリシー	学生のセキュリティグループ	教師のセキュリティグループ	パブリックサーバー
学生のセキュリティグループ	該当なし	TM1	該当なし
教師のセキュリティグループ	TM1	該当なし	該当なし

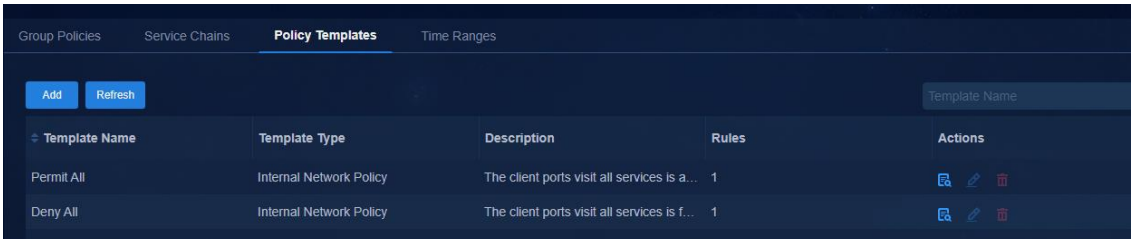
時間範囲の設定(オプション)

1. **Time Range** タブをクリックして、時間範囲を構成します。時間範囲はオプションで、必要に応じて設定できます。
2. **Add** をクリックして、Add Time Range ページで時間範囲を設定します。構成が完了したら、**Save**  をクリックして構成を保存し、**OK** をクリックします。

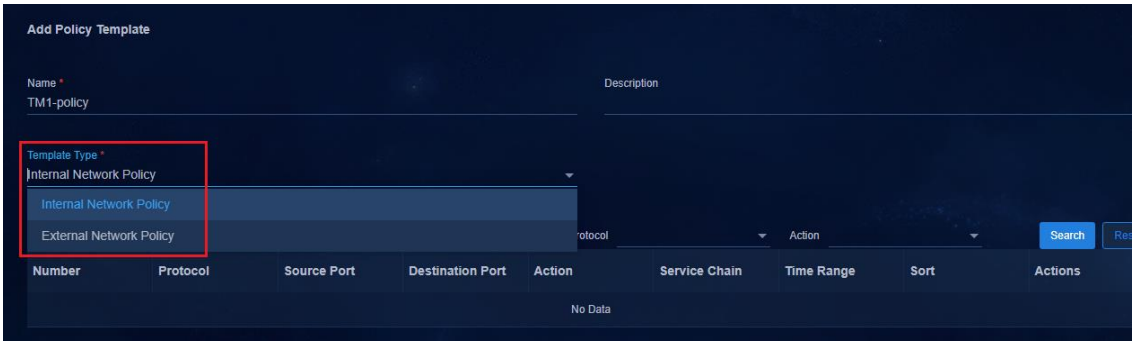


ポリシーテンプレートを構成する

1. **Policy Templates** タブをクリックします。システムは、**Permit All** と **Deny All** の 2 つのデフォルトテンプレートを定義しています。

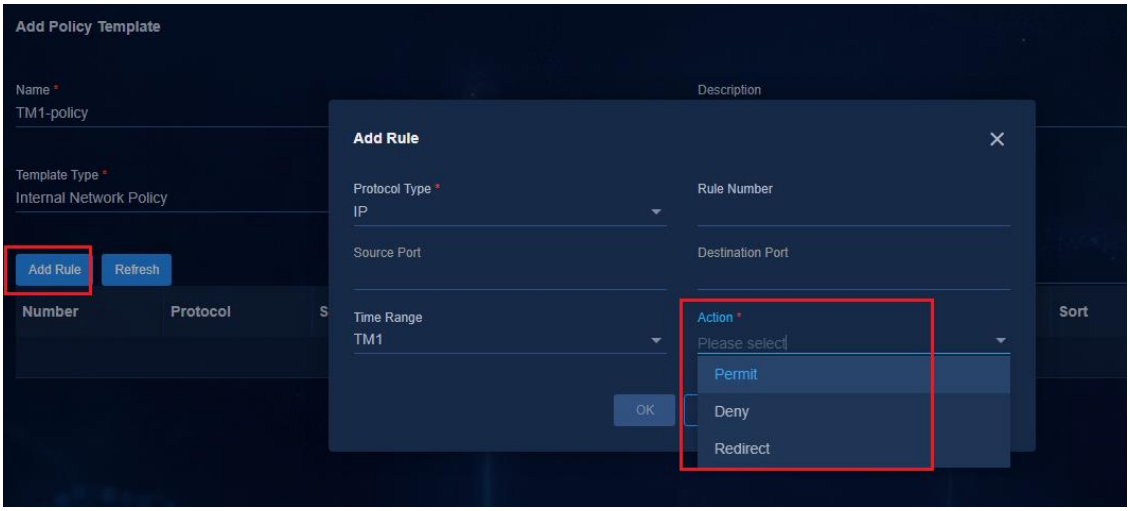


2. **Add** をクリックして、ポリシーテンプレートを追加するページを開きます。ポリシーテンプレートの名前を入力し、**Template Type** で **Internal Network Policy** を選択します。
   - **Internal Network Policy**: グループポリシーおよび east-west service chains の場合は、**Internal Network Policy** を選択します。
   - **External Network Policy**: south-north service chains の場合は、**External Network Policy** を選択します。



3. **Add Rule** をクリックします。パラメーターを設定し、**OK** をクリックして設定を保存します。パラメーターの説明は次のとおりです。

   - **Protocol Type**: **IP**、**UDP**、**TCP**、および **ICMP**。
   - **Time Range**: デフォルト設定は **None** で、すべての時間範囲が有効であることを示します。必要に応じて設定できます。
   - **Action**: オプションは、**Permit, Deny** と **Redirect** です。グループポリシーの許可または拒否を選択します。**Redirect** はサービスチェーンに適用されます。



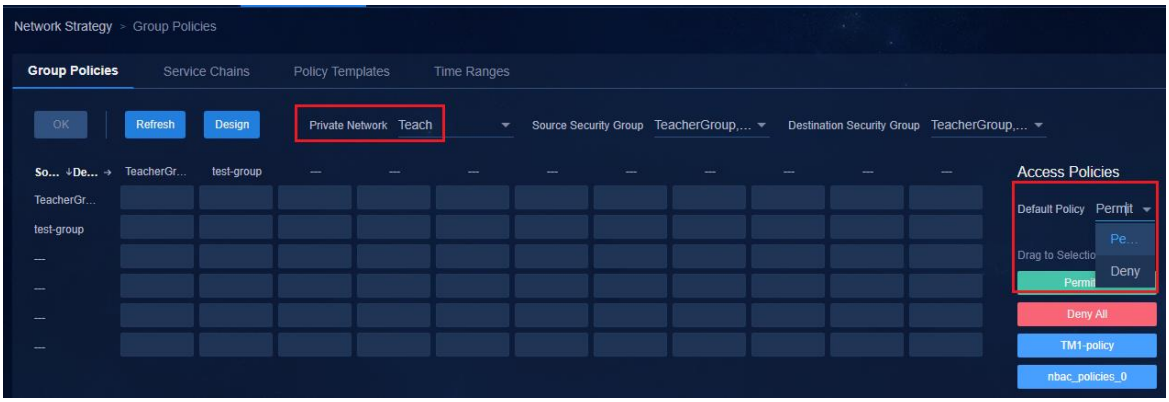
4. ポリシーテンプレートの追加が完了したら、**OK** をクリックしてポリシーテンプレートを保存します。

デフォルトアクセスポリシーを設定する

グループポリシータブをクリックして、グループポリシーページを開きます。既定のポリシー列(略して既定のアクセスポリシー)のドロップダウンリストボックスで、プライベートネットワークユーザーのアクセス許可を構成できます。グループポリシーを設定する場合は、最初にプライベートネットワークを選択し、次に既定のポリシーを設定します。

グループアクセスポリシーページで設定されたデフォルトのグループアクセスポリシーは、プライベートネットワークページで設定されたデフォルトのグループアクセスポリシーと同じです。設定する必要があるのは 1 つだけです。

- **Permit**: プライベートネットワーク内のすべてのユーザーが相互にアクセスできます。
- **Deny**: プライベートネットワーク内のすべてのユーザーは相互にアクセスできません。マイクロセグメンテーションソリューションでは、アクションを **Deny** に設定すると、ユーザーが同じセキュリティグループに属しているか、異なるセキュリティグループに属しているかに関係なく、相互にアクセスできなくなります。**Default Policy** が **Deny** に設定されている場合、セキュリティグループ内のユーザーが相互に通信するためのグループポリシーを構成する必要があります。



Deny を選択した場合、SeerEngine キャンパスコントローラは、グローバル deny PBR をスパイン/リーフデバイスに展開し、**permit IP** ポリシーをプライベートネットワークの VSI インターフェイスに展開します。

- スパインデバイスとリーフデバイスのプライベート VSI インターフェイスに **Permit IP** を設定します。

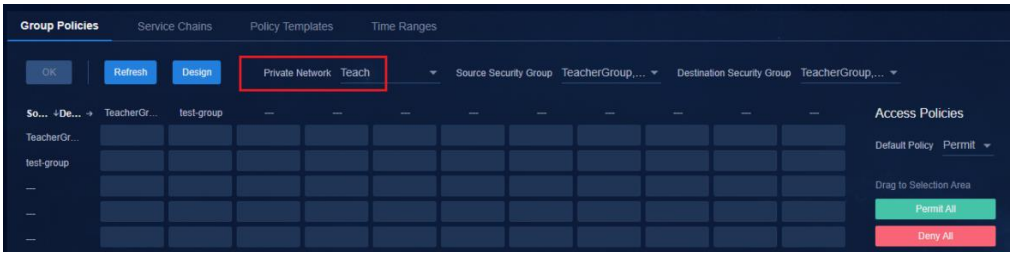
```
#
policy-based-route SDN_GLB_SC2 permit node 65535
 if-match acl name SDN_ACL_SC_PERMIT_ALL
#
#
acl advanced name SDN_ACL_SC_PERMIT_ALL
 description SDN_ACL_SC_PERMIT_ALL
 rule 0 permit ip
#
interface Vsi-interface2
 description SDN_VRF_VSI_Interface_2
 ip binding vpn-instance Teach
 ip policy-based-route SDN_GLB_SC2
ipv6 address auto link-local
 l3-vni 2
#
```

- スパイン デバイスとリーフ デバイスの **Deny** 設定をグローバルに発行します。

```
#
policy-based-route SDN_GLOBAL_SC permit node 60000
 if-match acl name SDN_ACL_GLOBAL_SC_e4a30470-a7cc-4008-8311-1e2cb1f978e5
 apply output-interface NULL0
#
#
acl advanced name SDN_ACL_GLOBAL_SC_e4a30470-a7cc-4008-8311-1e2cb1f978e5
 description SDN_ACL_GLOBAL_SC_e4a30470-a7cc-4008-8311-1e2cb1f978e5
 rule 0 permit ip vpn-instance Teach destination microsegment 3504 mask-length 2
//Mask length of the security group. Mask length n indicates that there are a total of 2^n (4) security groups and sub security groups, and 3504 is the security group.
 rule 1 permit ip vpn-instance Teach destination microsegment 3502
#
```

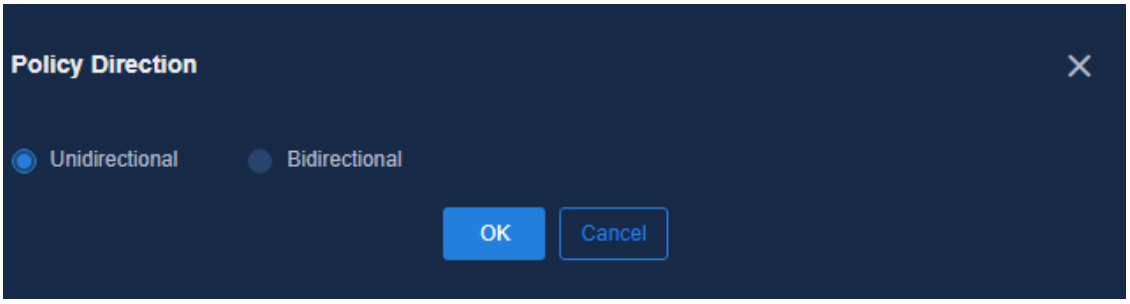
グループポリシー

1. **Group Policies** タブをクリックして、グループポリシーページを開きます。**Private Network** を選択し、**Private Network Tech** を次のようにクリックします。

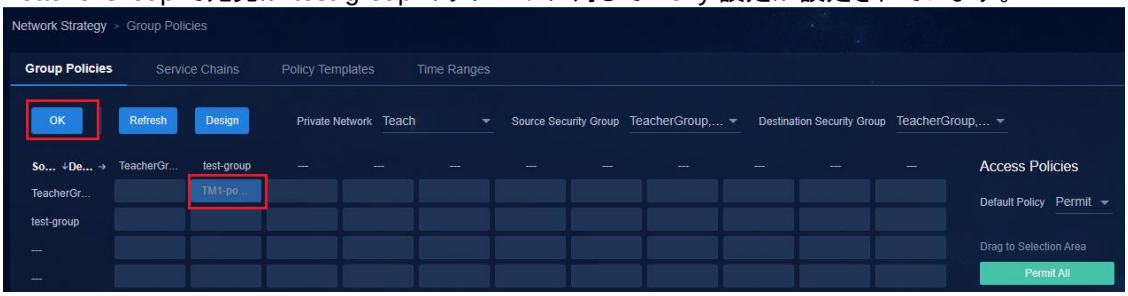


2. 右側でアクセスポリシーを選択し、対応する場所にドラッグして、**Policy Direction** ダイアログボックスを開きます。構成が完了したら、**OK** をクリックして構成を保存します。**Policy Direction** パラメーターには、**Unidirectional** と **Bidirectional** の 2 つのオプションがあります。

   - **Unidirectional**: 送信元から宛先へのアクセスポリシー。
   - **Bidirectional**: 送信元から宛先へのアクセスポリシーおよび宛先から送信元へのアクセスポリシー。



3. 設定が完了したら、左上隅にある **OK** をクリックします。次の図に示すように、送信元が TeacherGroup で宛先が test-group のグループに対して Deny 設定が設定されています。



4. コントローラは、PBR を Spine デバイスと Leaf デバイスにグローバルに展開します。コマンドは次のとおりです。

```
#
time-range SDN_NBAC_80002p 00:00 to 23:59 off-day
#
#
policy-based-route SDN_GLOBAL_SC permit node 1
```

```
 if-match acl name SDN_ACL_SC_80002q_3502_3504
 apply output-interface NULL0     // Configure Deny
#
#
acl advanced name SDN_ACL_SC_80002q_3501_3504
 description SDN_ACL_SC_80002q_3501_3504
 rule 0 permit ip vpn-instance Teach source microsegment 3502 destination microse
gment 3504 mask-length 2 time-range SDN_NBAC_80002p
#
```

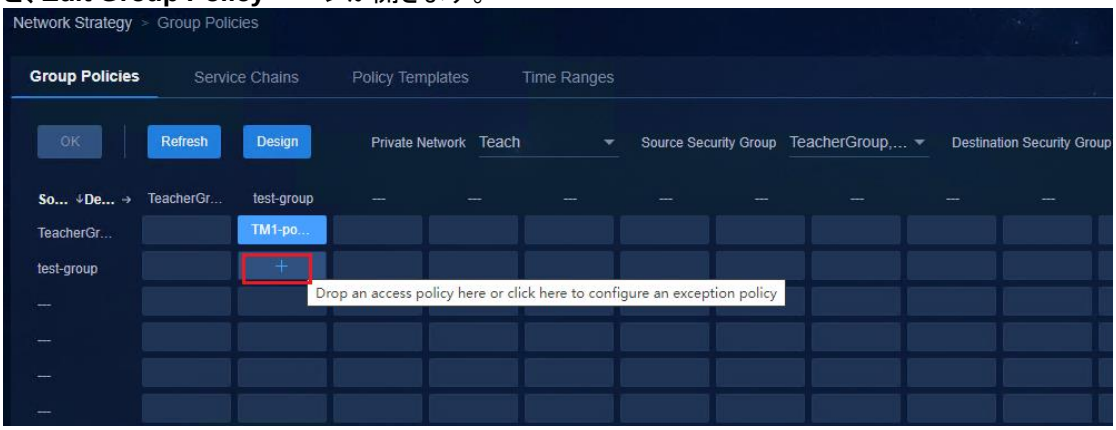
例外

グループポリシーは、例外を使用して構成することもできます。例外は、特殊な処理を示します。グループポリシーテンプレートが配信されたセキュリティグループ内の特定のトラフィックを除外する例外規則を構成できます。

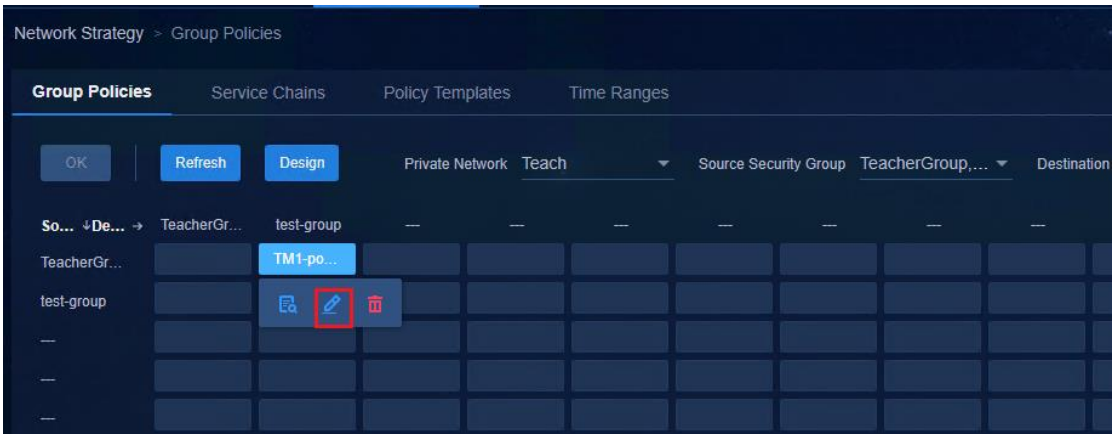
マイクロセグメンテーションの例外規則は、次のように IP ポリシーの例外規則と異なります。

- IP アドレス範囲は、IP ポリシー例外規則で指定されます。
- セキュリティサブグループは、マイクロセグメンテーション例外ルールで作成されます。

1. セキュリティグループの中央にマウスを移動すると、プラス記号(+)が表示されます。+をクリックすると、**Edit Group Policy** ページが開きます。

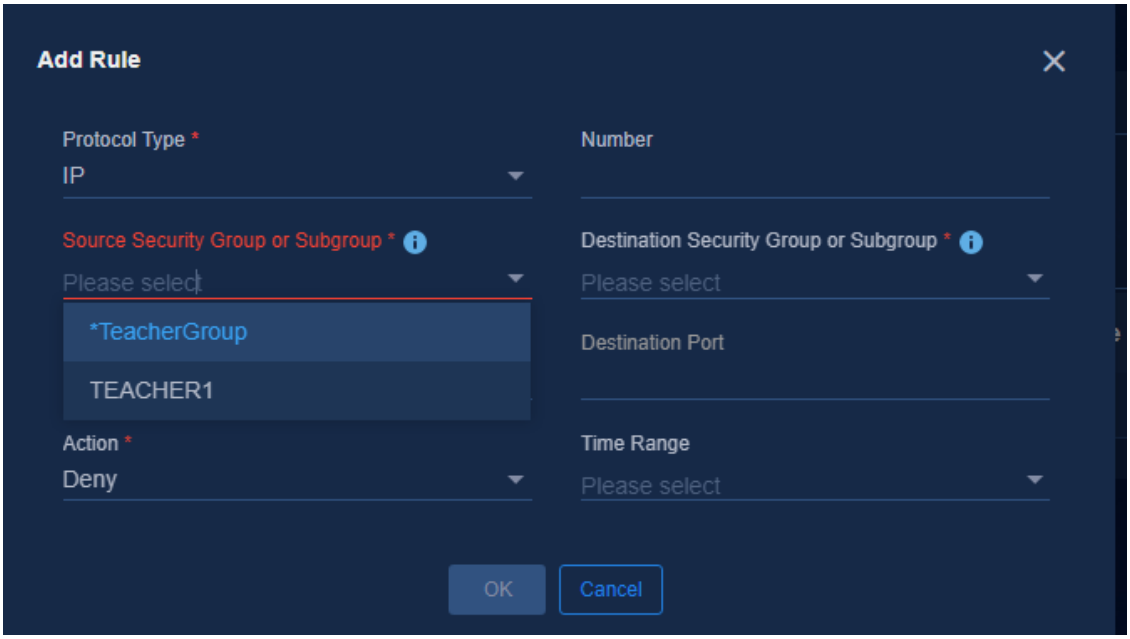


2. グループアクセスポリシーが既に存在する場合は、をクリックして、グループアクセスポリシーを編集するためのページを開きます。



3. **Exception Policy** タブをクリックし、+アイコンをクリックして、ルールを追加するためのページを開きます。ページでルールを設定し、OK をクリックして構成を保存します。

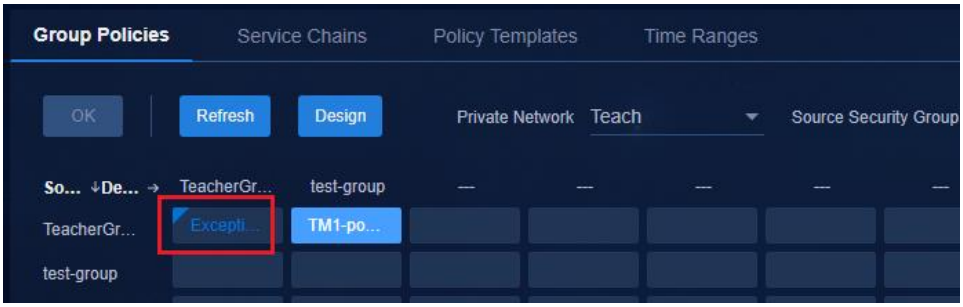
   マイクロセグメンテーションで構成される例外ポリシーは、セキュリティサブグループのアクセスポリシーです。サブセキュリティグループ名がアスタリスク(*)で構成されている場合、セキュリティサブグループには、セキュリティグループと、セキュリティグループ内のすべてのセキュリティサブグループが含まれます。たとえば、次の図の***TeacherGroup** は、セキュリティグループ **TeacherGroup** と、セキュリティグループ内のすべてのセキュリティサブグループを意味します。



4. 例外規則が設定されると、Exceptions Policy アイコンが表示されます。キャンパスコントローラは、次の設定をスパインデバイスとリーフデバイスに展開します。

```
#
policy-based-route SDN_GLOBAL_SC permit node 2
 if-match acl name SDN_ACL_SC_000005_3504_3504
 apply output-interface NULL0
#
acl advanced name SDN_ACL_SC_000005_3504_3504
```

```
 description SDN_ACL_SC_000005_3504_3504
 rule 0 permit ip vpn-instance Teach source microsegment 3504 mask-length 2 dest
ination microsegment 3505
#
```



ユーザークセス設定を構成する

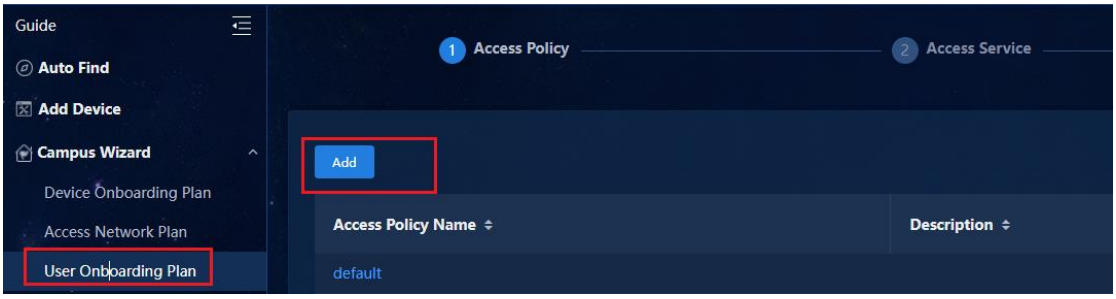
ユーザークセス設定は、アクセスポリシー設定、アクセスサービス設定、アクセスユーザー設定などの EIA 認証サーバー設定です。アクセスサービスを設定すると、ユーザーはオンラインになることができます。

アクセスポリシーの構成

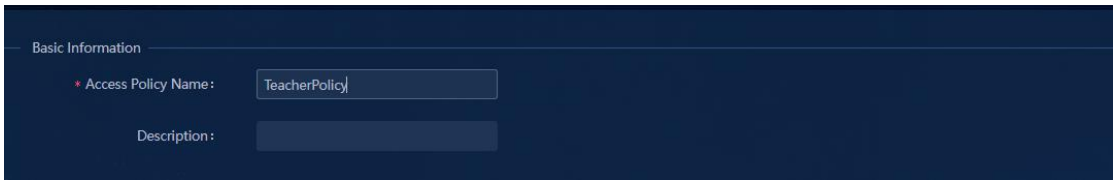
アクセスポリシー管理を設定するには、2 つの方法があります。このマニュアルでは、Campus ウィザードを使用します。

- キャンパスウィザードモード。**Wizard** > **Campus Wizard** > **User Onboarding Planning** ページに移動し、最初のステップで **Access Policy Management** を設定します。
- Non-Campus ウィザードモード。**Automation > User Service > Access Service** ページに移動し、右上隅にあるアクセスポリシーリンクをクリックしてアクセスポリシーページに移動します。

1. **Add** をクリックして、アクセスポリシー設定ページを開きます。



2. アクセスポリシー設定ページには、基本情報、認可情報、認証バインディング情報、およびユーザークライアント設定が含まれます。
   - **Basic Information**: アクセスポリシーの名前を入力し、デフォルトのサービスグループを使用します。

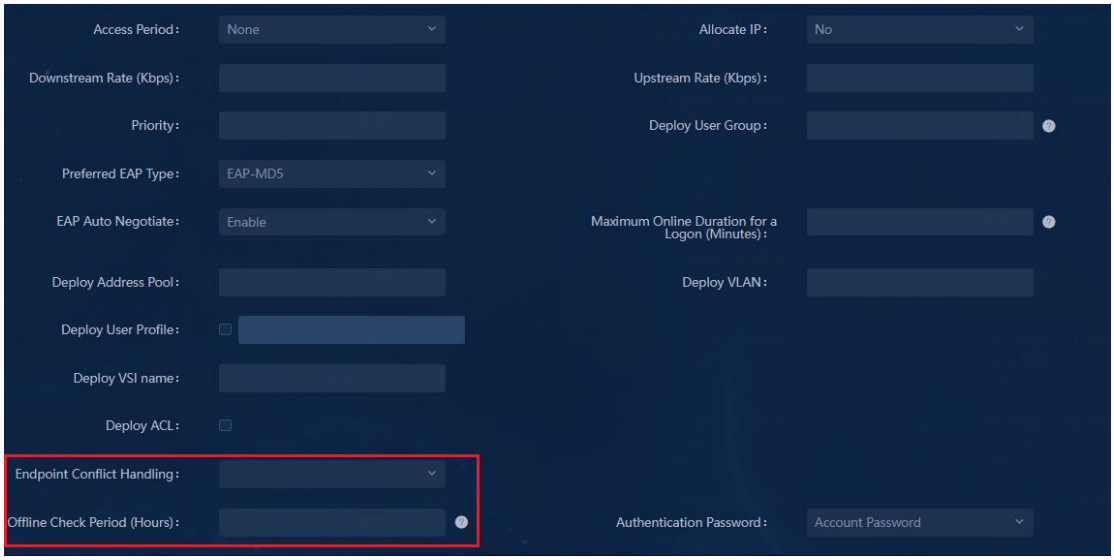


- **Authorization information**: 通常、デフォルト値を設定します。次のパラメーターを構成します。
  - **Allocate IP**: ユーザーに IP アドレスを割り当てるかどうかを選択します。キャンパスネットワークの場合は No を選択します。
  - **Endpoint Conflict Handling:**

    Log Conflict and Continue Authentication: 同じ MAC アドレスを使用する異なるエンドポイントがオンラインになることを要求すると、システムはログを生成し、認証後にエンドポイントがオンラインになることを許可します。

    Reject Authentication: 同じ MAC アドレスを使用する異なるエンドポイントがオンラインになることを要求した場合、システムはユーザーを拒否します。

    Deploy Blackhole MAC: MAC スプーフィングを回避するには、このオプションを選択します。同じ MAC アドレスを使用する別のエンドポイントがオンラインになることを要求すると、システムはそのエンドポイントを拒否し、MAC アドレスをサイレント MAC リストに追加します。
  - **Offline Check Period(Hours)**: パケットを送信しないプリンタなどのミュートエンドポイントをスイッチがログオフしないようにするには、このパラメーターを設定します。スイッチでの MAC 認証のデフォルトのオフライン検出期間は 5 分です。スイッチは、オフライン検出期間内にエンドポイントからのパケットを検出しない場合、エンドポイントをログオフします。認証に合格したエンドポイントがログオフされないように、ARP スヌーピングとともにオフラインチェック期間を設定します。値は 0～596523 の整数です。このパラメーターが 0 に設定されている場合、システムがオフラインにならないことを示します。パラメーターが none の場合、デバイスのオフライン検出期間はデフォルトの 5 分になります。



オフラインチェック期間を 1 時間に設定すると、次の設定がデバイスに展開されます。

```
Slot ID: 1
User MAC address: 0000-0a0b-0001
Access interface: Bridge-Aggregation1023
Username: 00000a0b0001
User access state: Successful
Authentication domain: hz1
IPv4 address: 20.0.0.2
IPv4 address source: IP Source Guard
Initial VLAN: 150
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3
Authorization microsegment ID: 3504
Authorization ACL number/name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Offline detection: 3600 sec (server-assigned) // Deployed offline check period.
Online from: 12/22/2020 9:52:45 AM
Online duration: 0h 3m 2s
Port-down keep online: Disabled (offline)
```

- 認証バインディング情報の次のオプションに注意してください。
  - **Bind User IP**: このオプションを選択して、オンラインエンドポイントをその静的 IP アドレスにバインドします。これを選択すると、エンドポイントユーザーは、バインドされた静的 IP アド

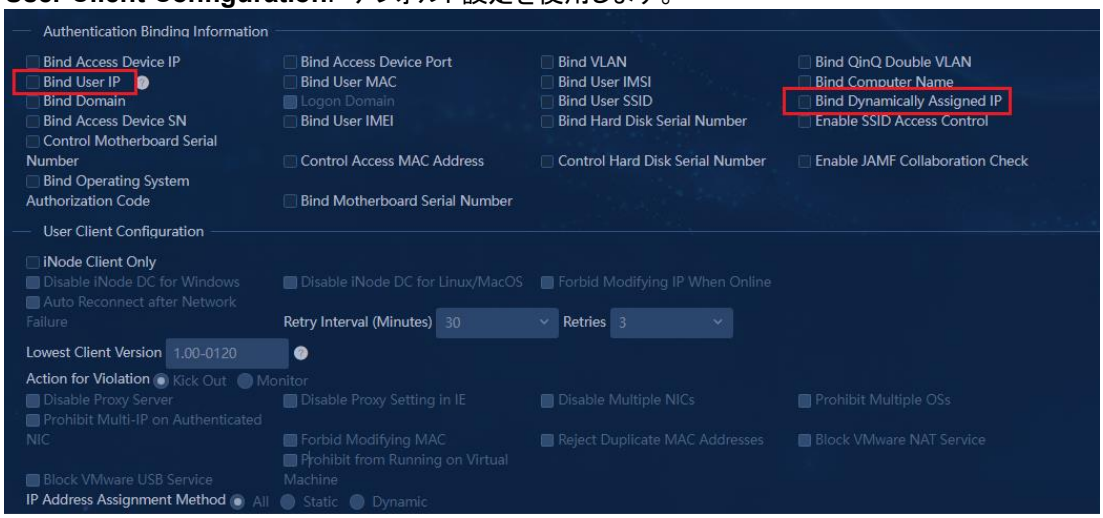
レスをオンラインになった後にユーザー詳細情報に記録します。

– **Bind Dynamically Assigned IP**: このオプションを選択すると、エンドポイントが初めてオンラインになったときに、そのエンドポイントの MAC アドレス、DHCP で割り当てられた IP アドレスおよびアカウント情報がバインドされます。これにより、エンドポイントはオンラインになるたびに同じ IP アドレスを取得できます。

重要:

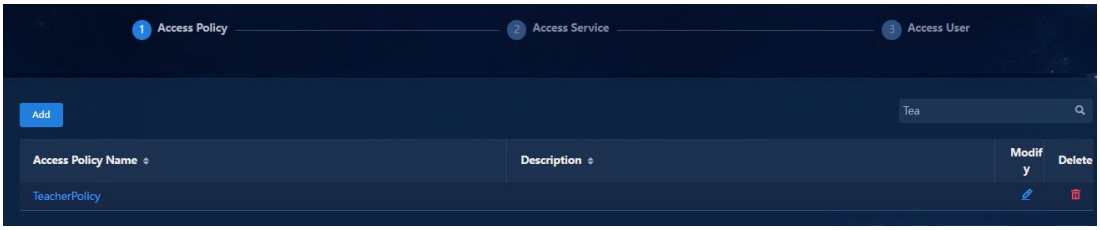
Bind User IP と **Bind Dynamically Assigned IP** は同時に設定できません。

○ **User Client Configuration**: デフォルト設定を使用します。



3. パラメーターを設定したら、**OK** をクリックして設定を保存します。アクセスポリシーがリストに表示されます。

   アクセスポリシーをさらに追加するには、上記の手順を繰り返します。



4. アクセスポリシーを設定したら、**Next** をクリックしてアクセスサービスを設定します。

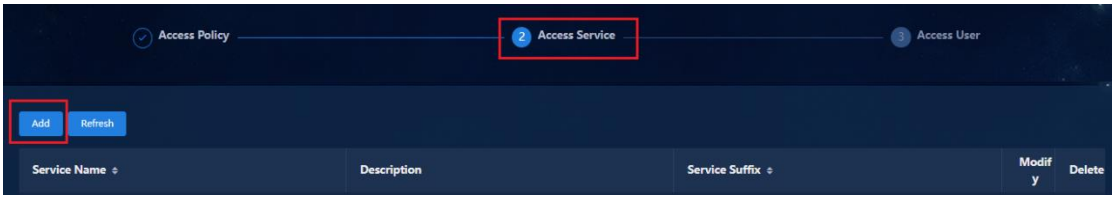
アクセスサービスの設定

2 つのアクセスサービス設定方法は、次のとおりです。このマニュアルでは、Campus ウィザードを使用します。

- キャンパスウィザードモード。**Wizard** > **Campus Wizard** > **User Onboarding Planning** ページに移動し、2 番目のステップ **Access Service Management** で設定します。

- Non-Campus wizard mode: **Automation > User Service > Access Service** ページに移動します。

1. **Add** をクリックして、アクセスサービス設定ページを開きます。



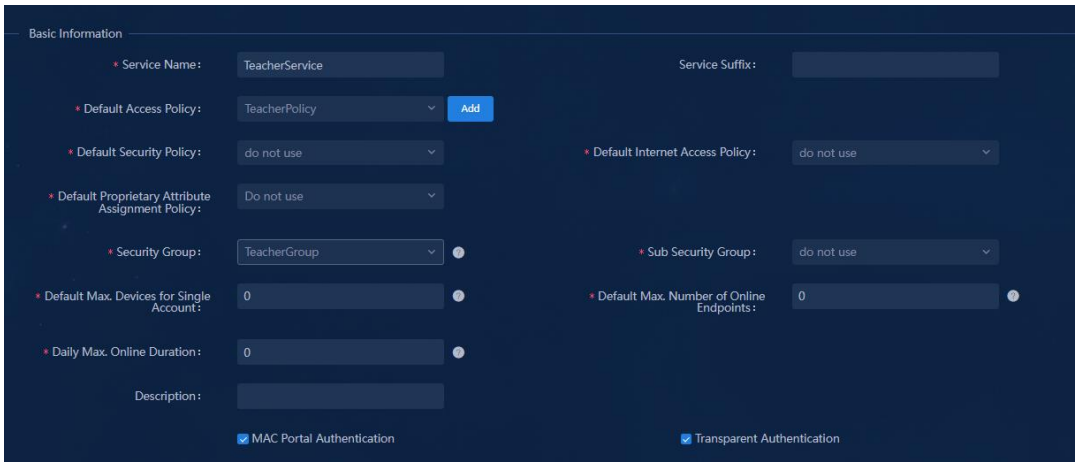
2. 次のパラメーターを設定します。

   Basic Information: サービスの名前を入力し、デフォルトのアクセスポリシーとセキュリティグループを選択し、その他のパラメーターにはデフォルト設定を使用します。

   - 基本情報エリア

     Basic Information 領域のパラメーターの説明:

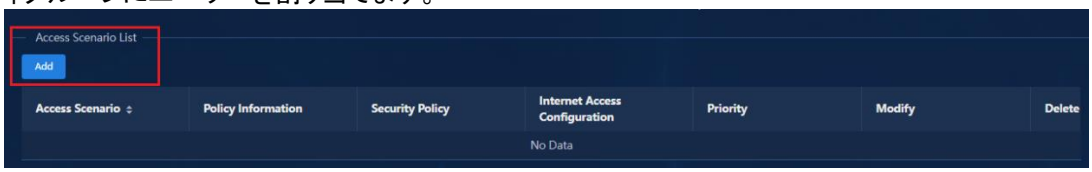
     - サービスグループ: デフォルトでは「グループ解除」に設定されています。デフォルト設定を使用します。
     - **Default Access Policy**: デフォルト設定は **Access Forbid** で、すべてのユーザーがオンラインになれないことを示します。ユーザーがオンラインになることを許可するには、デフォルトアクセスポリシーを構成する必要があります。**Add** をクリックすると、新しいデフォルトアクセスポリシーを追加できます。
     - **Security Group**: このパラメーターは構成する必要があります。ユーザーがオンラインになったら、対応するセキュリティグループを選択します。「Configure access network settings」で作成されたセキュリティグループおよびセキュリティサブグループがドロップダウンリストに表示されます。
     - **Sub Security Group**: オプション。サブセキュリティグループを選択した場合、アクセスサービスはそのサブセキュリティグループに適用されます。サブセキュリティグループを選択しない場合、アクセスサービスはそのセキュリティグループに適用されます。
     - **MAC Portal Authentication/Transparent Authentication**: デフォルトでは、2 つのオプションが選択されています。MAC ポータル認証を使用するユーザーがオンラインになることを許可するには、**MAC Portal Authentication** オプションを選択する必要があります。「≪ 透過認証 **Transparent Authentication** はオプションです。(ユーザーが初めてオンラインになったときにのみユーザーのリダイレクトページを開くには、Transparent Authentication オプションを選択します。ユーザーがオンラインになるたびにユーザーのリダイレクトページを開くには、**Transparent Authentication** オプションを選択しないでください。)



- **Access Scenario List**: オプション。

  アクセスサービスは複数のアクセスシナリオで設定でき、各アクセスシナリオにはセキュリティグループが設定されます。

  ユーザーがオンラインになると、システムは構成されたアクセスシナリオとユーザーを照合し、一致したシナリオで指定されたセキュリティグループにユーザーを割り当てます。ユーザーに一致するものが見つからない場合、システムはデフォルトのアクセスポリシーで指定されたセキュリティグループにユーザーを割り当てます。

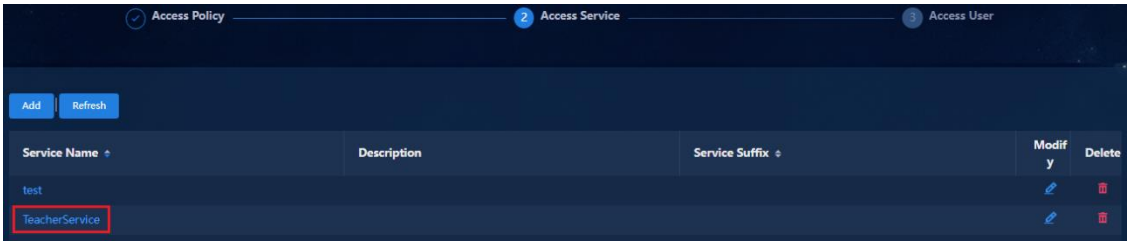


重要:

デバイスが自動的に展開されていないため、構成ウィザードでアクセスシナリオを構成しないことをお薦めします。デバイスが自動的に展開された後、必要に応じてアクセスシナリオを構成できます。

詳細については、「Managing access scenarios (optional)」を参照してください。

3. アクセスサービスを構成した後、追加されたアクセスサービスを表示できます。さらにアクセスサービスを追加するには、上記の手順を繰り返します。



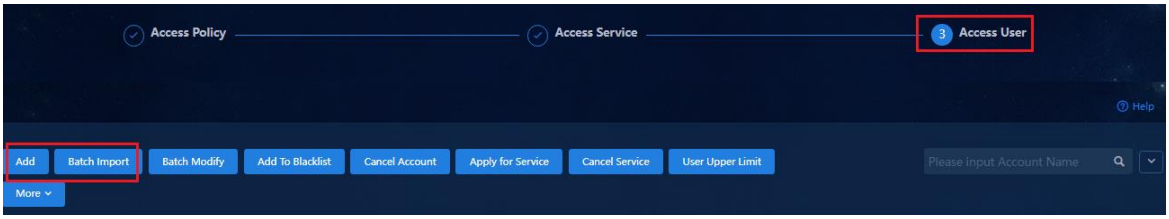
4. アクセスサービスを設定したら、**Next** をクリックしてアクセスユーザーを設定します。

アクセスユーザーの管理

アクセスユーザー管理を設定するには、2 つの方法があります。このドキュメントでは、Campus ウィザードを使用して設定について説明します。

- Campus wizard mode: **Wizard > Campus Wizard > Device Onboarding Planning** ページに移動し、3 番目のステップで **Access User Management** を設定します。
- Non-Campus wizard mode: **Automation > User Service > Access User** ページに移動します。

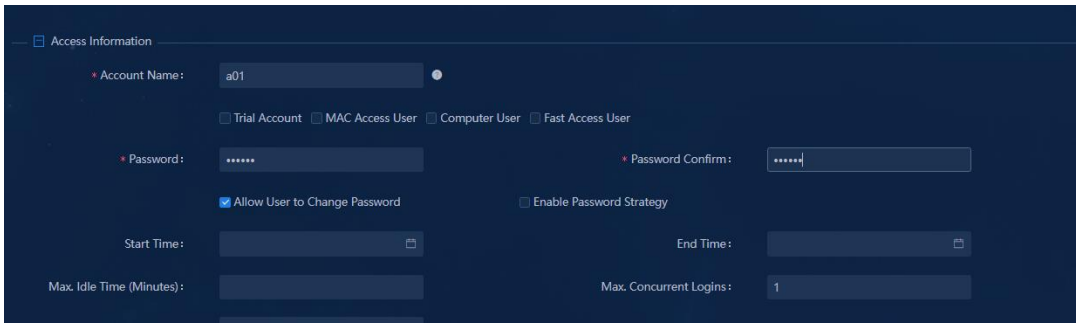
アクセスユーザー管理ページでは、手動追加とバッチインポートの 2 つの構成モードがサポートされています。アクセスユーザーが構成されると、認証サーバーで必要なすべての設定が完了します。自動デバイスオンボーディング後にユーザー認証を実行できます。



ユーザーを手動で追加する

1. **Add** をクリックします。**Add Access User** ページには、基本情報、アクセス情報、アクセスサービス、アクセスデバイスバインディング情報およびエンドポイントバインディング情報が表示されます。
   - **Basic Information**: **User Name** および **Identity Number** を入力します。その他のパラメーターについては、デフォルト値を使用できます。

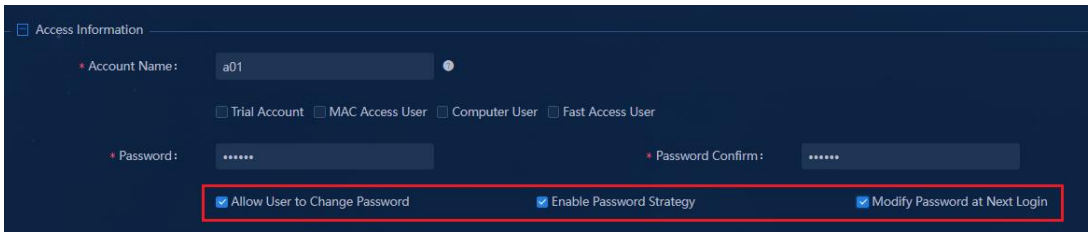
   - **Access Information**: **Account Name** と **Password** を入力します。その他のパラメーターについては、デフォルト値を使用できます。
     - **Max. Idle Time**: このフィールドを空白のままにすると、セッションはタイムアウトしません。
     - **Max. Concurrent Logins**: デフォルト値は 1 です。最大値は 255 です。**Max. Concurrent Login** は、ログインに同じアカウントを使用するエンドポイントの数を指定します。パラメーターの詳細は、「Setting the maximum number of online endpoints supported by an account」を参照してください。



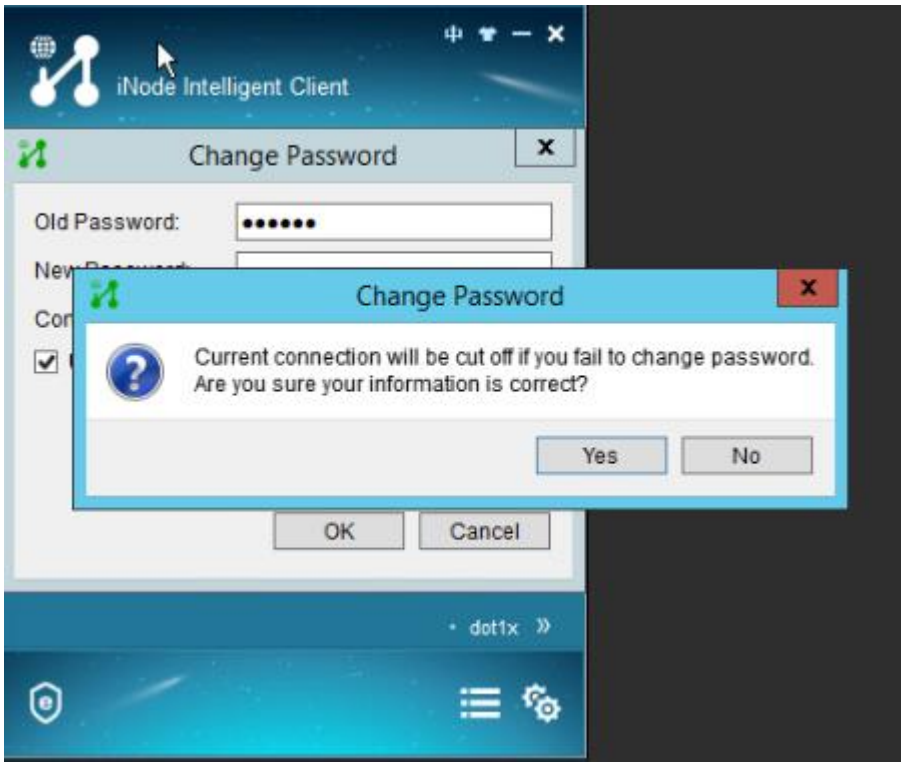
ユーザーパスワードのセキュリティを強化するには、**Allow User to Change Password**、**Enable Password Strategy** および **Modify Password at Next Login** を選択します。これらのオプションを選択すると、ユーザーはログインするたびにパスワードを変更する必要があります。

重要:

Modify Password at Next Login は 1 回かぎりのオプションです。ユーザーがパスワードを変更してシステムに正常にログインすると、このオプションは自動的にクリアされます。ユーザーが再度パスワードを使用する場合は、アクセスユーザーから手動で選択します。



Modify Password at Next Login を選択すると、パスワードを編集するためのページが表示されます。パスワードが正常に編集された後、新しいパスワードを使用してシステムにログインする必要があります。



- **Access Service**: 各アクセスユーザーは、アクセスサービスにバインドされている必要があります。認証に合格すると、ユーザーはアクセスサービスのセキュリティグループ内のネットワークリソースにアクセスできます。

- **Binding Information**: デフォルトでは、すべてのフィールドが空です。デフォルト設定を使用できます。

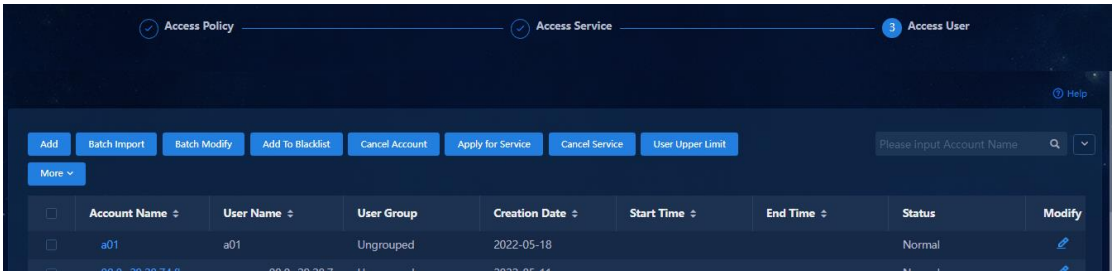
  バインド情報は手動で入力できます。フィールドに複数の値を入力する場合は、キャリッジリターンを使用して値を区切ります。

  システムは、アクセスサービスとアクセスポリシーの設定に基づいて、バインディング情報を自動的に指定することもできます。

重要:

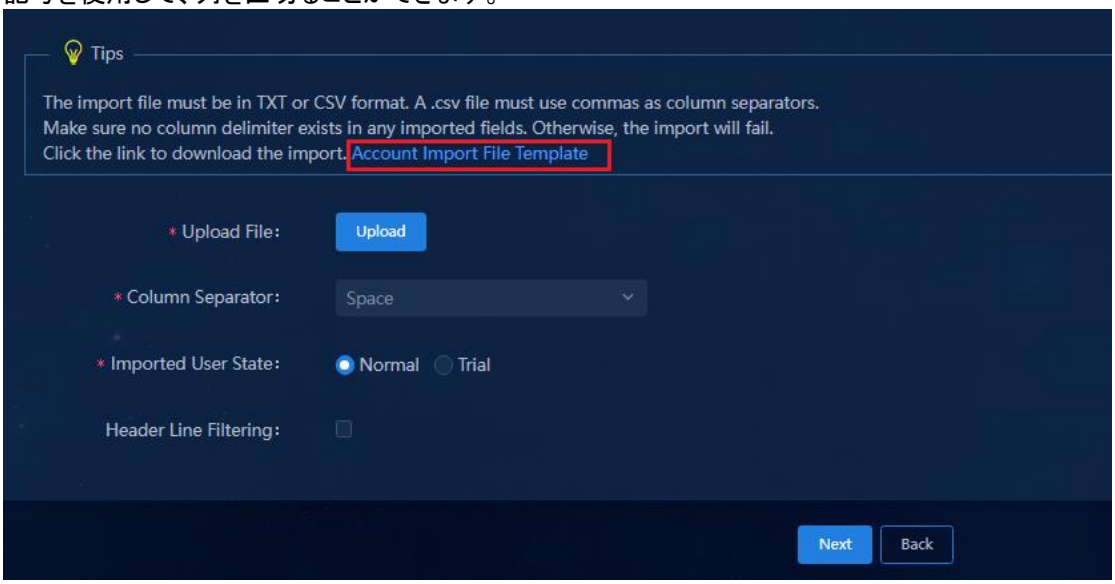
ユーザーバインディング情報で指定された IP アドレスは、「Configure access policies」の **Bind User IP Address** の IP アドレスと一致する必要があります。アクセスポリシーで **Bind User IP Address** を選択しない場合、「バインディング情報」列で指定された IP アドレスは有効になりません。

2. **OK** をクリックします。**Access User** ページで、正常に作成されたユーザーを表示できます。



ユーザーのバッチインポート

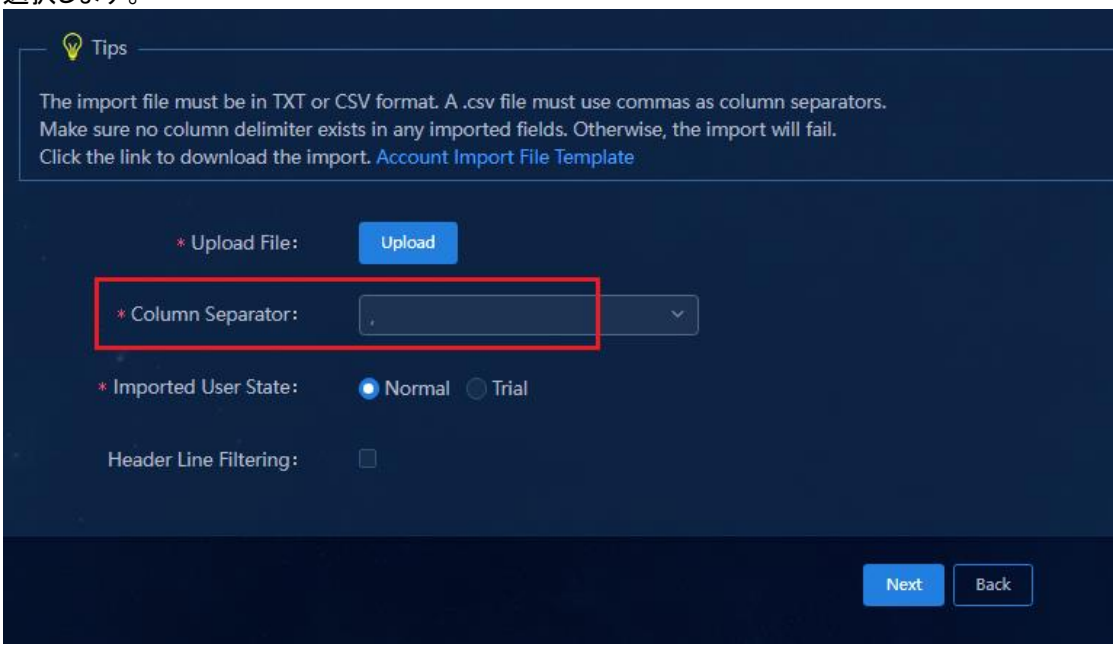
1. **Batch Import** ボタンをクリックして、バッチインポートページを開きます。**Account Import File Template** をクリックして、テンプレートをダウンロードします。**Tab** キーまたはカンマ(,)などの区切り記号を使用して、列を区切ることができます。



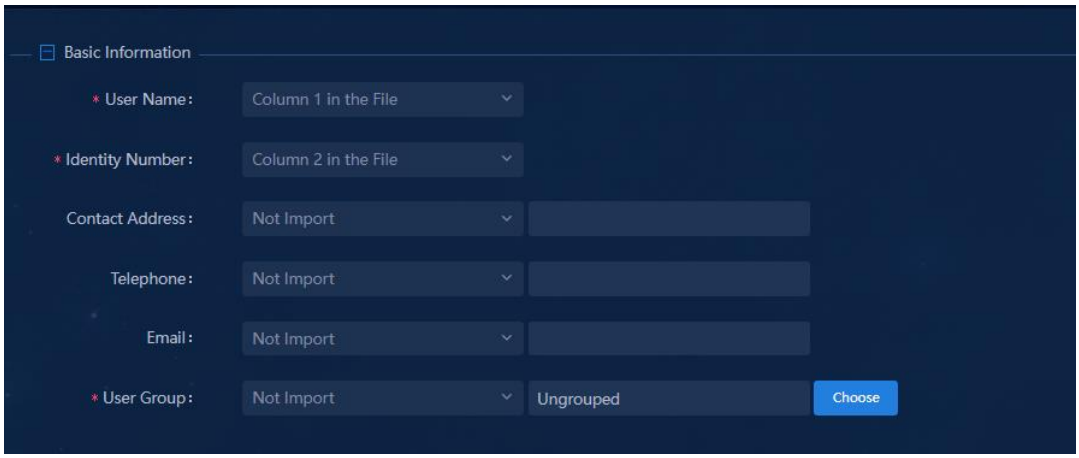
この例では、次の図に示すように、一括インポートのファイル形式は EXCEL です。

a10	21412354	a10	123456
a11	21412355	a11	123456
a12	21412356	a12	123456
a13	21412357	a13	123456
a14	21412358	a14	123456
a15	21412359	a15	123456
a16	21412360	a16	123456
a17	21412361	a17	123456
a18	21412362	a18	123456
a19	21412363	a19	123456
a20	21412364	a20	123456
a21	21412365	a21	123456
a22	21412366	a22	123456
a23	21412367	a23	123456
a24	21412368	a24	123456

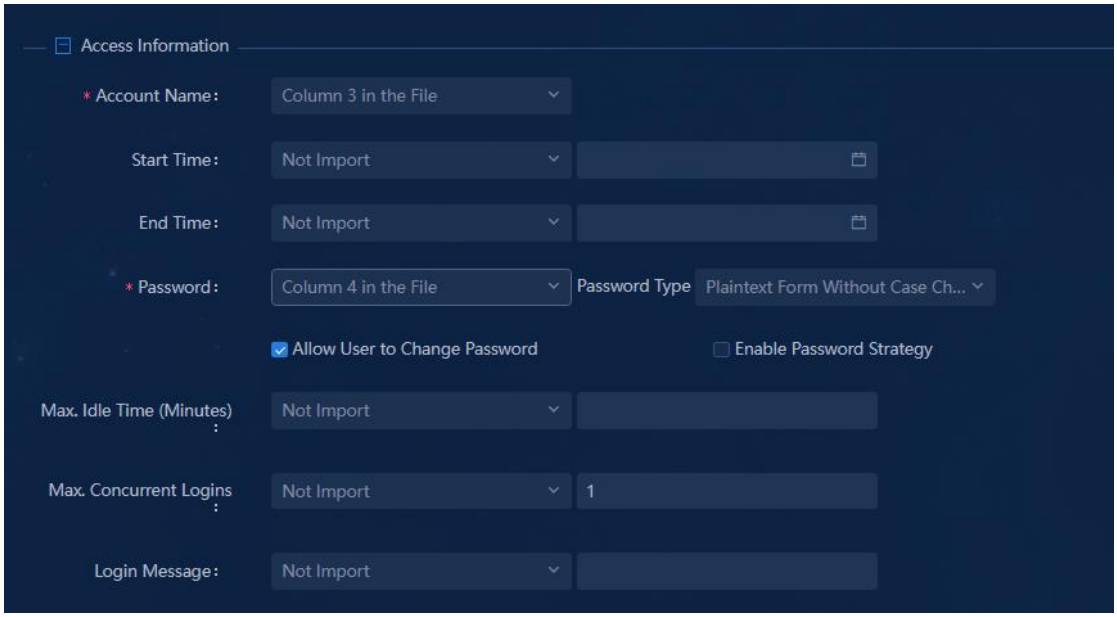
2. **Upload** をクリックします。ファイルと区切り文字を選択します。**Imported User State** で **Normal** を選択します。



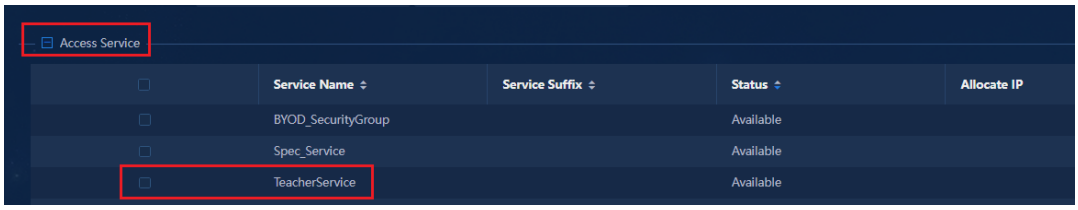
3. **Next** をクリックして、バッチインポート設定ページを開きます。
   - **Basic Information** ページで **User Name** と **Identity Number** を設定し、**User Group** を選択します。



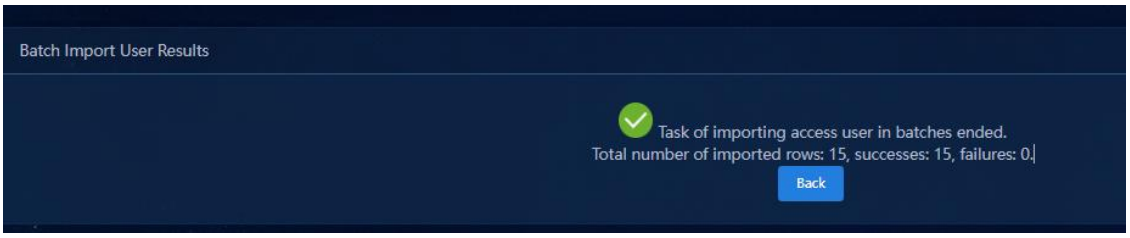
- **Access Information** 領域で、**Account Name** と **Password** を設定します。パスワードはファイルから選択することも、直接入力することもできます。パスワードを直接入力すると、すべてのユーザーが同じパスワードを使用します。



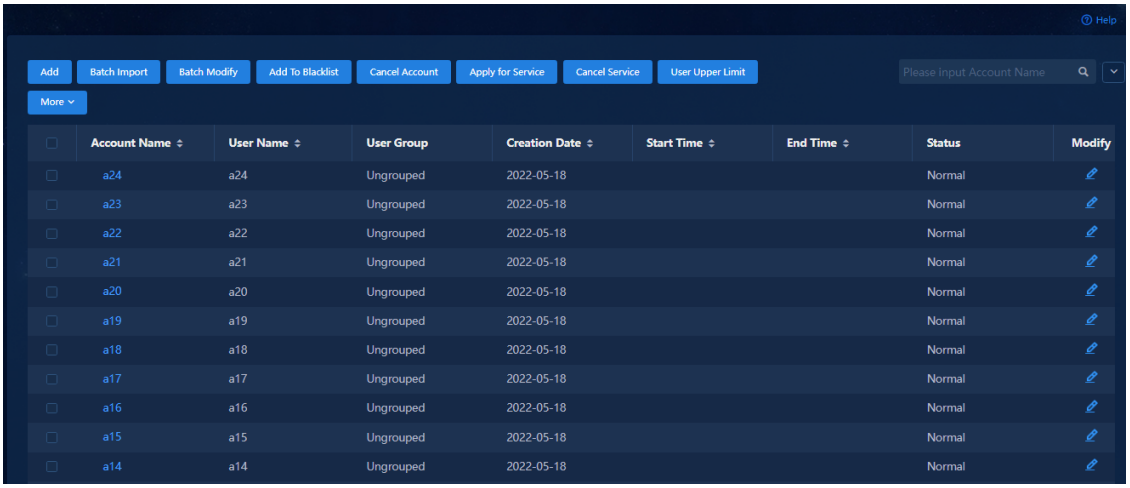
- **Access Service** フィールドで **Access Service** を選択します。これは必須フィールドです。



4. 設定が完了したら、**OK** をクリックしてユーザーをバッチインポートします。



5. ユーザーが正常にインポートされたら、**Access Users** ページでインポートされたユーザーを表示できます。

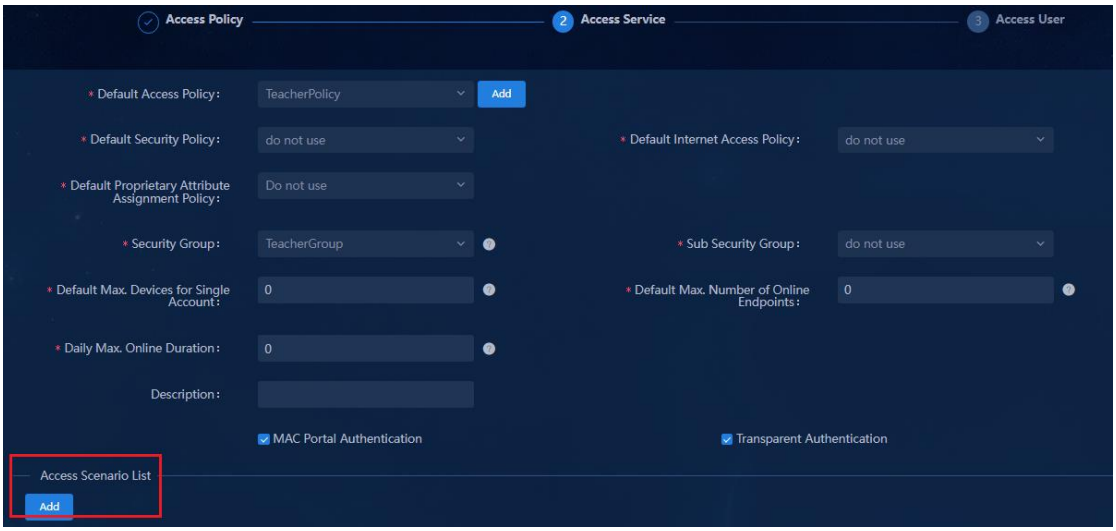


アクセスシナリオの管理(オプション)

1. **Automation** > **User Service** > **Access Service** にナビゲートします。**Edit Access Service** ページをクリックし、**Access Scenario List** で **Add** をクリックします。アクセスシナリオは、次の 2 つの方法で追加できます。

   - 対応する **Action** 列をクリックして、アクセスサービスを編集するためのページを開きます。**Access Scenario List** 列の **Add** をクリックして、ページにアクセスシナリオを追加します。
   - **Add** をクリックして、アクセスサービスを追加するためのページを開きます。**Access Scenario List** 列の **Add** をクリックして、ページにアクセスシナリオを追加します。

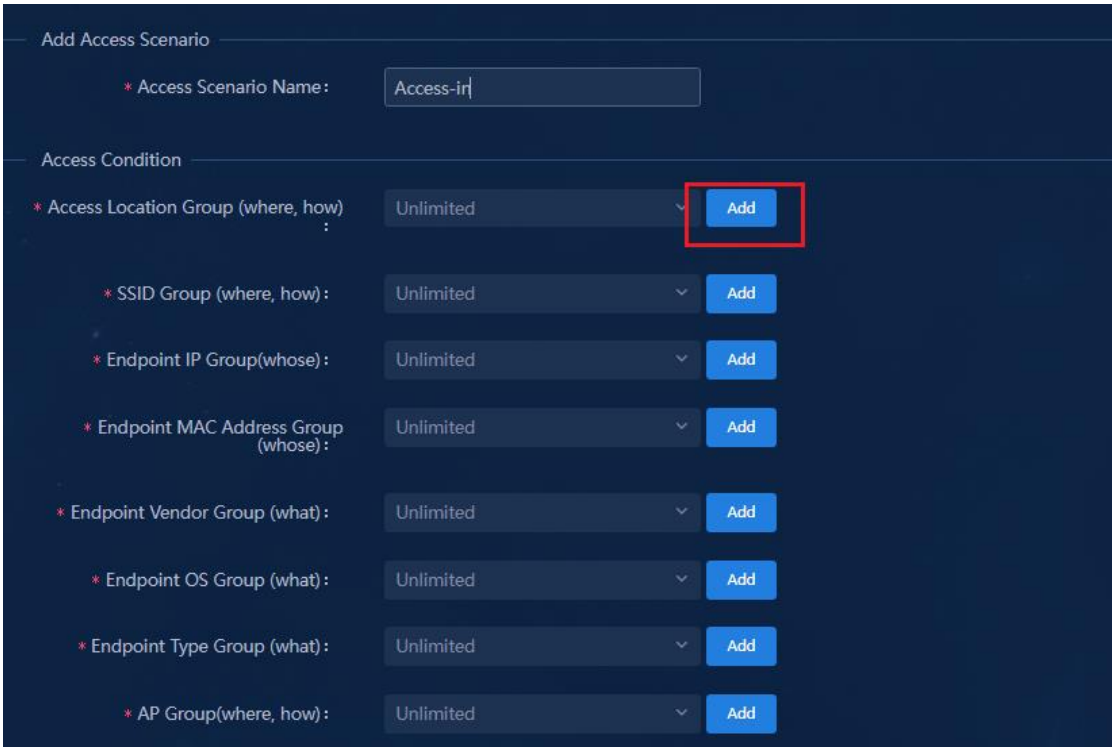
   ユーザーがオンラインになると、システムは構成されたアクセスシナリオとユーザーを照合し、一致するシナリオで指定されたセキュリティグループにユーザーを割り当てます。ユーザーに一致するものが見つからない場合、システムはデフォルトのアクセスポリシーで指定されたセキュリティグループにユーザーを割り当てます。



2. Who、Whose、What、When、Where、および How(5W1H)に基づいてアクセス条件を設定します。

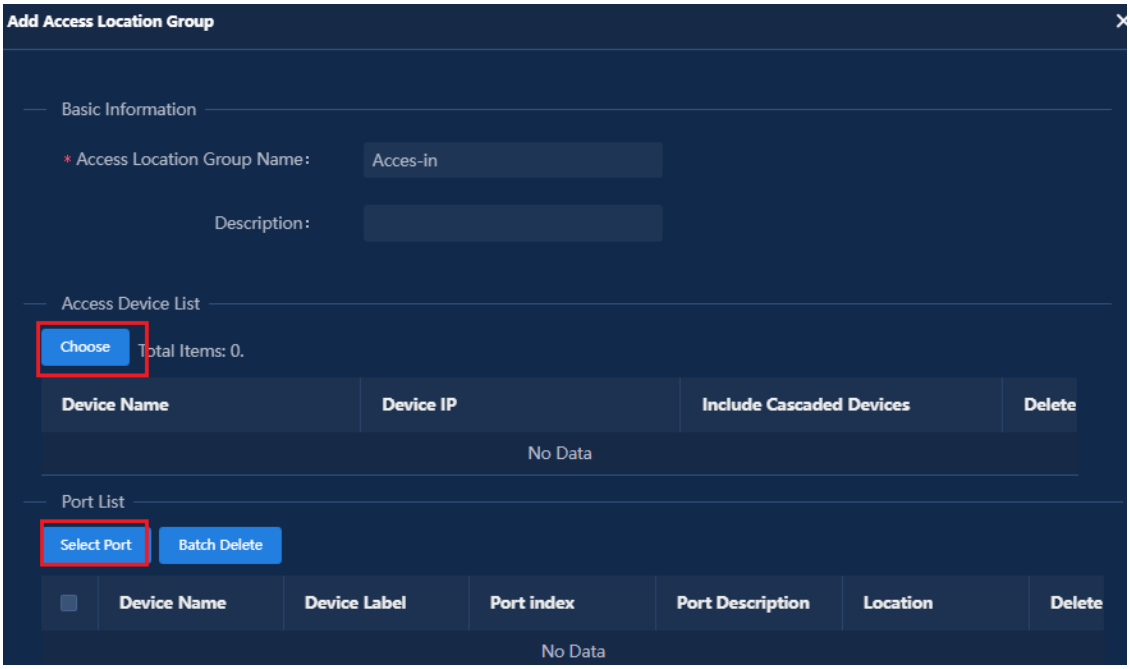
   5W1H に基づくユーザー認証は、Who、Whose(誰のデバイス)、What(どのデバイス)、When、Where、How などの次元に応じて様々なアクセスシナリオをカバーすることができ、ユーザーはニーズに応じて柔軟にシナリオをカスタマイズすることができる。

   たとえば、アクセスロケーショングループを設定するには、**Access Location Group**(Where, How)の Add をクリックして、アクセスロケーショングループを追加するためのページを開きます。スイッチにアクセスする場所、つまり 5W1H の「Where」を選択する必要があります。

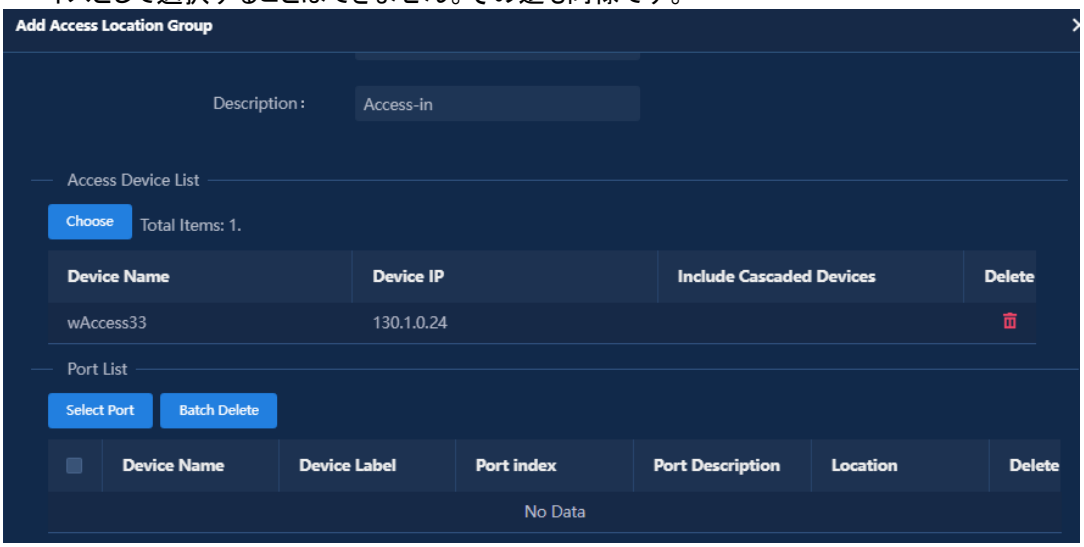


3. アクセスロケーショングループを追加するページで、アクセスデバイスまたはインターフェイスを選択します。基本パラメーターを設定し、アクセスデバイスまたはインターフェイスを選択して、Confirm を

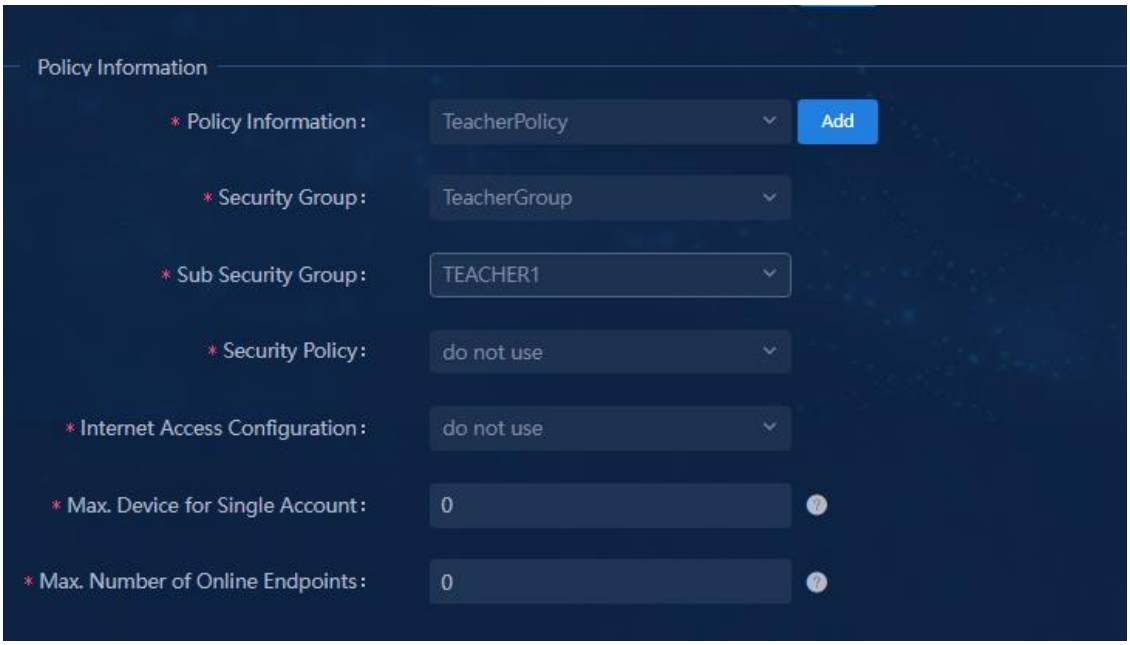
クリックします。

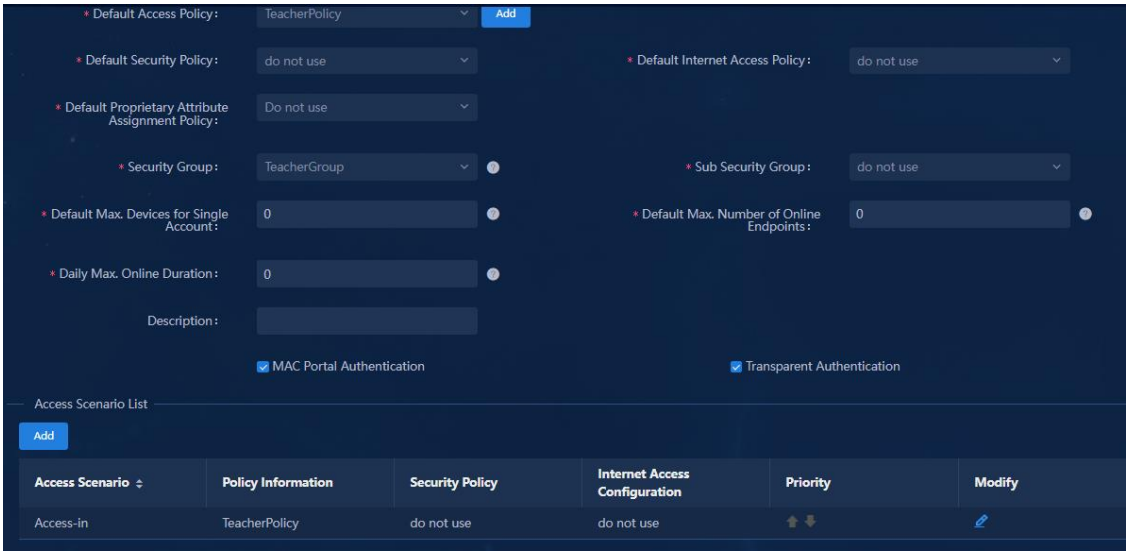


- リーフデバイス、アクセスデバイスまたはカスケードアクセスデバイスを選択できます。リーフデバイスを選択する場合は、カスケードアクセスデバイスを含めるかどうかを選択できます。
- リーフデバイスおよびアクセスデバイス上の特定のインターフェイスを選択できます。デバイスをアクセスデバイスとして選択した場合、そのデバイス上のインターフェイスをアクセスインターフェイスとして選択することはできません。その逆も同様です。



4. アクセスシナリオ構成ページで、アクセスポリシーパラメーターを構成し、Confirm をクリックしてアクセスシナリオの構成を終了します。構成したアクセスシナリオがアクセスシナリオリストに表示されます。

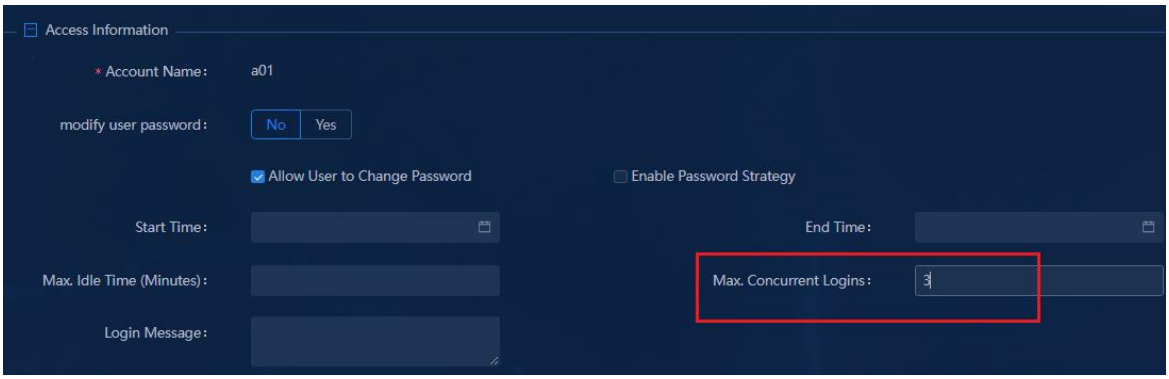




アカウントでサポートされるオンラインエンドポイントの最大数の設定

アカウントでサポートされるオンラインエンドポイントの最大数の設定

Max. Concurrent Logins パラメーターでは、ログインに同じアカウントを使用するエンドポイントの数を指定します。**Automation** > **User Service** > **Access User** > **All Access Users** ページにナビゲートします。たとえば、このパラメーターの値を 3 に設定すると、このアカウントを使用する最大 3 つのエンドポイントを同時にオンラインにできます。



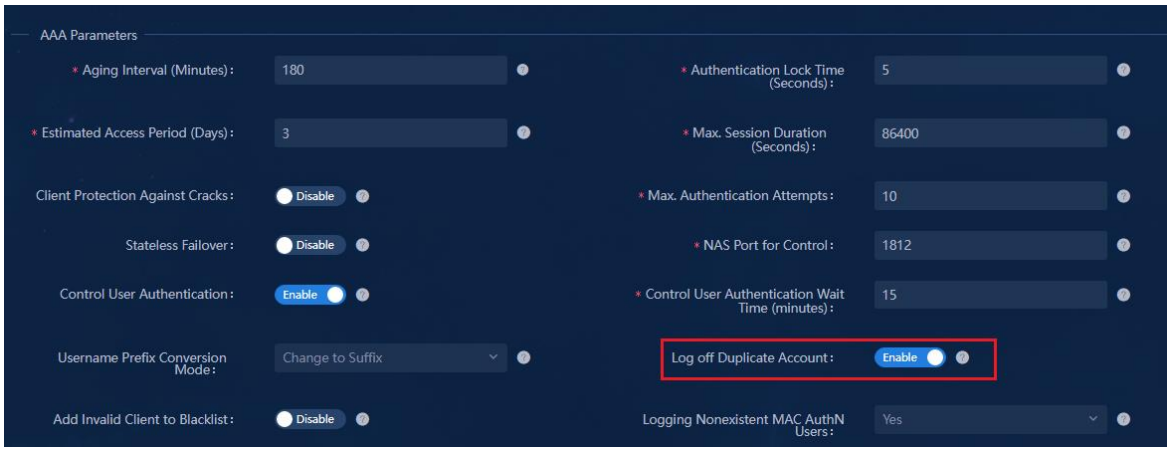
Max. Concurrent Logins パラメーターは、**Log Off Duplicate Account** および **Max. Device for Single Account** に関連付けられています。**Max. Device for Single Account** のパラメーターの説明については、「Configure user endpoint setting parameters」を参照してください。

重複するアカウントのログオフ

Automation > **User** > **Access Parameters** > **System Settings** ページに移動し、システムパラメーター設定の **Actions** カラムをクリックします。

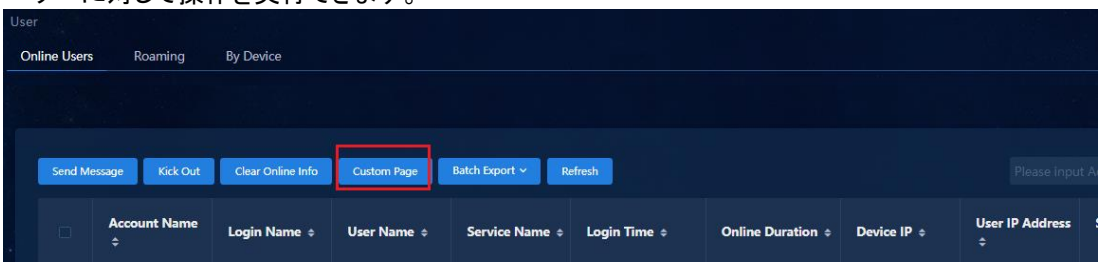
Log Off Duplicate Account パラメーターは、**Max. Concurrent Logins** パラメーターの値が 1 の場合にのみ有効になります。

- **Log Off Duplicate Account** を **Enable** に設定した場合:
  - **Max. Concurrent Logins** パラメーターの値が 1 の場合、2 つのエンドポイントが同じアカウントを使用してオンラインになると、システムはオンラインになった最初の認証済みエンドポイントを強制的にログアウトします。
  - **Max. Concurrent Logins** パラメーターの値が 1 より大きい場合は、**Log Off Duplicate Account を Enable** に設定しても、2 番目のエンドポイントはオンラインになりません。
- **Log Off Duplicate Account** を **Disable** に設定した場合:
  - **Max. Concurrent Logins** パラメーターの値が 1 の場合、2 つのエンドポイントが同じアカウントを使用してオンラインになると、2 番目のエンドポイントはオンラインになりません。

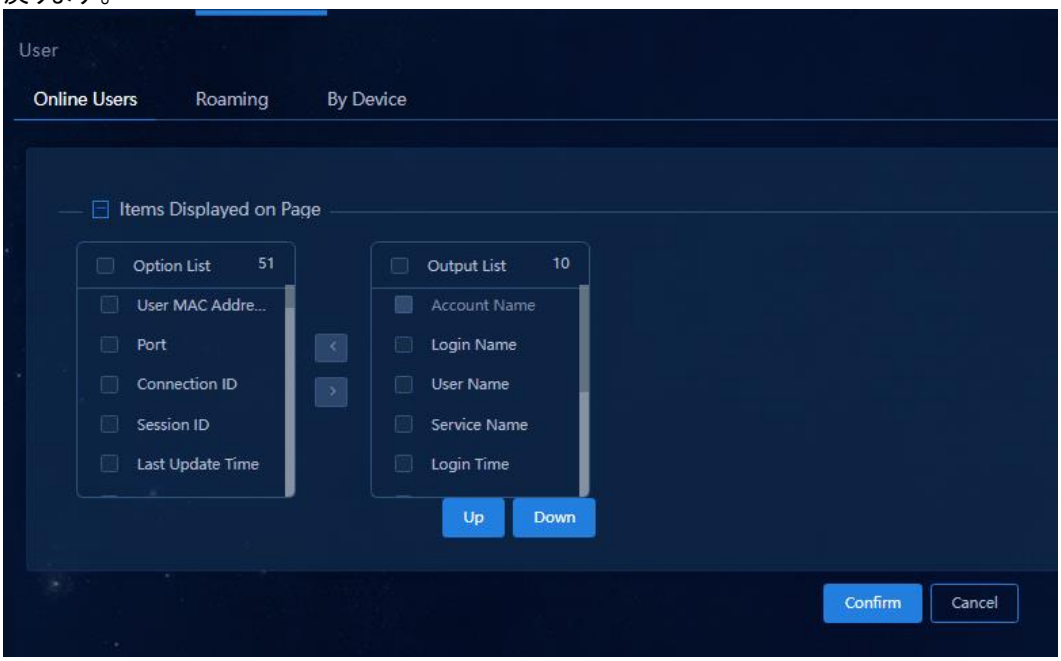


オンラインユーザーの管理

1. **Monitor** > **Monitor List** > **User** > **Online Users** ページにナビゲートします。すべてのオンラインユーザーがリストに表示されます。対応するボタンをクリックして、メッセージの送信、強制ログアウト、オンライン情報の消去、再認証、ページのカスタマイズ、一括エクスポートなど、オンラインユーザーを管理できます。詳細情報の表示、ログの収集、ブラックリストへの登録など、任意のオンラインユーザーに対して操作を実行できます。



2. **Custom Page** をクリックすると、オンラインユーザーリストに表示する情報をカスタマイズできます。**Add** をクリックして、プッシュポリシーを追加するページを開きます。**Option List** でアイテムを選択し、›ボタンをクリックして、選択したアイテムを Output List に追加します。‹ボタンをクリックして、**Output List** から不要なオプションを削除することもできます。削除したオプションは **Option List** に戻ります。



ユーザー認証

0 エンドポイントユーザーが認証を通過してオンラインになる前に、「AD-Campus configuration」で説明されている基本設定を完了する必要があります。この設定には、次の項目が含まれます。

- デバイスポリシーテンプレート(AAA、MAC 認証、802.1X 認証、および MAC 移動テンプレートを含む)およびインターフェイスグループテンプレート(MAC 認証および 802.1X 認証テンプレートを含む)。設定は、リーフデバイスグループおよびリーフダウンリンクインターフェイスグループに対して発行されます。
- プライベートネットワーク、セキュリティグループ、アクセスポリシー、およびアクセスユーザーの設定。

802.1X認証を設定する

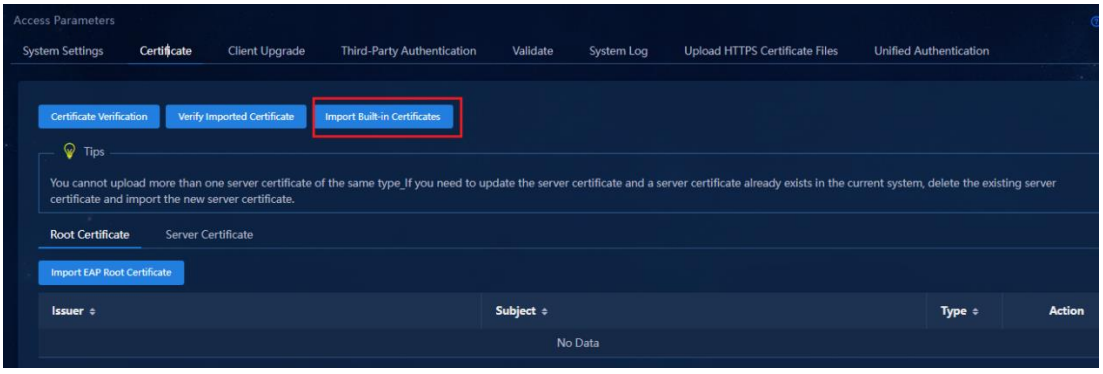
上記の設定が完了すると、802.1X 認証ソフトウェアを使用してユーザーを認証できます。

証明書をインストールする

注:

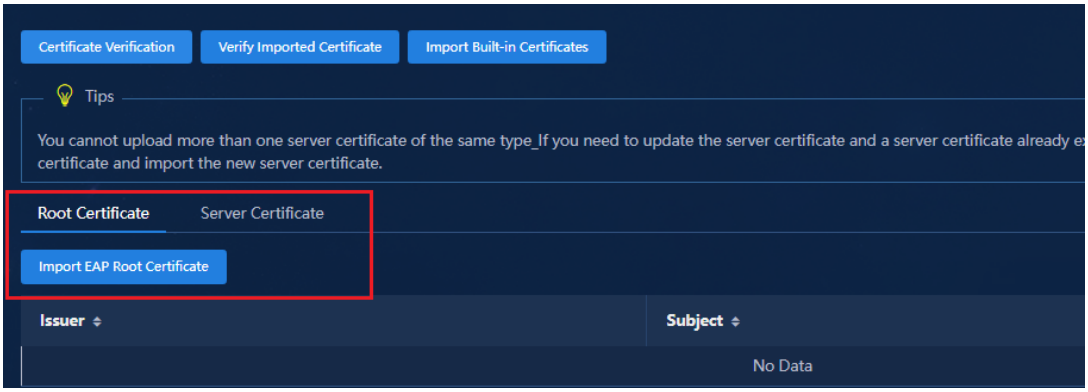
- H3C iNode クライアントを使用して DOT1X 認証を開始する場合、証明書は必要ありません。
- H3C iNode クライアントを使用しない場合は、EIA 認証サーバーに証明書をインストールする必要があります。証明書は、非 H3C 802.1X クライアント(たとえば、Windows の組み込み 802.1X クライアントや携帯電話の Wi-Fi クライアント)が正常に認証されることを保証します。

1. **Automation > User > Access Parameters > Certificate** ページに移動し、**Import Built-in Certificate** をクリックして、H3C 組み込み証明書をインポートします。設定後、802.1X 認証を開始する非 H3C iNode クライアントを正常に認証できます。



2. クライアントが非 H 3 C 証明書を使用する場合、クライアントは次の 2 つの方法で証明書をインポートできます。

- **Root Certificate** タブを選択し、**Import EAP Root Certificate** をクリックして証明書をインポートします。
- **Server Certificate** タブを選択し、**Import EAP Root Certificate** をクリックして証明書をインポートします。

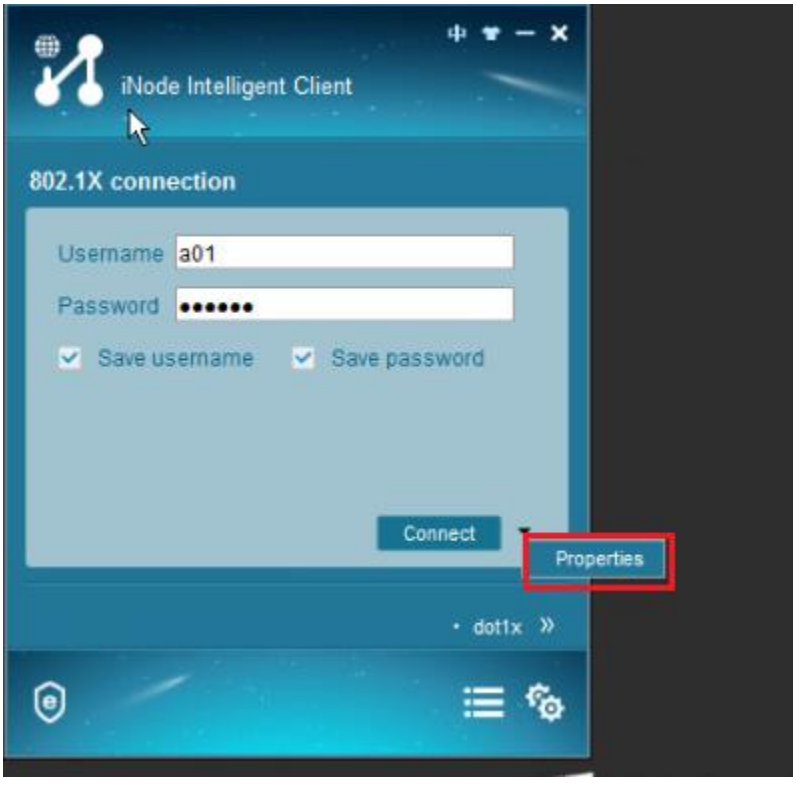


802.1X 認証を開始する

iNode クライアント

次の例では、H3C iNode クライアントを使用してユーザー認証を記述します。

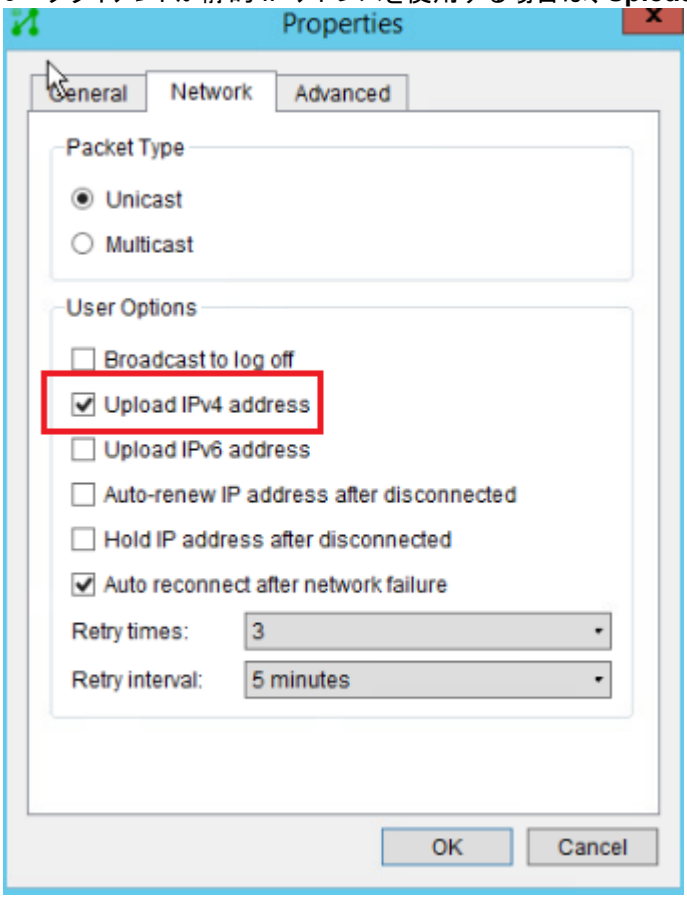
1. iNode クライアントを起動し、ユーザー名とパスワードを入力します。



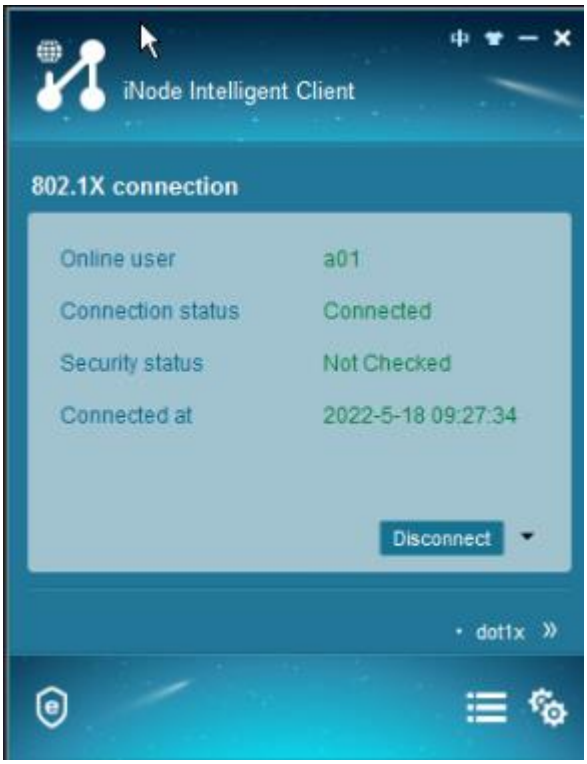
2. **Properties** を設定します。接続の横にある逆三角形をクリックし、**Properties** をクリックします。

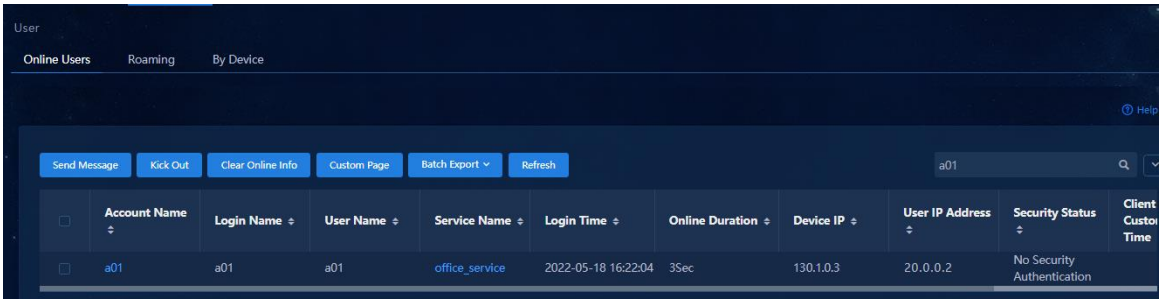
Properties ダイアログボックスの **Network** タブで、次のパラメーターを構成します。

- 認証をトリガーするパケットタイプとして **Unicast** または **Multicast** を選択します。
- クライアントが静的 IP アドレスを使用する場合は、**Upload IPv4 Address** を選択します。



3. **Connect** をクリックすると、エンドポイント PC でユーザーが正常にオンラインになったことを確認できます。**Monitor > Monitor List > User > Online Users** ページでオンラインユーザー情報を確認することもできます。



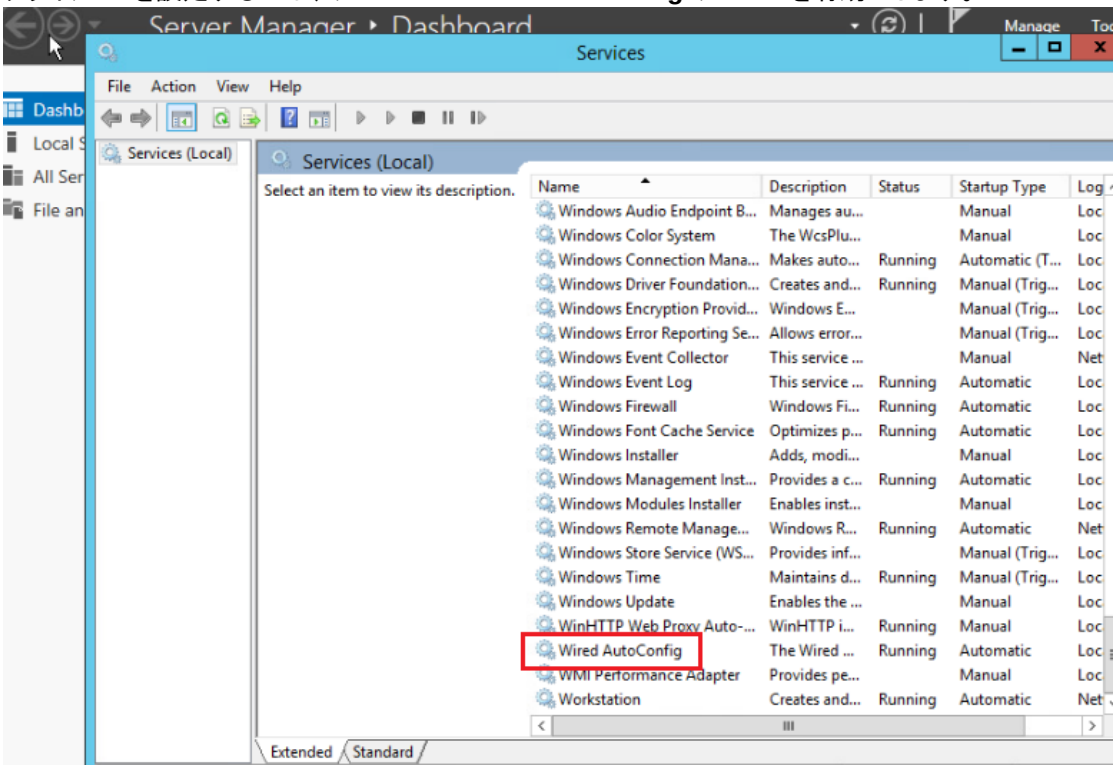


クライアントとしての非 H 3 C iNode

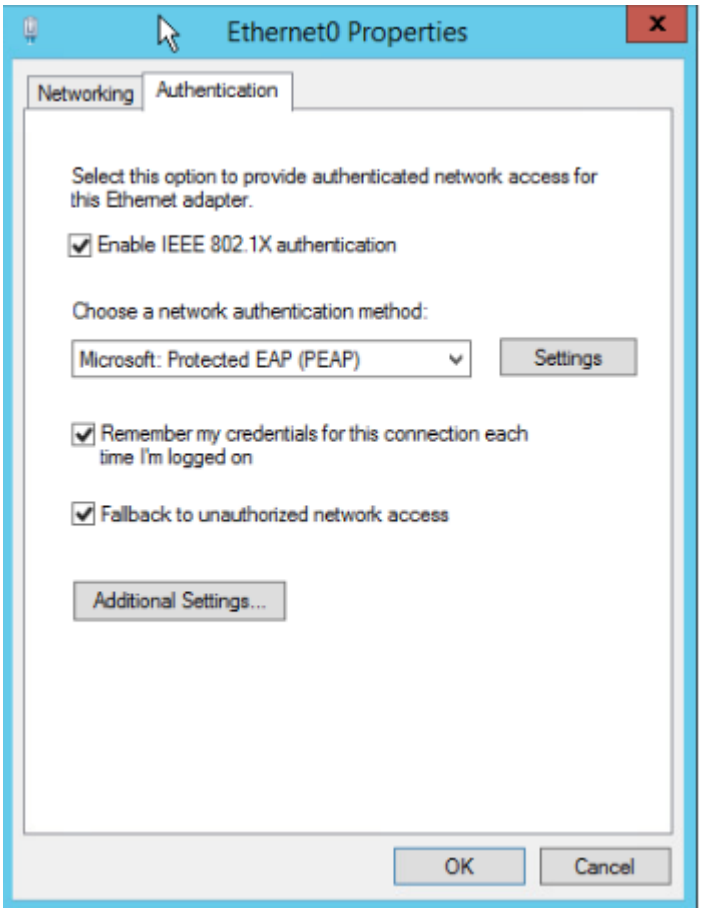
1. デバイスポリシーテンプレート:802.1X 認証。EAP 認証モードを選択します。詳細については、「Device policy template - 802.1X authentication」を参照してください。
2. リーフダウンリンクインターフェイスでハンドシェイク機能をディセーブルにする設定については、「Customizing a policy template」を参照してください。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 mac-based ac
 dot1x
 Undo dotlx handshake   //  Disable the shakehand function.
 undo dot1x multicast-trigger
#
```

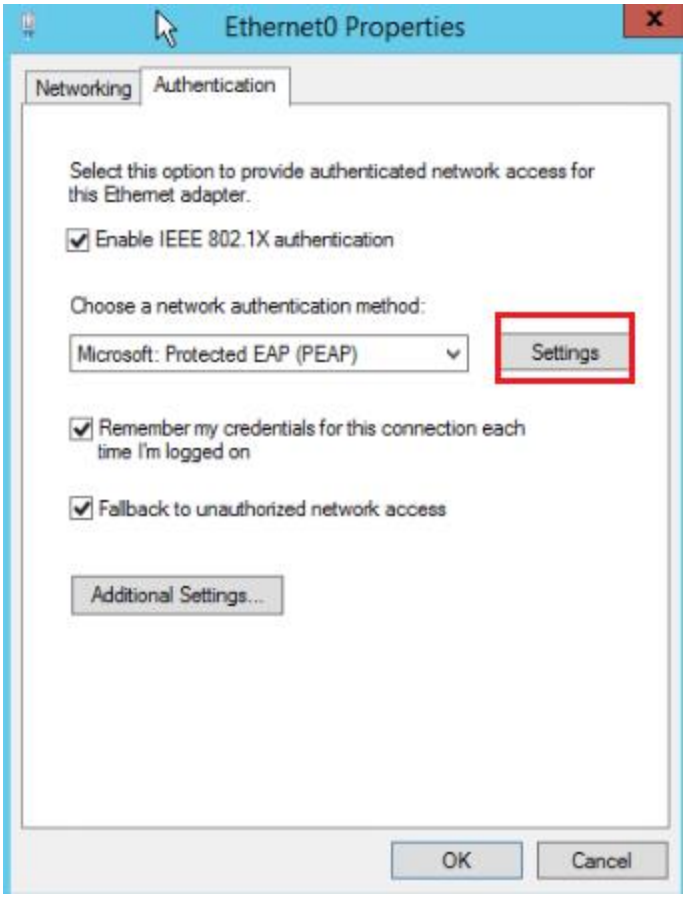
3. クライアントを設定するには、サービスで **Wired AutoConfig** サービスを有効にします。

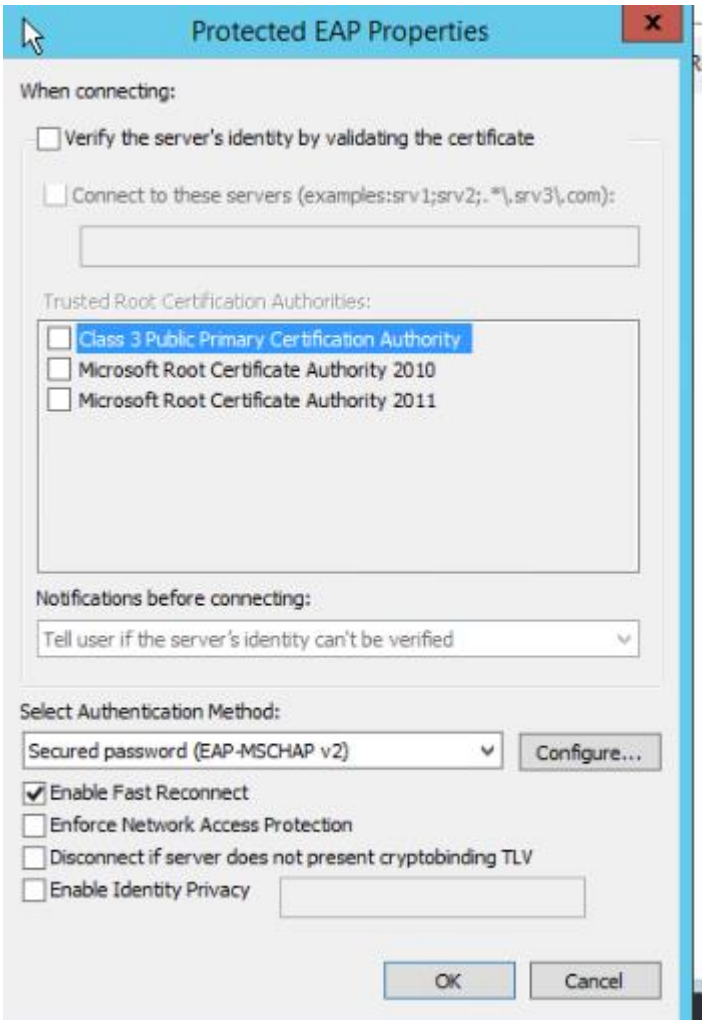


4. **Network Card > Properties > Authentication** ページで、**Enable 802.1X authentication** および **Fallback to unauthorized network access** を選択します。

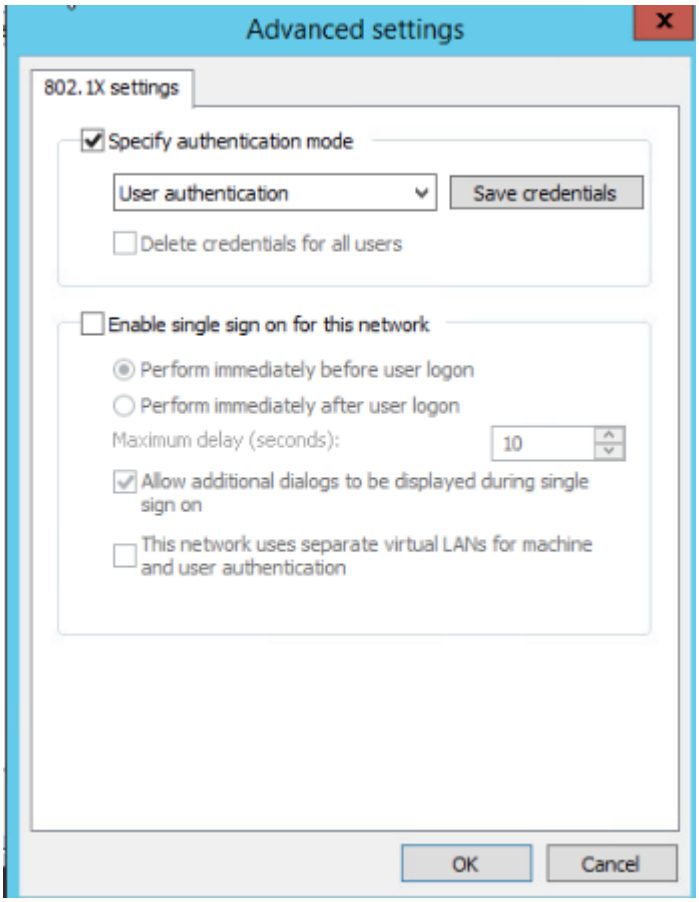


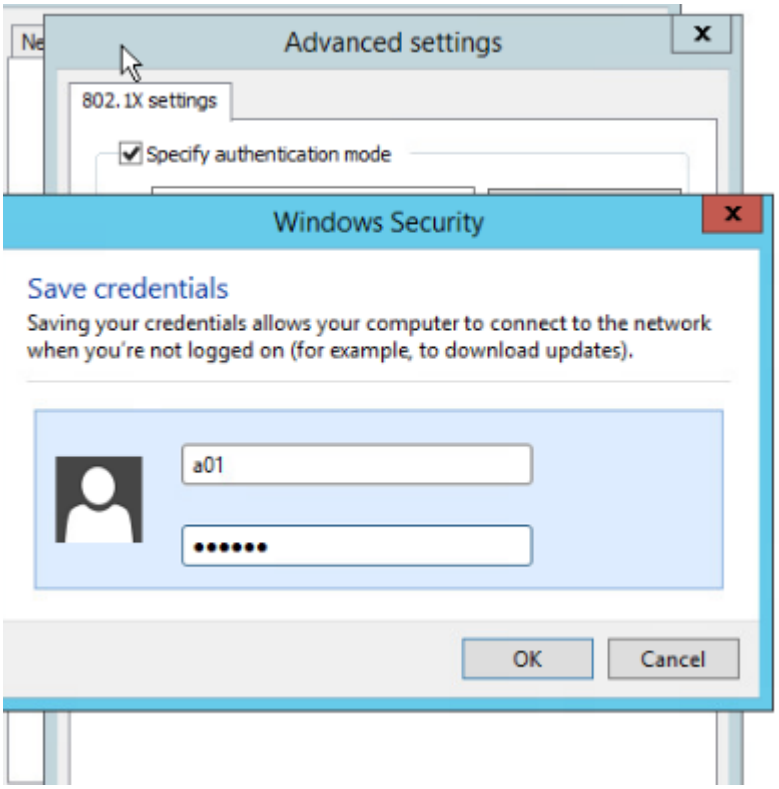
5. **Network Card** > **Properties** > **Authentication** > **Settings** ページで、証明書を検証してサーバーの ID を確認し、その他のパラメーターにはデフォルト設定を使用する(**Verify the Server's identity by validating the certificate**)を選択します


Ethernet0 Properties
Networking
Authentication
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Cancel



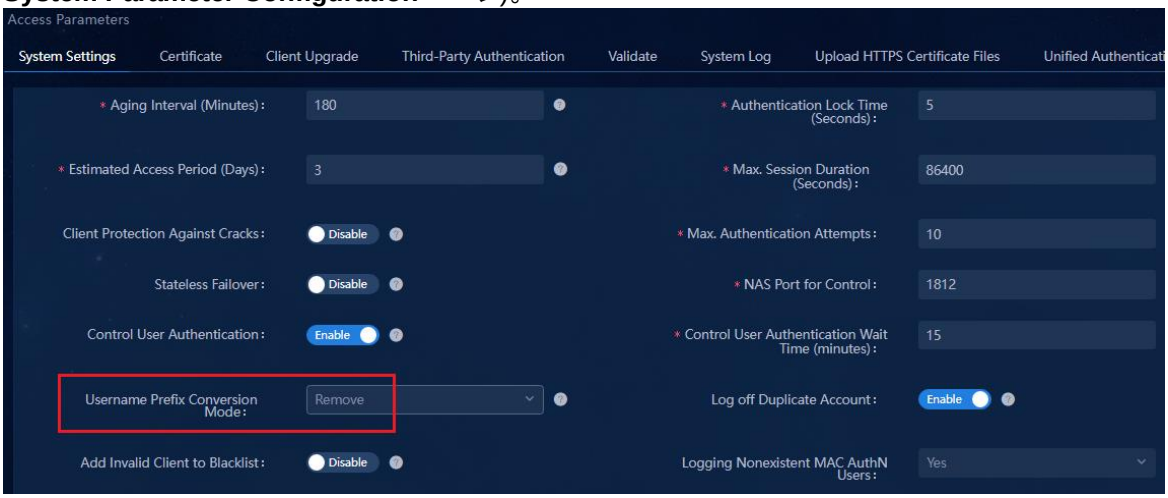
6. **Network Card** > **Properties** > **Authentication** > **Advanced Settings** ページで、**Specify authentication mode** を選択し、ドロップダウンボックスで **User authentication** を選択します。**Save credential** ページで認証ユーザー名とパスワードを入力します。





7. 設定後、ユーザーは正常に認証されます。

8. 特定のエンドポイントが認証されると、それらのエンドポイントは、ユーザーが存在しないというメッセージとともに認証の失敗を引き起こすプレフィクス情報を伝送します。この問題を解決するには、AAA 認証を設定し、サフィックスを持つドメイン名を追加します。詳細については、「Device policy template-AAA」を参照してください。さらに、ユーザー名プレフィクス変換方式を変更して、プレフィクス情報を削除できます(**Automation > User > Service Parameters > Access Parameters > System Parameter Configuration** ページ)。



MACポータル認証の設定

MAC ポータル認証は、主にクライアントのないユーザーに適用されます。認証用のユーザー名またはパスワードを直接入力することはできません。ユーザーがネットワークアクセスを要求したときに MAC ポータル認証ページをユーザーにプッシュすると、ユーザーは認証用のページにユーザー名とパスワードを入力できます。

第 1 段階:ユーザーのエンドポイントがアクセススイッチのポートに接続され、ポートがアップ状態になると、エンドポイントは MAC アドレスを含むパケットを送信して MAC 認証をトリガーします。スイッチはユーザーを BYOD 匿名ユーザーとして識別します。ユーザーエンドポイントは、セキュリティグループに指定されたサブネットから IP アドレスを取得します。

第 2 段階:ユーザーが Web ページを開くと、アクセススイッチは MAC ポータル認証ページにリダイレクトします。ページで、ユーザー名とパスワードを入力します。ユーザーが正常にログインすると、ユーザーは関連付けられたユーザーセキュリティグループに追加されます。次に、ユーザーエンドポイントは、ユーザーセキュリティグループに指定されたサブネットから IP アドレスを取得します。

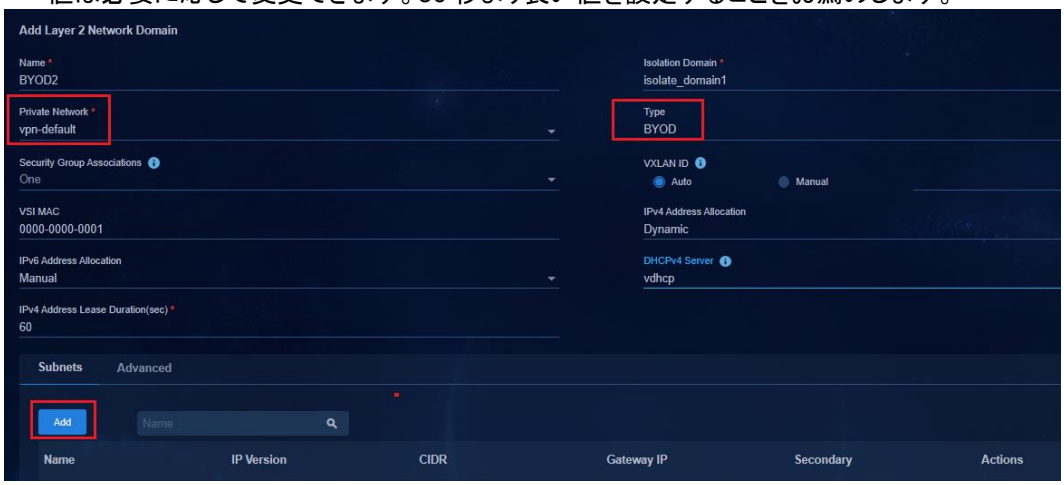
DHCP サーバーでの BYOD タイプのセキュリティグループの IP アドレスのデフォルトのリース時間は 1 分であるため、最初の段階でエンドポイントによって取得された IP アドレスのリース時間は 1 分です。プッシュされた認証ページでユーザー名とパスワードを入力してユーザーがログインすると、ユーザーは関連付けられたユーザーセキュリティグループに割り当てられます。最初の段階で取得された IP アドレスが期限切れになると、エンドポイントは別の IP アドレスを要求します。次に、アクセススイッチは、エンドポイント

のユーザーセキュリティグループに指定されたサブネットから IP アドレスを取得します。

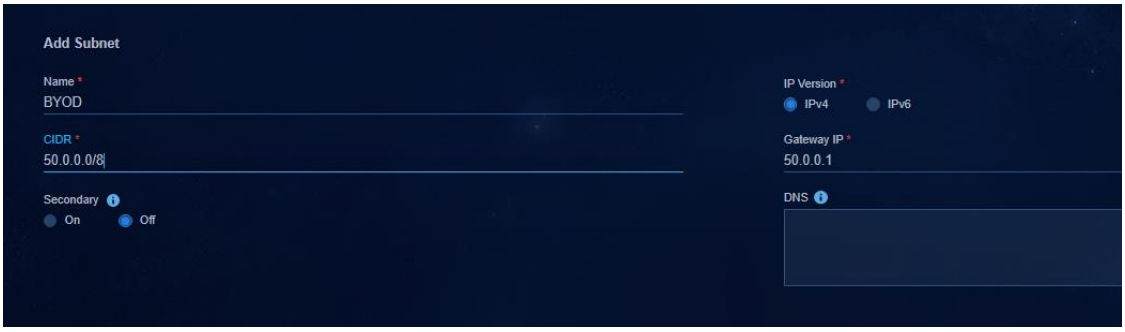
BYOD タイプのセキュリティグループを作成する

SeerEngine キャンパスにログインします。

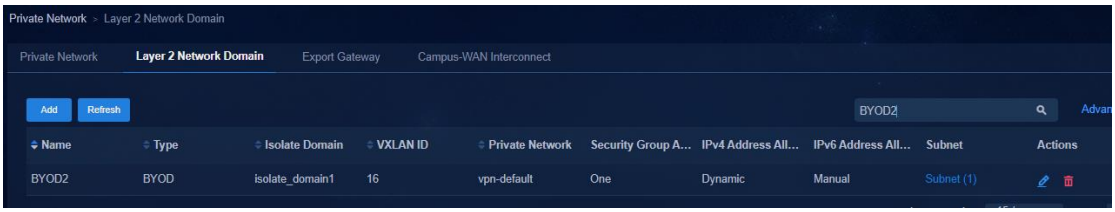
1. **Automation > Campus Network > Private Network > Layer 2 Network Domain** ページに移動し、**Add** をクリックします。
   - BYOD レイヤ 2 ネットワークドメイン:BYOD レイヤ 2 ネットワークドメインは、MAC ポータル認証に使用されます。
     - **Private Network**: vpn-default を選択します。
     - **Type**: BYOD を選択します。
     - **DHCPv4 server**: BYOD セキュリティグループに対して、H3C vDHCP を選択します。
     - **IP Address Lease Duration**: BYOD アドレスプールのデフォルトリースは 60 秒です。この値は必要に応じて変更できます。30 秒より長い値を設定することをお薦めします。



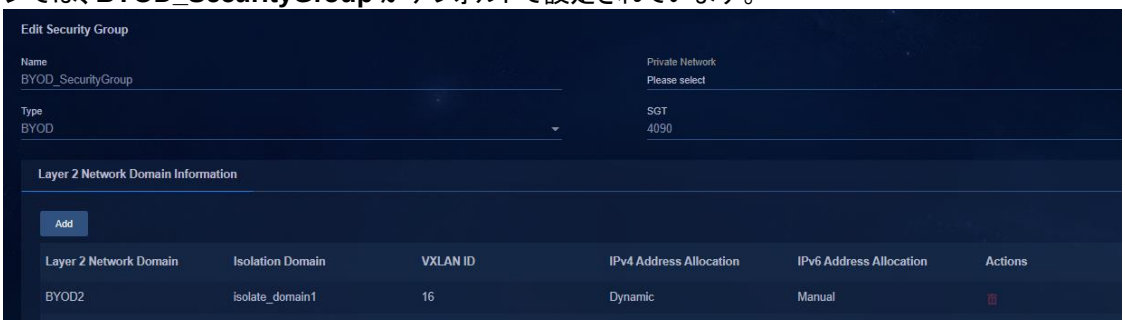
2. **Subnet** タブをクリックします。**Add** をクリックし、名前、IP バージョン、ネットワークセグメントおよびゲートウェイを入力します。**OK** をクリックします。



3. レイヤ 2 ネットワークドメインに戻ったら、もう一度 **OK** をクリックします。追加された BYOD レイヤ 2 ネットワークドメインは、レイヤ 2 ネットワークドメインページで確認できます。



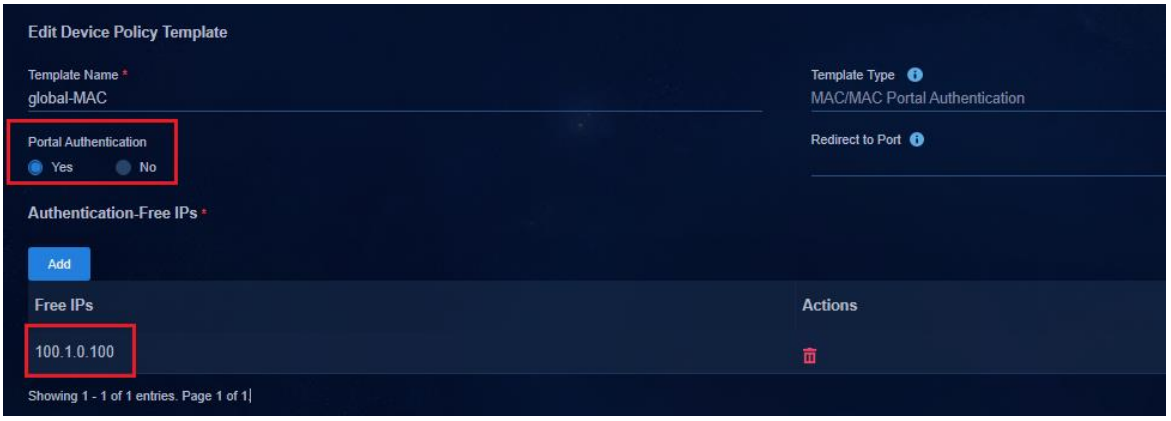
4. BYOD レイヤ 2 ネットワークドメインが追加されると、そのドメインは **Automation > Campus Network > SecurityGroup > User SecurityGroup** ページに自動的に追加されます。このページでは、**BYOD_SecurityGroup** がデフォルトで設定されています。



ACL3001 の設定

ACL 3001 は「Configure a policy template」で設定されています。

デバイスポリシーテンプレートの **Authentication-Free IPs** 領域で、EIA サーバーの IP アドレスを追加します。デバイスポリシーテンプレートがデバイスグループに適用されると、ACL3001 がデバイスグループ内のデバイスに展開されます。コントローラ上で空き IP を追加、変更、または削除すると、コントローラは変更をデバイスに展開します。



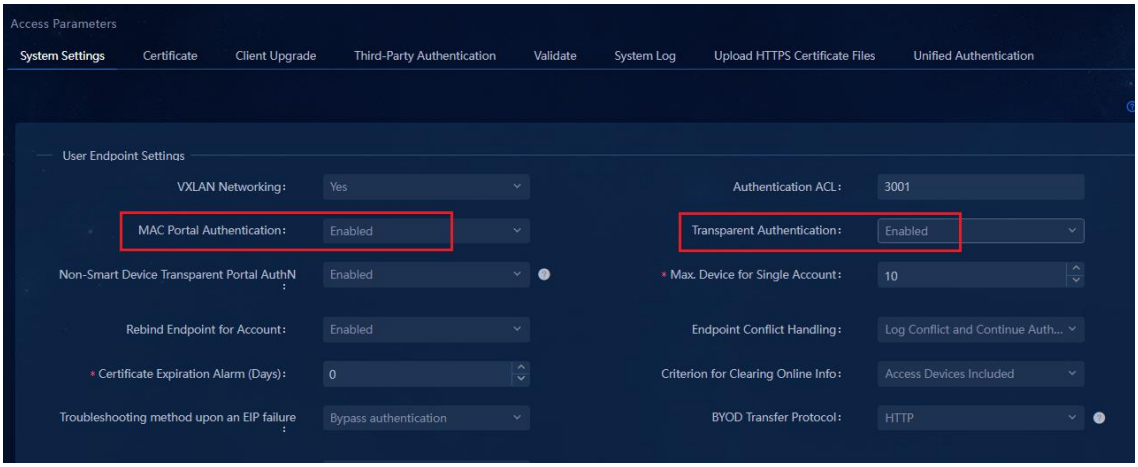
ポリシーは、デバイスグループポリシー設定に従って展開されます。

```
#

acl number 3001

description SDN_ACL_AUTH
```

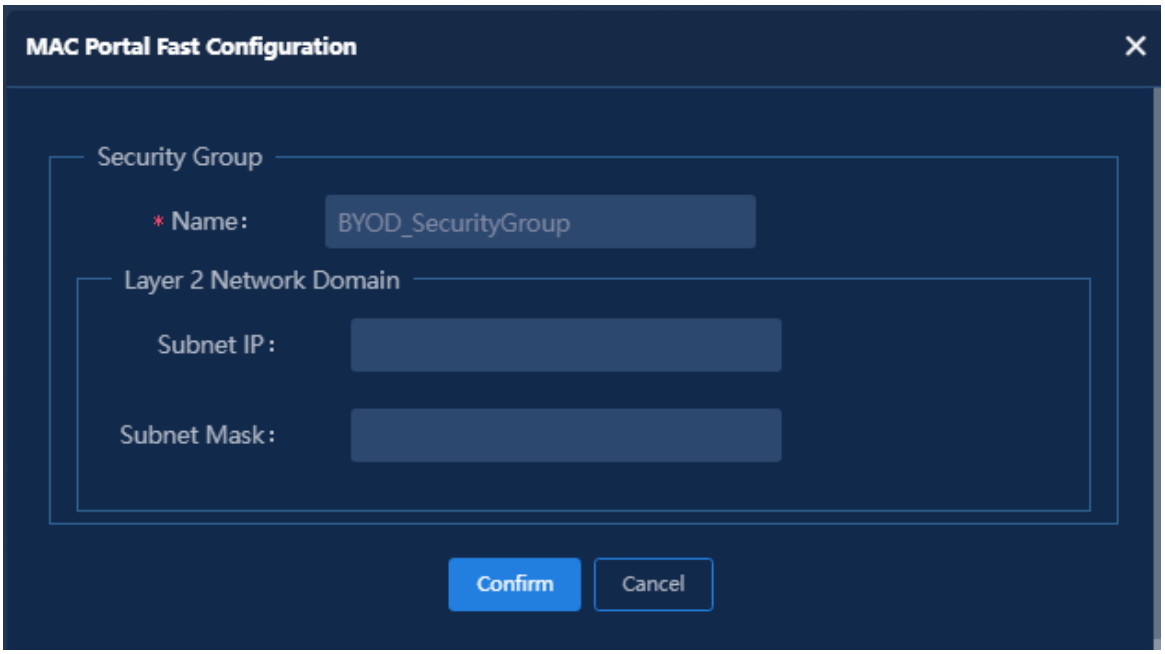
```
 rule 0 permit udp destination-port eq dns
 rule 1 permit ip vpn-instance vpn-default destination microsegment 65535
 rule 2 permit ip vpn-instance Teach destination microsegment 65535
#
#
microsegment 65535 name SDN_EPG_PORTAL_SERVER
 member ipv4 100.1.0.100 255.255.255.255 vpn-instance Teach
 member ipv4 100.1.0.100 255.255.255.255 vpn-instance vpn-default
#
```

MAC ポータル認証を有効にする

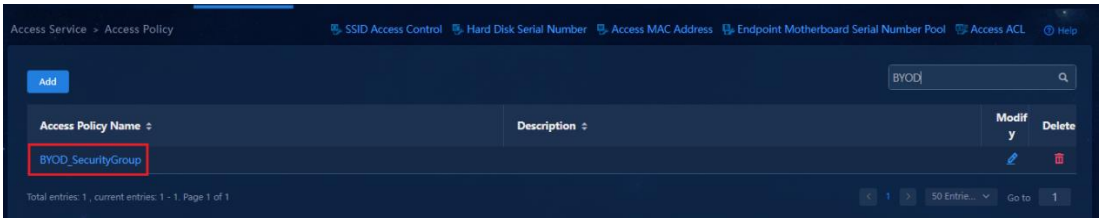
1. **Automation > User > Access Parameters > System Settings** ページに移動します。**System Settings** タブの **User Endpoint Settings** カラムで、**MAC Portal Authentication** をイネーブルにして、**MAC Portal Fast Configuration** ページを開きます(MAC ポータル認証がイネーブルになっている場合は、最初にディセーブルにしてから再度イネーブルにします)。さらに、transparent authentication をイネーブルにします。



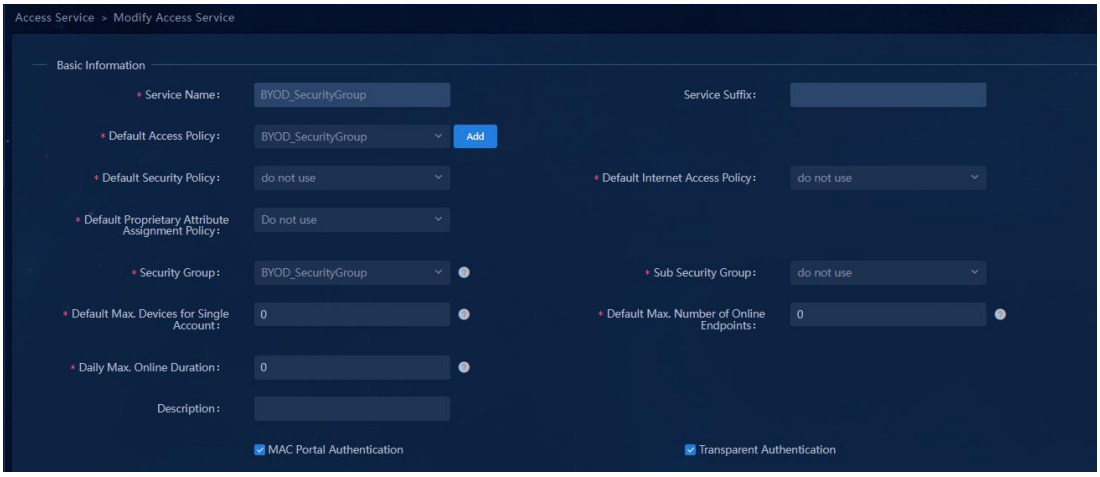
2. **MAC Portal Fast Configuration** ページで、**Confirm** をクリックします。BYOD アクセスポリシー、アクセスポリシーに関連付けられた BYOD アクセスサービス、および BYOD セキュリティグループ、BYOD ユーザーの作成、および BYOD アクセスサービスのバインドという一連の設定が自動的に作成されます。



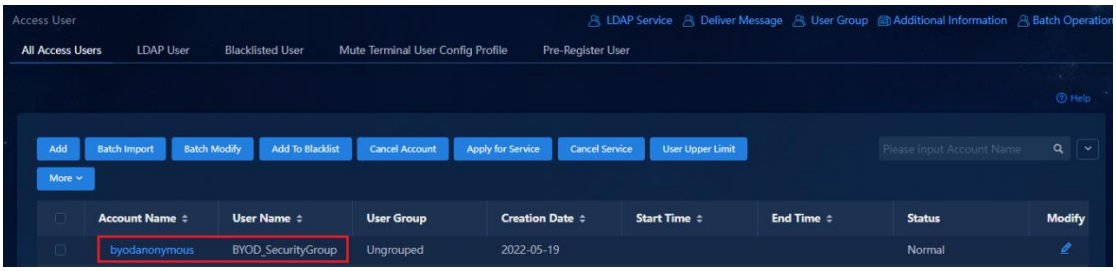
自動的に作成されたアクセスポリシー。



システムは自動的にアクセスサービスを作成します。アクセスサービスは、アクセスポリシーおよびセキュリティグループに関連付けられます。

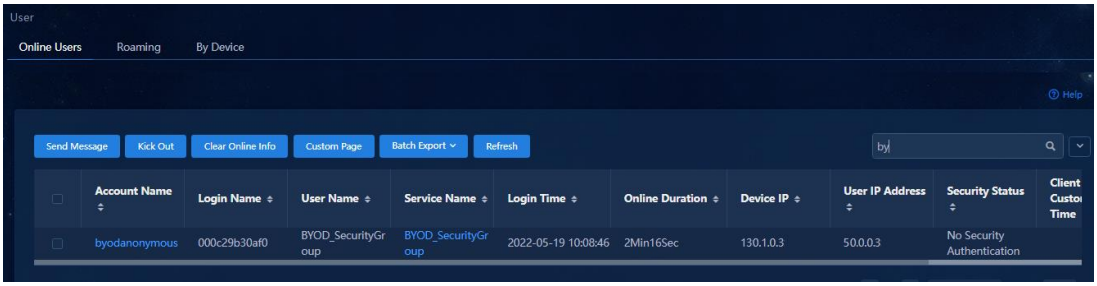


自動的に作成された BYOD ユーザー。



MAC ポータル認証を開始する

1. エンドポイントに接続されたポートがアップ状態になると、MAC 認証がトリガーされます。最初に BYOD 認証が実行されます。匿名アカウントの byodanonymous を使用してログインします。ユーザーが BYOD タイプのセキュリティグループに割り当てられ、エンドポイントが BYOD タイプのセキュリティグループに指定されたサブネットから IP アドレスを取得することを確認します。



アクセススイッチ(オーセンティケータとして機能)で、次のようにオンライン MAC 認証ユーザー情報を表示します。

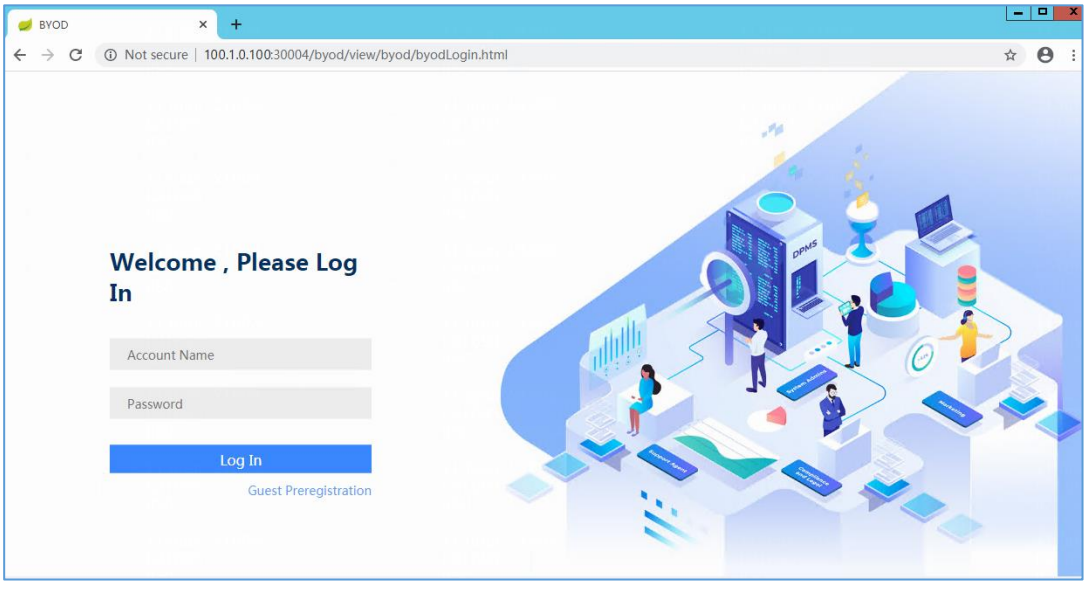
```
[Leaf-S105B]dis mac-authentication connection
Total connections: 1
Slot ID: 0
User MAC address: 000c-29b3-0af0
Access interface: Ten-GigabitEthernet0/0/37
Username: 000c29b30af0
User access state: Successful
Authentication domain: eia
IPv4 address: 50.0.0.3
IPv6 address: FE80::6D99:7824:2037:C6D
IPv4 address source: IP Source Guard
IPv6 address source: User packet
Initial VLAN: 102
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3
Authorization microsegment ID: 4090
Authorization ACL number/name: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization
```

```
http://100.1.0.100:30004/byod/index.html?usermac=%m&userip=%c&userurl=%o&original
=%o
Authorization IPv6 URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Online from: 01/15/2022 11:11:10 AM
Online duration: 0h 3m 58s
Port-down keep online: Disabled (offline)
[Leaf-S105B]
```

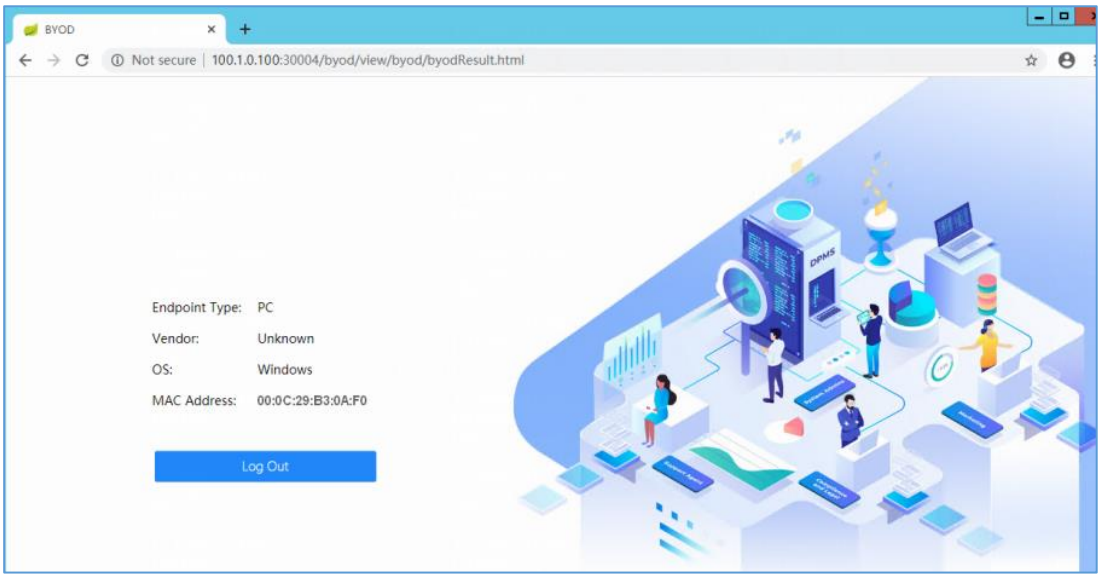
2. ユーザーの PC で、Web ブラウザを開き、1. 1. 1. 1 などの任意の IP アドレスを入力します。PC は、次の BYOD URL リダイレクションページに自動的にジャンプします。ユーザーがドメイン名を使用してネットワークにアクセスする場合、ユーザーは認証ページにリダイレクトできます。(DHCP を介して IP アドレスを取得するユーザーの場合は、分離ドメインまたはレイヤ 2 ネットワークドメインで DNS サーバーの IP アドレスを設定します。スタティック IP アドレスを持つユーザーの場合は、DNS サーバーの IP アドレスを手動で設定します。) さらに、Spine および Leaf デバイスに DNS サーバーへの到達可能なルーティングがあることを確認します。

重要:

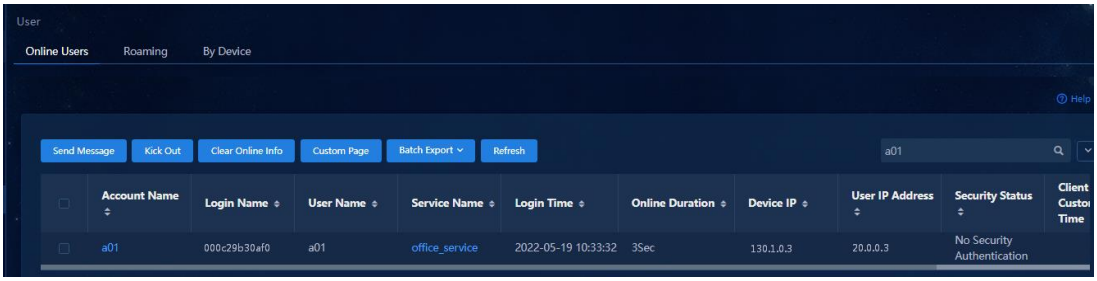
クライアントブラウザは Chrome でなければならず、Internet Explorer をサポートしていません。クライアントブラウザは Chrome V7.0 以降でなければなりません。



3. 正しいユーザー名とパスワードを入力し、Log In をクリックします。認証が成功すると、次のページが開きます。



4. EIA に関するユーザーのオンライン情報を表示します。ユーザーが関連付けられたアクセスサービスにアクセスし、ユーザーエンドポイントがアクセスサービスに関連付けられたサブネットから IP アドレスを取得したことを確認します。



アクセススイッチ(オーセンティケータとして機能)で、オンライン MAC 認証ユーザー情報を表示します。

```
[Leaf-S105B]dis mac-authentication connection
Total connections: 1
Slot ID: 0
User MAC address: 000c-29b3-0af0
Access interface: Ten-GigabitEthernet0/0/37
Username: 000c29b30af0
User access state: Successful
Authentication domain: eia
IPv4 address: 20.0.0.3
IPv4 address source: IP Source Guard
Initial VLAN: 102
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi4
Authorization microsegment ID: 3504
Authorization ACL number/name: N/A
Authorization user profile: N/A
```

```
Authorization CAR: N/A
Authorization URL: N/A
Authorization IPv6 URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Online from: 01/15/2022 11:18:37 AM
Online duration: 0h 2m 27s
Port-down keep online: Disabled (offline)
[Leaf-S105B]
```

MAC認証の設定

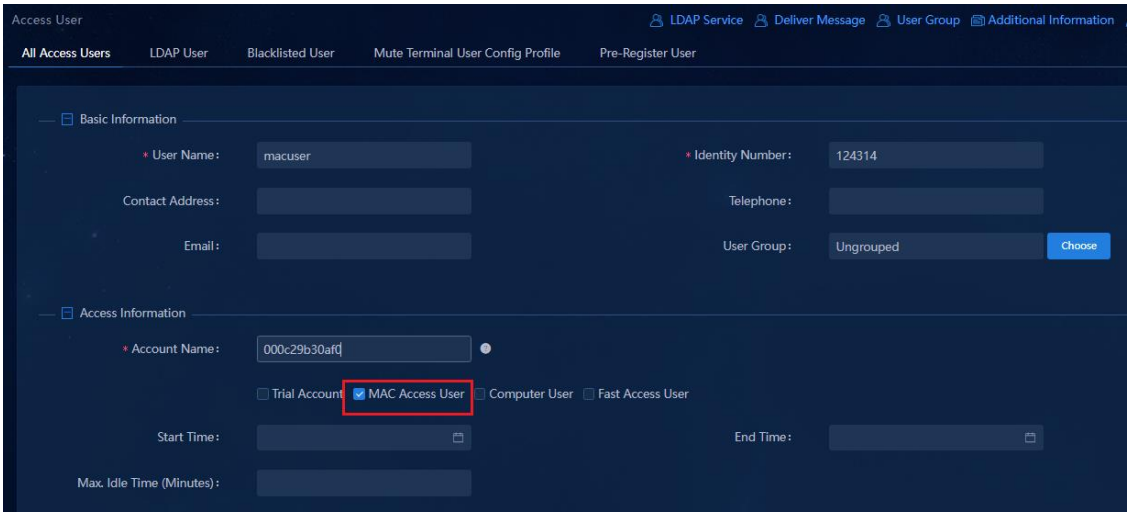
MAC 認証は主に、ユーザーがクライアントを持たず、エンドポイント MAC アドレスを介して直接オンラインになるように認証をトリガーするシナリオに適用されます。

MAC 認証ユーザーの設定

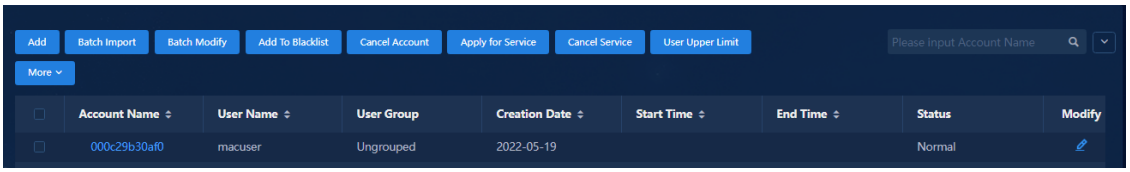
Automation > **User** > **Access User** ページにナビゲートし、**Add** をクリックしてアクセスユーザーを追加します。アクセスユーザーを手動で追加するか、アクセスユーザーを一括してインポートできます。

手動による組み込み

1. **Add** をクリックして、アクセスユーザーを追加するためのページを開きます。**Access Information** 列にアカウント名を入力し、**MAC Access User** を選択します。サーバーは、ユーザーのパスワードを自動的に構成します。アカウント名が xxxxxxxxxxxx の形式の MAC アドレスの場合は、**MAC Access User** を選択します。その後、サーバーはユーザーのパスワードを自動的に構成します。

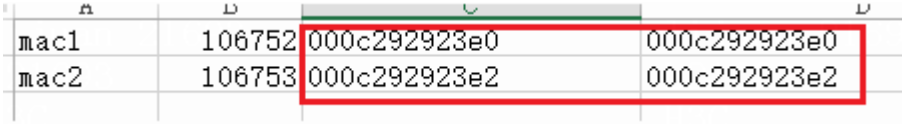


2. **Access Service** ページでユーザーのアクセスサービスを選択し、**OK** をクリックして MAC アクセスユーザーを追加します。

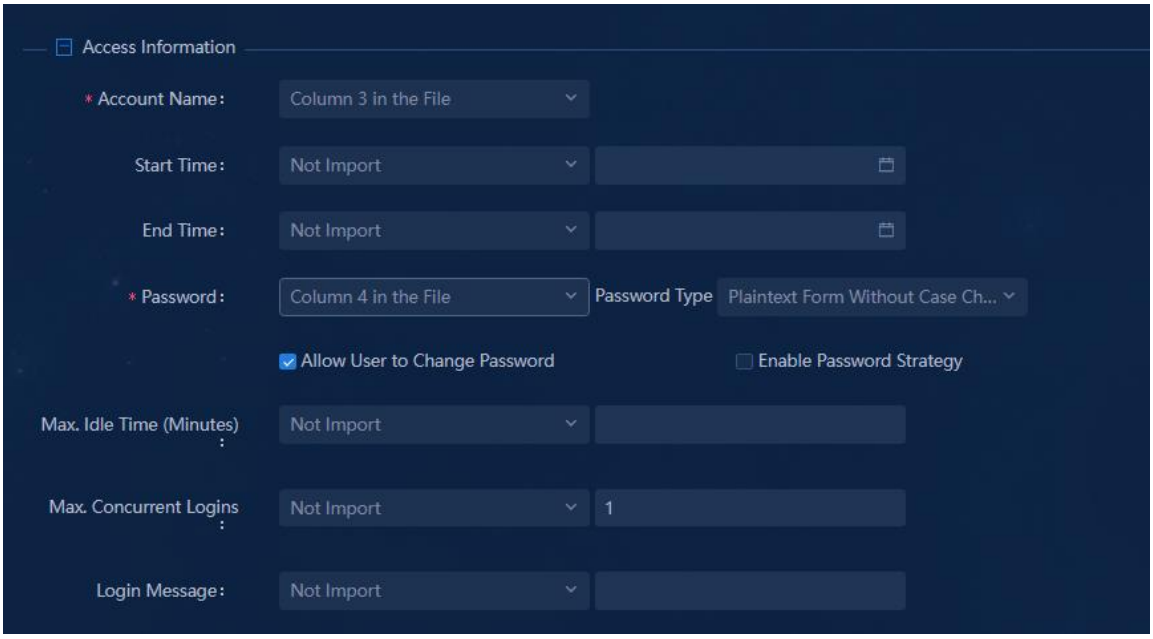


アクセスユーザーを一括インポートする

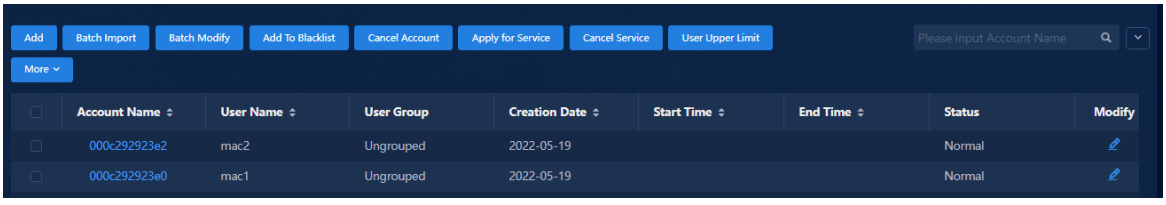
1. **Access User** ページで、**Batch Import** をクリックします。プロンプト領域の **Account Import file Template** リンクをクリックすると、インポートテンプレートをダウンロードできます。テンプレートに従って関連情報を指定します。
2. **Batch Import** をクリックして、ファイルを一括インポートします。ファイル内のユーザー名とパスワードは、次に示すように xxxxxxxxxxxx 形式の MAC アドレスである必要があります。



3. ファイルがアップロードされたら、ファイルの列セパレータを選択し、**Next** をクリックして、アクセスユーザー情報を構成するためのページを開きます。アクセス情報列のアカウント名とパスワードが両方とも MAC アドレスであることを確認します。

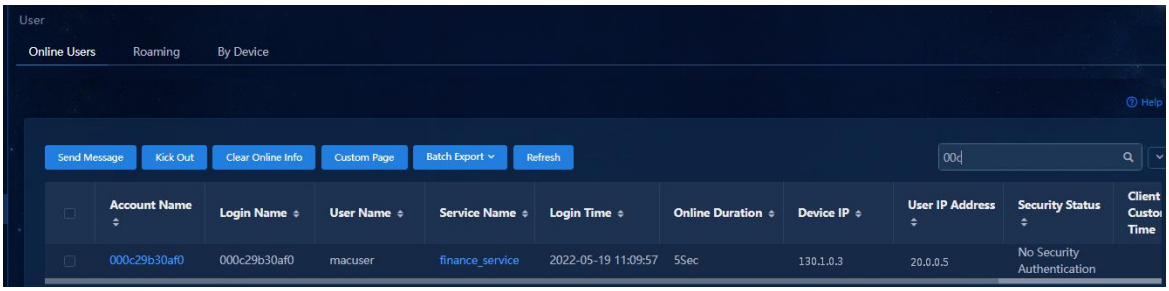


4. アクセスサービスを選択して **OK** をクリックすると、インポートされたユーザーを表示できます。



MAC 認証の開始

PC をアクセススイッチのポートに接続します。ポートが起動すると、PC は MAC アドレスを含むパケットを送信して MAC 認証をトリガーします。認証が成功すると、**Monito r> Monitor List > User > Online Users** ページで、オンライン MAC 認証ユーザーに関する情報を表示できます。



認証不要インターフェイスを構成する

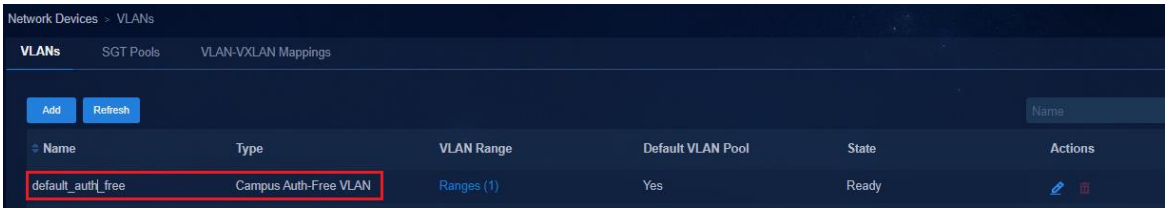
コントローラの認証不要インターフェイスを設定できます。認証不要インターフェイスからオンラインになったユーザーは、指定されたセキュリティグループに認証なしで直接参加して、IP アドレスを取得し、セキュリティグループの対応するネットワークリソースにアクセスできます。

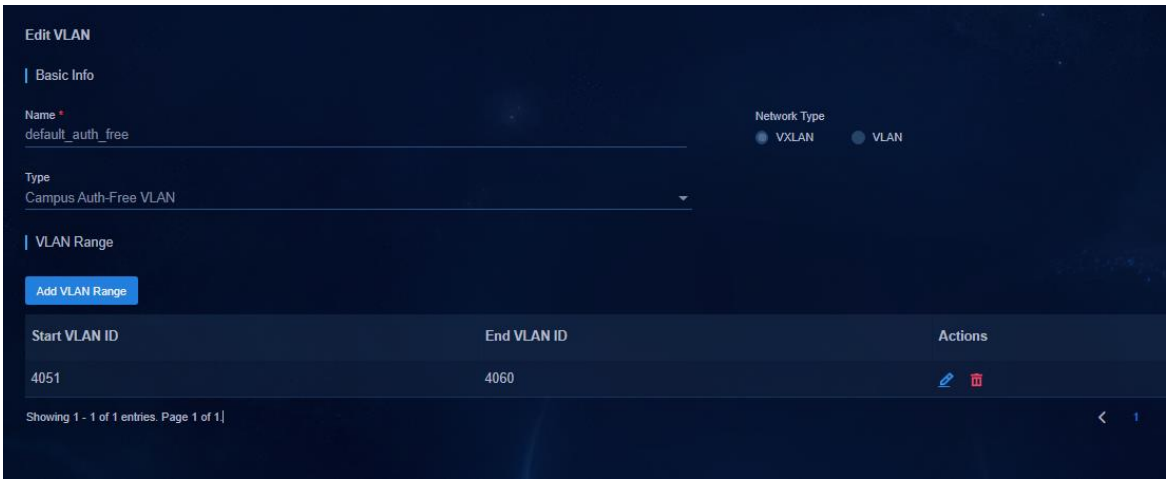
認証不要のインターフェイスを設定する場合は、まず認証不要のインターフェイスグループを作成する必要があります。デフォルトでは、認証不要のインターフェイスグループは作成されません。

認証不要 VLAN プールの設定

Automation > Campus Network > Network Devices > VNI Pools ページに移動します。システムには、デフォルトで証明書のない VLAN 範囲があらかじめ定義されています。

デフォルトの認証不要 VLAN 範囲は 4051～4060 です。をクリックすると、VLAN 範囲を変更できます。

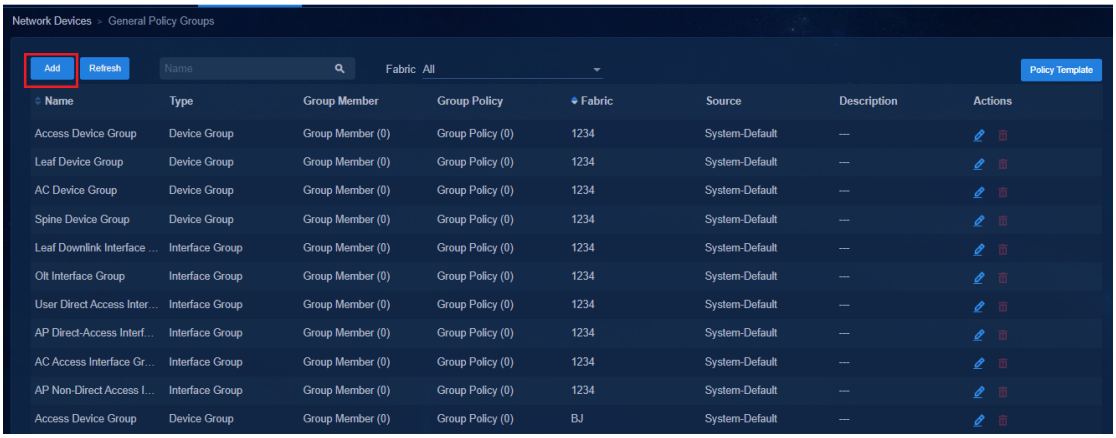




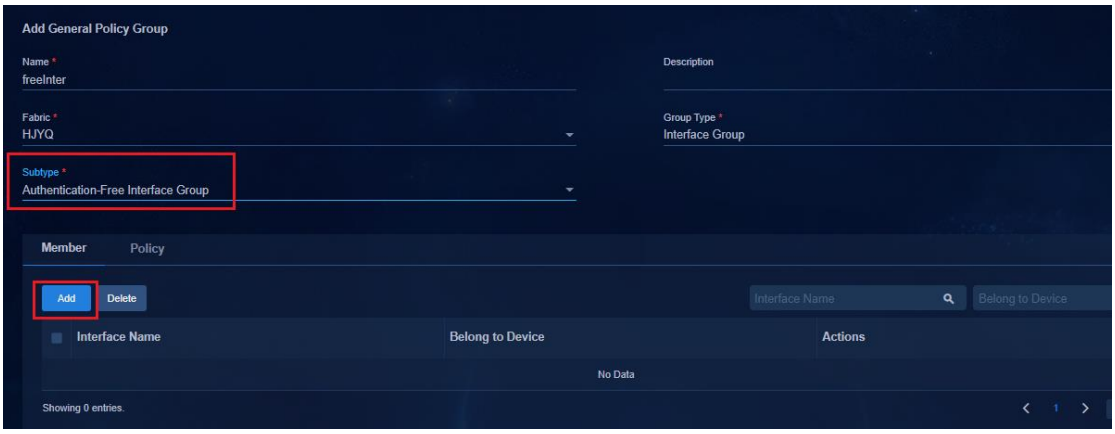
認証フリーインターフェイスグループを追加する

セキュリティグループで認証不要を設定するには、最初に認証不要インターフェイスグループを設定する必要があります。

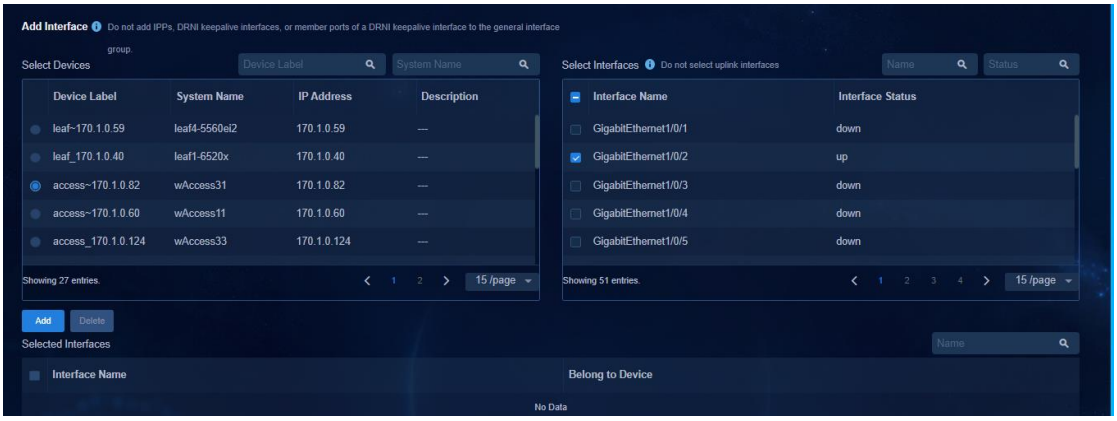
1. **Automation > Campus Network > Device Groups > General Device Groups** ページに移動し、**Add** をクリックします。



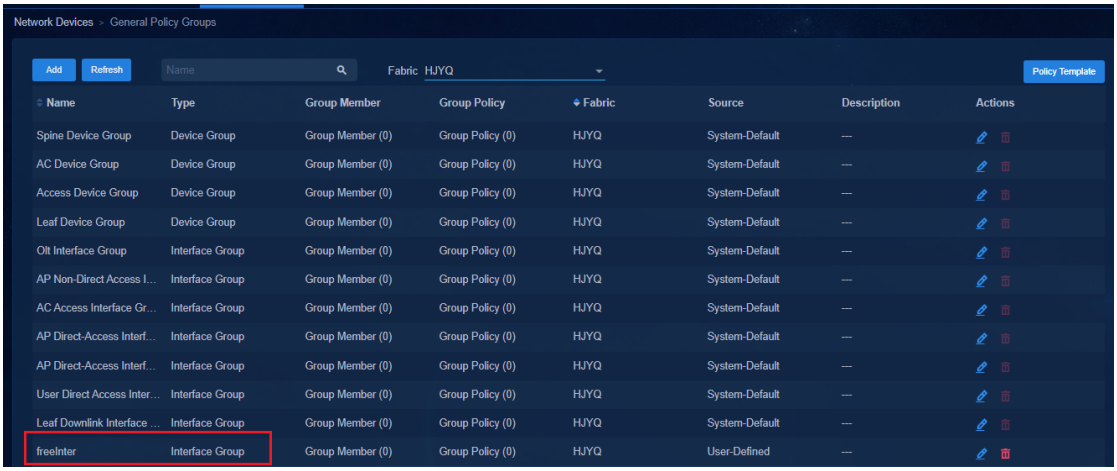
2. 認証不要インターフェイスグループを作成し、グループのメンバーを選択します。
   - **Type**: **Group Type** を **Interface Group** に設定します。
   - **Subtype**: **Authentication-Free Interface Group** を選択します。



3. ページの **Member** タブで、**Add** をクリックして **Add Interface** ページを開きます。デバイスおよびインターフェイスを選択し、**Add** をクリックして、選択したインターフェイスをリストに追加します。**OK** をクリックして、一般デバイスグループの追加ページに戻ります。



4. **OK** をクリックして、設定を保存します。一般デバイスグループリストでは、authenticatio-free インターフェイスグループを表示できます。

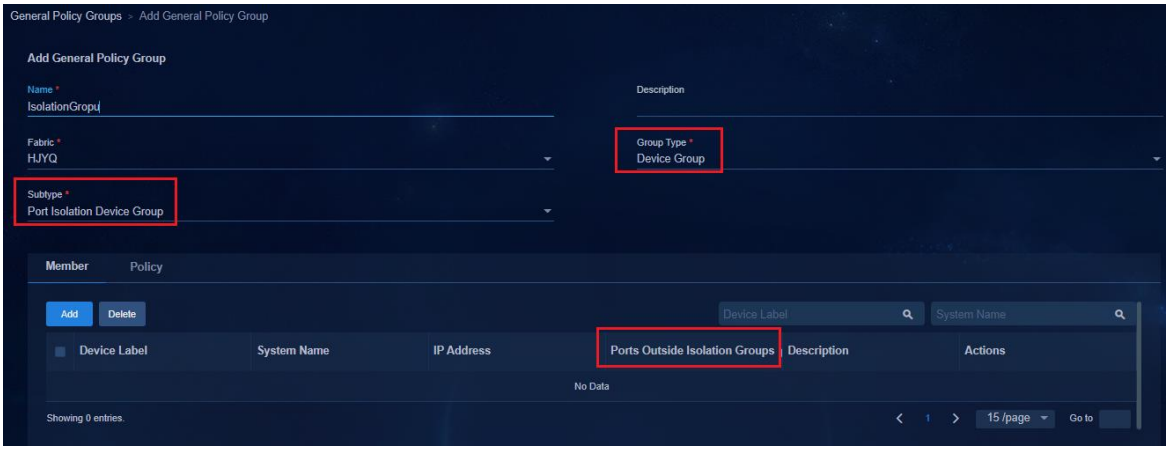


隔離ポートデバイスグループの追加

重要:

- 認証不要インターフェイスグループ内のインターフェイスがアクセスデバイス上のインターフェイスである場合、ポート隔離デバイスグループにアクセスデバイスを追加します。カスケードされたアクセスデバイスの場合、認証不要インターフェイスグループに加入しているアクセスデバイスだけがポート隔離デバイスグループに追加されます。
- 前に設定した認証不要ポートがリーフデバイスのポートである場合は、この手順を省略します。

1. **Automation > Campus Network > Network Devices > General Device Groups** ページに移動します。一般ポリシーページで **Add** をクリックして、一般デバイスグループを追加するためのページを開きます。
2. 次の図に示すように、隔離ポートデバイスグループを作成し、認証不要インターフェイスグループで設定されたアクセスデバイスを選択します。
   - **Group Type**: **Device Group** を選択します。
   - **Fabric**: アクセスデバイスのファブリックを選択します。
   - **Subtype**: **Port Isolation Device Group** を選択します。
   - **Group Type**: **Enable for DRNI networking** を選択します。
   - **Ports Outside Isolation Groups**: リーフデバイスをアクセスデバイスに接続するすべてのアップリンクインターフェイスは、隔離グループ外のポートに追加する必要があります。複数のアクセスデバイスがカスケードされている場合、下位レベルのアクセスデバイスを上位レベルのアクセスデバイスに接続するアップリンクインターフェイスも、隔離グループ外のポートに追加する必要があります。つまり、アクセスデバイスのアップリンクインターフェイスは、隔離グループ外のポートに追加する必要があります。



3. アクセスデバイスに展開された設定:
4. 隔離ポートグループをグローバルに発行します。

```
#
port-isolate group 1
#
```

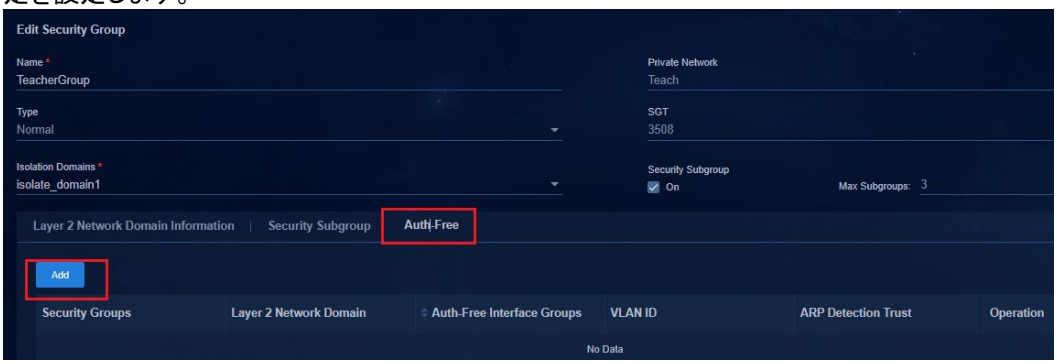
5. アクセスデバイスのすべてのポート(隔離グループ外のポートを除く)に対して、port-isolate enable group 1 コマンドを発行します。

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101

 port-isolate enable group 1
stp edged-port
#
```

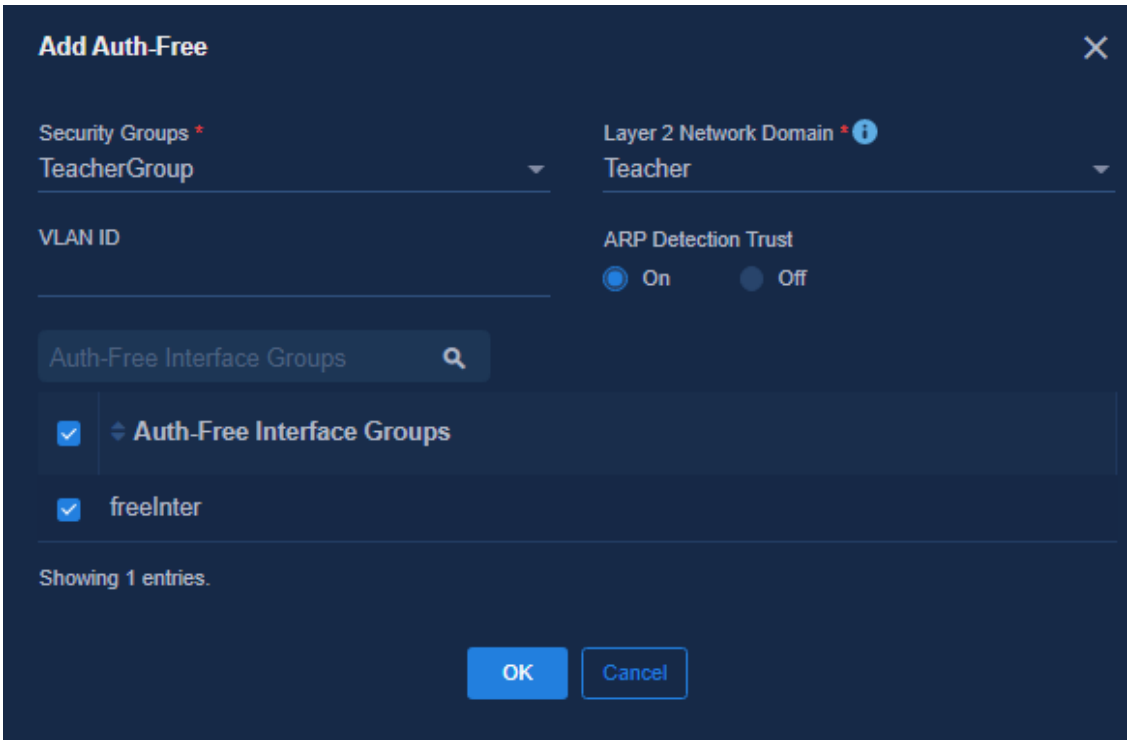
認証不要インターフェイスグループをセキュリティグループにバインドする

Automation > Campus Network > Security Group ページに移動します。**Actions** カラムをクリックして、セキュリティグループを編集するためのページを開きます。

1. セキュリティグループを追加するページで、**Auth-free** タブをクリックして、ユーザーの Auth-free 設定を設定します。



2. Auth-Free を設定し、**Auth-Free Interface Group** を選択します。
3. デフォルトでは、システムは「Configure authentication-free VLAN pool」で指定された VLAN 範囲に基づいて VLAN ID を設定します。VLAN ID を手動で設定することもできます。コントローラは設定された VLAN ID を配信します。



設定をデバイスに展開する

セキュリティグループが認証不要インターフェイスグループにバインドされると、次の設定がデバイスに展開されます。

1. 認証不要インターフェイスグループのメンバーは、アクセスデバイス上のインターフェイスです。

service-instance 4051 を、このアクセスデバイスに接続する Leaf ダウンリンクインターフェイスに追加します。

```
#
interface Ten-GigabitEthernet1/2/0/13
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port-security free-vlan 1 4051 4094
 #
 service-instance 4051
encapsulation  s-vid  4051              //VLAN 4051 to VLAN 4060 are used by the controller for the authentication-free service by default.
  xconnect vsi vsi4  microsegment 3504 on-demand
  arp detection trust
#
#
```

#アクセスデバイス上の認証不要インターフェイスにスタティック VLAN 設定を追加します。

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4051
```

```
 port-isolate enable group 1
stp edged-port
#
```

2. authentication-free インターフェイスグループのメンバーは、Leaf デバイス上のインターフェイスです。

service-instance 4051 を、認証不要インターフェイスに接続されたリーフデバイスに追加します。

```
interface Ten-GigabitEthernet1/2/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4051
 port trunk pvid vlan 4051
 port-security free-vlan 4051
 #
 service-instance 4051
encapsulation untagged
  xconnect vsi vsi4  microsegment 3504
  arp detection trust
#
```

静的AC認証の設定

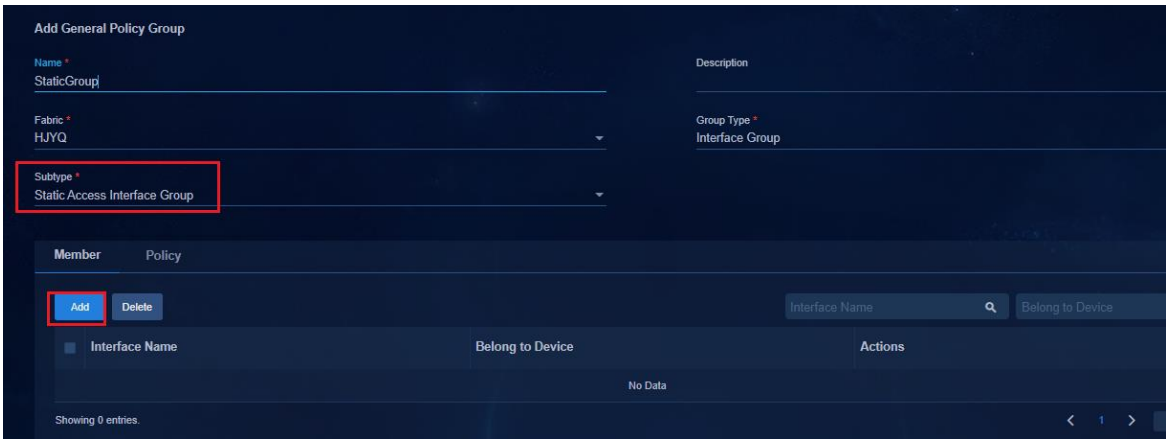
重要:

- スタティックアクセス用の VLAN プールは、事前に設定しておく必要があります。詳細については、「User VLAN planning」を参照してください。
- スタティック AC 認証は、同じ IP アドレスセグメント上のユーザーが異なるアクセス権限を持つ必要があるシナリオに適用されます。

スタティックアクセスインターフェイスグループを追加する

Automation > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動し、**Add** をクリックします。

- **Group Type**: **Interface Group** を選択します。
- **Subtype**: **Static Access Interface Group** を選択します。
- **Member**: **Member** タブをクリックします。**Add** をクリックし、エンドポイントがアクセスデバイスまたはスパインデバイスへの接続に使用するインターフェイスを選択します。

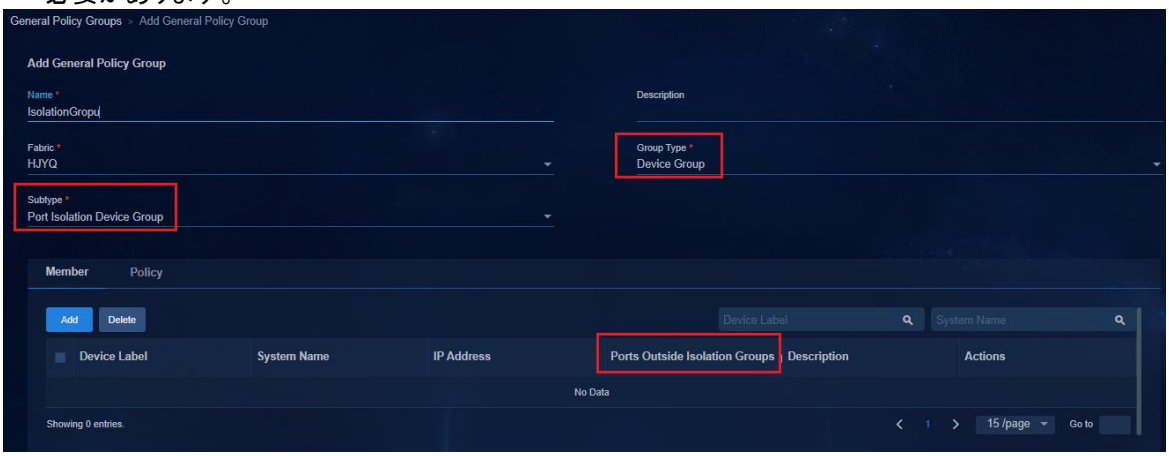


隔離ポートデバイスグループの追加

重要:

- スタティックインターフェイスグループがアクセスデバイスインターフェイスである場合は、ポート隔離デバイスグループにアクセスデバイスを追加する必要があります。マルチカスケードアクセスデバイスでは、スタティックインターフェイスグループに加入するアクセスデバイスをポート隔離デバイスグループに追加するだけで済みます。
- 前に設定した認証不要ポートが Leaf デバイスのポートである場合は、この手順を省略します。

1. **Automation** > **Campus Network** > **Devices** > **General Device Groups** に移動します。次に示すように、インターフェイス分離デバイスグループを作成し、認証不要インターフェイスグループで設定されたアクセスデバイスを選択します。
   - **Group Type**: **Device Group** を選択します。
   - **Fabric**: アクセスデバイスのファブリックを選択します。
   - **Subtype**: **Port Isolation Device Group** を選択します。
   - **Group Type**: DRNI ネットワーキングのデバイスグループを選択します。
   - **Ports Outside Isolation Groups**: リーフデバイスをアクセスデバイスに接続するすべてのアップリンクインターフェイスは、隔離グループ外のポートに追加する必要があります。複数のアクセスデバイスがカスケードされている場合、下位のアクセスデバイスを上位のアクセスデバイスに接続するアップリンクインターフェイスも、隔離グループ外のポートに追加する必要があります。つまり、アクセスデバイスのアップリンクインターフェイスは、隔離グループ外のポートに追加する必要があります。



2. アクセスデバイスに展開された設定:

3. 隔離ポートグループをグローバルに発行します。

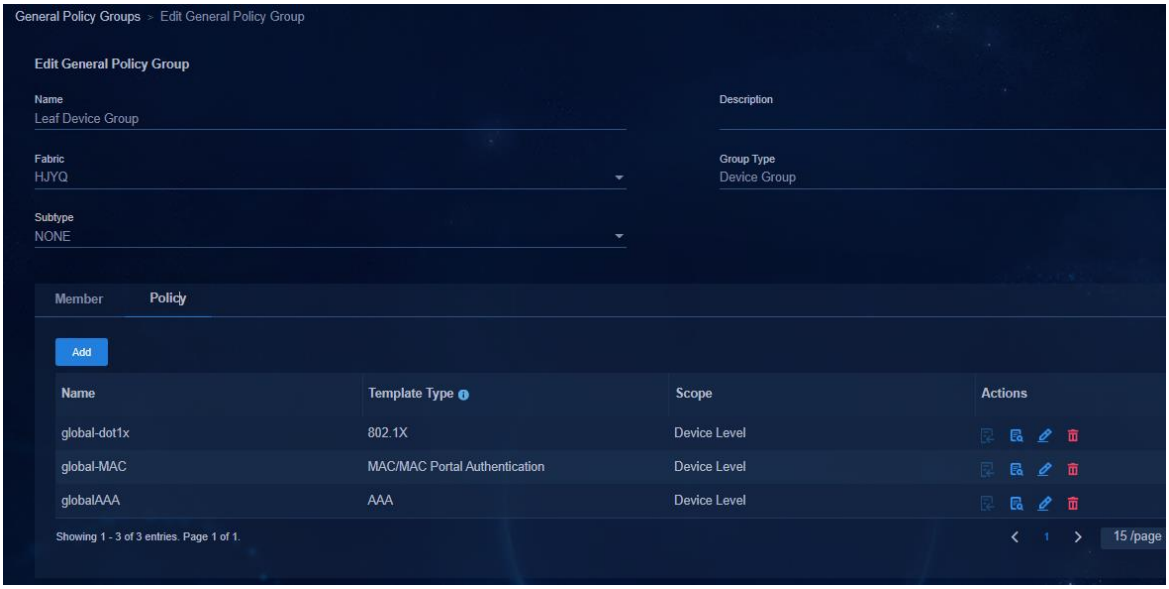
```
#
port-isolate group 1
#
```

4. アクセスデバイスのすべてのポート(隔離グループ外のポートを除く)に対して、**port-isolate enable group 1** コマンドを発行します。

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101

 port-isolate enable group 1
stp edged-port
#
```

リーフデバイスグループにポリシーテンプレートを発行します。

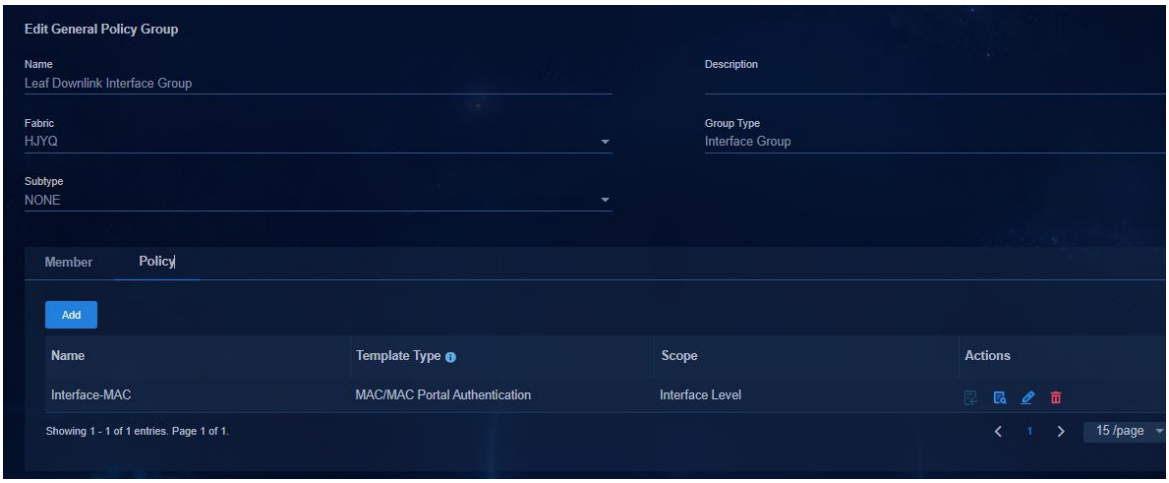
1. **Automation** > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。リーフデバイスグループの **Actions** カラムをクリックします。
2. **Policy** タブをクリックし、**Add** をクリックして、デバイスグループポリシーを追加するためのページを開きます。
3. AAA および MAC 認証または 802.1X 認証用のポリシーテンプレートを選択します。



リーフダウンリンクインターフェイスにポリシーテンプレートを発行します。

1. **Automation** > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。**Leaf Downlink Interface Group** の **Actions** カラムをクリックして、一般的なデバイスグループを編集するためのページを開きます。
2. **Policy** タブをクリックし、**Add** をクリックして、デバイスグループポリシーを追加するためのページを開きます。MAC ポータル認証または 802.1X 認証用のポリシーテンプレートを選択します。

   認証モードの 1 つを選択することをお勧めします。物理インターフェイスで 802.1X 認証と MAC ポータル認証の両方を設定しないでください。実際の要件に基づいて認証モードを設定してください。



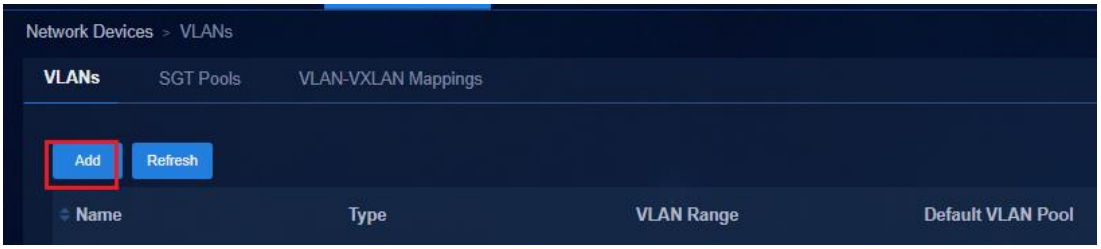
スタティックアクセス VLAN プールを作成する

重要:

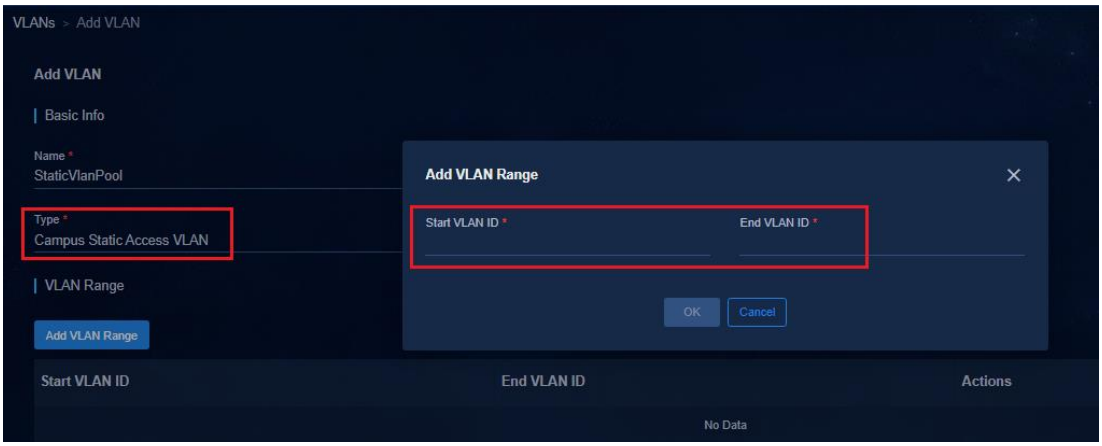
- VLAN プールを作成する場合、VLAN は他の VLAN プールと競合できません。
- VLAN プールのステータスが **In Use** になると、編集できなくなります。開始する前に、各 VLAN プールの VLAN 範囲を計画する必要があります。

1. **Automation** > **Campus Network** > **Network Devices** > **VNID Pools** ページに移動します。VLANs ページを開き、スタティックアクセス用の VLAN プールタイプの VLAN を作成します。

2. **VLAN** タブをクリックし、**Add** をクリックして **Add VLAN** ページを開きます。



3. 名前を入力します。タイプとして **Campus Static Access VLAN Pool** を指定します。**Add VLAN Range** をクリックし、**Add VLAN Range** ページで VLAN 範囲を入力します。

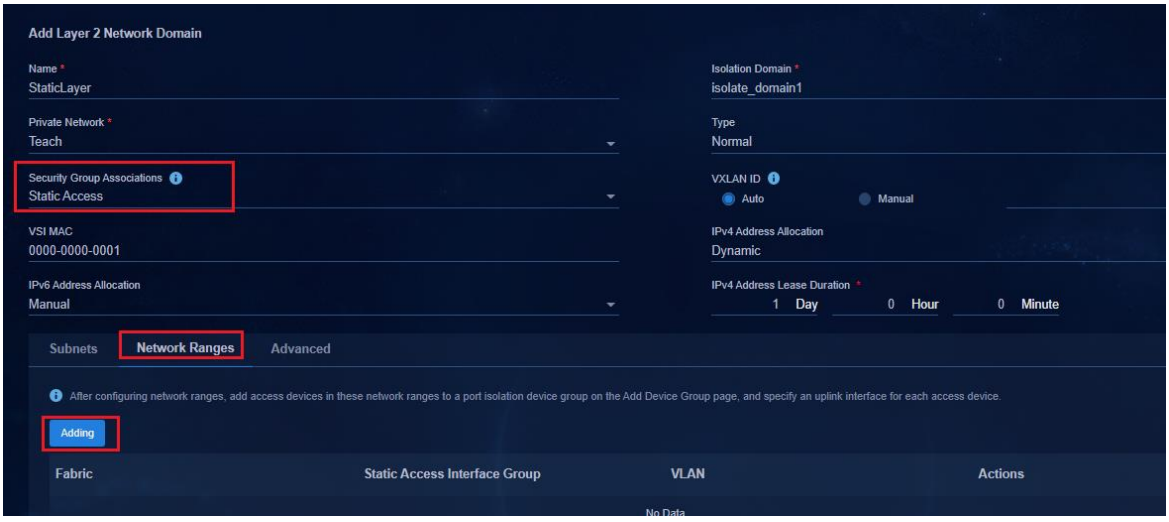


4. 設定が完了したら、**OK** をクリックして設定を保存します。

レイヤー2 ネットワークドメインを作成する

Automation > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動し、**Add** をクリックします。

- **Security Group Associations**: **Static Access** を選択します。
- **Network Ranges**: 作成したスタティックアクセスインターフェイスグループを選択して、スタティックアクセスインターフェイスグループをバインドします。
- **VLAN**: をクリックすると、設定されたスタティックアクセス VLAN プールに基づいて、VLAN プールが自動的に割り当てられます。レイヤー2 ネットワークドメイン内の VLAN に割り当てることができるスタティックアクセスグループは 1 つだけです。



- アクセスデバイスに展開された設定

  アクセスデバイスでは、スタティックアクセスインターフェイスグループで設定されたインターフェイスが、レイヤー2 ネットワークドメインで設定された VLAN の値に変更されます。

```
[Access3]dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
InLoop0              UP   UP(s)    --
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1024             UP   20G(a)  F(a)   T    1
GE1/0/1              UP   1G(a)   F(a)   A    2801
GE1/0/2              DOWN auto    A      A    2801
GE1/0/3              DOWN auto    A      A    2801
GE1/0/4              DOWN auto    A      A    2801
GE1/0/5              DOWN auto    A      A    2801
GE1/0/6              DOWN auto    A      A    106
GE1/0/7              DOWN auto    A      A    107
```

- リーフデバイスに展開された設定

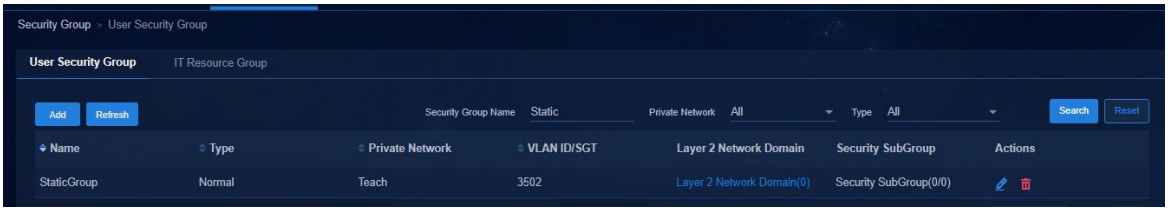
スタティック AC 設定は、スタティックアクセスインターフェイスグループ内のアクセスデバイスに接続されたリーフダウンリンクインターフェイスに展開されます。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 mac-authentication
 mac-authentication domain hz1
 mac-authentication parallel-with-dot1x
 port-security free-vlan 1 4094
 #
 service-instance 2801     // コントローラーによって発行された静的 AC 構成.
  encapsulation s-vid 2801
  xconnect vsi vsi6
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

セキュリティグループを作成する

Automation > **Campus Network** > **Security Group** > **User Security Group** ページに移動します。**Add** をクリックして、セキュリティグループを追加するページを開きます。レイヤー2 ネットワークドメインを追加せずにセキュリティグループを作成します。このドキュメントでは、Private Network に Tech を選択し、**Type** に **Normal** を選択します。**OK** をクリックして設定を保存します。

セキュリティグループ ID(この例では 3502)は、コントローラがデバイスに展開するマイクロセグメント ID です。SeerEngine キャンパスコントローラはセキュリティグループを EIA に同期し、EIA はユーザー認証時にこのマイクロセグメント ID を割り当てます。



ユーザー認証とオンライン

上記の設定が完了すると、エンドポイントはアクセスデバイス上の VLAN ID 2801 を使用してアクセスインターフェイスに接続されます。ユーザー認証中、ユーザーは認証用のリーフデバイスの VLAN のスタティック AC に割り当てられます。

クライアントの 802.1X 認証および MAC ポータル認証については、「Configure 802.1X authentication」および「Configure MAC portal authentication」を参照してください。

Webポータル認証の設定

注:

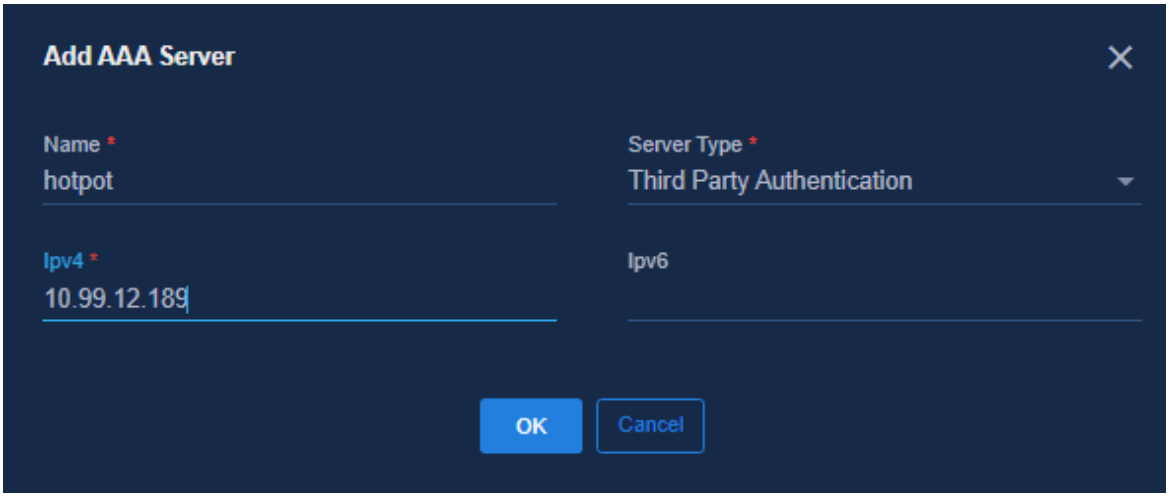
- Web ポータル認証は、認証分離機能に適用されます。サードパーティー製の AAA 認証サーバーをサポートします。
- サードパーティーAAA 認証サーバーは、ポータル認証および h3c-user-group アトリビュートをサポートする必要があります。H3C EIA 認証サーバーは、サードパーティーAAA 認証サーバーとして使用できます。また、H3C 以外のサードパーティーAAA 認証サーバーによるユーザー認証もサポートします。
- Web ポータル認証では、認証にスタティック AC インターフェイスを使用します。
- ここでは、コントローラおよびデバイスでの Web ポータル認証の設定について説明します。サードパーティー認証サーバーの設定については、ベンダーの関連情報を参照してください。

AAA サーバー

Automation > **Campus Network** > **Parameters** > **AAA** ページに移動します。**Add** をクリックして、認証サーバーを追加するためのページを開きます。

H3C EIA 認証サーバーの追加については、「AAA」を参照してください。

サーバータイプとして **Third Party Authentication** を選択し、EIA サーバーの IP アドレスを入力します。サードパーティー認証サーバーがスパインデバイスおよびリーフデバイスと通信できることを確認します。



Spine/Leaf デバイスは、認証サーバーと通信する必要があります。認証サーバーへのルートは、Spine/Leaf デバイスで構成する必要があります。ルーティング構成方法は次のとおりです:

- 各デバイスにログインし、手動で設定します。
- **Automation** > **Campus Network** > **Network Devices** > **General Device Groups** ページに移動し、**Policy Template** をクリックしてポリシーテンプレートのページを開きます。ユーザー定義のポリシーテンプレートを設定できます。
- **Automation** > **Campus Network** > **Fabrics** ページに移動します。**Action** カラムの設定アイコンをクリックして、Switching Device ページに入ります。**Settings** タブをクリックします。**Configuration Automation** ボタンをクリックして **Address Pool Setting** タブをクリックし、アドレスプール設定ページに入ります。サーバーの IPv4 管理ネットワークセグメントが認証サーバーの IP アドレスセグメントに設定されている場合、デバイスが自動的にオンラインになると、コントローラは設定を自動的に配信します。

```
#
ip route-static vpn-instance vpn-default 10.99.12.189 32 130.0.0.254
#
```

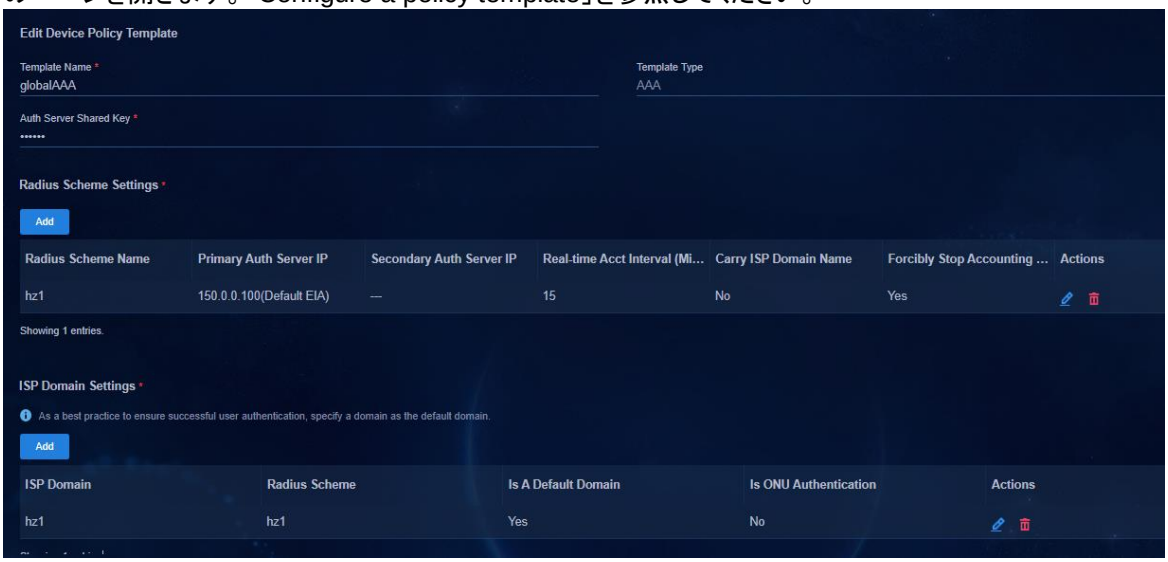
AAA デバイスポリシーテンプレート

Automation > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。

ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートのページを開きます。

- H3C EIA AAA テンプレート

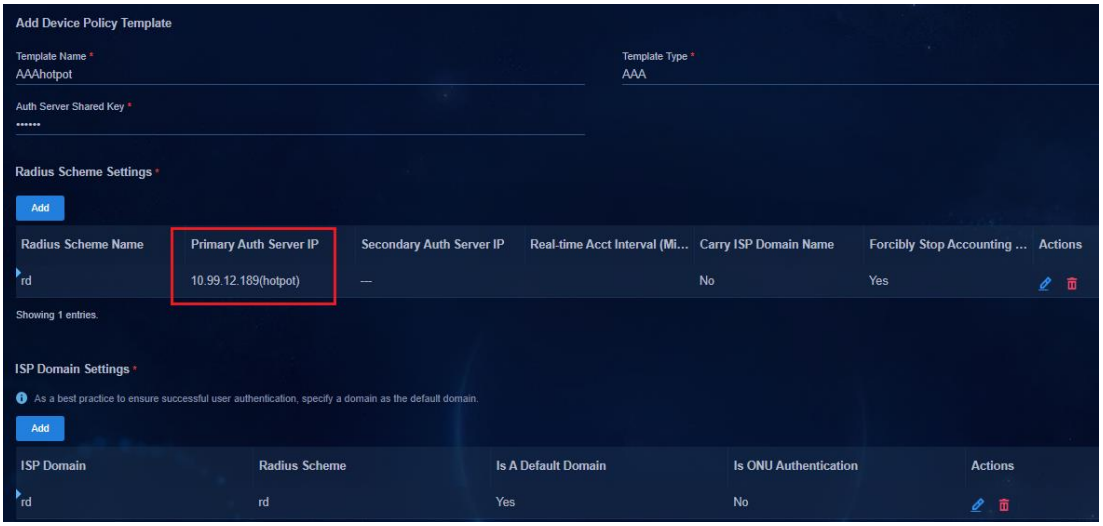
  リスト内の **AAA** に対応する **Actions** カラムをクリックして、ポリシーテンプレートを編集するためのページを開きます。「Configure a policy template」を参照してください。



- サードパーティー認証サーバーを設定する

  Add をクリックし、ドロップダウンリストから **Device Policy Template** を選択します。

  - **Template Type**: **AAA** を選択します。
  - **Auth Server Shared Key**: サードパーティー認証サーバー上のキーと同じであることを確認します。この例では、123456 を使用します。
  - 追加したサードパーティー認証サーバーを選択します。

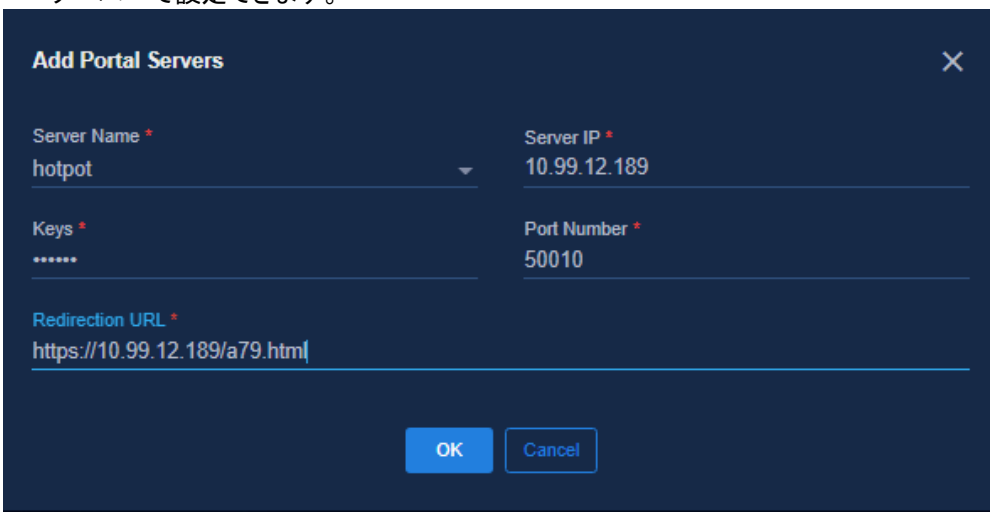


Web ポータルテンプレートを設定する

サードパーティー認証サーバーの Web ポータルテンプレートを設定する

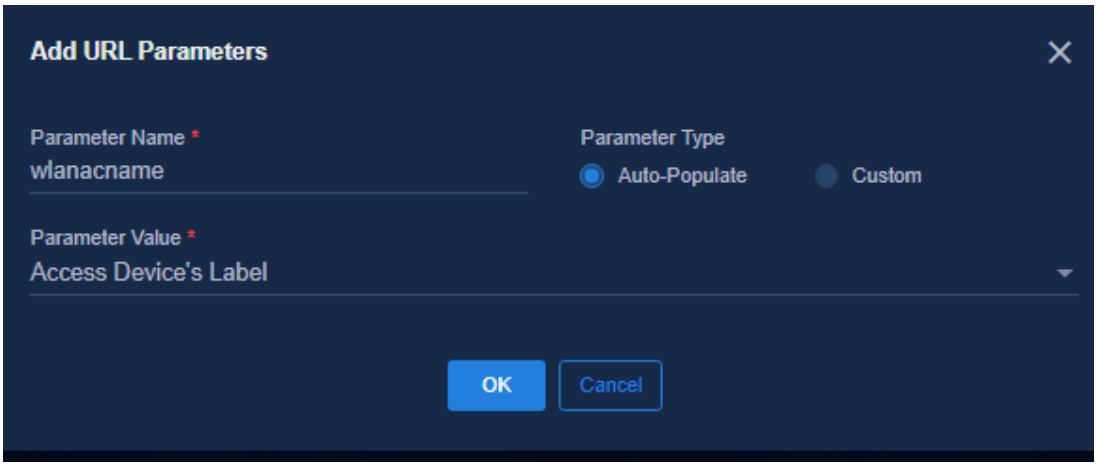
Automation > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートのページを開きます。

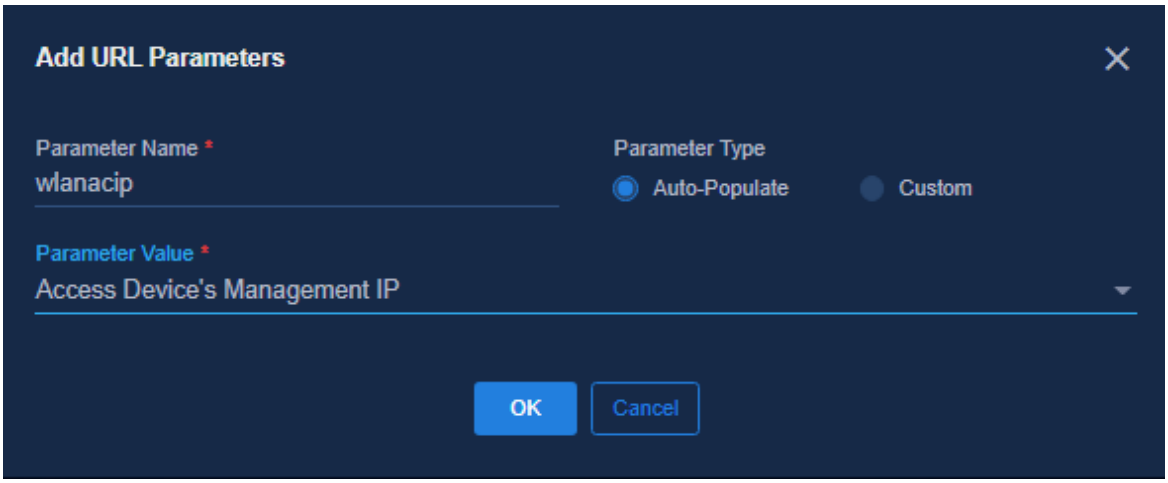
1. **Add** をクリックし、ドロップダウンリストから **Device Policy Template** を選択します。**Template Type** で **Web Portal Authentication** を選択します。
2. **Portal Server** カラムで **Add** をクリックし、次のパラメーターを設定します。
   - **Server Name**: 追加したサードパーティー認証サーバーを選択します。
   - **Key**: キーがサードパーティー認証サーバー上のキーと同じであることを確認します。この例では、123456 です。
   - **Port Number**: デフォルト値は 50010 です。デフォルト設定を使用します。
   - **Redirection URL**: ユーザーは Web ページにアカウントとパスワードを入力します。これは認証サーバーで設定できます。



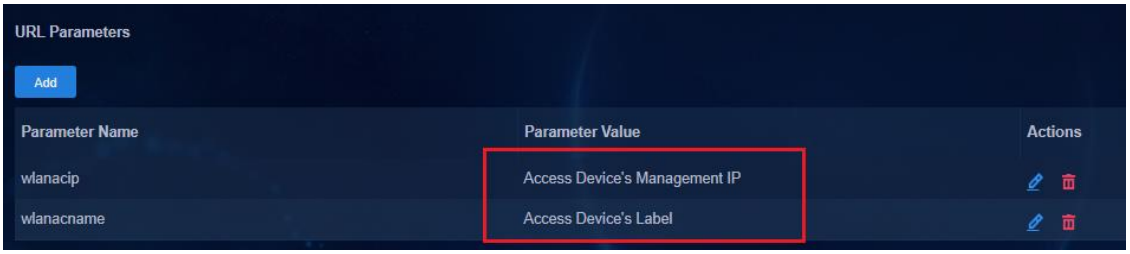
3. **URL Domain Settings** カラムの **Add** をクリックして、**Add URL Domain** ページを開きます。

   URL パラメーター:特定の認証サーバー要件に従ってパラメーターを設定します。Dr.COM の **wlanacname** と **wlanacip** を設定します。





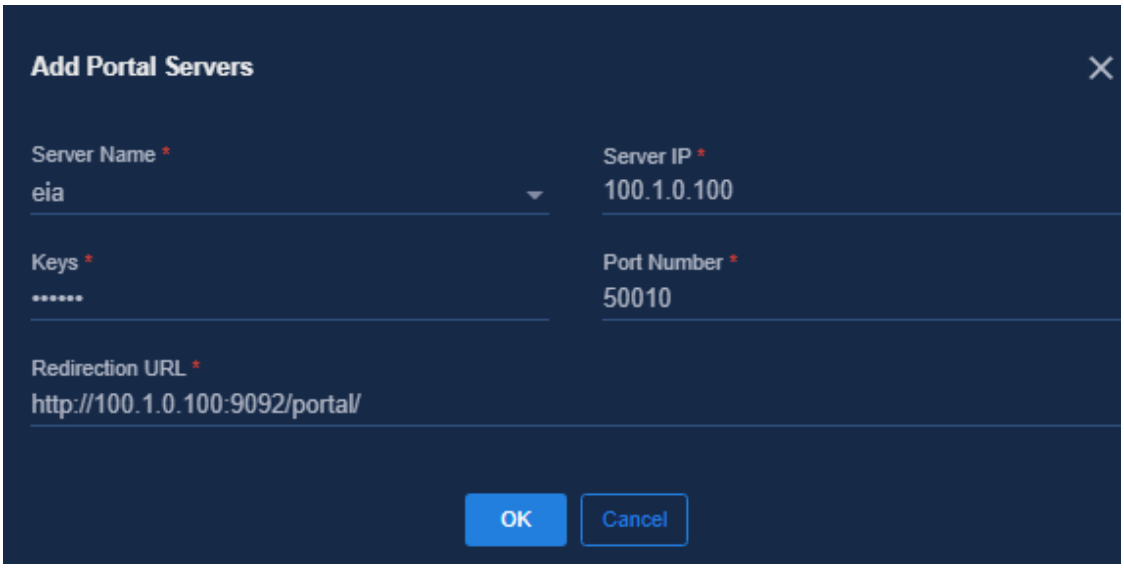
4. 構成が完了したら、**OK** をクリックして構成を保存します。次に示すように、**URL Parameters** 領域で構成結果を表示できます。



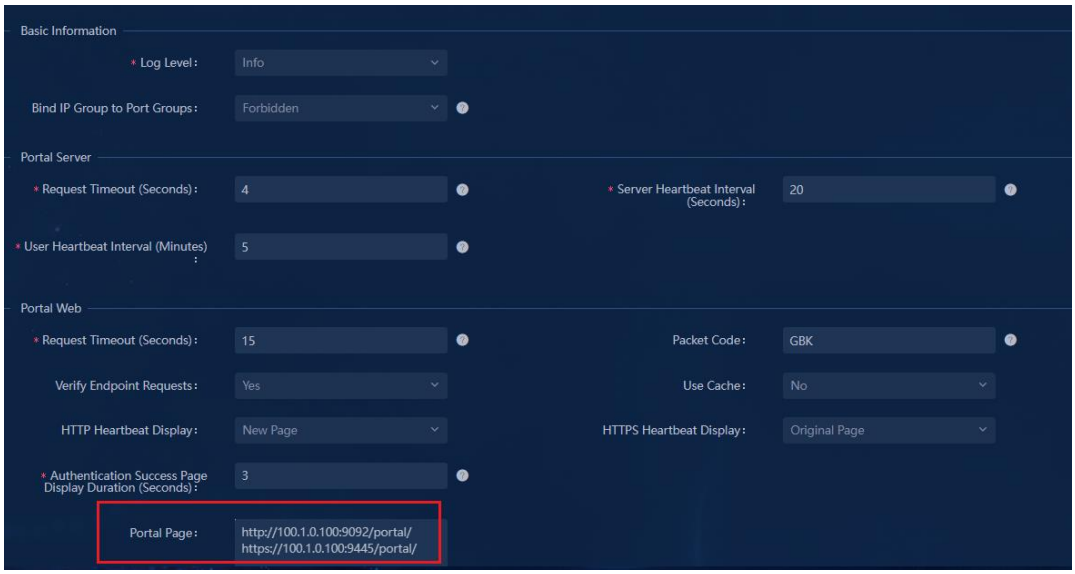
EIA V9 Web ポータルテンプレートの設定

Automation>Campus Network>Device Groups>General Device Groups ページに移動します。ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートのページを開きます。

1. **Add** をクリックし、ドロップダウンリストから **Device Policy Template** を選択します。**Template Type** で **Web Portal Authentication** を選択します。
2. **Portal Servers** 列の **Add** をクリックします。ポータルサーバーを追加するためのページが表示されます。

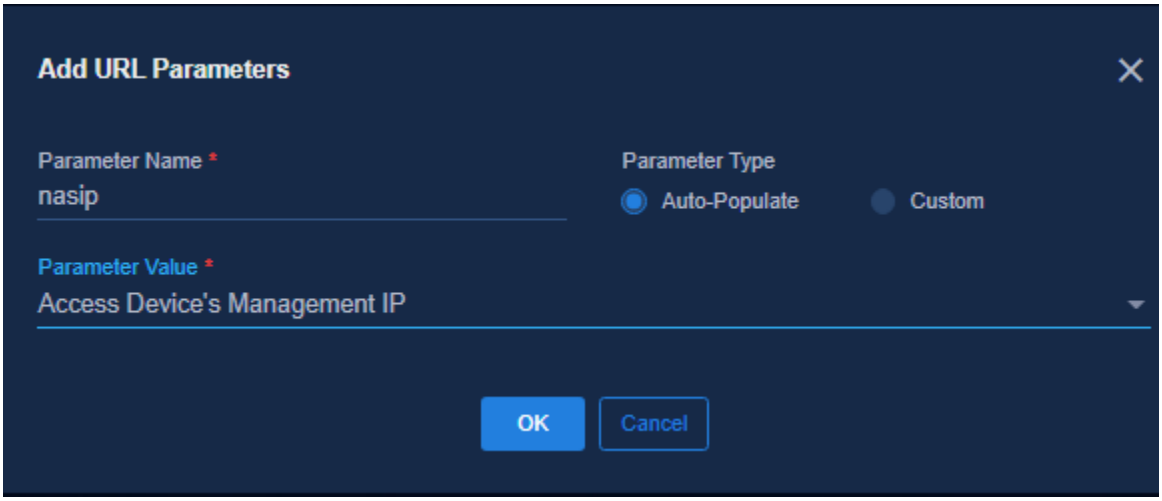


- **Server Name**: サーバー名を指定します。
- **Server IP**: EIA サーバーの IP アドレスを指定します。
- **Keys**: キーは、デバイスポリシーテンプレート AAA のキーと同じです。この例では、123456 です。
- **Port Number**: デフォルト値は 50010 です。デフォルト設定を使用します。
- **URL Redirection**: エンドポイントユーザーが Web ページを開くには、**Automation** > **User** > **Access Service** e ページでアカウントとパスワードを入力します。右上隅にある Portal service management リンクをクリックして、Portal service management ページにアクセスします。**Server Configuration** タブをクリックし、次に示すように、ポータル Web 領域のポータルホームページにリダイレクション URL を表示します。



3. **URL Domain Settings** 列の **Add** をクリックして、**Add URL Domain** ページを開きます。パラメーター名は **nasip** です。パラメーター値はアクセスデバイスの管理 IP を選択します。パラメーター構成

を次の図に示します。



4. 構成が完了したら、**OK** をクリックして構成を保存します。**URL Parameters** 領域で構成結果を表示できます。

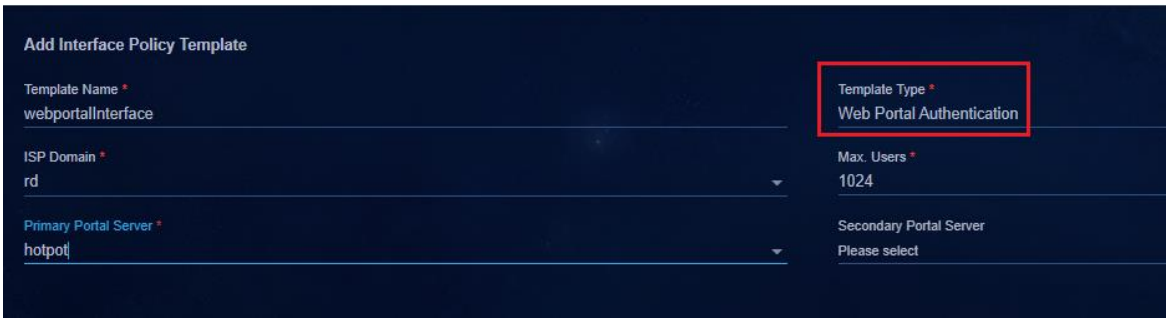
インターフェイスポリシーテンプレート(Web ポータルおよび MAC 認証)

Automation > **Campus Network** > **Device Groups** > **General Device Group** ページに移動します。ページの右上隅にある **Policy Template** をクリックして、ポリシーテンプレートのページを開きます。Add をクリックし、ドロップダウンリストから **Interface Policy Template** を選択して、インターフェイスポリシーテンプレートを追加するページを開きます。

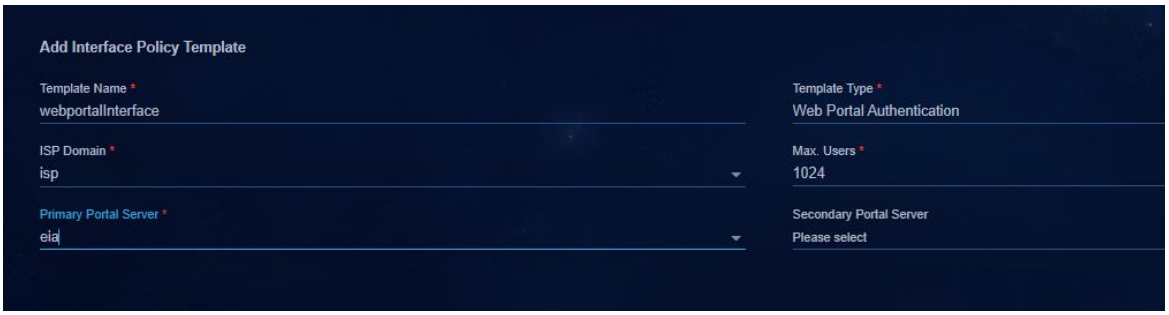
Web Portal インターフェイス ポリシーテンプレートの構成

Template Type として **Web Portal Authentication** を選択します。**ISP Domain** として、「AAA device policy template」で設定された ISP ドメインを選択します。**Primary Portal Server** として、「Configure the web portal template」で設定されたポータルサーバーを選択します。サードパーティー認証サーバーおよび EIA 認証サーバーに関する設定情報は、次のように表示されます。

都市のホットスポット AAA サーバーを設定します。



H3C EIA 認証サーバーを設定します。



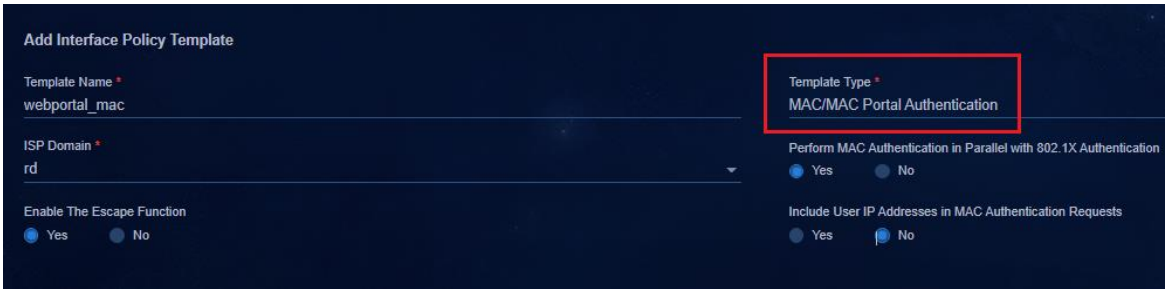
MAC 認証インターフェイスポリシーテンプレートを設定する

Template Type に **MAC/MAC Portal Authentication** を選択します。**ISP Domain** には、「AAA device policy template」で設定された ISP ドメインを選択します。サードパーティー認証サーバーおよび EIA 認証サーバーに関する設定情報は、次のように表示されます。

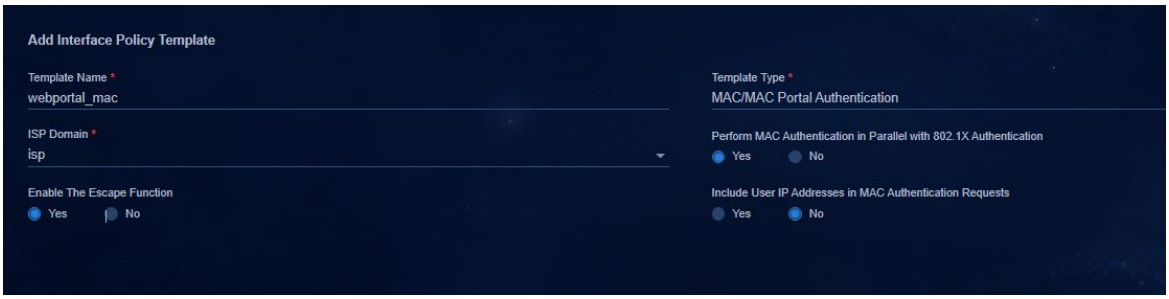
前に設定したAAAおよびWebポータルポリシーテンプレートを選択します。MAC認証ポリシーテンプレートを設定します。WebポータルとMAC認証を組み合わせて、高速MAC認証を実装できます。

- Fast MAC authentication: ユーザーが初めて Web ポータル認証を実行した後、サードパーティー認証サーバーはユーザーの MAC およびアカウント情報を記録します。ユーザーがオフラインになった後に再度認証をトリガーすると、最初に MAC 認証がトリガーされます。サードパーティー認証サーバーは、認証されたユーザーの MAC およびアカウント関係を識別し、ユーザー名やパスワードを必要とせずにユーザーが自動的にオンラインになることを許可します。
- MAC 高速認証には、サードパーティー認証サーバーのサポートが必要です。現在、Dr.COM と Srun の認証サーバーは MAC 高速認証をサポートしています。サードパーティー認証サーバーの詳細な設定については、ベンダーにお問い合わせください。

都市のホットスポット AAA サーバーを設定します。



H3C EIA 認証サーバーを設定します。



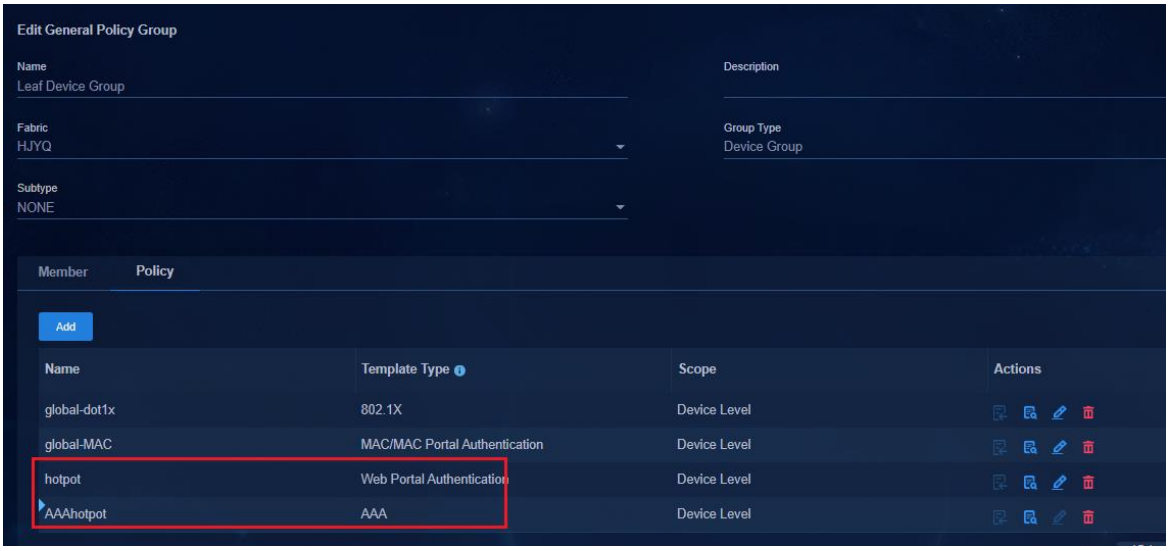
スタティックアクセスインターフェイスグループを追加する

スタティックアクセスインターフェイスグループを作成する設定は、「Add a static access interface group」の設定と同じです。

リーフデバイスグループへのポリシーの展開

Automation > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。**Leaf Device Group** の **Actions** カラムをクリックします。

Policy タブをクリックし、**Add** をクリックして、デバイスグループポリシーを追加するためのページを開きます。前に設定した AAA および Web ポータルポリシーテンプレートを選択します。MAC 認証ポリシーテンプレートを設定します。

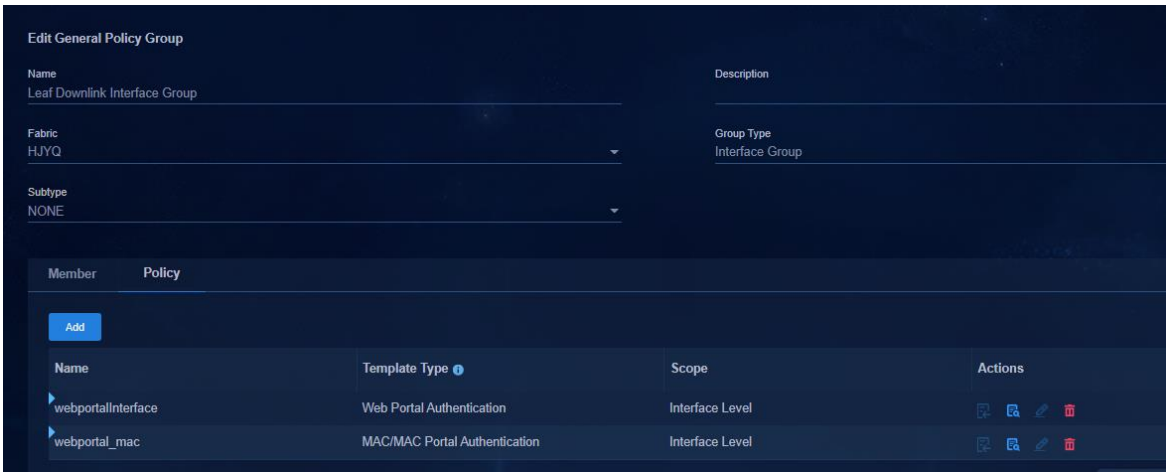


リーフダウンリンクインターフェイスグループへのポリシーの展開

Automation > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動します。**Leaf Downlink Interface Group** の **Actions** カラムをクリックします。

Policy タブをクリックし、**Add** をクリックして、デバイスグループポリシーを追加するためのページを開きま

す。次の図に示すように、インターフェイスを発行する Web ポータルのポリシーテンプレートと MAC 認証ポリシーテンプレートを選択します。



レイヤー2 ネットワークドメインおよびセキュリティグループの作成

レイヤー2 ネットワークドメインおよびセキュリティグループを作成する設定は、「Configure static AC authentication」の設定と同じです。詳しくは、「Create a Layer 2 network domain」および「Create a security group」を参照してください。

リーフデバイスへの設定の展開

サードパーティー認証サーバーを構成する

- AAA サーバーを次のように設定します。

```
#
radius scheme rd
 primary authentication 10.99.12.189 vpn-instance vpn-default  // サードパーティ認証サーバーの IP アドレス。
 primary accounting 10.99.12.189 vpn-instance vpn-default
 accounting-on enable send 255 interval 15
 key authentication cipher $c$3$01oCMscY9DPxDQb6Hca466591nHq92rWSQ==
 key accounting cipher $c$3$RCI/F6pW6YdEZ8kiKZ44niy+ubmo8FrrIg==
 timer realtime-accounting 15
 user-name-format without-domain
 vpn-instance vpn-default
 attribute translate
 stop-accounting-packet send-force
 attribute convert H3c-User-Group to H3C-Microsegment-Id received
 microsegment 3502 associate vsi vsi4
 microsegment 3504 associate vsi vsi3
 microsegment 3505 associate vsi vsi3
```

```
 microsegment 4090 associate vsi vsi5
#
```

- Web Portal を次のように構成します。

```
[Leaf-s75]dis web-auth server
Web server: Hotspot
  Type                    : Remote
  IP address              : 10.99.12.189
  IPv6 address            : Not configured
  URL                     : http://10.99.12.189/a79.html
     Track ID             : 1
     Server state         : Inactive
  URL parameters          : wlanacip=130.1.0.5
                            wlanacname=leaf-130.1.0.5
 [Leaf-s75]
```

- リーフダウンリンクインターフェイス設定を展開します。

  スタティックアクセスインターフェイスグループで設定されたアクセスデバイスに接続されたリーフデバイスで、サービスインスタンス設定をダウンリンクインターフェイスに展開します。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 mac-authentication            // MAC 認証
 mac-authentication domain rd
 mac-authentication parallel-with-dot1x
 port-security free-vlan 1 4094
 web-auth domain rd               // Web 認証
 web-auth enable apply server hotspot
 #
 service-instance 2801
  encapsulation s-vid 2801
  xconnect vsi vsi18
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

H3C EIA 認証サーバーの設定

```
#
radius scheme hz1
 primary authentication 110.0.0.100 vpn-instance vpn-default
 primary accounting 110.0.0.100 vpn-instance vpn-default
 accounting-on enable send 255 interval 15
```

```
 key authentication cipher $c$3$zHvt8Q9eIMKWJ/BOJgUXSJPg65IBSQ==
 key accounting cipher $c$3$Tp0bJhOUACFbng9D/kjF/hIKqM3Gsw==
 timer realtime-accounting 15
user-name-format without-domain
 vpn-instance vpn-default
 attribute translate
 stop-accounting-packet send-force
 attribute convert H3c-User-Group to H3C-Microsegment-Id received
microsegment 3502 associate vsi vsi4
microsegment 3504 associate vsi vsi3
microsegment 3505 associate vsi vsi3
microsegment 4090 associate vsi vsi5
#
```

- Web Portal を次のように構成します。

```
[6550xe-up]disp web-auth server
Web server: eia
  Type                  : Remote
  IP address            : 110.0.0.100
  IPv6 address          : Not configured
  URL                   : http://110.0.0.100:9092/portal/
     Track ID           : 1
     Server state       : Active
  URL parameters        : Not configured

[6550xe-up]
```

- リーフダウンリンクインターフェイス設定を展開します。

  スタティックアクセスインターフェイスグループで設定されたアクセスデバイスに接続されたリーフデバイスで、サービスインスタンス設定をダウンリンクインターフェイスに展開します。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 mac-authentication            // MAC 認証
 mac-authentication domain hz1
 mac-authentication parallel-with-dot1x
 port-security free-vlan 1 4094
 web-auth domain hz1               // Web 認証
 web-auth enable apply server eia
 #
 service-instance 2801
  encapsulation s-vid 2801
  xconnect vsi vsi3506
 #
```

```
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

サードパーティー認証サーバーを構成する

H3C EIA 認証サーバーを例にとると、Portal サーバーと RADIUS サーバーを設定する必要があります。

- ポータルサーバーの設定:リーフデバイスの **wlanacname** と **wranacip** の設定済みパラメーターに従って、パラメーターを設定します。
- RADIUS サーバーの設定:リーフデバイス上の RADIUS スキームの設定に従って、RADIUS サーバーの IP アドレスを設定します。
  - DRNI 以外の環境では、RADIUS NAS IP はリーフデバイスの VSI 4094 IP アドレスです。
  - DRNI 環境では、ローカルとピアの NAS IP アドレスは RADIUS スキームで構成されます。両方の IP アドレスを構成する必要があります。

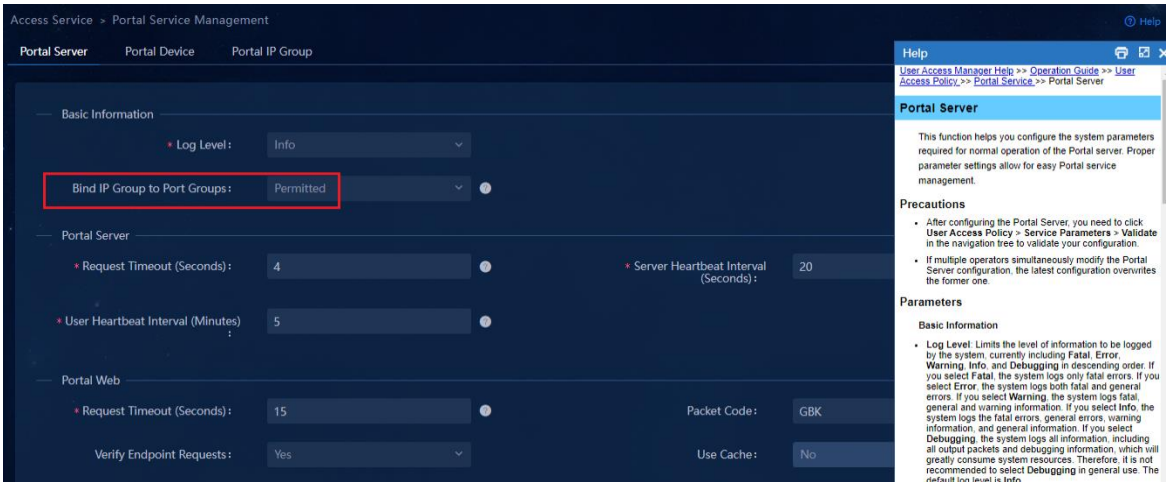
ポータルサーバーの構成

サーバーの設定

Automatic > **User Service** > **Access Service** ページにナビゲートします。右上隅にある **Portal Service** リンクをクリックして、**Portal Service Management** ページに移動します。このページで、サーバー、デバイス、および IP アドレスグループを設定できます。

Web ポータルのシナリオには、別の EIA を使用できます。この項では、EIA を使用して Web ポータルサーバーを説明します。

Basic Information のパラメーター、および **Portal Server** 列と **Portal Web** 列のパラメーターには、デフォルト設定を使用します。**Basic Information** 列で、**Permitted for Bind IP Group to Port Groups** を設定します。各パラメーターの詳細は、ページの右上隅にある **Help** リンクを参照してください。

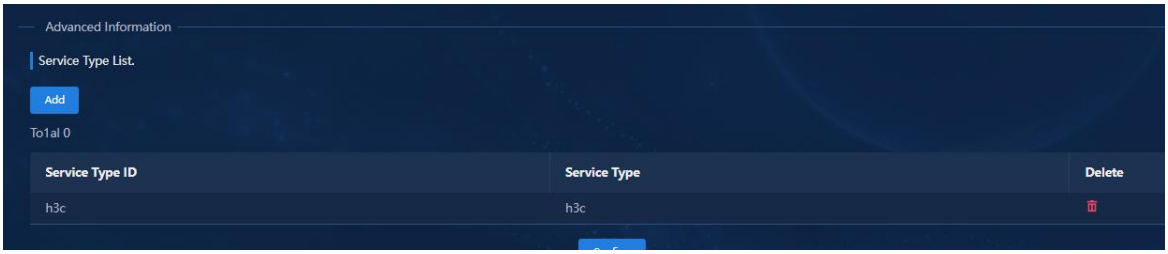


注:

- **Portal Server** の設定が完了したら、**Automation** > **User** > **Access Parameters** > **Validate** で、設定を有効にするために **Validate** をクリックする必要があります。
- 複数のオペレーターが Portal Server 構成に対して同時に変更を行った場合、最後に変更された変更が前の変更を上書きします。

Advanced Information 列の **Add** をクリックします。次の図に示すように、**Service Type List** を開き、必要に応じてサービスタイプを追加します。

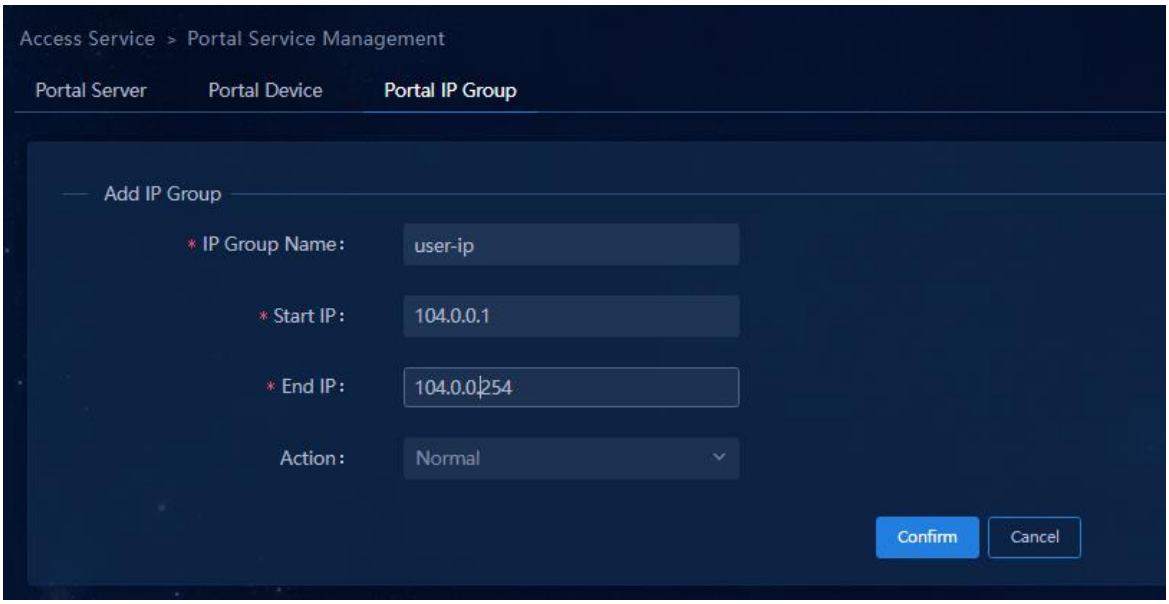
- **Service Type ID**: デバイスは、ユーザーが選択したサービスタイプに応じて、対応する認証スキームを決定します。管理者は、実際のネットワーキングおよび iMC サービスとデバイスの設定に応じて、対応する設定を行います。
- **Service Type**: **Service Type ID** は、デバイスで使用される情報です。ユーザーはこれを明確に理解できます。**Service Type ID** は、ユーザーがサービスタイプを理解するのに役立つように、ポータル認証ホームページに表示されます。サービスタイプ情報は必須であり、既存のサービスタイプ情報と同じにすることはできません。サービスタイプの数は 64 を超えることはできません。



IP アドレスプールの設定

Automatic > **User Service** > **Access Service** ページに移動します。右上隅にある **Portal Service** リンクをクリックして、**Portal Service Management** ページに移動します。**IP Address Group Configuration** タブをクリックし、IP アドレスグループを追加または変更します。

- **IP Group Name**: IP アドレスグループの名前を指定します。
- **IPv6**: IP アドレスグループが IPv6 アドレスであるかどうかを区別します。
- **Start IP**: IP アドレスグループの開始 IP アドレスを指定します。
- **End IP**: IP アドレスグループの終了 IP アドレスを指定します。
- **Action**: **Normal** を選択してください。



デバイスを構成する

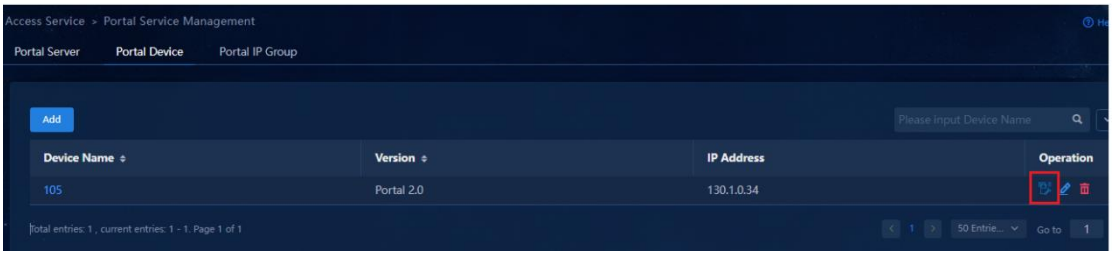
Automatic > **User Service** > **Access Service** ページにナビゲートします。右上隅にある **Portal Service** リンクをクリックして、**Portal Service Management** ページに移動します。**Device Configuration** タブをクリックします。

1. **Add** をクリックして、デバイス設定ページを開きます。

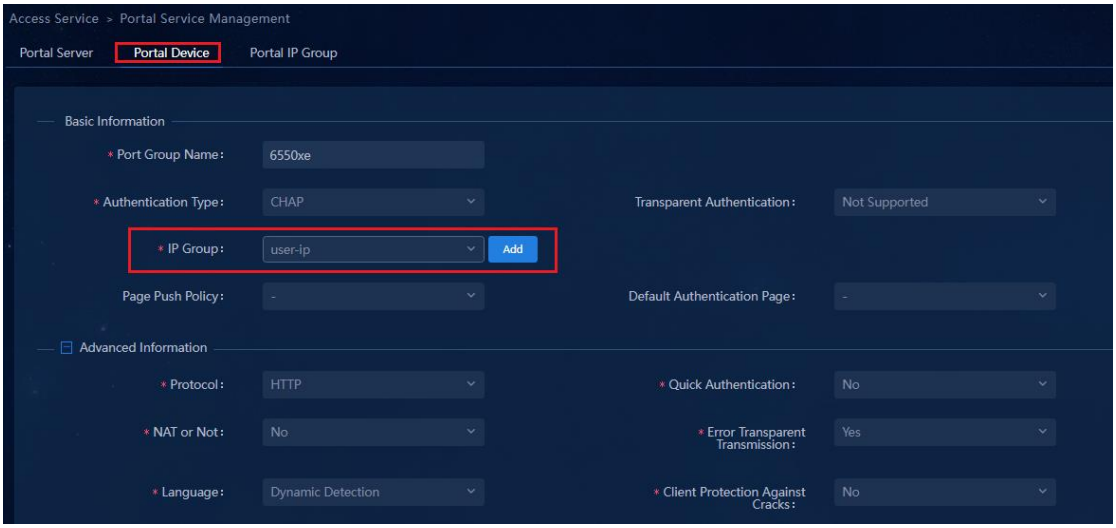
   さまざまな Leaf デバイスのデバイス設定を追加します。インターフェイスグループは、前に作成した IP アドレスグループを共有します。

   - **Device Name**: ポータルアクセスデバイスの名前は、既存のデバイスの名前と同じにすることはできません。
   - **Public IP address**: Portal アクセスデバイスの IP アドレスおよび VSI インターフェイス 4094 アドレス。
   - **Key**: ポータルサーバーの両端は、デバイスと通信するときに同じ共有キーを設定する必要があります。そうしないと、AAA ポリシーテンプレートが設定されているときに、受信者の検証とキーセットを通過できません。
   - **Advanced Information**: 既定の設定を使用します。

2. 構成が完了したら、**OK** をクリックして構成を保存します。リストの **Action** 列をクリックして、ポータルグループ情報管理ページに移動します。



3. ポートグループを追加するには、**Add** をクリックします。次のように、作成した IP アドレスグループをドロップダウンリストから選択します。



RADIUS サーバーの設定

アクセスデバイス設定は、RADIUS 認証に使用されます。デフォルトでは、コントローラはリーフデバイスに関する情報を EIA に同期します。手動設定は必要ありません。

EIA がサードパーティー認証デバイスとして設定されている場合は、アクセスデバイスに関する情報を手動で設定する必要があります。

- **Non-DRNI networking**: リーフデバイス VSI 4094 の IP アドレスをアクセスデバイスの IP アドレスとして設定します。
- **DRNI networking**: RADIUS のリーフデバイス nas-ip の IP アドレスと、ローカルおよびピアの IP アドレスを設定します。

ユーザー認証の構成

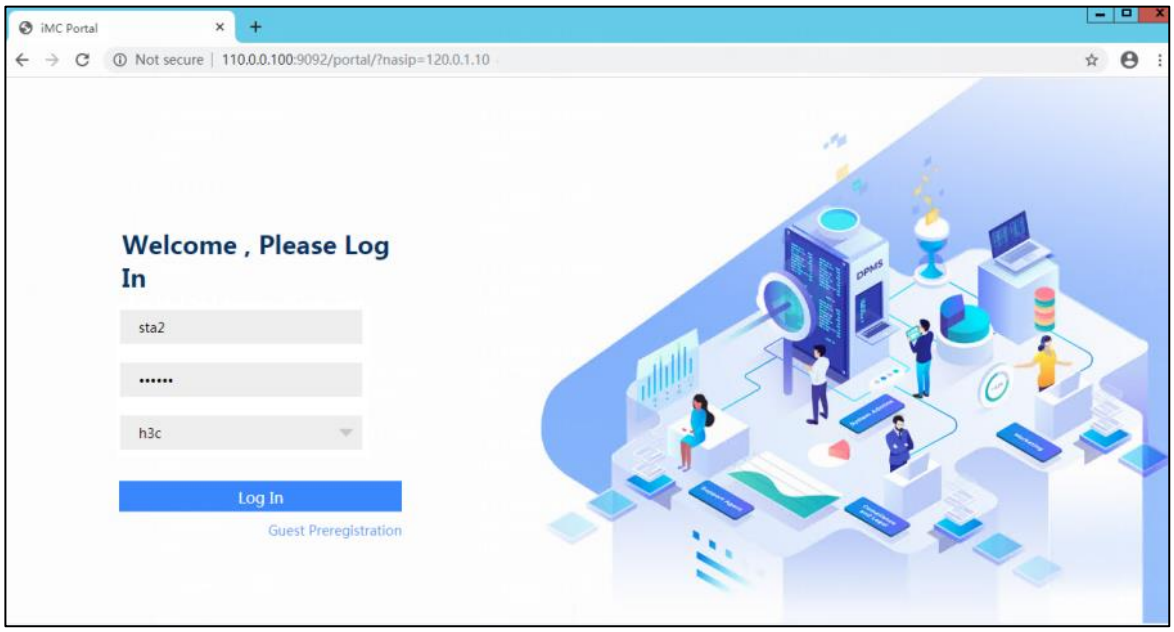
EIA 認証サーバーは、HTTP/HTTPS を実行するブラウザまたはポータルクライアント(iNode クライアント)

を実行するホストに接続できます。Web ポータルのシナリオ EIA アドレスは、別の EIA を使用できます。このセクションでは、EIA を使用して Web ポータルサーバーを説明します。

注:

異なるデバイスのポートグループは、IP アドレスグループを共有します。HTTP/HTTPS プロトコルを実行するブラウザは、現在のデバイスバージョンでサポートされています。iNode クライアントモードは、現在のデバイスバージョンではサポートされていません。

エンドポイントが Internet Explorer ページを開き、IP アドレスを入力すると、エンドポイントは Web Portal で設定された URL ページにリダイレクトされます。



ログインするためのユーザー名とパスワードを入力します。

iNode クライアントを使用して、ページの右上隅にある更新アイコンをクリックします。ポータルサーバー情報を取得します。認証を完了するには、ユーザー名とパスワードを入力します。

ゲストアクセスまたは認証失敗時のアクセス

重要:

- ゲストアクセスと認証失敗時のアクセスをサポートしているのは、802.1X だけです。
- ゲストアクセスをイネーブルにする場合は、ユニキャストトリガーをイネーブルにする必要があります。
- Guest と Mac Portal は相互に排他的です。

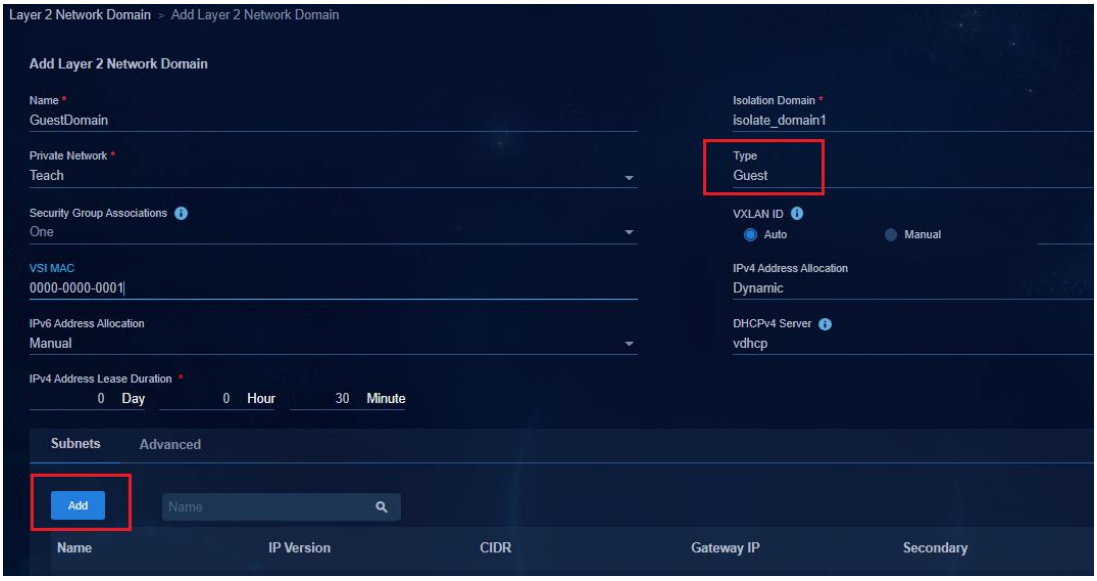
ゲストアクセス

ゲストオンラインは、主に、構成された認証サーバーなしでネットワークにアクセスした後、ユーザーが特定のセキュリティグループ内のリソースにアクセスできるようにするために使用されます。特定のセキュリティグループは、ゲストタイプのセキュリティグループです。

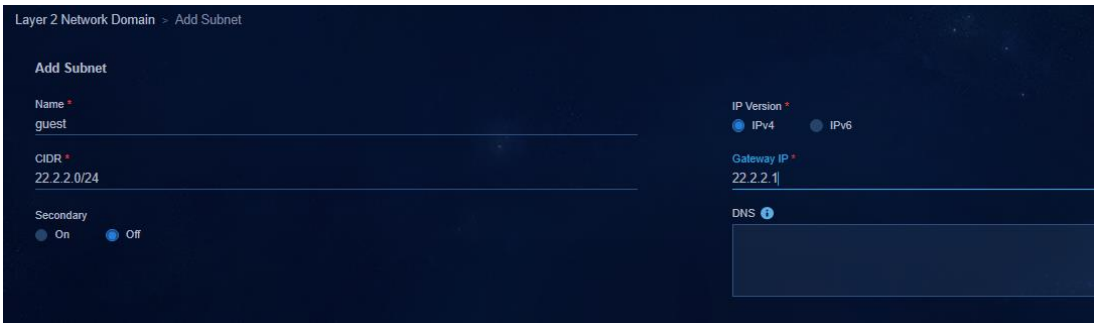
ゲストレイヤー2 ネットワークドメインを作成する

Automation > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動します。

1. **Add** をクリックして、**Layer 2 Network Domain** ページを開きます。パラメーターは次のように設定されます。
   - **Private Network**: **User Private Network** ユーザープライベートネットワークを選択することをお勧めします。
   - **Type**: **Guest** を選択します。
   - **IPv4 Address Allocation**: Auto を選択します。
   - **DHCP Server**: DHCPv4 サーバーを選択します。
   - **IPv4 Address Lease Duration**: デフォルトでは 30 分です。



2. **Subnets** タブをクリックし、**Add** をクリックしてサブネットネットワークセグメントを追加します。

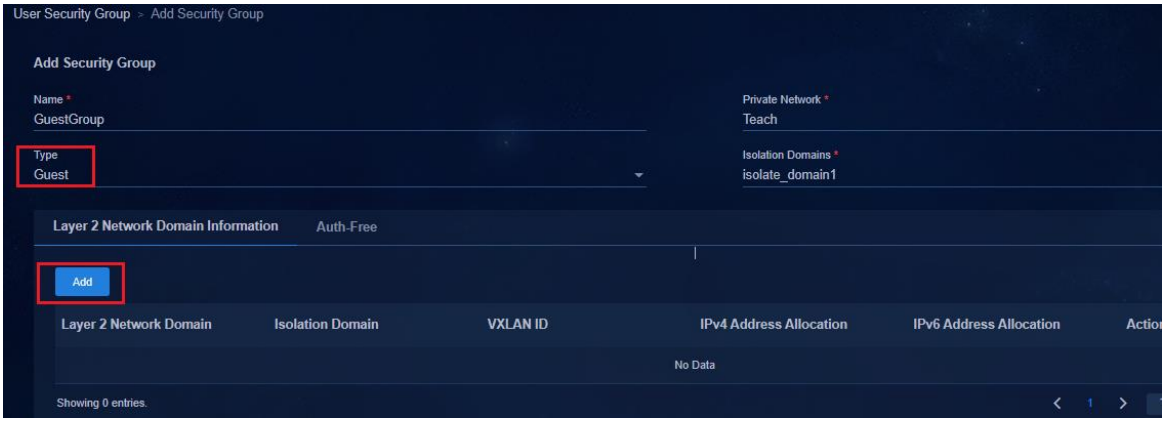


3. 設定が完了したら、**OK** をクリックして **Layer 2 Network Domain** ページに戻ります。設定を完了するには、**OK** をクリックします。

ゲストセキュリティグループを作成する

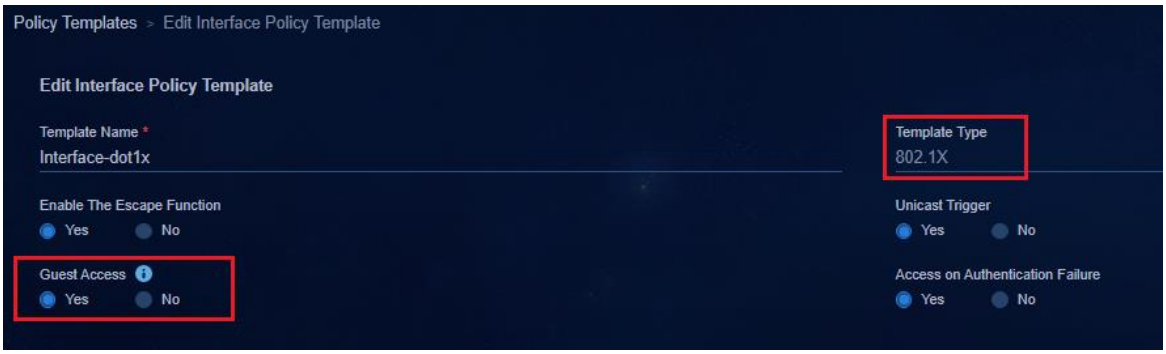
Automation > **Campus Network** > **Security Group** > **User Security Group** ページに移動します。**Add** をクリックして、セキュリティグループを追加するためのページを開きます。

分離ドメインに設定できるゲストセキュリティグループは 1 つだけです。分離ドメインに複数のファブリックがある場合、すべてのファブリックが 1 つのゲストセキュリティグループを共有します。**Type** に **Guest** を選択します。**Layer 2 Network Domain Information** タブを選択し、**Add** をクリックして、レイヤー2 ネットワークドメインを追加するページを開きます。以前に設定したゲストタイプのレイヤー2 ネットワークドメインを選択します。



ポリシーテンプレートのゲストアクセスを有効にする

『Interface policy template - 802.1X authentication』でゲスト機能を有効にします。

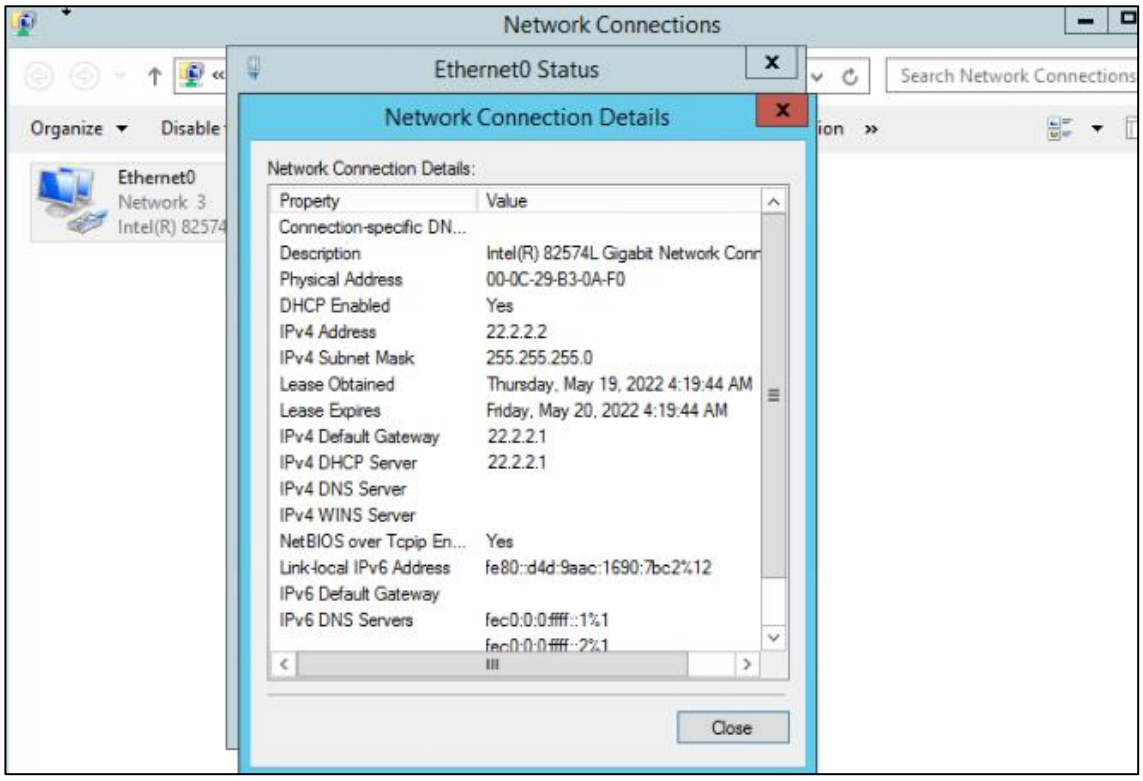


ポリシーテンプレートがリーフダウンリンクインターフェイスグループに適用されると、次の設定が配信されます。

```
#
interface Ten-GigabitEthernet1/0/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 stp tc-restriction
mac-based ac
 dot1x
undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x guest-vsi vsi10     // ゲストに対応する VSI
dot1x critical eapol
 dot1x critical profile SDN_GLOBAL_CRITICAL_PROFILE
 port-security free-vlan 1 4094
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

ユーザーのオンラインとアドレスの取得

エンドポイント PC がネットワークにアクセスすると、ユーザーはゲストの認可とアドレスを直接取得し、ゲストセキュリティグループの特定のネットワークリソースにアクセスします。



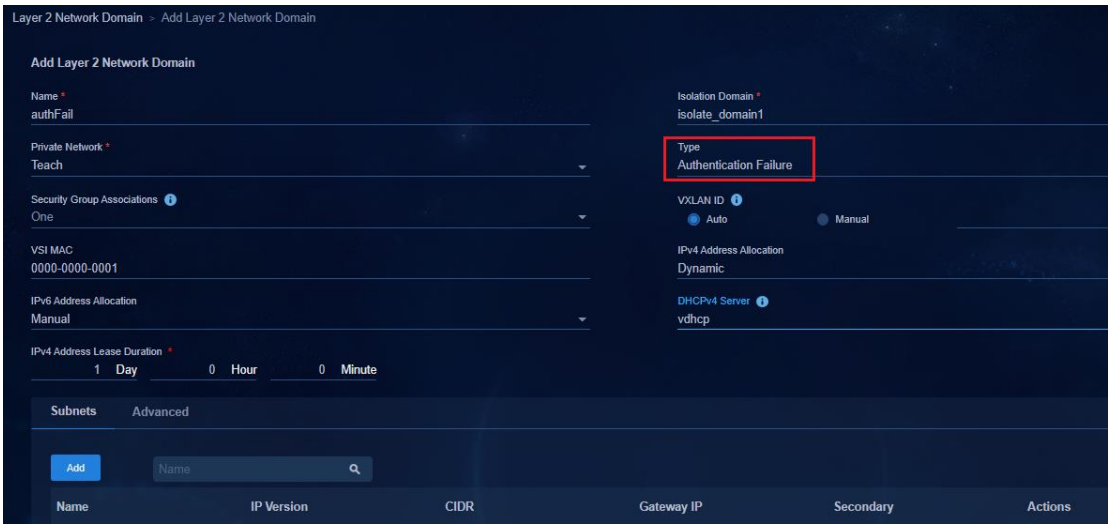
認証失敗時のアクセス

認証の失敗が発生した場合、ユーザーは 802.1X 認証の失敗後に特定のセキュリティグループのネットワークとリソースにアクセスできます。特定のセキュリティグループは、認証失敗タイプのセキュリティグループです。

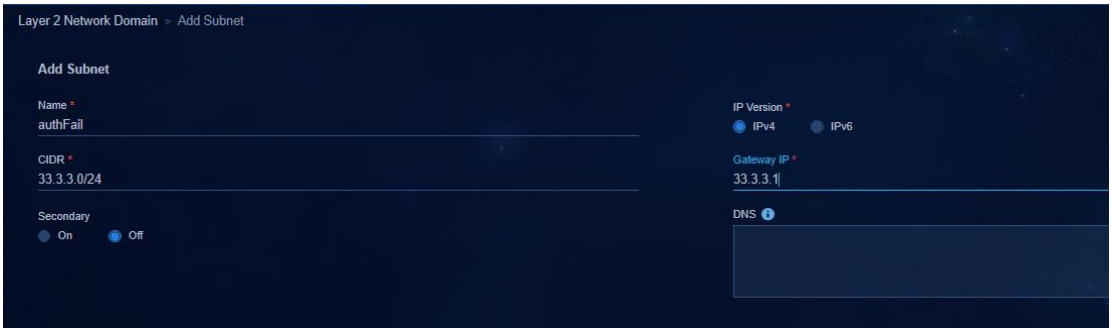
認証が失敗したときにアクセスするためのレイヤー2 ネットワークドメインの作成

Automation > **Campus Network** > **Private Network** > **Layer 2 Network Domai** ページに移動します。

1. **Add** をクリックして、**Layer 2 Network Domain** ページを開きます。パラメーターは次のように設定されます。
   - **Private Network**:: **User Private Network** を選択することをお勧めします。
   - **Type**: **Authentication Failure** を選択します。
   - **IPv4 Address Allocation**: **Auto** を選択します。
   - **DHCP Server**: DHCPv4 Server を選択します。
   - **IPv4 Address Lease Duration**: デフォルト設定は 1 日です。



2. **Subnets** タブをクリックし、**Add** をクリックしてサブネットネットワークセグメントを追加します。

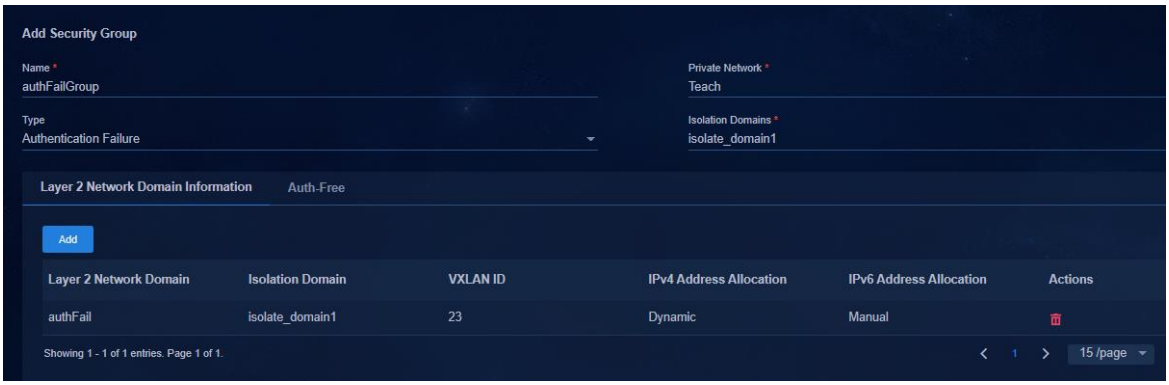


3. 設定が完了したら、**OK** をクリックして **Layer 2 Network Domain** ページに戻ります。設定を完了するには、**OK** をクリックします。

認証が失敗したときにアクセスするセキュリティグループを作成する

Automation > **Campus Network** > **Security Group** > **User Security Group** ページに移動します。**Add** をクリックして、セキュリティグループを追加するためのページを開きます。

1 つの分離ドメインに構成できる認証失敗セキュリティグループは 1 つのみです。1 つの分離ドメインに複数のファブリックが存在する場合、すべてのファブリックが同じ認証失敗セキュリティグループを共有します。**Type** で **Authentication Failure** を選択し、**Add** をクリックします。認証失敗タイプが前に構成されているレイヤー2 ネットワークドメインを選択します。



ポリシーテンプレートの認証失敗時のアクセスを有効にする

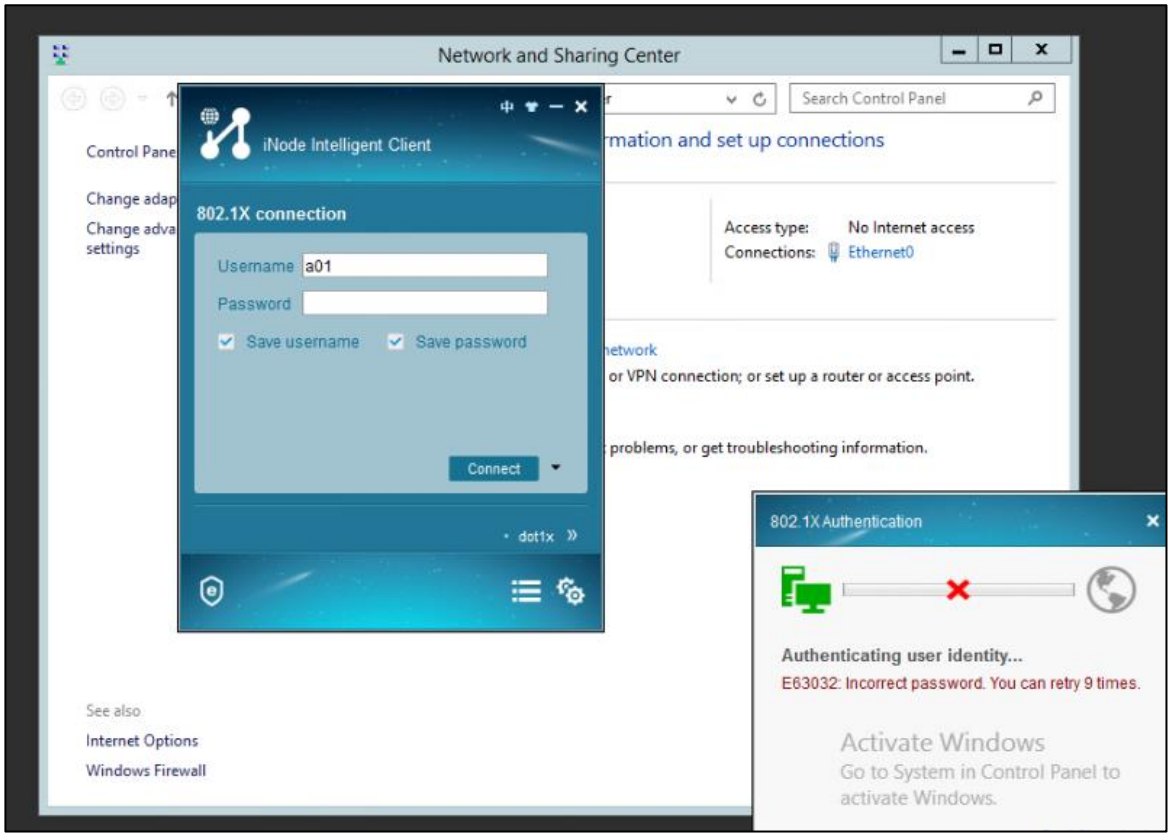
『Interface policy template - 802.1X authentication』で認証失敗時のアクセスを有効にする

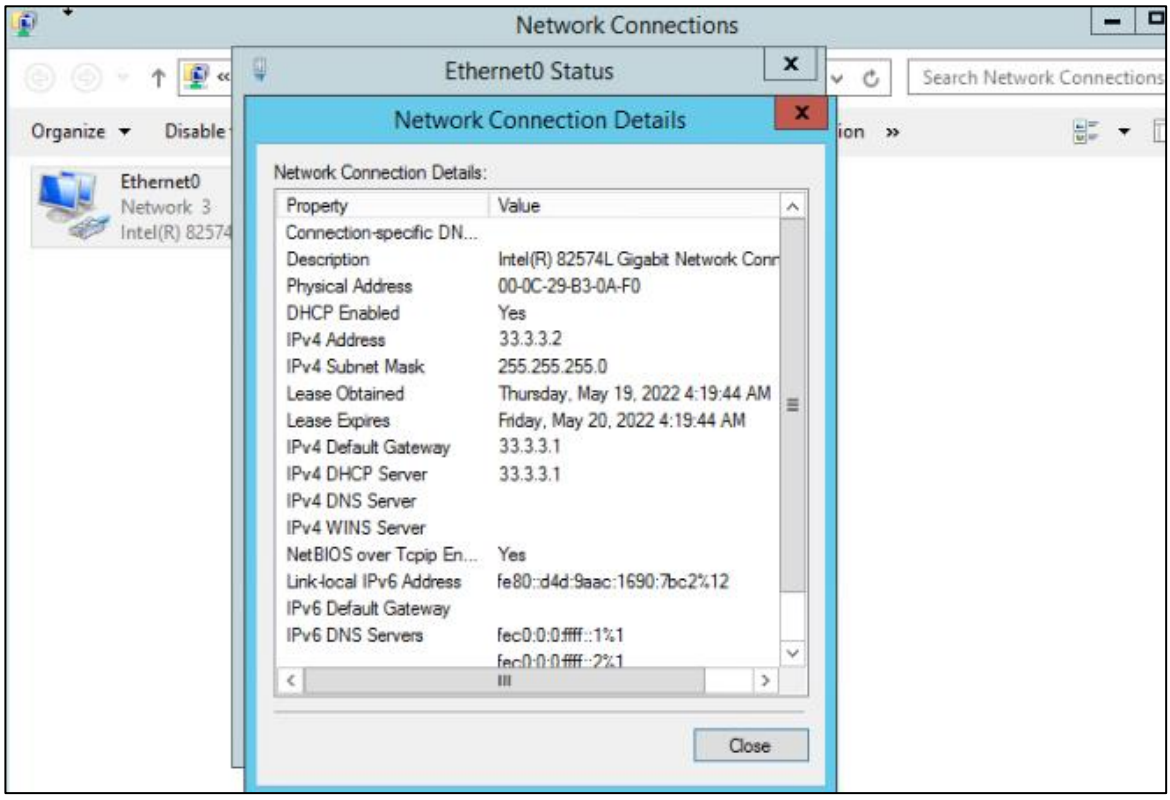
ポリシーテンプレートがリーフダウンリンクインターフェイスグループに適用されると、次の設定が発行されます。

```
#
interface Ten-GigabitEthernet1/0/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 stp tc-restriction
 mac-based ac
 dot1x
undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x guest-vsi vsi10
 dot1x auth-fail vsi vsi11  //認証失敗の VSI
 dot1x critical eapol
 dot1x critical profile SDN_GLOBAL_CRITICAL_PROFILE
 port-security free-vlan 1 4094
 #
service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

ユーザーのオンラインとアドレスの取得

エンドポイントまたは PC で 802.1X 認証を開始します。認証が失敗すると、ユーザーは、認証に失敗したユーザーに固有のセキュリティグループで指定されたネットワークリソースにアクセスできます。




Network Connections
Search Network Connections
Organize
Disable
Ethernet0
Network 3
Intel(R) 82574
Ethernet0 Status
Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DN...
Description
Intel(R) 82574L Gigabit Network Conn
Physical Address
00-0C-29-B3-0A-F0
DHCP Enabled
Yes
IPv4 Address
33.3.3.2
IPv4 Subnet Mask
255.255.255.0
Lease Obtained
Thursday, May 19, 2022 4:19:44 AM
Lease Expires
Friday, May 20, 2022 4:19:44 AM
IPv4 Default Gateway
33.3.3.1
IPv4 DHCP Server
33.3.3.1
IPv4 DNS Server
IPv4 WINS Server
NetBIOS over Tcpip En...
Yes
Link-local IPv6 Address
fe80::d4d:9aac:1690:7bc2%12
IPv6 Default Gateway
IPv6 DNS Servers
fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
Close

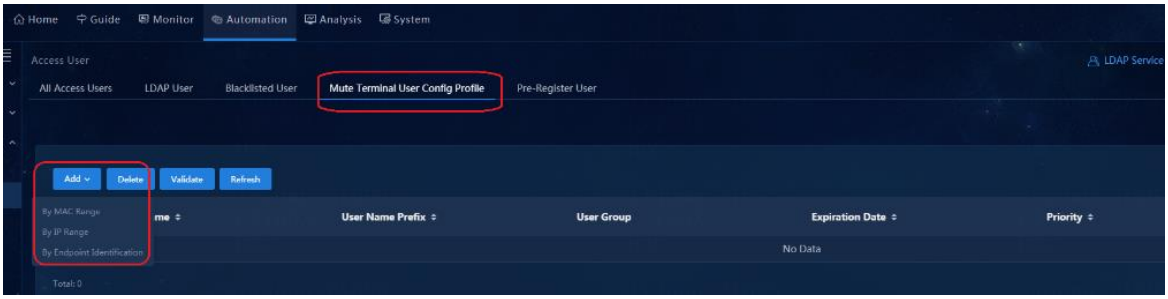
ブロードバンド IoT サービスを構成する

AD-Campus ソリューションのブロードバンド IoT サービスは、MAC アドレスを通じて認証されます。ユーザーはトラフィックを通じて認証をトリガーします。EIA はユーザーを識別し、ブロードバンド IoT サービス用に設定されたルールを照合します。システムは、ユーザーの MAC アドレスに基づいてアカウントとパスワードを自動的に作成するため、ユーザーはユーザー名とパスワードを入力せずに、認証を通じて直接オンラインになることができます。

設定は、MAC アドレス範囲、IP アドレス範囲、またはエンドポイント ID に基づいて行うことができます。

Identification method	Identification records	Defects	Endpoint information
OUI MAC	2616	Unable to distinguish different endpoint types from the same manufacturer, such as Lenovo PCs and printers	Vendor
DHCP fingerprint	373	The DHCP fingerprint of a PC using Linux system is the same as that of a non-intelligent endpoint	OS, type
HTTP User Agent	1249	IP monitors, access control, all-in-one cards and other endpoints will not send HTTP packets. In other scenarios, intelligent endpoints do not need to use HTTP, for example, mobile Internet access without browser	Vendor, OS, model

Automation > **User** > **Access User** > **Mute Terminal User Config Profile** ページに移動します。



- **By MAC Range**: MAC アドレス範囲を設定します。ユーザーの MAC アドレスが構成済の MAC アドレス範囲と一致する場合、システムは自動的にユーザーのアカウントを作成し、そのアカウントでユーザーを認証します。次に、認証済ユーザーをユーザーセキュリティグループに追加し、ユーザーセキュリティグループの IP アドレスをユーザーに割り当てます。
- **By IP Range**: IP アドレス範囲を設定します。Leaf デバイスのダウンリンクインターフェイスで **mac-authentication carry user-ip exclude-ip acl*****コマンドを設定します。
- **By Endpoint Identification**: エンドポイントデバイスパラメーター情報を設定します。エンドポイントフィンガープリント情報は、クライアントがオンラインになるように認証するときに伝送されます。エン

ドポイントフィンガープリント情報が設定されたエンドポイントデバイスパラメーター情報と一致する場合、システムは自動的にユーザーのアカウントを作成し、そのアカウントでユーザーを認証します。次に、システムは認証されたユーザーをユーザーセキュリティグループに追加し、ユーザーセキュリティグループの IP アドレスをユーザーに割り当てます。

重要:

- 設定された MAC アドレス範囲と IP アドレス範囲のプライオリティは異なる必要があります。クライアントが MAC アドレス範囲と IP アドレス範囲の両方に一致する場合、プライオリティの高い方が適用されます。プライオリティ値が小さいほど、プライオリティは高くなります。
- mac-authentication carry user-ip コマンドの制約事項:このコマンドは、**By IP Range authentication** および **Bind User IP Address authentication** がアクセスポリシーで設定されている場合にだけ設定します。それ以外の場合は、このコマンドを設定しないでください。エンドポイント装置に認証用のスタティック IP アドレスを設定する必要がある場合、コントローラは ARP snooping コマンドを発行して、スタティック IP アドレスを EIA に配信します。

MACアドレス範囲に基づく高速オンライン

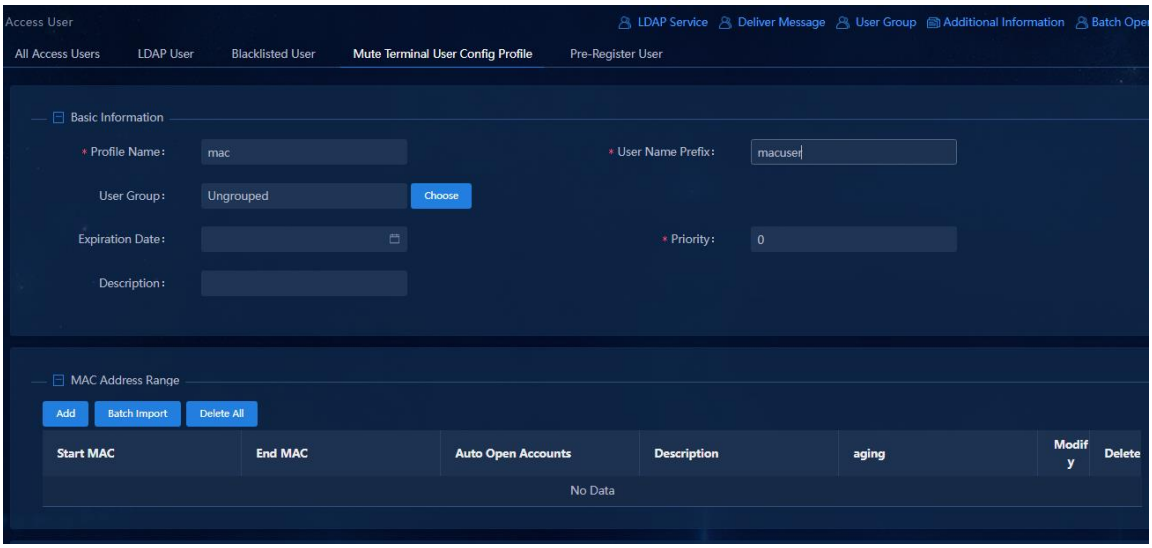
OUI MAC の範囲によって、手動追加とバッチインポートの 2 つのモードが使用可能です。

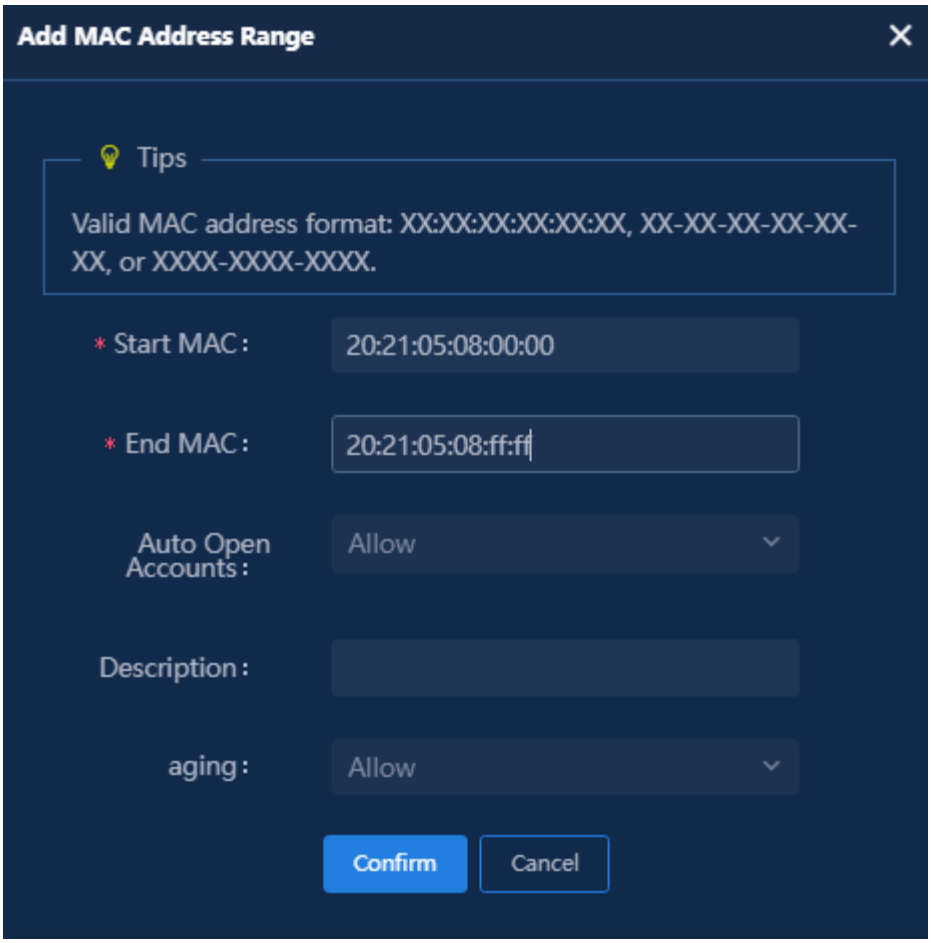
Add をクリックし、ドロップダウンリストから **By MAC Range** を選択します。プライオリティを 0～999 の範囲で設定します。デフォルト値は 0 です。値が小さいほど、プライオリティは高くなります。

MAC Address Range 領域では、MAC アドレス範囲を手動で追加したり、MAC アドレスをインポートしたりできます。

MAC アドレス範囲を手動で追加する

Add をクリックして、**Add MAC Address Range** ページを開きます。MAC アドレス範囲を入力し、**Confirm** をクリックします。複数の MAC アドレス範囲を追加できます。各アドレス範囲は、要件に従って構成できます。

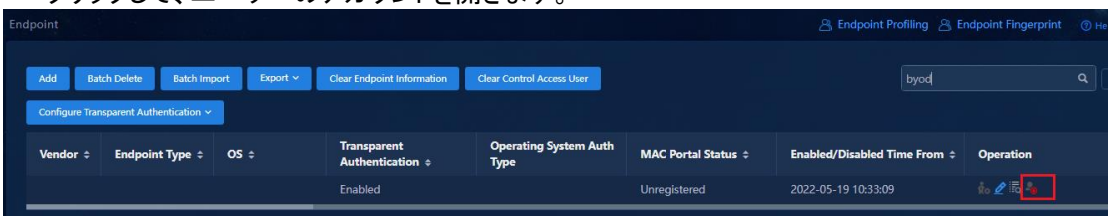




このページのパラメーターを次のように設定します。

- **Auto Open Accounts**: **Allow** または **Disable** を設定します。
  - **Allow**: エンドポイントが MAC アドレス範囲と一致する場合、システムはユーザーを認証するアカウントを自動的に作成し、認証されたユーザーを対応するセキュリティグループに追加し、ユーザーの IP アドレスを取得します。

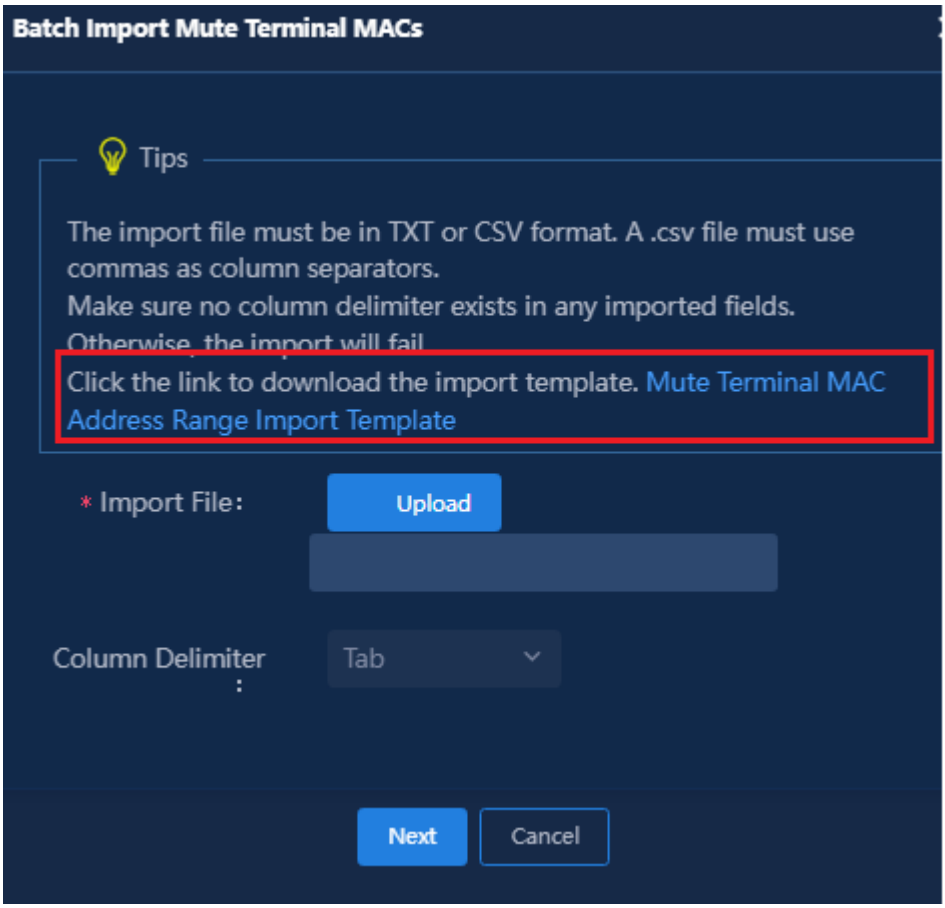
- **Disable**: アカウントは自動的に作成されません。認証されたユーザーは、MAC Portal 認証をトリガーして、BYOD セキュリティグループに入ります。管理者は、**Monitor** > **Monitor List** > **Endpoint** > **Access Endpoin** ページに移動し、**Operation** カラムの open account アイコンをクリックして、ユーザーのアカウントを開きます。



- **Aging**: **Allow** または **Prohibit** を設定します。
  - **Allow**: EIA は、トラフィックがなく、NAS がリブートし、NAS ポートがダウンした場合に、認証されたミュートエンドポイントがタイムアウト後にオフラインになることを許可します。
  - **Prohibit**: トラフィックがなく、NAS がリブートし、NAS ポートがダウンしている場合、EIA はミュートエンドポイントのエージングを許可せず、EIA 上のミュートエンドポイントはオンラインのままになります。Leaf デバイスが回復すると、Leaf は EIA からオンライン情報を要求して、ダム端末がトラフィックを送信せず、オンラインステータスへの復元に失敗した場合に、ミュートエンドポイントのオンラインステータスを復元します。

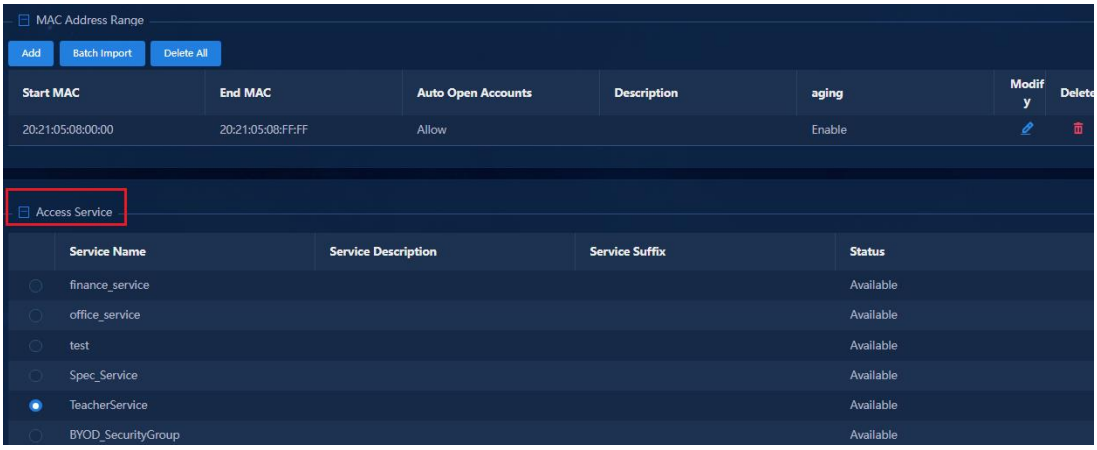
アクセスユーザーを一括インポートする

1. **Batch Import** をクリックして、**Batch Import Mute Terminal MACs** ページを開きます。バッチインポートでは、インポートテンプレートのダウンロードがサポートされます。**Mute Terminal Mac Address Range Import Template** リンクをクリックして、インポートテンプレートをダウンロードします。ダウンロードしたテンプレートに従ってインポートする MAC アドレス範囲を入力します。

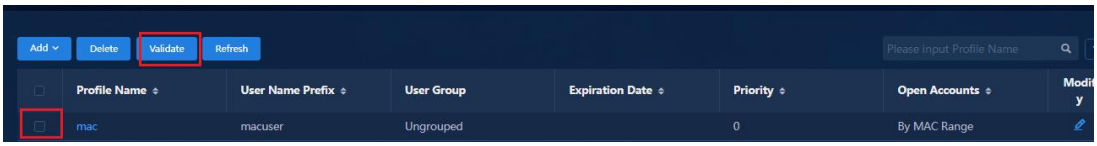


2. **Upload** をクリックしてファイルをインポートし、カラムの区切り文字を選択します。**Next** をクリックしてダム端末の MAC アドレス範囲を一括インポートし、**Confirm** をクリックして設定を完了します。

3. **Access Service** カラムでアクセスサービスを選択し、**Confirm** をクリックして設定を保存します。



4. 追加した MAC アドレス範囲をすぐに有効にするには、MAC アドレス範囲を選択して **Validate** をクリックする必要があります。**Validate** をクリックしない場合、MAC アドレス範囲はシステムのポーリング時間が終了するまで(10 分後)有効になりません。



MACアドレス範囲が正常に設定されると、エンドポイントデバイスからのトラフィックは認証をトリガーできます。システムはこれらを MAC アドレス範囲と照合し、自動的にユーザーカウントを作成し、認証されたユーザーを対応するセキュリティグループに追加して、IP アドレスを取得します。

重要:

手動の **Validate** 操作では、約 2000 の MAC アドレスが有効になる場合があります。MAC アドレスの数が多い場合は、MAC アドレス範囲を選択し、複数のバッチで検証するをクリックします。

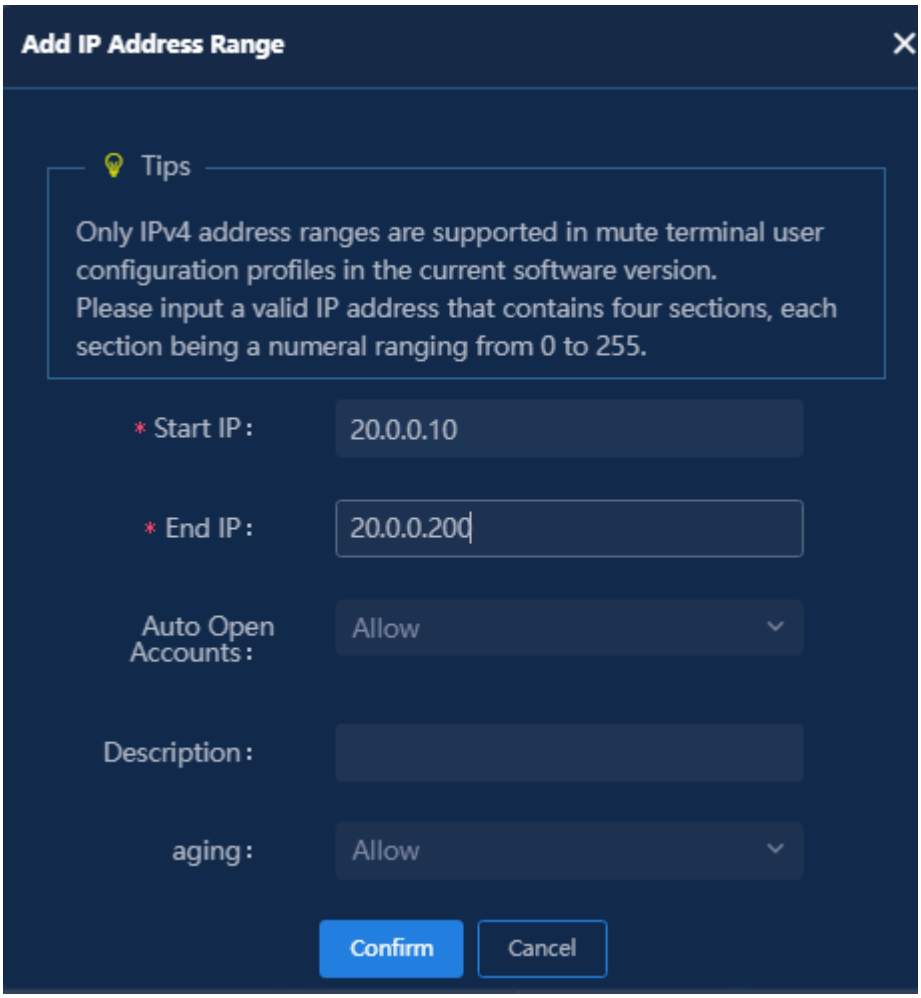
IPアドレス範囲に基づいた高速オンライン

Add をクリックし、ドロップダウンリストから **By IP Range** を選択します。プライオリティを 0～999 の範囲で設定します。デフォルト値は 0 です。値が小さいほど、プライオリティは高くなります。MAC アドレス範囲と IP アドレス範囲のプライオリティが比較されます。同じプライオリティに設定しないでください。

IP Address Range 領域では、MAC アドレス範囲を手動で追加したり、MAC アドレスをインポートしたりできます。

MAC アドレス範囲を手動で追加する

Add をクリックして、**Add IP Address Range** ページの **IP Address Range** 列を開きます。**Confirm** をクリックして設定を完了します。

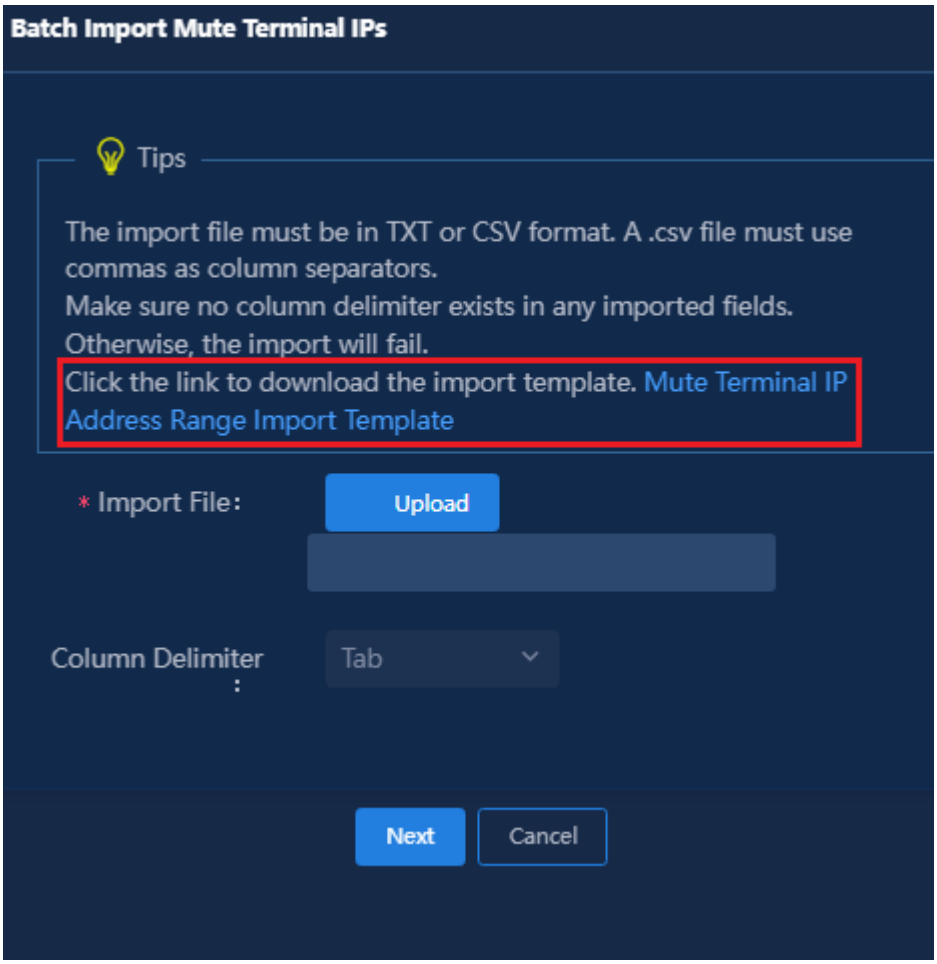


重要:

- 入力する IP アドレス範囲は、**Access Service** で設定されたセキュリティグループの **subnet** と同じである必要があります。セキュリティグループのサブネットネットワークセグメントを表示するには、SeerEngine キャンパスで **Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** に移動し、リスト内のサブネットリンクをクリックします。
- 複数の IP アドレス範囲を追加できます。各 IP アドレス範囲のパラメーターは、要件に応じて設定できます。

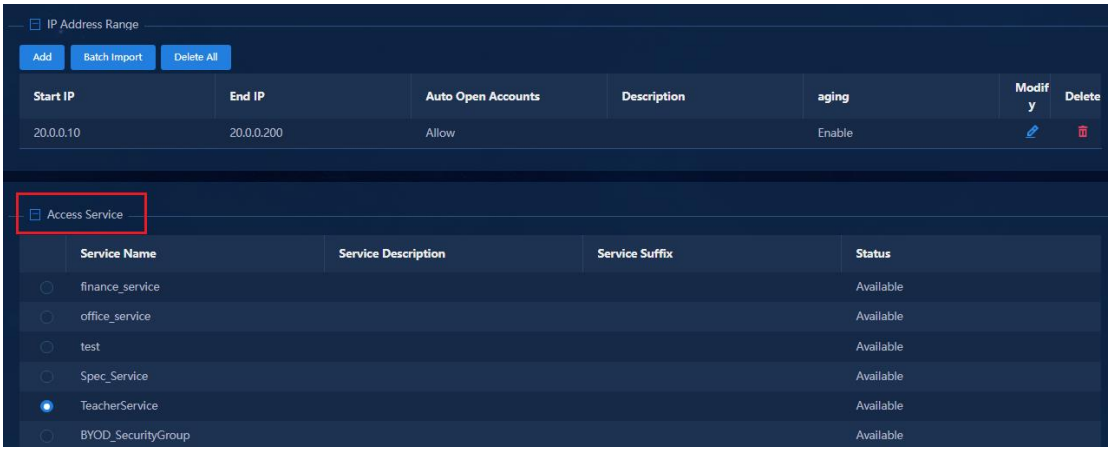
アクセスユーザーを一括インポートする

1. **Batch Import** をクリックします。テンプレートのダウンロードがサポートされています。**Mute Terminal IP Address Range Import Template** リンクをクリックして、テンプレートをダウンロードします。ダウンロードしたテンプレートに従ってインポートする IP アドレス範囲を入力します。

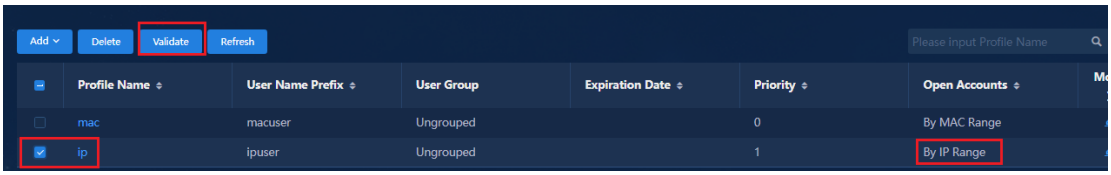


2. **Upload** をクリックしてファイルをインポートし、カラムの区切り文字を選択します。**Next** をクリックしてダム端末の MAC アドレス範囲を一括インポートし、**Confirm** をクリックして設定を完了します。

3. **Access Service** カラムでアクセスサービスを選択し、**Confirm** をクリックして設定を保存します。



4. 追加した IP アドレス範囲をすぐに有効にするには、IP アドレス範囲を選択して **Validate** をクリックする必要があります。**Validate** をクリックしない場合、MAC アドレス範囲はシステムのポーリング時間が終了するまで(10 分後)有効になりません。



IP アドレス範囲が正常に設定されると、エンドポイントデバイスからのトラフィックは認証をトリガーできます。システムはこれらを IP アドレス範囲と照合し、自動的にユーザーカウントを作成し、認証されたユーザーを対応するセキュリティグループに追加します。

5. **mac-authentication carry user-ip exclude-ip acl***コマンドを Leaf デバイスのダウンリンクインターフェイスに発行します。コマンドの発行後、クライアントはスタティック IP アドレスを設定します。クライアントが認証をトリガーすると、その IP アドレスが設定された IP アドレス範囲と一致する場合、システムはユーザーを認証するユーザーカウントを自動的に作成し、認証されたユーザーを設定されたアクセスグループに追加します。**mac-authentication carry user-ip exclude-ip acl***コマンドの説明は次のとおりです。

   - **mac-authentication carry user-ip**: エンドポイント装置のスタティック IP アドレスを取得し、EIA サーバーに送信して、クイックオンライン認証をトリガーします。
   - **exclude-ipacl**: ACL の指定されたネットワークセグメントからのユーザーパケットは、MAC 認証をトリガーしません。

   次のコマンドが Leaf デバイスに対して発行されます。

```
# fe80 のアドレスに一致する acl を作成します。
acl ipv6 basic 2000
rule deny source fe80:0::0:0 16
#
# リーフダウンリンクインターフェイスで mac-authentication carry user-ip コマンドを実行します。
interface gigabitethernet 1/0/1
mac-authentication carry user-ip exclude-ip acl 2000
#
```

重要:

- 現在の AD-Campus ソリューションでは、fe80 で始まる IPv6 リンクローカルアドレスをフィルタリングするには、**mac-authentication carry user-ip exclude-ip acl***コマンドが必要です。
- エンドポイントユーザーがスタティック IP アドレスを使用してにアクセスする場合、ユーザーパケットで伝送される IP アドレスは、ユーザーの実際の IP アドレスではない可能性があります。たとえば、IPv4 スタティックアドレスネットワーキングでは、ユーザーパケットで伝送される IP アドレスは、fe80 で始まる IPv6 リンクローカルアドレスです。**mac-authentication carry user-ip** コマンドが設定された後、デバイスは、ユーザーの実際の IP アドレスではない IP アドレスを使用して、サーバーへの MAC アドレス認証要求を開始します。これにより、サーバーがユーザーに対して誤った IP アドレスをバインドしたり、IP アドレスと MAC アドレスの照合に失敗したりします。これらの問題を回避するには、exclude-ip acl パラメーターを指定して、ACL で指定されたネットワー

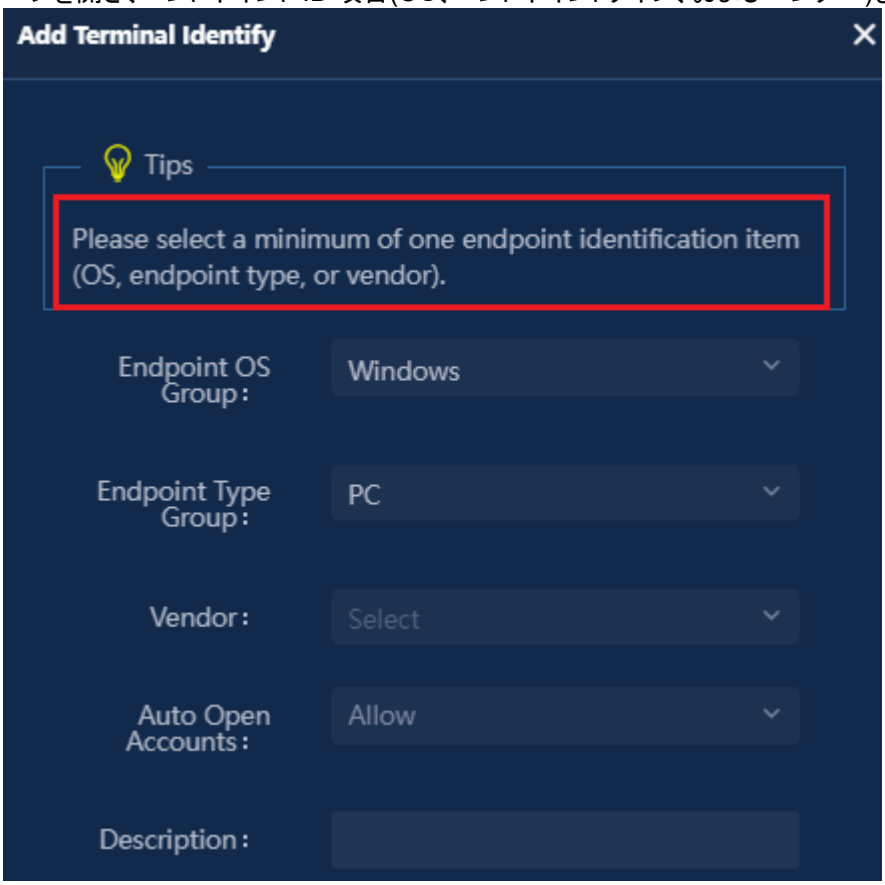
クセグメント内のユーザーの MAC アドレス認証を禁止します。

エンドポイントの識別に基づく高速オンライン

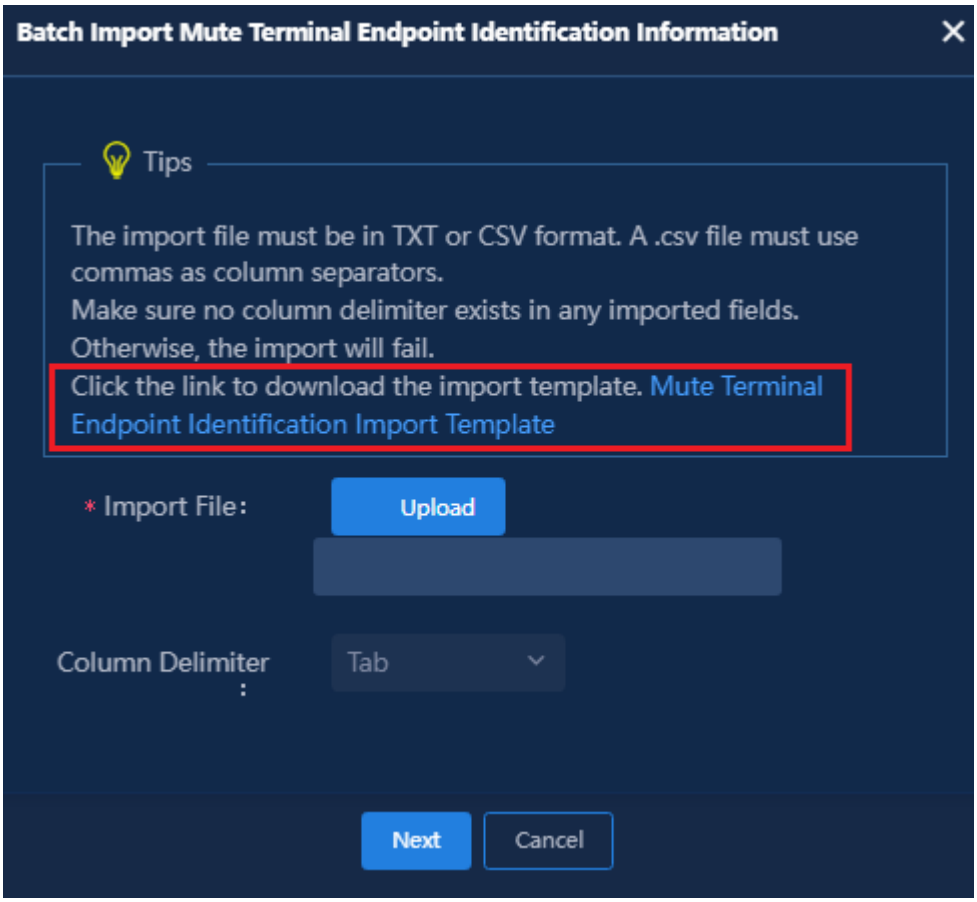
Add をクリックし、ドロップダウンリストで **By Endpoint Identification** を選択します。

0 エンドポイント ID エントリーは、手動で追加またはインポートできます。ここでは、特に注意が必要な内容についてのみ説明します。その他の設定については、「Fast online based on MAC address ranges」を参照してください。

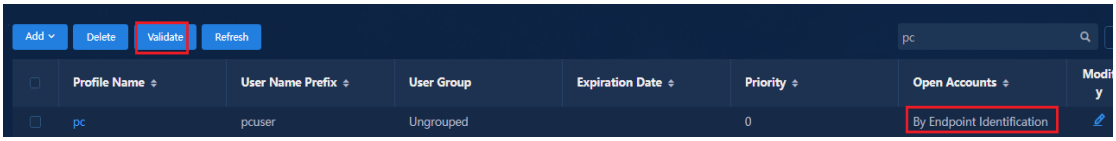
- エンドポイント ID エントリーを手動で追加するには、**Add** をクリックして **Add Terminal Identity** ページを開き、エンドポイント ID 項目(OS、エンドポイントタイプ、およびベンダー)を設定します。



- 識別品目をバッチでインポートするには、リンクのインポートテンプレートを使用できます。



- 設定が完了したら、追加した項目を選択し、**Validate** をクリックする必要があります。**Validate** をクリックしない場合、MAC アドレス範囲は、システムのポーリング時間が終了するまで(10 分後)有効になりません。



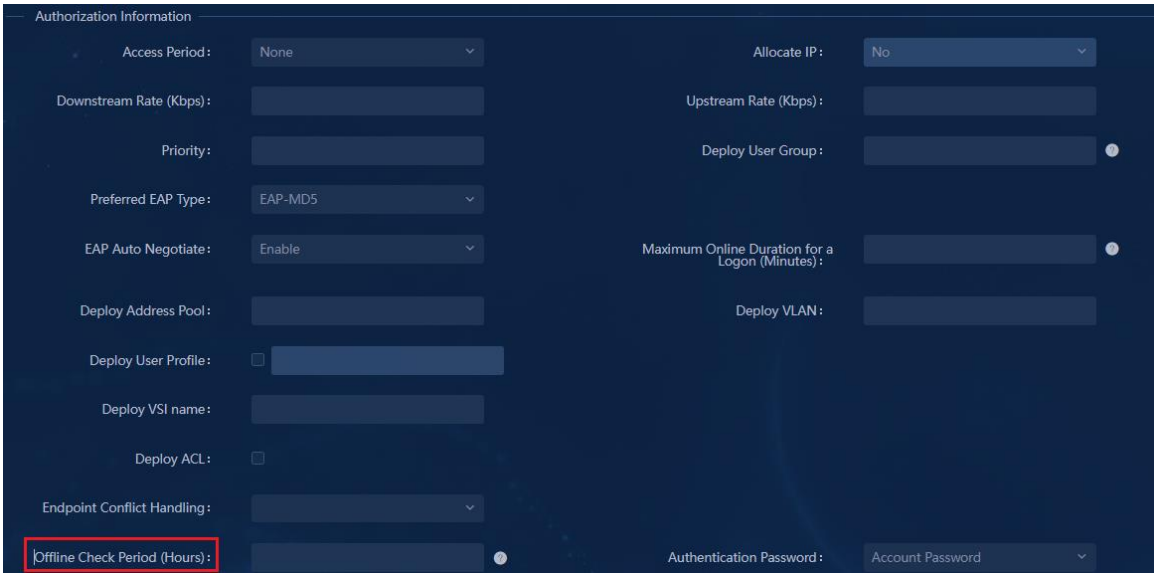
エンドポイントデバイスからのトラフィックによって認証がトリガーされます。システムは、エンドポイントのフィンガープリントをエンドポイント ID エントリーと照合します。一致するものが見つかった場合、システムは自動的にユーザーカウントを作成し、認証されたユーザーを対応するセキュリティグループに追加します。

ブロードバンドIoTエンドポイントを長期間オンラインに保つ

IoT エンドポイントを長期間オンラインに保つには、オフラインチェック期間(時間)を ARP/ND スヌーピングに関連付けます。ARP/ND エントリーが期限切れになる 30 秒前にキープアライブをトリガーして、ブロードバンド IoT エンドポイントをオンラインに保ちます。ブロードバンド IoT エンドポイントを 1～2 回のオフライ

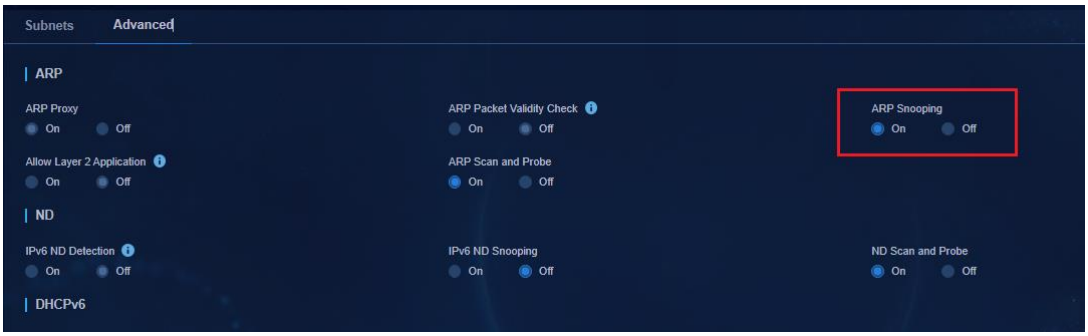
ンチェック期間オンラインに保つには、EIA のアクセスポリシーで **Offline Check Period** を次のように設定するだけです。

Automation > **User** > **Access Service** ページに移動し、**Access Policy Management** リンクをクリックして **Access Policy** ページを開きます。リストのアクセスポリシー名の **Edit** カラムをクリックします。**Authorization Information** カラムでアクセスポリシーの **Offline Check Period(Hours)**を変更します。推奨値は 24 時間です。



次の 2 つの方法は、ブロードバンド IoT エンドポイントを常にオンラインに保つことができる。

- 方法 1:オフラインチェック期間を 0 時間に設定します。オフラインチェックを無効にして、エンドポイントが長時間トラフィックなしでエージングせず、常にオンライン状態を維持するようにします。
- 方法 2:オフラインチェック期間の設定に基づいて、SeerEngine キャンパスで ARP スヌーピングを設定し、ARP スヌーピングと連携するようにデバイスでオフラインチェック期間を設定する必要があります。この方法は通常、特定のブロードバンド IoT エンドポイントを常にオンラインに保つために適用されます。
  a. **Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** に移動し、対応するカラムをクリックして **Edit Layer 2 Network Domain** ページを開きます。
  b. **Edit Layer 2 Network Domain** ページの **Advanced** タブで、**ARP Snooping** を **On** に設定し、**OK** をクリックします。



ARP スヌーピングイネーブル化コマンドをリーフデバイスに展開します。

```
#
vsi vsi4
 description SDN_VSI_4
 gateway vsi-interface 4
 statistics enable
 arp Snooping enable  //コントローラーによって展開されるコマンド.
 flooding disable all all-direction
 vxlan 4
 evpn encapsulation vxlan
  mac-advertising disable
  arp mac-learning disable
  nd mac-learning disable
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
 dhcp snooping binding record
#
```

オフラインチェック期間と ARP スヌーピング設定に加えて、**mac-authentication offline-detect mac-address xxxx-xxxx-xxxx timer xxxx check-arp-or-nd-snooping** コマンドを手動で設定して、オフラインチェック期間と ARP/ND スヌーピング間の連携をイネーブルにし、ARP/ND エントリーのエージングより 30 秒早くキープアライブをトリガーする必要があります。

コマンド設定は次のとおりです。

タイマーはオフラインチェック期間を参照します。この期間は、ARP エージングタイムよりも長くする必要があります(例:3600 秒)。

```
#
mac-authentication offline-detect mac-address 0001-0002-0003 timer 3600 check-arp-or-nd-snooping
#
```

重要:

mac-authentication offline-detect mac-address xxxx-xxxx-xxxx timer xxxx check-arp-or-nd-snooping コマンドは、各認証エンドポイントで設定する必要があります。mac-address キーワードは、エンドポイント

の MAC アドレスを指定します。このコマンドを設定せずに、オフラインチェック期間だけを設定した場合、ARP スヌーピングとオフラインチェック期間のコラボレーションは実現できません。オフラインチェック期間が終了すると、トラフィックが存在しない場合、エンドポイントはオフラインになります。

役割ベースの権限制御

はじめに

キャンパスコントローラは、ロールベースの権限制御をサポートしています。コントローラは、ログインオペレーターのロールに従って権限を割り当てます。このセクションでは、主に分離ドメインとファブリックに関連する権限設定について説明します。

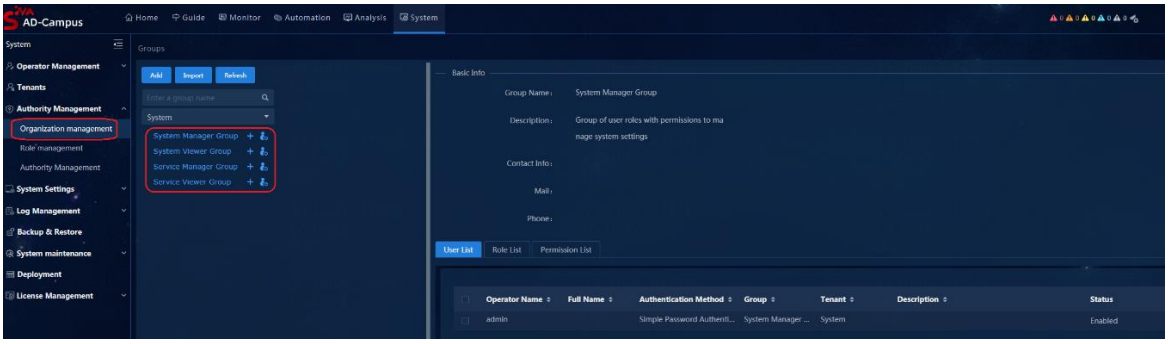
基本概念

グループ

システムでは、階層管理のために様々なグループにオペレーターが割り当てられます。グループのロールを構成して、グループ内のオペレーターの権限を制御できます。4 つのデフォルトグループが事前に定義されています。必要に応じてグループを作成することもできます。

- **System Manager Group**: システム設定を管理する権限を持つオペレーターのグループ。
- **System Viewer Group**: システム設定を表示する権限を持つオペレーターのグループ。
- **Service Manager Group**: ネットワークデバイスとアラームを管理する権限を持つオペレーターのグループ。
- **Service Viewer Group**: ネットワークデバイスとアラームを表示する権限を持つオペレーターのグループ。

System > **Authority management** > **Groups** ページに移動します。



重要:

- オペレーターによって使用されているグループは削除できません。
- グループの名前は変更できません。
- 既に存在するグループは追加できません。
- 最大 10 レベルのサブグループを作成できます。

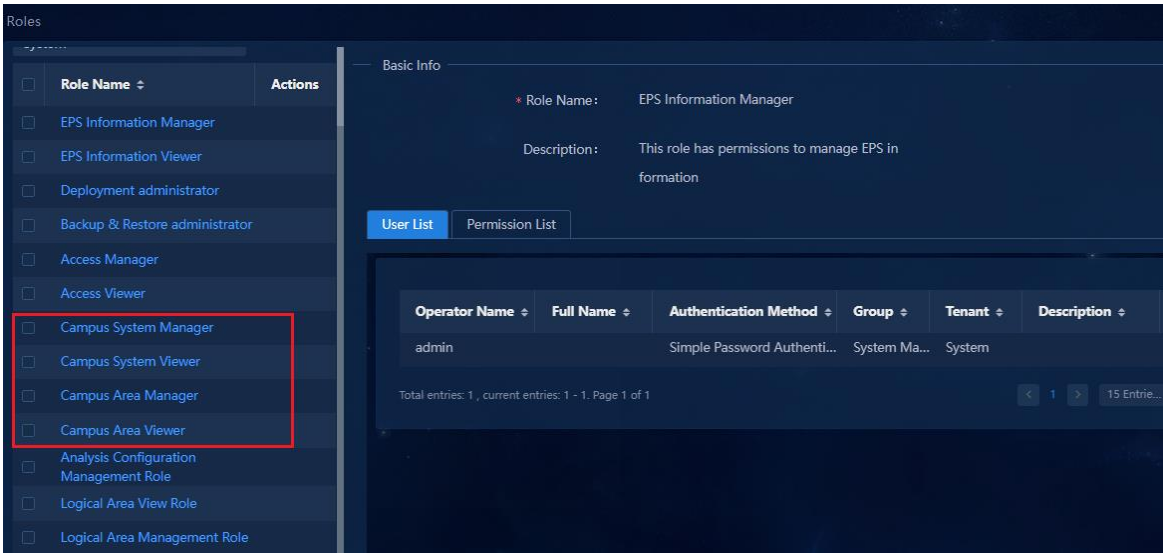
- パフォーマンスの制限により、最大 7 レベルのグループをインポートできます。

ロール

ロールは、ユーザーのタイプに対する一連の権限を定義します。システムでは、ロールベースの権限制御が採用されています。これにより、ユーザー権限のグループ化が改善され、ユーザー権限の管理が容易になります。システムにはデフォルトで一連のロールが用意されており、必要に応じてロールを定義することもできます。キャンパスネットワークには、主に次のデフォルトロールが含まれます。

- **Campus System Manager**: キャンパスネットワーク情報を管理する権限を持つロール。
- **Campus System Viewer**: キャンパスネットワーク情報を表示する権限を持つロール。
- **Campus Area Manager**: 特定のキャンパスネットワーク情報を管理する権限を持つロール。
- **Campus Area Viewer**: 特定のキャンパスネットワーク情報を表示する権限を持つロール。

System > **Authority management** > **Roles** ページに移動します



重要:

- キャンパスエリアロールには、デフォルトでは分離ドメインまたはファブリックの権限が含まれていないため、必要に応じてエリア権限を手動で追加する必要があります。
- 既に存在するロールは追加できません。
- ロールを削除した後、削除したロールと同じ名前で別のロールを追加できます。
- ロールの削除には注意が必要です。ロールを削除すると、そのロールを持つユーザーから権限が削除されます。

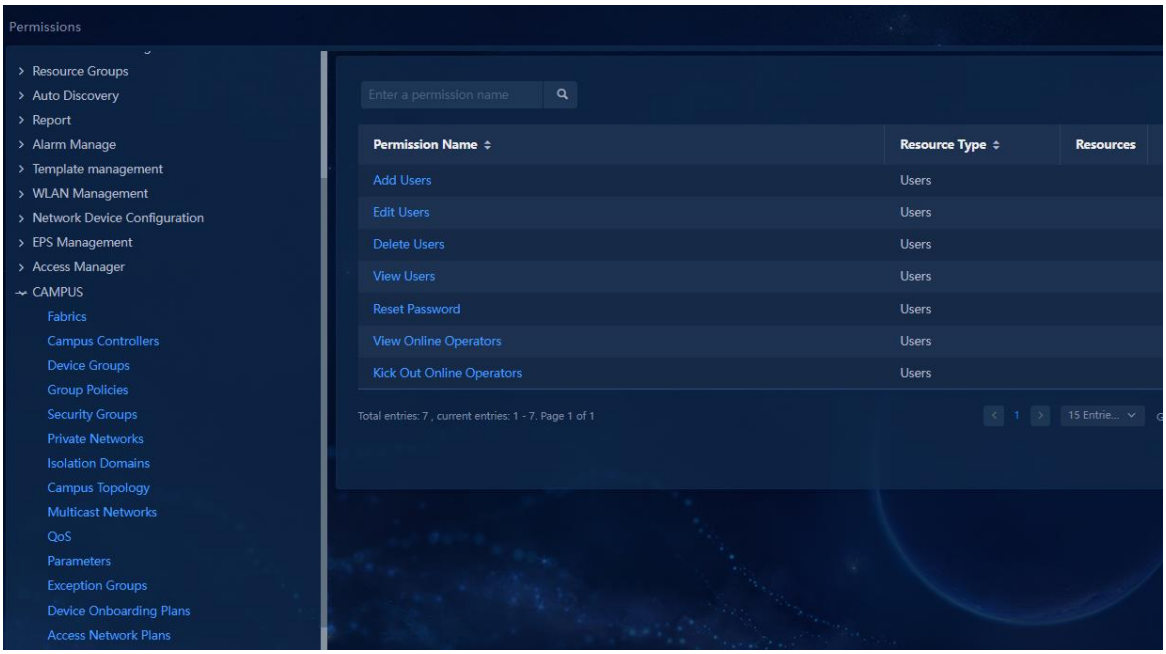
アクセス権

権限は、リソースタイプの操作およびデータリソースを定義します。権限を追加、変更、削除および表示で

きます。システムには、デフォルトで一連の権限が用意されています。必要に応じて権限を定義することもできます。デフォルトでは、新しいユーザー、グループまたは役割には、デフォルトでその権限の下にあるすべてのデータリソースがあります。

システムは、権限のデータリソースの構成もサポートします。たとえば、エリアマネージャは、対応する分離ドメインおよびファブリックを権限のリソースとして選択できます。この権限によって制御される操作は、権限で指定されたリソースのみを処理できます。

System > **Authority Management** > **Permissions** ページに移動します。



重要:

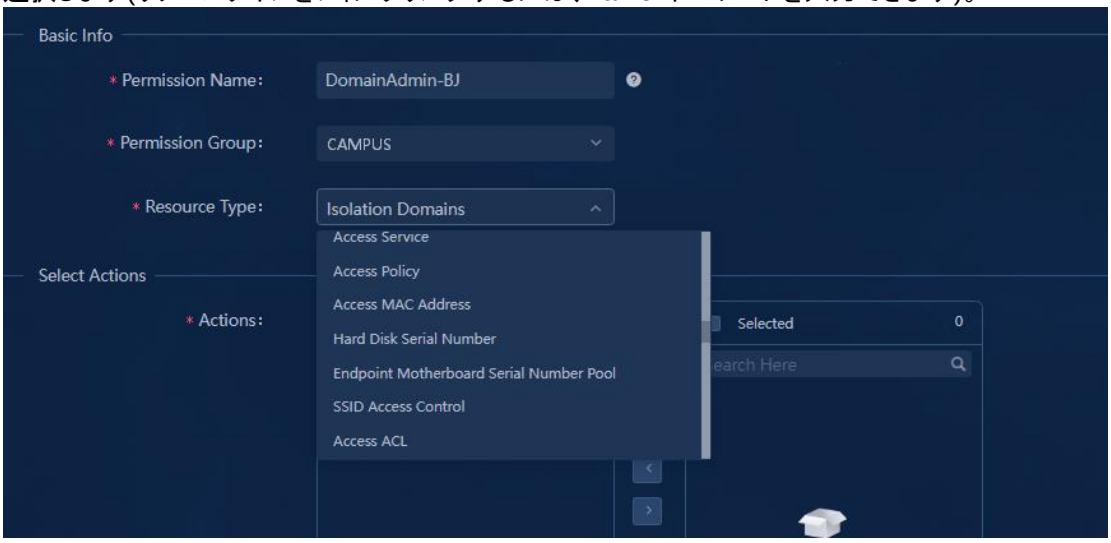
- admin オペレーターはスーパー管理者であり、デフォルトですべての権限を持っています。
- 権限の変更時に名前を変更することはできません。
- 既に存在するアクセス許可は追加できません。
- データを変更または削除する権限があり、データを表示する権限がない場合、関連付けられたデータはページに表示されません。
- リソースデータの一部のみがアクセス許可に指定されている場合、そのアクセス許可では、ユーザーが他のデータを表示、変更、または削除することはできません。
- 権限の削除には注意が必要です。権限を削除すると、対応する操作権限またはデータ権限がユーザーから削除されます。

役割ベースのアクセスコントロールの構成

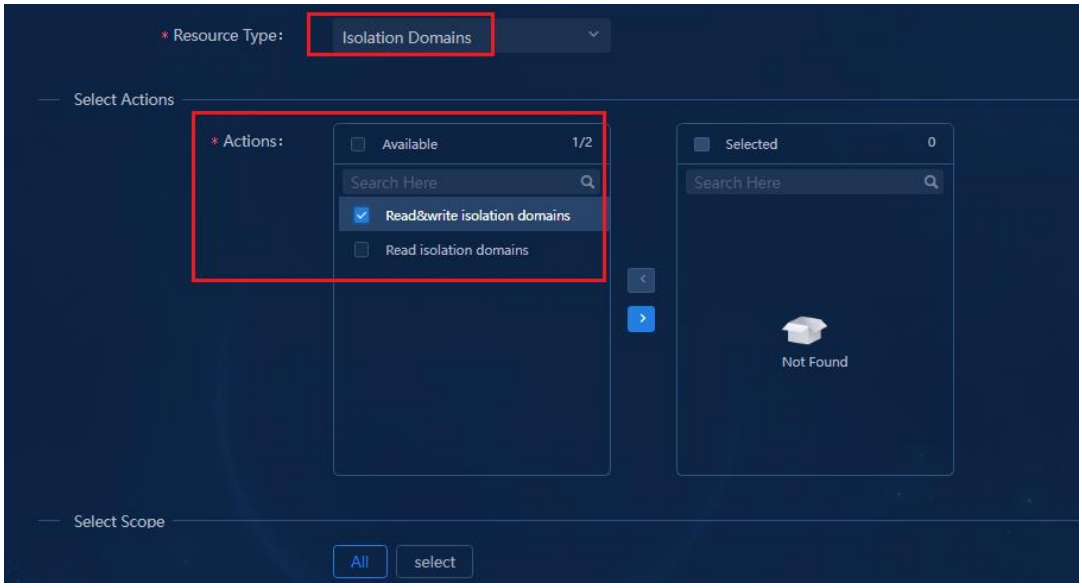
アクセス許可を追加する

エリアマネージャに分離ドメインのサブ権限を追加する

1. **System** > **Authority Management** > **Permissions** ページに移動し、**Add** をクリックします。権限名を入力し、権限グループとして **CAMPUS** を選択し、リソースタイプとして **Isolated Domains** を選択します(リソースタイプをフィルタリングするには、name キーワードを入力できます)。

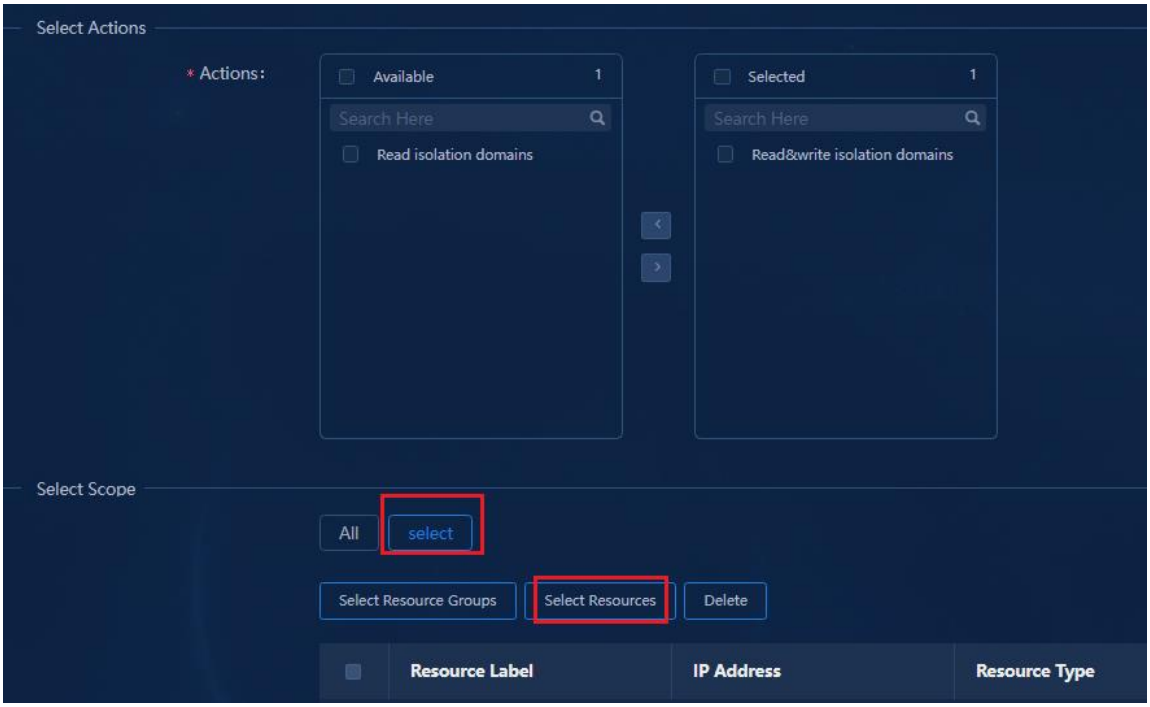


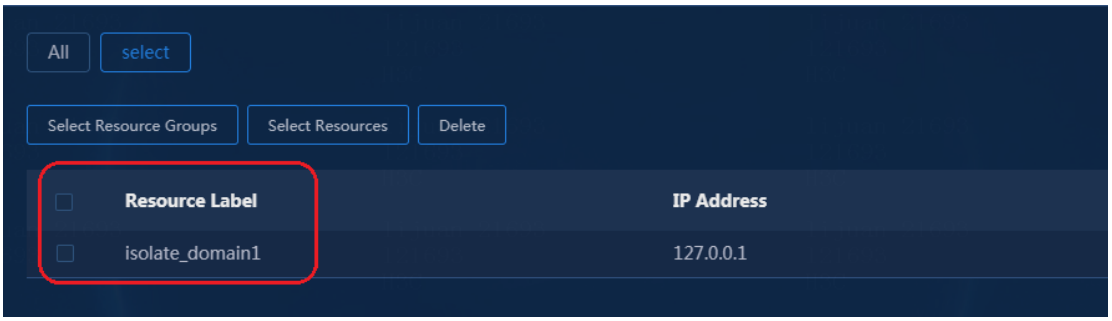
2. **Select Actions** 列で、**Read&write isolation domains**(エリアマネージャの場合)または **Read isolation domains**(エリアビューアの場合)を選択できます。次に、›クリックして選択内容を **Selected** リストに追加します。



3. **Select Scope** 列で、**All** または **Select** を選択します。このドキュメントでは、例として **Select** を使

用します。Select Resources をクリックして対応する分離ドメインを指定し、Select をクリックして選択を完了します。

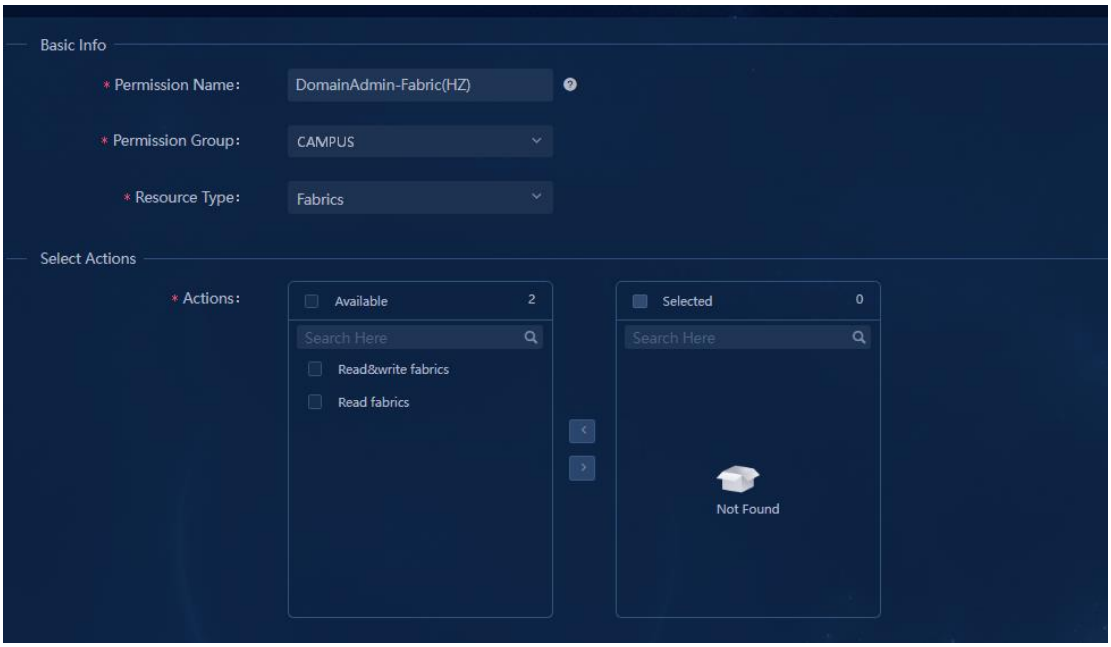




4. **OK** をクリックします。エリアマネージャのサブ権限が、**System** > **Permissions** > **Campus** > **Isolation Domains** に追加されます。

エリアマネージャのファブリックサブ権限の追加

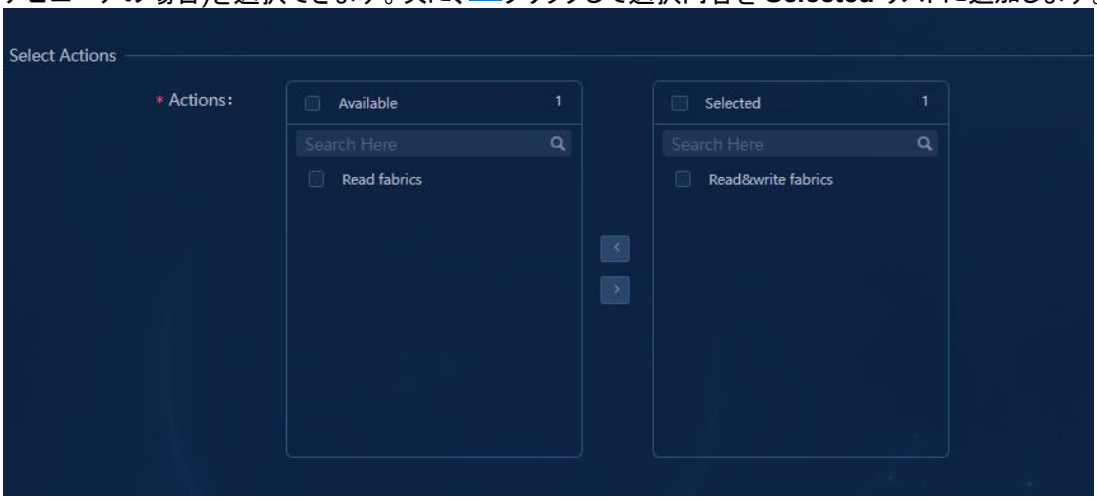
1. **System** > **Authority Management** > **Permissions** ページに移動し、**Add** をクリックします。権限名を入力し、権限グループとして **CAMPUS** を選択し、リソースタイプとして **Fabrics** を選択します。



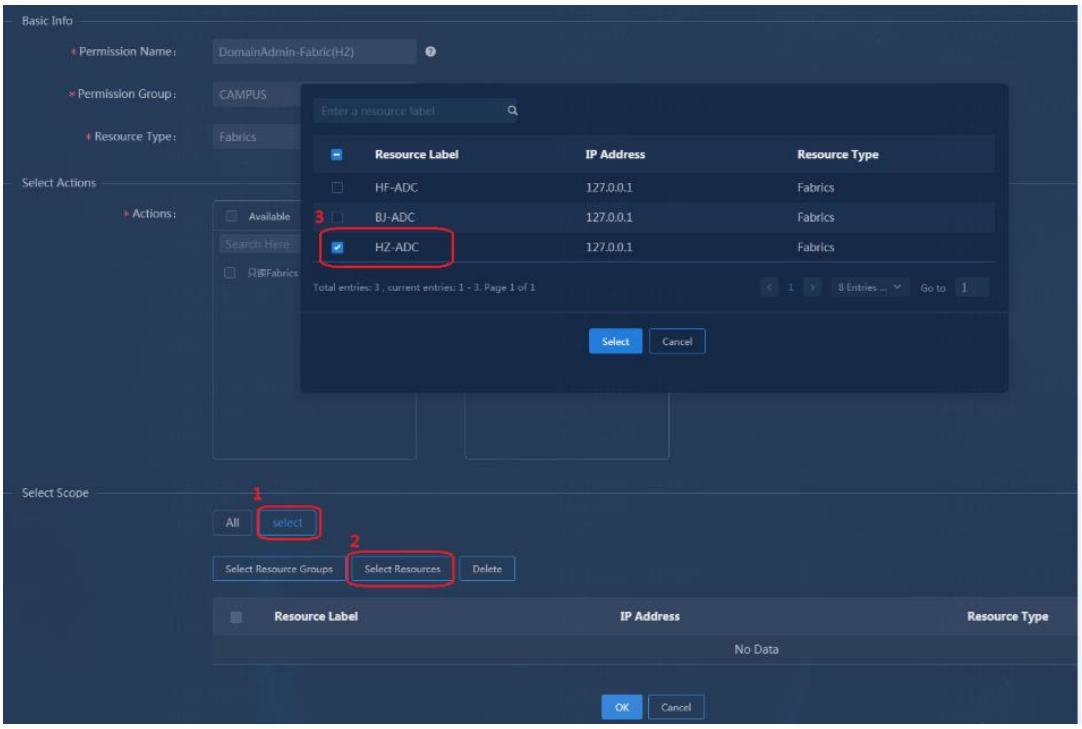
重要:

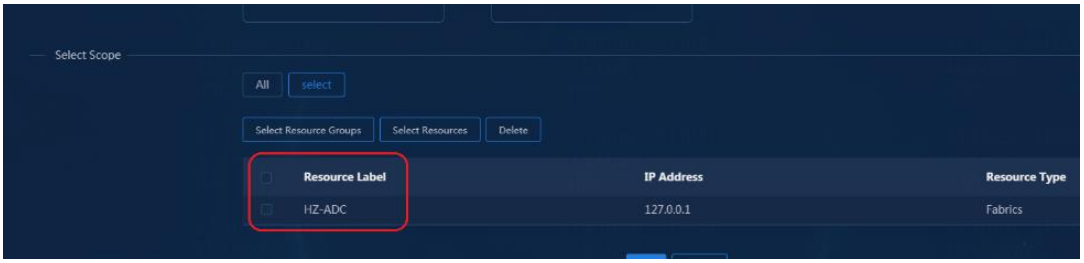
Campus と DC コントローラの両方が導入されている場合、2 つのファブリック権限を使用できます。スコープ構成の 1 つは、Campus のファブリック権限です。

2. **Select Actions** 列で、**Read&Write Fabrics**(エリアマネージャの場合)または **Read fabrics**(エリアビューアの場合)を選択できます。次に、 クリックして選択内容を **Selected** リストに追加します。



3. **Select Scope** カラムで、**All** または **Select** を選択します。このドキュメントでは、例として Select を使用しています。**Select Resources** をクリックして対応するファブリックを指定し、**Select** をクリックして選択を完了します。

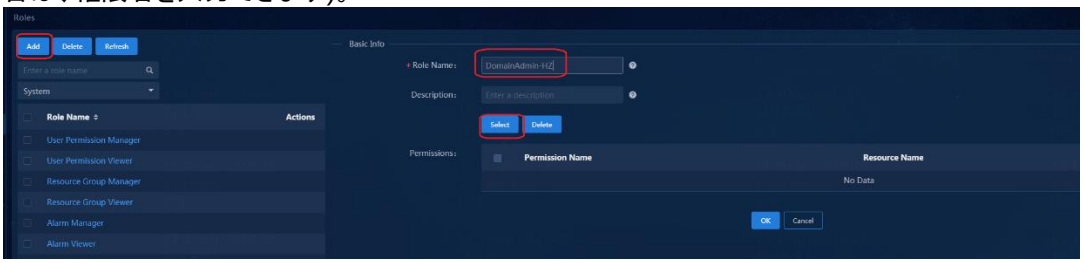




4. **OK** をクリックします。エリアマネージャのサブ権限が、**System** > **Permissions** > **Campus** > **Fabrics** に追加されます。

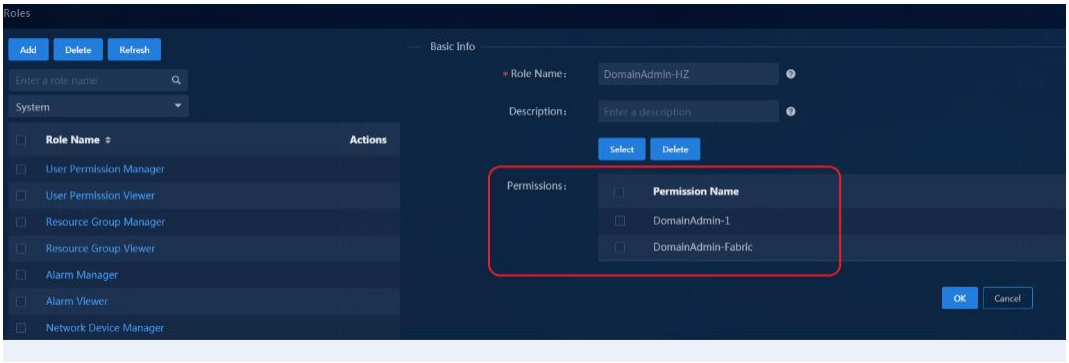
カスタマイズされた役割の追加

1. **System** > **Authority Management** > **Role** ページにナビゲートします。**Add** をクリックし、ロール名を入力します。**Select** をクリックして、権限の選択ページを開きます(複数の権限タイプがある場合は、権限名を入力できます)。

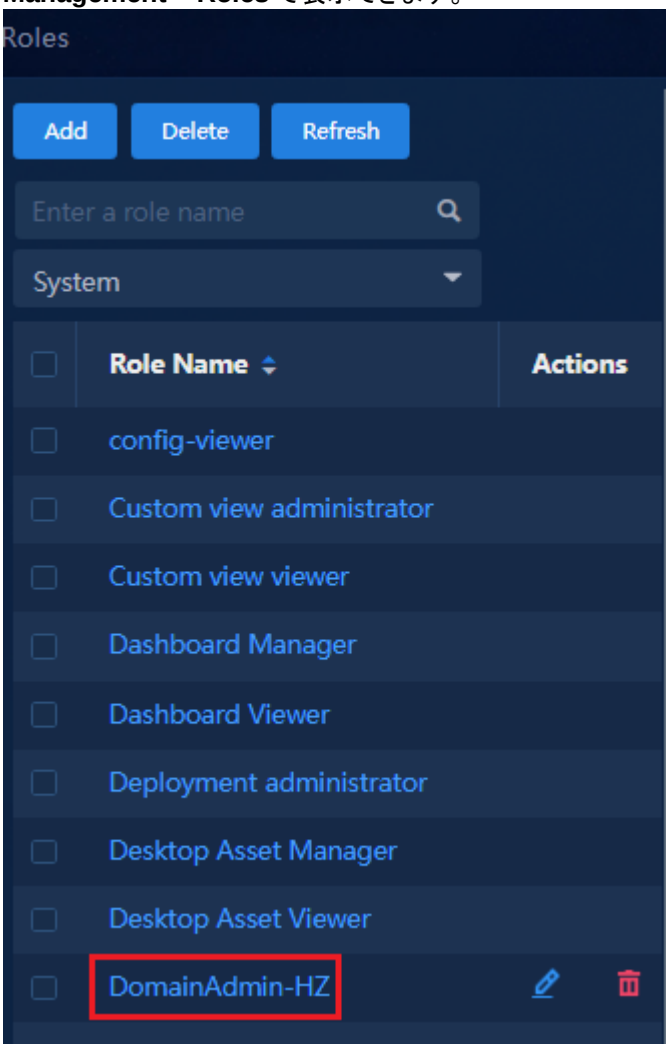


『Add a permission』に追加したアクセス許可の名前を入力し、**Search** をクリックします。アクセス許

可名を選択し、**OK** をクリックして **Select** ページに戻ります。



2. **OK** をクリックして、エリアロールの追加を完了します。追加されたロールは、**System** > **Authority Management** > **Roles** で表示できます。



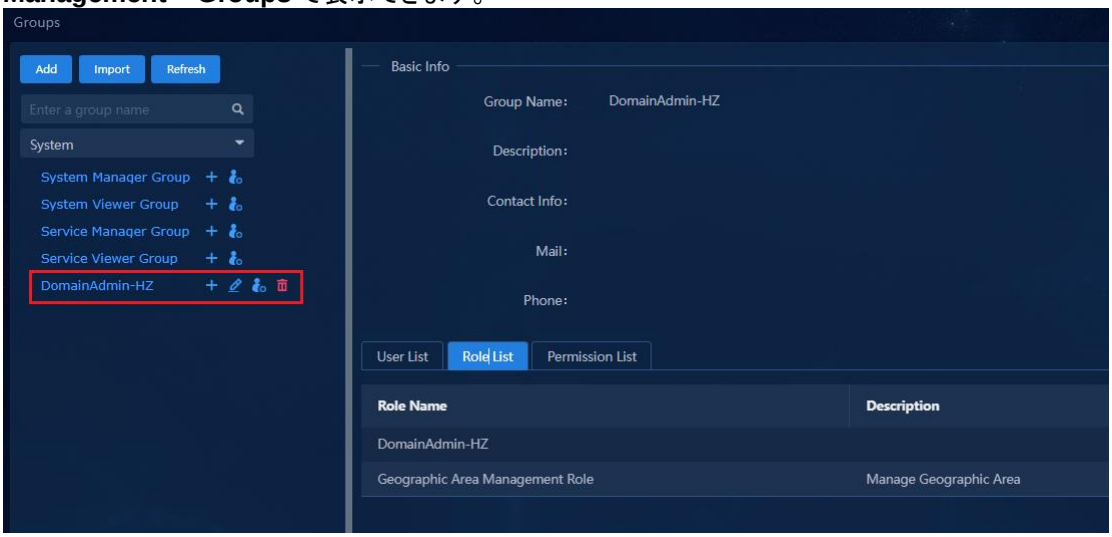
カスタマイズしたグループを追加する

1. **System** > **Authority Management** > **Groups** ページにナビゲートします。**Add** をクリックして、グ

ループ名、電子メール、および連絡先情報を入力します。

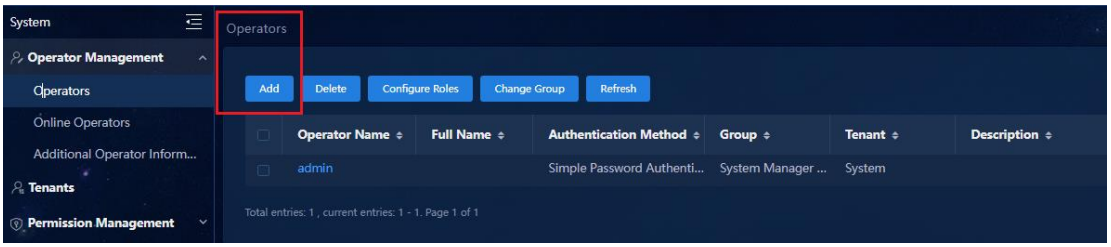
2. 『Add a customized role』で追加したロールとデフォルトの **Campus Area Manager** ロールを選択します(管理者がキャンパスネットワークの他の基本モジュールに必要な権限を持っていることを確認するため)。

3. **OK** をクリックして、グループの追加を完了します。追加されたグループは、**System** > **Authority Management** > **Groups** で表示できます。

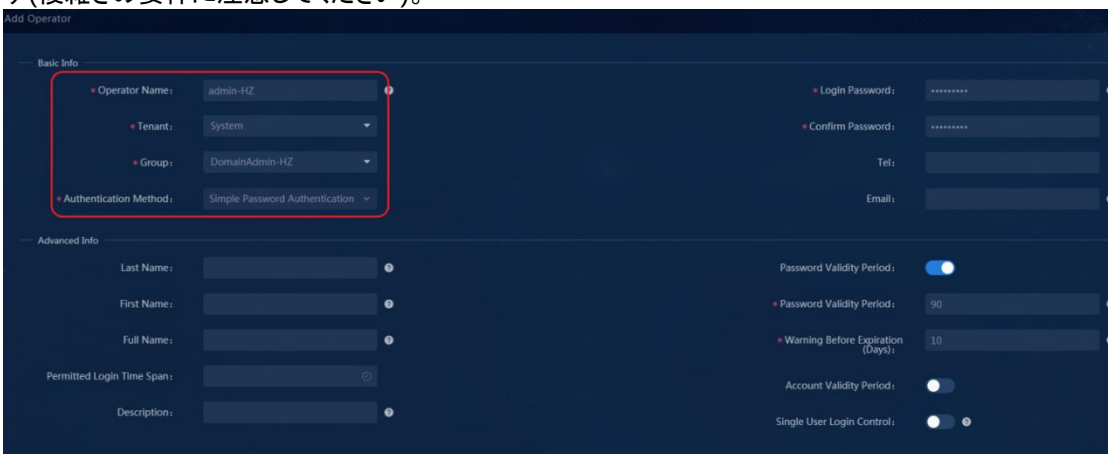


演算子を追加する

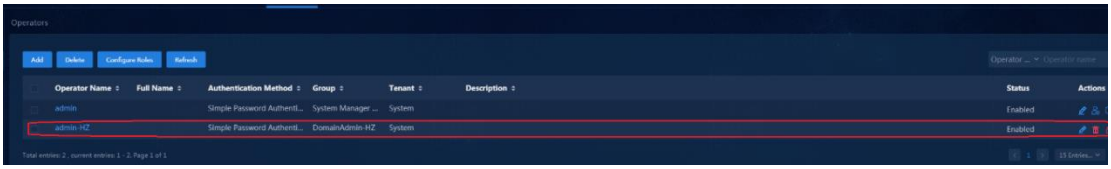
1. **System** > **Operator Management** > **Operators** ページに移動し、**Add** をクリックします。



2. カスタマイズしたグループを追加するオペレーター名を入力し、**Tenant** リストから **System** を選択し、**Group** リストから『Add a customized group』で追加されたカスタマイズされたグループを選択します。認証方式として **imple Password Authentication** を選択し、ログインパスワードを入力します(複雑さの要件に注意してください)。



3. **OK** をクリックして、オペレーターの追加を完了します。



権限とドメイン管理の確認

『Add an operator』で追加されたオペレーターを使用してコントローラ管理ページにログインし、オペレーターに設定された権限があるかどうかを確認します。

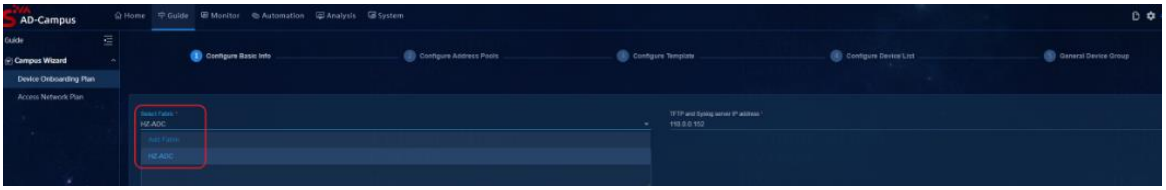
重要:

ファブリックを分離ドメインにバインドした後、ファブリックと対応する分離ドメインの両方に権限を追加する必要があります。それ以外の場合、関連するページは表示されません。

デバイスオンボーディングプラン

Guide > **Campus Wizard** > **Device Onboarding Plan** ページに移動します。

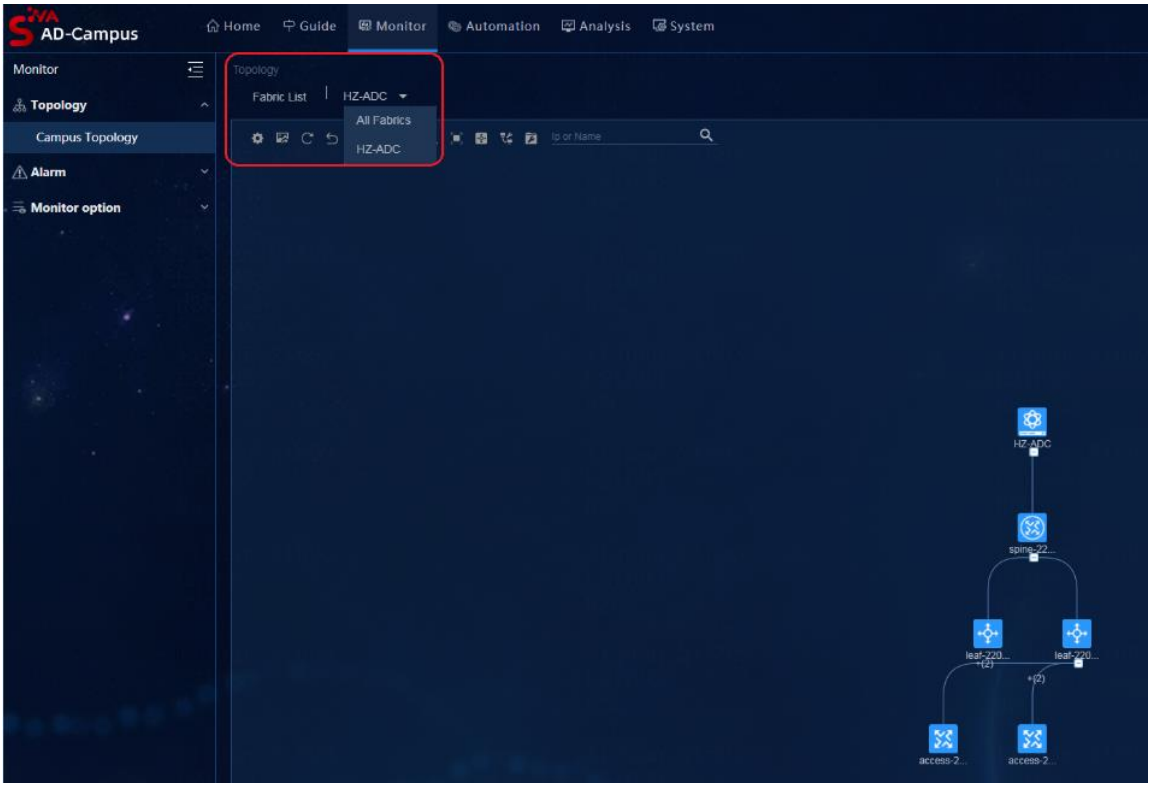
デバイスオンボーディングプラン設定に使用できるファブリックは、許可されたファブリックだけです。対応するアドレスプール設定、ロールテンプレートなどを表示できます。他のファブリックに関する情報を選択して表示することはできません。



キャンパストポロジ

Monitor > **Topology** > **Campus Topology** ページに移動します。

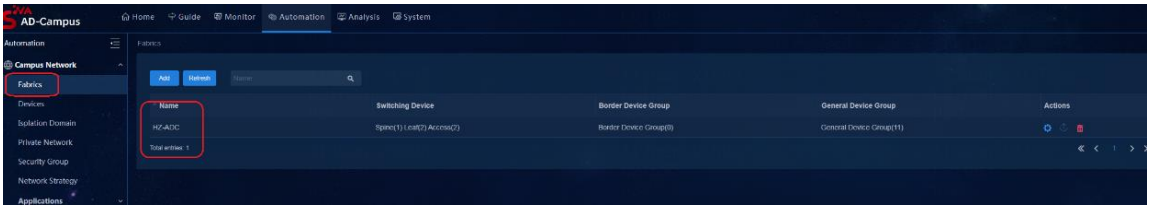
許可されたファブリックのトポロジおよびデバイス情報だけを表示できます。他のファブリックのトポロジ情報は表示できません。



ファブリック

Automation > **Campus Network** > **Fabrics** ページに移動します。

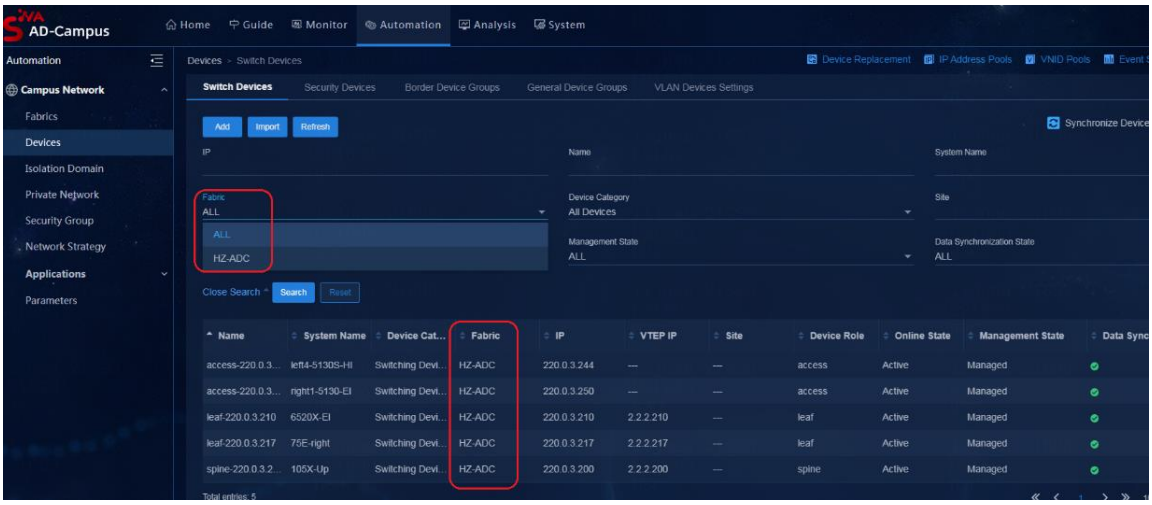
許可されたファブリックの情報だけを表示および変更できます。他のファブリックの情報は表示できません。



物理デバイス

Automation > **Campus Network** > **Devices** > **Physical Devices** ページに移動します。

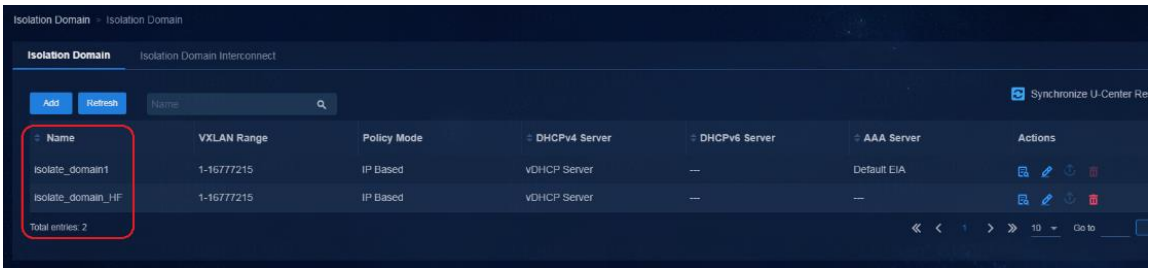
デバイスを表示および変更できるのは、許可されたファブリック内だけです。他のファブリックのデバイス情報は表示できません。



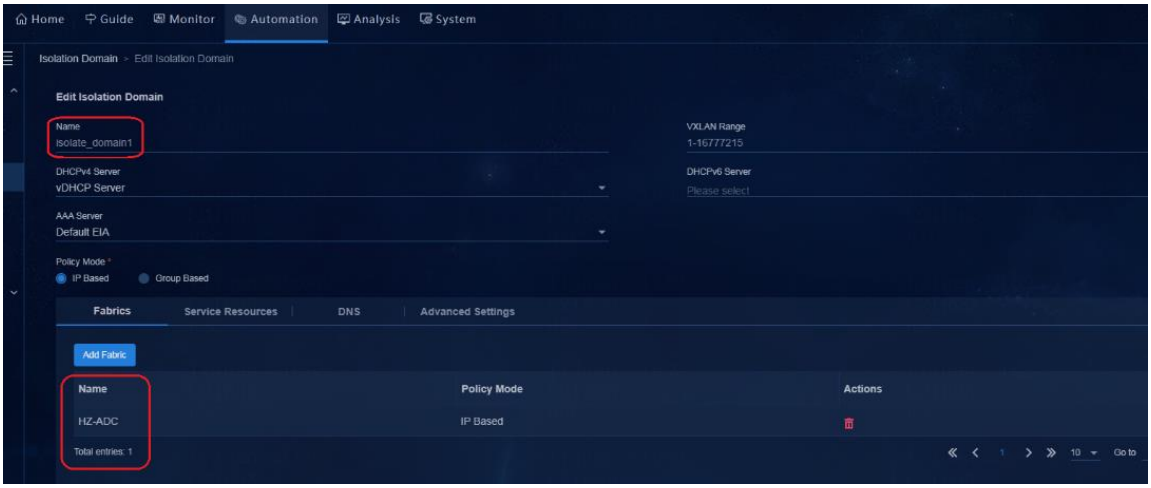
分離ドメイン

Automation > **Campus Network** > **Isolation Domain** > **Isolation Domain** ページに移動します。

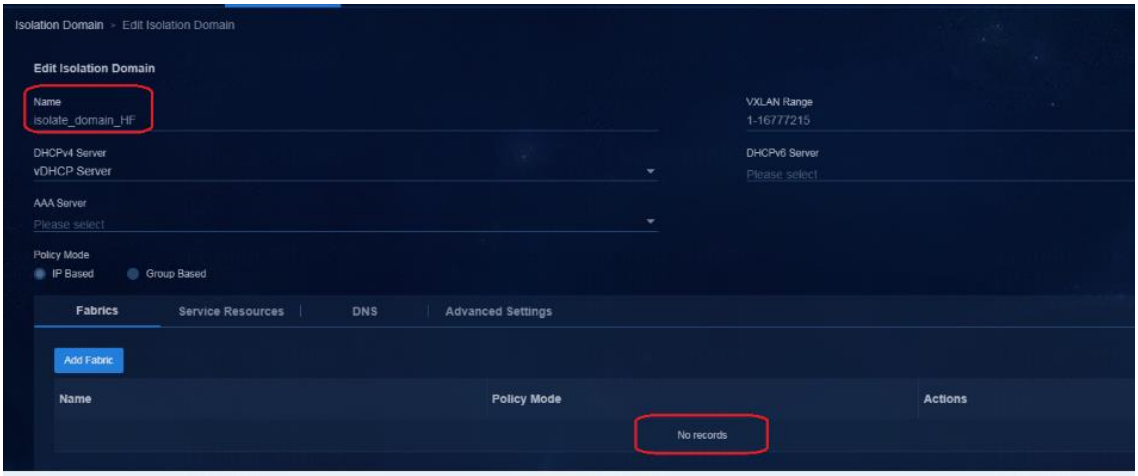
すべての分離ドメインを表示できます。



ただし、表示できるのは、オペレーターが権限を持つ分離ドメインにバインドされているファブリックだけです。



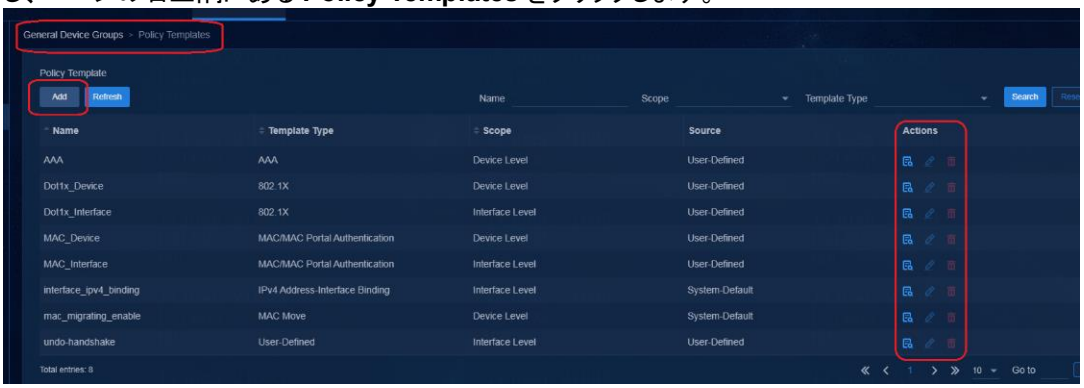
他の分離ドメインにバインドされているファブリックは表示できません。



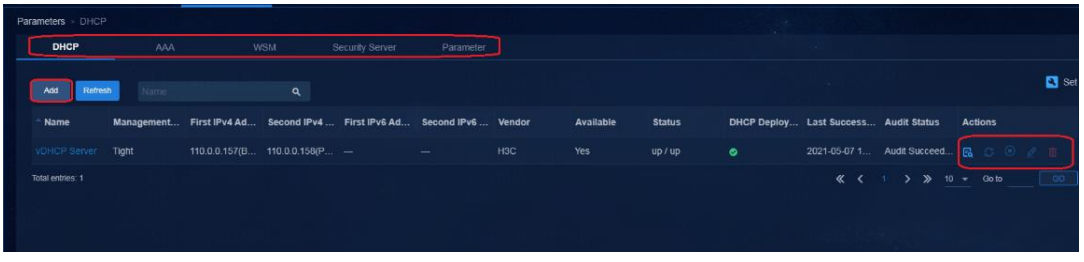
公的資源

一部のパブリックリソースは、オペレーターのエリア権限構成をサポートしていません。すべてのエリアマネージャには、リソースを表示する権限のみがあり、リソースを編集する権限はありません。すべての編集操作は、システム管理者が行う必要があります。主に次のページが関係します。

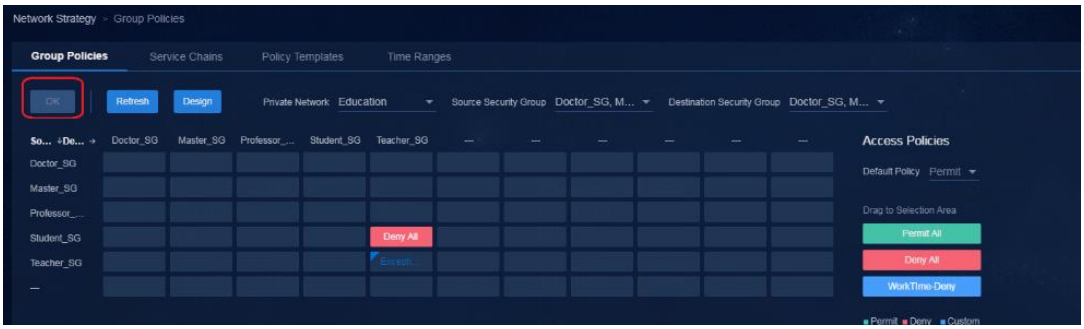
- **Automation** > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動し、ページの右上隅にある **Policy Templates** をクリックします。



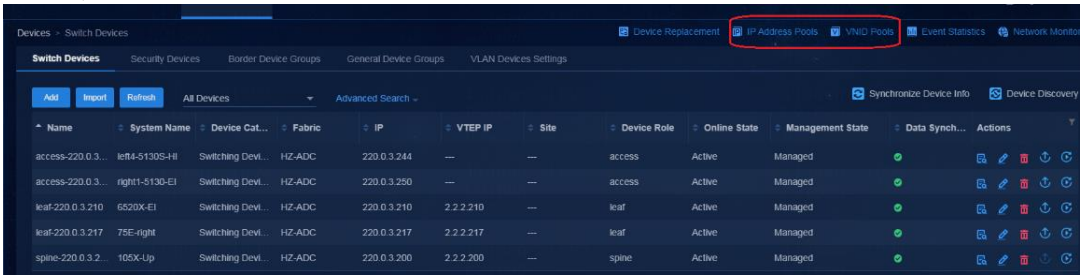
- **Automation** > **Campus Network** > **Parameters** で、**DHCP**、**AAA**、**Parameter**、およびその他のタブにアクセスします。



- **Automation** > **Campus Network** > **Network Strategy** で、**Group Policies**、**Service Chains**、**Policy Template**、および **Time Ranges** にアクセスします。



- **Automation** > **Campus Network** > **Device Groups** で、**Device Replacement**、**IP Address Pools**、**VNID Pools**、およびその他のパラメーターにアクセスします。

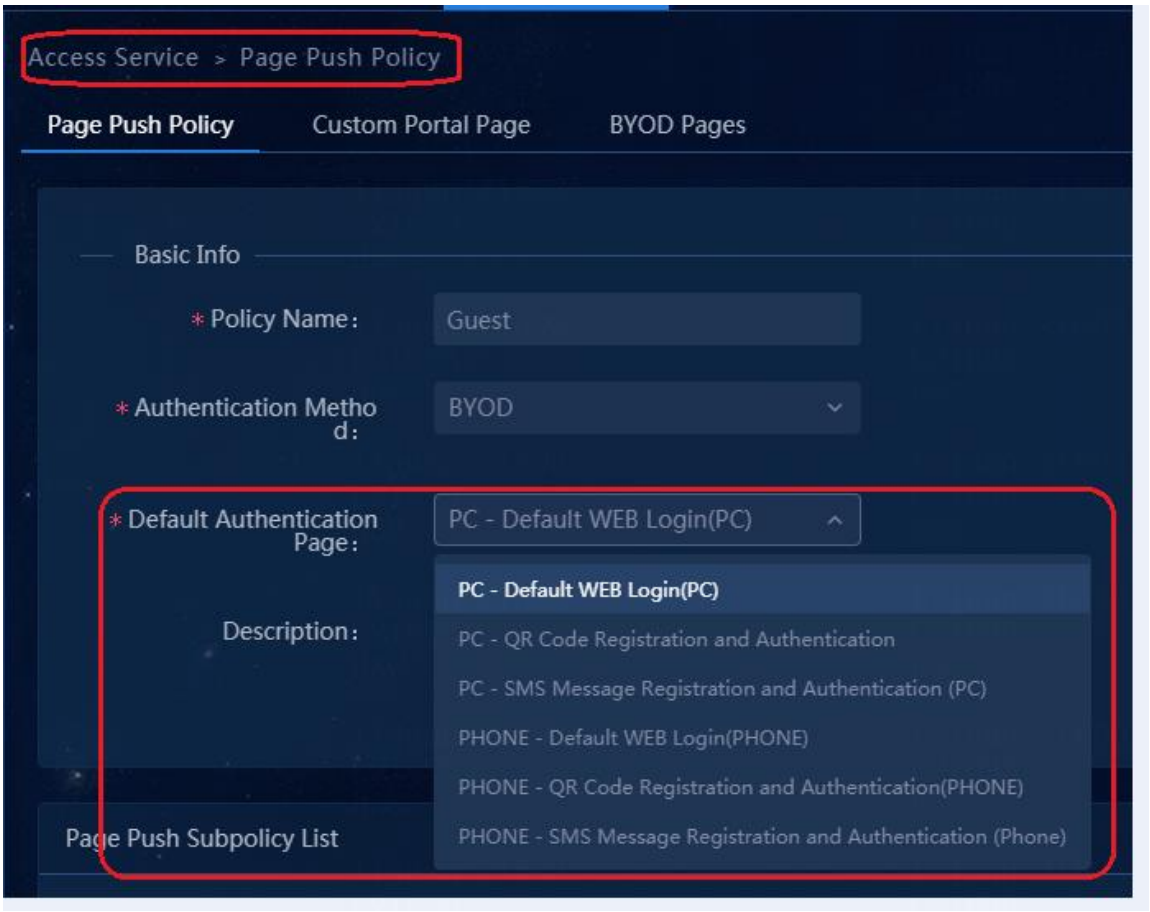


ゲストサービスの設定

ゲストは MAC ポータルユーザーでもあります。ゲストは外部の一時ユーザーであり、アクセス権は制限されています。一時ユーザーにはアカウントがないため、**Page Push Policy** および **BYOD Pages** を構成してゲスト機能を実装し、ゲスト登録機能を提供する必要があります。ゲストは、登録情報を送信して自動的に登録し、システムにログインできます。

システムは、ゲストに対して次のプッシュ方式をサポートします。

- **PC**: デフォルトの WEB ログイン(PC)、QR コードの登録と認証(PC)、SMS メッセージの登録と認証(PC)。
- **PHONE**: デフォルトの WEB ログイン(電話)、QR コードの登録と認証(電話)、SMS メッセージの登録と認証(電話)。
- SMS 認証ページでユーザーの事前登録が完了している場合は、SMS モデムまたは SMS ゲートウェイの設定を完了する必要があります。開かれた認証ページで、ゲストは携帯電話番号を入力し、SMS モデムを介してパスワードを取得してアカウントを開き、ログインします。
- QR コード方式を使用すると、ゲストユーザーは Web ページで QR コードを表示できます。管理者は QR コードをスキャンし、ユーザーを承認するための URL を開きます。ユーザーは、アカウントが正常に開かれた後、直接ログインできます。
- QR コードスキャン方式を使用する場合は、管理者は訪問者がログインするための QR コードを設定することを意味します。ユーザーは、ゲストのネットワークリソースにアクセスするために QR コードをスキャンする必要があります。



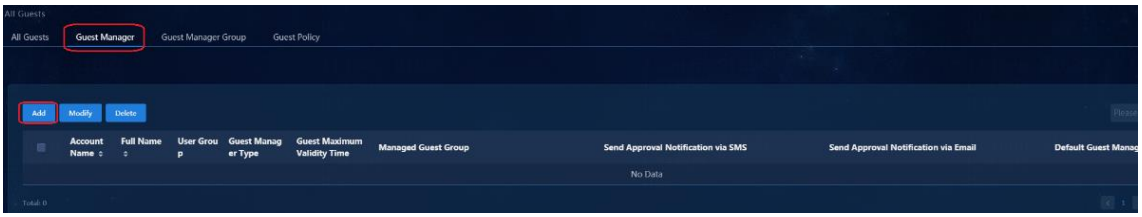
次の項では、**PC - Default Web Login(PC)**方式を紹介します。ゲストは **Guest Auto-Registration** を使用して設定されます。つまり、管理者が手動で承認しなくても、事前登録後にゲストは自動的にオンラインになります。

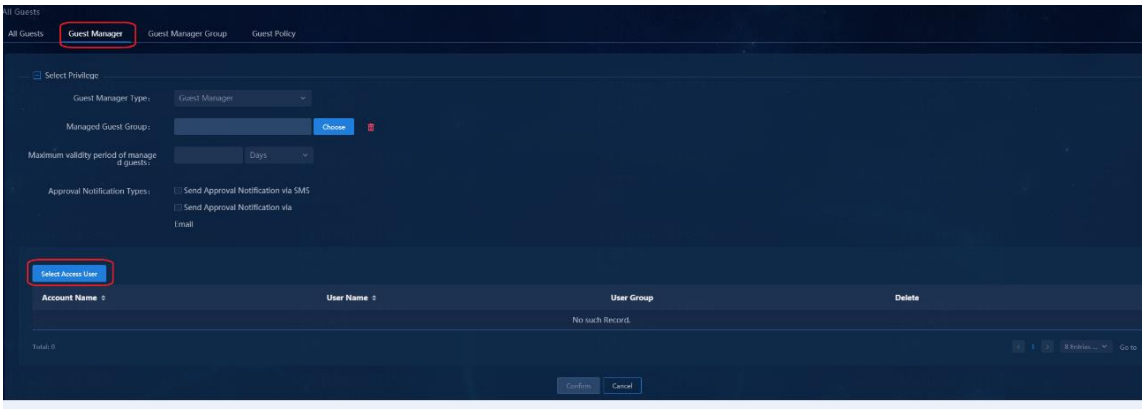
ゲスト管理の設定

ゲストマネージャの設定

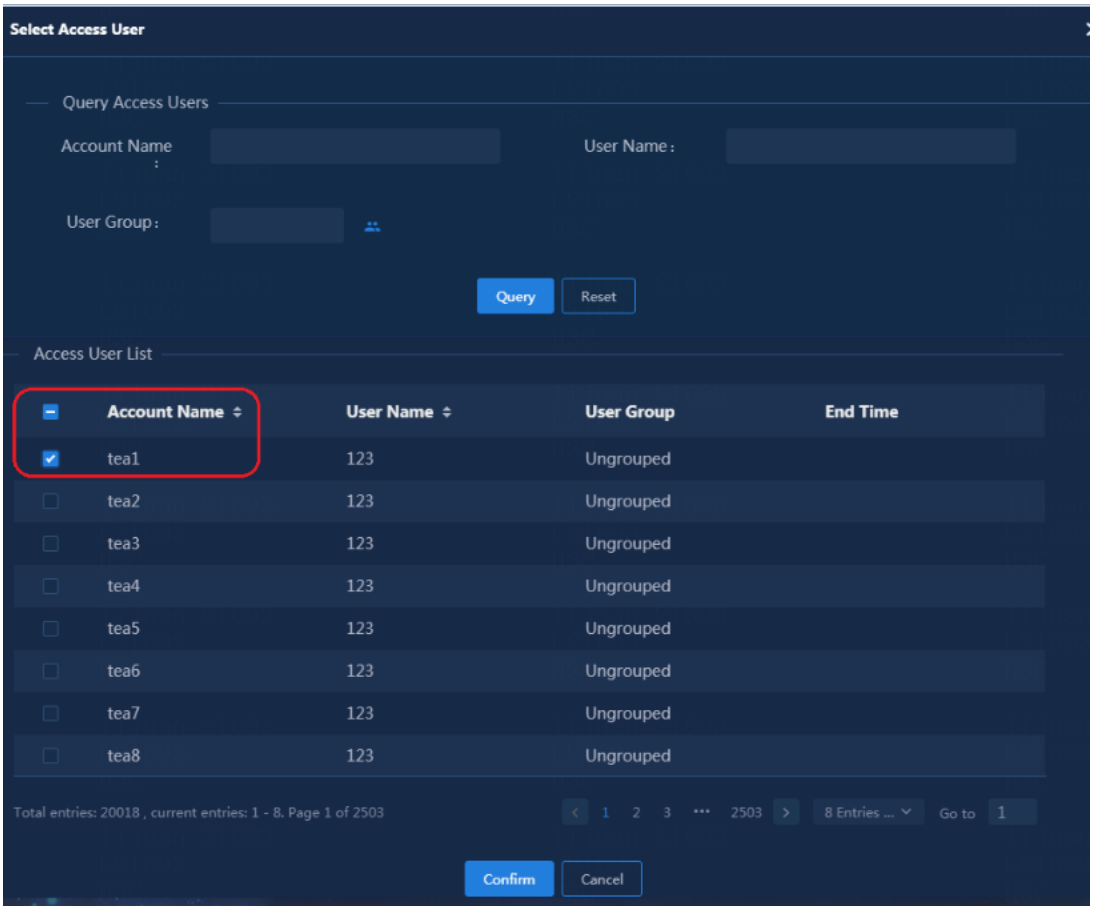
Automation > **User** > **Guest User** ページに移動し、**Guest Manager** タブをクリックして **Guest Manager** ページを開きます。

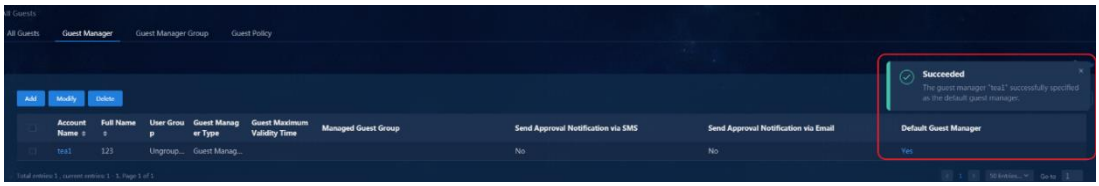
1. **Add** をクリックして、ゲストマネージャを追加するためのページを開きます。Select Access User をクリックして、**Select Access User** ページを開きます。すべてのアクセスユーザー情報を表示できます。**Select Access User** をクリックして、ゲストマネージャとしてアクセスユーザーを選択します。1 つのゲストに 1 つのゲストマネージャが必要です。デフォルトのゲストマネージャを設定することもできます。





2. アクセスユーザーを選択して **OK** をクリックすると、ゲストマネージャを追加するページに戻ります。**Confirm** をクリックすると、**Guest Manager** ページに戻ります。追加されたアクセスユーザーが **Access User List** に表示されます。デフォルトでは、**Default Guest Manager** 列は **No** です。**No** を **Yes** に切り替えると、次のようにアクセスユーザーをデフォルトゲストマネージャーとして設定することができます。



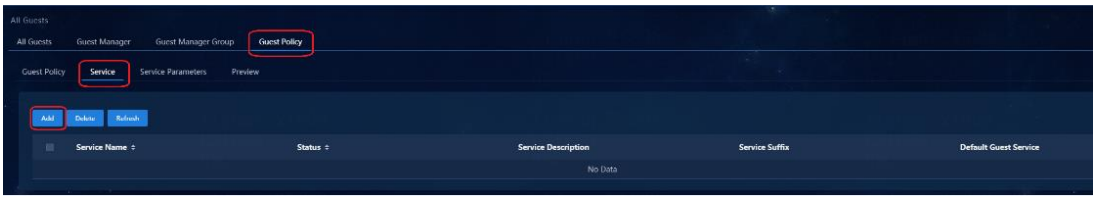


ゲストサービスを構成する

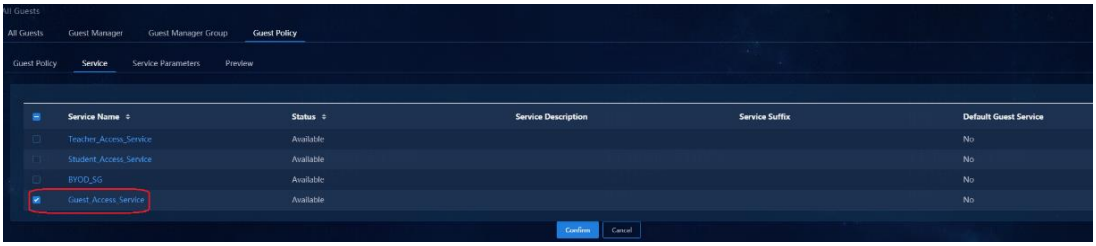
ゲストサービスを追加する前に、レイヤ 2 ネットワークドメイン、セキュリティグループ、アクセスポリシー、およびゲストサービスに対応するアクセスサービスを作成する必要があります。設定の詳細については、『Create a Layer 2 network domain』、『Configure a security group』、『Configure access policies』、および『Configure access services』を参照してください。たとえば、**Guest Security Group** を設定し、対応するアクセスポリシーを設定してから、**Guest Security Group** に関連付ける **Guest Access Service** を設定します。

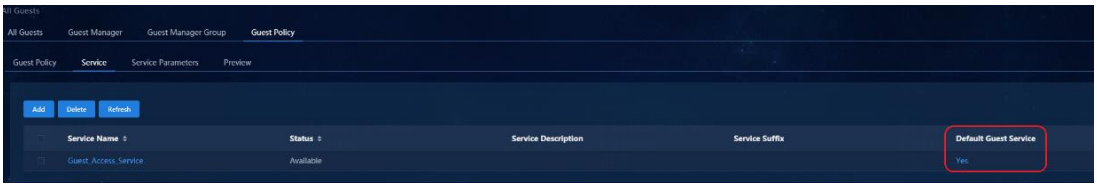
ゲストサービスを設定するには、次の手順を実行します。

1. **Automation** > **User** > **Guest User** > **Guest Policy** > **Service** ページに移動し、**Add** をクリックします。



2. **Service** ページで 1 つ以上の構成済アクセスサービスを選択します。**Confirm** をクリックしてアクセスサービスの追加結果のページを開きます。**Cancel** をクリックして **Service** ページに戻ります。デフォルトのゲストサービスを切り替えるには、**Default Guest Service** 列で **Yes** または **No** をクリックします。ゲストサービスリストにデフォルトのゲストサービスが必要であることに注意してください。

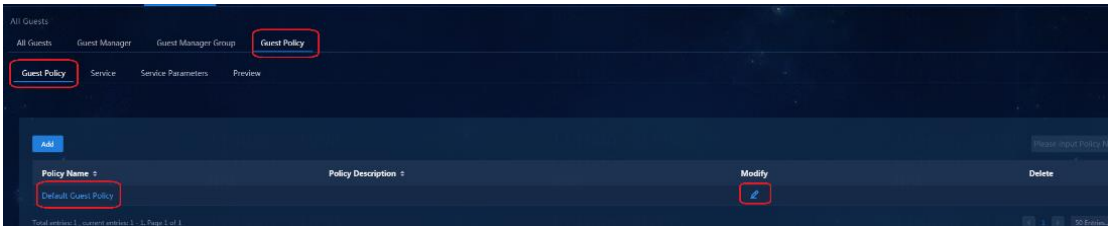




ゲストポリシーの設定

Automation > **User** > **Guest User** > **Guest Policy** > **Guest Policy** ページに移動します。

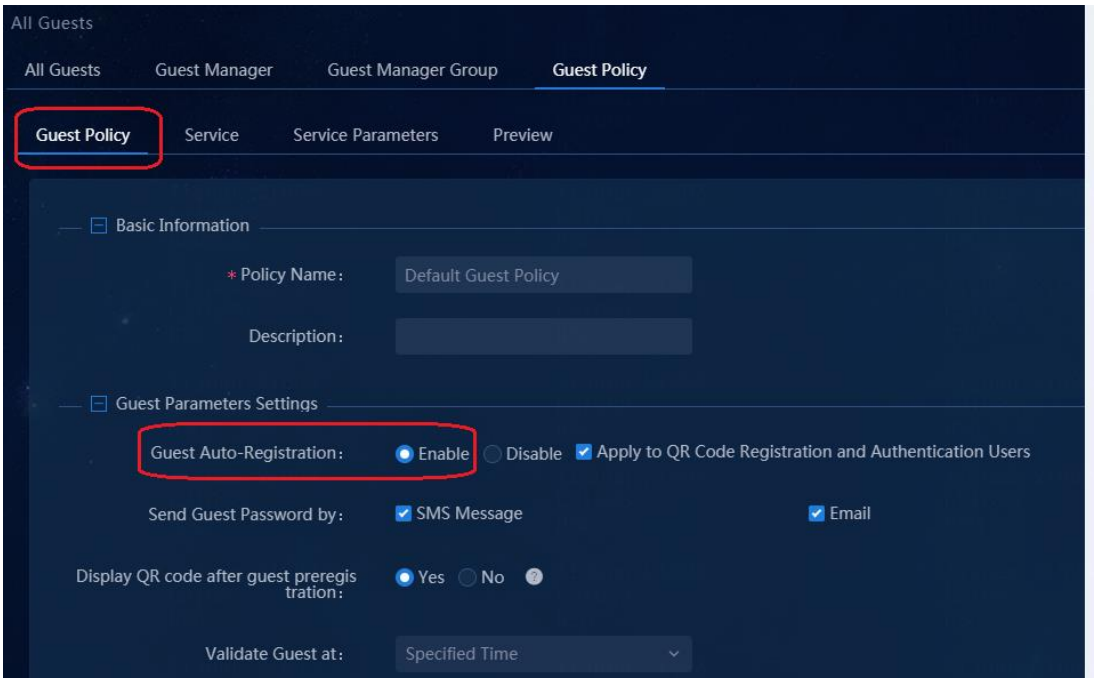
1. デフォルトでは、次の図に示すように、システムにはデフォルトのゲストポリシーがあります。



2. ポリシーを変更するには、をクリックします。

   Guest auto-registration を **Enable** に設定します。この設定により、ゲストユーザーは事前登録の完了後に自動的にオンラインになります。この機能を無効にした場合、ゲストユーザーはゲストマネージャの承認後にのみオンラインになります。

   Guest Auto-Registration を **Enable** に設定した後、**Apply to QR Code Registration and Authentication Users** オプションを選択します。この場合、『Configure page push policy』で **QR Code Registration and Authentication** が設定されていると、ゲスト管理者の承認なしに QR コードをスキャンすることでゲストユーザーが自動的に登録されます。



変更が完了したら、**OK** をクリックします。

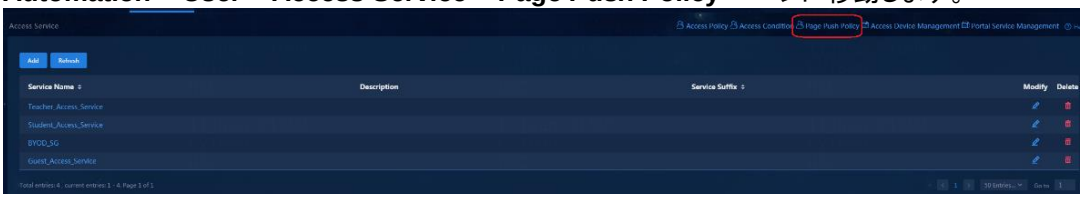
ゲストサービスパラメーターの設定

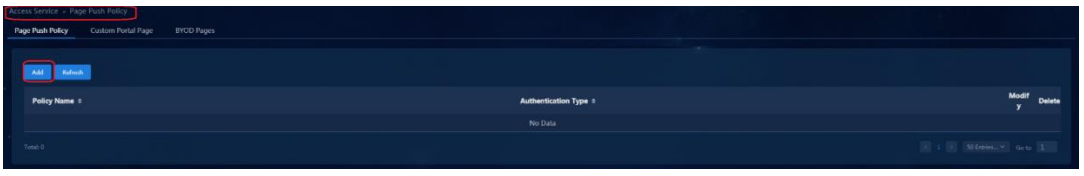
Automation > **User** > **Guest User** > **Guest Policy** > **Service Parameter Settings** ページに移動します。

デフォルトのパラメーターを使用するか、必要に応じて設定を変更できます。設定が完了すると、ゲストユーザーを認証してオンラインにすることができます。設定の詳細については、『Guest online』を参照してください。

ページプッシュポリシーの設定

1. **Automation** > **User** > **Access Service** > **Page Push Policy** ページに移動します。

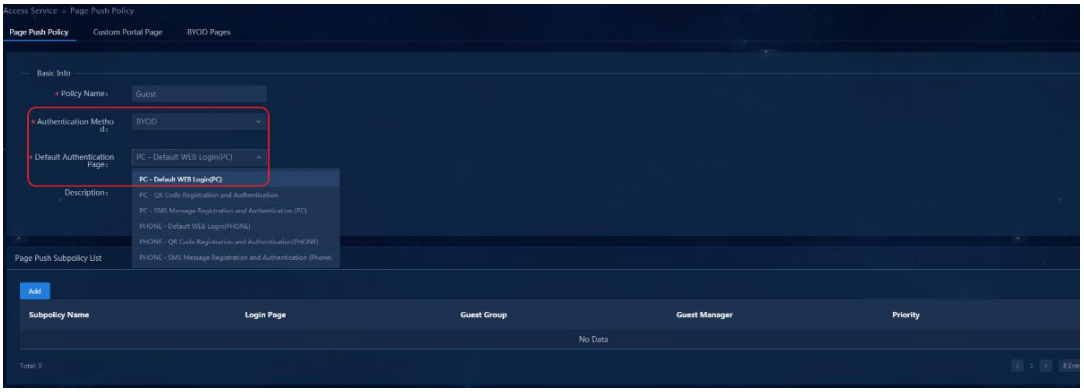




2. **Add** をクリックして、プッシュポリシーを追加するページを開きます。

- **Authentication Method** で **BYOD** を選択します。
- **Default Authentication** ページは **Default WEB Login(PC)**です。必要に応じて認証方法を設定できます。

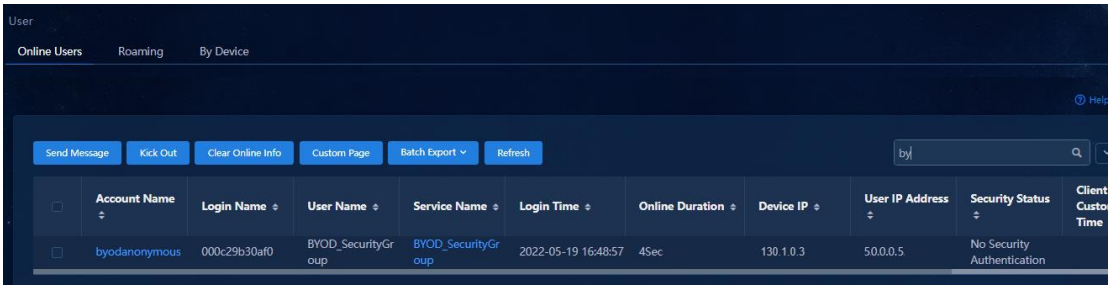
設定後、**OK** をクリックして設定を保存します。新しいプッシュポリシーは、ページのプッシュポリシーリストで表示できます。



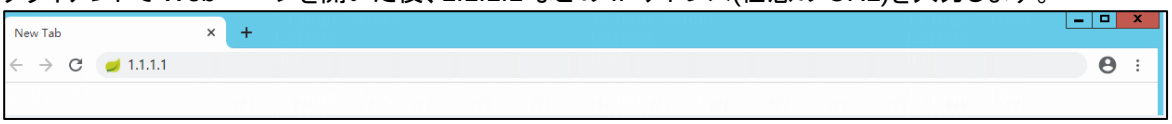
ゲストアクセス

ユーザー認証とオンライン

1. 認証デバイスポートが **UP** になると、MAC アドレス認証がトリガーされます。ゲストは匿名アカウントを使用してオンラインになります。ゲストは **Byodanonymous** アカウントを使用してオンラインになります。**Monitor** > **Monitor List** > **User** > **Online Users** ページに移動します。IP アドレスは、BYOD セキュリティグループのネットワークセグメントから取得されます。



2. クライアントで Web ページを開いた後、1.1.1.1 などの IP アドレス(任意の URL)を入力します。

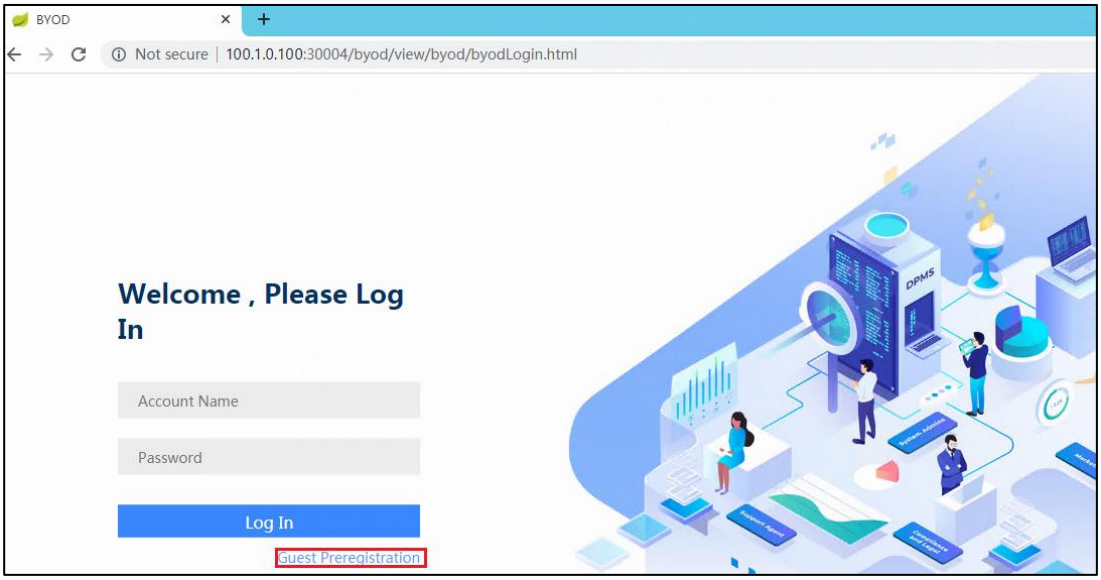


既定の Web ページ

1. デフォルトのページプッシュポリシーは **Default WEB page** です。つまり、ユーザーのコンピュータ

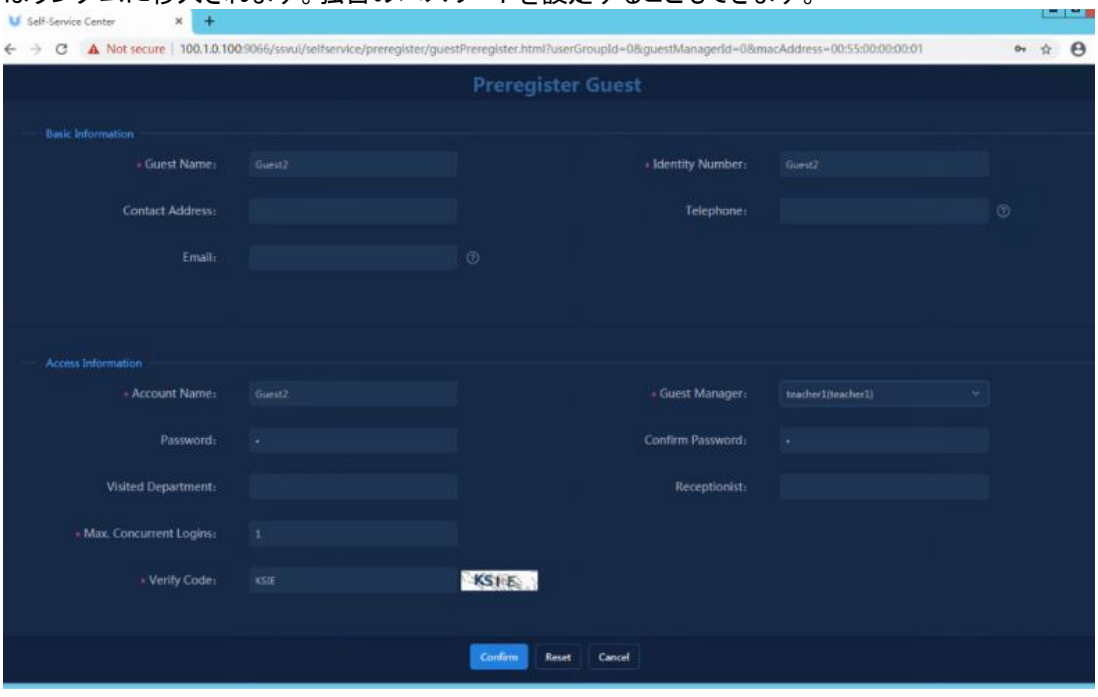
は自動的に次の BYOD デフォルトページにジャンプします。

:http://100.1.0.100:30004/byod/view/byod/byodLogin.html。



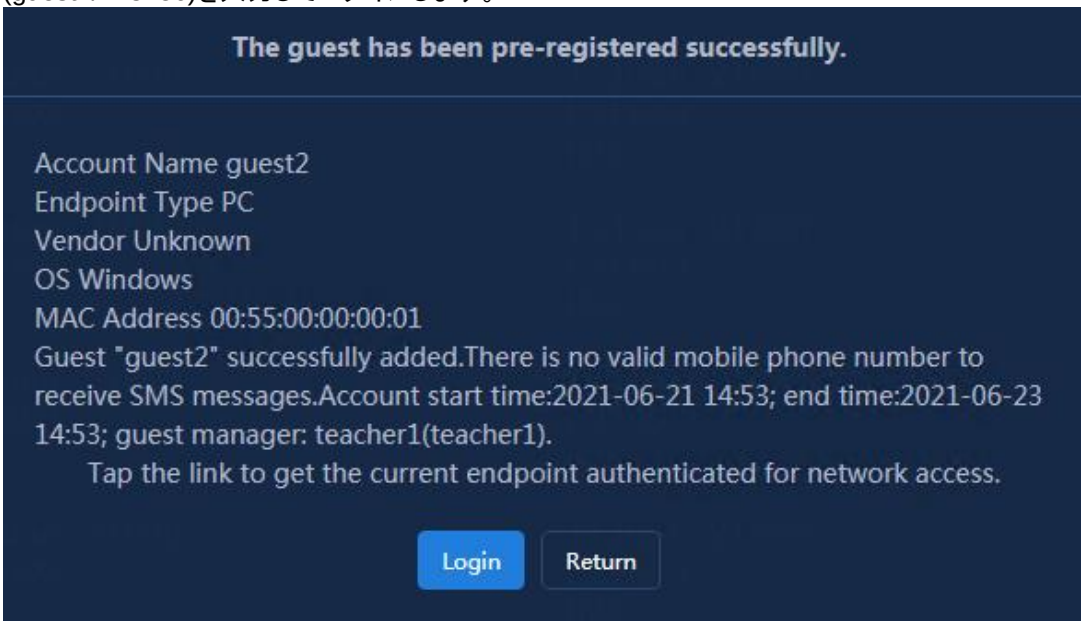
2. **Guest Preregistration** をクリックして次のページを開き、**Account Name**、**Identity Number**、**Verify Code**、および **Guest Manager** など、*印の付いた必須フィールドに入力します。**OK** をクリックして事前登録を完了します。

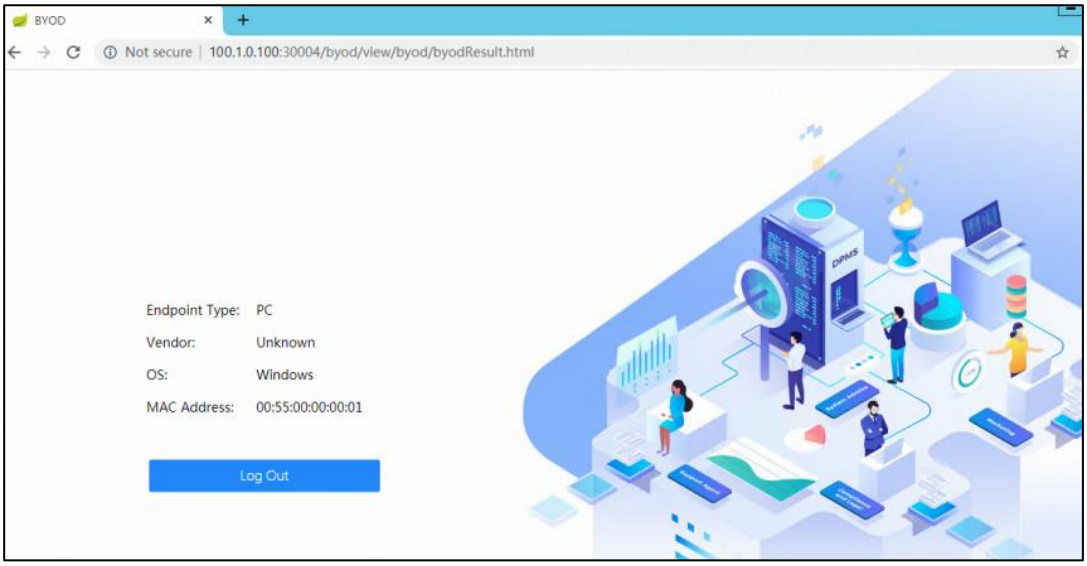
   マネージャは、以前に設定されたデフォルトのマネージャです。設定されていない場合、パスワードはランダムに移入されます。独自のパスワードを設定することもできます。



3. 登録に成功すると、登録結果の情報が表示されます。**Login** をクリックして直接ログインし、**Return** をクリックして BYOD ログインページに移動します。登録済みのアカウントとパスワード

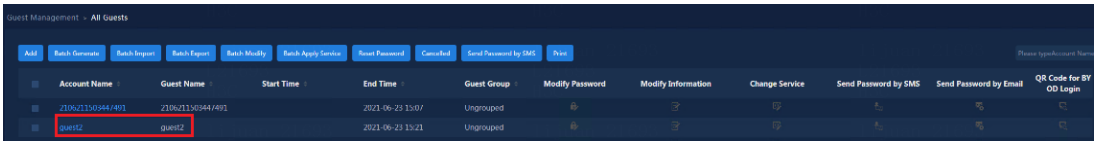
(guest2/123456)を入力してログインします。





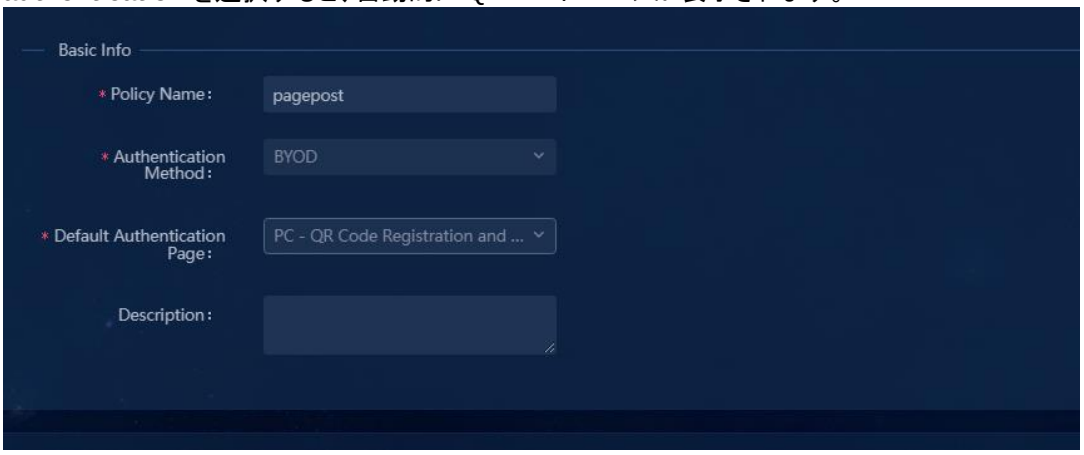
4. **Monitor** > **Monitor List** > **User** > **Online Users** に移動します。guest2 がゲストセキュリティグループの IP アドレスを正常に取得したことを確認できます。

5. **Automation** > **User** > **Guest User** > **All Guests** ページにナビゲートします。登録したゲストユーザーが表示されます。アカウント名をクリックして、登録済ゲストユーザーの詳細を表示します。

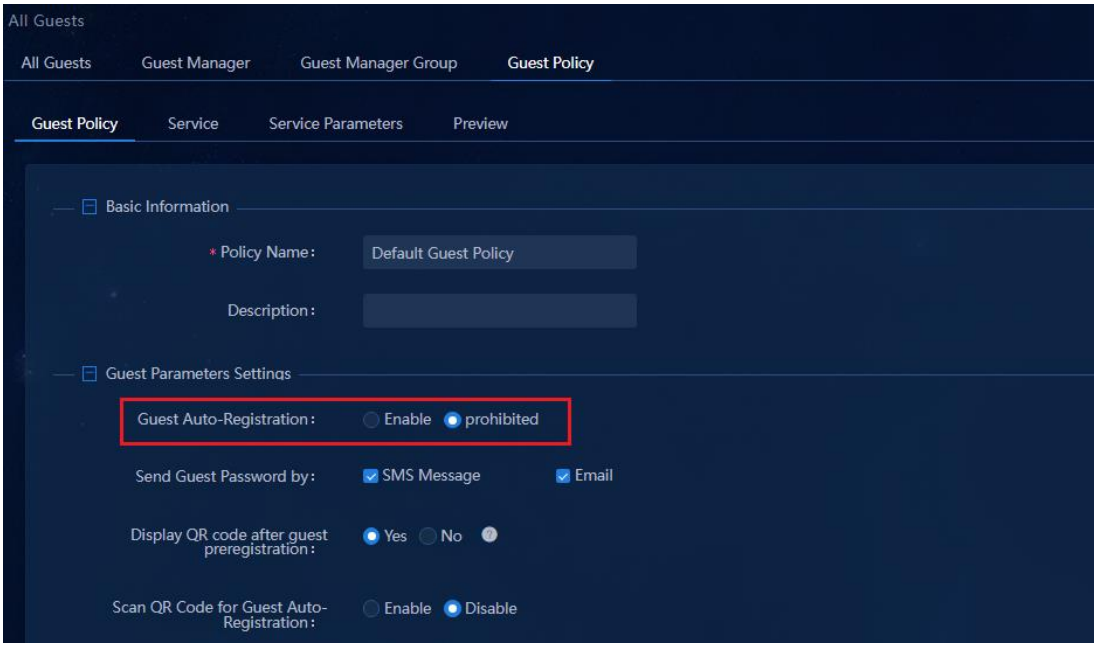


QR コード登録認証

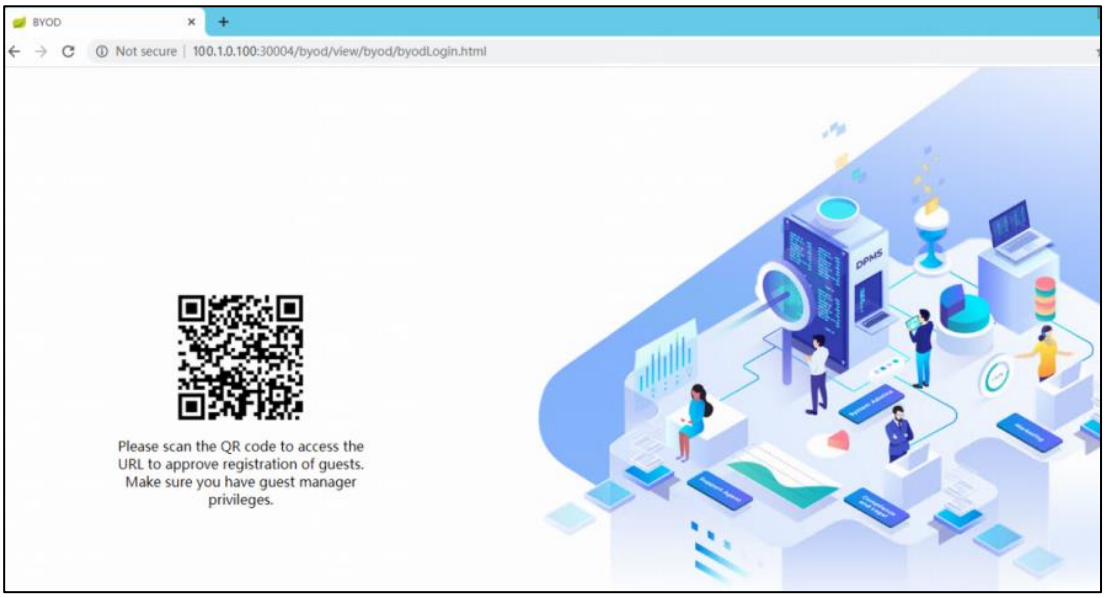
1. 『Configure page push policy』のページプッシュポリシーで **PC-Default PC QR code authentication** を選択すると、自動的に QR コードページが表示されます。



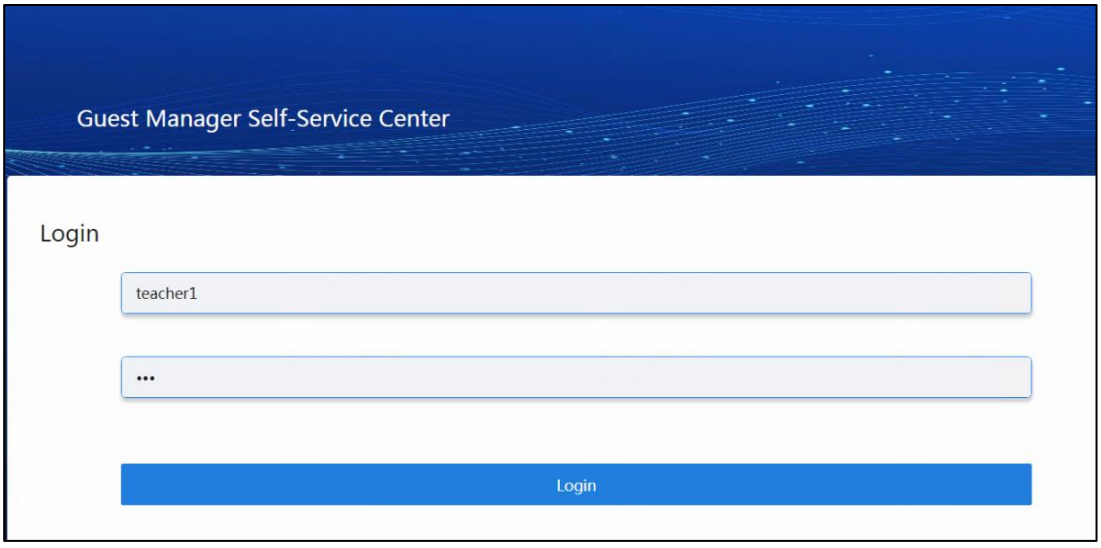
2. **Default Guest Policy** を変更し、**Guest Auto-Registration** を **prohibited** に変更します。ゲストがオンラインになるには、ゲストユーザーがマネージャによって承認される必要があります。



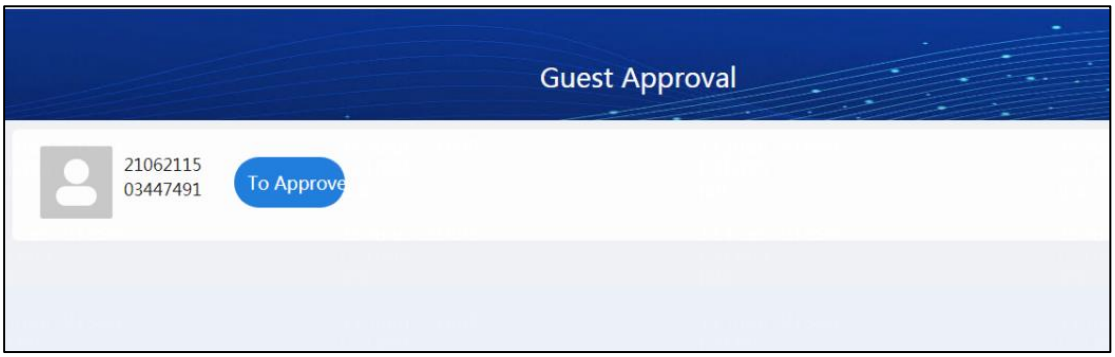
3. クライアント PC の認証ポートが UP になり、BYOD セキュリティグループに入ったら、クライアント PC の Google Chrome で任意の IP アドレスを入力します。QR コードのページは次のように開きます。



4. ゲスト管理者は、このゲスト PC 上の QR コードを携帯で読み取ることができます。Continue をクリックして、ログインページにアクセスします。
   携帯電話がクライアントと同じネットワークに接続されていない場合は、携帯電話に表示されている URL をパソコンに入力すると、次の画面が表示されますので、Guest Manager アカウント (g01/123456)でログインします。

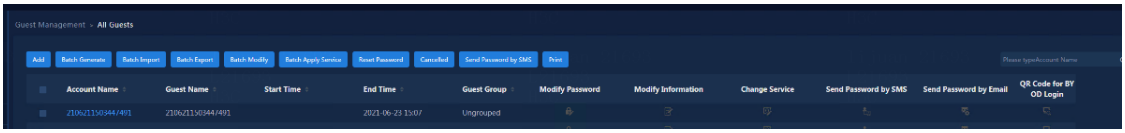


5. ログイン後、次のページが開きます。次に示すアカウントは、ゲストに付与されたアカウントです。マネージャは **To Approve** をクリックして承認ページを開きます。



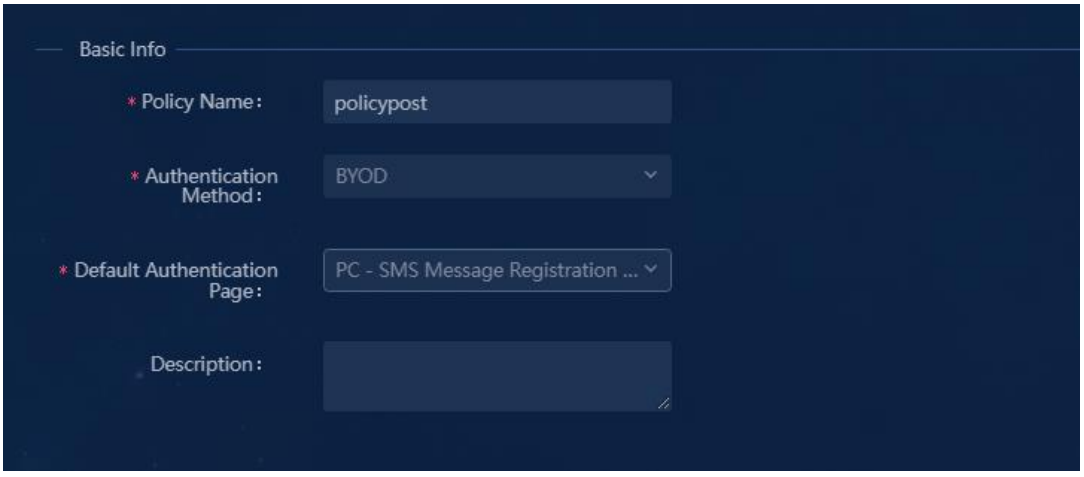
6. **Pass** をクリックしてゲストアカウントを登録します。次に、承認ページが登録成功のページに変わります。

7. 約 20～30 秒後に、ゲストは自動的にログインできます。登録が成功したゲスト情報は、EIA で表示できます。**Automation** > **User** > **Guest Management** > **All Guests** に移動します。ユーザーがゲストアクセスグループにログインし、ゲストアクセスグループの IP セグメントから IP アドレスを取得していることがわかります。



ショートメッセージ登録認証画面

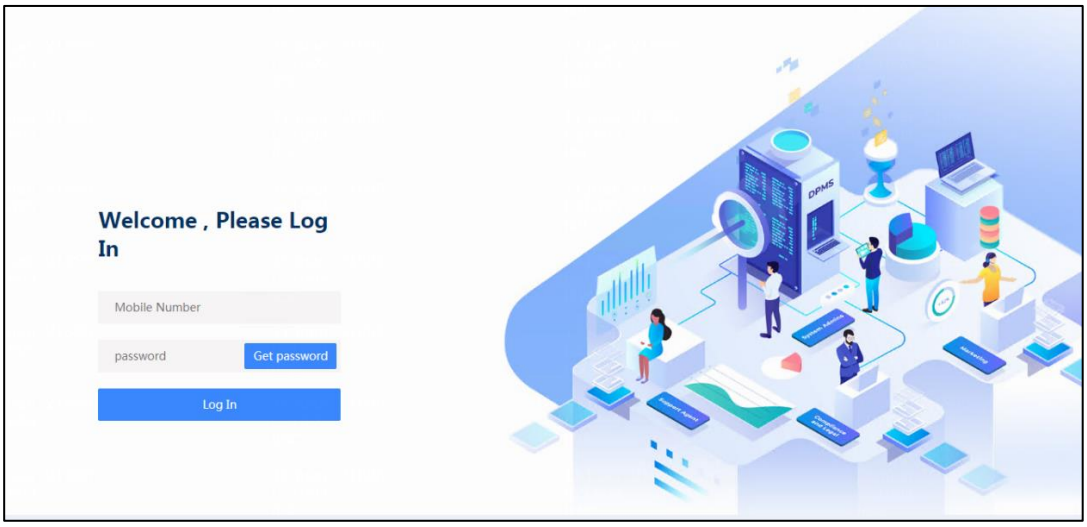
1. 『Configure page push policy』ページで **PC - SMS Message Registration and Authentication** を選択すると、ユーザーの PC はデフォルトの SMS ページに自動的にジャンプします。



2. クライアント PC 認証ポートが **UP** になり、BYOD アクセスグループに入ったら、クライアント PC の

Google Chrome で任意の IP アドレスを入力して、次のようにページを入力します。

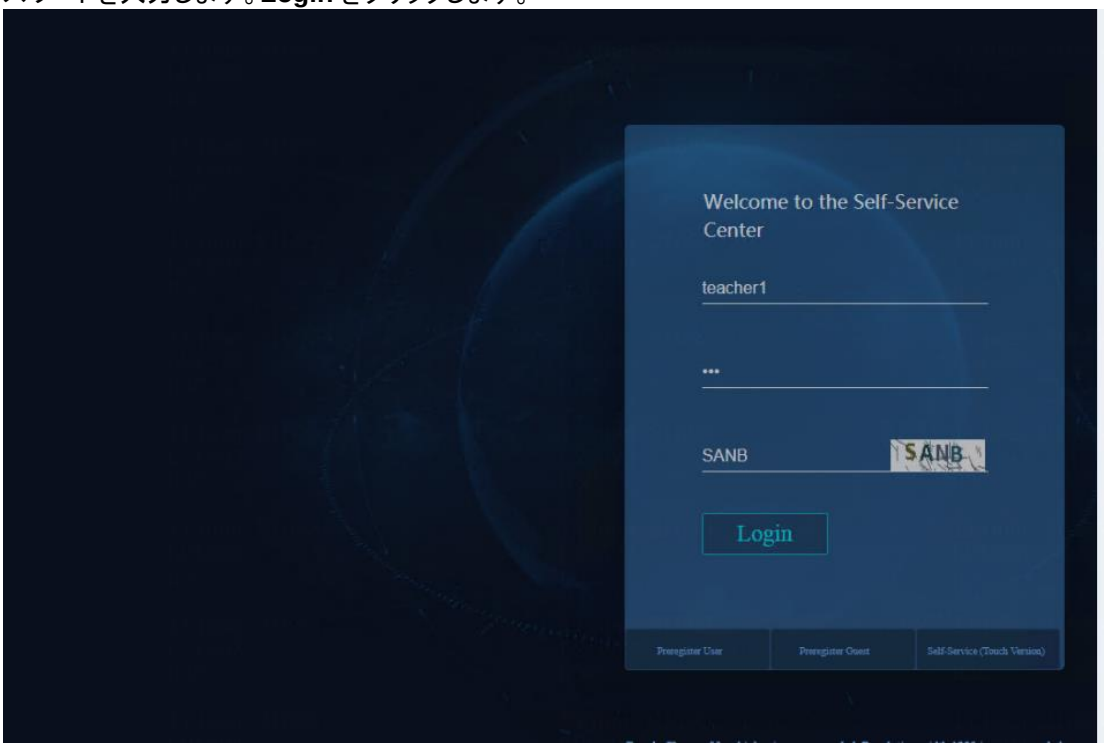
SMS モデムまたは SMS ゲートウェイが使用可能な場合は、携帯電話の番号を入力し、パスワードを取得してログインできます。



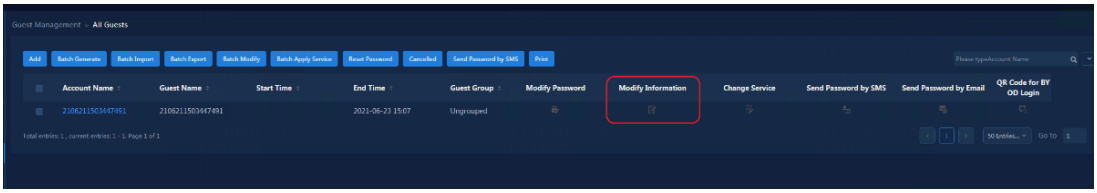
QR コードを読み取ってログイン

管理者はゲストログイン用の QR コードを設定し、ユーザーは QR コードをスキャンするだけでネットワークにログインし、ゲストユーザーのネットワークリソースにアクセスできます。

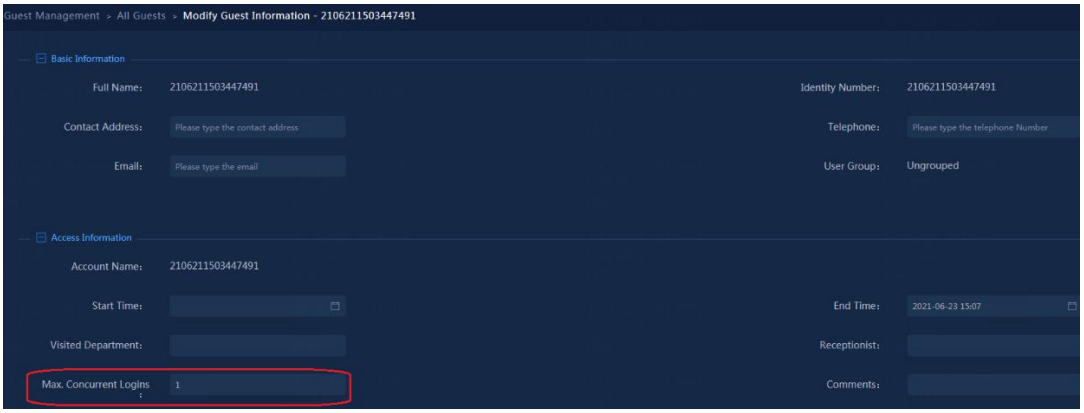
1. ゲストマネージャは、EIA サーバーhttp://100.1.0.100:9066/ssvui/login.html の IP アドレスをブラウザに入力して、**Self-Service Center** ページにログインします。ゲストマネージャのユーザー名とパスワードを入力します。**Login** をクリックします。



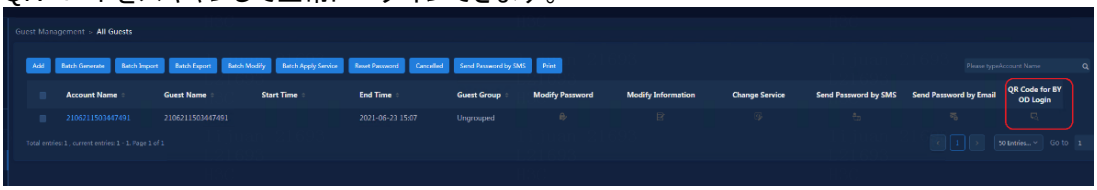
2. **Self-Service Center** にログインした後、**Guest Management** > **All guests** を選択します。ゲスト情報が表示されます。



3. **Add** をクリックしてゲストを追加するか、ゲストリストでゲストを選択し、 をクリックして **Max. Concurrent Logins** を変更します。実際の需要に応じて、QR コードのスキャンを許可するユーザー数を設定します。最大値は 999 です。



4. **Max. Concurrent Logins** を設定したら、 クリックして QR コードページを開きます。ユーザーは QR コードをスキャンして正常にログインできます。



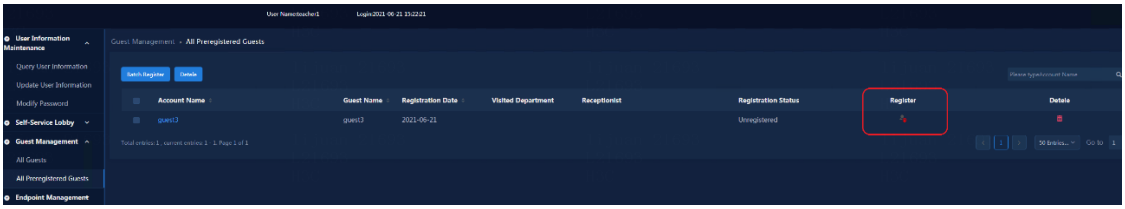
5. WeChat を使用してゲストの QR コードをスキャンしてログインを完了する場合、BYOD セキュリティグループアドレスが外部ネットワークに接続できない場合は、次の手順を実行します。

   ゲストの携帯電話が外部ネットワークに接続されている場合は、WeChat を使用して、マネージャによって生成された QR コードをスキャンし、QR コード内の URL を取得します。

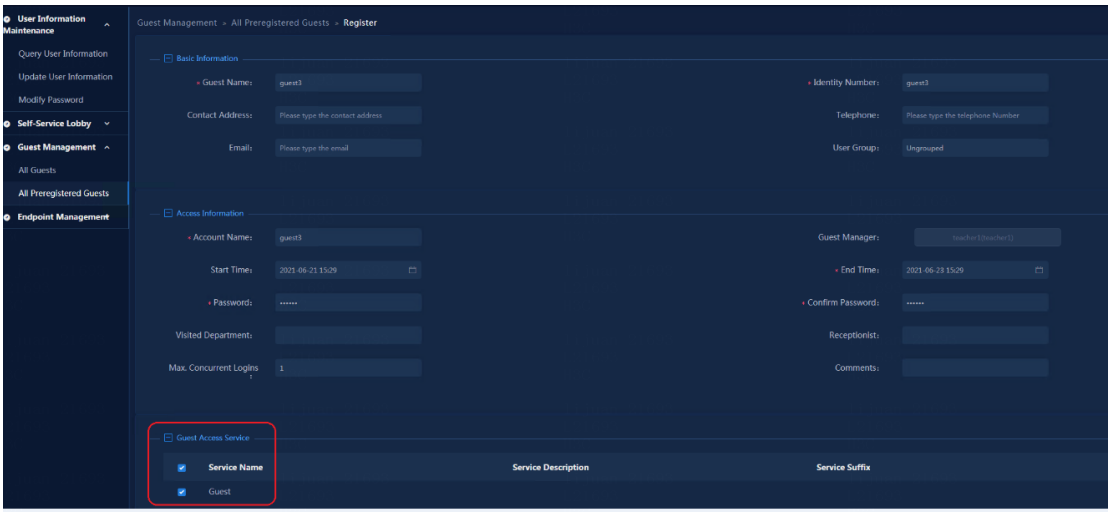
ゲストの承認

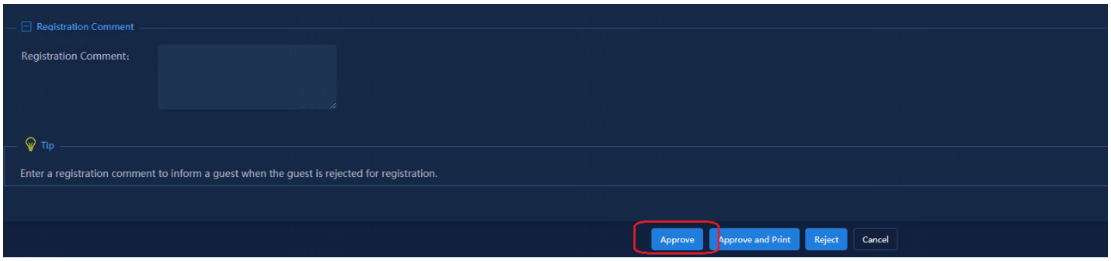
『Configure a guest policy』で **Guest Auto-Registration** が **Disable** に設定されている場合、ゲストはゲストマネージャによって承認される必要があります。ゲストは承認後に公式ゲストユーザーになることができます。

1. ゲストマネージャは、EIA サーバーhttp://100.1.0.100:9066/ssvui/login.html の IP アドレスをブラウザに入力して、**Self-Service Center** ページにログインします。ゲストマネージャのユーザー名とパスワードを入力します。**Login** をクリックします。
2. **Guest Management** > **All Preregistered Guests** に移動して、承認待ちのすべてのゲストユーザーを照会します。承認のために をクリックします。

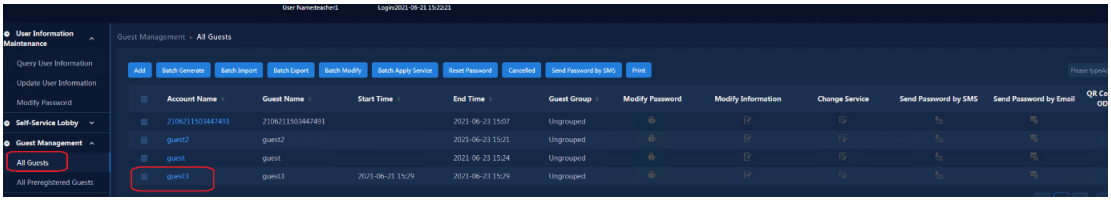


承認では、ゲストのアクセスユーザーを変更できます。『Configure a guest service』で構成されたすべてのアクセスサービスが一覧表示されます。承認をパスするには、**Approve** をクリックします。





3. 承認後、**Automation** > **User** > **Guest Management** > **All Guests** ページで、承認されたゲストユーザーを照会できます。



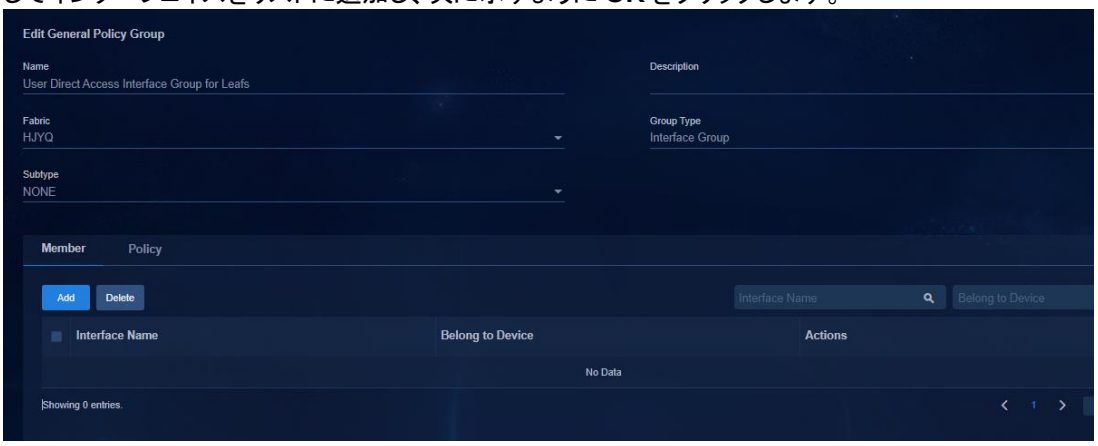
エンドポイントとリーフデバイス間の直接接続の設定

リーフインターフェイスは、アクセスデバイスに加えてエンドポイントに直接接続することもでき、エンドポイントは、リーフインターフェイスに直接接続することによってオンラインになるように認証されます。

インターフェイスグループへのメンバーの追加

1. **Automation** > **Campus Network** > **Device Groups** > **General Device Groups** ページに移動し、**User Direct Access Interface Group for Leafs** の **Actions** カラムをクリックします。

2. **Member** タブをクリックし、**Add** をクリックして、インターフェイスを追加するためのページを開きます。リーフデバイスのエンドポイントに接続されているインターフェイスを選択します。**Add** をクリックしてインターフェイスをリストに追加し、次に示すように **OK** をクリックします。

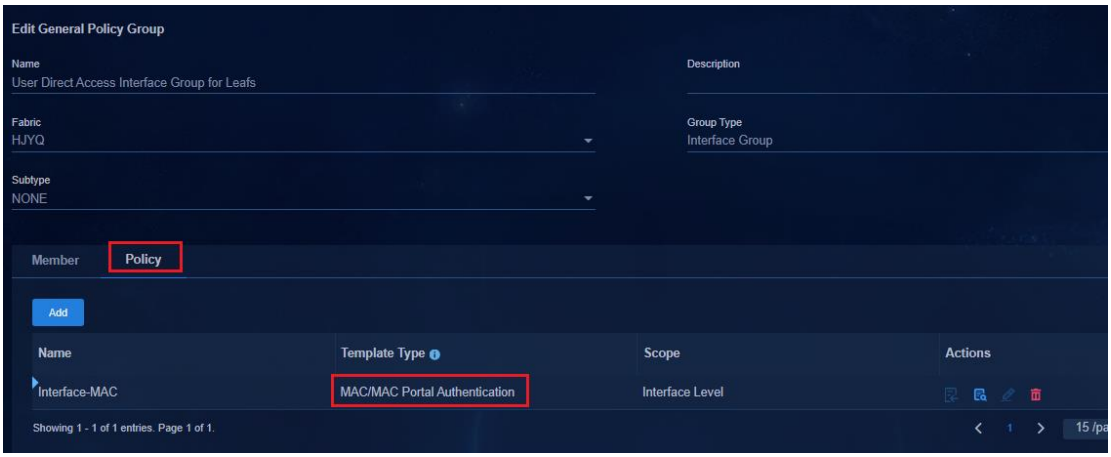


3. **OK** をクリックして、追加を完了します。

インターフェイスグループ展開ポリシーを設定する

1. **Automation** > **Campus Network** > **Devices** > **General Device Group** ページに移動し、**Add** をクリックしてセキュリティグループを追加するか、**Actions** カラムをクリックします。**Policy** タブをクリックし、グループポリシーに追加するために前に設定したカスタムポリシーモードを選択します。実際の状況に応じて、802.1X 認証テンプレートまたは MAC ポータル認証テンプレートを配信します。

2. 2 つの方法のうち 1 つだけを選択します。ベストプラクティスとして、物理インターフェイス上で 802.1X 認証と MAC ポータル認証の両方を設定しないでください。



3. 次のように、リーフデバイスに設定を展開します。

   実際の状況に基づいて、802.1X 認証または MAC/MAC ポータル認証設定を展開します。2 つの認証方法のうち 1 つだけを指定します。MAC/MAC ポータル認証を例に挙げます。

   //直接接続された Leaf デバイスのインターフェイス。

```
#
interface Ten-GigabitEthernet 0/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1
 mac-based ac
 mac-authentication
 mac-authentication domain hz1
 mac-authentication parallel-with-dot1x
 mac-authentication critical vsi vsi167 url-user-logoff
#
```

4. 設定が完了すると、リーフデバイスに接続されているエンドポイントを認証できます。

fail-permit スキームを設定する

fail-permit スキームは主に、EIA サーバーに障害が発生し、ユーザー認証が EIA サーバーに接続できない場合に、ユーザーが特定のセキュリティグループ内のリソースにアクセスできるようにするために使用されます。特定のセキュリティグループは、fail-permit セキュリティグループです。

Fail-Permit サービスを設定する場合、Fail-Permit サービス用に DHCP サーバーを設定する必要があり、Fail-Permit セキュリティグループに対応するサブネットが Fail-Permit DHCP サーバーに配信されます。H3C DHCP サーバーまたはサードパーティーの DHCP サーバーを使用できます。

マイクロセグメンテーションソリューションは、ダイナミック AC 認証ユーザー失敗許可とスタティック AC 認証ユーザー失敗許可を提供します。

- 動的 AC 認証ユーザー失敗許可:分離ドメインは、1 つの失敗許可セキュリティグループのみをサポートします。異なるプライベートネットワークのユーザーは、同じ失敗許可セキュリティグループを使用します。
- 静的 AC 認証ユーザー失敗許可:静的 AC ユーザー失敗許可は、静的 AC 認証ユーザー用の新しい失敗許可機能です。各プライベートネットワークは、失敗許可セキュリティグループで構成されます。ユーザーの IP アドレスは、ユーザーが失敗許可セキュリティグループに割り当てられても変更されません。システムは、ユーザーを認証する静的 AC が属するプライベートネットワークに基づいて、ユーザーの失敗許可セキュリティグループを決定します。

重要:

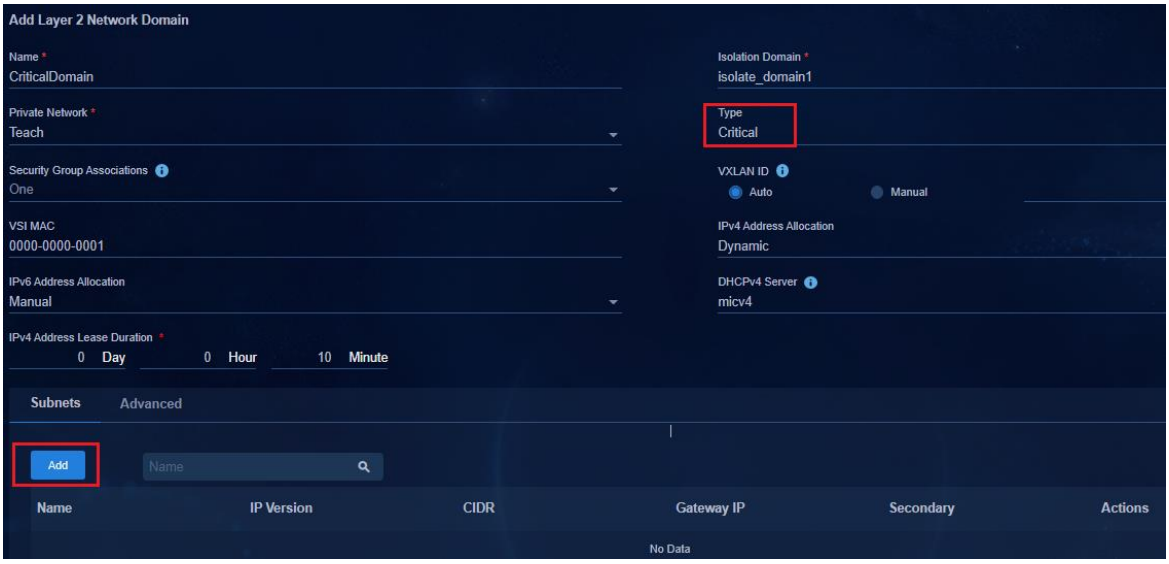
- fail-permit には、ダイナミック AC 認証ユーザーfail-permit とスタティック AC 認証ユーザーfail-permit の 2 つのモードがあります。
- 分離ドメインは、動的 AC ユーザーに対して 1 つの失敗許可セキュリティグループのみをサポートします。複数の分離ドメインが存在する場合、各ドメインに失敗許可セキュリティグループを構成するか、同じ失敗許可セキュリティグループを使用するようにドメインを構成できます。
- スタティック AC ユーザーの失敗許可では、各プライベートネットワークに失敗許可セキュリティグループが必要です。
- ユーザーのプライベートネットワークで fail-permit セキュリティグループを設定する必要があります。vpn-default で fail-permit セキュリティグループを設定することはできません。
- AD-Campus 6.0 ソリューションでは、fail-permit DHCP サーバーを設定する必要があります。
- fail-permit DHCP サーバーと、EIA サーバー、BYOD DHCP サーバー、およびサービス DHCP サーバーは、別のサーバーに設定する必要があります。fail-permit DHCP サーバーとデバイスが相互接続されていることを確認してください。
- EAD を使用しない場合は、ベストプラクティスとして **Enable the policy server** を選択しないでくださ

い(システムはデフォルトでこのオプションを選択します)。そうしないと、失敗許可時間が 3 ハートビート間隔を超えた後、iNode クライアントのオンライン 802.1X ユーザーは自動的にオフラインになります。パラメーターを設定するには、**Automation** > **User Service** > **Access Parameters** > **Policy Server Parameter Settings** ページに移動します。

fail-permitレイヤ2ネットワークドメインを作成する

Automation > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動します。**Add** をクリックして **Add Layer 2 Network Domain** ページを開き、次のようにパラメーターを設定します。

- **Isolation domain**: 分離ドメインを選択します。
- **Private Network**: プライベートネットワークを選択します。vpn-default は選択しないでください。
- **Type**: **Critical** を選択します。
- **IPv4 Address Allocation**: **Dynamic** を選択します。
- **DHCPv4 Server**: fail-permit の DHCP サーバーを選択します。実際の環境に合わせてパラメーターを設定してください。
- **IPv4 Address Lease Duration**: デフォルト設定は 10 分です。デフォルト設定を使用することをお薦めします。



重要:

分離ドメインは、1 つの失敗許可レイヤ 2 ネットワークドメインだけをサポートします。失敗許可レイヤ 2 ネットワークドメインは、ダイナミック AC 認証ユーザーに適用できます。スタティック AC 認証ユーザーの失敗許可では、失敗許可レイヤ 2 ネットワークドメインを作成する必要はありません。

リーフデバイスに設定を展開します。

#リーフデバイスの VSI インターフェイスの DHCP サーバーIP アドレスを、失敗許可サーバーの IP アドレスとして設定します。

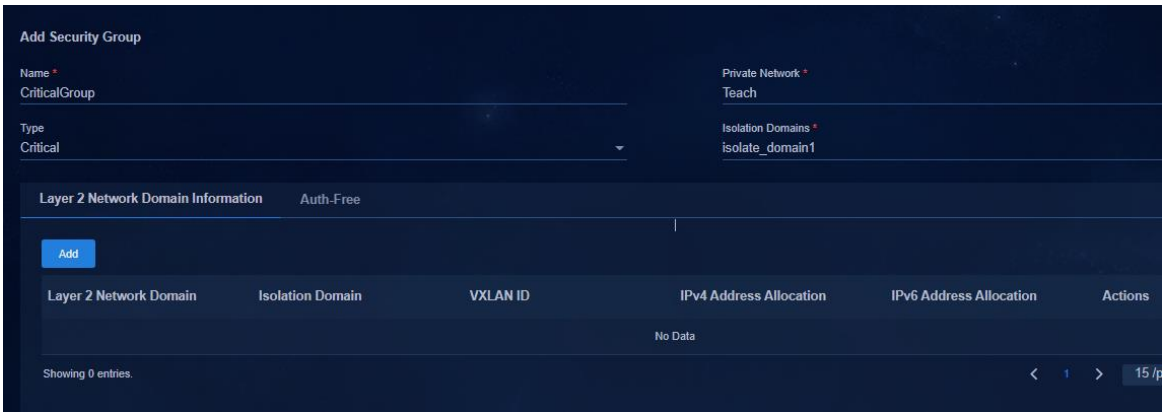
```
interface Vsi-interface7
 description SDN_VSI_Interface_7
 ip binding vpn-instance vpn1
 ip address 52.0.0.1 255.255.0.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 arp scan keepalive enable
 arp fib-miss drop
 dhcp select relay proxy
 dhcp relay information circuit-id vxlan-port
 dhcp relay information enable
 dhcp relay server-address 8.0.0.171     //fail-permitDHCP サーバーを指定します。.
 dhcp relay source-address interface Vsi-interface4094
 dhcp relay request-from-tunnel discard
 ipv6 nd scan keepalive enable
 ipv6 nd fib-miss drop
 distributed-gateway local
#
```

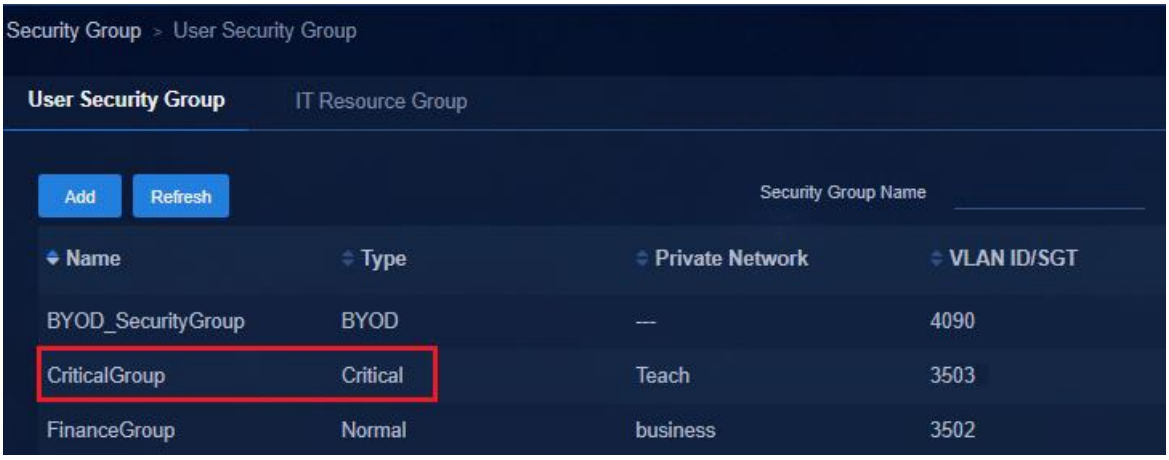
fail-permitセキュリティグループを作成する

Automation > **Campus Network** > **Security Group** > **User Security Group** ページに移動します。**Add** をクリックして、セキュリティグループを追加するためのページを開きます。

- **Private Network**: プライベートネットワークを選択します。動的 AC 認証失敗許可の場合、1 つのプライベートネットワークを選択します。静的 AC 認証失敗許可の場合、失敗許可を必要とする各プライベートネットワークには、失敗許可セキュリティグループが必要です。
- **Type**: **Critical** を選択します。
- **Isolation Domain**: 分離ドメインを選択します。複数の分離ドメインが存在する場合、複数の分離ドメインを選択できます。
- **Layer 2 Network Domain**: ダイナミック AC 認証失敗許可の場合、追加された失敗許可レイヤ 2 ネットワークドメインを選択します。スタティック AC 認証失敗許可の場合、レイヤ 2 ネットワークドメインを設定する必要はありません。

次の図は、ダイナミック AC 認証の失敗許可を示しています。





#マイクロセグメンテーション設定を展開します。

```
microsegment 3503 name SDN_EPG_3503
 member ipv4 52.0.0.0 255.0.0.0 vpn-instance Teach
#
```

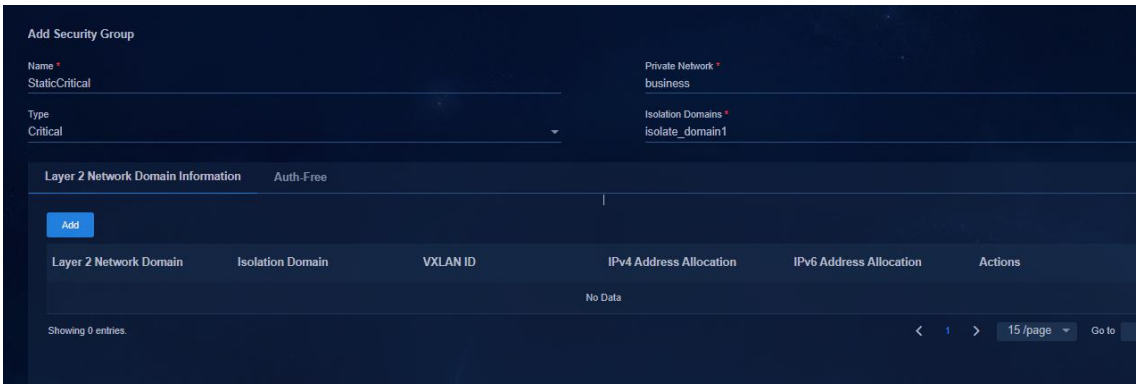
#Deploy the mapping between fail-permit and VXLAN.

```
radius scheme hz1
 primary authentication 100.1.0.100 vpn-instance vpn-default
 primary accounting 100.1.0.100 vpn-instance vpn-default
 accounting-on enable send 255 interval 15
 key authentication cipher $c$3$FXUDf5A1SBDyvwfeTdd0qCAAG2zCQQxibQ==
 key accounting cipher $c$3$4E53VM7criBNRPyjrfoHpsHIO5Va2gyDxA==
 timer realtime-accounting 15
 user-name-format without-domain
 vpn-instance vpn-default
 attribute translate
 stop-accounting-packet send-force
 attribute convert H3c-User-Group to H3C-Microsegment-Id received
 microsegment 3502 associate vsi vsi4
 microsegment 3503 associate vsi vsi7
 microsegment 3504 associate vsi vsi3
 microsegment 3505 associate vsi vsi3
 microsegment 4090 associate vsi vsi5
#
```

次の図は、スタティック AC 認証の失敗許可を示しています。

スタティック AC 認証失敗許可は、スタティック AC によって認証されたユーザーに適用されます。

スタティック AC 認証を使用する各プライベートネットワークに対して、失敗許可セキュリティグループを設定する必要があります。失敗許可セキュリティグループを設定する場合、レイヤ 2 ネットワークドメインを設定する必要はありません。



設定が完了すると、コントローラはマイクロセグメンテーション設定を発行します。

```
#
microsegment 3508 name SDN_EPG_3508
#
```

リーフダウンリンクインターフェイスにfail-permitを設定します。

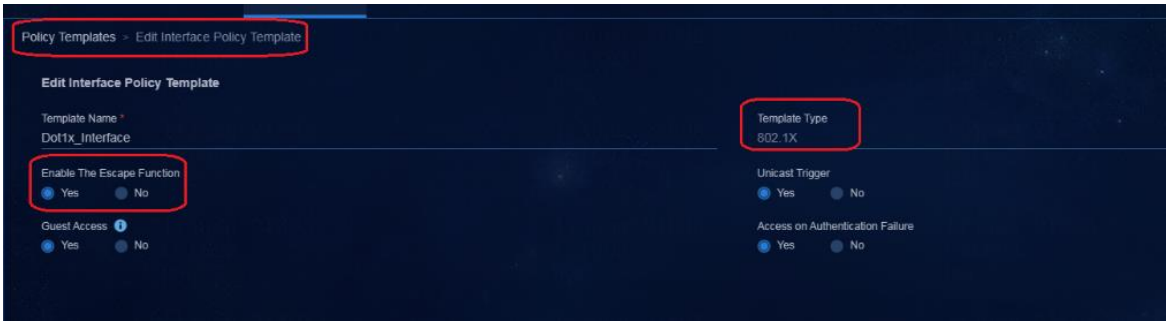
Automation > **Campus Network** > **Devices** > **General Device Group** > **Policy Template** ページでポリシーテンプレートを設定します。次の項では、インターフェイスポリシーテンプレートの設定について説明します。

802.1X 認証用のインターフェイスポリシーテンプレート

Enable The Escape Function で **Yes** を選択します。

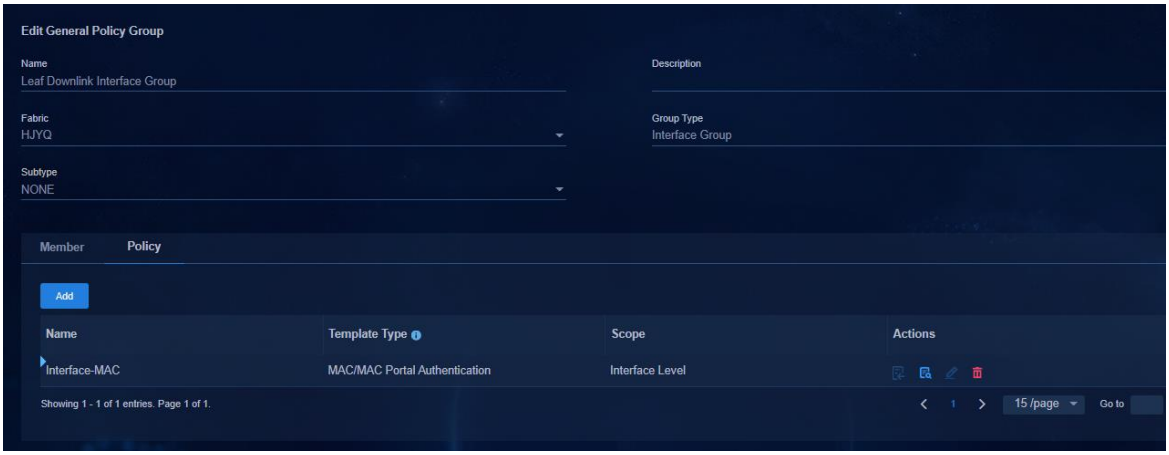
MAC 認証用のインターフェイスポリシーテンプレート

Enable The Escape Function で **Yes** を選択します。



リーフダウンリンクインターフェイスグループへのポリシーテンプレートの展開

ここまでの項では、802.1X 認証および MAC 認証の失敗許可の設定について説明しました。必要に応じて、802.1X 認証または MAC 認証の失敗許可を設定します。この例では、MAC 認証ポリシーテンプレートをリーフダウンリンクインターフェイスグループに展開します。



- コントローラによってリーフデバイスに展開されるコマンド:

  # fail-permit テンプレート設定を展開します。

  ```
  aaa critical-profile SDN_GLOBAL_CRITICAL_PROFILE
   default critical-microsegment 3503 vsi vsi7     //Dynamic AC fail-permit.
   if-match vpn-instance vpna critical-microsegment 3503     //Static AC fail-permit. This configuration is only issued on the private network of a Layer 2 network domain configured with static access.
   if-match vpn-instance vpnb critical-microsegment 3508
  #
  # Deploy configuration to the downlink interface on the leaf device.
  interface Bridge-Aggregation1024
   port link-type trunk
   port trunk permit vlan 1 101 to 3000 4093 to 4094
  ```

```
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 mac-authentication
 mac-authentication domain hz1
mac-authentication parallel-with-dot1x
 mac-authentication critical profile SDN_GLOBAL_CRITICAL_PROFILE  //MAC authentication fail-permit.
 port-security free-vlan 1 4094
 #
 service-instance 2801
  encapsulation s-vid 2801
  xconnect vsi vsi13
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

- 802.1X 認証失敗許可が設定されている場合、次の設定が展開されます。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4093 to 4094
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 dot1x
undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x critical eapo
 dot1X critical profile SDN_GLOBAL_CRITICAL_PROFILE//802.1X authentication fail-permit.
 port-security free-vlan 1 4094
 #
 service-instance 2801
  encapsulation s-vid 2801
  xconnect vsi vsi13
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

ITリソースアクセスの失敗を許可する設定を構成する

vpn-default には、fail-permit セキュリティグループを設定できません。分離ドメインに設定されている fail-

permit セキュリティグループは異なります。複数のプライベートネットワークからアクセスされる一部の IT リソースグループを vpn-default プライベートネットワークに展開することをお勧めします。次に、プライベートネットワークで IT リソースグループを設定し、fail-permit セキュリティグループと IT リソースグループのアクセス権限を設定します。

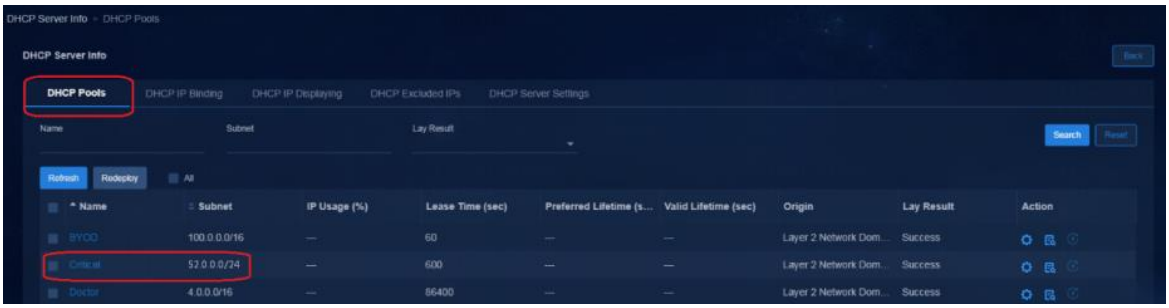
デフォルトでは、プライベートネットワークは vpn-default と通信できます。プライベートネットワークのデフォルトのアクセスポリシーが許可か拒否かにかかわらず、プライベートネットワークは vpn-default に関連付けられた IT リソースグループにアクセスできます。したがって、プライベートネットワークで IT リソースグループを構成し、セキュリティグループがアクセスを許可されていない IT リソースグループのアクセスポリシーを設定する必要があります。アクセスを許可されていない IT リソースグループに対して拒否グループポリシーを展開し、リソースへのアクセスを禁止します。

fail-permit DHCPサーバーを設定する

密結合の Microsoft DHCP サーバーを構成する

フェイル許可 DHCP サーバーが Microsoft DHCP サーバーである場合は、VXLAN 4094 アドレスプールを構成する必要があります。DHCP サーバーを Microsoft タイトカップリングとして設定する方法については、『Add a Microsoft DHCP server』の VXLAN 4094 アドレスプール構成を参照してください。

fail-permit セキュリティグループが作成されると、選択した fail-permit DHCP サーバー上に、次のように fail-permit サービスのアドレスプールが作成されます。



重要:

分離ドメイン内に複数のファブリックが存在する場合は、複数のファブリックに対して VXLAN 4094 のアドレスプールを設定する必要があります。

疎結合の Microsoft DHCP サーバーを構成する

疎結合の場合、SeerEngine キャンパスコントローラは DHCP サーバーに設定を展開しません。DHCP サーバー上の fail-permit セキュリティグループにサブネットのアドレスプールを手動で作成する必要があります。

VLAN 4094 スコープを作成する

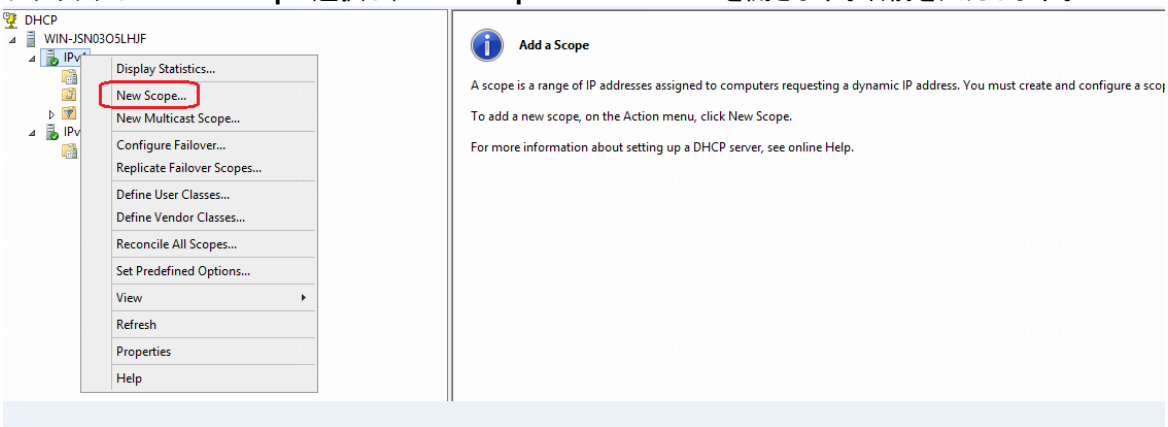
Microsoft DHCP サーバーで VLAN 4094 のスコープを手動で設定します。

このアドレススコープを設定する目的は、ユーザーが後で作成される fail-permit セキュリティグループの IP アドレスプールから IP アドレスを取得できるようにすることです。VLAN 4094 スコープを設定しない場合、ユーザーは他のセキュリティグループによって作成されたスコープから IP アドレスを取得できません。

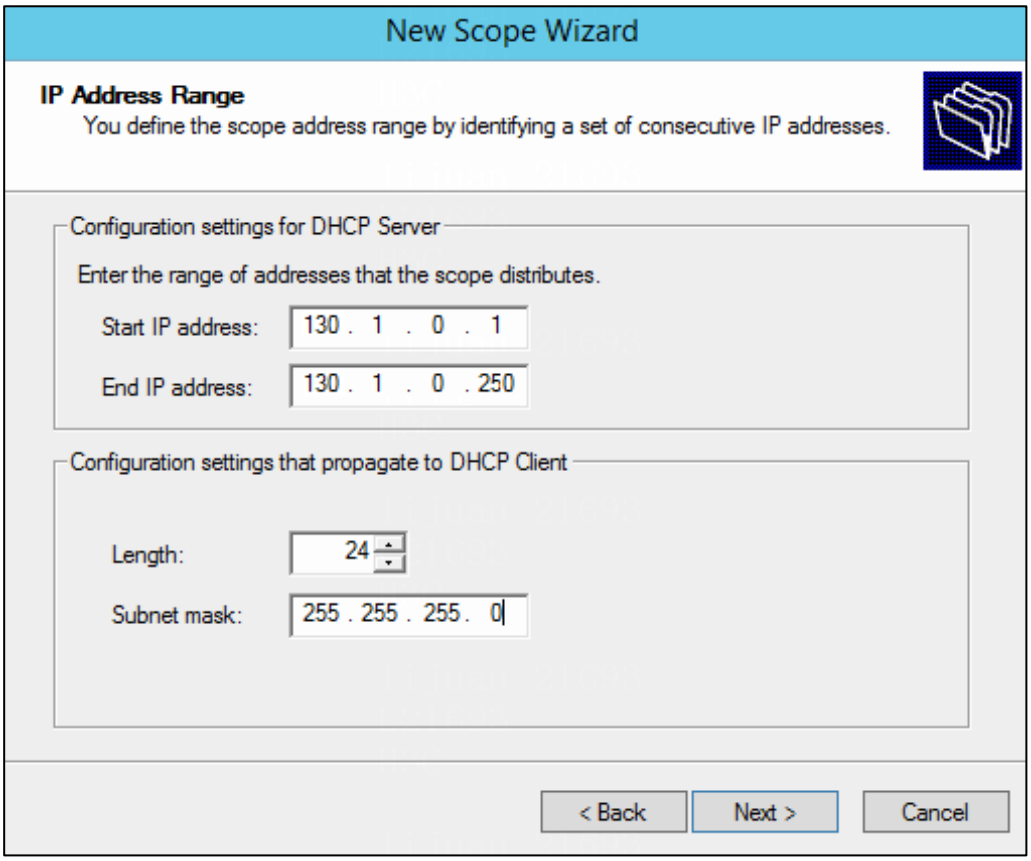
重要:

分離ドメインに複数のファブリックが存在する場合は、複数のファブリックに対して VXLAN 4094 のアドレスプールを設定する必要があります。

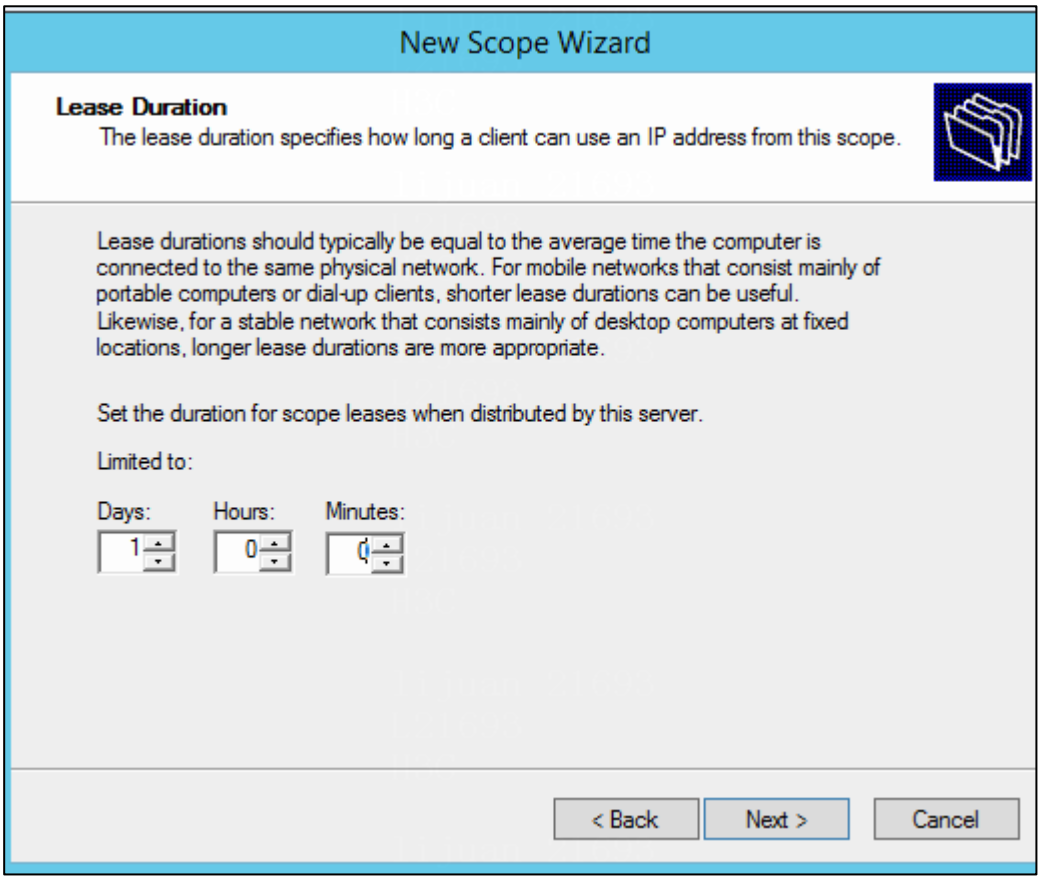
1. 右クリックして **New Scope** 選択し、**New Scope Wizard** ページを開きます。名前を入力します。



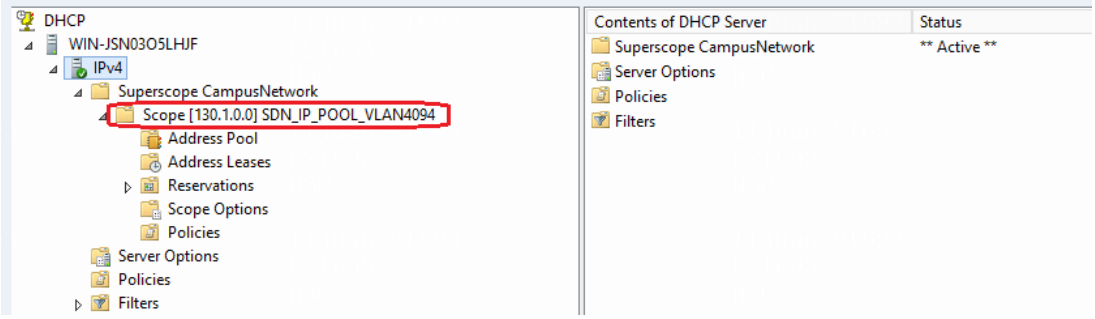
2. **Next** をクリックして、IP アドレス範囲ページを開きます。デバイス上の VXLAN 4094/VLAN 4094 の IP アドレス範囲と同じ IP アドレス範囲を入力します。



3. (オプション)**Next** をクリックして、除外する IP アドレス範囲を指定します。指定できるのはゲートウェイ IP のみです。**Add** をクリックしてリストに追加します。
4. **Next** をクリックします。リースを 1 日に設定します。

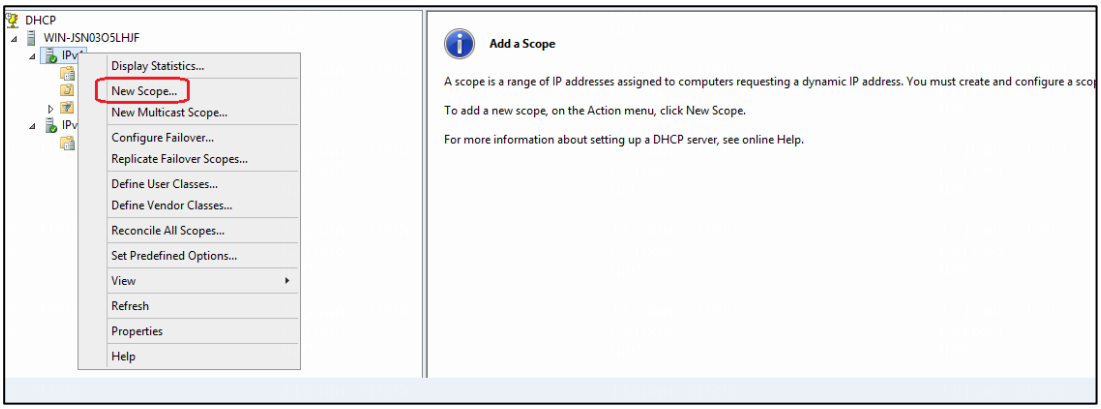


5. **Next** をクリックします。スコープのアクティブ化ページで、スコープをアクティブ化します。
6. **Next**、**Finish** の順にクリックして、設定を完了します。VLAN 4094 スコープは、次のように設定されます。

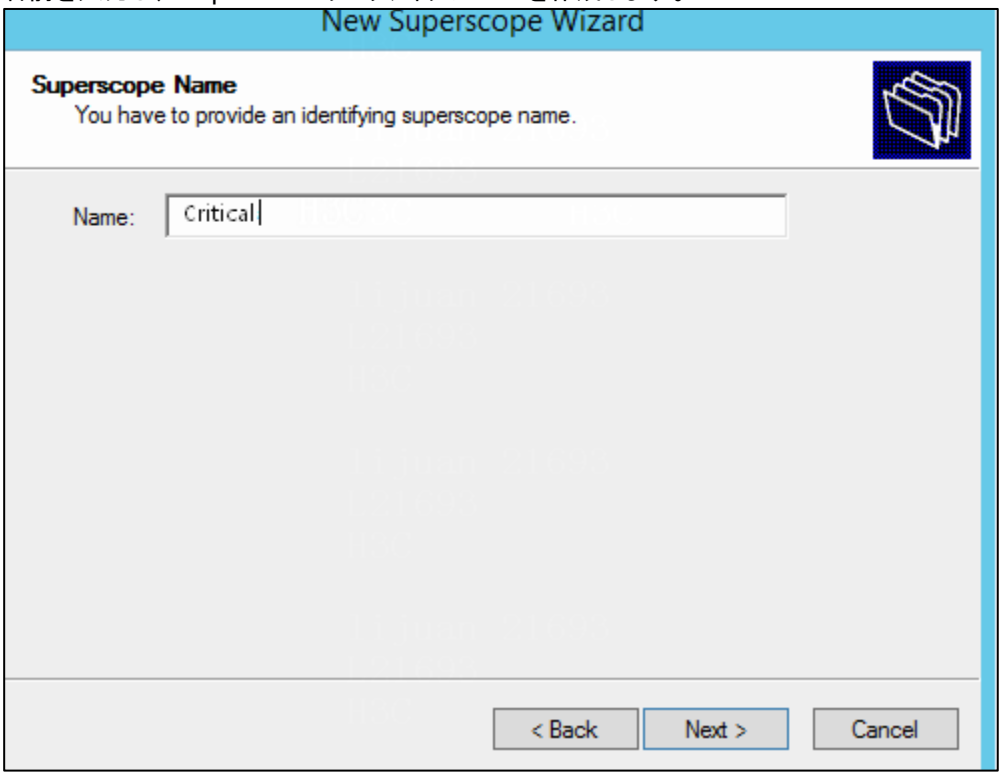


fail-permit セキュリティグループスコープを作成する

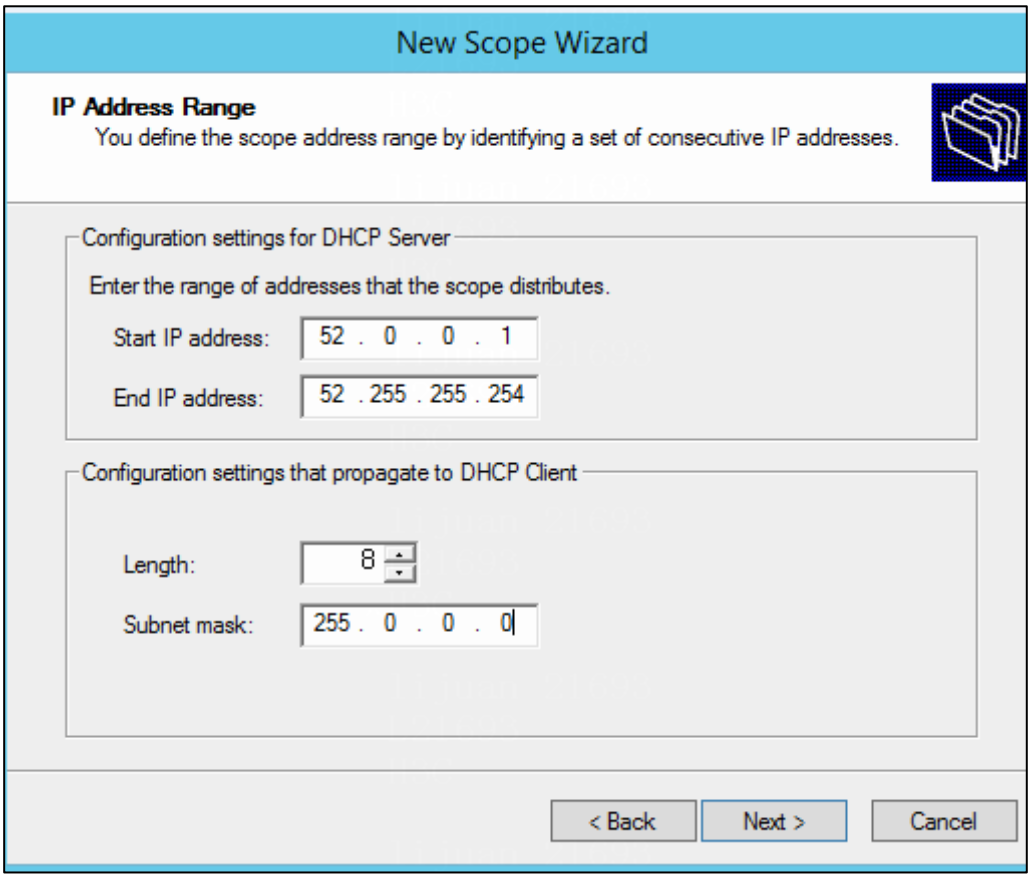
1. 右クリックし、**New Scope** を選択して、Microsoft DHCP サーバーの **New Scope Wizard** ページを開きます。



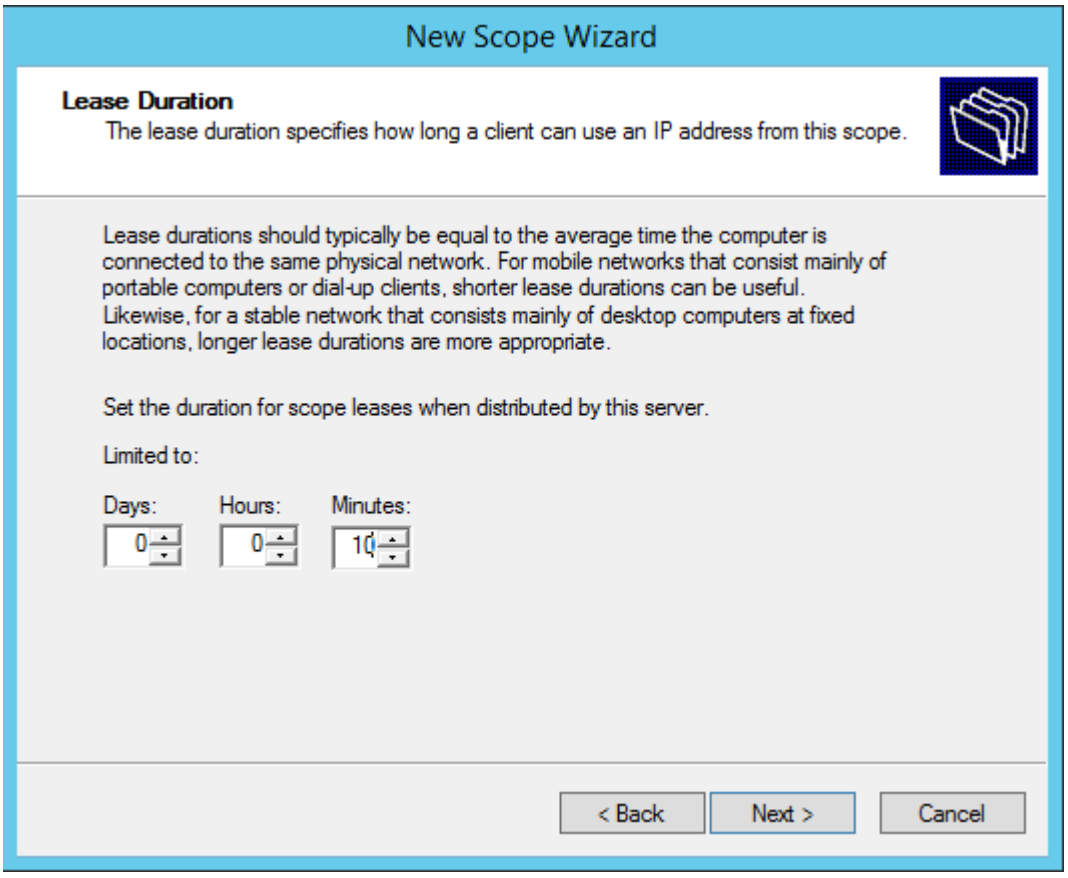
2. 名前を入力し、fail-permit セキュリティグループを作成します。



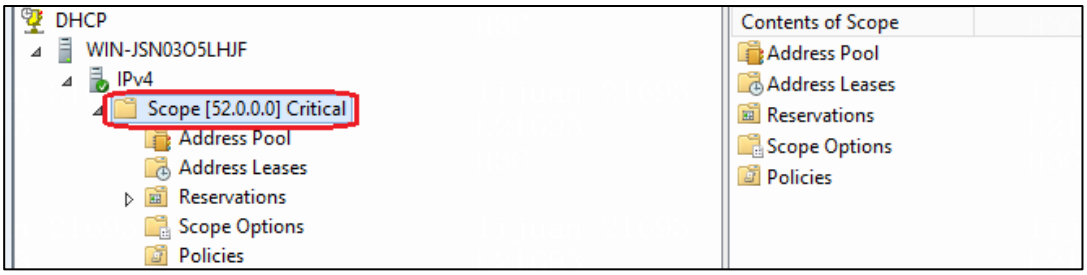
3. fail-permit レイヤ 2 ネットワークドメインを作成する **Add** をクリックして、IP アドレス範囲ページを開きます。『Create a fail-permit Layer 2 network domain』で設定したサブネットと同じ IP 範囲を入力します。



4. **Next** をクリックして、**Lease Duration** ページを開きます。fail-permit セキュリティグループの要件に従って、リースを 10 分に設定します。

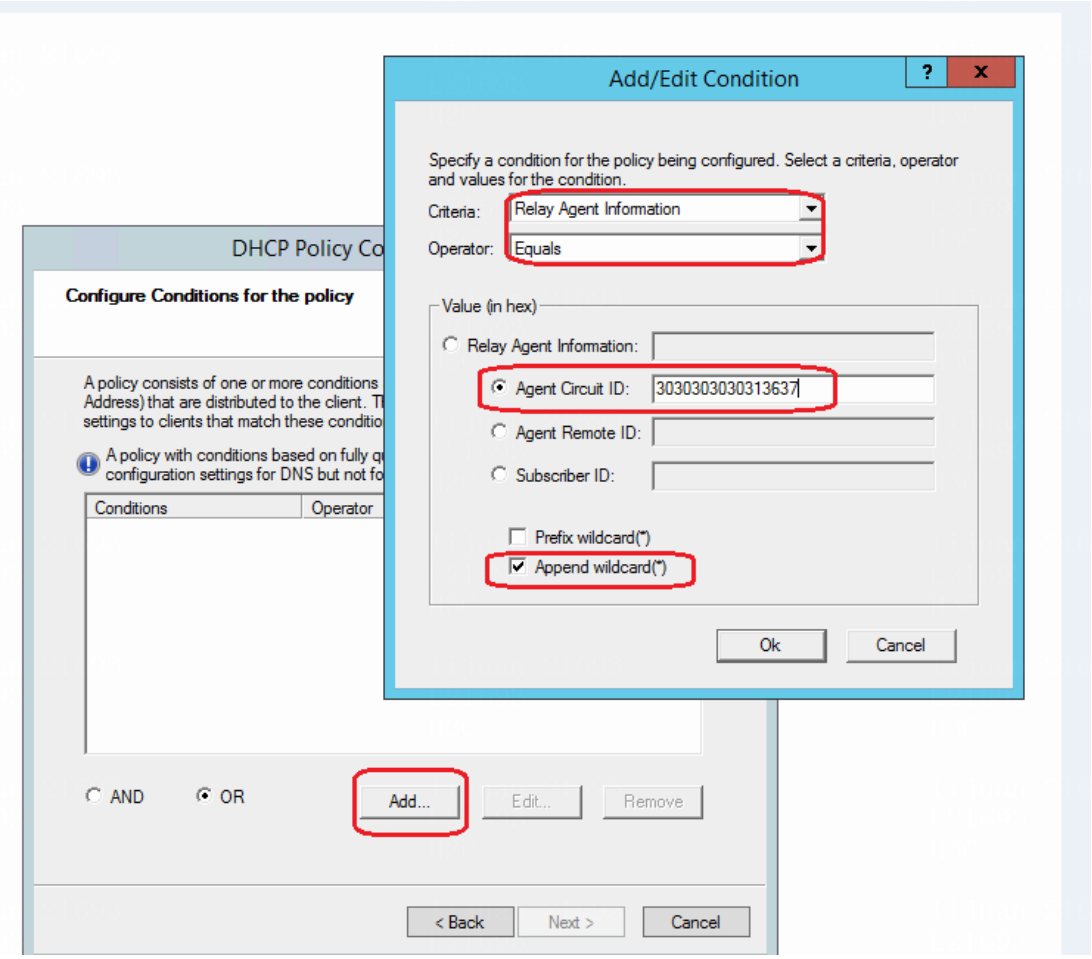


5. 設定が完了するまで、Next をクリックします。



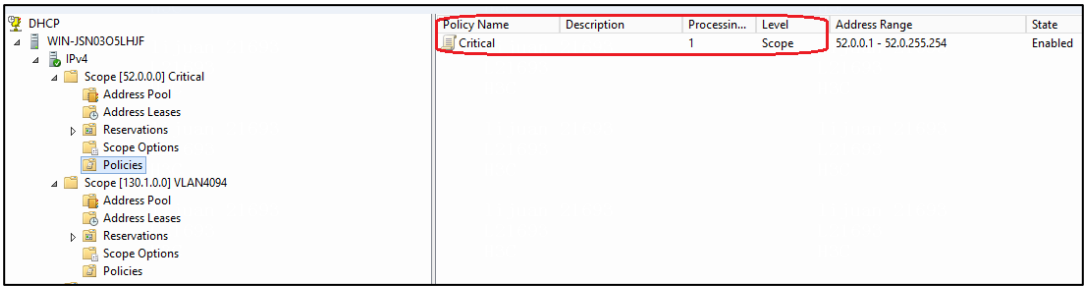
6. 次に、スコープのポリシーを構成します。その他の設定については、VLAN 4094 のスコープポリシー構成を参照してください(詳細は省略)。スコープを選択し、**Contents of Scope** 列の **Policies** を右クリックしてポリシーを追加します。ポリシー名を入力し、Next をクリックしてポリシー条件ページを開きます。

7. **Add** をクリックして、**Add/Edit Condition** ページを開き、ポリシー条件を設定します。**Criteria** で **Relay Agent Information** を選択し、**Operator** を **Equals** に設定します。エージェント回線 ID は ASCII コードで、30303030 で始まり、VXLAN ID 30313637 が続きます。これは、VXLAN ID が 167 であり、任意の値に一致するワイルドカード文字として*が続くことを示します。VXLAN ID は、失敗許可セキュリティグループの VXLAN ID です。



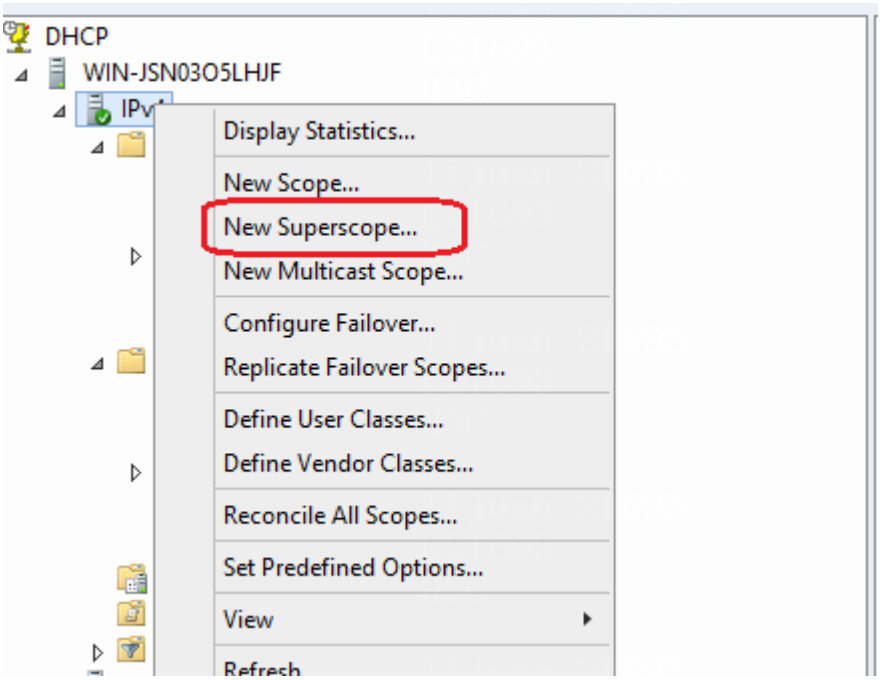
8. OK をクリックして構成を保存し、Next をクリックしてポリシー構成ページに入ります。ポリシーの IP アドレス範囲を構成しないことを選択します。

9. Next をクリックしてサマリーページを開きます。Finish をクリックして構成を完了します。結果を次の図に示します。

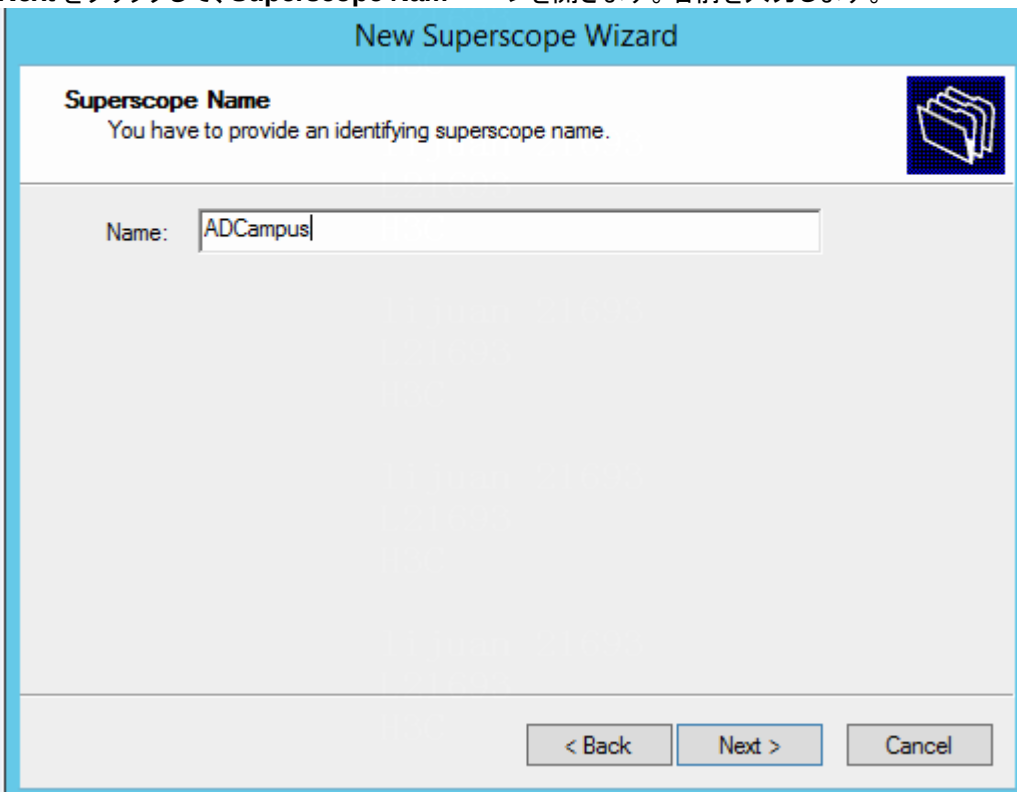


スーパースコープを作成する

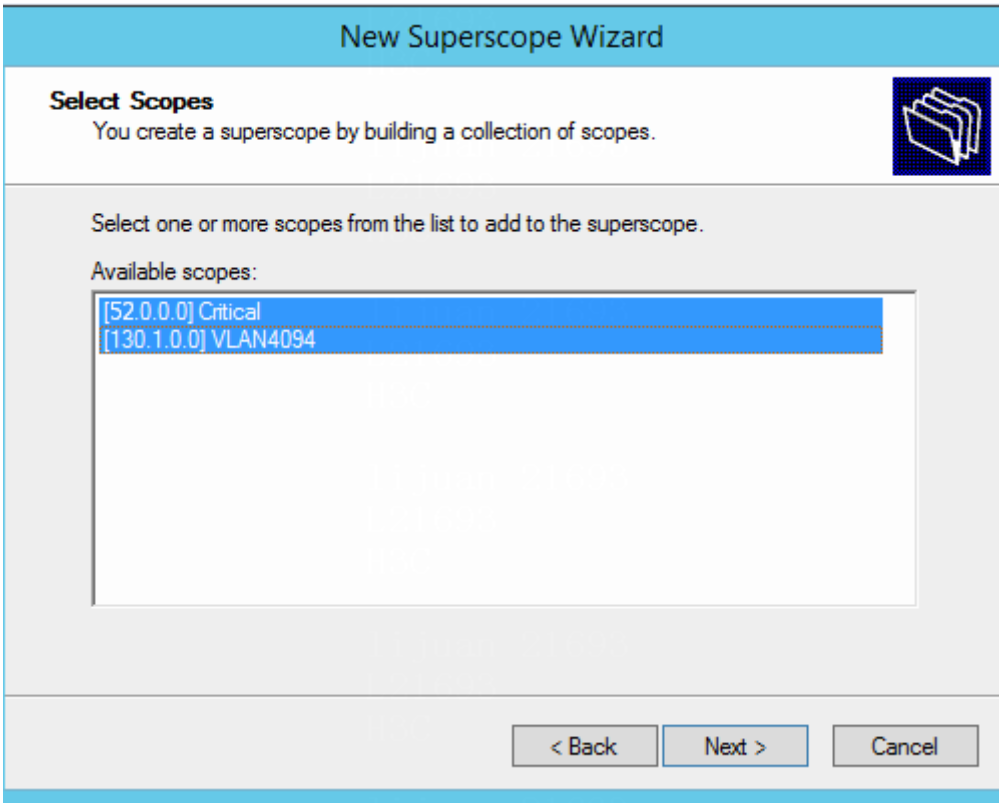
1. 右クリックして **New Superscope** を選択し、**New Superscope Wizard** ページを開きます。



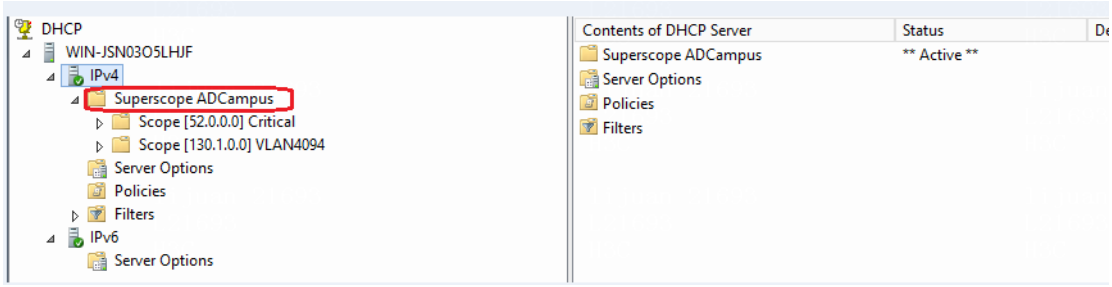
2. **Next** をクリックして、**Superscope Nam** ページを開きます。名前を入力します。



3. **Next** をクリックして、**Select Scopes** ページを開きます。以前に作成したクリティカルスコープと VLAN 4094 スコープを選択します。



4. **Next** をクリックして、スーパースコープの設定を完了します。スーパースコープには、以前に作成されたクリティカルスコープと VLAN 4094 スコープが含まれていることがわかります。



5. 設定後、すべての失敗許可プランの設定が完了します。EIA サーバーに障害が発生すると、ユーザーは自動的に失敗許可セキュリティグループに入り、オンラインになったときに失敗許可セキュリティグループの IP アドレスを取得します。

IT リソースグループ

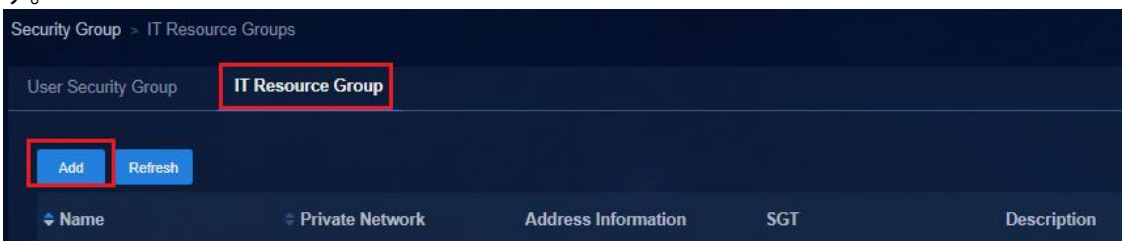
ITリソースグループを作成する

IT リソースグループは、ネットワークリソースへのユーザーアクセスを認証するために使用されます。IT リソースグループは、アクセスポリシーを展開することによって、サーバーリソースに対するセキュリティグループユーザーのアクセス許可を制御します。

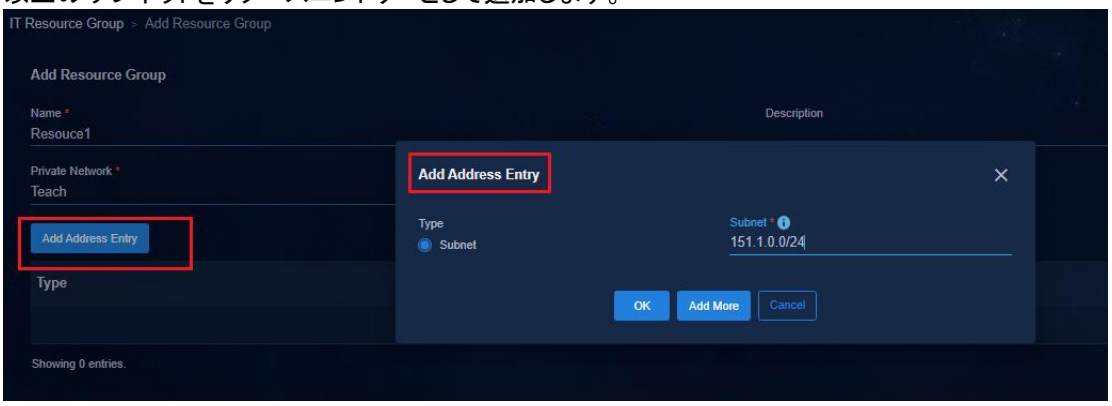
重要:

IT リソースグループ内の IP アドレスエントリーの数に制限はありません。1 つの IT リソースグループに追加する IP アドレスエントリーの数は、20 以下にすることをお勧めします。

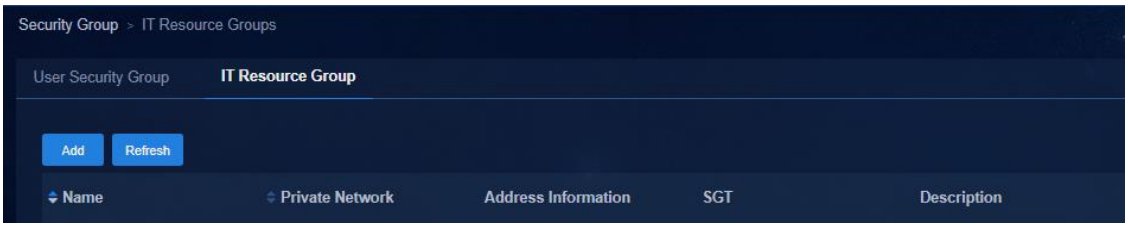
1. **Automation** > **Campus Network** > **Security Group** > **IT Resource Group** ページに移動します。



2. **Add** をクリックして、リソースグループを追加するためのページを開きます。名前を入力し、リソースグループが属するプライベートネットワークを選択します。**Add Address Entry** をクリックして、1 つ以上のサブネットをリソースエントリーとして追加します。



3. **OK** をクリックして、リソースグループを追加するページに戻ります。**OK** をクリックして構成を保存します。追加された IT リソースグループが、**IT Resource Group** ページに表示されます。マイクロセグメント ID は、IT リソースグループ内の各 IT リソースに割り当てられます。



- 4 つの IT リソースグループを作成し、次のように設定をデバイスに展開します。

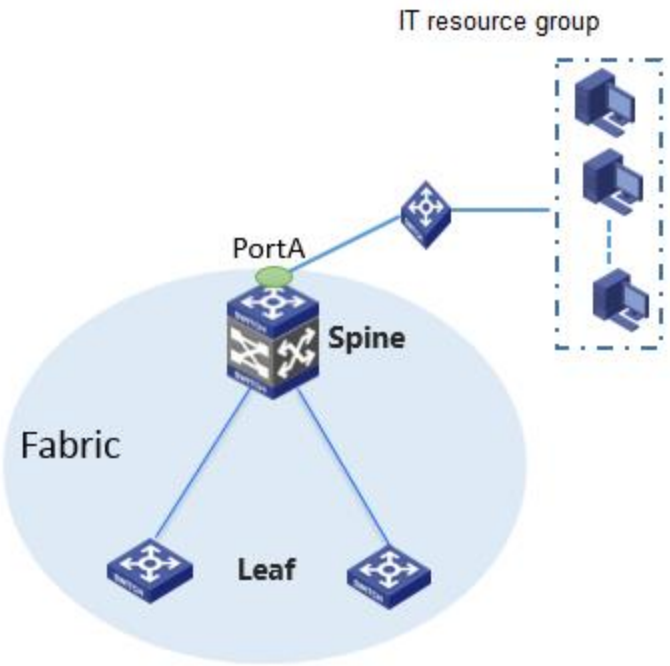
#リソースグループごとにマイクロセグメントを作成します。

```
microsegment 60001 name SDN_EPG_60001
 member ipv4 151.1.0.0 255.255.255.0 vpn-instance Teach
#
#
microsegment 60002 name SDN_EPG_60002
 member ipv4 151.2.0.0 255.255.255.0 vpn-instance Teach
#
#
microsegment 60003 name SDN_EPG_60004
 member ipv4 151.3.0.0 255.255.255.0 vpn-instance Teach
#
#
microsegment 60004 name SDN_EPG_60005
 member ipv4 151.4.0.0 255.255.255.0 vpn-instance Teach
#
#Deploy the supernet iterative static routes.
ip route-static vpn-instance Teach 151.1.0.0 24 151.1.0.0 preference 200 recursive-lookup description SDN_ROUTE
 ip route-static vpn-instance Teach 151.2.0.0 24 151.2.0.0 preference 200 recursive-lookup description SDN_ROUTE
 ip route-static vpn-instance Teach 151.3.0.0 24 151.3.0.0 preference 200 recursive-lookup description SDN_ROUTE
 ip route-static vpn-instance Teach 151.4.0.0 24 151.4.0.0 preference 200 recursive-lookup description SDN_ROUTE
#
```

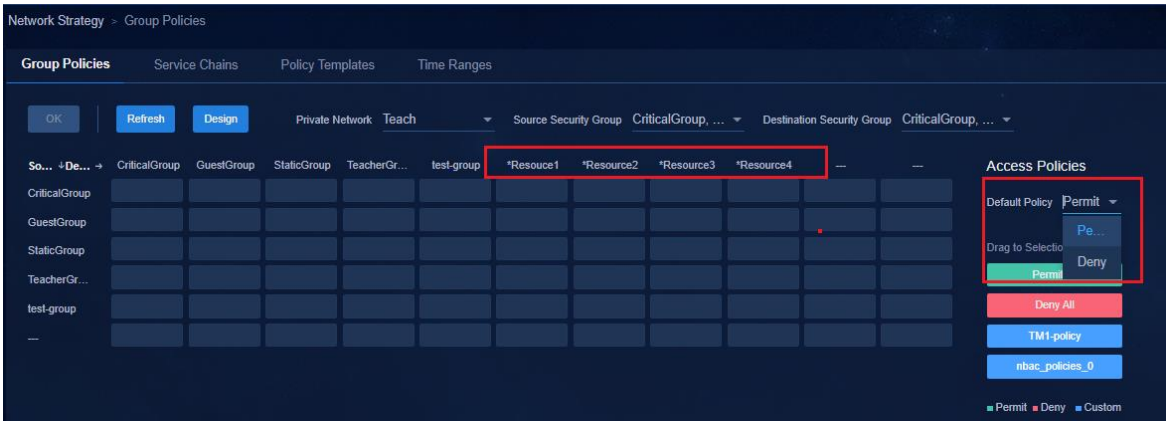
ITリソースグループのアクセス設定を構成する

IT リソースグループのサーバーは、リーフデバイスではなくスパインデバイスにマウントすることをお勧めします。これにより、特に次の図に示すように、ネットワーク内に複数のリーフデバイスが存在する場合に、不要なトラフィックを回避できます。

スパインデバイスは、物理インターフェイス PortA を使用して IT リソースグループに接続します。PortA は静的 AC ポートに設定されています。



Automation > **Campus Network** > **Network Strategy** > **Group Policies** ページに移動します。**Group Policies** タブで、グループ間ポリシーのプライベートネットワークの **Default Policy** 設定に対して **Permit** または **Deny** を選択できます。



- **Permit**: プライベートネットワーク内のすべてのユーザーが、IT リソースグループ内のリソースにアクセスできます。IT リソースグループへのユーザーアクセスには、グループ間ポリシーは必要ありません。ユーザーによる IT リソースグループへのアクセスを禁止するには、拒否モードのグループ間ポリシーを構成します。
- **Deny**: デフォルトでは、プライベートネットワークのユーザーは IT リソースグループ内のリソースにアクセスできません。ユーザーが IT リソースグループにアクセスできるようにするには、許可モードのグループ間ポリシーを構成します。ユーザーが IT リソースグループにアクセスできないようにするには、ポリシーを構成する必要はありません。

ベストプラクティスとしては、IT リソースグループ内のパブリックサーバーをスパインデバイス経由で接続

し、プライベートネットワークのデフォルトアクセスポリシー(Permit または Deny)に関係なく、vpn-default プライベートネットワークにサーバーを展開します。

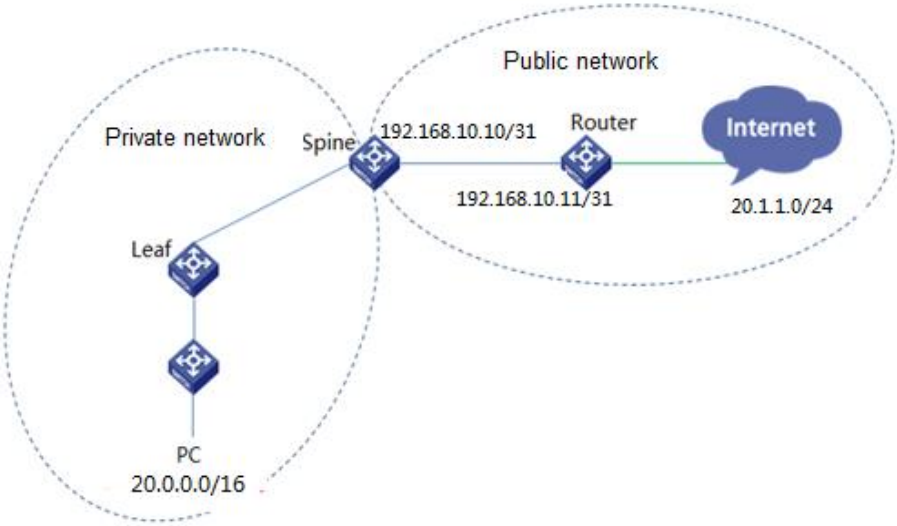
IT リソースグループが vpn-default プライベートネットワークに展開されている場合、セキュリティグループは、プライベートネットワークのデフォルトのアクセスポリシー(Permit または Deny)に関係なく、IT リソースグループにアクセスできます。プライベートネットワークから IT リソースグループへのアクセスを禁止するには、プライベートネットワークの IT リソースグループを指定し、IT リソースグループに拒否モードのグループ間ポリシーを展開します。

単一の境界デバイスを介した外部ルータへのアクセス

特定の VPN のオンラインユーザーが外部ネットワークと通信できるようにするには、外部ルートを再配布するように境界デバイスを設定します。現在のソフトウェアバージョンでは、境界デバイスとしてスパインまたは任意のリーフデバイスを指定できます。

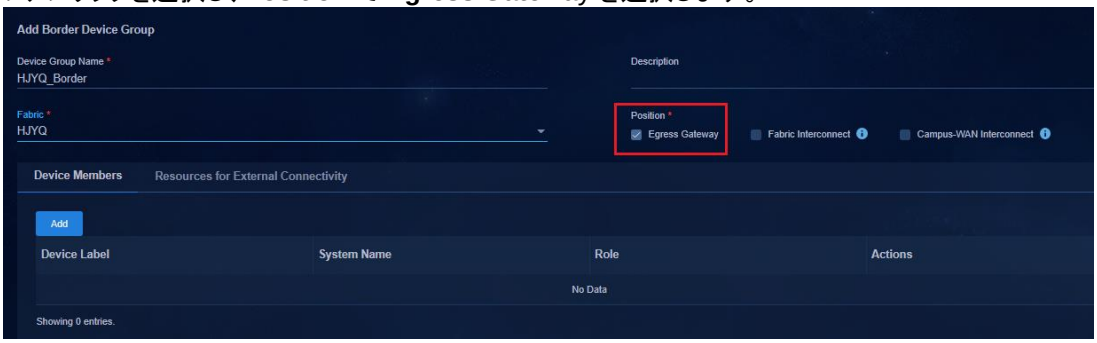
次の図では、境界デバイスとしてスパインデバイスを使用しています。

プライベートネットワークは、1 つまたは複数の VPN インスタンスを持つことができます。この例では、プライベートネットワーク内の PC(20.0.0.3)が外部ネットワーク(20.1.1.0/24)にアクセスできるようにするための、コントローラを介したルート設定および展開について説明します。

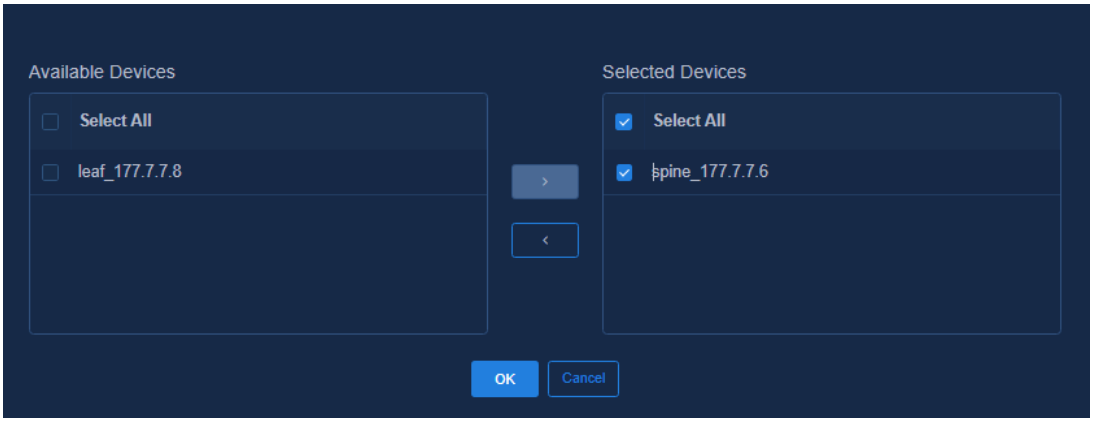


境界デバイスグループを作成する

1. **Automation** > **Campus Network** > **Devices** > **Border Device Groups** ページに移動します。
2. **Add** をクリックして、境界デバイスグループを追加します。
3. ファブリックを選択し、**Position** で **Egress Gateway** を選択します。

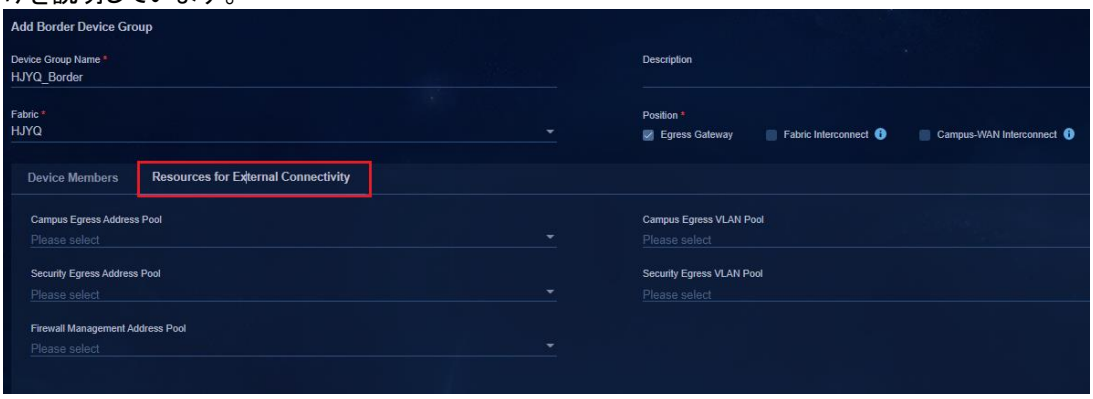


4. **Device Member** タブを選択し、**Add** をクリックします。境界デバイスグループメンバーとして、スパインデバイスまたはリーフデバイスを選択できます。例としてスパインデバイスを指定します。

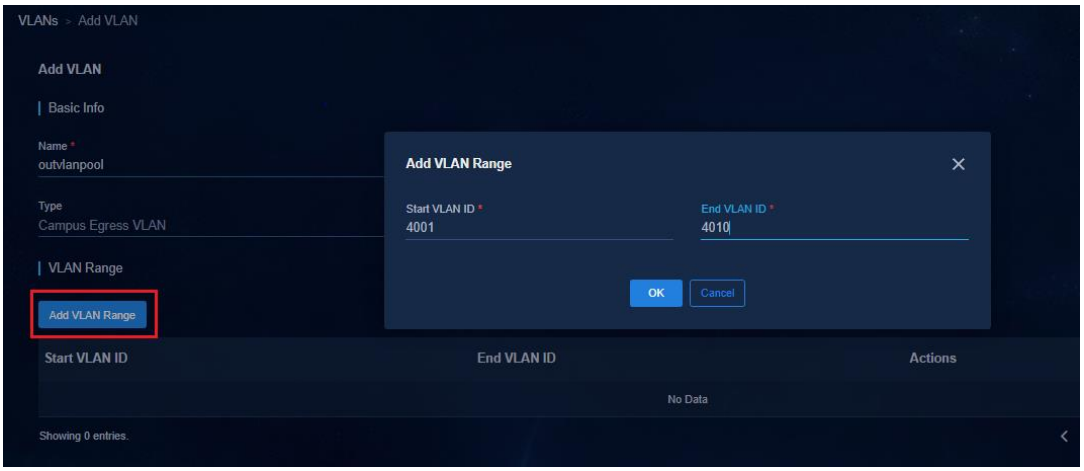


5. 出力ネットワークリソースを設定するには、**Resources for External Connectivity** タブをクリックします。ネットワークリソースの自動割り当てに使用されるアドレスプールと VLAN プールを指定できます。キャンパスが外部ネットワークと通信するときのリソース割り当て用に、**Campus Egress Address Pool** 設定と **Campus Egress VLAN Pool** 設定をペアで設定する必要があります。

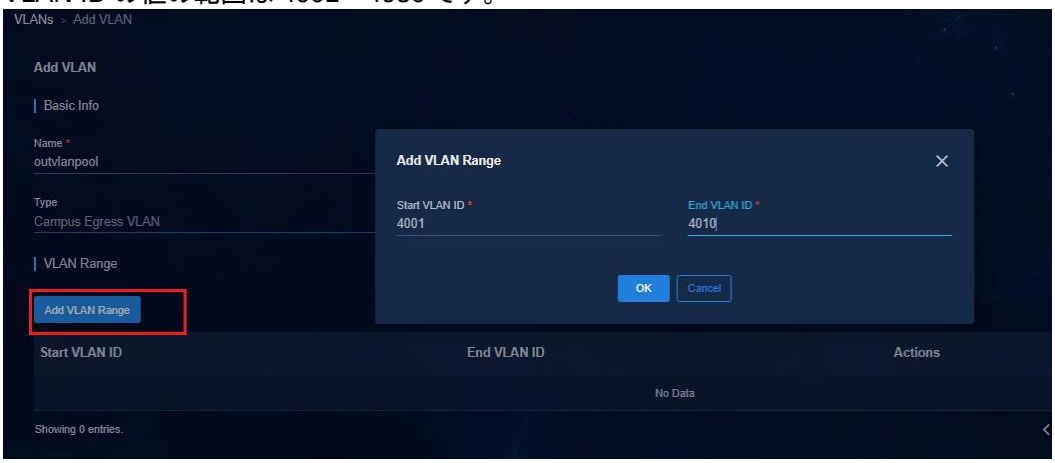
   これらの設定を行わない場合は、『Add an egress gateway』で出力ゲートウェイメンバーを追加するときに、**Egress Network Resource Allocation Mode** の **Manual Configuration** を選択する必要があります。**Security Egress Address Pool**, **Security Egress VLAN Pool**, 及び **Firewall Management Address Pool** の設定を使用して、ファイアウォールネットワークリソース割り当てを設定します。設定の詳細については、『AD-Campus 6.2 Security Convergence Configuration Guide』を参照してください。この例では、キャンパス出力ゲートウェイリソース設定だけを説明しています。



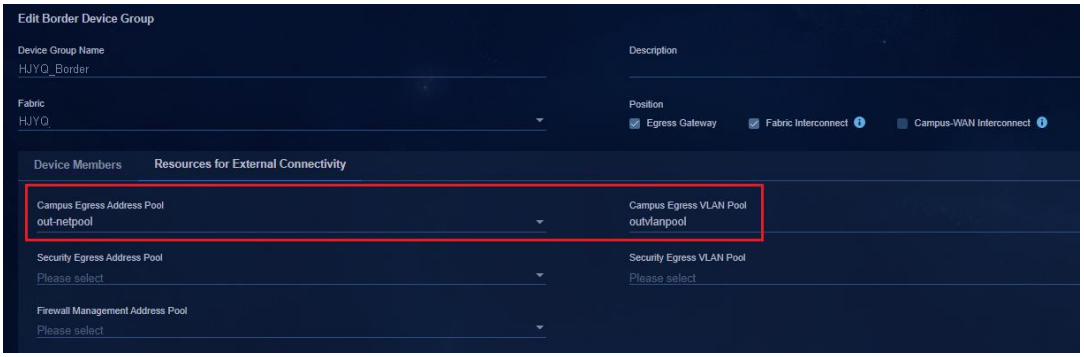
6. **Campus Egress Address Pool** をクリックして、既存のアドレスプールを選択するか、キャンパス出力アドレスプールを作成します。ローカルおよびリモート IP アドレスを出力ネットワークリソースに割り当てるためのキャンパス出力アドレスプールを作成します。IPv4 または IPv6 アドレスを指定できます。



7. 既存の VLAN プールを選択するか、**Campus Egress VLAN Poo** を作成するには、Campus Egress VLAN Pool をクリックします。ローカルネットワークとリモートネットワーク間の通信用の出力ネットワークリソースに VLAN を割り当てるために、キャンパス出力 VLAN プールを作成します。VLAN ID の値の範囲は 4001～4050 です。

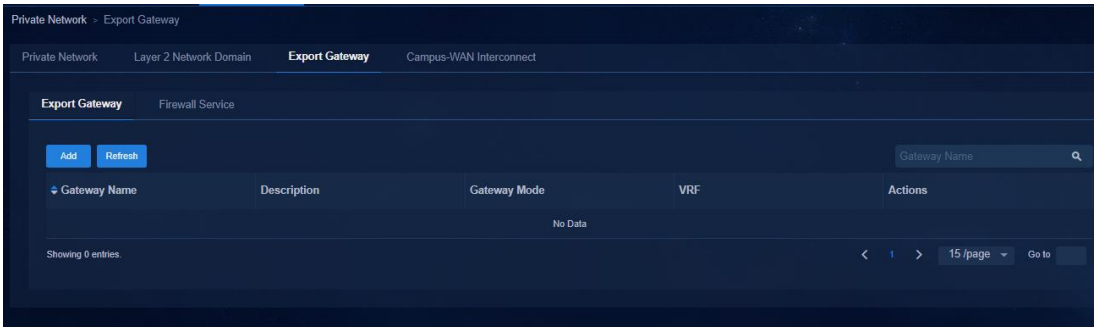


8. **OK** をクリックします。作成された境界デバイスグループは、境界デバイスグループリストに表示されます。

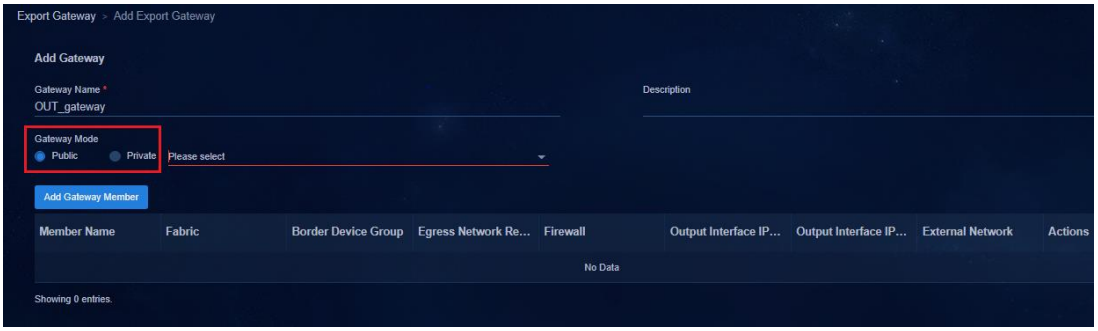


出力ゲートウェイを追加する

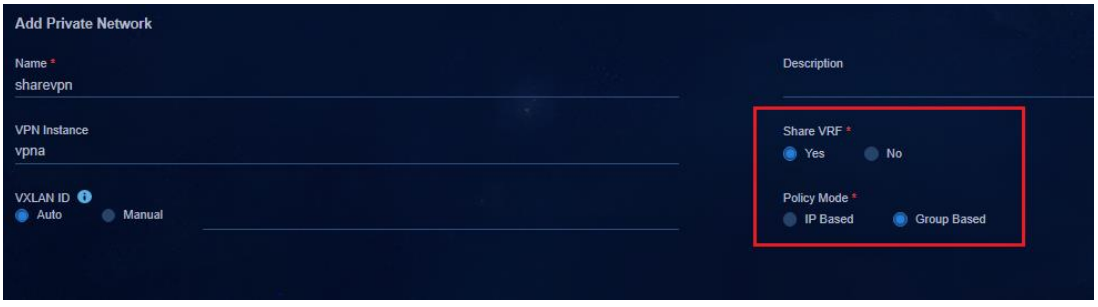
1. **Automation** > **Campus Network** > **Private Network** > **Export Gateway** ページに移動し、**Add** をクリックします。

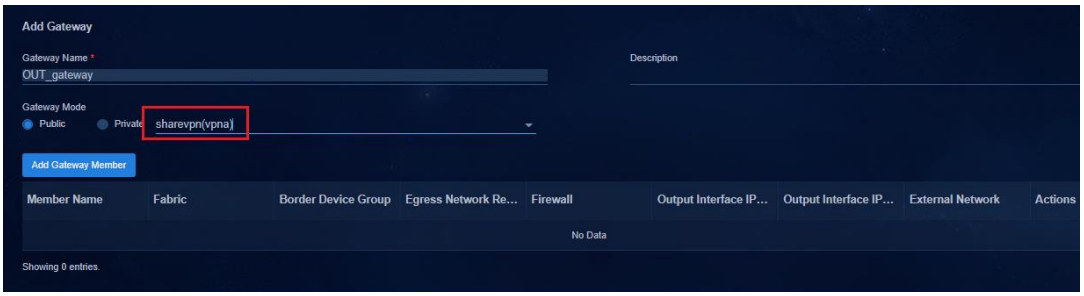


2. 必要に応じて、出力ゲートウェイモードを設定します。オプションは **Public** と **Private** です。
   - **Public**: パブリックゲートウェイは、複数のプライベートネットワークで使用できます。複数のプライベートネットワークは、出力ゲートウェイを共有します。
   - **Private**: プライベートゲートウェイは、1 つのプライベートネットワークでのみ使用でき、個別に作成する必要はありません。

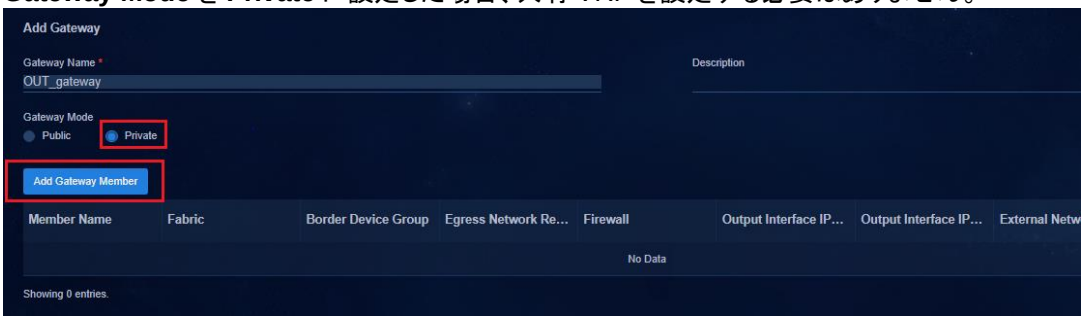


3. **Gateway Mode** を **Public** に設定する場合は、出力ゲートウェイにバインドされるプライベートネットワークとして、プライベートネットワーク内に VPN を作成する必要があります。
4. 共有 VRF を作成するには、**Automation** > **Campus Network** > **Private Network** > **Private** ページに移動します。**Share VRF** で **Yes** を選択します。

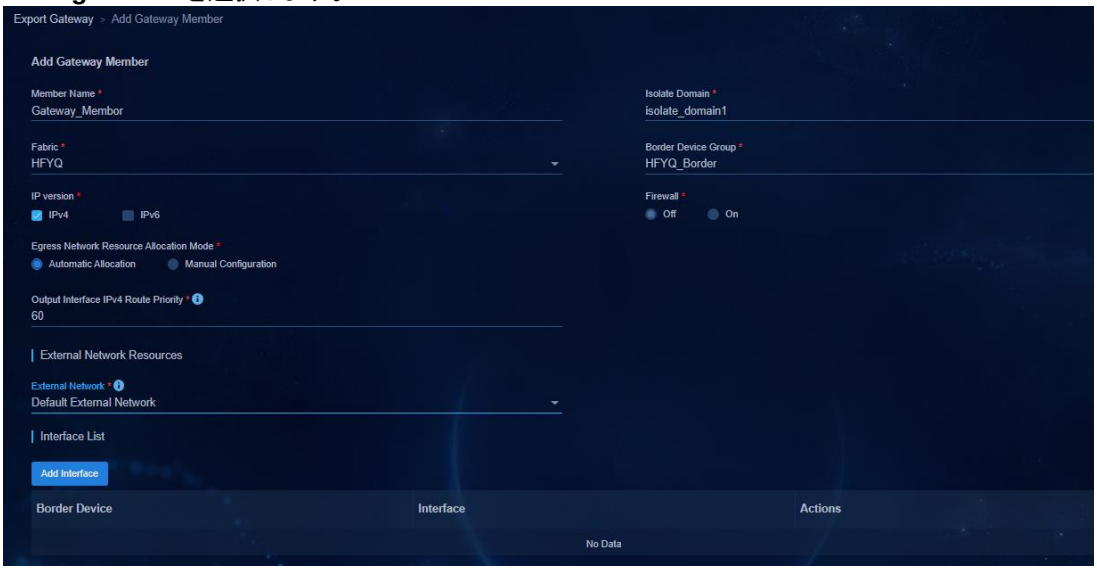




5. **Gateway Mode** を **Private** に設定した場合、共有 VRF を設定する必要はありません。



6. 以前に設定した境界デバイスグループをクリックします。**Automatic Allocation** または **Manual Configuration** を選択します。

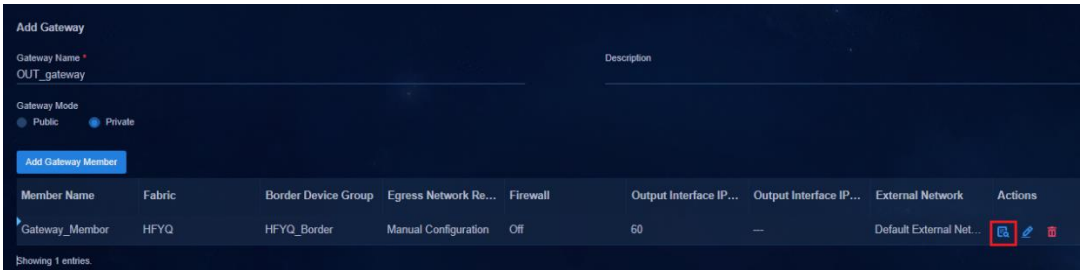


- **External Network Resource**: **Default External Network** または **Add IT Resource Group** を選択します。**Add IT Resource Group** オプションは、IT リソースへのアクセスの構成に使用されます。**Default External Network** オプションは、外部ネットワークへのアクセスの構成に使用されます。
- **Egress Network Resource Allocation Mode**: **Automatic Allocation** または **Manual Configuration** を選択します。
  - 0**Automatic Allocation** を選択すると、「Create a border device group」で設定されている

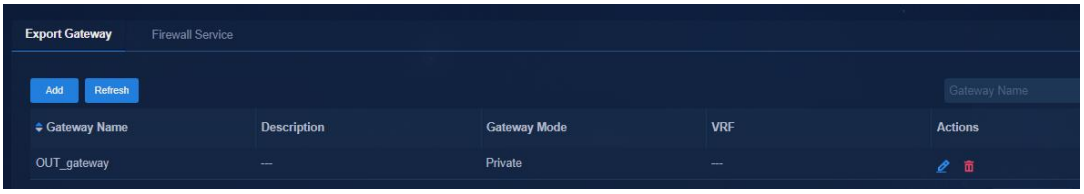
設定に従って、VLAN、出力ネットワークセグメント、およびリモートネットワークセグメントがボーダーデバイスに自動的に割り当てられます。

– **Manual Configuration** を選択した場合は、出力 VLAN、出力ネットワークセグメント、およびリモートネットワークセグメントを手動で設定する必要があります。リモートネットワークセグメントは、出力ネットワークセグメントと同じネットワークに存在する必要があります。

7. **OK** をクリックして **Add Gateway** ページに戻ります。ゲートウェイメンバーの **Actions** 列をクリックして、ボーダーデバイスと外部ネットワーク間の通信に関する VLAN およびネットワークセグメント情報を表示します。

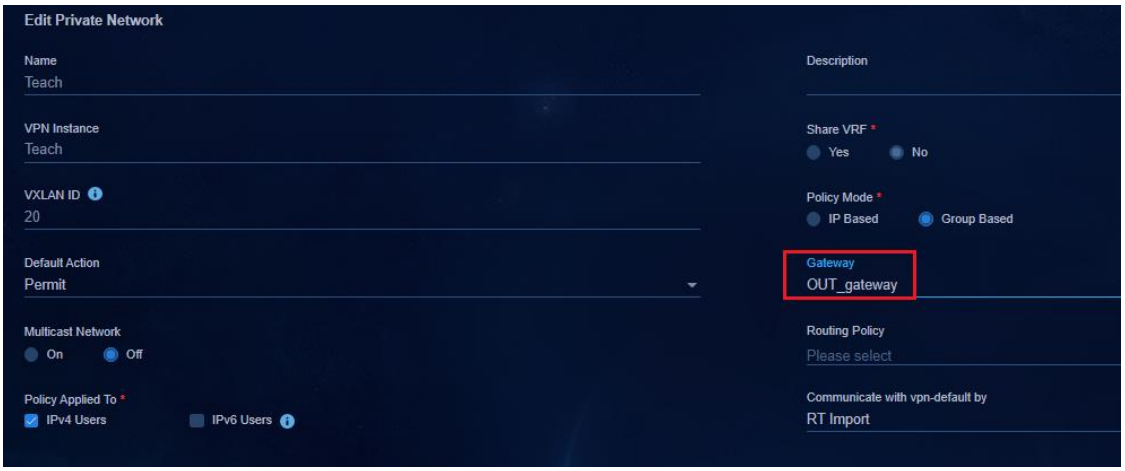


8. **OK** をクリックして、作成された出力ゲートウェイをゲートウェイリストに表示します。



出力ゲートウェイのプライベートネットワークへの関連付け

1. **Automation** > **Campus Network** > **Private Network** > **Private Network** ページに移動します。
2. プライベートネットワークの **Actions** カラム  をクリックします。
3. 開いたページで、外部通信に使用されるプライベートネットワークの出力ゲートウェイを設定します。



デバイスによって展開された出力ゲートウェイ設定

パブリックゲートウェイ

この例では、設定されている出力ゲートウェイはパブリックゲートウェイです。SeerEngine キャンパスコントローラは、デバイス上に VPN を作成します。ユーザーは、外部ネットワークと通信するための出力ゲートウェイインスタンスとして、新しく作成された VPN を使用します。

スパインデバイス上のコントローラによって展開された出力ゲートウェイ設定を表示できます。

- VLAN 設定を発行します。

```
#
Vlan 4001
#
```

- VPN インスタンスを作成します。

```
#
ip vpn-instance VPNa
 description SDN_VRF_fc248f21-f522-42b0-9882-cea78ee24a1dVPN1
 #
 address-family ipv4
  route-replicate from vpn-instance vpn1 protocol direct   //プライベートネットワークを複製する
 route of VPN 1.
  route-replicate from vpn-instance vpn1 protocol bgp 100
#
```

- VLAN インターフェイス設定を発行します。

```
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance VPNa     //共有ゲートウェイ VPNa をバインドする
ip address 192.168.10.10 255,255,255,254
#
```

- スタティックルートを BGP に再配布します。

```
#
bgp 100
#
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   default-route imported        //静的ルートを再配布します。
   preference 240 240 130
   import-route static
   network 20.0.0.0 255.255.0.0
   network 20.0.0.1 255.255.255.255
   network 30.0.0.0 255.255.0.0
   network 30.0.0.1 255.255.255.255
  #
  address-family ipv6 unicast
#
```

- デフォルトのスタティックルートを発行します。

```
#
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.10.11 description SDN_ROUTE
#
```

プライベートゲートウェイ

スパインデバイス上のコントローラによって展開された出力ゲートウェイ設定を表示できます。

- VLAN 設定を発行します。

```
#
Vlan 4001
#
```

- VLAN インターフェイス設定を発行します。

```
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance vpn1       // VPN インスタンス vpn1 をバインドする
 ip address 192.168.10.10 255,255,255,254
 ip policy-based-route SDN_SC_VLAN_4001   // PBR ポリシーを適用する.
#
policy-based-route SDN_SC_VLAN_4001 permit node 65535
 if-match acl name SDN_ACL_SC_PERMIT_ALL
#
#
acl acl advanced name SDN_ACL_SC_PERMIT_ALL
 description SDN_ACL_SC_PERMIT_ALL
 rule 0 permit ip
#
```

- 外部ネットワークへのデフォルトルートを設定します。

  #
  ip route-static vpn-instance vpn1 0.0.0.0 0 192.168.10.11 description SDN_ROUTE
  #

境界デバイスを外部ネットワークに接続するインターフェイスを設定します。

#出力ゲートウェイメンバーにインターフェイスが指定されていない場合は、インターフェイスを手動で設定する必要があります。インターフェイスが指定されている場合は、コントローラによってインターフェイスが自動的に展開されるため、手動で設定する必要はありません。

```
interface Ten-GigabitEthernet1/5/0/32
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 4001
#
```

境界デバイスに接続されたL3デバイスを設定します。

```
#
vlan 4001       // Egress ゲートウェイの VLAN の詳細
#
#
interface Ten-GigabitEthernet1/0/9
port link-type trunk
port trunk permit vlan 4001
#
#境界デバイスと通信するための IP アドレスを設定します。// 出力ゲートウェイ詳細のリモート IPv4 アドレス。
interface Vlan-interface 4001
ip address 192.168.10.11 255.255.0.0
#
パブリックネットワークへのデフォルトルートを設定します。ネクストホップは、外部ネットワークのゲートウェイアドレスです。
ip route-static 0.0.0.0 0 20.1.1.1
#
#パブリックネットワークからプライベートネットワークへのルートの場合、パブリックネットワークと通信する各ネットワークセグメントを設定する必要があります。ネクストホップは境界デバイスです。
#
ip route-static 20.0.0.0 16 192.168.10.10
ip route-static 30.0.0.0 16 192.168.10.10
#
```

2つの境界デバイスを介した外部ルートデバイスへのアクセス

現在のソフトウェアバージョンでは、コントローラは2つの境界出力設定をサポートしていません。次のように、2つの境界出力を手動で設定する必要があります。

境界1を設定

- パブリック出力用の VPN インスタンスを作成します。

```
#
ip vpn-instance VPNa
 description SDN_VRF_GW
 #
 address-family ipv4
  route-replicate from vpn-instance vpn1 protocol direct   // VPN ルートをレプリケートします。 複数のプライベート ネットワークが存在する場合、プライベート ネットワークのルート レプリケーションを構成する必要があります。
  route-replicate from vpn-instance vpn1 protocol bgp 100
#
```

- VLAN インターフェイスを作成します。

```
# VLAN 4001 は、境界デバイスと外部ネットワーク出力の間の接続に使用されます。
Vlan 4001
#
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance VPNa     //パブリックゲートウェイ VPNa をバインドする
 ip address 192.168.10.10 255,255,255,250
#
```

- L3 デバイスに接続された境界デバイスのインターフェイスで、許可 VLAN を設定します。

```
#
interface Ten-GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 4001
#
```

- デフォルトルートを BGP に再配布します。

```
#
bgp 100
#
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   default-route imported        //デフォルトルートを再配布する
   preference 240 240 130
```

```
  import-route static                  //静的ルートを再配布します。
  network 20.0.0.0 255.255.0.0
  network 20.0.0.1 255.255.255.255
  network 30.0.0.0 255.255.0.0
  network 30.0.0.1 255.255.255.255
 #
 address-family ipv6 unicast
#
```

- 境界デバイス間の接続用に VLAN インターフェイス 4002 を設定します。

```
#
interface Vlan-interface4002
 description to_border2_Interface_4002
 ip binding vpn-instance VPNa     // パブリックゲートウェイ VPNa をバインドする
 ip address 192.168.10.12 255,255,255,250
#
```

- 境界デバイスに接続するインターフェイス上で、許可 VLAN 4002 を設定します。

```
#
interface Ten-GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 4002
#
```

- NQA と Track を設定します。

```
#NQA を境界デバイスのアップリンクに関連付けます。
nqa entry admin border1   //ローカル ユーザーと同じ管理者ユーザー名を指定します.
type icmp-echo
destination ip 192.168.10.11   /   /宛先 IP アドレスは、レイヤー 3 VLAN インターフェイス 4001 の IP アドレスです。
frequency 100
reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna   // VLAN インターフェイス 4001 にバインドされた VPN.
#
#NQA を有効にします。
nqa schedule admin border1 start-time now lifetime forever
#
#NQA を境界デバイスのリンクに関連付けます
nqa entry admin border2   //   ローカル ユーザーと同じ管理者ユーザー名を指定します
type icmp-echo
destination ip 192.168.11.11   //   宛先 IP アドレスは、レイヤー 3 VLAN インターフェイス 4002 の IP アドレスです。
frequency 100
reaction 2 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna   //   VLAN インターフェイス 4002 にバインドされた VPN
#
#NQA を有効にします。
nqa schedule admin border2 start-time now lifetime forever
#
# トラックと NQA の関連付けを設定します。
```

```
Track 1 nqa entry admin border1 reaction 1
#
#
Track 2 nqa entry admin spine1 reaction 2
#
```

- スタティックルートを設定します。

```
# VPN 1 からパブリックネットワークへのスタティックルートを設定し、スタティックルートをトラックエントリに関連付けます。
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.10.11 track 1
#
# 境界 2 をネクストホップとして、VPN 1 からパブリックネットワークへのバックアップスタティックルートを設定します。
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.11.11 track 2 preference 61
#
# 境界 2 から境界 1 へのパケットをパブリックネットワークに転送します。
ip route-static vpn-instance vpna 0.0.0.0 0 192.168.10.11
#
```

境界2を設定

- VPN インスタンスを作成します。

```
#
ip vpn-instance VPNa
 description SDN_VRF_GW
 #
 address-family ipv4
  route-replicate from vpn-instance vpn1 protocol direct   //   vpn1 のプライベートルートを複製します。
  route-replicate from vpn-instance vpn1 protocol bgp 100
#
```

- VLAN インターフェイスを作成します。

```
#
Vlan 4002
#
#
interface Vlan-interface4002
 description SDN_VLAN_Interface_4002
 ip binding vpn-instance VPNa     //  パブリックゲートウェイ VPNa をバインドします。
 ip address 192.168.11.10 255,255,255,250
#
```

- L3 デバイスに接続された境界デバイスのインターフェイスで、許可 VLAN を設定します。

```
#
interface Ten-GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 4002
#
```

- デフォルトルートを BGP に再配布します。

```
#
bgp 100
#
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   default-route imported        //デフォルトルートを再配布する
   preference 240 240 130
   import-route static          //静的ルートを再配布する
   network 20.0.0.0 255.255.0.0
   network 20.0.0.1 255.255.255.255
   network 30.0.0.0 255.255.0.0
   network 30.0.0.1 255.255.255.255
  #
  address-family ipv6 unicast
#
```

- 境界デバイスを接続する VLAN インターフェイス 4001 を設定します。

```
#
interface Vlan-interface4001
 description to_border1_Interface_4001
 ip binding vpn-instance VPNa     //  パブリックゲートウェイ VPNa をバインドします。
 ip address 192.168.10.12 255,255,255,250
#
```

- 境界デバイスを接続するインターフェイス上で、許可 VLAN 3 を設定します。

```
#
interface Ten-GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 4001
#
```

- NQA と Track を設定します。

```
# NQA を境界デバイスのアップリンクに関連付けます。
nqa entry admin border2   //  ローカルユーザーと同じ admin ユーザー名を指定します
type icmp-echo
destination ip 192.168.11.11   //  宛先 IP アドレスは、レイヤー3 VLAN インターフェイス 4002 の IP アドレスです。
frequency 100
reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna   //  VLAN インターフェイス 4002 にバインドされた VPN.
#


# nqa を有効にします。
nqa schedule admin border2 start-time now lifetime forever
#
# nqa を設定し、境界デバイスのリンクを接続します。
nqa entry admin border1   //  ローカル ユーザーと同じ管理者ユーザー名を指定します
type icmp-echo
destination ip 192.168.10.11   //  宛先 IP アドレスは、レイヤー 3 VLAN インターフェイス 4001 の IP アドレスです。
```

frequency 100
reaction 2 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna // VLAN インターフェイス 4001 にバインドされた VPN
#
#NQA を有効にします。
nqa schedule admin border1 start-time now lifetime forever
#
トラックと NQA の関連付けを設定します。
Track 1 nqa entry admin border2 reaction 1
#
Track 2 nqa entry admin border1 reaction 2
#

- スタティックルートを設定します。

VPN 1 からパブリックネットワークへのスタティックルートを設定し、スタティックルートをトラックエントリに関連付けます。
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.11.11 track 1
#
境界 2 をネクストホップとして、VPN 1 からパブリックネットワークへのバックアップスタティックルートを設定します。
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.10.11 track 2 preference 61
#
境界 1 から境界 2 へのパケットをパブリックネットワークに転送します。
ip route-static vpn-instance vpna 0.0.0.0 0 192.168.11.11
#

境界デバイスに接続されたL3デバイスを設定します。

- VLAN インターフェイスを作成します。

#
Vlan 4001
#
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip address 192.168.10.11 255,255,255,254
#
#
Vlan 4002
#
#
interface Vlan-interface4002
 ip address 192.168.11.11 255,255,255,254
#

- 境界 1 に接続されたインターフェイスで許可 VLAN を設定します。

#

interface Ten-GigabitEthernet2/0/1

port link-type trunk

port trunk permit vlan 4001

#

- 境界 2 に接続されたインターフェイスで、許可 VLAN を設定します。

  #

  interface Ten-GigabitEthernet2/0/2

  port link-type trunk

  port trunk permit vlan 4002

  #

- スタティックルートを設定します。

  #ネクストホップとしてパブリックネットワークゲートウェイを使用して、L3 デバイスからパブリックネットワークへのスタティックルートを設定します。

  ip route-static 0.0.0.0 0 21.1.0.1

  #

  #パブリックネットワークと通信するすべてのネットワークセグメントに対して、パブリックネットワークからプライベートネットワークへのスタティックルートを設定します。ネクストホップは境界 1 と境界 2 です。

  #

  ip route-static 20.0.0.0 16 192.168.10.10

  #

  ip route-static 20.0.0.0 16 192.168.11.10

  #

  ip route-static 30.0.0.0 16 192.168.10.10

  #

  ip route-static 30.0.0.0 16 192.168.11.10

  #

2 層ネットワーク構成の制約事項およびガイドライン

シングルリーフ ネットワーク

シングルリーフネットワークでは、ネットワーク内にリーフデバイスが 1 つだけ存在します。すべてのエンドポイントは、アクセススイッチを介してこのリーフに接続されます。SeerEngine キャンパスや DHCP サーバーなどのサーバーも、このリーフに直接接続されます。このリーフデバイスをリーフデバイスグループに追加する必要があります。リーフ構成は、従来のリーフ構成とは異なります。このセクションでは、構成の違いについてのみ説明します。その他の構成については、標準ネットワーキングの前のセクションを参照してください。

- 設定 1: リーフデバイスは DHCP スヌーピングでイネーブルになっているため(スパインデバイスは DHCP スヌーピングでイネーブルになっていません)、DHCP サーバーに接続されたサービスインスタンスに DHCP スヌーピングの信頼できるポートを追加する必要があります。

```
#
interface Ten-GigabitEthernet2/2/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4094
 service-instance 4094
     encapsulation s-vid 4094
     xconnect vsi vxlan4094
     dhcp snooping trust
#
```

- 設定 2: ネットワークにはリーフが 1 つしか存在しないため、BGP ピアを確立する必要はありません。カスタムプライベートネットワークが存在する場合は、次のように VPN 間ルート再配布を設定する必要があります。
  - 方法 1:

```
#
bgp 100
  non-stop-routing
address-family l2vpn evpn
#
ip vpn-instance vpn-default
   #
   address-family ipv4 unicast
   import-route static
   import-route direct
   #
#
```

```
ip vpn-instance Teach
  #
  address-family ipv4 unicast
  import-route static
  import-route direct
  #
#
```

- 方法 2:

```
#
ip vpn-instance vpn-default
 route-distinguisher 1:1
 vpn-target 1:1 1:4 import-extcommunity
 vpn-target 1:1 export-extcommunity
 #
 address-family ipv4
  route-replicate from vpn-instance vpn1 protocol direct   //   vpn1 インスタンスの直接ルートを vpn-default インスタンスにインポートします。複数の VPN が存在する場合は、この操作を複数回実行します。
 #
 address-family evpn
  vpn-target 1:1 1:4 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
ip vpn-instance Teach
 route-distinguisher 1:4
 vpn-target 1:1 1:4 import-extcommunity
 vpn-target 1:4 export-extcommunity
 #
 address-family ipv4
  route-replicate from vpn-instance vpn-default protocol direct
//    vpn-default の直接ルートだけをインポートします。他の VPN との通信についても同様の設定を実行します。
 #
 address-family evpn
  vpn-target 1:1 1:4 import-extcommunity
  vpn-target 1:4 export-extcommunity
#
```

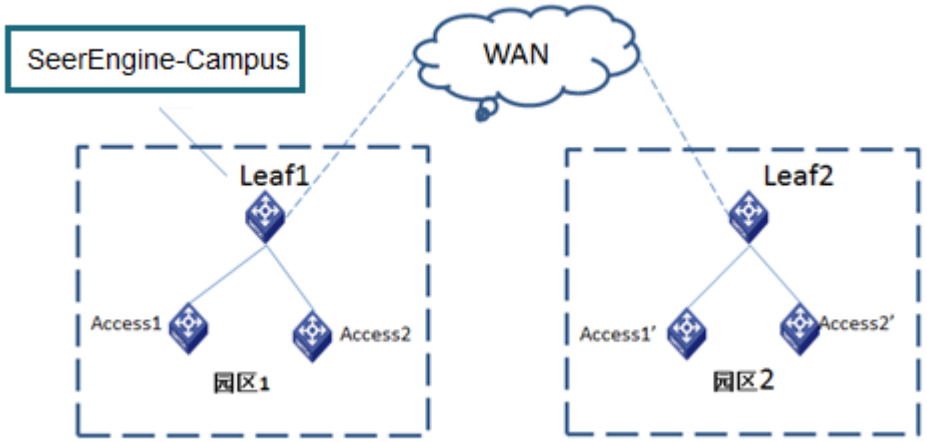
- 設定 3: リーフで、次の STP 設定を行います。

```
#
stp ignored vlan 2 to 4094
stp global enable
stp root primary
#
# リーフダウンリンクインターフェイスで、stp tc-restriction コマンドを設定します。
stp tc-restriction
#
```

マルチリーフ ネットワーキング

マルチリーフネットワーキングは、クロスキャンパスネットワークに適用されます。サーバー(SeerEngine キャンパスなど)に接続されたコアデバイス(ルートリフレクタ)もリーフデバイスグループに追加する必要があり、他のリーフデバイスと同じ設定であることを確認します。

この特殊なネットワークが正しく動作するようにするには、の説明に従って設定を追加する必要があります。その他の設定については、標準のネットワーク構成を参照してください。




```
#
interface Vsi-interface4094
 ip binding vpn-instance vpn-default
 ip address 130.0.3.1 255.255.255.0
 local-proxy-arp enable        // ARP プロキシを設定する
#
```

- 追加設定 1: リーフデバイスでは DHCP スヌーピングがイネーブルになっているため(スパインデバイスではこの機能がイネーブルになっていません)、DHCP サーバーに接続されたサービスインスタンスに DHCP スヌーピングの信頼できるポートを追加する必要があります。

  ```
  #
  interface Ten-GigabitEthernet2/2/0/5
   port link-mode bridge
   port link-type trunk
   port trunk permit vlan 1 4094
   service-instance 4094
       encapsulation s-vid 4094
       xconnect vsi vxlan4094
       dhcp snooping trust
  #
  ```

- 追加設定 2: サーバーに接続されたコアデバイス上のエンドポイント(カスタム VPN 内)は、vpn-default または外部ネットワーク内のサーバーとの通信を必要とします。サーバーに接続されたコア

デバイスの BGP VPN インスタンスに直接ルートをインポートする必要があります。

```
#
bgp 100
#
 ip vpn-instance vpn-default
  #
  address-family ipv4 unicast
   import-route direct
 #
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   import-route direct
#
```

- 追加設定 3: 各リーフを次のように設定します。

```
#
stp ignored vlan 2 to 4094
stp global enable
stp root primary
#
# リーフダウンリンクインターフェイスで、stp tc-restriction コマンドを設定します。
stp tc-restriction
#
```

デュアル スパイン アップリンクの設定

AD-Campus ソリューションは、冗長性とロードシェアリングの目的で、デュアルスパインアップリンクをサポートしています。

図 1 デュアルスパインネットワーク

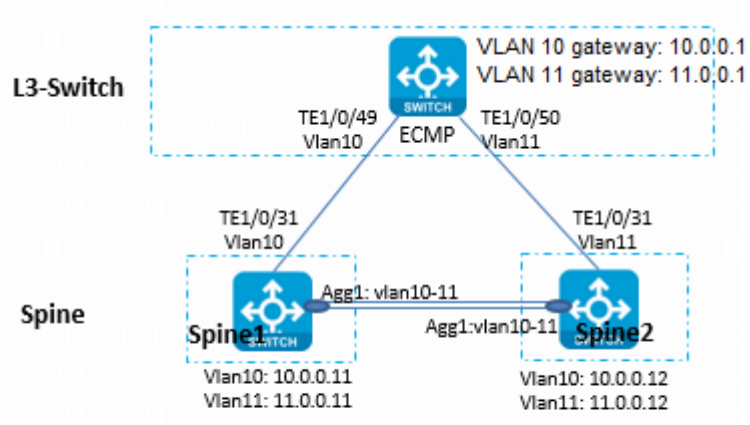


表 1 スパインと L3 デバイスを接続するインターフェイスの IP アドレス

デバイスタイプ	インターフェイス	IP アドレス	接続されているデバイス	インターフェイス	IP アドレス
スパイン1	TE2/0/31	10.0.0.11	レイヤー3スイッチ	TE1/0/49	10.0.0.1
スパイン2	TE2/0/31	11.0.0.12	レイヤー3スイッチ	TE1/0/50	11.0.0.1
スパイン1	Aggr1(VLAN 10、VLAN 11)	10.0.0.11 11.0.0.11	スパイン2	Aggr1(VLAN 10、VLAN 11)	10.0.0.12 11.0.0.12

0 デュアルスパインアップリンクは、レイヤー3 スイッチに接続します。ECMP は、L3 スイッチ上の 2 つのスパインデバイスへの等コストデフォルトルートを設定することによって実装されます。この項では、デュアルスパインアップリンクネットワーキングに固有の設定についてのみ説明します。その他の設定については、このマニュアルの「Manually incorporating a device」を参照してください。

レイヤー3スイッチを設定する

VLAN 10 と VLAN 11 を作成します。
#
vlan 10 to 11
#
STP を設定します。
#
stp global enable
#
スパインデバイスに接続されている VLAN 10 と VLAN 11 を無視される VLAN として設定します。
stp ignored vlan 10 to 11
#
VLAN 10 および VLAN 11 用の VLAN インターフェイスを作成します。
#
interface Vlan-interface10
 ip address 10.0.0.1 255.255.255.0
#
interface Vlan-interface11
 ip address 11.0.0.1 255.255.255.0
#
スパイン 1 に接続されたインターフェイスで VLAN 10 を許可します。

#
interface Ten-GigabitEthernet1/0/25
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 // 実際のネットワーキングに基づいて、許可された VLAN を設定します。
#
スパイン 2 に接続されたインターフェイスで VLAN 11 を許可します。

#
interface Ten-GigabitEthernet1/0/26
 port link-mode bridge
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 11 // 実際のネットワーキングに基づいて、許可された VLAN を設定します。
#
トラックを設定します。
#
track 1 interface Ten-GigabitEthernet1/0/49 physical
track 2 interface Ten-GigabitEthernet1/0/50 physical
#
2 つのデフォルトルートを設定します。ネクストホップはスパイン 1 とスパイン 2 の IP アドレスです。
#
 ip route-static 0.0.0.0 0 10.0.0.11 track 1
 ip route-static 0.0.0.0 0 11.0.0.12 track 2

#
スパイン 1 またはスパイン 2 への 32 ビットホストルートを設定して、スパイン間のリンク障害時にトラフィックのスイッチオーバーを回避します。
#
ip route-static 130.1.0.101 32 10.0.0.11　//130.1.0.101 is the IP address of VSI-interface 4094 on Spine1.
 ip route-static 130.1.0.102 32 11.0.0.12　//130.1.0.102 is the IP address of VSI-interface 4094 on Spine2.
#

スパイン1とL3スイッチ間の接続

STP を設定します。
#
stp instance 0 root primary
 stp ignored vlan 2 to 4094
 stp global enable
#
VLAN 10 を作成します。
#
Vlan 10
#
VLAN-interface 10 を設定し、vpn-default にバインドします。
#
interface Vlan-interface10
 ip binding vpn-instance vpn-default
 ip address 10.0.0.11 255.255.255.0
#
L3 スイッチに接続しているインターフェイスで VLAN 10 を許可します。
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 10　// 実際のネットワーキングに基づいて、許可された VLAN を設定します。
#
サーバーへのルートを設定します。ネクストホップは L3 スイッチの IP アドレスです。
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1
#

スパイン2とL3スイッチ間の接続

STP を設定します。
#
stp instance 0 root secondary
 stp ignored vlan 2 to 4094
 stp global enable

```
#
VLAN 11 を作成します。
#
Vlan 11
#
VLAN-interface 11 を設定し、vpn-default にバインドします。
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 11.0.0.12 255.255.255.0
#
L3 スイッチに接続するインターフェイスで VLAN 11 を許可します。
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11    //    実際のネットワーキングに基づいて、許可された VLAN を設定します。
#
ネクストホップとして L3 スイッチの IP アドレスを使用して、サーバーへのルートを設定します。
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1
#
```

スパイン1とスパイン2の間の結合

スパイン 1 を設定

```
Fast Reroute(FRR)を設定します。
#
ip route-static fast-reroute auto
#
VLAN 11 を作成します。
#
Vlan 11
#
#VLAN-interface 11 を作成します。
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 11.0.0.11 255.255.255.0
#
アンダーレイとの通信用に VLAN 3 を作成します。
#
Vlan 3
#
```

#VLAN-interface 3 を作成します。
#
interface Vlan-interface3
 ip address 3.0.0.1 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
集約グループを作成します。
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
#
集約グループにポートを追加します。
#
interface Ten-GigabitEthernet1/0/30
 port link-mode bridge
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/30
 port link-mode bridge
 port link-aggregation group 1
#
VLAN 10、VLAN 11、および VLAN 3 を許可するように集約グループを設定します。
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1   // 実際のネットワーキングに基づいて、許可された VLAN を設定します。
 port trunk permit vlan 3 10 to 11
 link-aggregation mode dynamic
#
//FRR が設定されている場合は、NQA と Track を設定する必要はありません。
スパインデバイス間の物理リンクで障害が発生した場合に、高速ルートスイッチオーバーを行うようにトラックを設定します。
#
track 1 interface Bridge-Aggregation1 physical
#
スパイン 2 VXLAN 4094 へのスタティックルートを設定します(ネクストホップは VLAN 10 または VLAN 11 に属することができます)。
#
ip route-static vpn-instance vpn-default 130.1.0.102 32 11.0.0.12 track 1
#
NQA および Track を設定します。L3 スイッチ上の VLAN 10 および VLAN 11 のゲートウェイ IP アドレスをネクストホップとして使用して、サーバークラスタへのスタティックルートを設定し、スタティックルートを Track に関連付けます。
#
nqa entry admin server1
 type icmp-echo
  destination ip 10.0.0.1
  frequency 100
  reaction 3 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default

```
#
nqa entry admin server2
 type icmp-echo
  destination ip 11.0.0.1
  frequency 100
  reaction 4 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default
#
 nqa schedule admin server1 start-time now lifetime forever
 nqa schedule admin server2 start-time now lifetime forever
#
track 3 nqa entry admin server1 reaction 3
track 4 nqa entry admin server2 reaction 4
#
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1 track 3
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1 track 4 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1 track 3
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1 track 4 preference 61
#
//NQA および Track が設定されていない場合にスタティックルートを設定します。
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1 preference 61
#
スタティックルートを BGP vpn-default にインポートします。
#
bgp 100
#
 ip vpn-instance vpn-default
  #
  address-family ipv4 unicast
   import-route direct
   import-route static
 #
```

スパイン 2 の設定

```
FRR を設定します。
#
ip route-static fast-reroute auto
#
VLAN 10 を作成します。
#
Vlan 10
#
```

#VLAN-interface 10 を作成します。
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 10.0.0.12 255.255.255.0
#
アンダーレイとの通信用に VLAN 3 を作成します。
#
Vlan 3
#
#VLAN-interface 3 を作成します。
#
interface Vlan-interface3
 ip address 3.0.0.2 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
集約グループを作成します。
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
#
集約グループにポートを追加します。
#
interface Ten-GigabitEthernet1/0/30
 port link-mode bridge
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/30
 port link-mode bridge
 port link-aggregation group 1
#
VLAN 10、VLAN 11、および VLAN 3 を許可するように集約グループを設定します。
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1   //Configure permitted VLANs based on the actual networking.
 port trunk permit vlan 3 10 to 11
 link-aggregation mode dynamic
#
//FRR が設定されている場合は、NQA と Track を設定する必要はありません。
スパインデバイス間の物理リンクで障害が発生した場合に、高速ルートスイッチオーバーを行うようにトラックを設定します。
#
track 1 interface Bridge-Aggregation1 physical
#
スパイン 1 VXLAN4094 へのスタティックルートを設定します(ネクストホップは VLAN 10 または VLAN 11 に属することができます)。
#
ip route-static vpn-instance vpn-default 130.1.0.101 32 11.0.0.11 track 1

```
#
NQA および Track を設定します。L3 スイッチ上の VLAN 10 および VLAN 11 のゲートウェイ IP アドレスをネクストホップとして使用して、サーバークラスタへのスタティックルートを設定し、スタティックルートを Track に関連付けます。
#
nqa entry admin server1
 type icmp-echo
  destination ip 10.0.0.1
  frequency 100
  reaction 3 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default
#
nqa entry admin server2
 type icmp-echo
  destination ip 11.0.0.1
  frequency 100
  reaction 4 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default
#
 nqa schedule admin server1 start-time now lifetime forever
 nqa schedule admin server2 start-time now lifetime forever
#
#
track 3 nqa entry admin server1 reaction 3
rack 4 nqa entry admin server2 reaction 4
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1 track 3 preference 61
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1 track 4
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1 track 3 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1 track 4
#
//   NQA および Track が設定されていない場合にスタティックルートを設定します。
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1 preference 61
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1
#
スタティックルートを BGP vpn-default にインポートします。
#
bgp 100
#
 ip vpn-instance vpn-default
  #
  address-family ipv4 unicast
   import-route direct
   import-route static
 #
```

リーフデバイスおよびアクセスデバイスからサーバーへのルートの設定

リーフデバイスからサーバーへのルートを設定します。

リーフデバイス上のサーバーネットワークセグメントへのスタティックルートを設定しないでください。スパインデバイスは、BGP を介してリーフデバイスへのルートを同期します。

アクセスデバイスでスタティックルートを設定します。

アクセスデバイス上のサーバーへの 2 つのスタティックルートを設定します。ゲートウェイをスパインデバイスの VXLAN 4094 アドレスとして指定します。

```
#
ip route-static 100.1.0.0 24 130.1.0.101      // スパイン 1 の VXLAN 4094 アドレス。
ip route-static 100.1.0.0 24 130.1.0.102      // スパイン 2 の VXLAN 4094 アドレス。
ip route-static 110.1.0.0 24 130.1.0.101
ip route-static 110.1.0.0 24 130.1.0.102
#
```

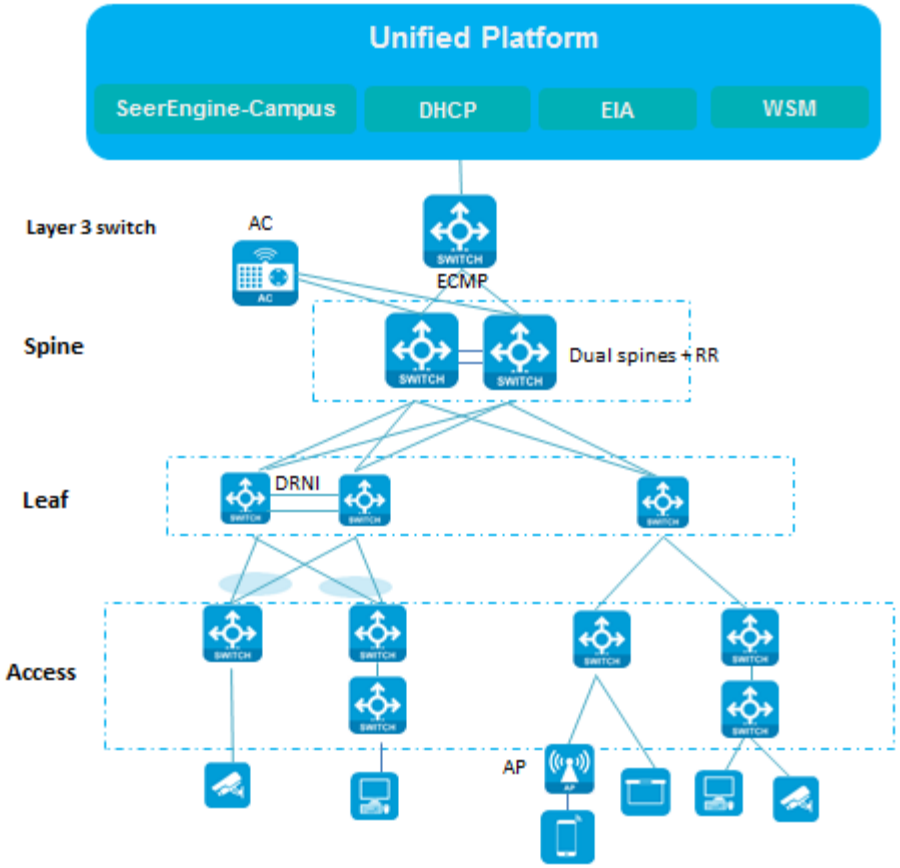
DRNI の設定

DRNIネットワーキング

Distributed Resilient Network Interconnect(DRNI)は、集約レイヤーで 2 つの物理デバイスを 1 つのデバイスに仮想化して、デバイス間のリンク集約を実現し、デバイスレベルの冗長化とトラフィックの負荷分散を実現する。

AD-Campus ソリューションは、DRNI 構成をサポートし、デバイスの冗長化とロードバランシングを実装する DR システムを形成します。

図 2 DRNI ネットワーキング



DRNIの設定

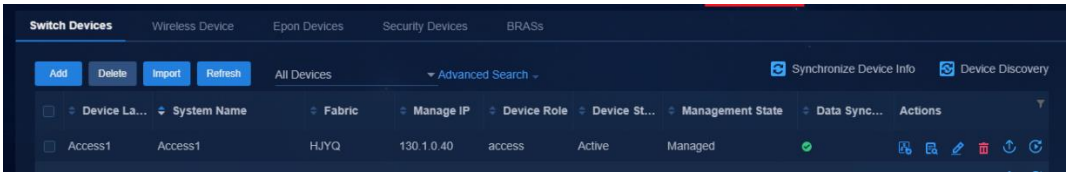
0 デュアルスパイン構成については、「Configure dual spine uplinkAD-Campus configuration」を参照してください。デュアルスパインデバイスは、コントローラによって手動で組み込まれます。コントローラがリーフデバイスを組み込んだ後、DRNI 構成を実行します。コントローラによるスパインまたはリーフデバイ

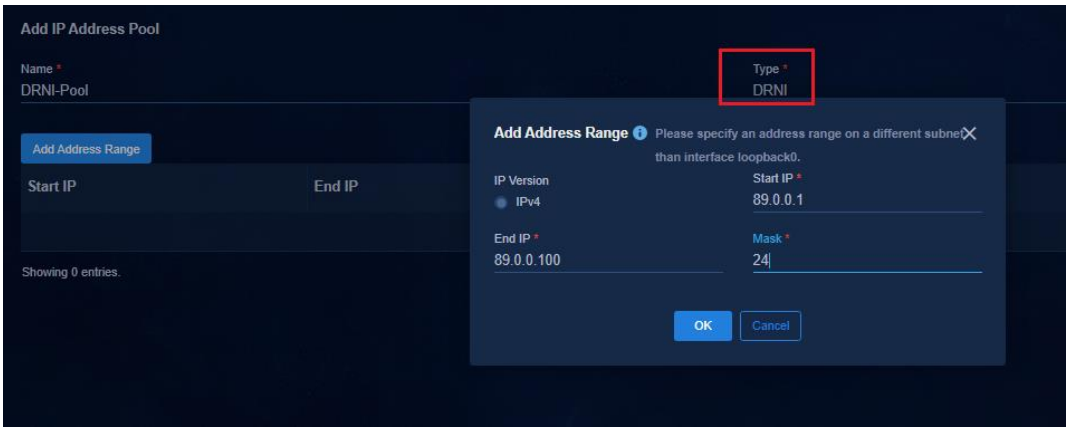
スの組み込みについては、「」を参照してください。この項では、コントローラによるリーフデバイスの組み込み後の DRNI 固有の構成についてのみ説明します。

重要:

- DRNI がイネーブルになっているファブリックでは、自動的に割り当てられた DRNI 仮想 IP アドレスの確認を容易にするために、VLAN 4094 アドレスプールをファブリックにバインドする必要があります。
- BGP ピアは、デュアルスパインおよびリーフデバイスに対して確立する必要があります。設定の詳細については、「Manually incorporating a device」を参照してください。
- キープアライブリンクと IPL リンクは、異なるレートでのインターフェイスの使用をサポートしています。IPL リンクレートが一貫していることを確認する必要があります。
- 複数の DR システムを同時に展開しないでください。次の DR システムを展開する前に、各 DR システムが展開されていることを確認してください。
- アクセスデバイスでリーフスタックネットワーキング、アクセス DRNI、および BFD MAD 検出を行うには、アクセスデバイスのアップリンクインターフェイスで BFD MAD VLAN をディセーブルにします。
- リーフ DRNI ネットワーキングでは、サービストラフィックを正しく転送するために、ユーザーがオンラインになる前に DRNI 環境が確立されていることを確認します。
- IPP または DR インターフェイスをさらに追加するには、IPP または DR インターフェイスを変更してから、対応する物理インターフェイスを追加します。

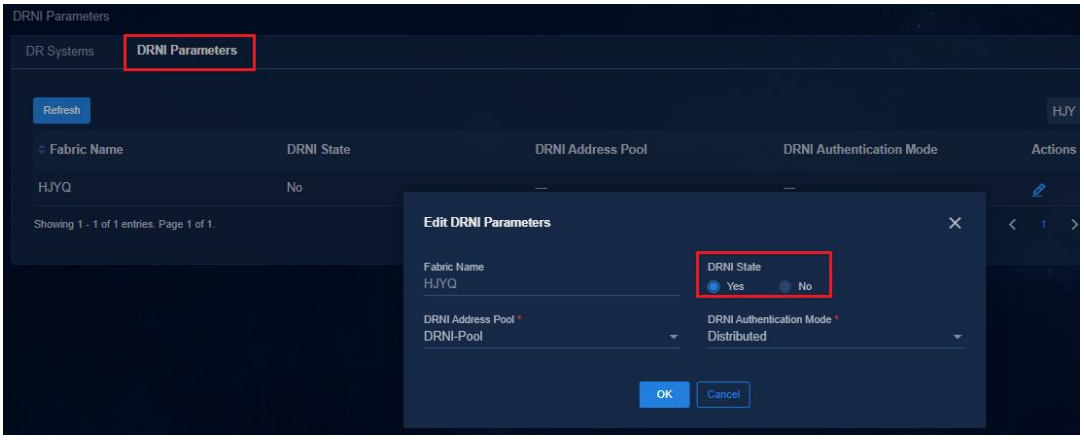
1. **Automation** > **Campus Network** > **Network Devices** ページに移動し、右上隅にある **IP Address Pools** をクリックします。
2. IP アドレスプールを追加するページで、IP アドレスプールタイプとして DRNI を設定します。
3. DRNI IP アドレスプールは、DRNI アドレスの設定に使用されます。各 DRNI 集約グループには、次の 3 つのアドレスを割り当てる必要があります。
   - LoopBack 2 の IP アドレス(2 つのデバイスが同じ LoopBack 2 アドレスを持つ):DRNI の evpn drni グループの IP アドレスを指定します。
   - VLAN インターフェイス 2 の IP アドレス(各デバイスには IP アドレスがあります):2 つの DR デバイス間でアンダーレイルートを同期するために使用されます。



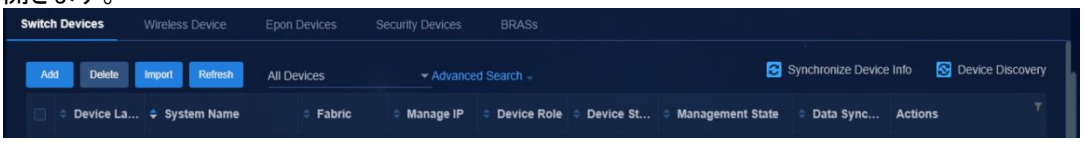


4. **Automation** > **Campus Network** > **Network Devices** ページに移動し、右上隅にある DRNI リンクをクリックします。**DRNI Parameters** タブをクリックし、をクリックして、DRNI パラメーターを変更するためのページを開きます。

   - **DRNI**: **Yes** を選択します。
   - **DRNI Address Pool**: 作成された DRNI アドレスプールを選択します。
   - **DRNI Authentication Mode**: **Distributed** を選択します。



5. **Automation** > **Campus Network** > **Network Devices** ページに移動し、右上隅にある DRNI リンクをクリックします。**Add** をクリックして、クロスデバイス集約グループを追加するためのページを開きます。

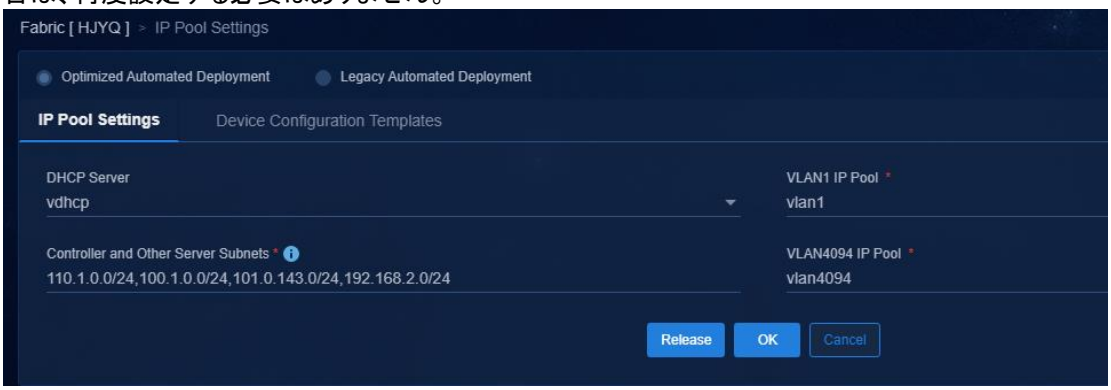


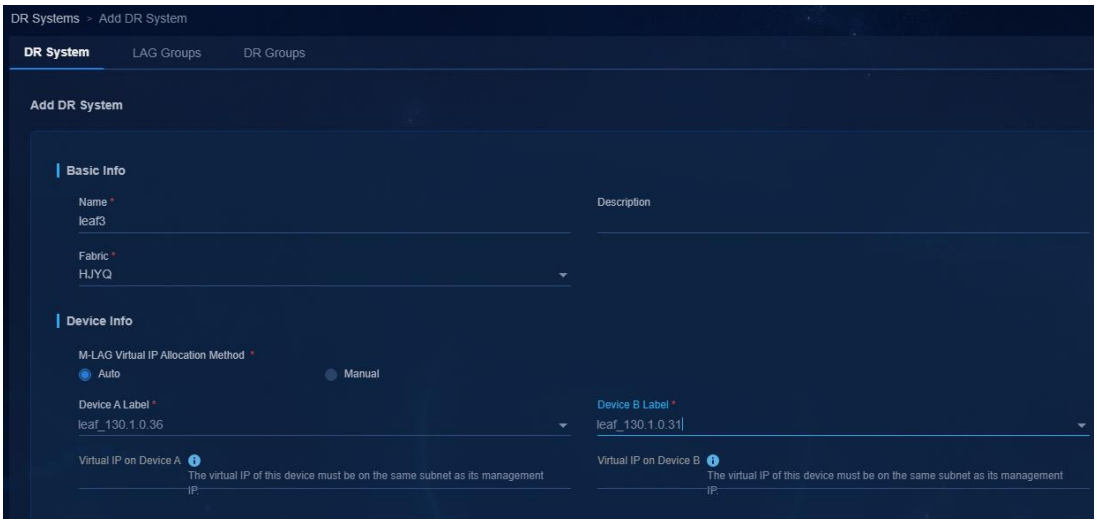
次のパラメーターを設定します。

- **Name**: 名前を無制限で入力します。
- **Fabric**: DRNI を有効にするには、**HJYQ** を選択します。
- **Device A Label/Device B Label**: DRNI を形成する 2 つのデバイスを選択します。

- **M-LAG Virtual IP Allocation Method**: デフォルトでは、IP アドレスはデバイス管理アドレスプールから自動的に割り当てられます。**Manual** を選択するには、仮想 IP アドレスがデバイス管理アドレスと同じネットワークセグメントにあることを確認し、アドレスの競合を回避します。

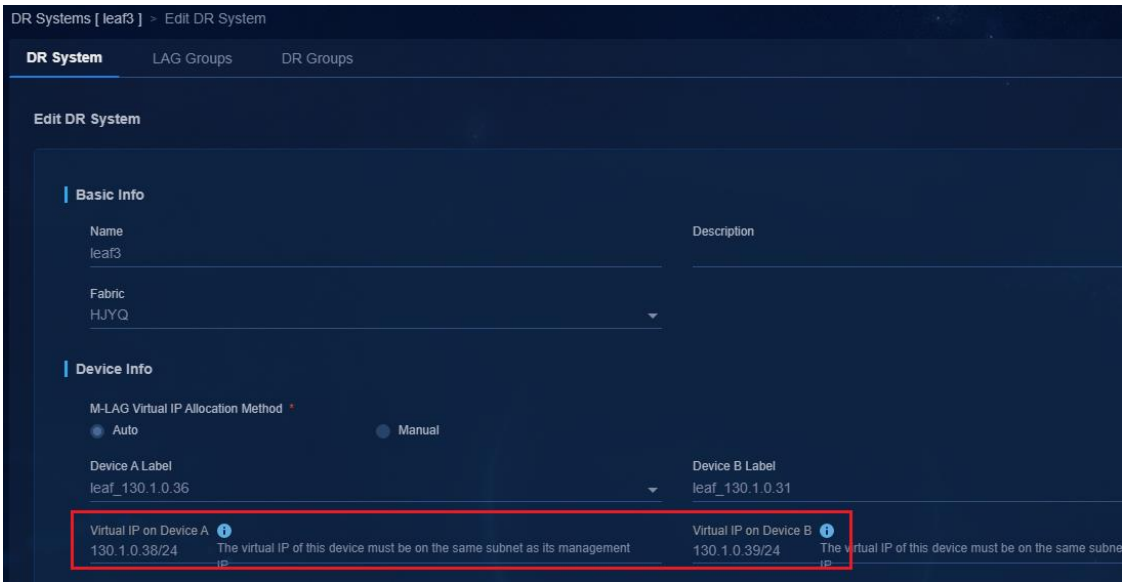
ファブリックに自動化テンプレートが設定されておらず、**Auto** が選択されている場合は、**Automation** > **Campus Network** > **Fabrics** ページの自動化テンプレートでアドレスプールを設定します。VLAN 4094 アドレスプールを VXLAN 4094 と同じネットワークセグメントに設定します。それ以外の場合は、次のメッセージが表示されます。自動化テンプレートがすでに設定されている場合は、再度設定する必要はありません。



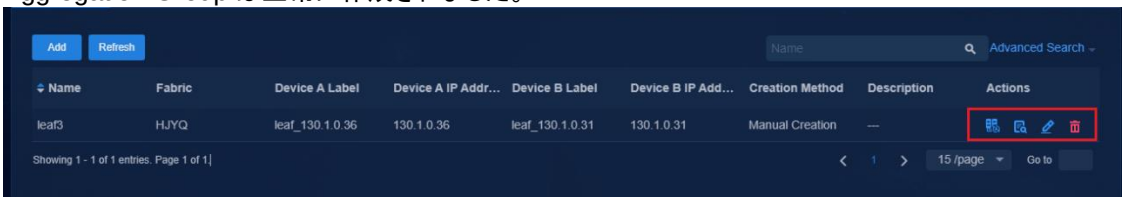


6. 設定が完了すると、コントローラは自動的に DRNI IPP リンクを生成します。**DR Systems** タブでは、自動的に設定された DRNI 仮想 IP を表示できます。

7. クロスデバイス集計グループの作成にかかる時間は、デバイスによって異なります。配布ステータスが完了したら、次の手順を実行します。複数のクロスデバイス集計グループを同時に配布しないでください。

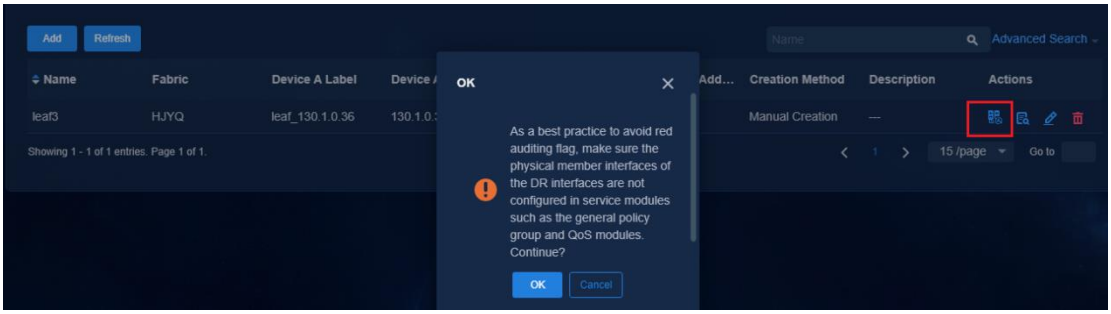


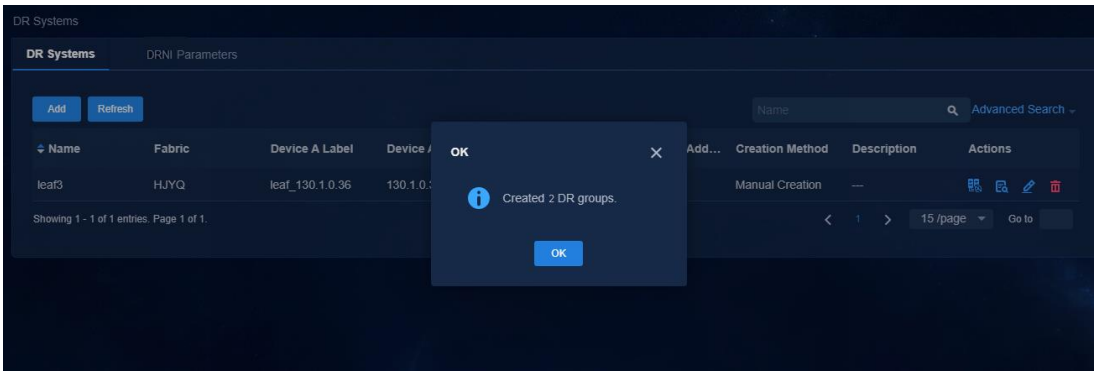
8. **Return** をクリックして、Cross-Device Aggregation Group ページに戻ります。Cross-Device Aggregation Group は正常に作成されました。



9. をクリックすると、デバイスはリーフデバイスとアクセスデバイスの間に DR 集約グループを自動的に作成します。

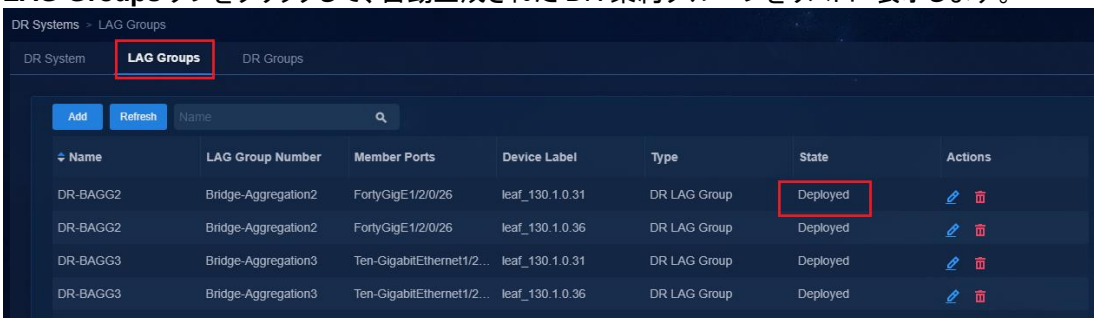
10. DR 集約グループを設定する前に、**Monitor** > **Topology View** > **Campus Topology** ページに移動して、リーフデバイスとアクセスデバイス間のトポロジリンクを表示します。リーフデバイスとアクセスデバイスがアクティブ化され、トポロジが正常であることを確認します。



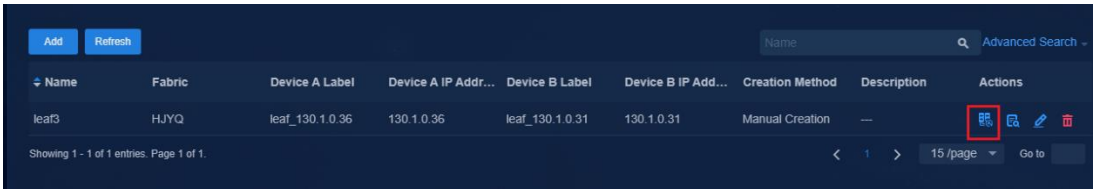


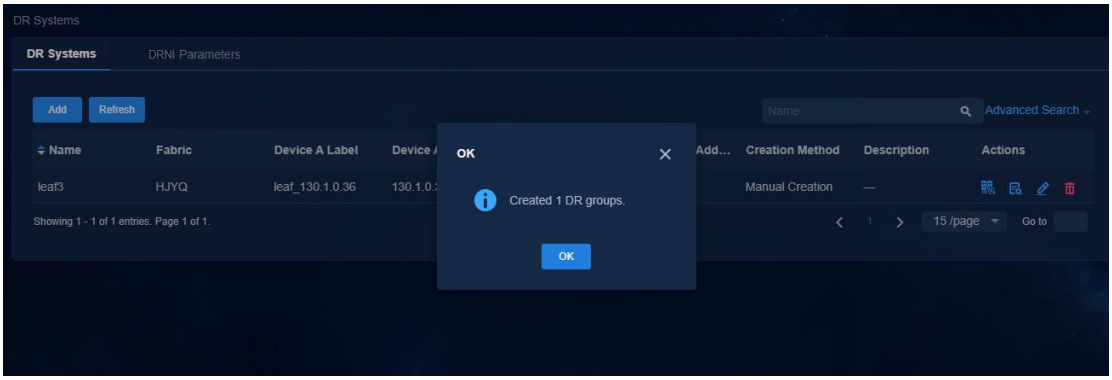
11. 集約グループの作成後、**Actions** 列をクリックして集約グループを編集します。

12. **LAG Groups** タブをクリックして、自動生成された DR 集約グループをリストに表示します。



13. DR 集約グループを設定するには、をクリックします。





14. 構成が完了したら、**Actions** 列をクリックします。追加された DR 集計インターフェイスを表示でき

ます。

15. 設定が完了したら、デバイスの DRNI ステータスを表示できます。

```
<Leaf-S105A>dis drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG1
IPP state (cause): UP
Keepalive link state (cause): UP

                        DR interface information
DR interface   DR group   Local state (cause)   Peer state   Remaining down time(s)
BAGG2          1          UP                    UP           -
BAGG3          2          UP                    UP           -
BAGG4          3          UP                    UP           -
<Leaf-S105A>
```

デュアルスパインデバイス用の DRNI の構成 (手動)

現在のソフトウェアバージョンでは、コントローラはリーフデバイスの DRNI 設定のみをサポートしています。スパインデバイスの DRNI 設定には、この項で説明するように手動設定が必要です。

0 現在のソフトウェアバージョンでは、コントローラはスパインデバイスの手動 DRNI 設定のみをサポートしています。このセクションでは、デュアルスパイン DRNI ネットワーキングに固有の設定についてのみ説明します。その他の設定については、「Manually incorporating a device」を参照してください。

レイヤー3スイッチを設定する

VLAN 10 と VLAN 11 を作成します。

#

vlan 10 to 11

#

VLAN 10 および VLAN 11 用の VLAN インターフェイスを作成します。

#

interface Vlan-interface10

ip address 10.0.0.1 255.255.255.0

#

interface Vlan-interface11

ip address 11.0.0.1 255.255.255.0

#

VLAN 10 が通過できるように、スパイン 1 に接続されたインターフェイスを設定します。

interface Ten-GigabitEthernet1/0/25

port link-mode bridge

port link-type trunk

port trunk permit vlan 10 // 実際のネットワーキングに基づいて、許可された VLAN を設定します。設定が不要な場合は、undo permit vlan1 コマンドを実行します。

#

VLAN 11 が通過できるように、スパイン 2 に接続されたインターフェイスを設定します。

#

interface Ten-GigabitEthernet1/0/26

port link-mode bridge

port link-type trunk

port trunk permit vlan 11 // 実際のネットワーキングに基づいて、許可された VLAN を設定します。設定が不要な場合は、undo permit vlan1 コマンドを実行します。

#

トラックを設定します。

#

track 1 interface Ten-GigabitEthernet1/0/25 physical

track 2 interface Ten-GigabitEthernet1/0/26 physical

#

2 つのデフォルトルートを設定します。ネクストホップはスパイン 1 とスパイン 2 の IP アドレスです。

```
#
 ip route-static 0.0.0.0 0 10.0.0.11 track 1
 ip route-static 0.0.0.0 0 11.0.0.11 track 2
#
```

スパイン1とL3スイッチ間の接続

VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
```

VLAN 10 および VLAN 11 の VLAN インターフェイスを作成し、vpn-default にバインドします。

```
#
interface Vlan-interface10
 ip binding vpn-instance vpn-default
 ip address 10.0.0.11 255.255.255.0
#
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 11.0.0.11 255.255.255.0
#
```

VLAN 10 が通過できるように、L3 スイッチに接続されたインターフェイスを設定します。

```
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10    //    実際のネットワーキングに基づいて、許可された VLAN を設定します。設定が不要な場合は、undo permit vlan1 コマンドを実行します。
#
```

NQA および Track を設定します。L3 スイッチ上の VLAN 10 および VLAN 11 のゲートウェイ IP アドレスをネクストホップとして使用して、サーバークラスタへのスタティックルートを設定し、スタティックルートを Track に関連付けます。

```
nqa entry admin server1
 type icmp-echo
   destination ip 10.0.0.1
   frequency 100
   reaction 3 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
   vpn-instance vpn-default
#
nqa entry admin server2
 type icmp-echo
   destination ip 11.0.0.1
   frequency 100
   reaction 4 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
   vpn-instance vpn-default
#
nqa schedule admin server1 start-time now lifetime forever
nqa schedule admin server2 start-time now lifetime forever
```

```
#
track 3 nqa entry admin server1 reaction 3
track 4 nqa entry admin server2 reaction 4
#
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1 track 3
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1 track 4 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1 track 3
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1 track 4 preference 61
#
```

スパイン2とL3スイッチ間の接続

VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
```

VLAN 10 および VLAN 11 の VLAN インターフェイスを作成し、vpn-default にバインドします。

```
#
interface Vlan-interface10
 ip binding vpn-instance vpn-default
 ip address 10.0.0.12 255.255.255.0
#
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 11.0.0.12 255.255.255.0
#
```

VLAN 11 が通過できるように、L3 スイッチに接続されたインターフェイスを設定します。

```
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 11    //    実際のネットワーキングに基づいて、許可された VLAN を設定します。設定が不要な場合は、undo permit vlan1 コマンドを実行します。
#
```

NQA および Track を設定します。L3 スイッチ上の VLAN 10 および VLAN 11 のゲートウェイ IP アドレスをネクストホップとして使用して、サーバークラスタへのスタティックルートを設定し、スタティックルートを Track に関連付けます。

```
nqa entry admin server1
 type icmp-echo
  destination ip 10.0.0.1
  frequency 100
  reaction 3 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default
#
nqa entry admin server2
 type icmp-echo
  destination ip 11.0.0.1
```

```
  frequency 100
  reaction 4 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
  vpn-instance vpn-default
#
 nqa schedule admin server1 start-time now lifetime forever
 nqa schedule admin server2 start-time now lifetime forever
#
#
track 3 nqa entry admin server1 reaction 3
track 4 nqa entry admin server2 reaction 4
#
 ip route-static vpn-instance vpn-default 100.1.0.0 24 10.0.0.1 track 3 preference 61
 ip route-static vpn-instance vpn-default 100.1.0.0 24 11.0.0.1 track 4
 ip route-static vpn-instance vpn-default 110.1.0.0 24 10.0.0.1 track 3 preference 61
 ip route-static vpn-instance vpn-default 110.1.0.0 24 11.0.0.1 track 4
#
```

スパイン1のDRNIを設定する

OSPF FRR を設定します。

```
#
ospf 1 router-id 200.1.1.254    //    ネットワーク全体で一意のルータ ID を指定します。LoopBack 0 の IP アドレスを借用します。
 non-stop-routing
fast-reroute lfa
 area 0.0.0.0
#
```

LoopBack 2 を設定します。スパイン 1 とスパイン 2 の IP アドレスは同じである必要があります。

```
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
#
```

VLAN 2 を作成します。VLAN-interface 2 を設定します。スパイン 1 とスパイン 2 は異なる IP アドレスを使用します。VLAN 2 は、2 つの DR デバイス間のアンダーレイルートを同期するために使用されます。

```
#
Vlan 2
#
interface Vlan-interface2
 ip address 99.99.0.11 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```

VSI インターフェイス 4094 に MAC アドレスを設定し、スパイン 1 とスパイン 2 に同じ MAC アドレスを設定します。

```
#
interface Vsi-interface4094
 ip binding vpn-instance vpn-default
 ip address 120.0.0.1 255.255.255.0
```

mac-address 0001-0001-0005
 local-proxy-arp enable
#
ループ検出を設定して、VXLAN 4094 でのループを防止します。
#
vsi vxlan4094
        loopback-detection action block
 loopback-detection enable vlan 4094
      #
EVPN 分散集約モードを設定します。スパイン 1 とスパイン 2 の設定は同じです。

#
l2vpn drni peer-link ac-match-rule vxlan-mapping
evpn drni group 99.99.0.10   // VTEP アドレスをループバック 2 インターフェイスの IP アドレスとして指定します。デバイスが再アクティブ化されます。
evpn global-mac 0001-0001-0004 // スパイン 1 and スパイン 2 は同じ MAC アドレスを使います
#
#
 vxlan default-decapsulation source interface LoopBack0
#
BGP によってアドバタイズされる MAC アドレスを、drni グループアドレスとして設定します。
#
bgp 1
address-family l2vpn evpn
nexthop evpn-drni group-address
#
キープアライブインターフェイスを設定します(レイヤー3 インターフェイス。論理インターフェイスと物理インターフェイスがサポートされます)。
#
ip vpn-instance DRNI_KeepAlive   // キープアライブ専用の VPN インスタンスを設定します。
#
#
interface FortyGigE3/0/33
 port link-mode route
 ip binding vpn-instance DRNI_KeepAlive   // VPN インスタンスをバインドする
 ip address 192.168.0.1 255.255.255.252   // サブネットマスクを 30 ビットに設定します。スパイン 1 とスパイン 2 は異なる IP アドレスを使用します。
#
キープアライブのローカルおよびリモート IP アドレスを設定します。
#
drni keepalive ip destination 192.168.0.2 source 192.168.0.1 vpn-instance DRNI_KeepAlive
#
DR システムパラメーターを設定する
同じシステム MAC アドレスと異なるシステム番号を使用して、DR グループ内のデバイスを設定します。
#
drni restore-delay 180
drni system-mac 542b-de08-8200
drni system-number 1
drni system-priority 10

```
#
IPP(レイヤー2 集約インターフェイス)を設定します。
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4094                    //  PVID 4094 が必要です。
 link-aggregation mode dynamic
 port drni intra-portal-port 1                //  IPP を設定します
 undo mac-address static source-check enable  //  MAC アドレス送信元チェックをディセーブルにします。
#
#
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4094
 port link-aggregation group 1
#
#
interface Ten-GigabitEthernet2/0/15
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4094
 port link-aggregation group 1
#
DRNI MAD を設定します。
#
drni mad default-action none
#
track 1024 drni-mad-status
#
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
 ospf track 1024 adjust-cost max
#
MAC アドレスのエージングタイムは、20 分以上にする必要があります。
#
mac-address timer aging 1560
#
スパイン 1 をリーフデバイスに接続するインターフェイスの MAC アドレス送信元チェックをディセーブルにします。
#
interface Ten-GigabitEthernet1/2/0/47
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 1 3497
 lldp source-mac vlan 3497
 lldp management-address arp-learning vlan 3497
 lldp tlv-enable basic-tlv management-address-tlv interface LoopBack0
 undo mac-address static source-check enable
#
```
デバイスの再起動時の自動リカバリ時間を設定します。
DR デバイス間のロールプリエンプションを回避するには、デバイスの再起動時間よりも大きいタイマーを設定します。
```
drni auto-recovery reload-delay delay-value 600
#
```

スパイン2のDRNIを設定する

OSPF FRR を設定します。
```
#
ospf 1 router-id 200.1.1.253
```
//　ネットワーク全体で一意のルータ ID を指定します。LoopBack 0 の IP アドレスを借用します。
```
 non-stop-routing
fast-reroute lfa
 area 0.0.0.0
#
```
LoopBack 2 を設定します。スパイン 1 とスパイン 2 の IP アドレスは同じである必要があります。
```
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
#
```
VLAN 2 を作成します。VLAN-interface 2 を設定します。スパイン 1 とスパイン 2 は異なる IP アドレスを使用します。
```
#
Vlan 2
#
interface Vlan-interface2
 ip address 99.99.0.12 2    55.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```
VSI インターフェイス 4094 の MAC アドレスを設定します。スパイン 1 とスパイン 2 は同じ MAC アドレスを使用します。
```
#
interface Vsi-interface4094
 ip binding vpn-instance vpn-default
 ip address 120.0.0.2 255.255.255.0
mac-address 0001-0001-0005
 local-proxy-arp enable
#
```
ループ検出を設定して、VXLAN 4094 でのループを防止します。
```
#
interface Vsi-interface4094
 ip binding vpn-instance vpn-default
```

```
 ip address 120.0.0.2 255.255.255.0
mac-address 0001-0001-0005
 local-proxy-arp enable
#
```
EVPN 分散集約モードを設定します。スパイン 1 とスパイン 2 の設定は同じです。
```
#
l2vpn drni peer-link ac-match-rule vxlan-mapping
evpn drni group 99.99.0.10       //   VTEP アドレスをループバック 2 インターフェイスの IP アドレスとして指定します。デバイスが再アクティブ化されます。
evpn global-mac 0001-0001-0004   //   スパイン 1 とスパイン 2 は同じ MAC アドレスを使用します。
#
#
 vxlan default-decapsulation source interface LoopBack0
#
```
BGP によってアドバタイズされる MAC アドレスを、drni グループアドレスとして設定します。
```
#
bgp 1
address-family l2vpn evpn
nexthop evpn-drni group-address
#
```
キープアライブインターフェイスを設定します(レイヤー3 インターフェイス。論理インターフェイスと物理インターフェイスを使用できます)。
```
#
ip vpn-instance DRNI_KeepAlive        //   キープアライブ専用の VPN インスタンスを設定します。
#
#
interface FortyGigE3/0/33
 port link-mode route
 ip binding vpn-instance DRNI_KeepAlive      //   VPN インスタンスをバインドします
 ip address 192.168.0.2 255.255.255.252      //   サブネットマスクを 30 ビットに設定します。スパイン 1 とスパイン 2 は異なる IP アドレスを使用します。
#
```
キープアライブのローカルおよびリモート IP アドレスを設定します。
```
#
drni keepalive ip destination 192.168.0.1 source 192.168.0.2 vpn-instance DRNI_KeepAlive
#
```
DR システムパラメーターを設定します。DR グループ内のデバイスに同じシステム MAC アドレスと異なるシステム番号を設定します。
```
#
drni restore-delay 180
drni system-mac 542b-de08-8200
drni system-number 2
drni system-priority 10
#
```
IPP(レイヤー2 集約インターフェイス)を設定します。
```
#
interface Bridge-Aggregation1
 description SDN_LAGG
 port link-type trunk
```

```
 port trunk permit vlan all
 port trunk pvid vlan 4094                          //  PVID 4094 が必要です。
 link-aggregation mode dynamic
 port drni intra-portal-port 1                      //  IPP を構成します。
 undo mac-address static source-check enable   //  MAC アドレス送信元チェックをディセーブルにします。
#
#
interface Ten-GigabitEthernet3/0/15
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port trunk pvid vlan 4094
 port link-aggregation group 1
#
#
interface Ten-GigabitEthernet3/0/22
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port trunk pvid vlan 4094
 port link-aggregation group 1
#
DRNI MAD を設定します。
#
drni mad default-action none
#
track 1024 drni-mad-status
#
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
 ospf track 1024 adjust-cost max
#
MAC アドレスのエージングタイムは、20 分以上にする必要があります。
#
mac-address timer aging 1560
#
スパイン 1 をリーフデバイスに接続するインターフェイスの MAC アドレス送信元チェックをディセーブルにします。
#
interface Ten-GigabitEthernet1/2/0/47
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3498
 lldp source-mac vlan 3498
 lldp management-address arp-learning vlan 3498
```

```
 lldp tlv-enable basic-tlv management-address-tlv interface LoopBack0
 undo mac-address static source-check enable
#
デバイスの再起動時の自動リカバリ時間を設定します。
DR デバイス間のロールプリエンプションを回避するには、このタイマーをデバイスの再起動時間よりも長く設定します。
drni auto-recovery reload-delay delay-value 600
#
```

IP-SGT の設定

IP-SGT は、業界をリードするソリューションです。デバイスは、サブスクリプションを通じて AAA サーバーから IP-SGT ロールを取得します。ユーザーは、別の場所でオンラインになったときに同じ権限を取得できます。IP-SGT 設定には、2 つの部分が含まれます。デバイスは、EIA からの IP-SGT 情報に添字を付け、EIA はその情報をデバイスにプッシュします。

IP-SGT は、ネットワーキング要件が少なく、さまざまなシナリオでの統一されたポリシー実施ソリューションの適応性が向上します。

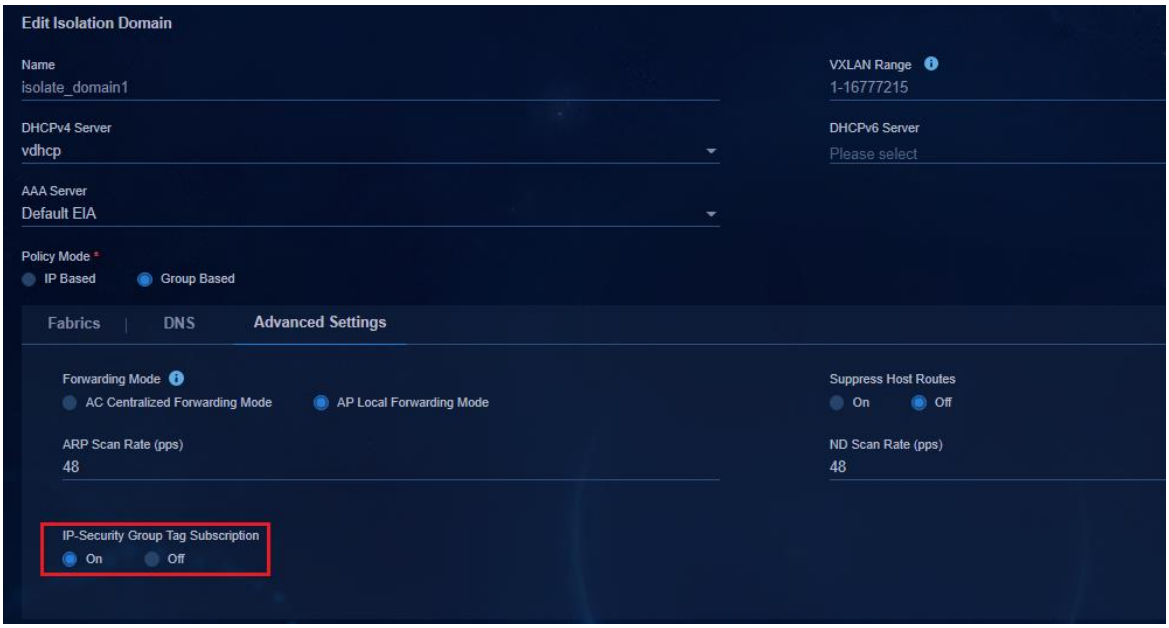
- 認証ポイントと統一ポリシー実施ポイントは、分離できます。
- IP-Transit のシナリオでは、複数の分離されたドメインにわたって、均一なポリシー適用がサポートされます。
- VLAN からセキュリティグループを分離します。Wireless User IP Role(SGT)は、サブスクリプションを通じて取得されます。

注:

IP-SGT では、デバイスが VLAN 1 を介してコントローラと WebSocket チャネルを確立する必要があります。IP-SGT を設定する場合は、デバイスが VLAN 1 を介してコントローラと通信できることを確認してください。

キャンパス構成

1. **Automation** > **Campus Network** > **Isolation Domain** ページに移動し、をクリックして、隔離ドメインを編集するためのページを開きます。
2. **Advanced Settings** タブをクリックし、**IP-Security Group Tag Subscription** を **On** に設定します。

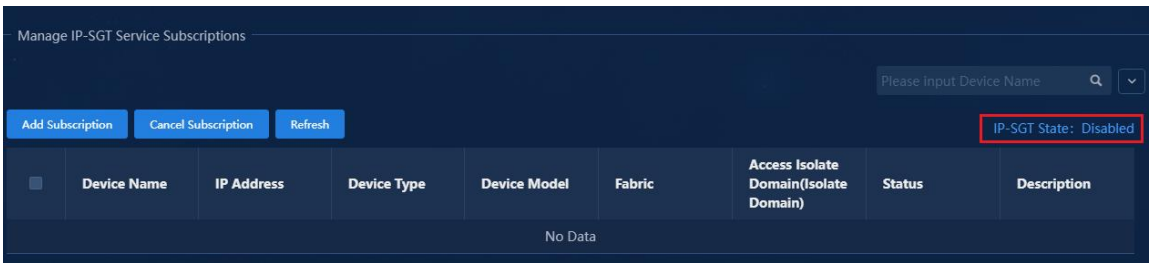


3. 設定後、コントローラはデバイスに次のコマンドを発行します。

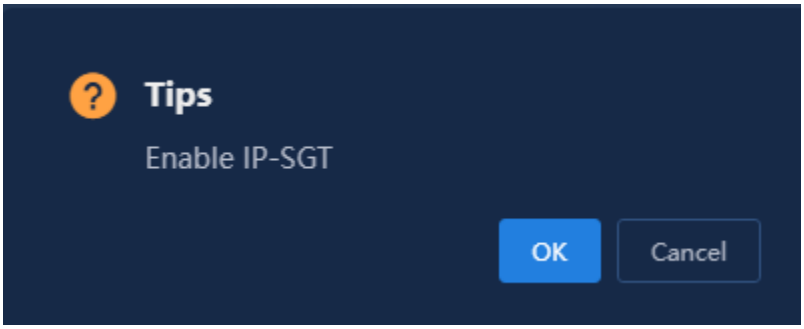
```
#
ipsgt enable       //Enable IPSG function.
 ipsgt on-demand ip 20.0.0.0 255.255.0.0 vpn-instance Teach     //Enable the on-demand deployment function for each network segment.
 ipsgt on-demand ip 30.0.0.0 255.255.0.0 vpn-instance Teach
 ipsgt on-demand ip 30.1.0.0 255.255.0.0 vpn-instance Teach
#
```

EIAコンフィギュレーション

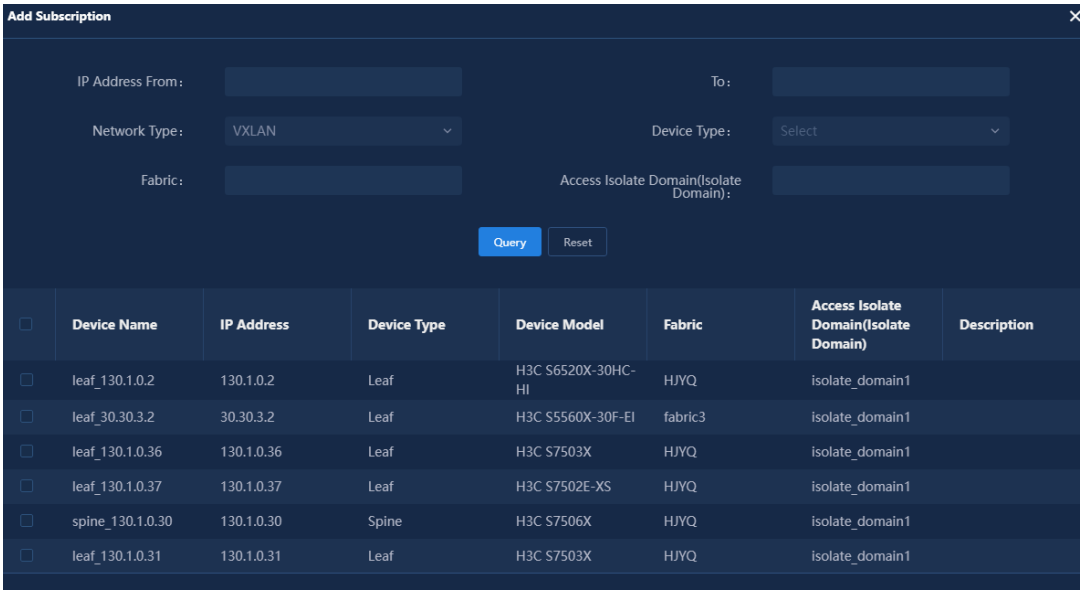
1. **Automation** > **Campus Network** > **User** > **Service Parameters** > **Access Parameters** > **Manage IP-SGT Service Subscriptions** ページに移動します。



2. **IP-SGT State** をクリックし、ダイアログボックスで **OK** をクリックして、IP-SGT サービスをイネーブルにします。



3. **Add Subscription** をクリックします。**Add Subscription** ページのデバイスは、コントローラに組み込まれます。



4. サブスクリプション用のデバイスを選択し、**OK** をクリックします。
5. コントローラはデバイスとの Websocket 接続を確立します。接続後、接続ステータスは **UP** になります。

// 次のコマンドを使用して、ステータスを表示できます。

```
[Leaf-S105A]dis cloud-management state
Cloud connection state     : Established
```

```
Device state                    : Request_success
Cloud server address        : 100.1.0.100
Cloud server domain name : 100.1.0.100
Cloud server port             : 443
Connected at                    : Mon Jan 24 07:47:24 2022
Duration                        : 00d 03h 38m 17s
Process state                 : Message received
Failure reason                : N/A
[Leaf-S105A]
```

//次のコマンドを使用して、エンドユーザーがオンラインになったときにサブスクリプション情報を表示します。

```
[Leaf-S105A]dis ipsgt map
Total IPv4 IP-SGT entries: 2
  Microsegment ID: 3503
     IPv4 address                Vpn instance
     23.3.0.3                    vpn1
     23.3.0.4                    vpn1
Total IPv6 IP-SGT entries: 0
[Leaf-S105A]
```

O&M モニタリング

詳細については、『AD-Campus 6.2 Maintenance Guide』を参照してください。