AD-キャンパス 6.2

IP ポリシーの基本設定ガイド

内容

制限事項およびガイドライン 1

はじめに 4

概要 4
単一ファブリックネットワークモデル 5
デュアルスパインネットワークモデル 5
IRF ネットワークモデル 8
サーバーとネットワークデバイス間の接続 12
デュアルスパインネットワーク 13
Spine IRF ネットワーキング 14
ネットワーク構成 14
設定ワークフロー 15

ソフトウェアとハードウェアの情報 17

ソフトウェア情報 17
ハードウェア情報 18

リソースと IP アドレスの計画 19

サーバーリソースのプランニング 19
ユーザーリソースプランニング 25
ユーザーVLAN プランニング 26

AD-Campus の設定 28

AD-Campus コントローラーへのログイン 28
ライセンスの登録 29
前提条件 31
ユーザーエンドポイント設定の構成 31
AAA サーバーの設定 33
DHCP サーバー設定の構成 35
スタティックイーサネットサービスインスタンスの従来の転送エントリー学習のイネーブル化 40
デバイスのオンボード 41
従来の自動導入 41
最適化された自動導入 41
導入の半分を自動化 41
手動による組み込み 41
ポリシーテンプレートの設定 66
アクセスネットワークの設定 76
分離ドメインの構成 76
プライベートネットワークの設定 77
セキュリティグループの構成 84
ネットワークポリシーの構成 85
ユーザーのオンボーディング 92
アクセスポリシーの構成 92
アクセスサービスの設定 95
アクセスユーザーの管理 96
アクセスシナリオの管理(オプション) 101
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 104
オンラインユーザーの管理 106

ユーザー認証とアクセス 107

802.1X 認証の設定 107
証明書のインストール 107
ユーザー認証 108

MAC ポータル認証の設定……116
BYOD セキュリティグループの作成……117
ACL 3001 の設定 ……118
MAC ポータル認証の有効化……118
MAC ポータル認証の開始……120
MAC 認証の設定……123
MAC 認証ユーザーの設定 ……123
MAC 認証の設定 ……124
ブロードバンド IoT サービスの設定……125
MAC アドレス範囲に基づく高速オンライン ……126
IP アドレス範囲に基づいた高速オンライン ……129
エンドポイントの識別に基づく高速オンライン ……132
ブロードバンド IoT エンドポイントを長期にわたってオンライン状態に維持する……134
認証不要インターフェイスの設定……136
認証不要インターフェイスグループの追加……136
隔離ポートデバイスグループの追加 ……138
認証不要のインターフェイスグループへのセキュリティグループのバインド……139
デバイスに展開された設定 ……140
ゲストがオンラインであるか、認証がオンラインで失敗しました ……141
ゲストオンライン ……141
認証に失敗したユーザーがオンラインになることを許可する ……144
ゲストサービス ……147
ゲスト管理の設定 ……148
ページプッシュポリシーの設定 ……151
ゲストオンライン ……152
権限とドメインの管理 ……162
概要 ……162
基本概念 ……162
グループ ……162
ロール ……162
アクセス権 ……163
アクセス許可とドメインの構成……164
権限の追加……164
ユーザー定義の役割の追加……168
ユーザー定義グループの追加 ……170
演算子の追加……171
権限とドメイン管理の確認 ……172
Wizard > **Campus Wizard** > **Device Onboarding Plan**……172
Monitor > Topology > Campus Topology ……173
Automation>Campus Network>Fabrics の順に選択……173
Automation>Campus Network>Devices>Switch Devices ……173
Automation > **Campus Network** > **Isolation Domain** > **Isolation Domain**……174
公的資源……175
リーフデバイスに直接接続されたエンドポイントの設定 ……177
インターフェイスグループへのメンバーの追加……177
インターフェイスグループへのポリシーの展開……178
ユーザークリティカルなソリューションの構成 ……179
重要なレイヤー2 ネットワークドメインの作成 ……179
重要なセキュリティグループの作成……180
ポリシーテンプレートの設定 ……182
重要な IT リソースへのアクセス設定 ……183
重要な DHCP サーバーの設定 ……183
Microsoft の密結合 DHCP サーバーの構成 ……184
Microsoft の疎結合 DHCP サーバーの構成 ……184

IT リソースグループ ……193
IT リソースグループの作成 ……193
IT リソースグループへのアクセス ……194
境界デバイスを介した外部ネットワークへのアクセス(シングルスパイン) ……196
境界デバイスグループの作成 ……196
プライベートネットワークの追加(オプション)……199
出力ゲートウェイの追加 ……199
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 ……202
デバイスに展開された出力ゲートウェイ設定の表示 ……202
境界デバイス上の外部ネットワークに接続されたインターフェイスに展開された設定 ……204
境界デバイスに接続された L3 デバイスの手動設定 ……204
ボーダーデバイスと外部ルートデバイスの関連付け(デュアルボーダー) ……206
border 1 の設定 ……206
border 2 の設定 ……208
境界デバイスに接続された L3 デバイスの設定 ……210
マルチキャスト設定 ……212
マルチキャストサービスコンフィギュレーション ……212
レイヤー2 マルチキャスト ……212
レイヤー3 マルチキャスト ……214
スパインがルータ経由でマルチキャスト送信元に接続されている場合のマルチキャストサービスの設定 ……218
出力ゲートウェイの設定 ……219
境界と外部ネットワーク間の接続のためのインターフェイスの手動設定 ……219
境界デバイスに接続されたレイヤー3 マルチキャストデバイスでの手動設定 ……220
QoS ……222
QoS のグローバルなイネーブル化 ……222
アプリケーション分類子の追加 ……223
アプリケーションポリシーの追加 ……224
デバイスに展開された設定の表示 ……228
リーフアクセスネットワークモデルの制約事項とガイドライン ……230
シングルリーフシナリオ ……230
マルチリーフ シナリオ ……231
冗長デュアルスパインアップリンクの設定 ……234
レイヤー3 スイッチの設定 ……234
Spine 1 のレイヤー3 スイッチへの接続 ……236
Spine 2 のレイヤー3 スイッチへの接続 ……236
Spine 1 と Spine 2 の接続 ……237
Spine 1 の設定 ……237
Spine 2 の設定 ……239
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 ……242
リーフデバイスからサーバーへのルートの設定 ……242
アクセスデバイスでのスタティックルートの設定 ……242
デュアルスパインデバイス用の DRNI の構成(手動) ……243
レイヤー3 スイッチの設定 ……243
Spine 1 のレイヤー3 スイッチへの接続 ……244
Spine 2 のレイヤー3 スイッチへの接続 ……245
Spine 1 での DRNI の設定 ……246
Spine 2 での DRNI の設定 ……249

DRNI の設定 ……252
DRNI ネットワーキング ……252
DR システムの設定 ……252
O&M モニタリング ……258

制限事項およびガイドライン

- このソリューションでサポートされているモデルの詳細については、このソリューションの仕様マニュアルを参照してください。
- S5560X-EI、S5560X-HI、S6520X-EI、および S6520X-HI スイッチは、Edge Device(ED)として動作できません。
- S5560X-EI、S5560X-HI、S6520X-EI、または S6520X-HI スイッチが共有ゲートウェイを持つ境界デバイスとして動作する場合、バックワードトラフィックが通過できるように、バックワードトラフィックが通過するインターフェイスで PBR ポリシーを設定する必要があります。
- S5560X または 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 および MLD プロトコルパケットを含む)を、CPU 保護のために CPU に配信しないでください。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実行します。
  - **b.** VSI ビューで flooding disable all コマンドまたは flooding disable broadcast コマンドを使用します。VSI ビューで flooding disable all all-direction コマンドまたは flooding disable broadcast all-direction コマンドが使用されている場合は、undo flooding disable コマンドを実行して設定を削除してから、VSI ビューで flooding disable all コマンドまたは flooding disable broadcast コマンドを使用する必要があります。
  - **c.** forwarding vxlan-packet inner-protocol { IPv4 | ipv6 }コマンドをグローバルに実行します。IPv4 サービスと ipv6 サービスの両方が使用可能な場合は、このコマンドに IPv4 キーワードと ipv6 キーワードの両方を指定します。
  - **d.** ポート分離グループ設定をグローバルに設定し、リーフデバイスのすべてのダウンリンクインターフェイスをポート分離グループに追加します。一部のリーフダウンリンクインターフェイス間に従来の VLAN サービスの相互通信が存在する場合、これらのインターフェイスをポート分離グループに追加する必要はありません。ただし、ポート分離が設定されていない場合、リーフデバイスは、これらのダウンリンクインターフェイス間でブロードキャストトラフィック、不明なマルチキャストトラフィック、および不明なユニキャストトラフィックを分離できません。
- BYOD セキュリティグループを使用するには、vDHCP サーバーを構成する必要があります。
- リーフアクセスのシナリオでは、コントローラーはループバックインターフェイスに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を設定するには、ページで、対応するファブリック上のデバイスの VTEP IP アドレスを変更します。
- ルータをアクセスデバイスに接続するには、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する必要があります。さらに、ルータで DHCP および NAT をディセーブルにする必要があります。
- 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。MAC ポータル認証は、複数のユーザーアカウントで共有されるパブリックホストではサポートされません。
- Microsoft DHCP サーバーが IPv6 アドレス割り当てをサポートするのは、スタンドアロンモードで動作し、疎結合方式を使用する場合だけです。
- 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。
- アクティブな Microsoft DHCP サーバーに障害が発生した場合、スタンバイサーバーは IP アドレスを割り当てることしかできず、バインディングエントリーを生成できません。アクティブなサーバーに障害が発生したときにオンラインになるエンドポイントのバインディングエントリーを生成するには、まずエンドポイントをオフラインにしてから、アクティブなサーバーが回復した後にオンラインにする必要があります。
- グループポリシーの既定のポリシーが 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 IT リソースグループを展開します。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、deny アクション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、permit アクションを含むポリシーを構成する必要があります。

- サーバーに接続されたレイヤー3 スイッチでは、PVST モードではなく MSTP モードで動作するようにスパニングツリー機能を設定する必要があります。
- 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。
- 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、必要なポートを開く必要があります。ポートの詳細については、このソリューションのポートマトリックスを参照してください。
- ユーザーが所属するレイヤー2 ネットワークドメインにセカンダリサブネットがある場合は、ユーザーのアクセスポリシーで Bind User IP 機能を使用しないでください。
- mac-authentication carry user-ip コマンドは、次の場合にだけ使用します。
  - IP セグメントベースの認証が使用されます。
  - Bind User IP 機能は、ユーザーが認証に使用するアクセスポリシーでイネーブルになっています。

  上記の状況を除き、他の認証状況でこのコマンドを使用しないでください。他の認証状況でエンドポイントにスタティック IP アドレスを設定する必要がある場合は、スタティック IP アドレスを EIA に配信するために、ARP スヌーピング設定をコントローラー経由でデバイスに展開できます。
- 802.1X 認証および MAC/MAC ポータル認証がサポートされています。必要に応じて、一方または両方を構成できます。必要な場合以外は、両方を構成しないことをお薦めします。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構成がサポートされています。
- spine、leaf、access、または AC デバイスを使用して IRF ファブリックを手動で設定する場合は、irf mac-address persistent always コマンドを使用して、マスター/下位スイッチオーバー後も IRF 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。
- VLAN モードのマルチキャスト送信元は、次のデバイスにだけ接続できます。
  - S12500G-AF スイッチです。
  - S10500 および S10500X スイッチ上の SH モジュール。
  - S6550XE スイッチ。
  - S6525XE スイッチ。
- 現在のソフトウェアバージョンでは、このソリューションは同じ分離ドメイン内の複数のファブリック間のレイヤー3 マルチキャストだけをサポートし、マルチキャスト送信元とマルチキャストメンバは同じプライベートネットワークに属している必要があります。このシナリオでは、リーフアクセスモデルはサポートされず、マルチキャスト送信元とマルチキャストメンバは ED に接続できません。
- ユーザーが DHCP サーバーからアドレスを取得した後に、DHCP サーバーバインディングを変更することはできません。
- 同じグループ内のデバイスは、複数のコントローラーセットに同時に組み込むことはできません。
- DHCP サーバーのセットは、複数のコントローラーセットに同時に組み込むことはできません。
- S5130-EI および S5130-HI スイッチは、qos priority dscp 0 コマンドをサポートしていません。エンドポイントによる DSCP 値の変更を防ぐことはできません。
- 一部のスイッチは、チップの制限のためにレートの自動ネゴシエーションをサポートしていません。たとえば、S6525XE-HI スイッチのポートレートは、自動ネゴシエーションを使用して Giga に変更できません。

- ARP フラッディングが存在するシナリオでは、攻撃検出および防御コマンドを設定できます。詳細については、製品のマニュアルを参照してください。
- ベストプラクティスとして、多数のセキュリティグループが存在する場合は、デバイス上の AC に対して会話型転送エントリー学習をイネーブルにします。
- DR システムがリーフデバイスとして動作する場合は、リーフデバイスに接続されているスパインデバイスの VSI インターフェイス 4094 で arp send-gratuitous-arp interval コマンドを使用します。間隔は 30 秒より大きい値に設定することをお勧めします。
- Automation > Campus Network > Network Parameters > vDHCP ページに移動します。syslog 機能は、DDI 表示ページでのエンドポイント IP コリジョン検出に必要です。リーフデバイスを手動で展開する場合は、info-center loghost vpn-instance vpn-default 100.1.0.100 コマンドを追加します。
- スパインデバイスまたはリーフデバイスをモニタリストに追加する場合は、次のコマンドを使用して、SNMP トラップの宛先 IP アドレスに VPN パラメーターを追加する必要があります。

  snmp-agent target-host trap address udp-domain xx.xx.xx.xx vpn-instance vpn-default params securityname public v2c<サーバー名>
- 手動展開モードとレガシー自動展開モードの両方で展開されたデバイスがファブリックに含まれている場合、次の制約事項およびガイドラインが適用されます。
  - 各デバイスの VSI インターフェイス 4094 または VLAN インターフェイス 4094 に、一意の IP アドレスが割り当てられていることを確認します。
  - 手動で展開されたデバイスによって使用されるアンダーレイ IP およびアンダーレイ VLAN の範囲が、自動化テンプレートで自動的に展開されたデバイス用に設定された範囲と重なっていないことを確認します。

重要:

ベストプラクティスとして、この種の混合配置は使用しないでください。

- コントローラーがリーフデバイスを含む DR システムを追加または削除すると、リーフデバイスは一時的にネットワークから切断されます。この問題を解決するには、evpn irb asymmetric コマンドを使用して、管理ネットワークセグメントの非対称 IRB 転送を有効にします。接続が安定している場合は、undo evpn irb asymmetric コマンドを使用して、非対称 IRB 転送を無効にします。
- Name-Address Binding 設定は、IP Source Guard(IPSG;IP ソースガード)および ARP 検出設定と相互に排他的です。
- ユーザー展開の場合、ベストプラクティスとして、リーフデバイスに IPSG を展開しないでください。
- DR システムでは、競合を回避するために、DR メンバーデバイスごとに一意のルータ ID を指定する必要があります。

はじめに

概要

このドキュメントでは、次の項目を含む、AD-Campus 6.2 ソリューションの基本的な展開を完了する方法について説明します。

- ソフトウェアのインストールと導入
- 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ー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。

H3C には、さまざまな機能の設定ガイドが用意されています。機能の設定の詳細については、表 1 に示す設定ガイドを参照してください。

表 1 機能設定ガイド

機能	説明	マニュアル
Automation	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(最適化された自動化の設定ガイド)*
Half automation	スパインデバイスまたはリーフデバイスは手動で組み込まれ、アクセスデバイスは自動的に組み込まれます。	*AD-Campus 6.2 Half Automation設定ガイド*
Wireless	AC組み込みおよびワイヤレスユーザー認証。	*AD-Campus 6.2ワイヤレス設定ガイド*
IPv6	IPv6ネットワークを使用してデバイスを組み込み、ユーザーがIPv6アドレスを取得できるようにします。	*AD-Campus 6.2 IPv6サービスコンフィギュレーションガイド*
Multi-campus interconnection	単一の分離ドメイン内での分離ドメイン相互接続およびマルチファブリック相互接続。	*AD-Campus 6.2 Multi-Campus and Multi-Fabricコンフィギュレーションガイド*
Service chain	東西および南北のサービスチェーン。	*AD-Campus 6.2サービスチェーンコンフィギュレーションガイド*
Microsoft DHCP	Microsoft DHCPの緊密に結合された環境のセットアップと構成。	*AD-Campus 6.2 Microsoft DHCP Tight Coupling Solution設定ガイド*
Security convergence	利用者向けのセキュリティ構築サービス。	*AD-Campus 6.2 Security Convergenceコンフィギュレーションガイド*
EPON	EPONネットワーキングのセットアップとサービス設定。	*AD-Campus 6.2 EPONネットワークコンフィギュレーションガイド*
Replacement of faulty device	デバイス障害後のターゲット交換と異種交換。	*障害のあるデバイスを交換するためのAD-Campus 6.2設定ガイド*

単一ファブリックネットワークモデル

AD-Campus ソリューションは、デュアルスパインおよび IRF ネットワークモデルをサポートします。デュアルスパインネットワークモデルでは、2 つのスパインデバイスが DR システムを形成するか、2 つのスパインデバイスが冗長性保護およびトラフィック負荷分散のためにデュアルホーム接続されます。IRF ネットワークモデルでは、2 つのデバイスが 1 つのデバイスに仮想化され、複数のデバイスの処理能力、相互作用、統合管理、および中断のないメンテナンスを提供します。2 つのモデルは、デバイスアーキテクチャによってさらに次のネットワークモデルに分割できます。

- **Spine-leaf-access network model**: Spine、Leaf、およびアクセスデバイスを含む一般的なキャンパスネットワークモデル。このモデルでは、Spine、Leaf、およびアクセスデバイスは IRF ファブリックセットアップをサポートし、アクセスデバイスはマルチレベルカスケードもサポートします。
- **Spine-leaf network model**: スパインデバイスとリーフデバイスが含まれます。このモデルでは、アクセスロールを持つデバイスは展開されません。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。
- **Leaf-access network model**: リーフデバイスとアクセスデバイスが含まれます。このモデルでは、スパインロールを持つデバイスは展開されません。このモデルは主に小規模なネットワークで使用されます。リーフデバイスは、2 シャーシの IRF ファブリックを形成できます。アクセスデバイスは、IRF ファブリックのセットアップとマルチレベルのカスケードをサポートします。

このマニュアルでは、単一ファブリックの Spine-Leaf-Access、Spine-Leaf、および Leaf-Access ネットワークモデルだけを対象としています。マルチファブリックネットワーキング設定の詳細については、『AD-Campus 6.2 Multi-Campus and Multi-Fabric Configuration Guide』を参照してください。

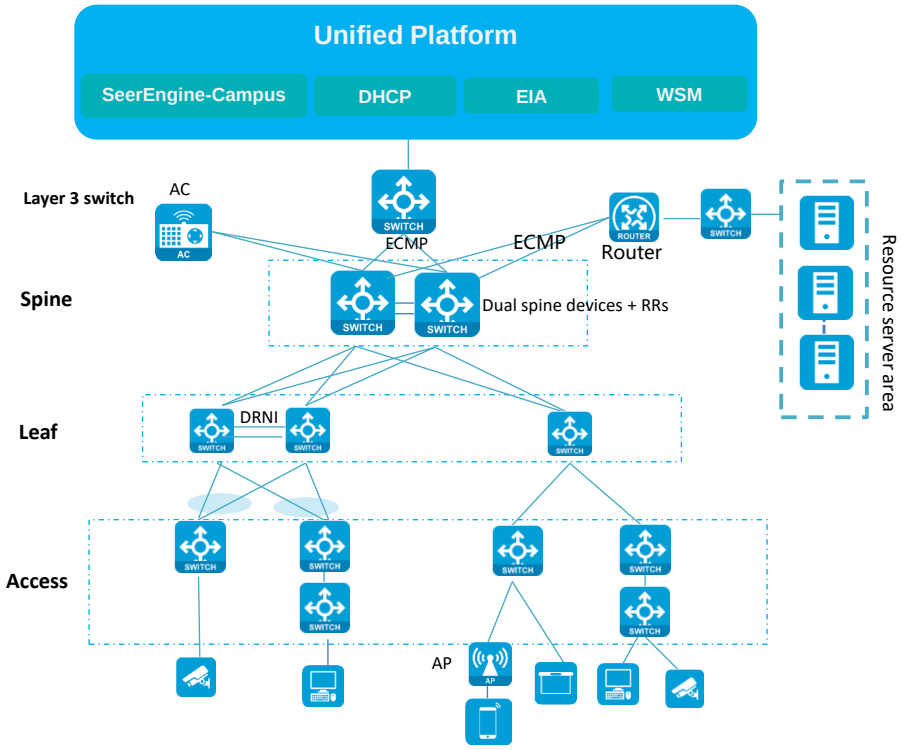
デュアルスパインネットワークモデル

スパインリーフアクセスネットワークモデル

図 1 に示すように

- スパインデバイスは、VXLAN をサポートする必要があります。主に、ルートリフレクタ(RR)およびルート転送デバイスとして機能し、異なるリーフデバイス間でルートを転送し、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。デュアルスパインネットワークは、さらに DRNI ネットワークモデルと非 DRNI ネットワークモデルに分けることができます。有線シナリオでは、デュアルスパインデバイスに DRNI 設定は必要ありません。ワイヤレス AC がスパインデバイスに接続されている場合は、スパインデバイスを使用して DR システムを形成し、AC に接続されているすべてのインターフェイスを DR インターフェイスに割り当てる必要があります。
- リーフデバイスは VXLAN をサポートする必要があります。リーフデバイスは、ユーザー認証とルート転送に使用されます。
- アクセスデバイスは AP とエンドポイントに接続され、マルチレベルのカスケードをサポートします。

図 1 スパイン-リーフ-アクセスネットワークモデルのネットワーク図



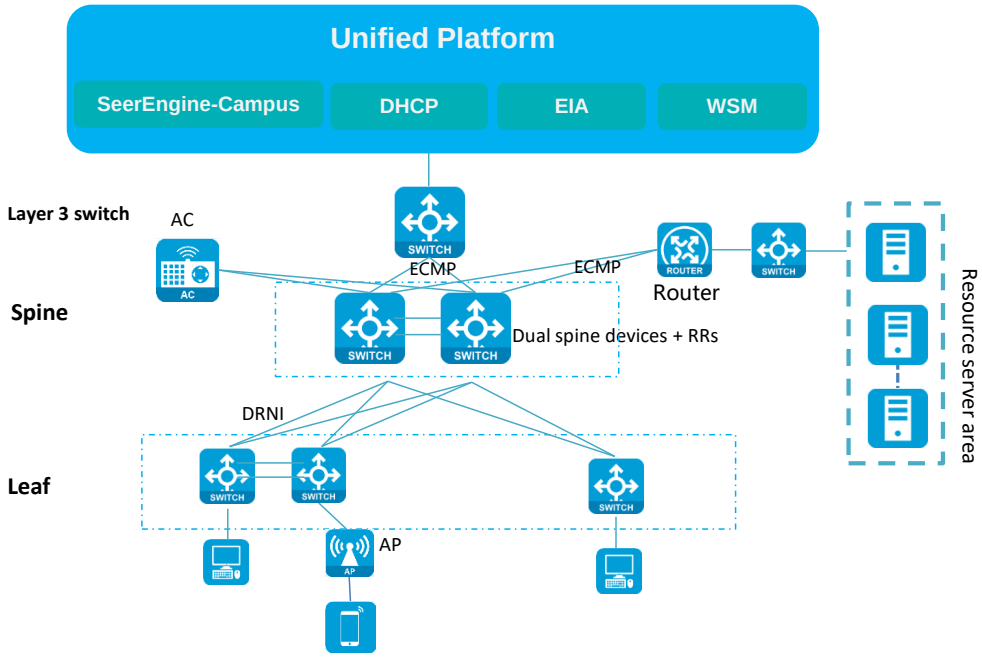
デュアルスパインのシナリオでは、スパインデバイスを手動で組み込む必要があります。詳しくは、『Configuring redundant dual-spine uplinks』または『Configuring DRNI for dual spine devices (manual)』を参照してください。

スパインリーフネットワークモデル

スパインリーフネットワークモデルは、AD-Campus ソリューションでは特別であり、スパインデバイスとリーフデバイスだけが含まれます。このモデルでは、アクセスデバイスは配置されません。無線 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を手動で設定する必要があります。

図 2 示すように、スパインデバイスは VXLAN をサポートする必要があります。スパインデバイスは主に、異なるリーフデバイス間でルートを転送するための RR およびルート転送デバイスとして機能し、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。デュアルスパインネットワークは、さらに DRNI ネットワークモデルと非 DRNI ネットワークモデルに分けることができます。有線シナリオでは、デュアルスパインデバイスに DRNI 設定は必要ありません。ワイヤレス AC がスパインデバイスに接続されている場合は、スパインデバイスを使用して DR システムを形成し、AC に接続されているすべてのインターフェイスを DR インターフェイスに割り当てる必要があります。

図 2 スパインリーフネットワークモデルのネットワーク図



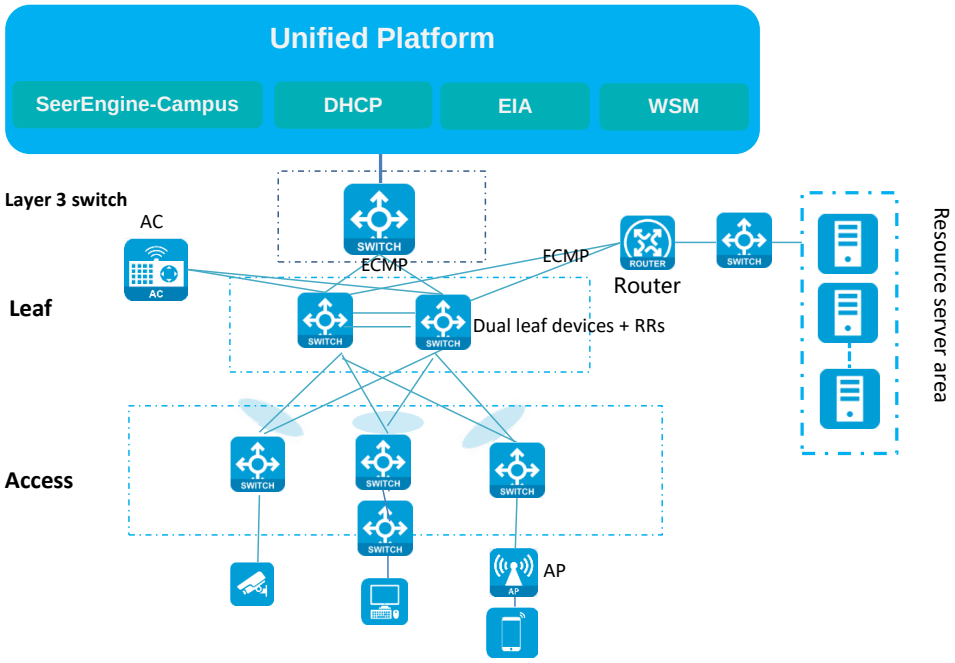
- A special network model that does not include access devices.
- APs and wired users are directly connected to leaf devices.

リーフアクセスネットワークモデル

このモデルでは、複数のアクセスデバイスがリーフデバイスに接続されます。スパインデバイスは配置されません。ネットワーク配置は単純です。このモデルは主に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、ボーダーデバイスとして様々なタイプのサーバーに通信サービスを提供します。2 つのリーフデバイスが配置されている場合は、ベストプラクティスとしてリーフデバイスを使用して DR システムを設定します。ワイヤレス AC がリーフデバイスに接続されている場合は、リーフデバイスを使用して DR システムを設定し、AC に接続されているすべてのインターフェイスを DR インターフェイスに割り当てる必要があります。

図 3 に、リーフアクセスネットワークモデルのネットワークダイアグラムを示します。

図 3 リーフアクセスネットワークモデルのネットワーク図



- The network model contains only leaf and access devices. No spine devices are deployed. This model is mainly used in small-sized networks.

IRF ネットワークモデル

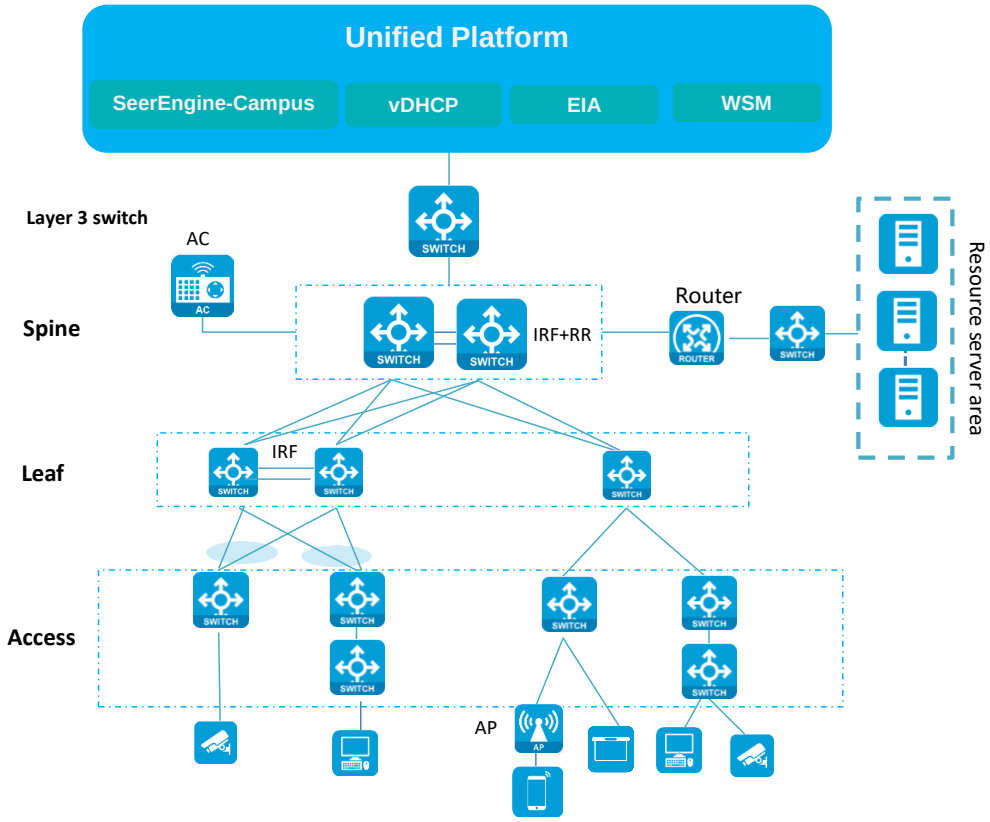
スパインリーフアクセスネットワークモデル

スパイン-リーフ-アクセスネットワークモデルには、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 ソリューションの典型的なネットワークモデルです。

- スパインデバイスは、VXLAN をサポートする必要があります。主に、異なるリーフデバイス間でルートを転送するための RR およびルート転送デバイスとして機能し、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。スパインデバイスは、スタンドアロンモードで動作することも、IRF ファブリックを形成することもできます。
- リーフデバイスは VXLAN をサポートしている必要があります。リーフデバイスは、ユーザー認証とルート転送に使用されます。
- アクセスデバイスは AP とエンドポイントに接続され、マルチレベルのカスケードをサポートします。

図 4 に、スパインリーフアクセスネットワークモデルのネットワークダイアグラムを示します。

図 4 スパインリーフアクセスネットワークモデル



- A typical campus network model that includes spine, leaf, and access devices.
- APs and wired users are connected to access devices.

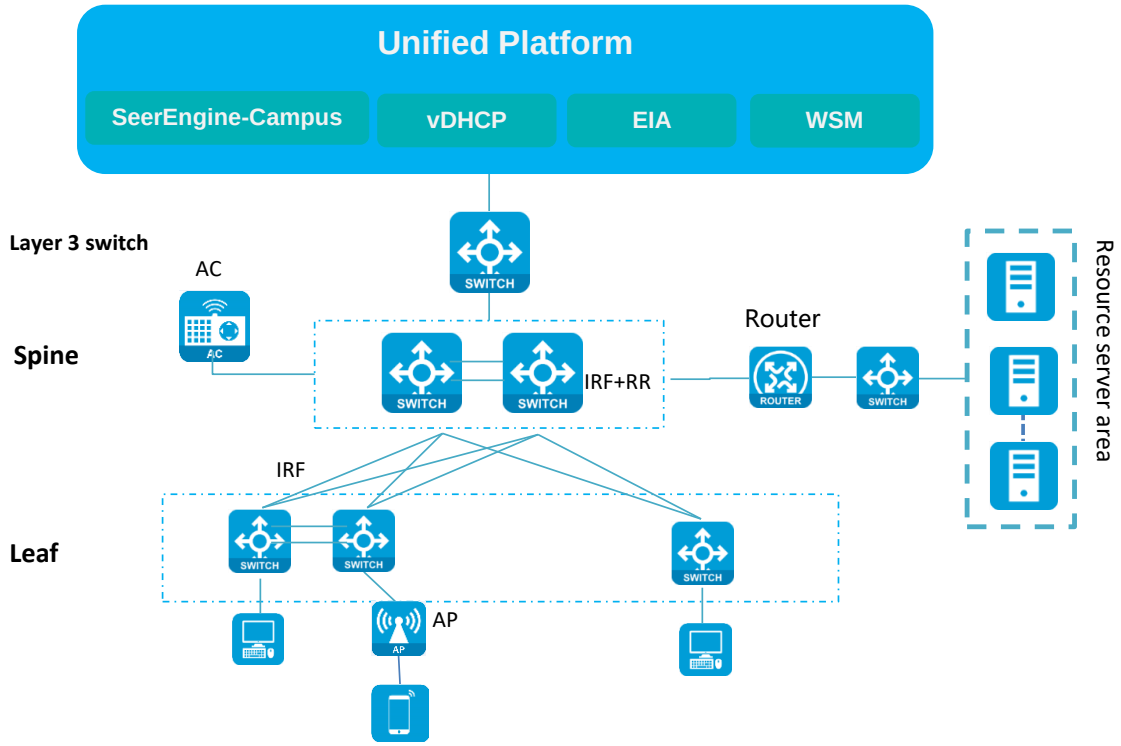
スパインリーフネットワークモデル

スパインリーフネットワークモデルは、AD-Campus ソリューションでは特別であり、スパインデバイスとリーフデバイスだけが含まれます。アクセスデバイスは配置されません。無線 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を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ます。主に、異なるリーフデバイス間でルートを転送するための RR およびルート転送デバイスとして機能し、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。スパインデバイスは、スタンドアロンモードで動作することも、IRF ファブリックを形成することもできます。

図 5 に、スパインリーフネットワークモデルのネットワークダイアグラムを示します。

図 5 スパインリーフネットワークモデル



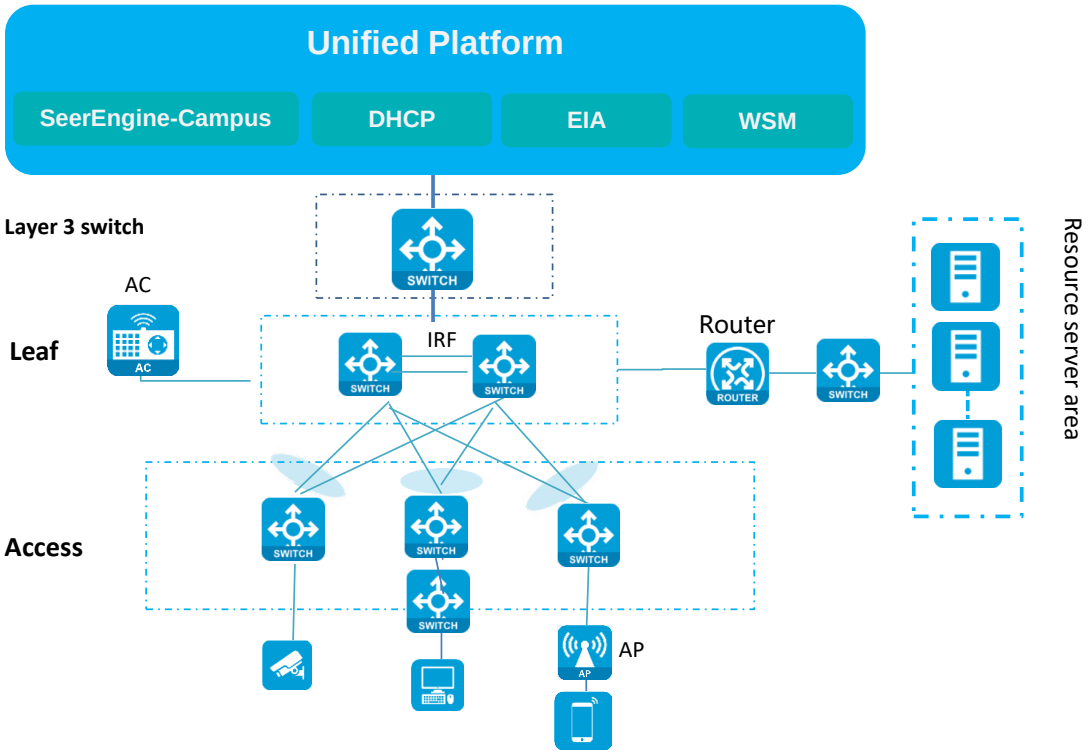
- A special network model without access devices.
- APs and wired users are directly connected to leaf devices.

リーフアクセスネットワークモデル

このモデルでは、複数のアクセスデバイスがリーフデバイスに接続されます。スパインデバイスは展開されません。ネットワーク展開は簡単です。このモデルは主に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、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。それらはスタンドアロンモードで動作することも、IRF ファブリックを形成することもできます。

図 6 に、リーフアクセスネットワークモデルのネットワークダイアグラムを示します。

図 6 リーフアクセスネットワークモデル



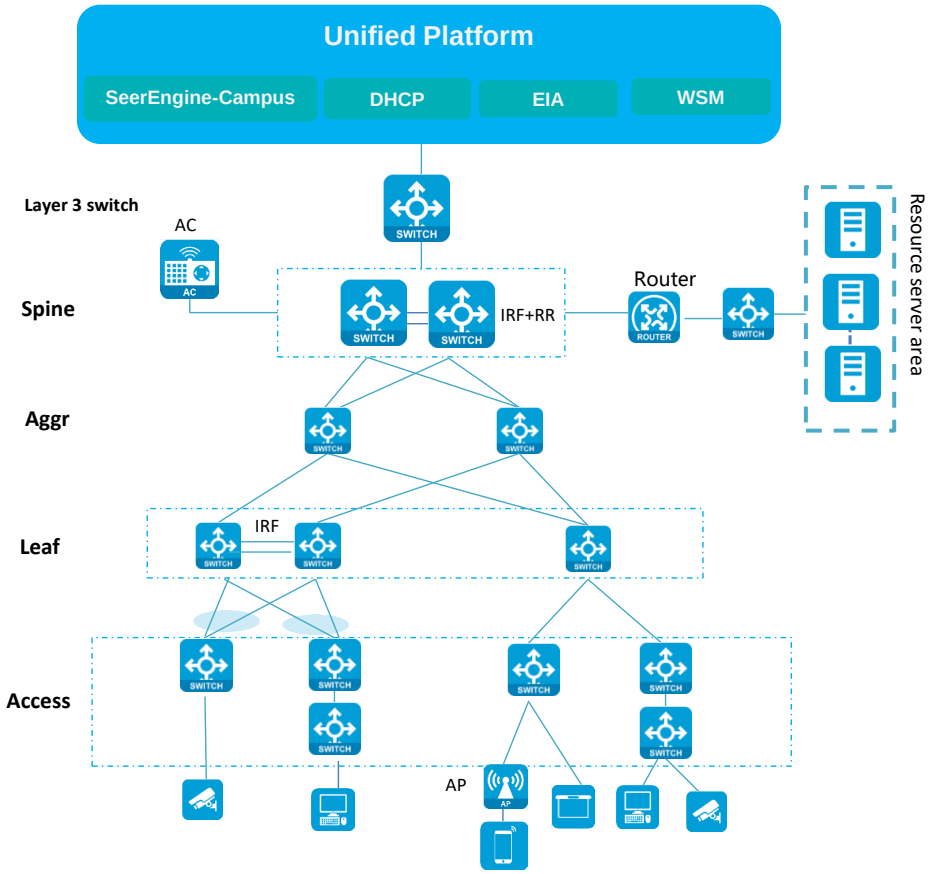
- The network model includes only leaf and access devices. No spine devices are deployed. This model is mainly used in small-sized networks.

spine-aggregation-leaf-access または spine-aggregation-leaf ネットワークモデル

図 7 に示すように:

- 標準的なスパインリーフアクセスまたはスパインリーフネットワークモデルと比較して、集約ネットワークモデルでは、スパインデバイスとリーフデバイスの間に集約レイヤー3 スイッチが追加されます。集約レイヤー3 スイッチは、VXLAN または EVPN をサポートする必要はありません。
- すべてのスパイン、リーフ、およびアクセスデバイスは、スタンドアロンモードで動作することも、IRF ファブリックを形成することもできます。
- 集約デバイスには、スパインデバイスとリーフデバイスに到達する ECMP ルートがあり、その逆も同様です。
- マルチシャーシリンク集約は、リーフデバイスとアクセスデバイスの間で形成されます。

図 7 スパイン集約リーフアクセスネットワークモデル



- In optimized automated deployment, aggregation devices can be deployed between spine and leaf devices.
- An aggregation switch is a beryllium copper Layer 3 switch, which is used only for underlay routing and forwarding. It does not need to support VXLAN or EVPN.

サーバーとネットワークデバイス間の接続

ここでは、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)をネットワークデバイスに接続するために使用するレイヤー3 ネットワーク接続方式について説明します。

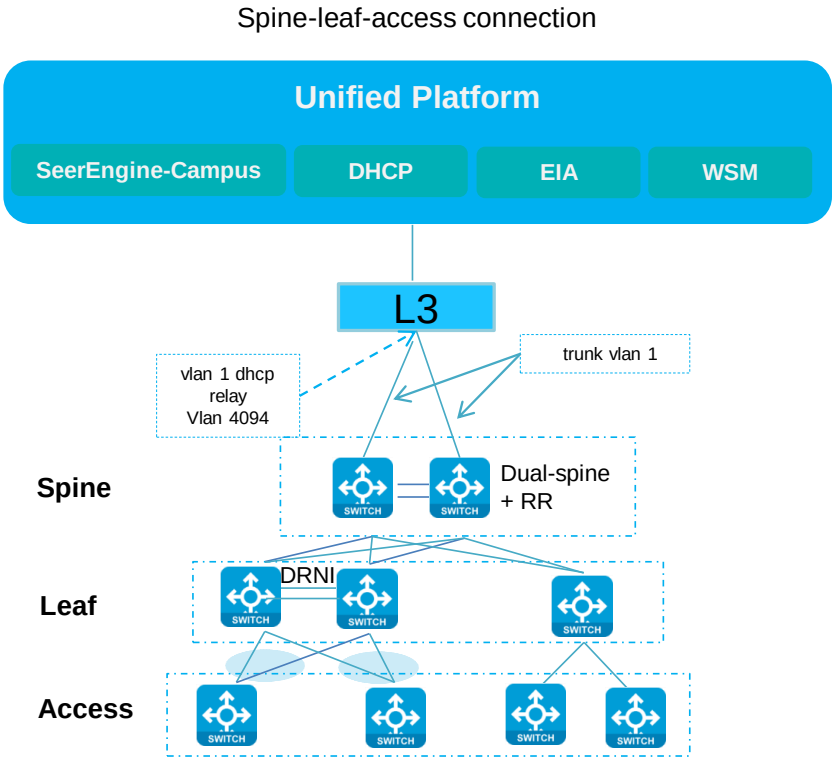
レイヤー3 ネットワーク接続方式は、コントローラーとネットワークデバイスの管理 IP アドレスが同じネットワークセグメント上にない場合に使用されます。レイヤー3 ルーティングを介して相互に到達できることを確認してください。

コントローラーはリモートエンドに配置できます(コントローラーとデバイスが同じレイヤー2 ネットワークドメインに属している必要はありません)。配置に 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 NIC を共有します。配置に 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別々の NIC を使用します。

デュアルスパインネットワーク

図 8 デュアルスパインネットワークにおけるサーバーとデバイス間の接続のネットワーク図

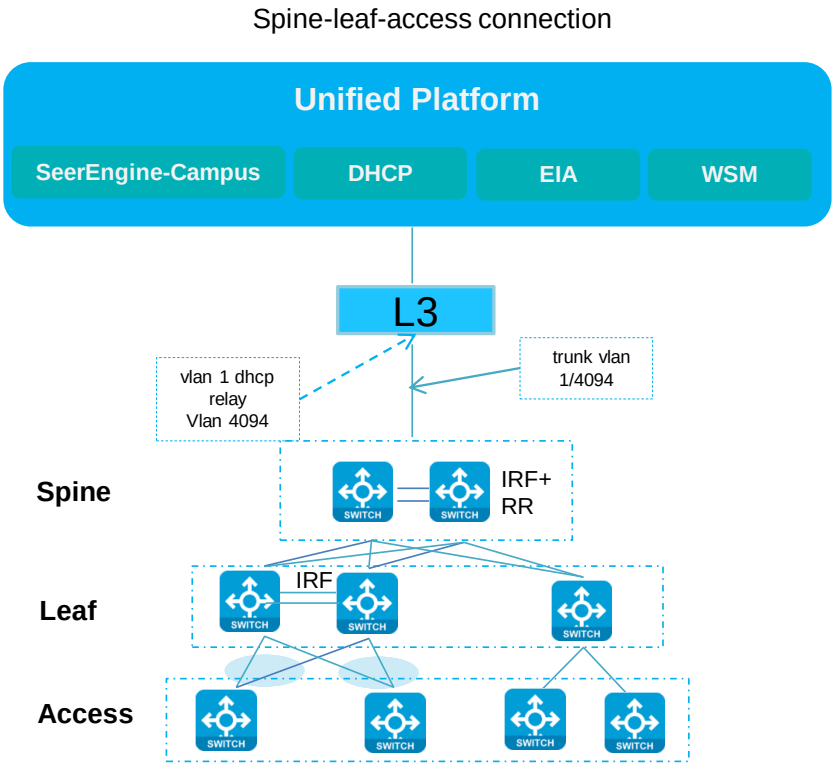
Connections between servers and devices



Spine IRF ネットワーキング

図 9 スパイン IRF ネットワーキングにおけるサーバーとデバイス間の接続のネットワーク図

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 で相互接続されます。IRF ファブリックがスパインデバイスとして動作する場合、スパインデバイスのアップリンクインターフェイスで port trunk permit vlan1 4094 コマンドを使用する必要があります。
2. スパインデバイスは VXLAN をサポートする必要があります。主に RR およびルート転送デバイスとして機能し、異なるリーフデバイス間でルートを転送し、ボーダーデバイスとしてさまざまなタイプのサーバーに通信サービスを提供します。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が互いに到達するルートを持っていることを確認する必要があるだけです。
3. リーフデバイスでは、アクセスデバイスに接続されるインターフェイスはリーフダウンリンクインターフェイスです。リーフダウンリンクインターフェイスは、ユーザー認証用の認証インターフェイスとして設定されます。ユーザーがリーフデバイスでオンラインになると、リーフデバイスはそのユーザーのリーフダウンリンクインターフェイスと VLAN ID を使用して、ユーザーが接続されているアクセスデバイス上のインターフェイスを識別します。さらに、リーフデバイスは、ユーザーのログインアカウントに従って、ユーザーを異なるユーザーセキュリティグループに割り当てることができます。
4. レイヤー2 アクセスデバイスとして動作するアクセスデバイスは、主にエンドポイントに接続されます。アクセスデバイスでは、リーフデバイスに接続されるインターフェイスはアクセスアップリンクインターフェイスです。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カスケードをサポートします。最大 3 層のカスケードがサポートされます。自動展開中にアクセスデバイス間でカスケードするには、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ーは、各エンドポイントの場所を示すために、アクセスデバイス上の各ダウンリンクインターフェイスに VLAN ID を割り当てます。VLAN ID は、VLAN ID 101 から始まり、多層カスケードアクセスデバイス上で順番に増加します。たとえば、2 層のアクセスデバイスが展開されている場合、アクセスデバイスの第 1 層のダウンリンクインターフェイスには VLAN ID 101～152 が割り当てられ、アクセスデバイスの第 2 層のダウンリンクインターフェイスには VLAN ID 153 が割り当てられます。同じリーフデバイス上の異なるリーフダウンリンクインターフェイスに接続されているアクセスデバイスの場合、各アクセスデバイス上のアクセスダウンリンクインターフェイスに割り当てられる VLAN ID は、VLAN ID 101 から始まります。
6. アクセスデバイス上のユーザーエンドポイントに接続されたインターフェイスをスパニングツリーエッジポートとして設定するには、stp edged-port コマンドを使用します。次に例を示します。

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

重要:

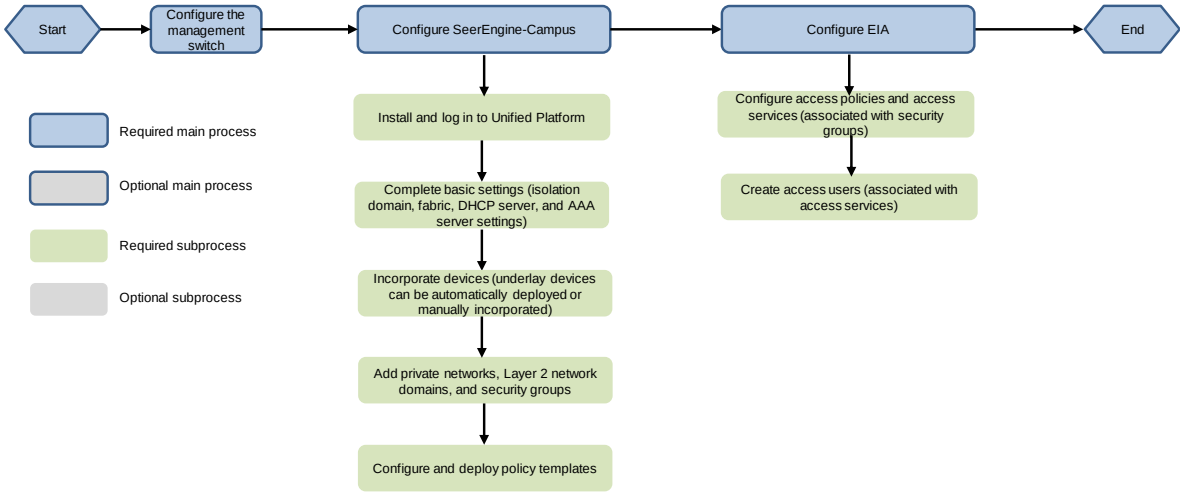
アクセスデバイスがコントローラーに組み込まれた後、コントローラーは、アクセスデバイス上のエンドポイントに接続されたインターフェイスに stp edged-port コマンドを自動的に展開します。このようなインターフェイスをエンドポイントから切断し、リーフデバイスに接続した場合、インターフェイスに展開された stp edged-port コマンドは自動的に削除できません。コマンドコンフィギュレーションを手動で削除する必要があります。

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、デバイス間の物理的な接続に関連する設定や、デバイスの自動オンボード構成または手動オンボード構成など、コントローラーがデバイスを組み込むための基礎となります。
- 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、およびセキュリティグループを作成する設定、グループポリシーおよびサービスチェーンを設定する設定など、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。

図 10 設定ワークフロー



SeerEngine キャンパス環境と EIA 環境の両方で、スタンドアロン配置とクラスタ配置がサポートされています。詳細については、『Unified Platform and Components Deployment Guide for AD-Campus 6.2 Solution』を参照してください。

注:

アンダーレイ構成では、デバイスの自動展開と手動構成がサポートされます。自動展開の詳細については、『AD-Campus 6.2 Automation Configuration Guide』または『AD-Campus 6.2 Optimized Automation Configuration Guide』を参照してください。手動構成の詳細については、『Manual incorporation』を参照してください。

ソフトウェアとハードウェアの情報

ソフトウェア情報

Table 1 ソフトウェア情報

製品	名前	機能の説明	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します。	必ず指定します。
	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。	必ず指定します。
	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。	必ず指定します。
	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、および電子メールとSMS転送サービス。	必ず指定します。
	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、およびiCC)。	必ず指定します。
	カーネル領域	階層管理。	オプション。
	ダッシュボード	大画面のフレームワークを提供します。	必ず指定します。
	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。	必ず指定します。
	Syslog	Syslog機能とログセンターを提供します。	オプション。
	ウェブソケット	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します。	必ず指定します。
キャンパスネットワークのコンポーネント	SeerEngineキャンパス	キャンパスネットワークコントローラー。基本的なキャンパスサービス設定を提供します。	必ず指定します。
	vDHCP	DHCPサーバー。自動的にオンボードされたデバイスとエンドポイントユーザーにアドレスを割り当てます。	必ず指定します。
	EIA	エンドポイントインテリジェントアクセス。ユーザー認証サービスコンフィギュレーションを提供します。	必ず指定します。
	WSM	ワイヤレスサービス管理。ワイヤレスアクセスネットワークサービスを提供します。	オプション。
	EAD	エンドポイントアドミッション防御。エンドポイントアクセスを制御および制限します。	オプション。
	EPS	エンドポイントプロファイリングシステム。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します。	オプション。

製品	名前	機能の説明	備考
	SeerAnalyzer	ネットワークデータの収集と分析をサポートします。	オプション。
	SMP	ファイアウォール管理機能を提供します。	オプション。
密結合モードをサポートするDHCPサーバー	vDHCPサーバー	H3C DHCPサーバー。	必ず指定します。
	Microsoft DHCPサーバー	密結合モードと疎結合モードをサポートします。	該当なし

ハードウェア情報

Table 2 ハードウェア情報

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
S10500X	スパイン	• リーフ • アクセス
S7500X	リーフ	• スパイン • 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	アクセス	なし
S5130-EI S 5130-HI S5130S-EI S5130S-HI	アクセス	なし

リソースと IP アドレスの計画

サーバーリソースのプランニング

サーバーとネットワークデバイス間の中間スイッチは L3 スイッチです。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ー間の接続を確保するには、中間 L3 スイッチで手動設定を行う必要があります。

ネットワークを構成する前に、ネットワークを計画する必要があります。SeerEngine キャンパスコントローラーと統合プラットフォームは、1 つの NIC を共有することも、NIC を個別に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 サービスと VLAN 4094 サービス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。

デュアルスパインアップリンクネットワーキング

SeerEngine キャンパスのコントローラーと統合プラットフォームが 1 つの NIC を共有するシナリオ

図 11 シナリオのネットワーク図

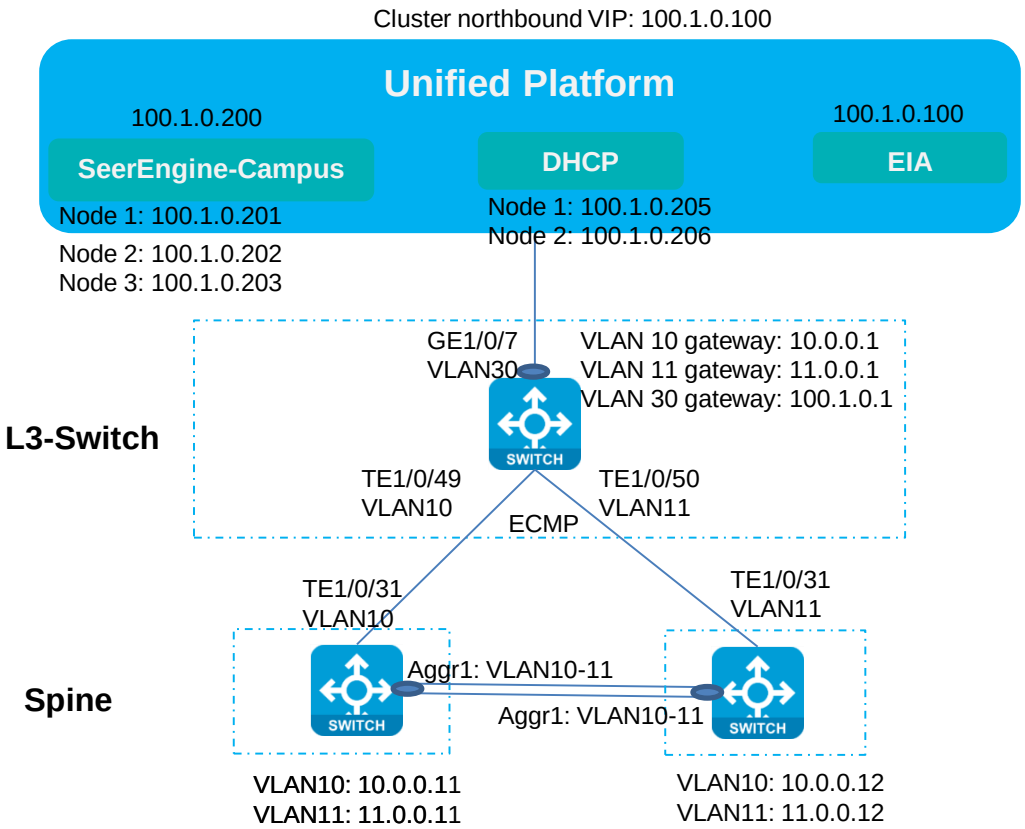


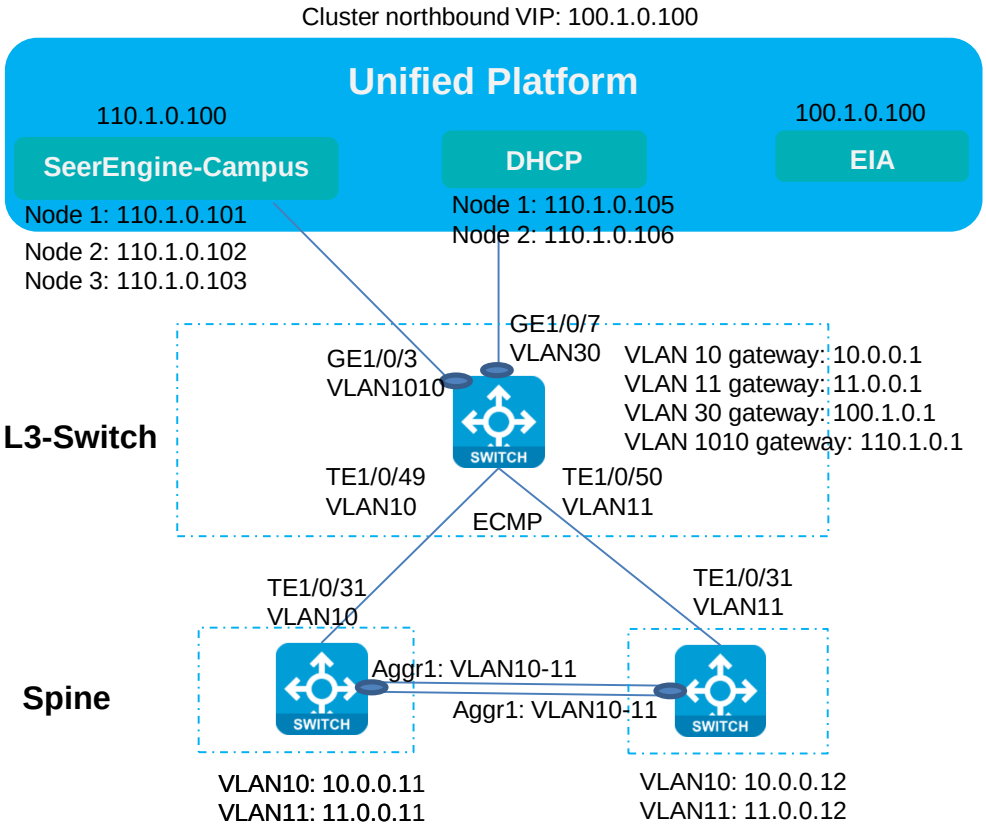
Table 3 サーバーIP および L3 スイッチネットワークセグメント計画のリスト

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)	自動展開に使用されるVLAN 1ネットワーク。

項目	例	備考
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)	コントローラーとデバイス間の通信に使用される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)	スパインデバイスとのレイヤー3通信に使用されます。
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)	スパインデバイスとのレイヤー3通信に使用されます。
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、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のIPアドレス。
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にログインするためのの IPアドレス。
EIA	100.1.0.100	EIAサーバーのIPアドレス。コンバージド展開では、EIAサーバーは Unified Platformのノースバウンドサービス IPアドレスを使用します。
SeerEngineキャンパスクラスタの IPアドレス	100.1.0.200	SeerEngineキャンパスコントローラークラスタの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キャンパスコントローラークラスタ内のノードの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(未使用)。
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サーバー上のノードのIPアドレス。
Microsoft DHCP IPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス。

SeerEngine キャンパスコントローラーと統合プラットフォームが別々の NIC を使用するシナリオ

図 12 シナリオのネットワーク図



この例では、SeerEngine キャンパスコントローラーと Unified Platform で別々の NIC が使用されています。アドレスプランニングを表 5 に示します。

表 5 サーバーIP および L3 スイッチネットワークセグメント計画のリスト

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)	自動展開に使用される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)	コントローラーとデバイス間の通信に使用される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)	スパインデバイスとのレイヤー3通信に使用されます。
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)	スパインデバイスとのレイヤー3通信に使用されます。
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がコントローラーと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NICを使用する場合に設定)。

項目	例	備考
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のIPアドレス。
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にログインするためのの IP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キャンパスコントローラークラスタの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キャンパスコントローラークラスタ内のノードの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(未使用)。
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サーバー上のノードのIPアドレス。
Microsoft DHCP IPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス。

Spine IRF アップリンクネットワーキング

SeerEngine キャンパスのコントローラーと統合プラットフォームが 1 つの NIC を共有するシナリオ

このシナリオでは、Unified Platform、SeerEngine キャンパスコントローラー、vDHCP サーバー、および EIA サーバーが、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 シナリオのネットワーク図

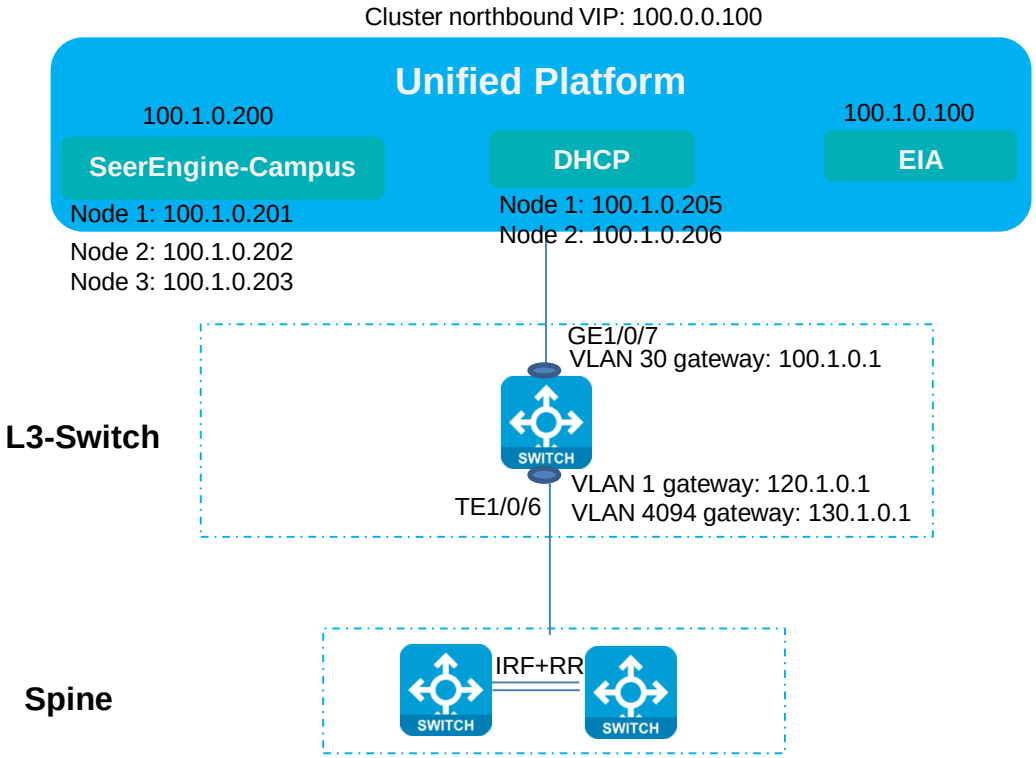


表 6 サーバーIP のリスト

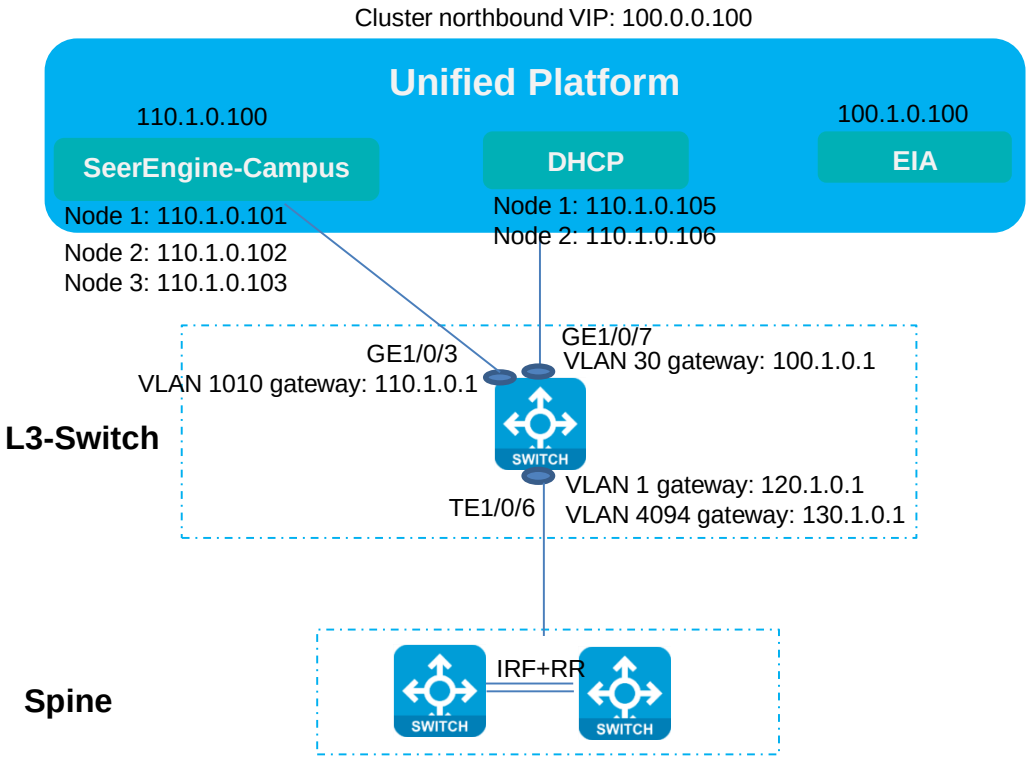
項目	例	備考
VLAN 1ネットワークセグメント(ゲートウェイ)	120.1.0.0/24(120.1.0.1)	自動展開に使用されるVLAN 1ネットワーク。
VLAN 4094ネットワークセグメント(ゲートウェイ)	130.1.0.0/24(130.1.0.1)	コントローラーとデバイス間の通信に使用されるVLAN 4094ネットワーク。
VLAN 30ネットワークセグメント(ゲートウェイ)	100.1.0.0/24(100.1.0.1)	Unified Platform、SeerEngineキャンパス、およびvDHCPで使用されるネットワークセグメント。
VLAN 91ネットワークセグメント	91.1.0.0/24	手動による組み込み中に、スパインデバイスとリーフデバイス間の通信に使用される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のIPアドレス。
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にログインするためのの IPアドレス。
EIA	100.1.0.100	EIAサーバーのIPアドレス。コンバージド展開では、EIAサーバーは Unified Platformのノースバウンドサービス IPアドレスを使用します。
SeerEngineキャンパスクラスタの	100.1.0.200	SeerEngineキャンパスコントローラ

項目	例	備考
IPアドレス		ークラスタの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キャンパスコントローラークラスタ内のノードの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(未使用)。
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サーバー上のノードのIPアドレス。
Microsoft DHCP IPアドレス	8.0.1.171	Microsoft DHCPサーバーのIPアドレス。

SeerEngine キャンパスコントローラーと統合プラットフォームが別々の NIC を使用するシナリオ

このシナリオでは、SeerEngine キャンパスコントローラーと Unified Platform は異なるネットワークセグメントの IP アドレスを使用します。EIA サーバーと Unified Platform クラスタは同じネットワークセグメントに存在し、SeerEngine キャンパスコントローラーと vDHCP サーバーは同じネットワークセグメントを共有します。

図 14 シナリオのネットワーク図



この例では、SeerEngine キャンパスコントローラーと Unified Platform で別々の NIC が使用されています。アドレスプランニングを表 7 に示します。

表 7 サーバーIP 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)	自動展開に使用される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)	コントローラーとデバイス間の通信に使用される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)	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がコントローラーと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NIC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	手動による組み込み中に、スパインデバイスとリーフデバイス間の通信に使用される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のIPアドレス。
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にログインするためのの IP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キャンパスコントローラークラスタの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キャンパスコントローラークラスタ内のノードの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(未使用)。
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サーバー上のノードのIPアドレス。
Microsoft DHCP 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

Table 4 に、ユーザーサービスのリソースプランニングを示します。

Table 4 ユーザーサービスリソースプランニング

項目	例	備考
教師セキュリティグループ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)	teacherセキュリティグループのユーザーが使用します。

項目	例	備考
BYODセキュリティグループネットワークセグメント(ゲートウェイ)	50.0.0.0/16(50.0.0.1)	BYODユーザーが使用します。
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)	ゲストユーザーが使用します。
認証に失敗した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)	ユーザー認証に失敗したユーザーが使用します。
クリティカルセグメント(ゲートウェイ)	40.0.0.0/16(40.0.0.1)	クリティカルセグメント(クリティカルVLANやVSIなど)に割り当てられたユーザーが使用します。

ユーザーVLAN プランニング

VLAN プールを使用した後で VLAN プールを変更することはできないため、事前に VLAN リソースプランニングを行う必要があります。変更には、VLAN 範囲の追加または削除、および VLAN 範囲の予約が含まれます。

次のタイプの VLAN プールがサポートされています。

- **Campus access VLAN pool**: デバイスのオンボード後に、アクセスデバイスに VLAN 設定を展開します。デフォルトの VLAN 範囲は 101～3000 です。
- **Security group VLAN pool**: ユーザーアクセスのために、隔離ドメイン内のセキュリティグループに VLAN ID を割り当てます。デフォルトの VLAN 範囲は 3501～4000 です。
- **Campus auth-free VLAN pool**: 隔離ドメイン内の認証不要エンティティに VLAN ID を割り当て、認証不要エンティティがバインドされているアクセスデバイスに VLAN 設定を展開します。デフォルトの VLAN 範囲は 4051～4060 です。
- **Wired service VLAN pool**: VLAN ネットワークタイプの分離ドメイン内の有線ユーザーに VLAN ID を割り当てます。デフォルトの VLAN 範囲は 101～3000 です。
- **Wireless service VLAN pool**: VLAN ネットワークタイプの分離ドメイン内のワイヤレスユーザーに VLAN ID を割り当てます。デフォルトの VLAN 範囲は 3501～3600 です。

制限事項およびガイドライン

SeerEngine キャンパスコントローラーは、事前定義された VLAN プールを提供します。次の prefefined VLAN プールの名前は変更できません。

- default_access。キャンパスアクセス VLAN プールです。
- default_security_group。セキュリティグループ VLAN プールです。
- default_auth_free:キャンパス認証フリーVLAN プールです。
- default_wireless。無線サービス VLAN プールです。
- default_wired。有線サービス VLAN プールです。

VLAN プールが使用された後は、その VLAN プールを変更できません。変更には、VLAN 範囲の追加または削除、および VLAN 範囲の予約が含まれます。

異なる VLAN プールの VLAN はオーバーラップできません。

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。

デフォルトでは、SeerEngine キャンパスコントローラーは、BFD MAD 用に自動的に設定された IRF ファブリックに VLAN 100 を割り当て、VLAN 4090～VLAN 4094 は予約済み VLAN です。

デフォルトでは、コントローラーは DR システム内の DR メンバーデバイスに VLAN 2 を展開して、アンダーレイルートの同期を行います。

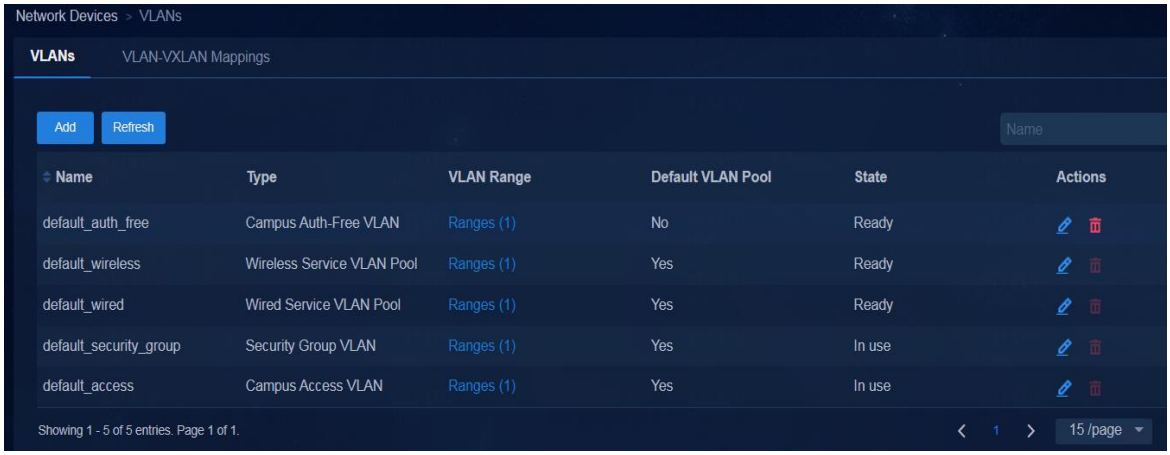
ユーザー環境を以前のバージョンからバージョン 6.2 にアップグレードすると、VLAN 構成に違いが生じる場合があります。違いを解消するには、『データの同期』をクリックします。

手順

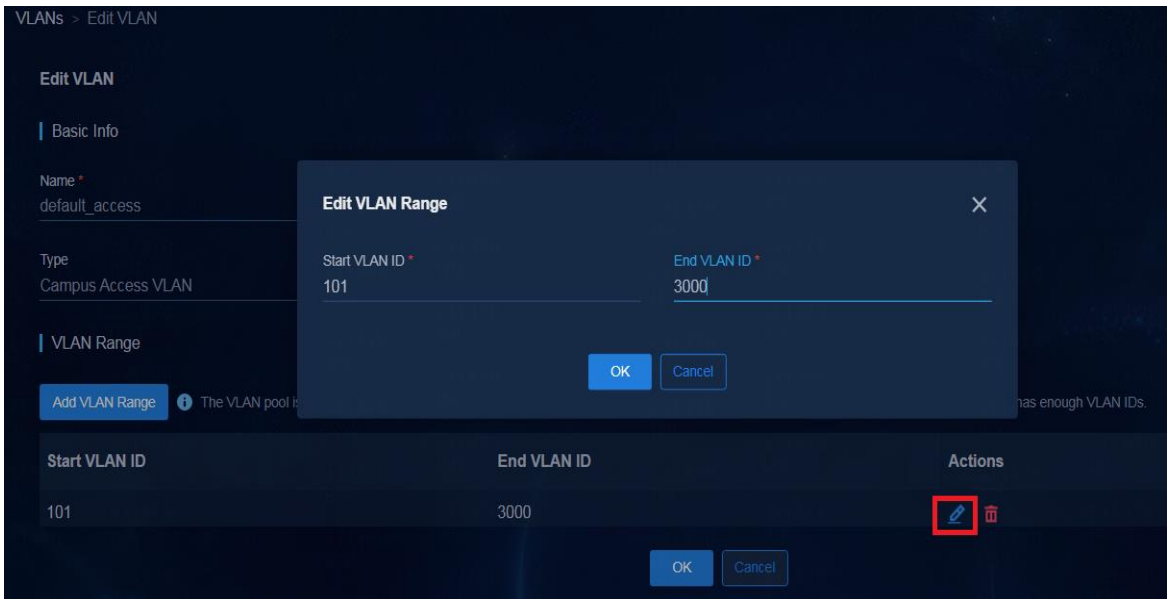
VLAN プールを設定し、システム内のすべての VLAN プールに関する情報を表示するには、次の手順を実行します。

1. **Automation** > **Campus Network** > **Devices** ページに移動します。
2. ページの右上隅にある **VNID Pools** をクリックします。
3. **VLANs** タブをクリックして、**VLANs** ページを開きます。

図 15 VLANs ページ



VLAN プールの VLAN 範囲を調整するには、VLAN プールの **Actions** カラムにある **Edit** アイコンをクリックします。**VLAN Range** 領域で、VLAN 範囲の **Actions** カラムにある **Edit** アイコンをクリックして、VLAN 範囲を変更します。

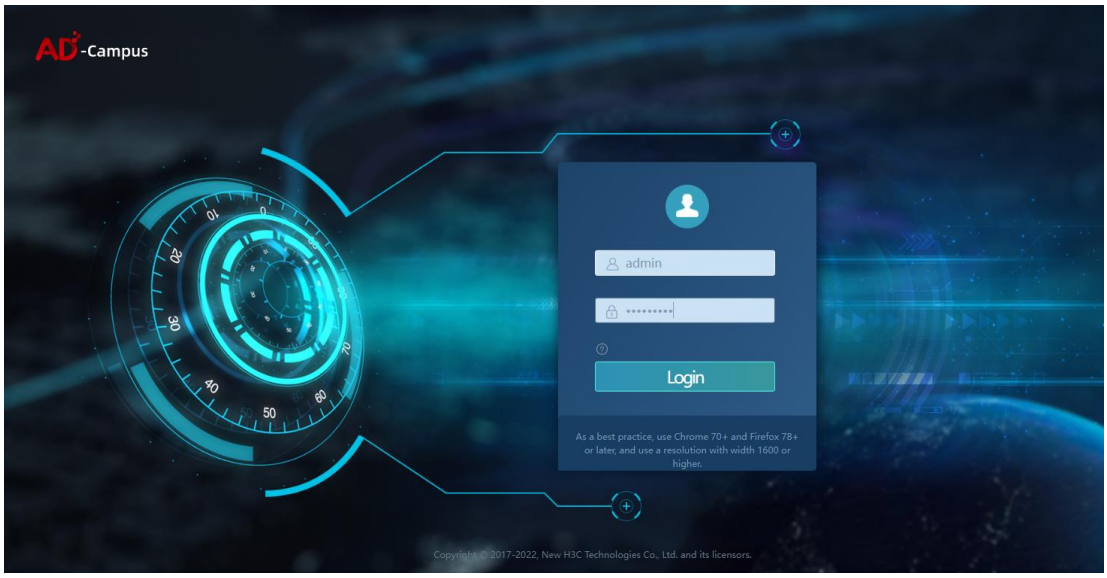


AD-Campus の設定

AD-Campusコントローラーへのログイン

1. 0 インストールと展開が完了したら、に示すように、ブラウザのアドレスバーにコントローラーのログインアドレスを入力して、AD-Campus コントローラーのログインページを開きます。ログインアドレスの形式は、central-ip:30000/http://login です。ログイン IP は、Unified Platform クラスタのノースバウンドサービス VIP です。この例では、ログイン IP は 100. 1.0.100 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。

図 16 ログインページ

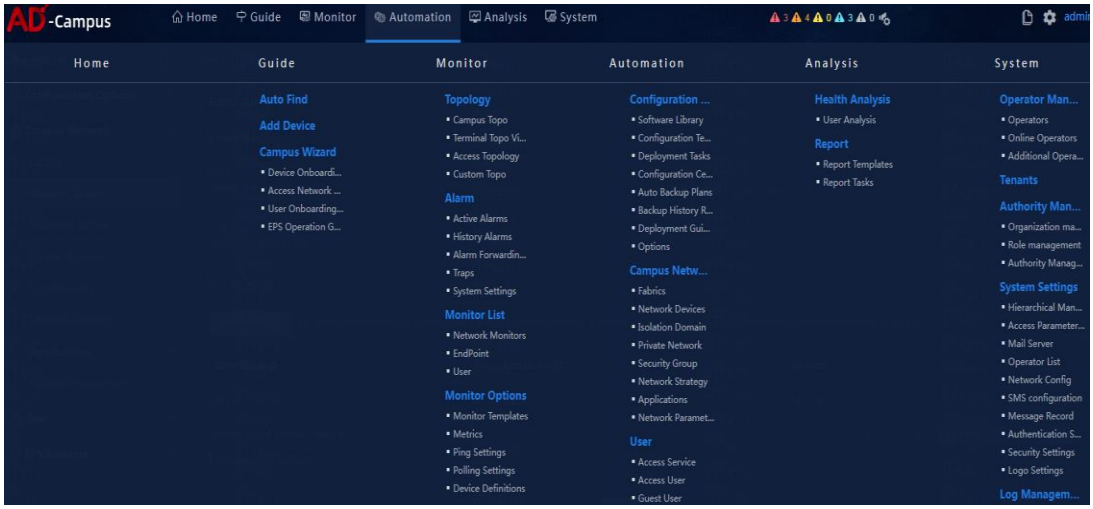


2. 図 17 に示すようにユーザー名とパスワードを入力し、Login をクリックして AD-Campus コントローラーにログインします。

図 17 ホームページ

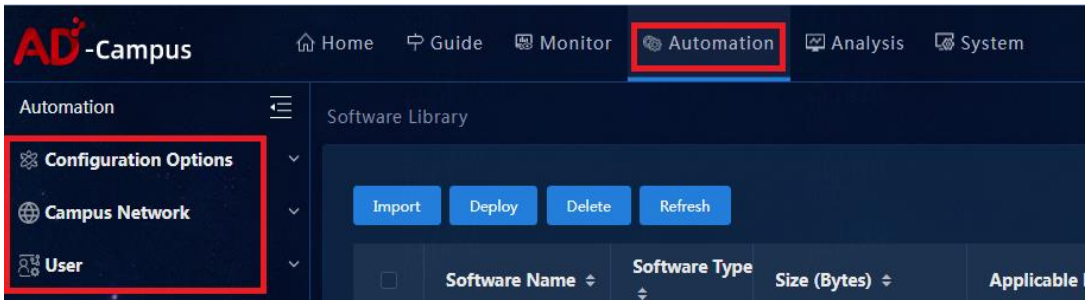
3. 図 18 に示すようにページの左上にあるアイコン  をクリックすると、すべてのメニューが表示されます。

図 18 すべてのメニューの表示



4. 自動化モジュールは、キャンパスネットワークサービスを設定するために使用されます。図 19 に示すように、上部ナビゲーションバーの **Automation** 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展開します。
   - **Configuration Options**: デバイスのバックアップ、構成の復元、ソフトウェアライブラリなど、サービスの設定を構成します。
   - **Campus Network**: 主に、SeerEngine キャンパスコントローラーサービスに関連する設定メニューを提供します。これには、デバイスオンボーディング用の自動テンプレートの作成、および分離されたドメイン、ファブリック、セキュリティグループ、ユーザーグループポリシー、およびサービスチェーンの設定が含まれます。
   - **User:** アクセスサービス、アクセスポリシー、およびアクセスユーザーの設定を含む、EIA 認証サーバーのサービス設定メニュー。

図 19 Automation メニューのオプション



ライセンスの登録

このタスクについて

コントローラー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 Unified Platform 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、正式なライセンスを登録することも、試用ライセンスを使用することもできます。

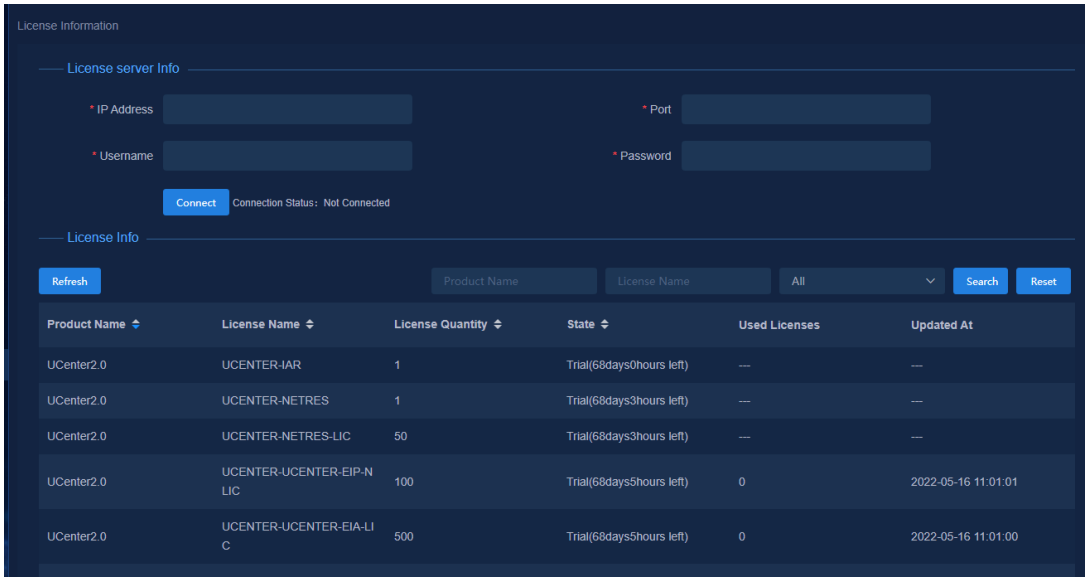
ここでは、AD-Campus コントローラーの Web インターフェイスでのライセンス登録についてのみ説明します。ライセンスサーバーのセットアップと設定の詳細については、ライセンスサーバーのマニュアルを参照してください。

手順

1. **System** > **License Management** > **License Info** ページに移動します。

   システムをインストールして展開すると、図 20 に示すように、デフォルトで試用ライセンスが使用可能になります。

   図 20 ライセンスサーバー情報



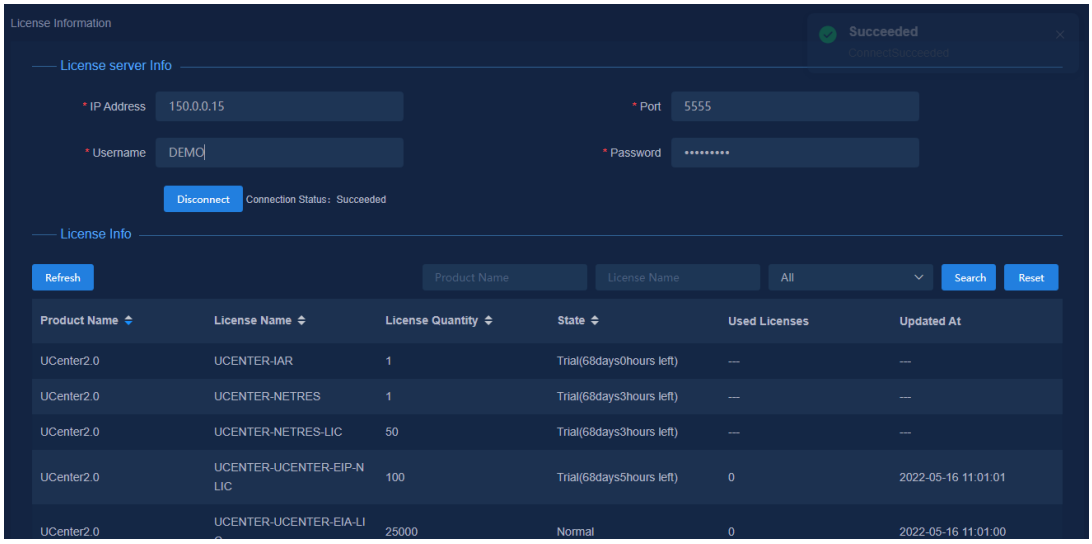
2. ライセンスサーバー情報領域で、ライセンスサーバーのパラメーターを設定します。

   パラメーター:

   - **IP Address**: ライセンスサーバーの IP アドレスを入力します。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てください。
   - **Port**: ポート番号(この例では 5555)を入力します。
   - **Username**: ライセンスサーバーへのアクセスに使用するユーザー名を入力します(この例では **DEMO**)。
   - **Password**: ライセンスサーバーへのアクセスに使用するパスワードを入力します(この例では **admin@123**)。

3. **Connect** をクリックします。システムがライセンスサーバーに正常に接続すると、図 21 に示すように、ライセンス情報ページに使用可能なライセンスが表示されます。

図 21 ライセンス情報



前提条件

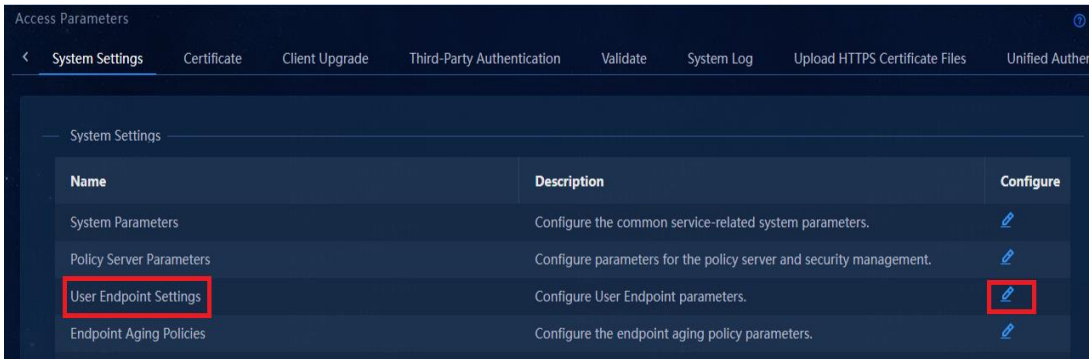
構成ウィザードを使用する前に、ユーザーエンドポイント、認証サーバー、および DHCP サーバーの設定を構成する必要があります。

ユーザーエンドポイント設定の構成

ユーザー認証サーバーで VXLAN ネットワーキングを有効にするようにユーザーエンドポイント設定を構成するには、次の手順を実行します。

1. **Automation** > **User** > **Service Parameters** > **Access Parameters** > **System Settings** ページに移動します(図 22 を参照)。

図 22 ユーザーエンドポイント設定の構成



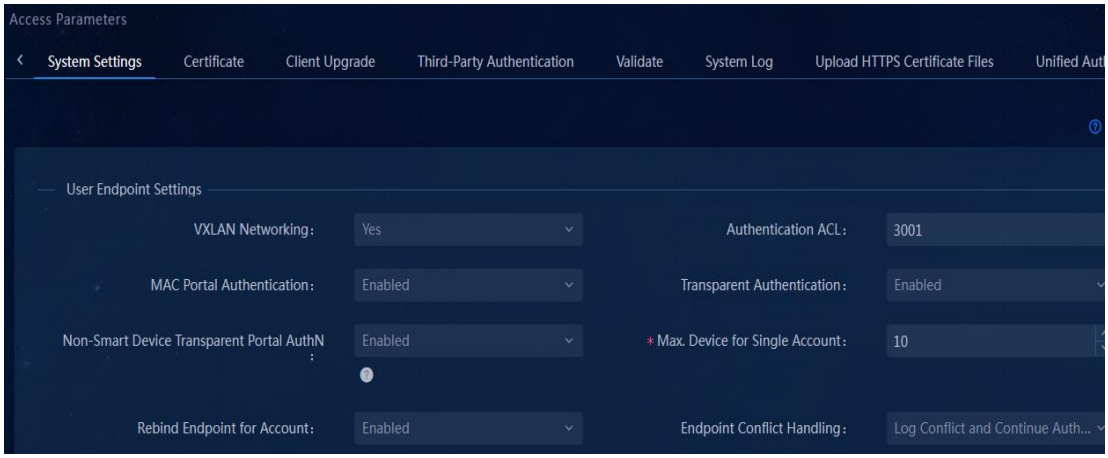
2. 図 23 に示すように、**User Endpoint Settings** という名前のテンプレートの **Configure** カラムにある **Edit** アイコンをクリックして、ユーザーエンドポイント設定ページにアクセスします。**User Endpoint Settings** 領域と **Director Controller Configuration** 領域でパラメーターを設定します。

   User Endpoint Settings 領域のパラメーター:

   - **VXLAN Networking**: **Yes** を選択します。
   - **MAC Portal Authentication**: **Enabled** を選択します。
   - **Transparent Authentication**: **Enabled** を選択します。

- **Unbind IP for Duplicate Account**: デフォルトでは、値は **No** です。
  - IP プリエンプションをディセーブルにするには、**No** を選択します。1 つのエンドポイントがオフラインになると、そのバインドされた IP アドレスは、オンラインになることを要求する別のエンドポイントにバインドできなくなります。
  - IP プリエンプションをイネーブルにするには、**Yes** を選択します。1 つのエンドポイントがオフラインになった後、そのバインドされた IP アドレスを、オンラインになることを要求する別のエンドポイントにバインドできます。
- **Max. Device for Single Account:** 1 つのアカウントを使用してオンラインになることができるエンドポイントの最大数を設定します。デフォルトの数は 10 です。たとえば、このフィールドを 10 に設定すると、最大 10 のエンドポイントがこのアカウントを使用してオンラインになることができます。

図 23 ユーザーエンドポイント設定の構成



Director Controller Configuration 領域のパラメーター:

Embedded Controller: デフォルトでは、値は **Yes** です。SeerEngine キャンパスコントローラーと EIA が同じプラットフォームにデプロイされている場合は、**Yes** を選択します。パラメーターを手動で構成する必要はありません。No を選択した場合は、次のパラメーターを構成します。

- **IP Address**: SeerEngine キャンパスコントローラーへのログインに使用するアドレスを入力します。
- **Port**: Unified Platform にログインするためのポート番号を入力します。この例では、ポート番号は 30000 です。
- **Username/Password**: ユーザー名とパスワードを入力します。デフォルトでは、ユーザー名は **admin**、パスワードは **Pwd@12345** です。
- **Protocol**: Unified Platform のデプロイ時に設定されたプロトコルに従って、**HTTP** または **HTTPS** を選択します。デフォルトでは、HTTP が使用されます。

図 24 コントローラーの設定

AAA サーバーの設定

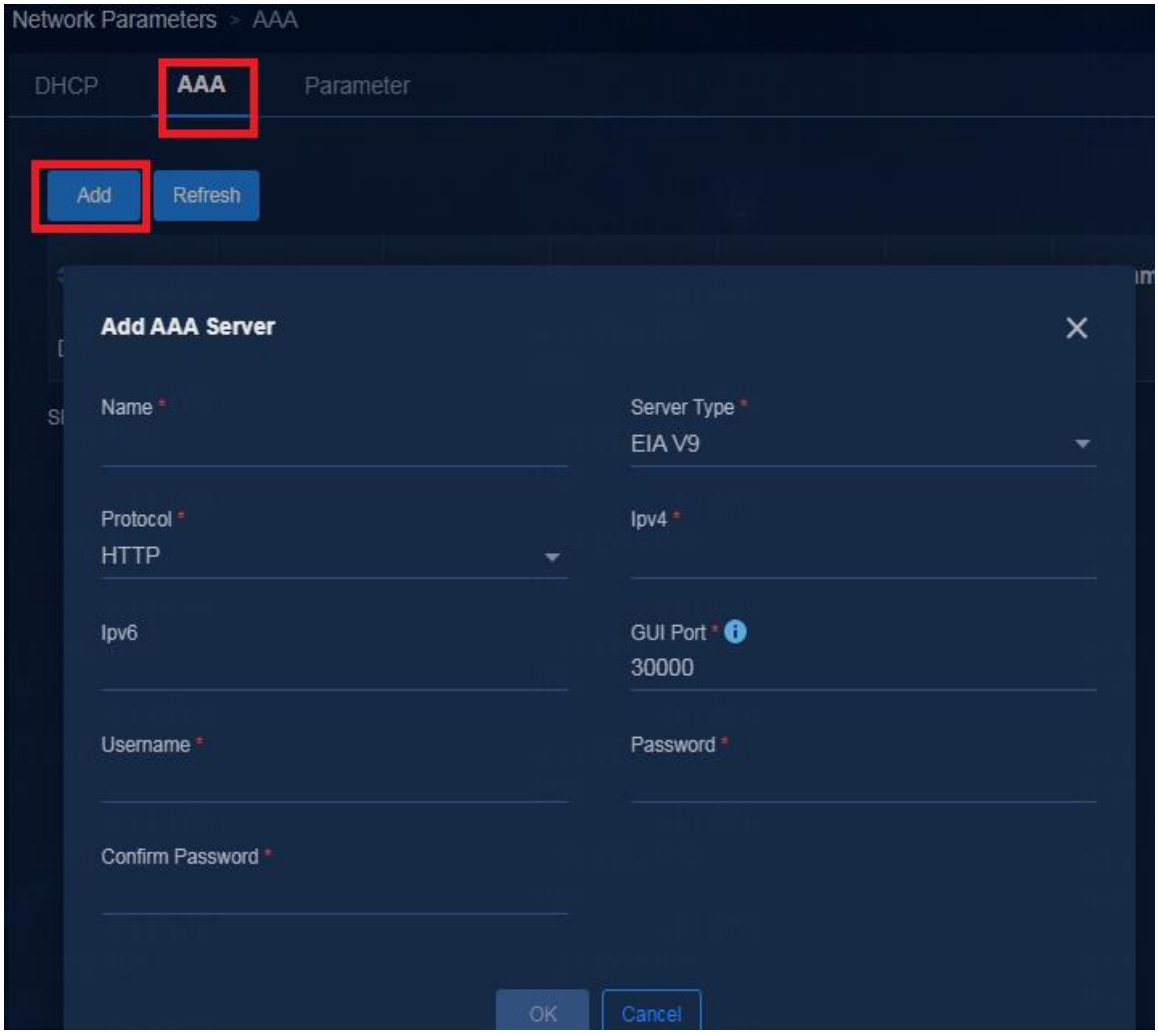
サポートされる AAA サーバーには、H3C EIA V7(iMC EIA)、EIA V9(コンテナ化された EIA)、およびサードパーティの認証サーバーがあります。

AAA サーバーを追加するには、**Automation** > **Campus Network** > **Network Parameters** > **AAA** ページに移動し、**Add** をクリックします。

パラメーター:

- **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**:
  - **EIA V9**: 統合プラットフォームに展開された EIA サーバー。これは EIA クラスタです。EIA 階層展開は、現在のソフトウェアバージョンではサポートされていません。
  - **EIA V7**: iMC プラットフォームにデプロイされた EIA サーバー。EIA 階層デプロイメントがサポートされています。
  - サードパーティ認証:MAC ポータル認証用のインターフェイスを提供するために使用されます。
- **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。デフォルトでは、HTTP です。
- **Ipv4**: EIA サーバーの IP アドレスを入力します。
- **GUI Port**: 選択したサーバータイプに応じて、このフィールドに自動的に値が入力されます。
- **Username**: 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。

図 25 AAA サーバーの追加



EIA V9

EIA V9 では、コンテナ化された展開が使用されます。EIA コンポーネントを Unified Platform クラスタ環境に展開すると、システムは自動的にコンポーネントを **Default EIA** という名前で AAA サーバーリストに追加します。

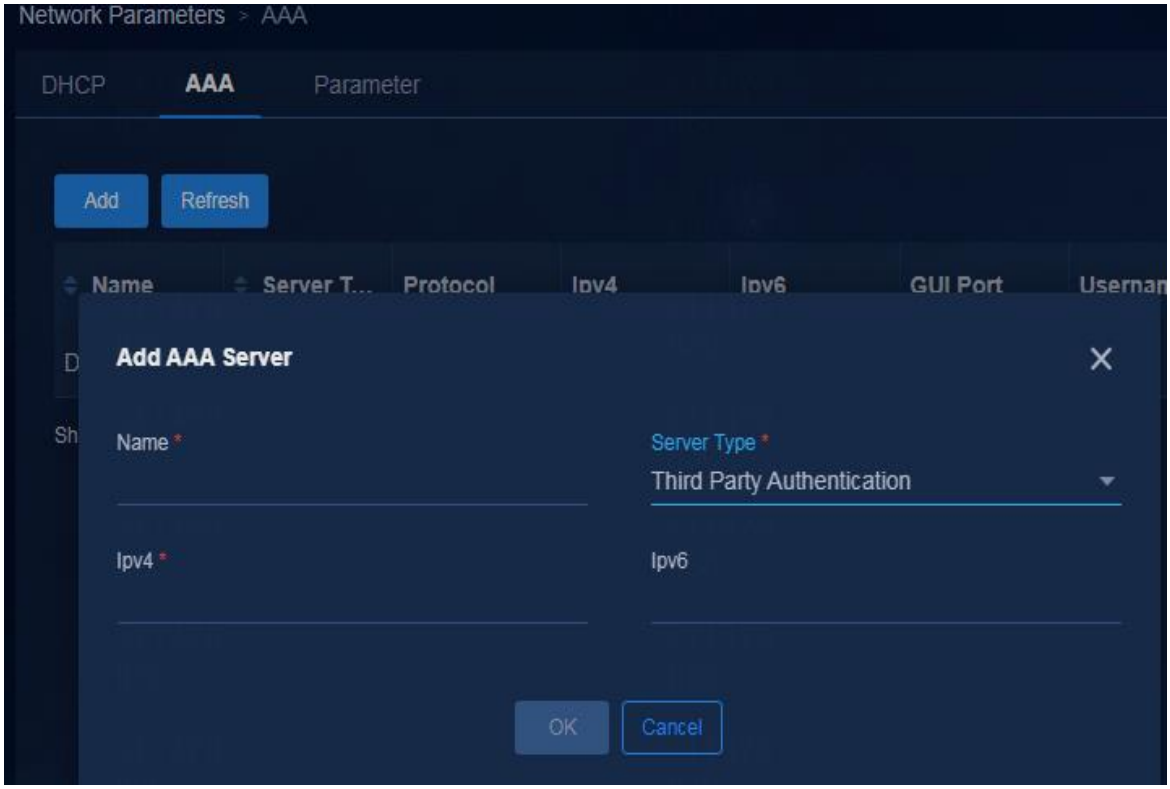
EIA V7

EIA V7 サーバーは、Windows または Linux オペレーティングシステム(OS)に基づく 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。

- **Single-host mode**: Windows または Linux OS を使用する物理サーバーまたは VM が必要です。
- **Cluster mode**: 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 台のサーバーは、ステートフルフェイルオーバークラスタを形成します。
- **Hierarchical deployment mode**: 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。現在、階層型配置モードをサポートしているのは EIA V7 のみです。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。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は、バージョン 5.7 を使用してください。

サードパーティ認証

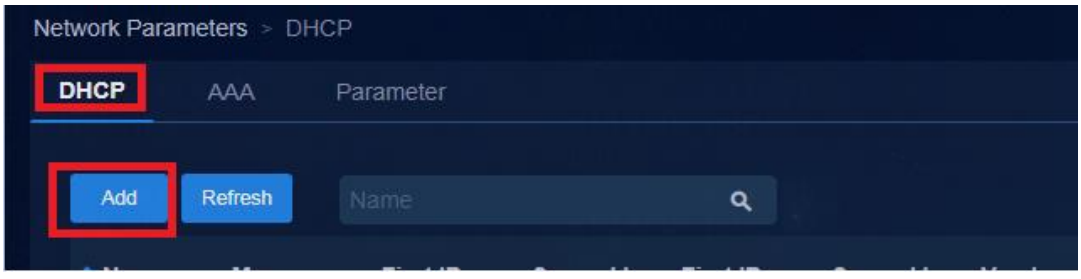
Web ポータル認証には、サードパーティ認証サーバーが使用されます。SeerEngine キャンパスコントローラーでサードパーティサーバーの IP アドレスを設定し、サードパーティ認証サーバーとユーザークセスデバイスが相互に到達できることを確認するだけです。



DHCP サーバー設定の構成

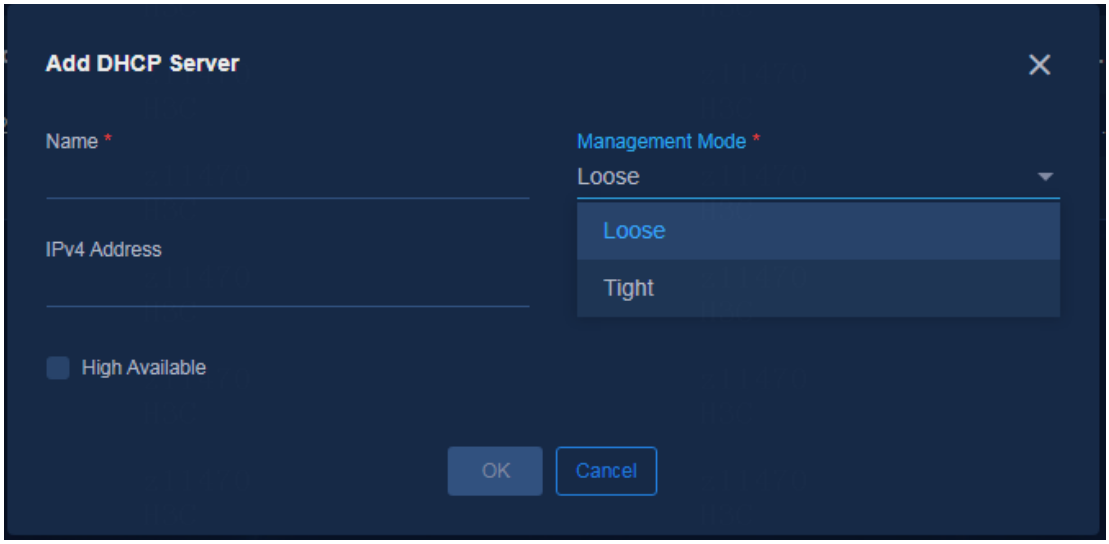
1. **Automation** > **Campus Network** > **Network Parameters** > **DHCP** ページに移動します。
2. **Add** をクリックします。

図 26 DHCP サーバーの追加



3. **Add DHCP Sever** ページで、**Management Mod** に **Tight** または **Loose** を選択します。

図 27 管理モードの選択



密結合

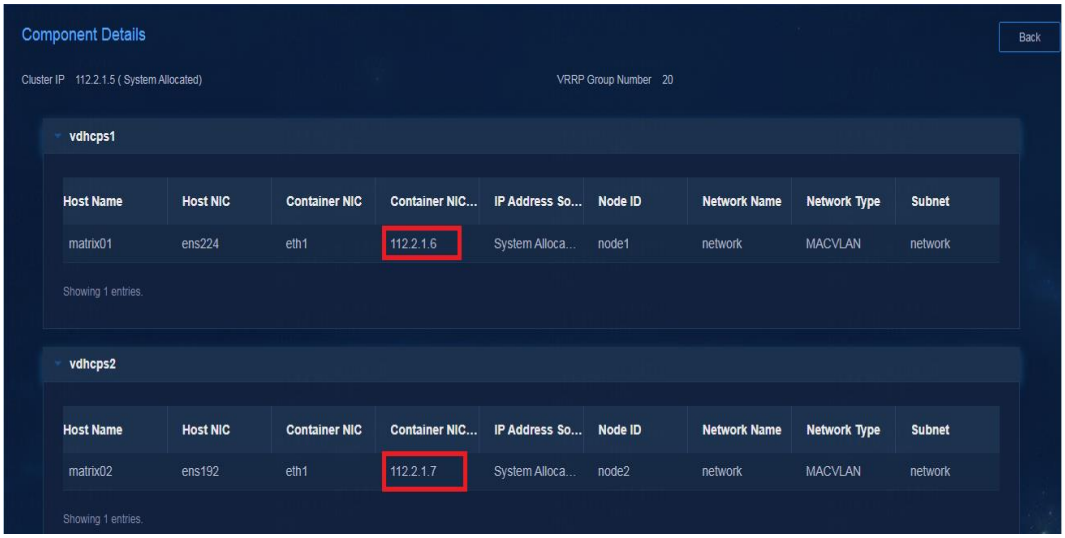
H3C vDHCP サーバーと Microsoft DHCP サーバーは、密結合をサポートしています。

密結合モードでは、SeerEngine キャンパスコントローラーは、ページで設定された IP アドレスセグメントに従って IP アドレスプールを作成するよう DHCP サーバーに要求します。IP アドレスバインディングはサポートされています。

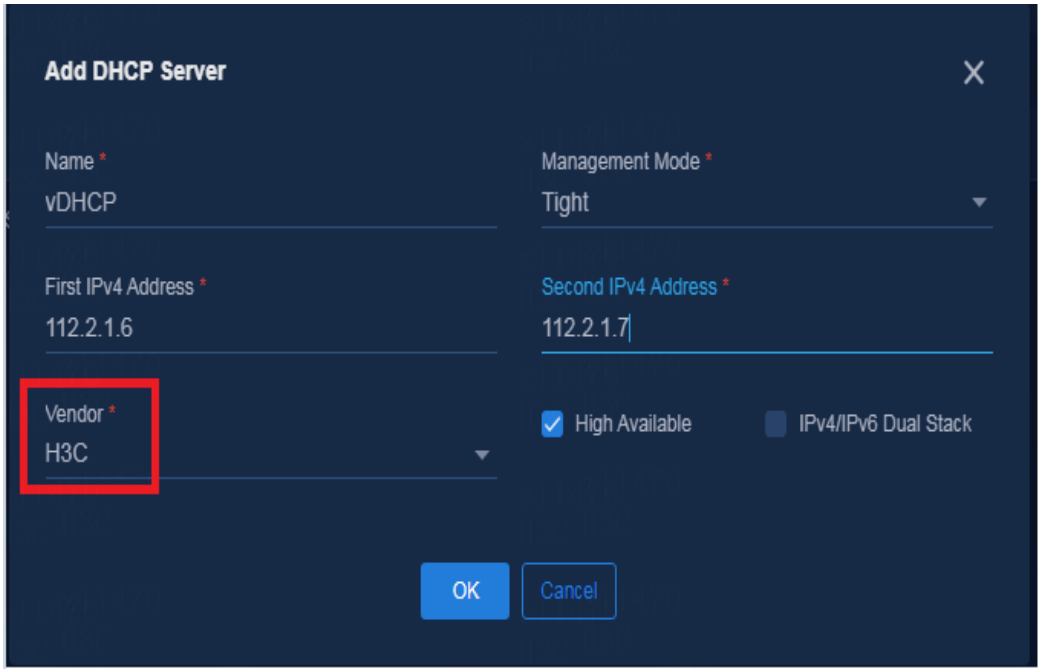
自動デバイス展開の場合、DHCP サーバーは H3C vDHCP サーバーである必要があります。

vDHCP サーバーの追加

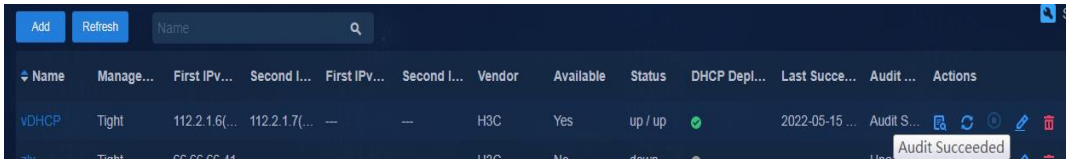
1. **DHCP** タブで次のパラメーターを設定し、設定が完了したら **OK** をクリックします。
   - **Management Mode**: **Tight** を選択します。vDHCP サーバーは、密結合のみをサポートします。
   - **High Availability**: クラスタモードでこのオプションを選択します。スタンドアロンモードでは、このオプションを選択する必要はありません。
   - **IPv4/IPv6 Dual Stack**: IPv6 自動展開またはユーザーIPv6 サービスが使用可能な場合は、このオプションを選択します。設定の詳細については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。
   - **IPv4/IPv6 Address**: vDHCP サーバーの展開時に割り当てられたアドレスを入力します。IP アドレスを取得するには、**System** > **Deployment Management** ページに移動し、**Public Service** 項目を展開して vDHCP deployment ページにアクセスし、アイコンをクリックして詳細を表示します。



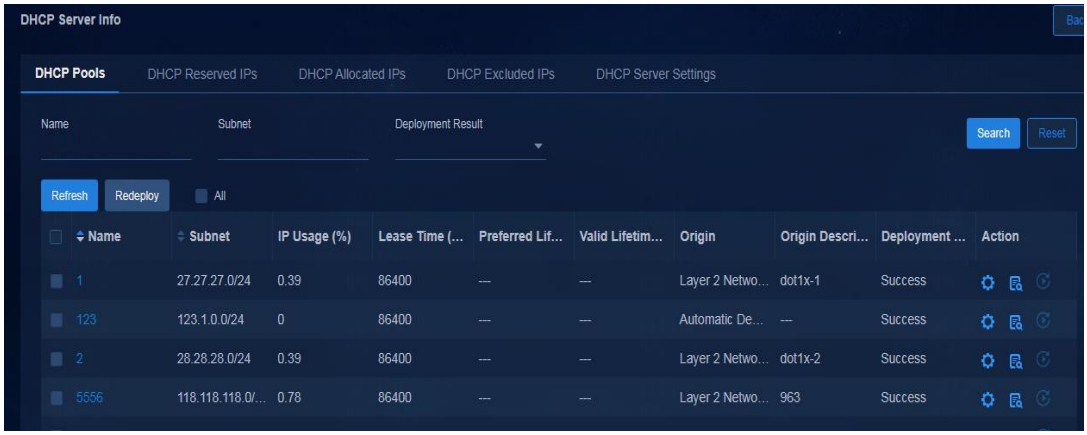
- **Vendor**: **H3C** を選択します。



2. DHCP サーバーを追加した後、**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 Succeeded** と表示されます。

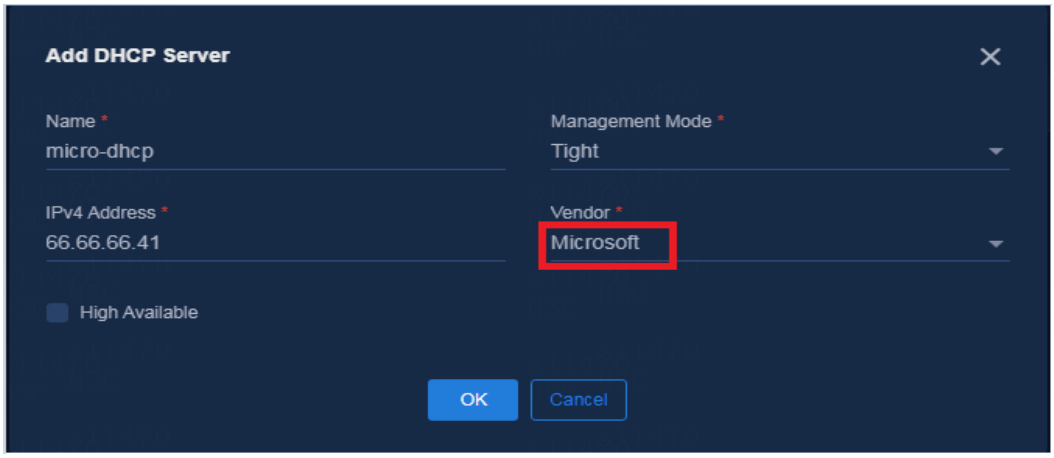


3. DHCP サーバーのアドレスプールおよび IP アドレス割り当て情報を表示するには、DHCP サーバーの名前をクリックします。

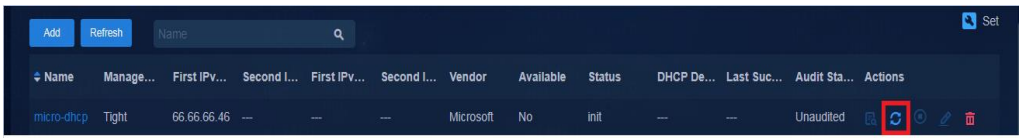


Microsoft DHCP サーバーの追加

1. DHCP サーバーを追加します。
   a. **Add DHCP Server** ページで、**Vendor** 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**: アクティブ/スタンバイ環境の Microsoft DHCP HA に対して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 Address**: Microsoft DHCP サーバーの IP アドレスを入力します。HA 環境では、2 つの 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、**Action** 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 Succeeded** と表示されます。
   c. Microsoft DHCP HA ステータスを監視するには、DHCP サーバーリストページの右上隅にあるアイコン 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ーは、DHCP HA ステータスを定期的に監視します。コントローラーは、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。

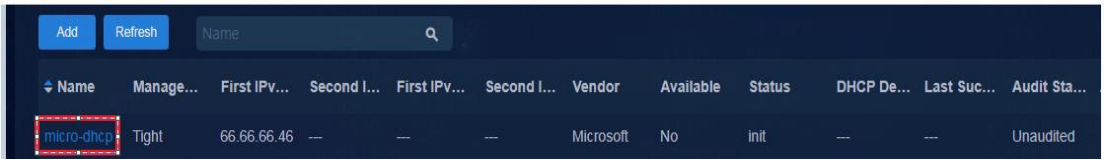


2. VXLAN 4094 アドレスプールを設定します。

重要:

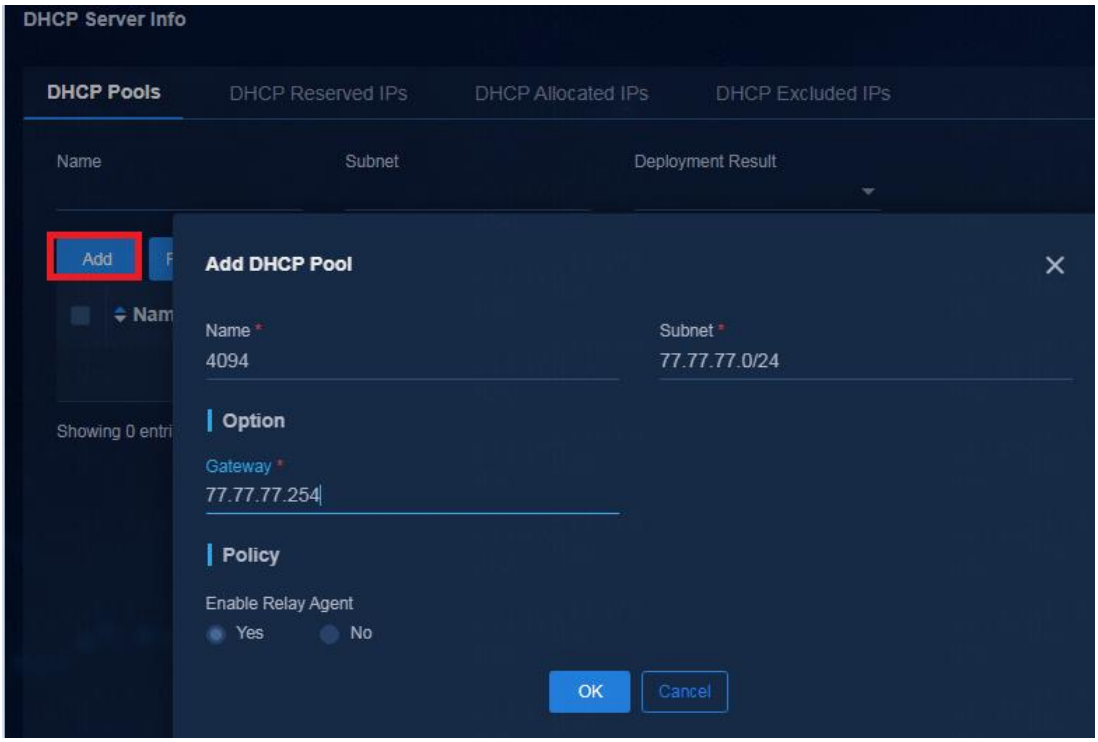
Microsoft DHCP サーバーを追加した後、SeerEngine キャンパスコントローラーにアドレスプールを手動で作成する必要があります。アドレスプールがデバイス上の VXLAN 4094 と同じネットワーク上にあることを確認してください。このようなアドレスプールを作成しない場合、Microsoft DHCP サーバーはリーフデバイスから送信された DHCP 要求に応答できません。

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、次のパラメーターを設定します。

- **Subnet** ト: 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。

疎結合

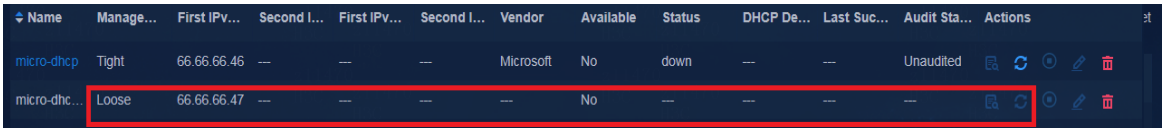
Microsoft DHCP サーバーと WRD DHCP サーバーは、疎結合をサポートしています。

疎結合モードでは、SeerEngine キャンパスコントローラーは 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。

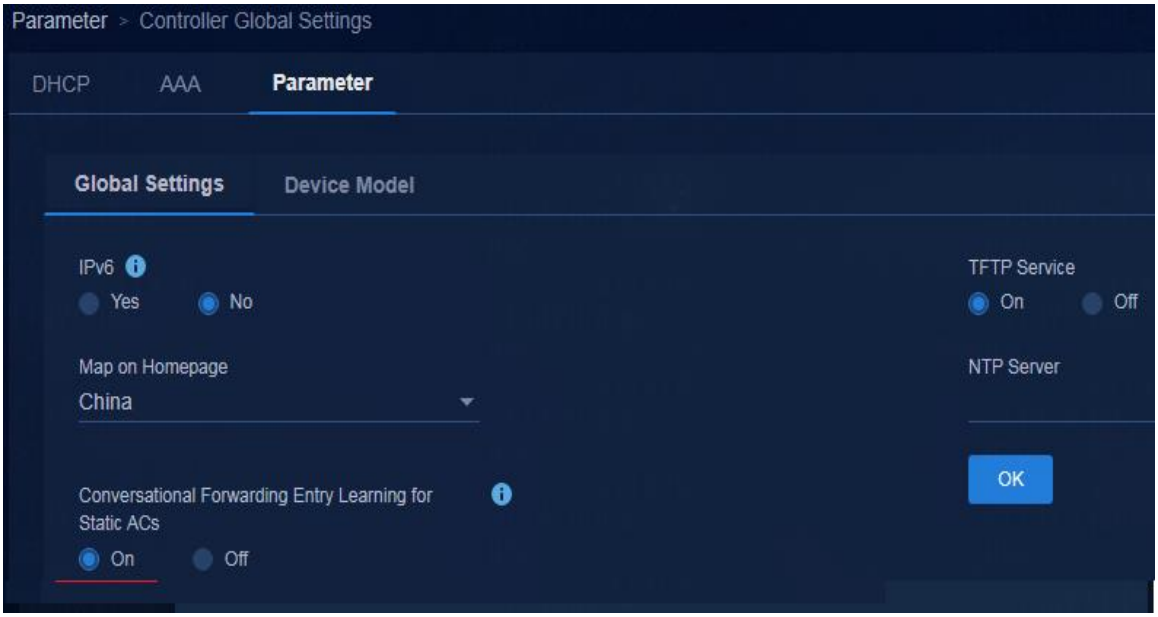
DHCP サーバーが異なれば、構成方法も異なります。Microsoft DHCP サーバーの構成の詳細については、『Configuring the critical DHCP server』を参照してください。

疎結合モードの DHCP サーバーは同期できません。DHCP サーバーで使用できるアイコンがありません。DHCP サーバーの **Audit Status** 列には、3 つのハイフン(---)が表示されます。



スタティックイーサネットサービスインスタンスの従来の転送エントリー学習のイネーブル化

ネットワークに S6520X シリーズまたは S5560X シリーズスイッチが含まれている場合は、**Automation** > **Campus Network** > **Network Parameters** > **Parameter** ページに移動して、スタティック AC の従来のフォワーディングエントリーラーニングをイネーブルにすることを推奨します。



スタティック AC の従来の転送エントリー学習がイネーブルになっている場合、デバイスは、イーサネットサービスインスタンスでのパケット転送に転送エントリーが必要な場合にだけ、ハードウェアに転送エントリーを発行します。次の設定は、リーフインターフェイス上のスタティックイーサネットサービスインスタンスに展開されます。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 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 domain
 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

従来の自動導入

従来の自動展開では、コントローラーとデバイスが連携して自動展開プロセスを完了します。詳細については、『AD-Campus 6.2 Automation Configuration Guide』を参照してください。

最適化された自動導入

最適化された自動展開では、自動展開はデバイスに依存することなく、コントローラーによって完全に実行されます。詳細については、『AD-Campus 6.2 Optimized Automation Configuration Guide』を参照してください。

導入の半分を自動化

半自動展開では、スパインデバイスとリーフデバイスは手動で組み込まれ、アクセスデバイスは自動的に展開されます。スパインデバイスとリーフデバイスを手動で組み込む方法については、『Manual incorporation』を参照してください。アクセスデバイスの自動展開、および半自動展開に関連するその他の設定については、『AD-Campus 6.2 Half Automation Configuration Guide』を参照してください。

手動による組み込み

ここでは、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が自動的に展開されない場合の、手動設定の基本的な設定手順について説明します。アンダーレイの設定が完了すると、SeerEngine キャンパスコントローラーはデバイスを組み込み、オーバーレイ設定をデバイスに展開できます。

注:

- このセクションでは、手動によるアンダーレイの展開についてのみ説明します。自動アンダーレイ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。
- この項では、レイヤー3 スイッチの設定は、スパインデバイスがスタンドアロンノードまたは IRF ファブリックであるシナリオに適用できます。ネットワークにデュアルホーム接続されたスパインデバイスが配置されている場合、レイヤー3 スイッチの設定については、『Configuring redundant dual-spine uplinks』を参照してください。
- レイヤー3 スイッチが使用できない場合、または VLAN 4094 ネットワークセグメントのゲートウェイがスパインデバイス上にある場合は、リーフデバイス上のコントローラーのネットワークセグメントを宛先とする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 スイッチの設定

#DHCP を有効にします。

```
dhcp enable
#
```

Enable the spanning tree feature globally.

```
stp global enable
#
```

Create VLAN-interface 4094.

```
#
vlan 4094
#
#
interface Vlan-interface4094
 ip address 130.1.0.1 255.255.255.0
#
```

#VLAN-interface 1 を設定します。VLAN-interface 1 は、自動デバイスオンボーディングに使用されます。ネットワーク内のすべてのデバイスが手動で組み込まれている場合は、VLAN-interface 1 の設定をスキップします。

```
interface Vlan-interface1
 ip address 120.1.0.1 255.255.255.0
 dhcp select relay       //DHCP relay related settings are used for automatic device onboarding. If spine, leaf, and access nodes are all manually incorporated, the DHCP relay related settings are not required.
 dhcp relay server-address 110.1.0.105      //IP address of the vDHCP server node.
 dhcp relay server-address 110.1.0.106
#
```

#VLAN-interface 30 と VLAN-interface 1010 を作成します。

```
#
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する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  // ネットワーク内のすべてのスパイン、リーフ、およびアクセスデバイスが手動設定によってオンボードされている場合は、undo permit vlan 1 コマンドを使用します。
```

#Unified Platform に接続されてい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  //  レイヤー3 スイッチをサーバーに接続するポートは、STP エッジポートとして設定されます。
#
```

#SeerEngine キャンパスと vDHCP に接続されてい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  //  レイヤー3 スイッチをサーバーに接続するポートは、STP エッジポートとして設定されます。
#
```

#デフォルトルートを追加します。認証ユーザーと EIA 間の通信のデフォルトルートのネクストホップとして、スパインノード上の VSI インターフェイス 4094 のアドレスを設定します。

```
ip route-static 0.0.0.0 0 130.1.0.2  //  デフォルトルートのネクストホップは、スパインノード上の VSI インターフェイス 4094 のアドレスです。
#
```

スパインデバイスの設定

SeerEngine キャンパスコントローラーにスパインデバイスを組み込む前に、次のタスクを実行する必要があります。

1. スパインの役割とシステム名を設定します。

   #ロール設定を有効にするには、デバイスを再起動する必要があります。デバイスのデフォルトロールがスパインの場合は、ロール設定をスキップします。

   ```
   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. スパニングツリー機能を設定します。

   ```
   #
   stp ignored vlan 2 to 4094
   stp global enable
   stp root primary   //Configure the spine device as the STP root.
   #
   ```

4. SNMP、NETCONF、Telnet、および SSH の設定を行います。

#SNMP 設定を構成します。次の構成がデフォルトの構成です。実際のネットワーク条件に従って SNMP コミュニティを構成する必要があります。

```
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 の設定を行います。

```
netconf soap http enable
 netconf soap https enable
 netconf ssh server enable
 restful https enable
#
```

#Telnet の設定を行います。

```
telnet server enable //  Telnet を使用する場合に必要です。
#
```

#SSH の設定を行います。

```
ssh server enable
#
```

5. Telnet または SSH で使用する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   //   パスワードは、パスワードの複雑さの要件を満たしている必要があります。修飾パスワードは、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 2 種類以上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の文字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
#
```

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. Loopback 0 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     //Configure OSPF.
#
```

9. スパイン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使用可能な場合は、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 インタフェースを作成する
interface Vlan-interface91
 ip address 91.1.0.1 24      //  実際の計画に応じて、未使用のサブネットアドレスを使用します。
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```

#スパインダウンリンクインターフェイスを VLAN に割り当てます。

```
#
interface Ten-GigabitEthernet3/0/16
 port link-mode bridge
 port link-type trunk
port trunk permit vlan 1 91     //  ネットワーク内のすべてのスパイン、リーフ、およびアクセスデバイスが手動設定によってオンボードされている場合は、undo permit vlan 1 コマンドを使用します。
#
```

重要:

ベストプラクティスとして、ルートアドバタイズメントの VLAN インターフェイスには、VLAN 3～99、VLAN 4001～4050、および VLAN 4061～4089 を使用します。

SeerEngine キャンパスコントローラーは、デフォルトで次の VLAN をデバイスに自動的に展開します。

- **VLAN 2:** この VLAN は、DR システム内の 2 つの DR メンバーデバイス間のアンダーレイルート同期に使用されます。
- **VLAN 100**: この VLAN は、自動設定された IRF ファブリック上の BFD MAD に使用されます。
- **VLAN 101～2800**: VLAN は、アクセススイッチによって使用されます。
- **VLAN 2801～3000**: VLAN は、スタティック AC によって使用されます。
- **VLAN 3001～3500**: VLAN は、リンクで相互接続されたスパインデバイスおよびリーフデバイスへの自動デバイス展開に使用されます。
- **VLAN 3501～4000**: VLAN はセキュリティグループによって使用されます。
- **VLAN 4090～4094**: VLAN は予約されています。

VLAN 3～99 および VLAN 4001～4089 は、自動的に割り当てることはできません。VLAN 4051～4060 は、認証フリーVLAN として使用されます。

スパインノードとリーフノードが複数のリンクを介して接続されている場合、これらのリンクは ECMP リンクです。VLAN 1 ではスパニングツリー機能がイネーブルになっているため、スパインノードとリーフノード間のリンクが破棄状態になるのは正常です。

10. L2VPN をイネーブルにします。

```
#
l2vpn enable
```

```
#
```

11. コントロールチャネルの接続のために、VPN インスタンス **vpn-default**、VSI-interface 4094、および VSI インターフェイス IP アドレスを設定し、L3 VXLAN ID を指定します。

#VPN インスタンス **vpn-default** を作成します。RD およびルートターゲットを手動で設定します。RD およびルートターゲットは、ネットワーク全体で 1:1 です。

```
#
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 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 要求プロキシをイネーブルにして、ネットワーク接続タイムアウトのためにデバイスにサーバーARP エントリーが存在しない場合に、エンドポイントがサーバーに接続できない問題を解決します。
#
```

#レイヤー3 転送の VSI インターフェイスと L3 VXLAN ID を設定します。この例では、VPN インスタンス **vpn-default** に対して VSI-interface 4092 を作成し、L3 VXLAN ID 4092 を設定します。ip address unnumbered コマンドを使用して、指定したインターフェイスの IP アドレスを借用するようにインターフェイスを設定します。VPN インスタンス **vpn-default** にセキュリティグループを作成する場合は、レイヤー3 発信パケットの送信元 IP として VSI-interface 4094 の IP を指定します。

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

#VSI **vxlan4094** 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。

重要:

複数のリーフノードが使用可能な場合は、複数のピアを設定する必要があります。

BGP AS 番号が、SeerEngine キャンパスコントローラーのファブリックに設定されている AS 番号と同じであることを確認します。

```
#
bgp 100
 non-stop-routing
 router-id 200.1.1.254  //  各デバイスのルータ ID を同じにすることはできません。
peer 200.1.1.252 as-number 100  //  BGP ピアを設定します。IP アドレスは、リーフデバイスのループバックインターフェイスです。
 peer 200.1.1.252 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  reflector cluster-id 200.1.1.254  //  デュアルスパインネットワーク環境で必要です。2 つのスパインデバイスのクラスタ ID は同じです。

  undo policy vpn-target      //  受信した VPNv4 ルートをフィルタリングしないために必要です。
  peer 200.1.1.252 enable  //  複数のリーフノードが存在する場合は、このコマンドを繰り返して複数のピアを設定します。
  peer 200.1.1.252 reflect-client // 異なるリーフ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  //  直接接続されたルートをインポートします。この設定は、リーフデバイスで IPv4 会話型学習がイネーブルになっている場合に必要です。
   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 スイッチに接続されているインターフェイス)を AC インターフェイスとして設定し、VSI vxlan4094 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   //If all spine, leaf, and access devices in the network are onboarded through manual configuration, use the undo permit vlan 1 command.
    service-instance 4094          //Create Ethernet service instance 4094.
    encapsulation s-vid 4094     //Match VLAN tag 4094.
    xconnect vsi vxlan4094       //Bind the Ethernet service instance to VSI vxlan4094.
#
```

14. スタティックルートを設定します。

#スパインノードと SeerEngine キャンパス、EIA、またはその他のサーバー間の接続がレイヤー3 接続である場合、サーバーを宛先とするスタティックルートを設定する必要があります。スタティックルートのネクストホップは、レイヤー3 スイッチの VLAN インターフェイス 4094 の IP アドレスです。

```
ip route-static vpn-instance vpn-default 110.1.0.0 24 130.1.0.1  //The destination IP is the subnet IP of the controller.
#
ip route-static vpn-instance vpn-default 100.1.0.0 24 130.1.0.1  //The destination IP is the subnet IP of the server.
#
# If the DHCP server and spine device belong to different subnets, you must add a static route destined for the DHCP server.
ip route-static vpn-instance vpn-default  132.0.0.0 24 130.1.0.1  //DHCP server subnet IP.
#
```

15. VXLAN トンネル上で、リモート MAC エントリー学習とリモート ARP および ND 学習をディセーブルにします。

#VXLAN トンネルでのリモート ARP 学習を無効にします。

```
vxlan tunnel arp-learning disable
#
```

#IPv6 サービスが設定されている場合は、VXLAN トンネルでのリモート ND ラーニングを無効にします。

```
vxlan tunnel nd-learning disable
#
```

#VXLAN トンネルでのリモート MAC エントリー学習をディセーブルにします。

```
vxlan tunnel mac-learning disable
#
```

16. NTP を設定します。

```
#
 clock timezone beijing add 08:00:00
#
```

#IP アドレスが NTP サーバーの IP アドレスである場合、Unified Platform はデフォルトで組み込みの NTP サーバーを使用して設定され、IP アドレスはクラスタノースバウンド IP です。

```
ntp-service enable
 ntp-service unicast-server 100.1.0.100  vpn-instance vpn-default
#
```

17. スパインが IRF ファブリックの場合は、マスター/下位スイッチオーバー後も IRF ブリッジ MAC アドレスが変更されないように設定します。

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

リーフデバイスの構成

重要:

デバイスが S5560X または S6520X スイッチの場合は、デバイスの動作モードを VXLAN に設定します。モードの変更を有効にするには、デバイスを再起動する必要があります。

リーフデバイスを SeerEngine キャンパスコントローラーに組み込む前に、次のタスクを実行します。

1. デバイスの動作モードを VXLAN に設定します。

#デバイスの動作モードを表示し、デバイスが VXLAN モードで動作していることを確認します。

```
display switch-mode status
  Switch-mode in use: VXLAN MODE.
```

```
    Switch-mode for next reboot: VXLAN MODE.
#
```

#サポートされているデバイスの動作モードを表示します。

```
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
#
```

2. リーフの役割とシステム名を設定します。

   #ロール設定を有効にするには、デバイスを再起動する必要があります。デバイスのデフォルトロールが leaf の場合は、ロール設定をスキップします。

   ```
   # vcf-fabric role leaf
   #
   ```

   #システム名を設定します。

   ```
   sysname leaf1
   #
   ```

3. トポロジを決定するように LLDP を設定します。

   ```
   #
   lldp global enable
   #
   ```

4. スパニングツリー機能を設定します。

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

5. リーフダウンリンクインターフェイスで、TC-BPDU 伝送制限をイネーブルにします。

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

重要:

エンドポイントに接続されていないリーフダウンリンクインターフェイスでは、TC-BPDU 伝送制限をイネーブルにする必要があります。リーフダウンリンクインターフェイスがエンドポイントに接続されている場合は、そのインターフェイスをスパニングツリーエッジポートとして設定する必要があります。

6. SNMP、NETCONF、Telnet、および SSH の設定を行います。

   #SNMP 設定を構成します。次の構成がデフォルトの構成です。実際のネットワーク条件に従って SNMP コミュニティを構成する必要があります。

   ```
   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 の設定を行います。

```
#
 netconf soap http enable
 netconf soap https enable
 netconf ssh server enable
 restful https enable
#
```

#Telnet の設定を行います。

```
telnet server enable
#
```

#SSH の設定を行います。

```
ssh server enable
#
```

7. Telnet または SSH で使用する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  //  パスワードは、パスワードの複雑さの要件を満たしている必要があります。修飾パスワードは、数字、大文字、小文字および特殊文字の 2 種類以上の文字を含む 10 から 63 文字の文字列である必要があります。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の文字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
#
```

8. VLAN 4094 を作成します。

```
vlan 4094
#
```

9. OSPF を設定します。

```
#
ospf 1 router-id 200.1.1.252
non-stop-routing
area 0.0.0.0
#
```

10. Loopback 0 を設定します。

```
#
interface LoopBack0
 ip address 200.1.1.252 255.255.255.255     //Used to establish a BGP peer with the spine device.
 ospf 1 area 0.0.0.0
#
```

11. スパインノードと通信するための 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 は、スパインノードの VLAN と同じである必要があります。

#

#VLAN インターフェイスを作成します。

```
interface Vlan-interface91
 ip address 91.1.0.2 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```

#リーフアップリンクインターフェイスを VLAN に割り当てます。

```
#
interface Ten-GigabitEthernet1/2/0/13
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 91
#
```

重要:

ベストプラクティスとして、ルートアドバタイズメントの VLAN インターフェイスには、VLAN 3～99、VLAN 4001～4050、および VLAN 4061～4089 を使用します。

SeerEngine キャンパスコントローラーは、デフォルトで次の VLAN をデバイスに自動的に展開します。

- **VLAN 2**: この VLAN は、DR システム内の 2 つの DR メンバーデバイス間のアンダーレイルート同期に使用されます。
- **VLAN 100**: この VLAN は、自動設定された IRF ファブリック上の BFD MAD に使用されます。
- **VLAN 101～2800**:　VLAN は、アクセススイッチによって使用されます。
- **VLAN 2801～3000**:　VLAN は、スタティック AC によって使用されます。
- **VLAN 3001～3500**:　VLAN は、リンクで相互接続されたスパインデバイスおよびリーフデバイスへの自動デバイス展開に使用されます。
- **VLAN 3501～4000**:　VLAN はセキュリティグループによって使用されます。
- **VLAN 4090～4094**:　VLAN は予約されています。

VLAN 3～99 および VLAN 4001～4089 は、自動的に割り当てることはできません。VLAN 4051～4060 は、認証フリーVLAN として使用されます。

スパインノードとリーフノードが複数のリンクを介して接続されている場合、これらのリンクは ECMP リンクです。VLAN 1 ではスパニングツリー機能がイネーブルになっているため、スパインノードとリーフノード間のリンクが破棄状態になるのは正常です。

12. L2VPN をイネーブルにします。

l2vpn enable

#

13. 制御チャネルを接続するには、次のタスクを実行します。

- VPN インスタンス **vpn-default**、VSI **vxlan4094**、および VSI インターフェイス IP アドレス設定を設定し、L3 VXLAN ID を指定します。
- ダウンリンク AC インターフェイス(アクセスデバイスに接続されたインターフェイス)でイーサネットサービスインスタンスを設定し、イーサネットサービスインスタンスを VSI **vxlan4094** にマッピングします。

Create VPN instance **vpn-default**. Configure the RD and route targets manually. The RD and route targets are 1:1 in the whole network.

```
#
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
#
```

Configure the IP address of VSI-interface 4094.

```
#
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 //Enable ARP request proxy to resolve the issue that an endpoint cannot connect to a server if no server ARP entry exists on the device because of network connection timeout.
#
```

Configure VSI interface and L3 VXLAN ID settings for Layer 3 forwarding. In this example, create VSI-interface 4092 and configure L3 VXLAN ID 4092 for VPN instance **vpn-default**. The **ip address unnumbered** command is used to configure an interface to borrow the IP address of the specified interface. When a security group is created in VPN instance **vpn-default**, specify the IP of VSI-interface 4094 as the source IP of Layer 3 outgoing packets.

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

Configure VSI **vxlan4094**.

```
#
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
#
```

Configure the leaf downlink interface connected to the access device as an AC interface.

```
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
#
```

14. BGP EVPN を設定します。

Configure BGP instance 100 and specify the spine device as a peer.

```
#
bgp 100
 non-stop-routing
 router-id 200.1.1.252   //The router ID of each device cannot be the same. Configure a loopback interface address as the router ID.
 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
#
```

15. スタティックルートを設定します。

When the connections between the spine device and servers are Layer 3 connections, you must configure static routes destined for the servers. The next hop of the static routes is the IP address of VLAN-interface 4094 on the Layer 3 switch.

```
ip route-static vpn-instance vpn-default 110.1.0.0 24 130.1.0.1  //The destination IP is the subnet IP of the controller.
#
ip route-static vpn-instance vpn-default  100.1.0.0 24 130.1.0.1  //The destination IP is the subnet IP of the server.
#
```

If the DHCP server and spine device belong to different subnets, you must add a static route destined for the DHCP server.

```
ip route-static vpn-instance vpn-default  132.0.0.0 24 130.1.0.1  //DHCP server subnet IP.
#
```

16. DHCP スヌーピングを設定します。

```
#
 dhcp snooping enable vlan 2 to 4094
#
```

17. VLAN 1 および VLAN 4094 からの IPv4 パケットを IPSG フィルタリングから除外します。

The configuration is required when IPSG is configured on the leaf downlink interface. If IPSG is not configured, the configuration in this step does not affect services.

```
ip verify source exclude vlan 1
```

```
ip verify source exclude vlan 4094
#
```

18. VXLAN トンネルでのリモート MAC エントリー学習およびリモート ARP 学習をディセーブルにします。

Disable remote ARP learning on VXLAN tunnels.

```
vxlan tunnel arp-learning disable
#
```

Disable remote-MAC entry learning on VXLAN tunnels.

```
vxlan tunnel mac-learning disable
#
```

19. (任意)エントリー転送の会話型学習をイネーブルにします(デフォルトでは、この機能はディセーブルになっています。必要に応じてイネーブルにできます)。

転送エントリーの会話型学習がリーフデバイスでイネーブルになっている場合は、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をリーフデバイスおよびスパインデバイスにインポートするために、スパインデバイス上の BGP VPN インスタンス vpn-default に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、サーバー、および外部ネットワーク間の到達可能性が保証されます。

#ハードウェアリソースを節約するために、障害によって EVPN を介して同期されたリモート ARP エントリーは、エントリーが受信された直後にハードウェアに発行されません。代わりに、デバイスは、エントリーがパケット転送に必要な場合にのみ、ARP エントリーをハードウェアに発行します。

```
ip forwarding-conversational-learning        //Enable conversational learning for host route FIB entries.
```

Specify an aging timer for host route FIB entries. The default aging time is 60 minutes.

```
[leaf1]ip forwarding-conversational-learning aging ?
  INTEGER<60-1440>  Aging time in (minutes)
#
```

重要:

ベストプラクティスとして、S5560X-HI および S6520X-HI スイッチでエントリーを転送するための会話型学習を有効にします。

リーフデバイスがボーダーデバイスとしても機能する場合は、ベストプラクティスとして、エントリー転送の会話型学習をイネーブルにしないでください。

20. NTP を設定します。

```
#
 clock timezone beijing add 08:00:00
#
#  The IP address is the IP address of the NTP server.
 ntp-service enable
 ntp-service unicast-server 100.1.0.100 vpn-instance vpn-default
#
```

21. 設定を確認します。

```
[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-interface 4094 and VSI-interface 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      --       //The 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 successfully.
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]
```

22. IRF ブリッジ MAC パーシステンスを設定します。

リーフが IRF ファブリックの場合、マスター/下位スイッチオーバー後に IRF ブリッジ MAC アドレスが変更されないように設定する必要があります。

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

```
#
```

アクセスデバイスの設定

1. アクセスロールとシステム名を設定します。

   #ロール設定を有効にするには、デバイスを再起動する必要があります。デバイスのデフォルトロールがアクセスである場合は、ロール設定をスキップします。

   ```
   #
   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. スパニングツリー機能を設定します。

   ```
   #
   stp global enable
   #
   ```

4. SNMP、NETCONF、Telnet、および SSH の設定を行います。

   #SNMP 設定を構成します。次の構成がデフォルトの構成です。実際のネットワーク条件に従って SNMP コミュニティを構成する必要があります。

   ```
   #
   snmp-agent
   snmp-agent community write private
   snmp-agent community read public
   snmp-agent sys-info version all
   snmp-agent packet max-size 4096
   #
   # Configure NETCONF settings.
   netconf soap http enable
    netconf soap https enable
    netconf ssh server enable
    restful https enable
   #
   # Configure Telnet settings.
    telnet server enable
   #
   # Configure SSH settings.
   ssh server enable
   #
   ```

5. Telnet または SSH で使用する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//パスワードは、パスワードの複雑さの要件を満たしている必要があります。修飾パスワードは、数字、大文字、小文字および特殊文字の 2 種類以上の文字を含む 10 から 63 文字の文字列である必要が

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の文字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        //Set to none if username and password are not used.
 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をすべての VLAN に割り当てます。

```
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-interface 1 を設定します。

#ベストプラクティスとして、アクセスデバイスで 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 インターフェイス 4094 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組み込むことができます。

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

10. 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間の接続がレイヤー3 接続の場合、サーバーを宛先とするスタティックルートを設定する必要があります。スタティックルートのネクストホップは、レイヤー3 スイッチ上の VLAN インターフェイス 4094 の IP アドレスです。

```
ip route-static 110.1.0.0 24 130.1.0.1      //The destination IP is the subnet IP of the controller.
ip route-static 100.1.0.0 24 130.1.0.1      //The destination IP is the subnet IP of the server.
```

11. NTP サーバーを設定します。

```
#
 clock timezone beijing add 08:00:00
#
# The IP address is the IP address of the NTP server.
ntp-service enable
 ntp-service unicast-server 100.1.0.100
#
```

12. エンドポイントに接続されたインターフェイスをスパニングツリーエッジポートとして設定します。

SeerEngine キャンパスコントローラーは、アクセスデバイスを組み込んだ後、アクセスデバイス上のユーザーエンドポイントに接続されたインターフェイスをスパニングツリーエッジポートとして自動的に設定し、各インターフェイスに VLAN ID を割り当てます。コントローラーは設定を自動的に完了します。手動設定は必要ありません。コントローラーが設定を配信しない場合は、設定を手動で設定できます。

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

13. IRF ブリッジ MAC パーシステンスを設定します。

アクセスが IRF ファブリックの場合は、マスター/下位スイッチオーバー後も IRF ブリッジ MAC アドレスが変更されないように設定する必要があります。

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

集約デバイスの設定

集約デバイスは、スパインデバイスとリーフデバイスを接続します。手動で組み込む場合、そのデバイスロールは評価されません。したがって、デバイスロールを構成する必要はありません。集約デバイスを手動で構成するには、次の手順を実行します:

1. システム名を設定します。

#集約デバイスのデバイスロールは、手動で組み込むときには評価されません。したがって、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. スパニングツリー機能を設定します。

```
#
stp global enable
#
```

4. SNMP、NETCONF、および SSH の設定を行います。

#SNMP 設定を構成します。次の構成がデフォルトの構成です。実際のネットワーク条件に従って SNMP コミュニティを構成する必要があります。

```
#
snmp-agent
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent packet max-size 4096
#
```

Configure NETCONF settings.

```
netconf soap http enable
 netconf soap https enable
 netconf ssh server enable
```

```
 restful https enable
#
```

Configure SSH settings.

```
ssh server enable
#
```

5. Telnet または SSH で使用する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。

```
service-type http https ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
#
line vty 0 63
 authentication-mode scheme        //Set to none if username and password are not used.
 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. Loopback 0 を設定します。

```
#
interface LoopBack0
 ip address 200.1.1.200 255.255.255.0
 ospf 1 area 0.0.0.0
#
```

8. スパインノードと通信するための VLAN インターフェイスを設定します。

#VLAN を作成します。

```
vlan 92                          //Add the corresponding VLAN for the spine device and the VLAN is the same as the spine.
#
```

Create a VLAN interface.

```
interface Vlan-interface92
 ip address 91.2.0.2 255.255.255.0       //In the same subnet as the IP address of VLAN-interface 92 on the spine.
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```

Assign the aggregation uplink interface to the VLAN.

```
#
interface Ten-GigabitEthernet1/1/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 92
#
```

9. リーフデバイスと通信するための VLAN インターフェイスを設定します。

   #VLAN を作成します。

```
vlan 93                          //Add the corresponding VLAN for the leaf device and the VLAN is the same as the leaf.
# Create a VLAN interface.
interface Vlan-interface93
 ip address 91.3.0.2 255.255.255.0       // In the same subnet as the IP address of VLAN-interface 92 on the leaf.
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
# Assign the aggregation uplink interface to the VLAN.
#
interface Ten-GigabitEthernet1/1/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 93
#
```

10. VLAN-interface 1 を設定します。コントローラーは、VLAN-interface 1 を介して集約デバイスを組み込みます。VLAN-interface 1 が、コントローラーをホストする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
#
```

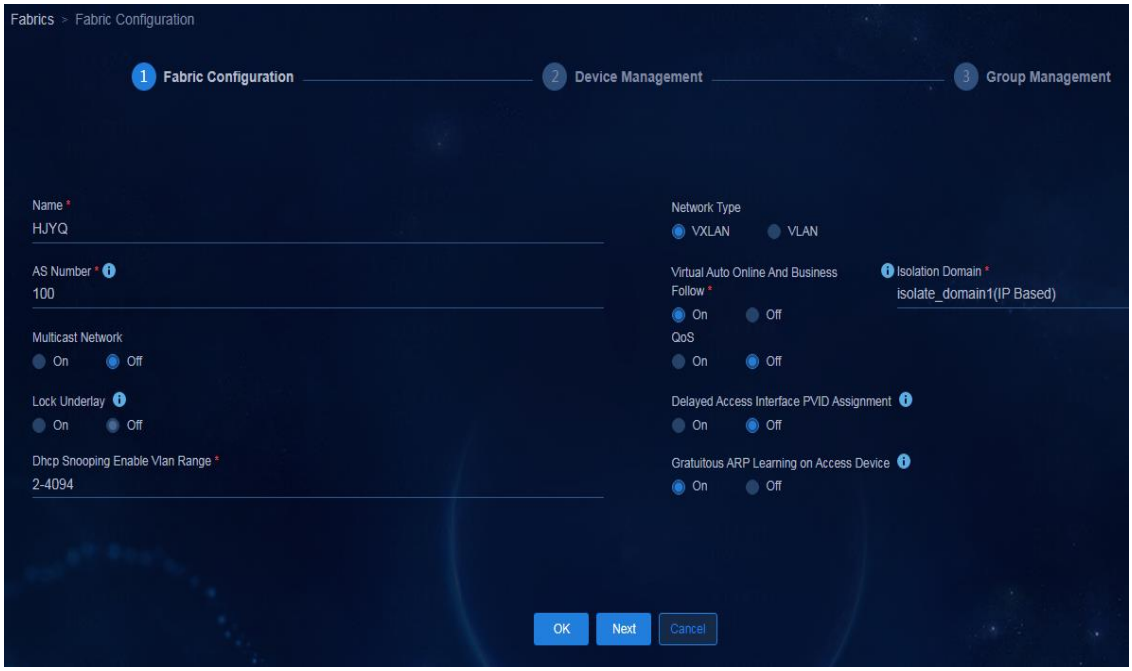
11. NTP サーバーを設定します。

```
#
 clock timezone beijing add 08:00:00
#
# The IP address is the IP address of the NTP server.
ntp-service enable
 ntp-service unicast-server 100.1.0.100
#
```

ファブリックの設定

1. **Automation** > **Campus Network** > **Fabrics** ページに移動し、**Add** をクリックします。
2. **Fabric Configuration** ページでファブリックを構成します。パラメーターは次のとおりです。
   - **Name**: ファブリックの名前を入力します。
   - **AS Number**: 1～4294967295 の範囲の整数を入力します。手動取り込みモードでは、ファブリックに設定されている AS 番号が、デバイスに設定されている BGP AS 番号と同じであることを確認します。
   - **Isolation Domain**: ファブリックの分離ドメインを選択します。
   - **Multicast Network** : デフォルトでは、値は **Off** です。必要に応じて有効にできます。
   - **QoS**: デフォルトでは、値は **Off** です。必要に応じて有効にできます。
   - **Lock Underlay**: 既定では、この値は **Off** です。ファブリックの追加時にこのパラメーターを変更することはできません。デバイスの自動展開中は無効にし、デバイスの自動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、この値は **Off** です。デバイスがアクティブ化されると、コントローラーは自動的に PVID をデバイス上のインターフェイスに割り当てます。**On** を選択すると、デバイスがアクティブ化されるときにコントローラーは PVID を割り当てないため、デバイスのアクティブ化後に PVID を手動で構成できます。
- **Virtual Auto Online と Business Follow**: デフォルトでは、値は **On** です。これは、VXLAN ネットワークの認可を制御し、セキュリティグループ間のポリシーにアクセスするために使用されます。注意事項をよく読んでから操作してください。



3. **OK** をクリックします。追加したファブリックが **Fabrics** ページに表示されます。各ファブリックに対して 11 の一般ポリシーグループが作成されます。

デバイスの組み込み

デバイスをコントローラーに手動で追加したり、デバイスを自動的に検出するようにコントローラーを設定したりできます。

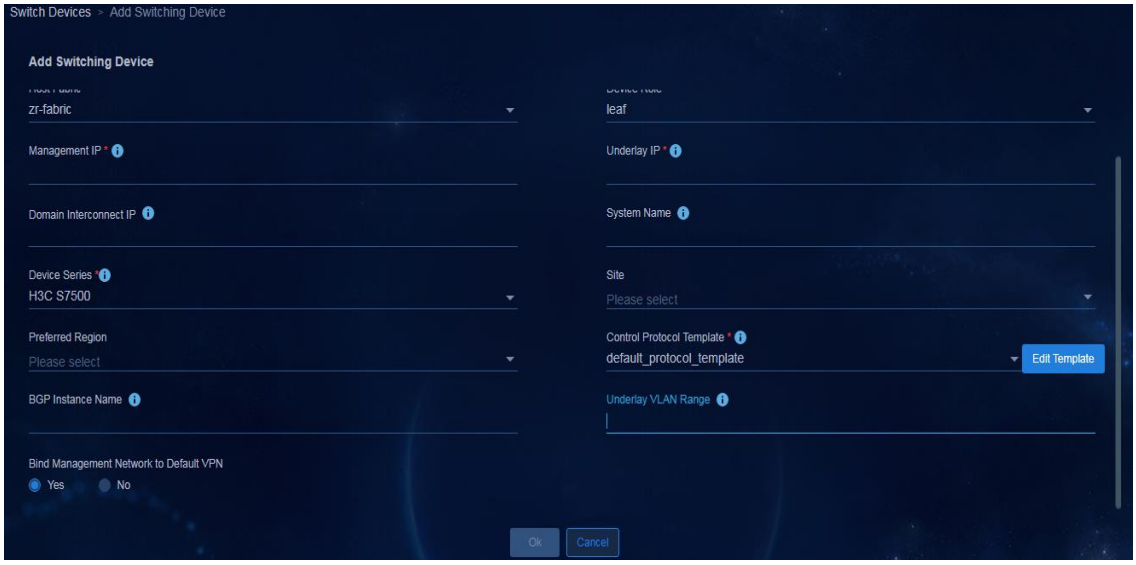
デバイスを手動で追加する

Guide > **Add Device** ページに移動し、デバイス名を入力して、**Basic Info** と **Control Protocol Template** 領域でパラメーターを設定します。

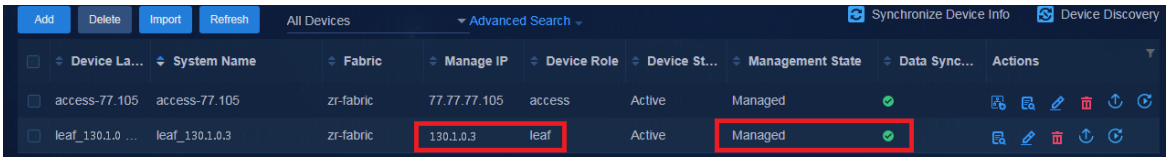
スパインまたはリーフデバイスを追加するには:

- **Basic Information** 領域で、次の操作を行います。
  - **Host Fabric**: ファブリックのポリシーモードは、IP ベースのポリシーである必要があります。
  - **Device Role**: Spine、Leaf、Access、または Aggregation を選択します。選択したロールが、デバイスに設定されているロールと同じであることを確認してください。集約ロールは、集約ネットワークモデルに使用されます。元のスパインリーフアクセスネットワークモデルまたはスパインリーフネットワークモデルと比較すると、集約ネットワークモデルでは、スパインデバイスとリーフデバイスの間に集約レイヤー3 スイッチが追加されます。集約レイヤー3 スイッチは、VXLAN または EVPN をサポートする必要はありません。集約ネットワークモデルの詳細については、『Spine-aggregation-leaf-access or spine-aggregation-leaf network model』を参照してください。集約デバイスを手動で組み込む必要がある場合は、H3C R&D にお問い合わせください。
  - **Management IP**: VXLAN-interface 4094(スパインデバイスおよびリーフデバイスの場合)または VLAN-interface 4094(アクセスデバイスの場合)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**: デバイスモデルに対応する製品シリーズを選択します。
- **Control Protocol Template**: デバイスと同じ設定を持つテンプレートを選択します。選択しないと、デバイスをアクティブ化できません。
- その他のパラメーター:デフォルト値を使用します。



デバイスが追加されると、データの同期に一定の時間が必要になるため、初期の **Device State** は **Inactive** になります。データが同期された後、**Refresh** をクリックします。**Device State** が **Active** になると、デバイスは正常に接続されます。



デバイスを組み込んだ後、display openflow instance 1 controller コマンドを使用して、SeerEngine キャンパスコントローラーに接続されているデバイスに関する詳細情報を表示できます。

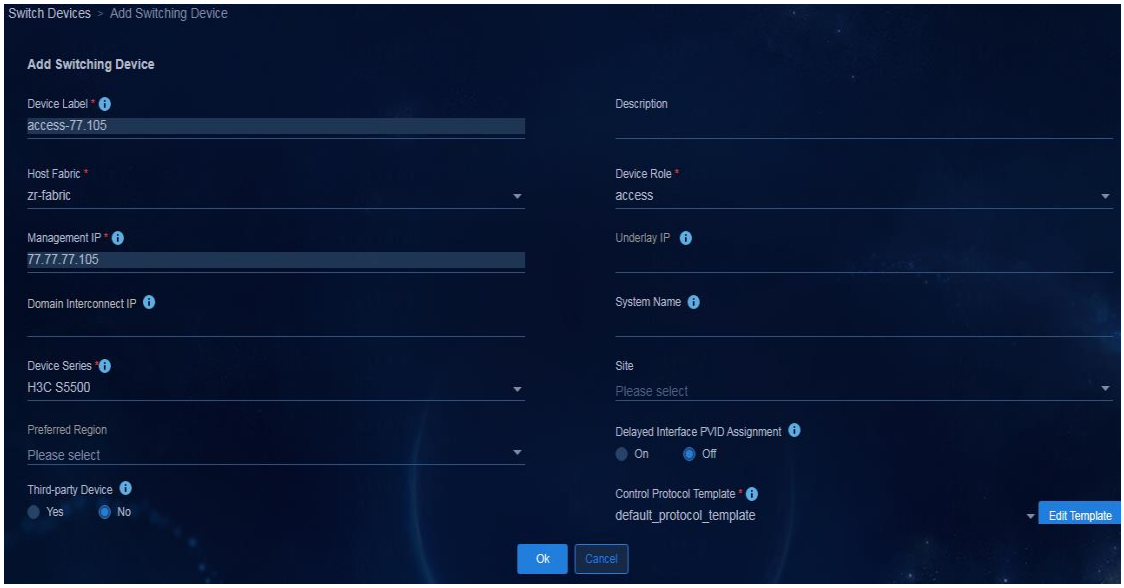
```
[Leaf1]display openflow instance 1 controller
Instance 1 controller information:
 Reconnect interval: 60 (s)
 Echo interval     : 5  (s)

 Controller ID          : 1
 Controller IP address   : 110.1.0.102
 Controller port        : 6633
 Local IP address       : 130.1.0.3
 Local port            : 20870
 Controller role        : Master
 Connect type           : TCP
 Connect state          : Established
 Packets sent           : 88
 Packets received       : 158
 SSL policy            : --
 Control SSL policy     : --
```

```
VRF name              : vpn-default

Controller ID          : 2
Controller IP address   : 110.1.0.103
Controller port        : 6633
Local IP address       : 130.1.0.3
Local port            : 20872
Controller role        : Slave
Connect type          : TCP
Connect state          : Established
Packets sent          : 84
Packets received       : 154
SSL policy            : --
Control SSL policy     : --
VRF name              : vpn-default

[Leaf1]
```

アクセスデバイスを追加するには、次の手順を実行します。

AD キャンパス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、『ハードウェア情報』を参照してください。

- **Basic Information** 領域で、次の操作を行います。
  - **Host Fabric**: ファブリックのポリシーモードは、IP ベースのポリシーである必要があります。
  - **Device Role**: access を選択します。
  - **Management IP**: VLAN インターフェイス 4094 の IP アドレスを入力します。
  - **Underlay IP**: アクセスデバイス用に設定する必要はありません。
  - **Device Series**: デバイスモデルに対応する製品シリーズを選択します。
  - **Delayed Interface PVID Assignment** : デフォルトでは、この値は **Off** です。デバイスがアクティブ化されると、コントローラーは自動的に PVID をデバイスのインターフェイスに割り当てます。**On** を選択すると、デバイスがアクティブ化されてもコントローラーは PVID を割り当てません。デバイスのアクティブ化後に PVID を手動で構成できます。
  - **Third-party Device**: デフォルトでは、値は **No** です。デバイスがサードパーティ製デバイスの場合は、Yes を選択します。
  - **Control Protocol Template**: デバイスと同じ設定を持つテンプレートを選択します。選択しないと、デバイスをアクティブ化できません。
  - その他のパラメーター: デフォルト値を使用します。



注:

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。

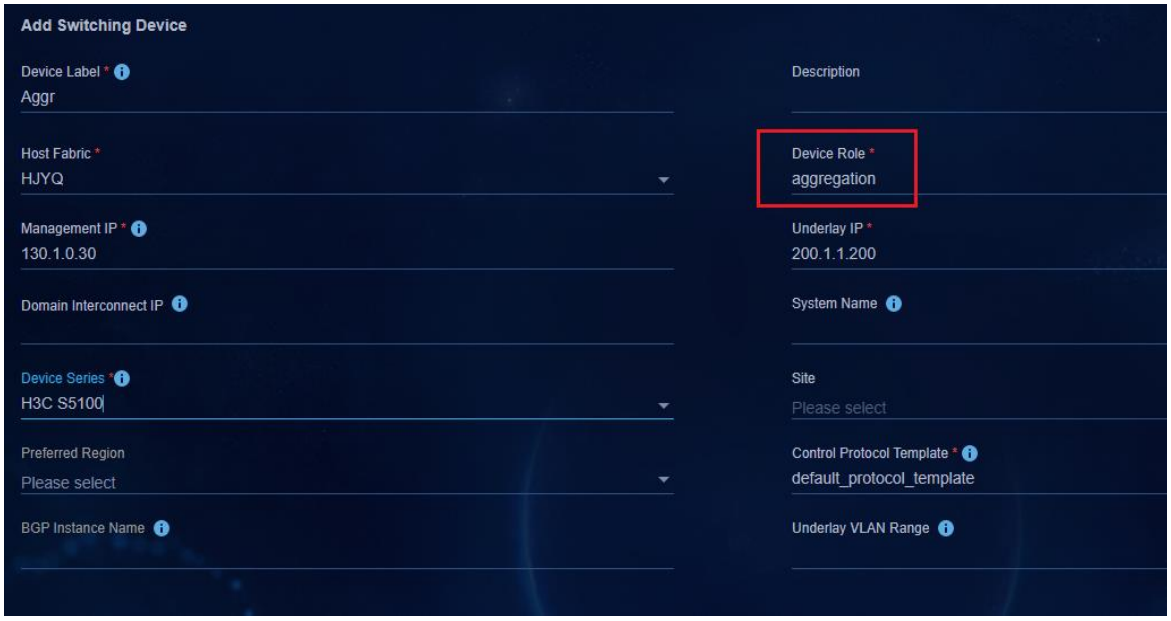
集約デバイスを追加するには、次の手順を実行します。

集約デバイスは、スパインデバイスとリーフデバイスの中間のデバイスです。集約デバイスを組み込む前に、いくつかの基本構成を構成する必要があります。集約デバイスの基本構成の詳細は、『Configuring an aggregation device』を参照してください。

集約デバイスに接続されているリーフデバイスの基本設定については、『Configuring a leaf device』を参照してください。

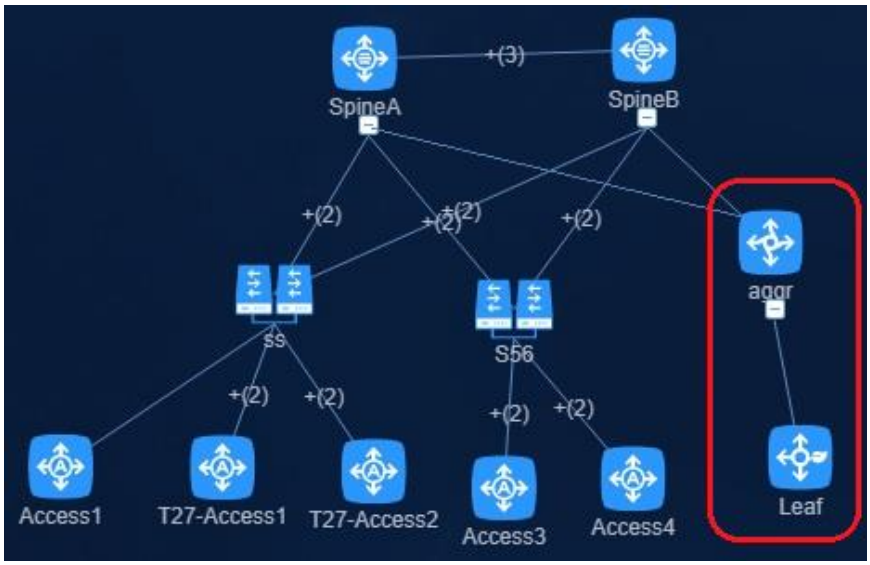
Add Switching Device ページで、次のパラメーターを設定します。

- **Device Role**: **aggregatio** を選択します。集約デバイスを手動で組み込んだ場合、コントローラーはデバイスのロール情報を確認しません。
- **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**: 追加するデバイスのデバイスモデルを選択します。
- **Control Protocol Template**: 新しいテンプレートを作成することも、デフォルトのテンプレートを使用することもできます。



集約デバイスが正常に組み込まれると、**Device State** は **Active** になり、**Device Role** は **aggregation** になります。

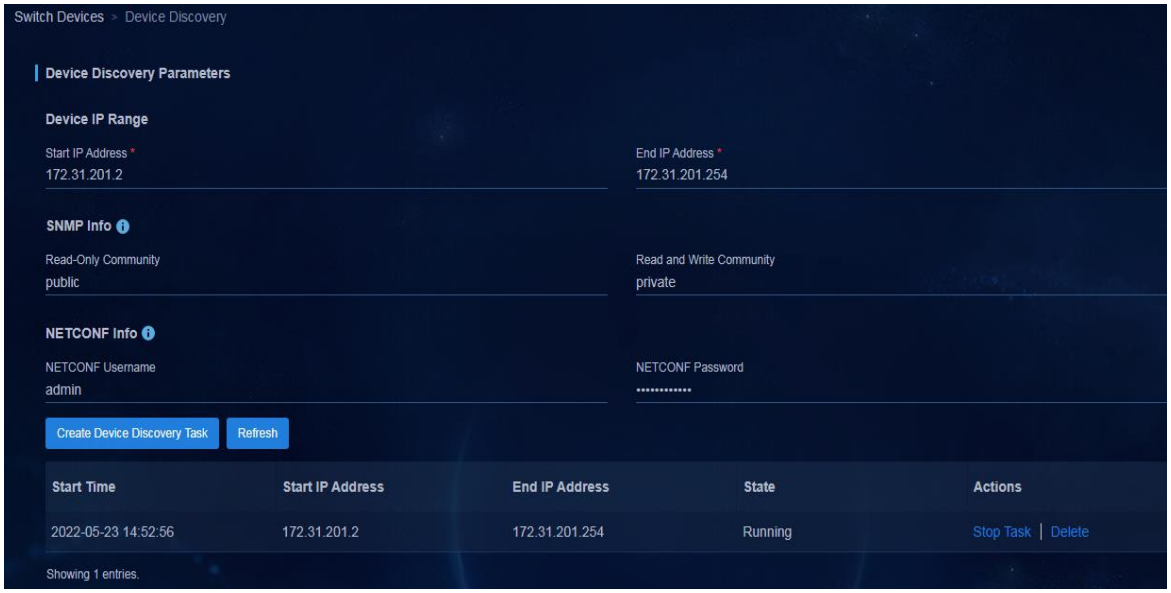
集約デバイスのトポロジ接続を表示するには、**Monitor** > **Topology** > **Campus Topo** ページに移動します。

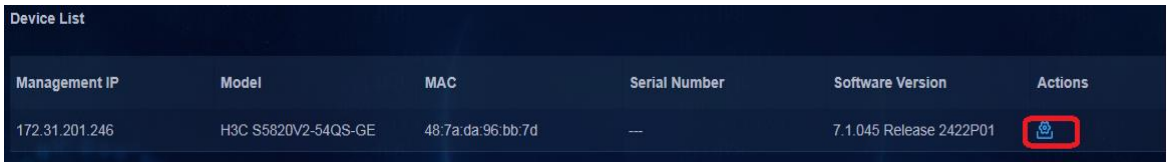


デバイスの自動検出

Guide > **Auto Find** ページに移動します。

IP アドレス範囲および SNMP パラメーターを構成し、**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。次の図に示すように、組み込まれていないデバイスが **Device List** に表示されます。





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。**Device List** でデバイスを選択し、デバイス組み込みアイコン をクリックして、**Add Switching Device** ページに入ります。このページのパラメーター設定については、『Manually adding devices』を参照してください。

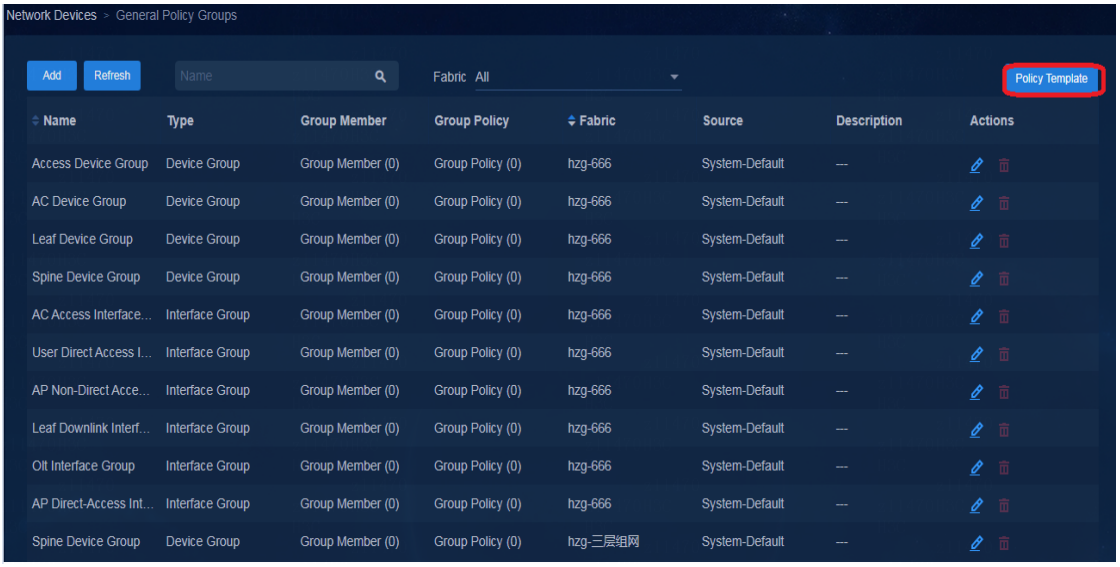
ポリシーテンプレートの設定

ポリシーテンプレートを設定するには、次の 2 つの方法があります。このセクションでは、キャンパスウィザードを例にして設定について説明します。

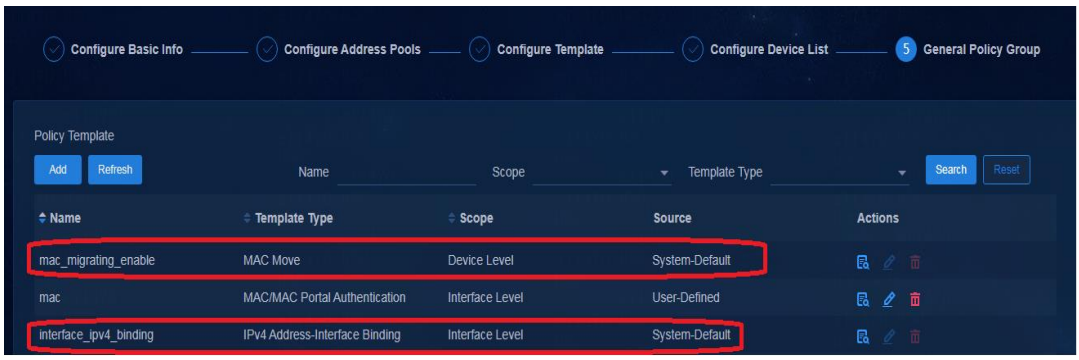
- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Device Onboarding Plan** ページに移動し、**Step 5 Policy Template** でポリシーテンプレートを設定します。
- **Not using the campus wizard**: **Automation** > **Campus Network** > **Device Groups** > **General Policy Groups** ページに移動し、ページの右上隅にある **Policy Template** をクリックします。

ポリシーテンプレートを設定するには、次の手順を実行します。

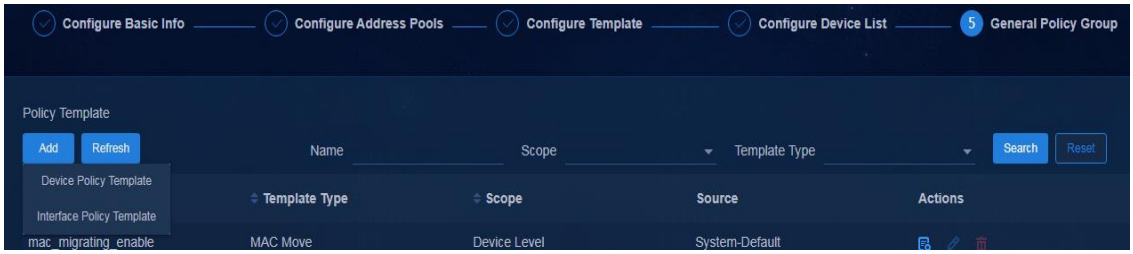
1. 次の図に示すように、**General Policy Groups** ページで、**Policy Template** をクリックします。



2. **Policy Template** の設定ページでは、次の図に示すように、**interface_ipv4_binding** と **mac_migrating_enable** の 2 つのデフォルトポリシーが定義されています。
   - **interface_ipv4_binding**: このポリシーを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します。ip verify source ip-address mac-address コマンドは、このポリシーテンプレートがインターフェイスに適用された後にインターフェイスに展開されます。ベストプラクティスとして、現在のソリューションではこのポリシーを使用しないでください。
   - **mac_migrating_enable**: このポリシーを MAC 移動のリーフデバイスグループに適用します。ユーザーが同じリーフデバイスの同じダウンリンクインターフェイス上で移動する場合、または同じリーフデバイスの異なるダウンリンクインターフェイス間で移動する場合は、このポリシーを設定します。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インターフェイス間または異なる VLAN 間で移動する場合、または異なるアクセスデバイス間で移動する場合は、このポリシーを設定します。ポリシーの設定後、port-security mac-move permit コマンドが展開されます。現在のソリューションでこのポリシーを使用する必要があります。



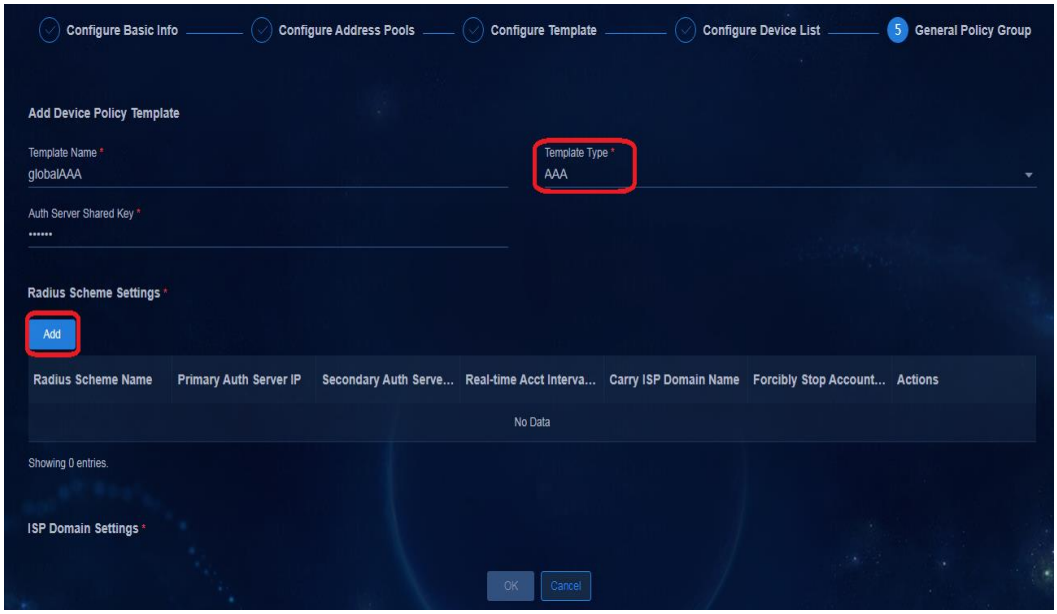
3. **Add** をクリックし、ドロップダウンリストから **Device Policy Template** または Interface Policy Template を選択して、ポリシーテンプレートを追加します。
   - **Device Policy Template**: デバイスポリシーテンプレートは、AAA、802.1X 認証、MAC 認証、および MAC 移動設定のデバイスグループに適用できます。
   - **Interface Policy Template**: インターフェイスポリシーテンプレートは、802.1X 認証および MAC 認証設定用のインターフェイスグループ(主にリーフダウンリンクインターフェイス)に適用できます。



次の項では、デバイスポリシーテンプレート、インターフェイスポリシーテンプレート、およびユーザー定義ポリシーテンプレートの設定と、ポリシーテンプレートを表示する方法について説明します。

AAA タイプのデバイスポリシーテンプレートの設定

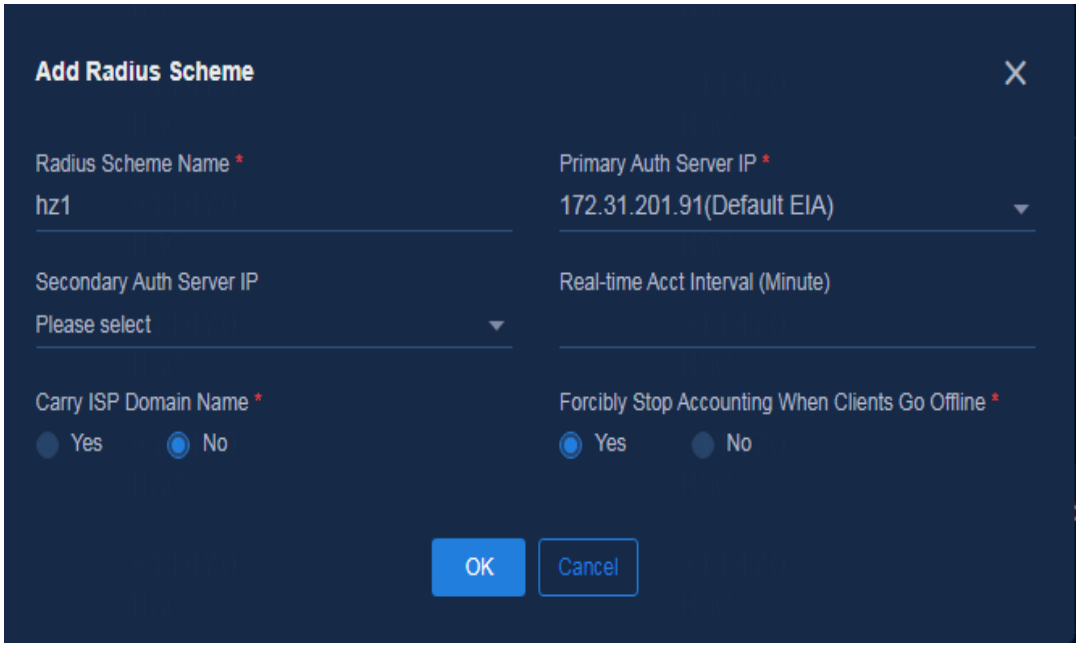
1. 次のパラメーターを設定します。
   - **Template Name**: テンプレートの一意の名前を入力します。
   - **Template Type**: **AAA** を選択すると、AAA の設定ページが表示されます。
   - **Auth Server Shared Key**: 必要に応じてキーを構成します。キー情報はデバイスに配布され、デバイスと EIA 間の通信用に EIA に同期化されます。キーは最大 64 文字をサポートし、大文字と小文字が区別されます。漢字、スペースおよび特殊文字<>&?はサポートされていません。



2. RADIUS スキーム設定を構成します。

   Radius Scheme 領域で **Add** をクリックし、次のパラメーターを設定します。
   - **Primary Auth Server IP**: ユーザー認証用の EIA サーバー(EIA V9 または EIA V7)の IP アドレスを入力します。パラメーターの詳細については、『Configuring AAA』を参照してください。
   - **Real-time Acct Interval(Minute)**: デフォルトでは **15**。
   - **Carry ISP Domain Name**: デフォルトで **No** を選択します。
     - No に設定されている場合は、RADIUS 認証パケットで使用されるユーザー名にドメイン名が含まれていないことを意味します。デフォルトでは、EIA にドメイン名サフィックスは含まれていません。
     - **Yes** に設定されている場合は、RADIUS 認証パケット内のユーザー名にドメイン名が含まれていることを意味します。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@ドメイン名を続ける必要があります。

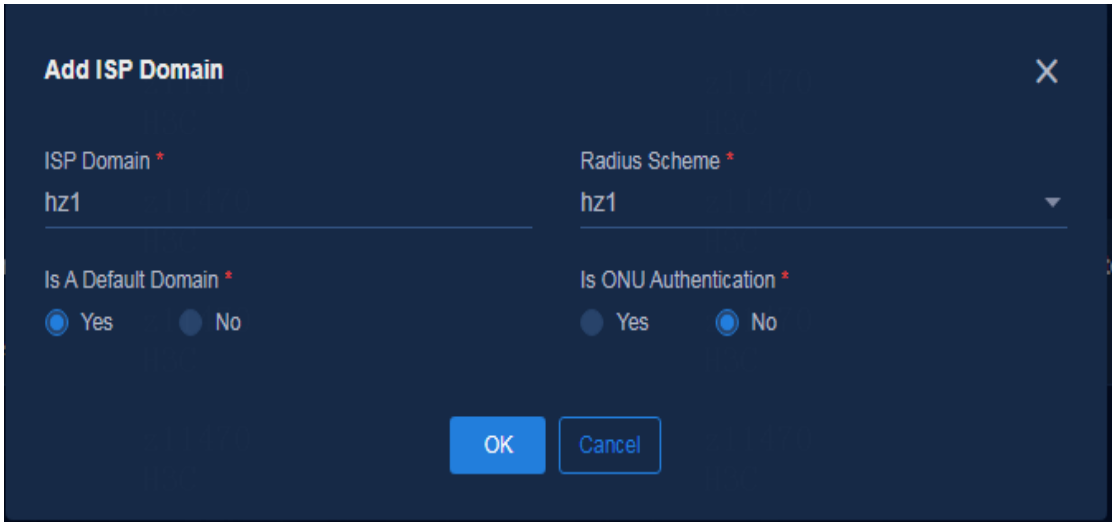
- **Forcibly Stop Accounting When Clients Go Offline**: **Yes** を選択すると、クライアントがオフラインになった直後にアカウンティングが停止します。**No** を選択すると、クライアントがオフラインになった直後にアカウンティングが停止しません。



3. ISP ドメインの設定を構成します。

   ISP Domain Settings 領域で **Add** をクリックし、次のパラメーターを設定します。

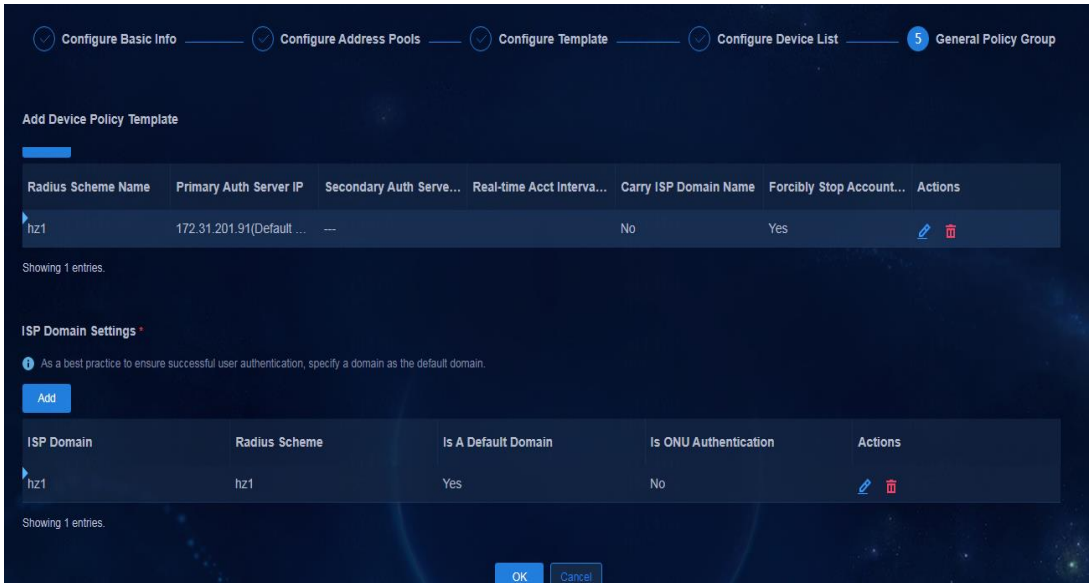
   - **Radius Scheme** : ドロップダウンリストから RADIUS スキームを選択します。前の手順で追加した RADIUS スキームの名前が表示されます。
   - **Is A Default Domain**: **Yes** を選択します。
   - **Is ONU Authentication**: **No** を選択します。



重要:

各 AAA テンプレートには、デフォルトドメイン名が 1 つだけ必要です。複数の ISP ドメイン名を追加できます。ただし、通常は、RADIUS スキーム名と ISP ドメイン名を 1 つずつ追加します。

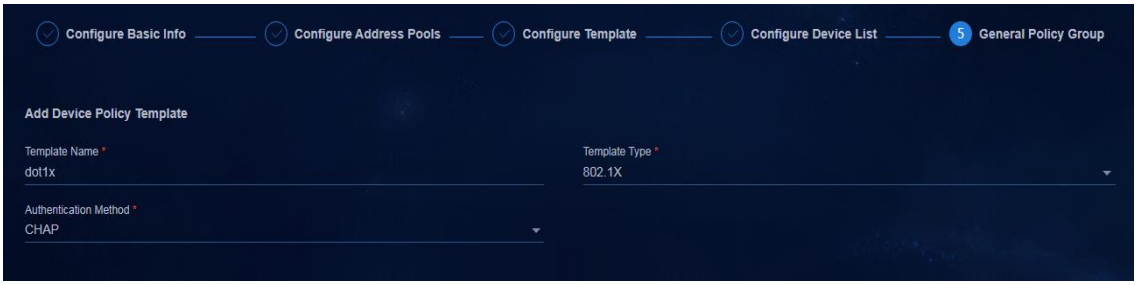
AAA テンプレートが設定されると、次のように表示されます。



802.1X タイプのデバイスポリシーテンプレートの設定

次のパラメーターを設定します。

- **Template Type**: **802.1X** を選択します。
- **Authentication Method**： 必要に応じて認証方法を選択します。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、ワイヤレス認証には **EAP** を選択することをお薦めします。



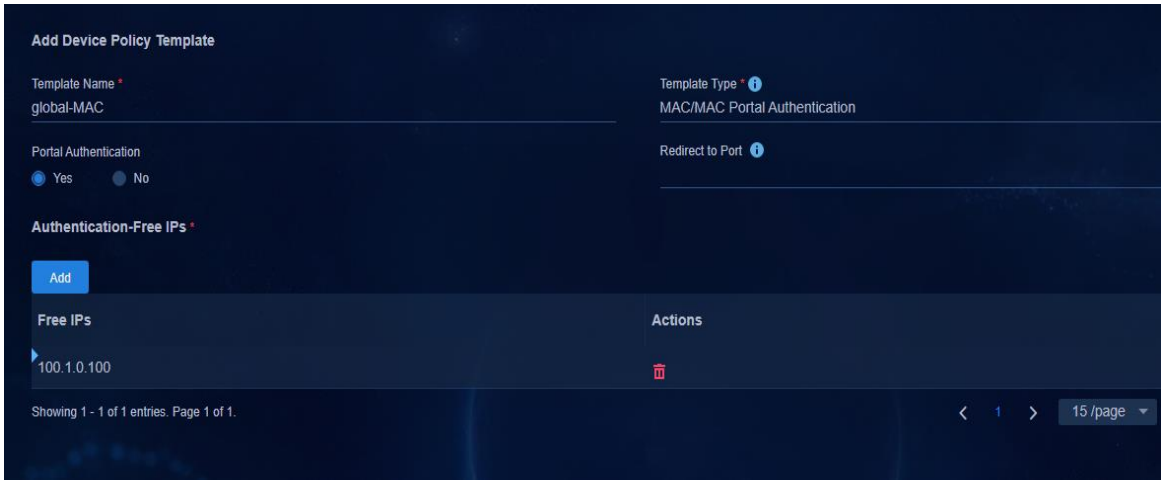
MAC/MAC ポータル認証タイプのデバイスポリシーテンプレートの設定

次のパラメーターを設定します。

- **Template Type**: **MAC/MAC Portal Authentication** を選択します。
- **Portal Authentication**: **Yes** を選択して、MAC ポータル認証をイネーブルにします。
- **Redirect to Port** : HTTPS パケットリダイレクションのリスニングポートを指定します。既知のプロトコルで使用されるポートは指定せず、そのポートが他のサービスで使用されていないことを確認します。ポートを指定しない場合、デフォルトのポート番号 6654 が使用されます。display tcp コマンドを実行すると、使用されている TCP ポート番号を表示できます。
- **Authentication-Free IPs**: ポータル認証がイネーブルになっている場合は、EIA サーバーの IP アドレスを認証フリーIP として指定する必要があります。

重要:

AAA テンプレートにプライマリ認証サーバーとセカンダリ認証サーバーが設定されている場合は、プライマリ認証サーバーとセカンダリ認証サーバーの両方の 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。



802.1X タイプのインターフェイスポリシーテンプレートの設定

次のパラメーターを設定します。

- **Template Type**: **802.1X** を選択します。
- **Enable The Escape Function**： デフォルトでは、値は **Yes** です。必要に応じて、この機能を無効にできます。
- **Unicast Trigger**： デフォルトでは、値は **Yes** です。デフォルト設定を使用します。
- **Guest Access**: デフォルトでは、値は **No** です。詳細については、『Guest online or authentication failure online』を参照してください。
- **Access on Authentication Failure**： デフォルトでは、値は **Yes** です。詳細は、『Guest online or authentication failure online』を参照してください。この機能と MAC ポータル認証は相互に排他的です。MAC ポータル認証を構成する必要がある場合は、**No** を選択します。

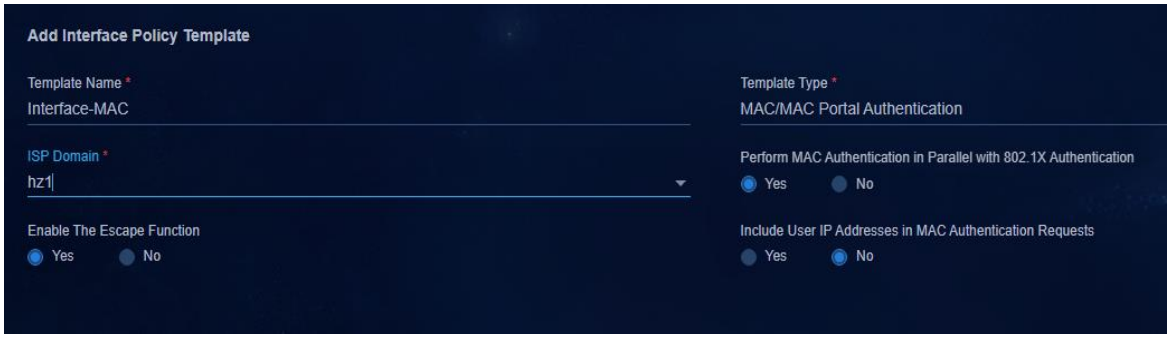
MAC/MAC ポータル認証タイプのインターフェイスポリシーテンプレートの設定

次のパラメーターを設定します。

- **Template Type**: **MAC/MAC Portal Authentication** を選択します。
- **ISP Domain**: 前の AAA 設定のドメイン名がドロップダウンリストに表示されます。ISP ドメイン名が選択されていない場合は、AAA テンプレート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**: デフォルトでは、値は **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**: デフォルト設定を使用します。
- **Include User IP Addresses in MAC Authentication Requests**: デフォルトでは、値は **No** です。**Yes** に設定すると、システムは mac-authentication carry user-ip コマンドをインターフェイスに展開します。スタティック IP アドレスを使用するエンドポイントに接続されたインターフェイスに対して、この機能をイネーブルにします。

> ⚠ **警告!**
>
> mac-authentication carry user-ip コマンドは、By IP Range 認証の場合と、Bind User IP 認証がアクセスポリシーで設定されている場合にだけ使用します。それ以外のユーザー認証の場合は、このコマンドを使用しないでください。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、コントローラーは ARP スヌーピング設定を発行して、スタティック IP アドレスを EIA に配信します。
>
> mac-authentication carry user-ip コマンドの制限の詳細については、『IP アドレス範囲に基づく高速オンライン』を参照してください。

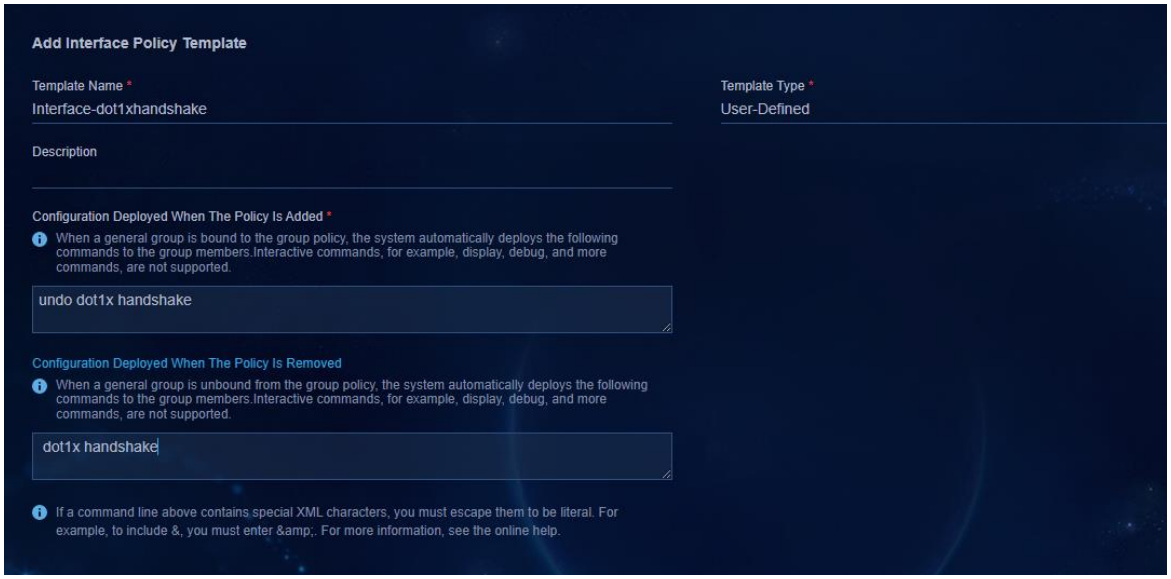


ユーザー定義のポリシーテンプレートの構成

システムは、定義済みのテンプレートを除き、ユーザー定義のデバイスポリシーテンプレートとインターフェイスポリシーテンプレートもサポートしています。この項では、ユーザー定義の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。

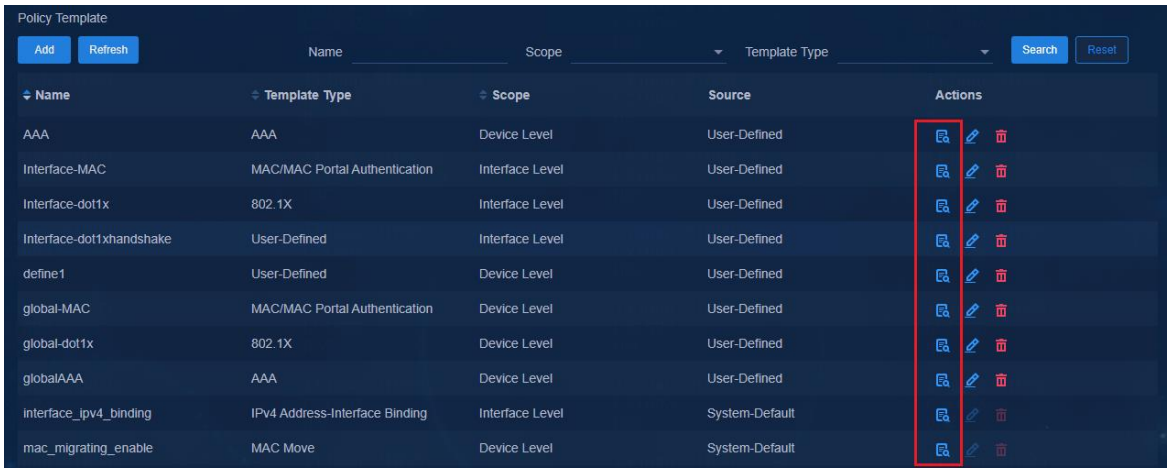
次のパラメーターを設定します。

- **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た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。構成しないと、ポリシーの削除時にデプロイされた構成を削除できません。



ポリシーテンプレートの表示

ポリシーテンプレートを構成した後、テンプレートの **Actions** 列のアイコンをクリックして詳細を表示し、アイコンをクリックしてテンプレートを編集できます。事前定義済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一般ポリシーグループのグループポリシーに適用する必要があります。

ポリシーテンプレートを設定したら、デバイスグループでグループポリシーを設定する必要があります。現在、AD-Campus ソリューションでは、リーフデバイスグループとリーフダウンリンクインターフェイスグループのグループポリシーを設定するだけで済みます。

デバイスグループのグループポリシー設定の構成

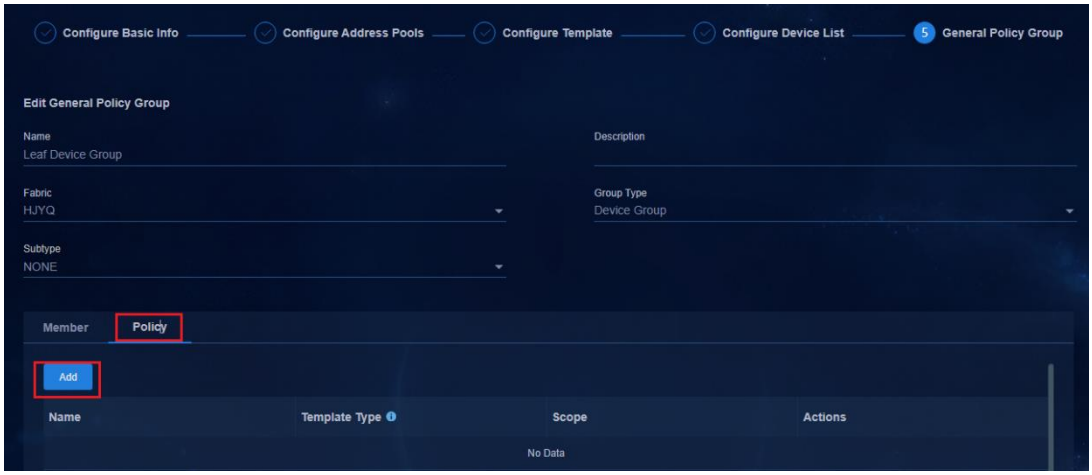
リーフデバイスグループには、定義済みのデバイスポリシーテンプレート(AAA、802.1X 認証、MAC/MAC ポータル認証、**mac_migrating_enable** という名前の MAC 移動など)を指定できます。また、ユーザー定義のポリシーテンプレートも指定できます。

リーフデバイスグループのグループポリシー設定を構成するには、以下の手順に従ってください。

1. デバイスグループリストで、**Leaf Device Group** という名前のデバイスグループの **Actions** カラムにある **Edit** アイコンをクリックします。

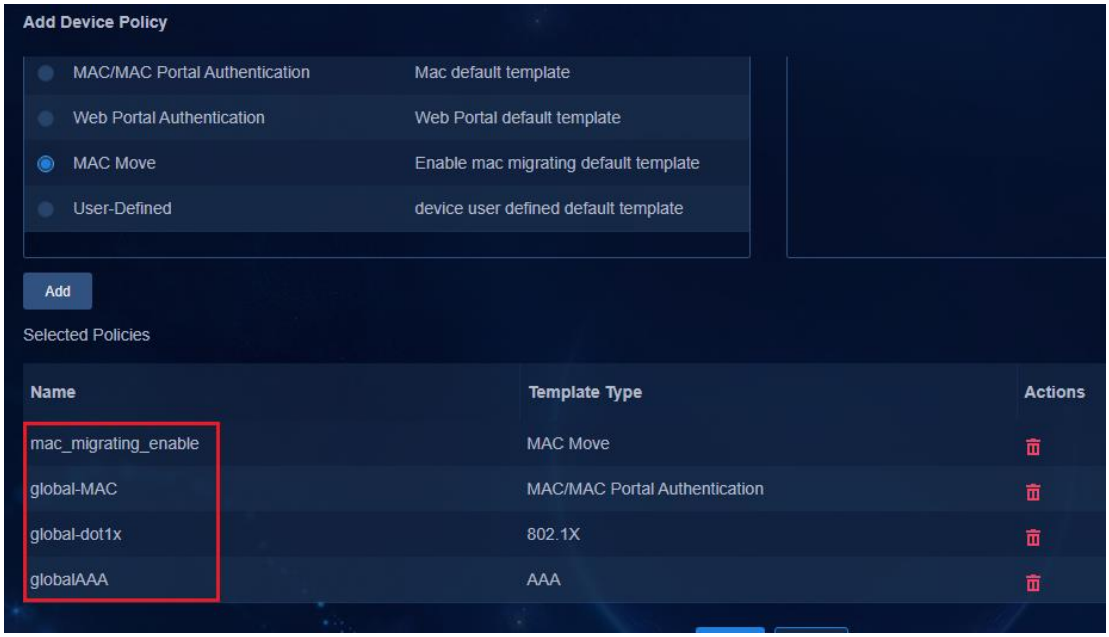
2. **Policy** タブをクリックし、**Add** をクリックします。

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



3. **Available Policy Templates** リストからテンプレートタイプを選択し、**Available AAA Policies** リストからポリシーテンプレートを選択して、**Add** をクリックします。

4. 前の手順を繰り返して、**802.1X**、**MAC/MAC Portal Authentication**、および **MAC Move** タイプのポリシーテンプレートを追加します。**OK** をクリックして設定を保存します。

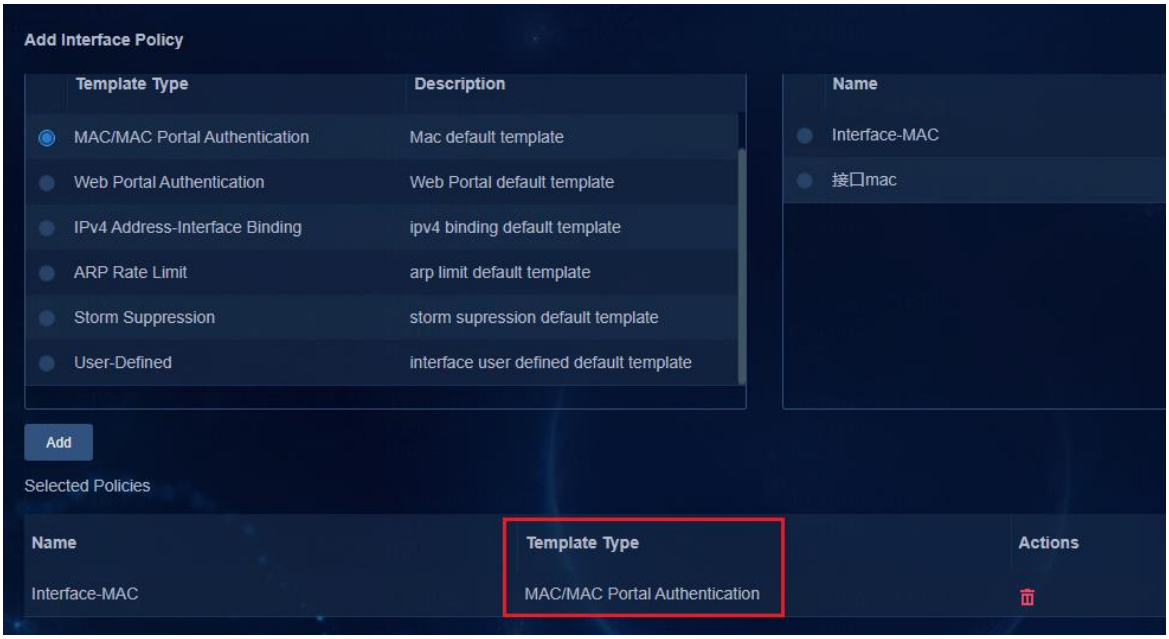


インターフェイスグループのグループポリシー設定の構成

ポリシーテンプレートをリーフデバイスグループに適用するのと同じ方法で、ポリシーテンプレート(802.1X 認証、MAC/MAC ポータル認証、およびユーザー定義ポリシーテンプレートを含む)を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。**OK** をクリックして、設定を保存します。

注:

必要に応じて、リーフダウンリンクインターフェイスで 802.1X および MAC 認証を設定します。たとえば、エンドポイントで MAC 認証を使用する場合、MAC/MAC ポータル認証テンプレートをインターフェイスに適用するだけで済みます。エンドポイントで 802.1X 認証を使用する場合、802.1X 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適用する必要があります。



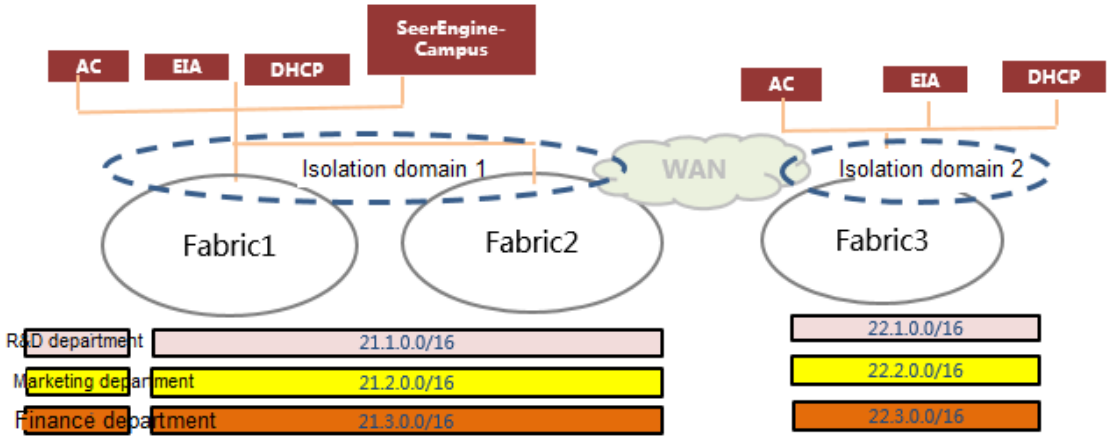
アクセスネットワークの設定

ここでは、キャンパスウィザードを使用したアクセスネットワークの設定について説明します。**Guide** > **Campus Wizard** > **Access Network Plan** ページに移動します。このページでは、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を含むオーバーレイ設定を設定する方法について説明します。

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。各分離ドメインには、独自の DHCP システム、認証システム、および無線 AC があります。

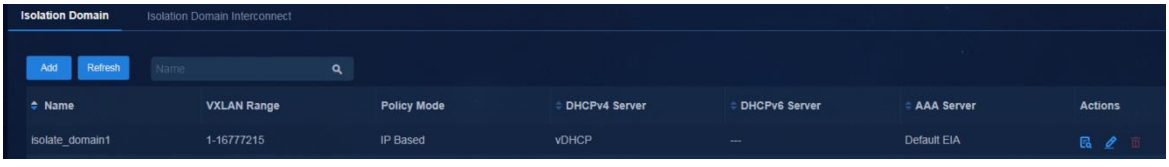
分離ドメインには複数のファブリックを含めることができますが、ファブリックは 1 つの分離ドメインにのみ属することができます。



分離ドメインの構成には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Access Network Plan** ページに移動し、**Step 1 Isolation Domain** で **Isolation Domain** タブをクリックして、隔離ドメインを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: 隔離ドメインを設定するには、**Automation** > **Campus Network** > **Isolation Domain** > **Isolation Domain** ページに移動します。

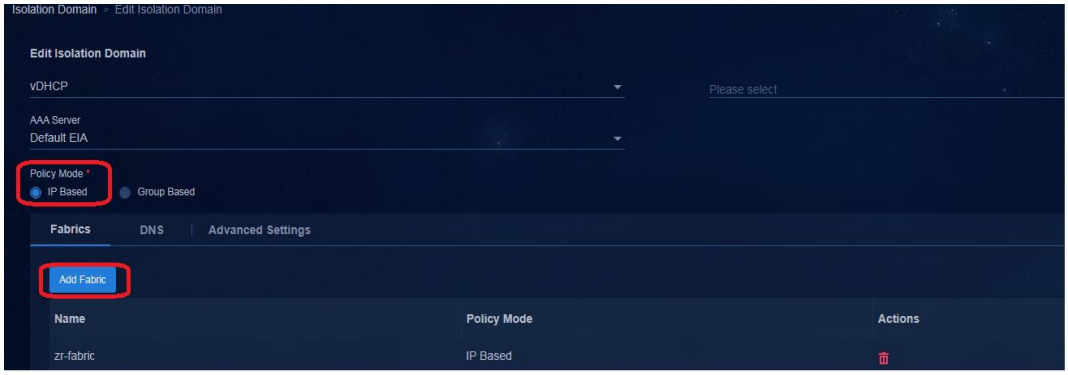
デフォルトでは、システムには **isolate_domain1** という名前の分離ドメインがあり、デフォルトのポリシーモードは **IP Based** です。このドメインを変更する必要はありません。この項では、単一ファブリックシナリオでの分離ドメインの設定についてのみ説明します。分離ドメインの相互接続設定の詳細については、『AD-Campus 6.2 Multi-Campus and Multi-Fabric Configuration Guide』を参照してください。



分離ドメインを構成するには、次の手順に従います。

1. その分離ドメインの **Actions** コラムにある **Edit** アイコンをクリックし、次のパラメーターを設定します。

- **DHCP Server**: 分離ドメインの 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 サーバーがあります。必要に応じて構成できます。
  - DHCPv4 サーバーは、密結合と疎結合の両方をサポートしています。密結合モードでは、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。疎結合モードでは、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、IPv6 サービスにのみ必要です。詳細については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。
- **AAA Server**: 分離ドメイン内のユーザーの認証サーバーを指定します。
- **Policy Mode**: デフォルトでは、値は **IP Based** です。
- **Add Fabric**: 分離ドメインのファブリックを選択します。分離ドメインと同じポリシーモードを使用するファブリックのみを選択できます。
- **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**: 分離ドメインの DNS サーバーの IP アドレスを指定します。



プライベートネットワークの設定

プライベートネットワークの作成

プライベートネットワークの設定には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Access Network Plan** ページに移動し、**Step 2 Private Network** で **Private Network** タブをクリックして、プライベートネットワークを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: プライベートネットワークを設定するには、**Automation** > **Campus Network** > **Private Network** > **Private Network** ページに移動します。

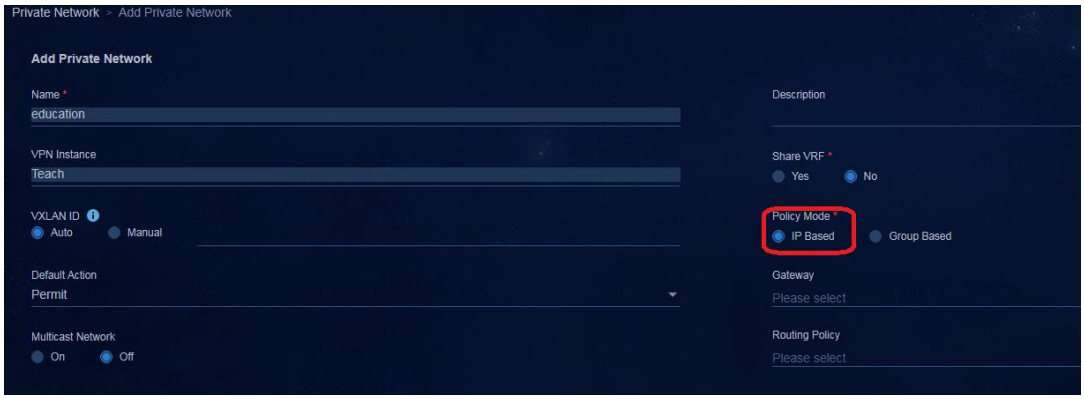
プライベートネットワークを構成するには:

1. 分離ドメインの構成が完了したら、**Next** をクリックして、プライベートネットワーク構成ページにアクセスします。**Add** をクリックして、**Add Private Network** ページに入ります。
2. **Add Private Network** ページで、次の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。
   - **Share VRF**: デフォルトでは、値は **No** です。値が **Yes** の場合、プライベートネットワークは、共有ゲートウェイが作成され、共有ゲートウェイによって使用される IT リソースグループが作成された場合にのみ使用できます。
   - **VXLAN ID**: VPN インスタンスに関連付けられた L3VNI ID。デフォルトでは、値は Auto です。
   - **Default Action**: 次のオプションがサポートされています。

- **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どのユーザーも相互にアクセスできません。

○ **Multicast Network**: No を選択します。必要に応じて有効にできます。

○ **Policy Mode**: IP Based を選択します。



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の作成

レイヤー2 ネットワークドメインの設定には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Access Network Plan** ページに移動し、**Step 2 Private Network** で **Layer 2 Network Domain** タブをクリックして、レイヤー2 ネットワークドメインを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: **Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動して、レイヤー2 ネットワークドメインを設定します。

レイヤー2 ネットワークドメインを設定するには、次の手順を実行します。

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

2. **Add** をクリックします。表示されたページで、次のパラメーターを構成します。

○ **Isolation Domain**: プライベートネットワークが配置されている分離ドメインを選択します。

○ **Private Network**: 作成され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、指定された分離ドメイン内のデバイスにプライベートネットワークの設定が展開されます。

○ **Type**:

- **Normal**: ユーザーサービスの場合は **Normal** を選択します。
- **Escape**: エスケープサービスの構成時に **Escap** を選択します。

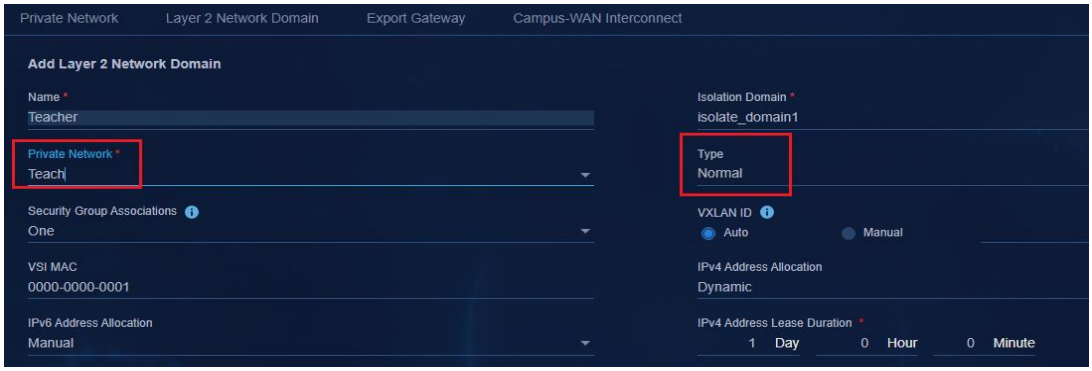
- **Guest**: ゲストサービスの構成時に **Guest** を選択します。詳細は、『Guest online or authentication failure online』を参照してください。
- **Authentication Failure**: このタイプは、認証失敗がないシナリオで使用されます。詳細は、『Guest online or authentication failure online』を参照してください。

- **Security Group Associations**: IP ベースのポリシーでは **Only one** を選択できます。つまり、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にしか割り当てることができません。
- **VXLAN ID**: レイヤー2 ネットワークドメインの VXLAN ID を設定します。デフォルトでは **Auto** に設定されています。これは、システムが自動的に VXLAN ID を割り当てることを意味します。**Manual** に設定して、VXLAN ID を手動で設定することもできます。
- **VSI MAC**: デフォルト値は 0000-0000-0001 です。必要に応じてこのパラメーターを変更できます。他のパラメーターのデフォルト設定を保持します。
- IPv4 アドレス割り当て:動的とは、ユーザーが DHCP サーバーから IP アドレスを取得することを意味します。手動とは、DHCP アドレスプールが構成されておらず、オンラインになるために静的 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。

重要:

IPv4 Address Allocation パラメーターが **Dynamic** に設定されていて、静的 IP アドレスを使用する一部のユーザーエンドポイントをオンラインにするために認証する必要がある場合は、**Network Parameters** > **DHCP Server** > **Prohibited IP Address Allocation** ページにエンドポイントの静的 IP アドレスを追加する必要があります。

- IPv6 アドレス割り当て: オプションには、手動、SLACC、ステートフル DHCPv6、およびステートレス DHCPv6 があります。IPv6 サービス構成の詳細については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。
- **IPv4 Address Lease Duration**: IPv4 アドレスのデフォルトのリース期間を設定します。



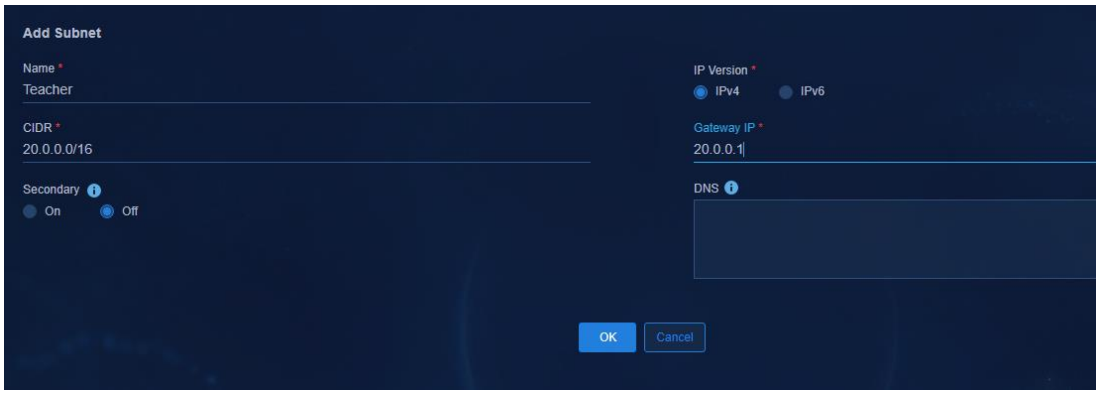
3. **Subnets** タブで、**Add** をクリックして **Add Subnet** ページを開きます。パラメーターを構成し、**IP Version** に **IPv4** を選択し、**OK** をクリックして構成を保存します。IPv6 サービス構成の詳細については、『AD-Campus 6.2 IPv6 Service Configuration Guide』を参照してください。

   このページの **Secondary** パラメーターには、次のオプションがあります。

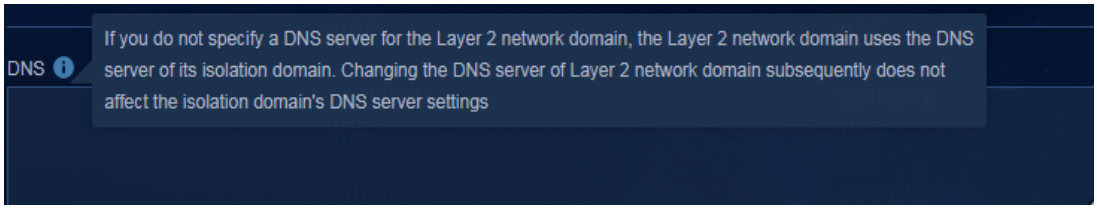
   - **No**: **No** を選択すると、サブネットがプライマリネットワークとして使用されます。IPv4 アドレス割当てモードが動的の場合、ユーザーアドレス割当て用のサブネットアドレスに基づいて、DHCP サーバー上にアドレスプールが作成されます。
   - **Yes**: **Yes** を選択すると、サブネットがセカンダリネットワークとして使用されます。システムは、サブネットアドレスに基づいて DHCP サーバーにアドレスプールを作成しません。これは、エンドポイントが静的 IP アドレスを使用する場合に適用されます。セカンダリネットワークを作成する前に、プライマリネットワークが作成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** 機能を使用できません。

⚠ **警告!**

- セキュリティグループには、1 つのプライマリネットワークと複数のセカンダリネットワークのみを含めることができます。実際のネットワークの状態に基づいて 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。
- **Bind User IP** 機能は、セカンダリネットワークが使用されている場合、アクセスポリシーでは使用できません。
- 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、古い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し、複数のエンドポイントのセグメントを 1 つのセキュリティグループに割り当て、ACL リソースを節約するために使用されます。

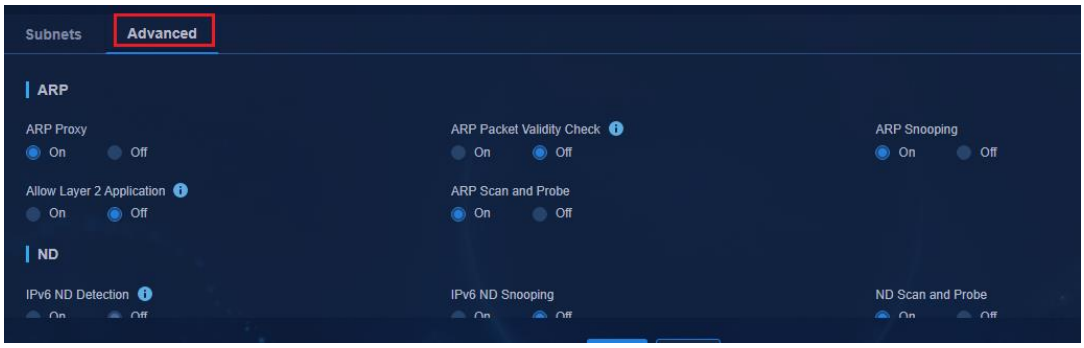


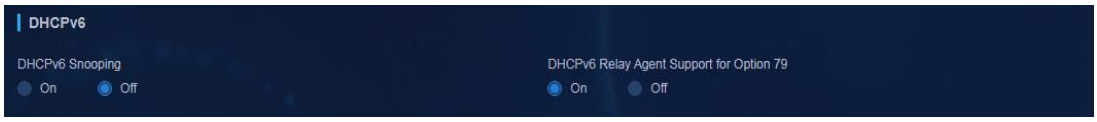
Add Subnet ページの **DNS** 設定では、レイヤー2 ネットワークドメインの DNS サーバーIP アドレスを指定する必要があります。



4. **OK** をクリックして設定を保存し、**Add Layer 2 Network Domain** 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**: デフォルトでは、値は On です。これは、ARP プロキシがイネーブルであることを意味します。
   - **ARP Packet Validity Check** : デフォルトでは、この値は **Off** です。このパラメーターはアクセスデバイスに適用されます。この機能を使用すると、アクセスデバイスは権限のないユーザーの ARP パケットを検出して廃棄し、不正なユーザーおよびゲートウェイからの攻撃を防止します。IPv4 アドレス割当てモードが **Manual** の場合、この機能は有効にできません。
   - **ARP Snooping**: ARP スヌーピングエントリーは、高速な ARP 応答を提供するために、ARP パケットをリッスンすることによって設定されます。ブロードバンド IoT エンドポイントをオフラインにできない場合は、**On** を選択します。
   - **Allow Layer 2 Application**: デフォルトでは、値は **Off** です。**Yes** を選択すると、作成されたセキュリティグループはレイヤー2 アプリケーションをサポートし、セキュリティグループ内のレイヤー2 相互接続が許可されます。

- **ARP Scan and Probe**: デフォルトでは、値は **Off** です。値が **Yes** の場合、ARP ブロードキャストはネットワーク全体にフラッディングされず、ARP 学習はリーフデバイスのローカルスキャンに依存し、テーブルエントリーは EVPN を介して同期化され、スイッチは ARP パケットを転送しません。
- **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 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 サービスがない場合は、このパラメーターを有効にしないでください。
- **ND Scan and Probe**: デフォルトでは、値は **Off** です。値が **Yes** の場合、ND ブロードキャストはネットワーク全体にフラッディングされず、ND ラーニングはリーフデバイスのローカルスキャンに依存し、テーブルエントリーは EVPN を介して同期され、スイッチは ND パケットを転送しません。
- **DHCPv6 Snooping**: デフォルトでは、値は **Off** です。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、IPv6 アドレス/IPv6 プレフィクスと MAC アドレス間のマッピングを記録するようにするには、この機能をイネーブルにします。
- **DHCPv6 Relay Agent Support for Option 79**: デフォルトでは、値は **On** です。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には、この機能をイネーブルにします。





⚠ 警告!

- **Allow Layer 2 Application** 機能をイネーブルにすると、セキュリティグループは、ブロードキャストパケット、不明マルチキャストパケット、および不明ユニキャストパケットの AC インターフェイスおよびトンネルインターフェイスへの転送を許可し、EVPN を介した VXLAN MAC 同期を許可します。つまり、SeerEngine キャンパスコントローラーは、VSI 設定をデバイスに展開するときに、flooding disable all all-direction コマンドまたは mac-advertising disable コマンドをデバイスに展開しません。
- **Allow Layer 2 Application** 機能をイネーブルにした後、リーフダウンリンクインターフェイスでブロードキャスト抑制を設定する必要があります。しきい値は、デバイスモデルとパケット量によって決定されます。詳細については、製品の R&D にお問い合わせください。

Allow Layer 2 Application 機能がイネーブルの場合、フラッド抑制は物理インターフェイスに展開できますが、集約インターフェイスには展開できません。リーフダウンリンクインターフェイスが集約インターフェイスの場合は、フラッド抑制を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設定します。

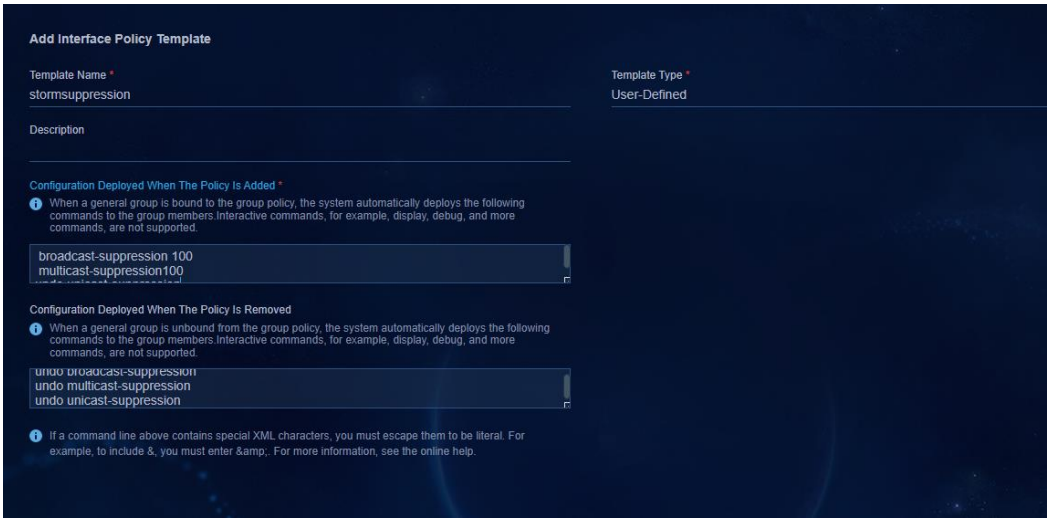
Automation > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Policy Templates** をクリックします。**Add** をクリックし、ドロップダウンリストから **Interface Policy Template** を選択します。**Template Type** で **User-Defined** を選択し、対応するテキストボックスに次のコマンドを追加します。

ポリシーが追加されたときに展開される設定:

```
#
broadcast-suppression pps 100   //The threshold is determined by the device
model and packet quantity. For more information, contact the product R&D.
 multicast-suppression pps 100
 unicast-suppression pps 100
#
```

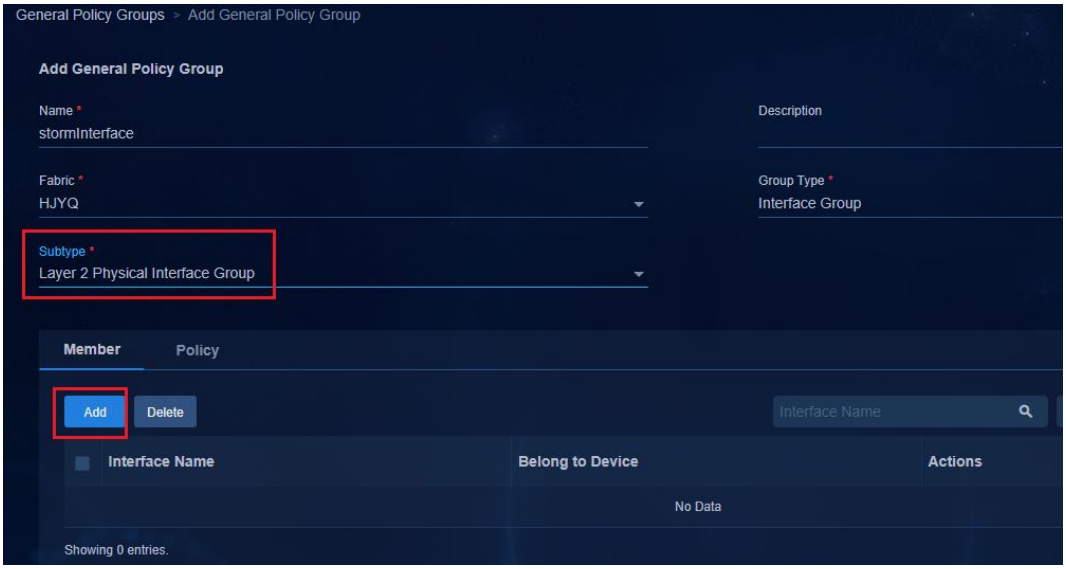
ポリシーが削除されたときに展開される設定:

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

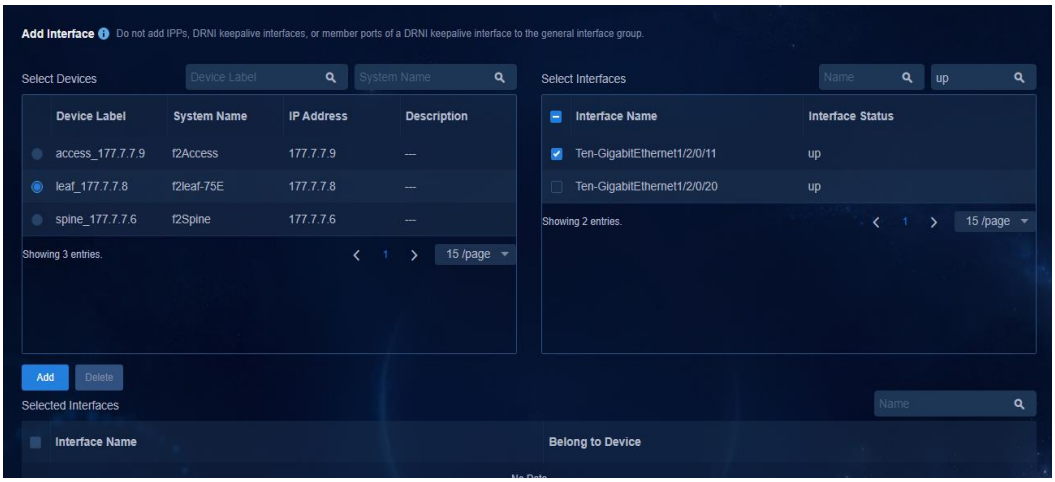


b. ユーザー定義のインターフェイスグループを設定します。

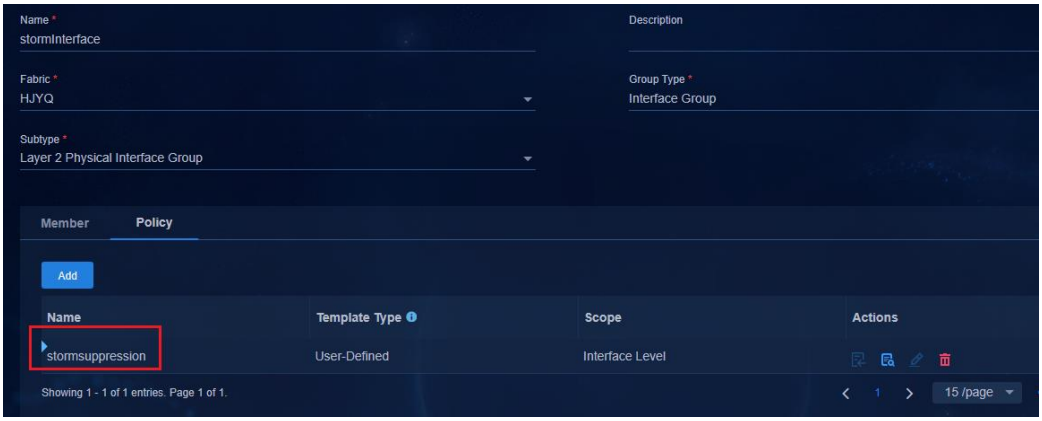
Automation > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Add** をクリックします。次の図に示すように、**Group Type** に **Interface Group** を選択し、**Subtype** に **Layer 2 Physical Interface Group** を選択します。



Member タブで、**Add** をクリックして **Add Interface** ページを開きます。フラッド抑制を構成する必要があるリーフダウンリンク集計インターフェイスのメンバーインターフェイスを選択し、**Add** をクリックします。次の図に示すように、選択したインターフェイスがインターフェイスリストに表示されます。



メンバーインターフェイスを選択した後、**OK** をクリックして **Add General Policy Grou**p ページに戻ります。Policy タブをクリックし、Add をクリックして Add Interface Group Policy ページを開きます。前の手順で構成したユーザー定義のフラッド抑制ポリシーを追加し、構成が完了したら **OK** をクリックします。



次に、メンバーインターフェイスに展開されたフラッド抑制関連の設定を表示できます。

```
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094
 broadcast-suppression pps 100
 multicast-suppression pps 100
unicast-suppression pps 100
 port link-aggregation group 1024
#
```

⚠ **警告!**

レイヤー2 ネットワークドメインでは、VSI MAC、VXLAN ID、および **Advanced** タブのパラメーター(**ARP Proxy**、**ARP Packet Validity Check**、**Allow Layer 2 Application**、**IPv6 ND Detection** など)は、展開後に編集できません。そのため、設定の前に、どの機能をイネーブルにする必要があるかを決定します。

セキュリティグループの構成

セキュリティグループの構成には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Access Network Plan** ページに移動し、**Step 3 Security Group** で U**ser Security Group** タブをクリックして、セキュリティグループを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: **Automation** > **Campus Network** > **Security Group** > **User Security Group** ページに移動して、セキュリティグループを設定します。

セキュリティグループを構成するには、次の手順に従います。

1. プライベートネットワークを作成した後、Next をクリックして Add Security Group : Configuration ページを開きます。User Security Group タブをクリックし、Add をクリックします。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 パラメーターに Norma を選択します。

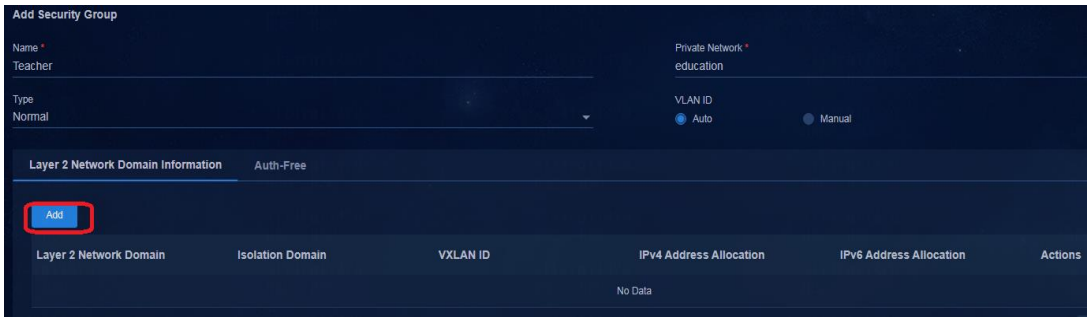
   次の種類のセキュリティグループがサポートされています。

   - **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。**User Security Group** タブで作成できる BYOD セキュリティグループは 1 つだけで、プライベートネットワーク **vpn-default** に属している必要があります。
   - **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。
   - **Critical** : エスケープセキュリティグループは、エスケープサービスに使用されます。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、クリティカル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クリティカル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。

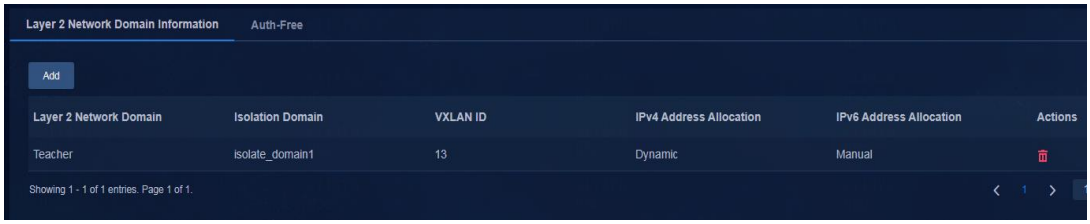
- **Guest**: ゲストセキュリティグループは、ユーザーが認証なしで特定のリソースにアクセスするために使用されます。通常、このグループには、ユーザーがクライアントソフトウェアやその他のアップグレードプログラムをダウンロードするサーバーが含まれます。
- **Authentication Failure**: 認証失敗セキュリティグループは、認証失敗のシナリオでユーザーが特定のリソースにアクセスするために使用されます。ここでの認証失敗とは、サーバーが、認証タイムアウトやネットワーク切断ではなく、ユーザーパスワードエラーなどの特定の理由でユーザー認証を拒否することを意味します。

VLAN ID:セキュリティグループの VLAN ID。割当て方法を選択する必要があります。

Manual を選択した場合、VLAN ID を手動で指定する必要があります。



2. **Layer 2 Network Domain Information** タブで **Add** をクリックし、レイヤー2 ネットワークドメインを追加します。**Available Layer 2 Network Domain** フィールドでレイヤー2 ネットワークドメインを選択し、アイコンをクリックして **Selected Layer 2 Network Domain** リストに追加します。**OK** をクリックし、**Add Security Group** ページに戻ります。



3. **OK** をクリックすると、次の図に示すように、User Security Group ページで追加したセキュリティグループを表示できます。

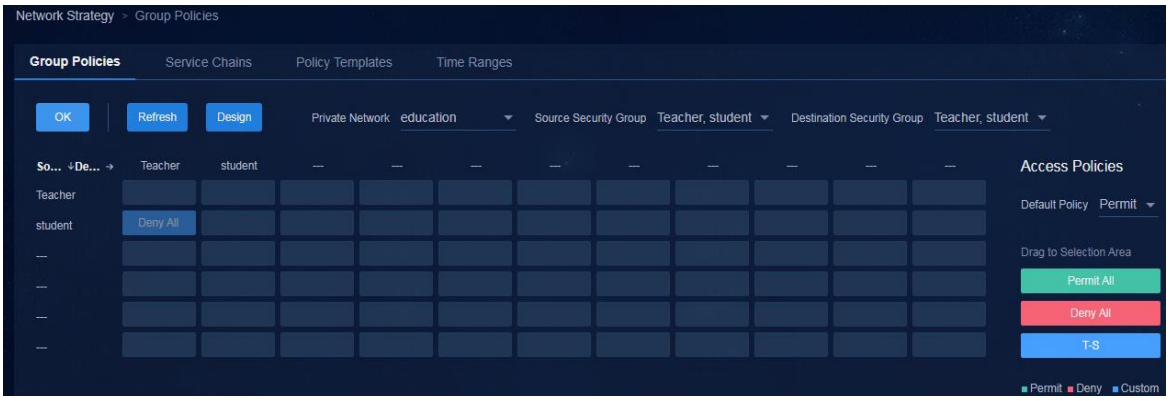
ネットワークポリシーの構成

ネットワークポリシーの設定には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **Access Network Plan** ページに移動し、**Step 4 Network Strategy** でネットワークポリシーを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: **Automation** > **Campus Network** > **Network Policy** ページに移動して、ネットワークポリシーを設定します。

Group Policies ページでは、グループポリシーテンプレートをマトリクスに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、設定が簡素化されます。

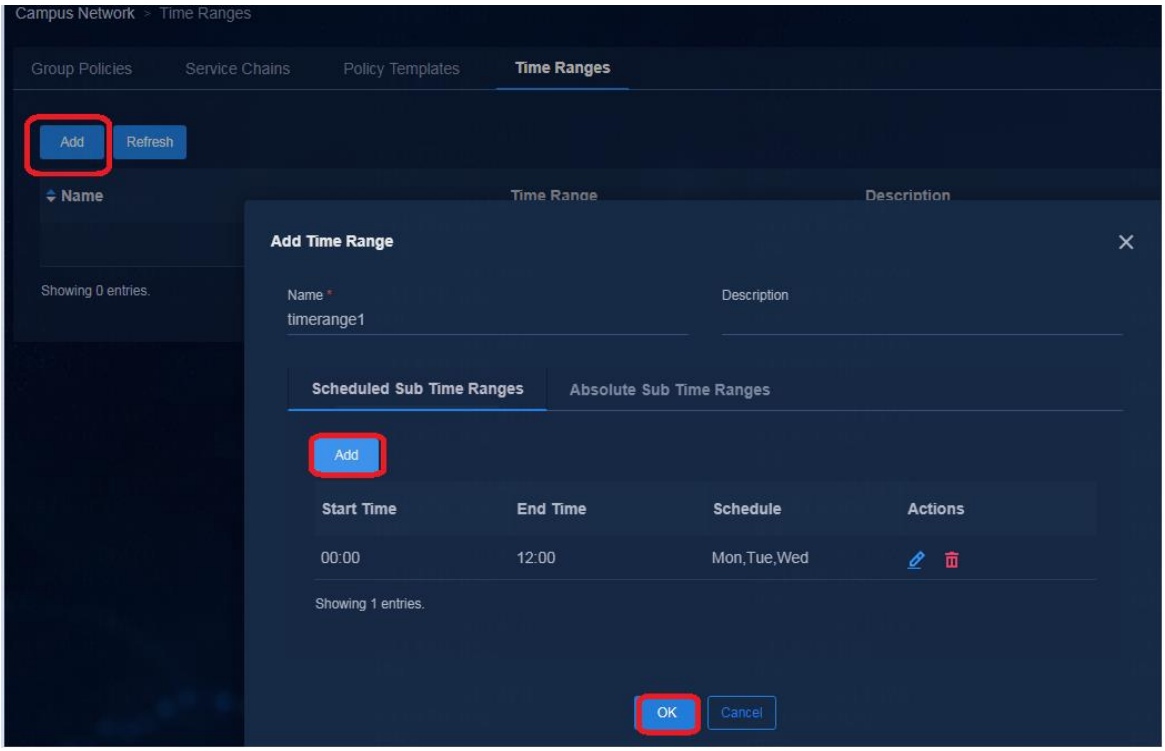
たとえば、教師セキュリティグループと生徒セキュリティグループを分離するには、**Deny All** ポリシーテンプレートをマトリックス内の対応する場所にドラッグし、**OK** をクリックします。



時間範囲の設定(オプション)

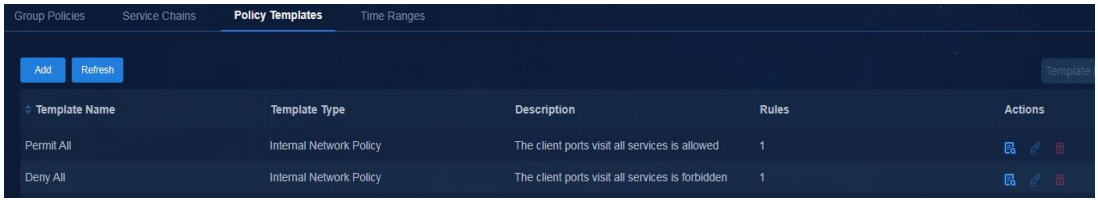
Time Range タブをクリックします。必要に応じて時間範囲を構成できます。

Add をクリックし、**Add Time Range** ページでパラメーターを構成します。構成が完了したら、アイコンをクリックしてパラメーター構成を保存し、**OK** をクリックして時間範囲を保存します。

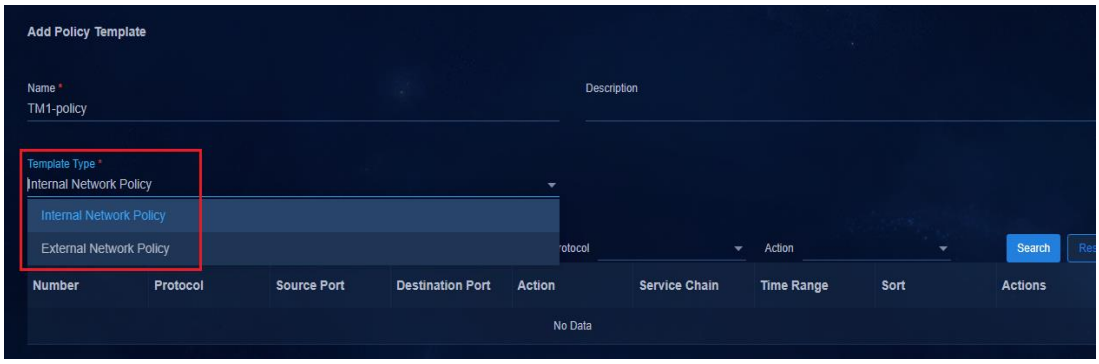


ポリシーテンプレートの設定

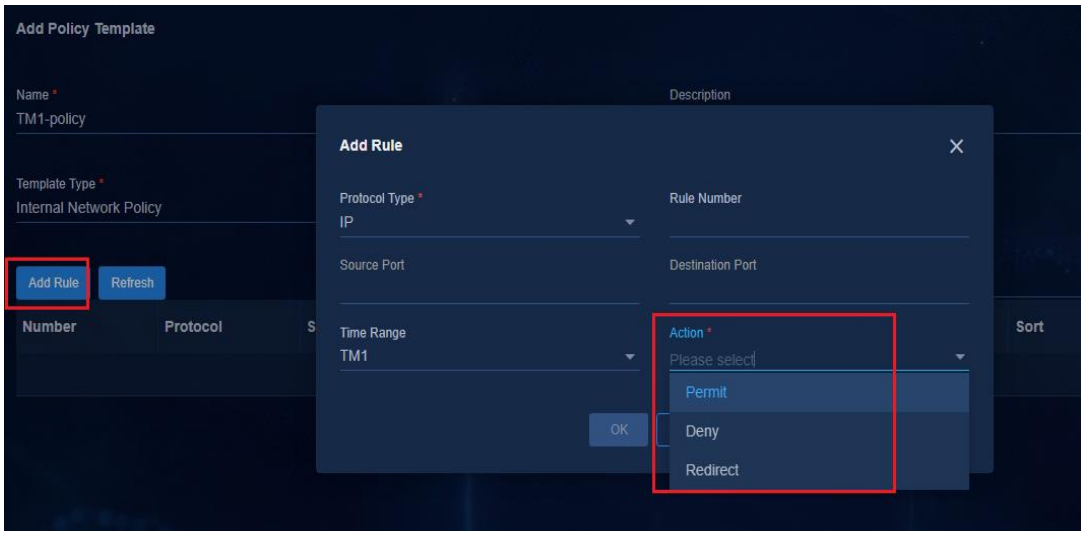
1. **Policy Templates** タブをクリックします。システムには、事前定義されたテンプレート **Permit All** および **Deny all** が現れます。



2. **Add** をクリックします。ポリシーテンプレートの名前を入力し、**Template Type** パラメーターで **Internal Network Policy** を選択します。
   - **Internal Network Policy**: グループポリシーおよび東西サービスチェーンの場合は、**Internal Network Policy** を選択します。
   - **External Network Policy**: 南北サービスチェーンの場合は、**External Network Policy** を選択します。



3. **Add Rule** をクリックして、**Add Rule** ページを開きます。次のパラメーターを構成し、OK をクリックします。
   - **Protocol Type**: オプションは、**IP**、**UDP**、**TCP**、および **ICMP** です。
   - **Time Range**: デフォルトでは **none** です。これは、すべての時間範囲が有効であることを示します。
   - **Action**: オプションは、**Permit**, **Deny** 及び **Redirect** です。グループポリシーの場合は **Permit** 又は **Deny** を選択し、サービスチェーンの場合は **Redirect** を選択します。



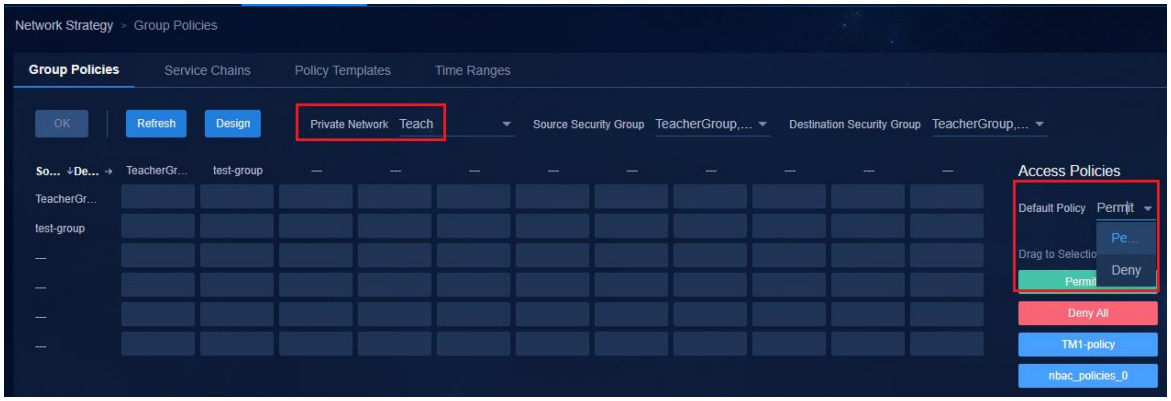
4. ポリシーテンプレートを追加したら、**OK** をクリックしてテンプレートを保存します。

デフォルトのアクセスポリシーの構成

Group Policies タブをクリックします。**Access Policies** 領域の **Default Policy** フィールドのドロップダウンリストで、選択したプライベートネットワーク内のユーザーのアクセス権限を設定できます。グループポリシーを構成する場合、最初にプライベートネットワークを選択してからデフォルトポリシーを設定する必要があります。

Group Policies ページで設定した **Default Policy** は、プライベートネットワークページで設定した **Default Group Policy** と同じです。グループポリシーを設定するページを 1 つ選択できます。

- **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ず、同じプライベートネットワーク内のセキュリティグループは相互にアクセスできず、同じセキュリティグループ内の異なるユーザーは相互にアクセスできません。



Deny を選択した場合、SeerEngine キャンパスコントローラーは、グローバル deny PBR をスパインデバイスと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 L3VNI インターフェイスに展開します。

#スパインデバイスおよびリーフデバイス上のプライベートネットワーク内の L3VNI インターフェイスに許可 IP 設定を設定します。

```
#
acl advanced name SDN_ACL_SC_PERMIT_ALL
 description SDN_ACL_SC_PERMIT_ALL
 rule 0 permit ip
#
#
policy-based-route SDN_GLOBAL_SC2 permit node 0
 if-match acl name SDN_ACL_SC_PERMIT_ALL
#
#
interface Vsi-interface2          //L3VNI interface.//
 description SDN_VRF_VSI_Interface_2
 ip binding vpn-instance Teach
 ip policy-based-route SDN_GLOBAL_SC2
 l3-vni 2
#
```

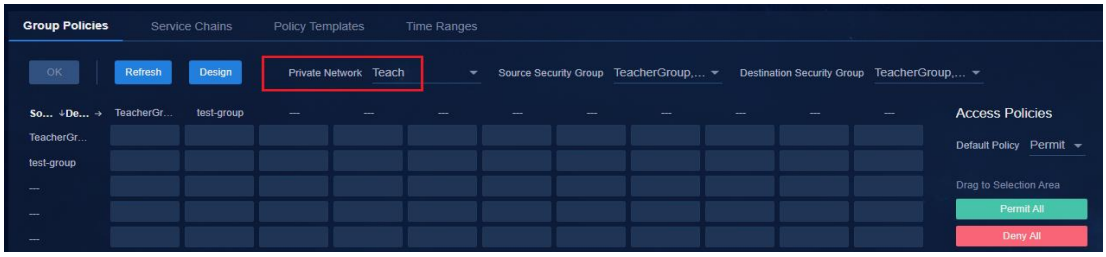
Deploy the global deny action to spine and leaf devices.

```
#
acl advanced name SDN_ACL_GLOBAL_SC_6ee86fb4-6139-4db6-8eee-b114ad328cc1
 description SDN_ACL_GLOBAL_SC_6ee86fb4-6139-4db6-8eee-b114ad328cc1
```

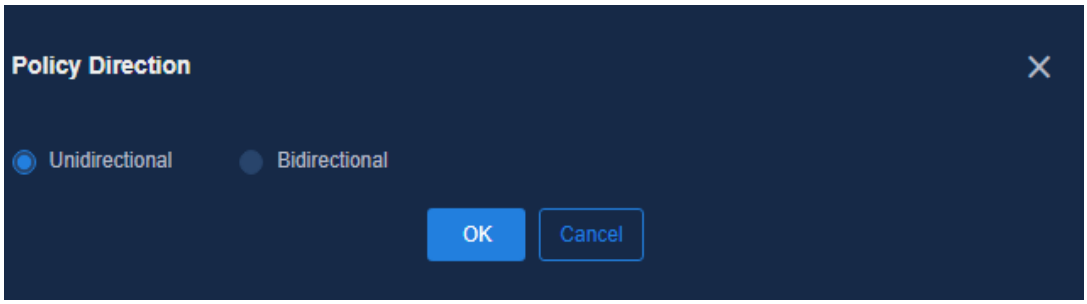
```
 rule 0 permit ip destination 20.0.0.0 0.0.255.255
 rule 1 permit ip destination  30.0.0.0 0 0.0.255.255
#
#
policy-based-route SDN_GLOBAL_SC permit node 0
 if-match acl name SDN_ACL_GLOBAL_SC_6ee86fb4-6139-4db6-8eee-b114ad328cc1
 apply output-interface NULL0
#
#
ip global policy-based-route SDN_GLOBAL_SC //Globally deliver.//
#
```

グループポリシーの設定

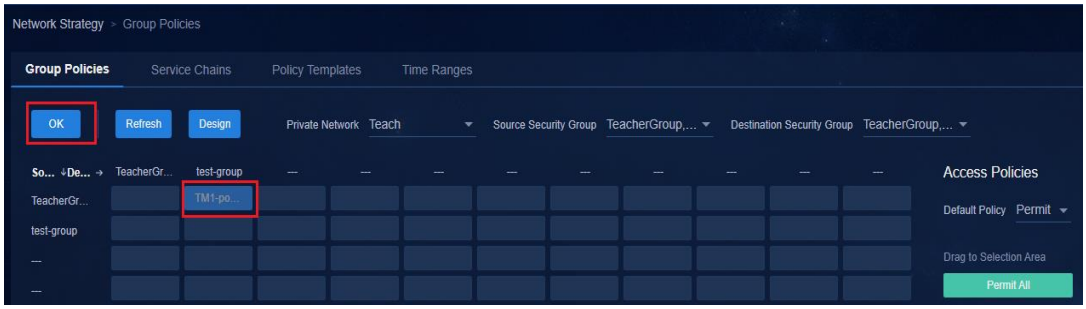
1. **Group Policies** タブをクリックします。最初にプライベートネットワークを選択すると、次の図に示すようなマトリックスが表示されます。



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。必要に応じてオプションを選択し、**OK** をクリックします。**Policy Direction** には次のオプションがあります。
   - **Unidirectional**: 送信元セキュリティグループから宛先セキュリティグループへのアクセスポリシーを設定します。
   - **Bidirectional**: 送信元セキュリティグループから宛先セキュリティグループへ、および宛先セキュリティグループから送信元セキュリティグループへのアクセスポリシーを設定します。



3. この例では、次の図に示すように、送信元セキュリティグループを **Student Security Group**、宛先セキュリティグループを **Teacher Group** として **Deny All** を設定します。グループポリシーが設定されたら、左上隅にある **OK** をクリックして設定を保存します。



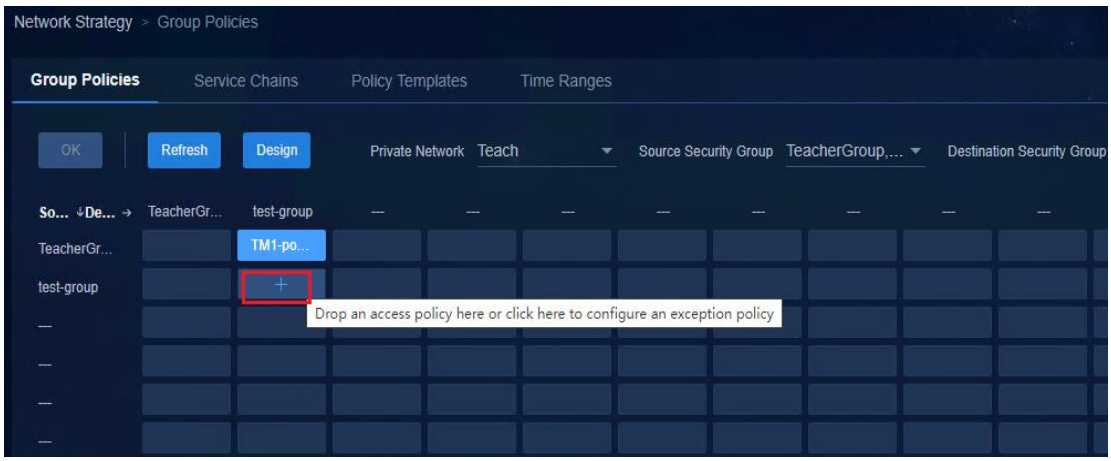
4. コントローラーは、PBR ポリシーをスパインデバイスとリーフデバイスに展開します。コマンドは次のとおりです。

```
#
acl advanced name SDN_ACL_SC_000002_4_3
 description SDN_ACL_SC_000002_4_3
 rule 0 permit ip destination 20.0.0.0 0.0.255.255
#
#
policy-based-route SDN_SC_4 permit node 0
 if-match acl name SDN_ACL_SC_000002_4_3
 apply output-interface NULL0
#
#
interface Vsi-interface4      //L2VNI interface corresponding to the student security group.//
 description SDN_VSI_Interface_4
 ip binding vpn-instance Teach
 ip address 30.0.0.1 255.255.0.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 ip policy-based-route SDN_SC_4
 local-proxy-nd enable
 distributed-gateway local
#
```

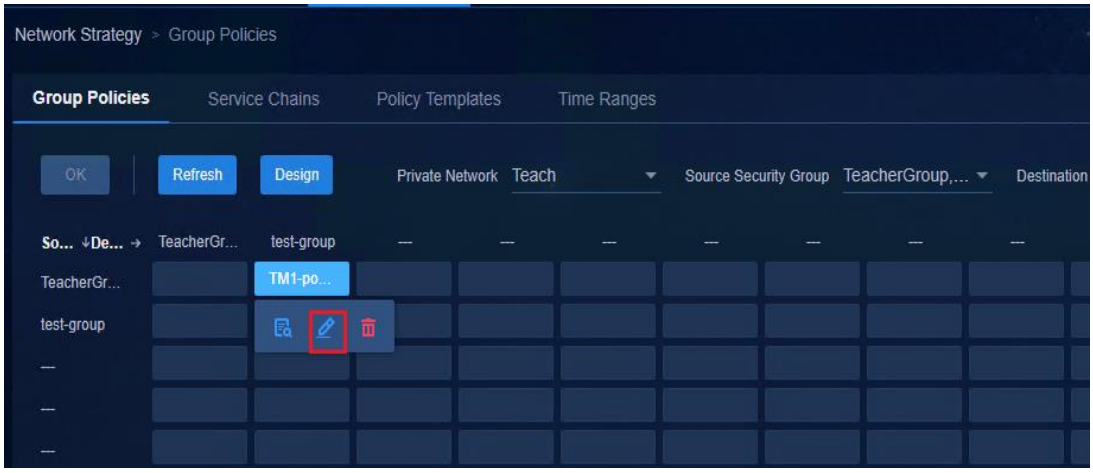
例外ルールの設定

例外規則を設定して、特定のトラフィックをグループポリシーの制御から除外できます。

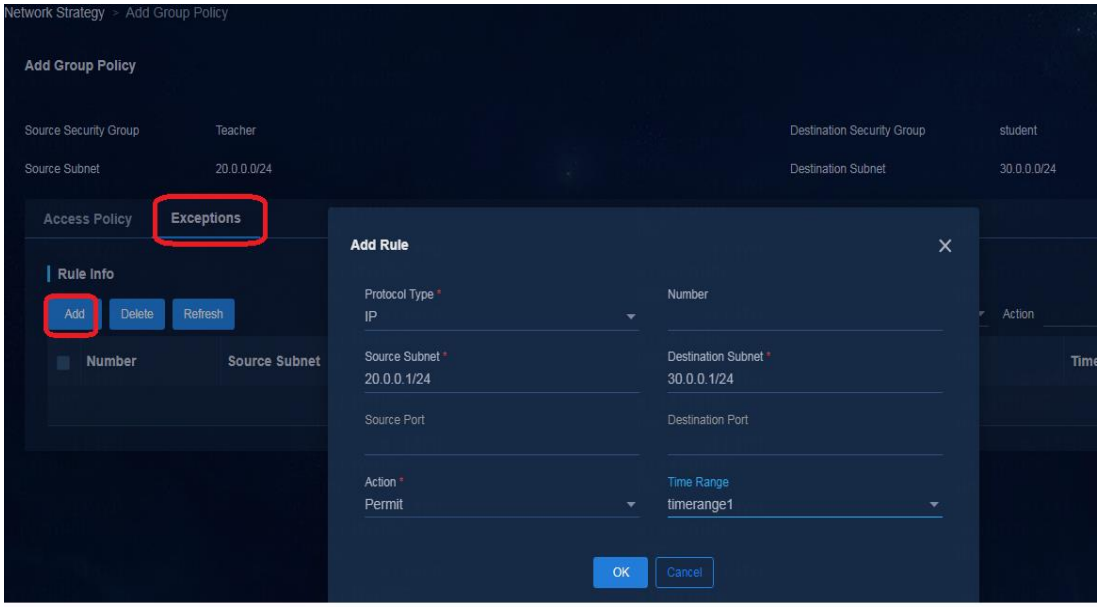
1. マトリクス内の任意の場所にマウスを移動し、+をクリックして **Edit Group Policy** ページを開きます。



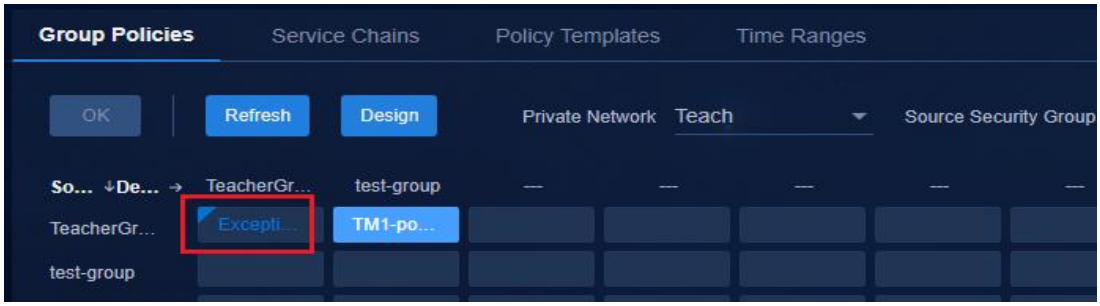
2. アクセスポリシーがロケーションにすでに存在する場合は、アイコンをクリックして、**Edit Group Policy** ページを開きます。



3. **Exceptions** タブで **Add** をクリックし、**Protocol Type**、**Source Subnet**、**Destination Subnet**、および **Action** フィールドを設定して、**OK** をクリックします。



4. 例外規則が **Group Policies** タブに表示されます。



リーフデバイス上の展開済み設定を表示するには、以下の手順に従ってください。

```
[leaf]display ip policy-based-route
Policy name: SDN_SC_3
```

```
  node 0 permit:
    if-match acl name SDN_ACL_SC_100005_3_4
[leaf]acl name SDN_ACL_SC_100005_3_4
[leaf-acl-ipv4-adv-SDN_ACL_SC_100005_3_4]dis th
#
acl advanced name SDN_ACL_SC_100005_3_4
 description SDN_ACL_SC_100005_3_4
 rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 50.0.0.0 0.0.0.255
#
return
[leaf10510-acl-ipv4-adv-SDN_ACL_SC_100005_3_4]
```

ユーザーのオンボーディング

ユーザーオンボーディングプランは、ユーザーアクセスポリシー、ユーザーアクセスサービスおよびアクセスユーザーの構成を含む、EIA サーバーの構成をガイドします。ユーザーアクセスサービスの構成後、ユーザーはアクセス認証を通過することでオンラインになることができます。

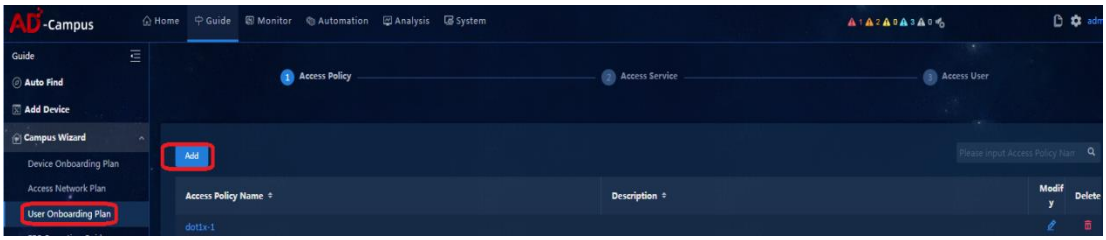
アクセスポリシーの構成

アクセスポリシーの設定には、次の方法を使用できます。

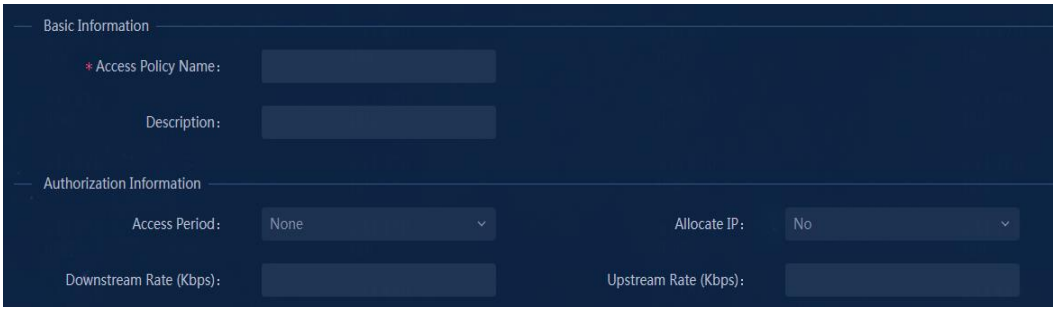
- **Using the campus wizard**: **Guide** > **Campus Wizard** > **User Onboarding Plan** ページにナビゲートし、**Step 1 Access Policy** でアクセスポリシーを構成します。この項では、この方法を使用します。
- **Not using the campus wizard**: アクセスポリシーを設定するには、**Automation** > **User** > **Access Service** > **Access Policy** ページに移動します。

アクセスポリシーを設定するには、次の手順を実行します。

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. 次のパラメーターを設定します。
   - **Basic Information**: アクセスポリシーの名前を入力し、デフォルトのユーザーグループ設定(グループ化解除)を使用します。ユーザーグループを追加するには、**Automation** > **User** > **Access User** ページにナビゲートし、**User Group** をクリックして、ユーザーグループを追加します。



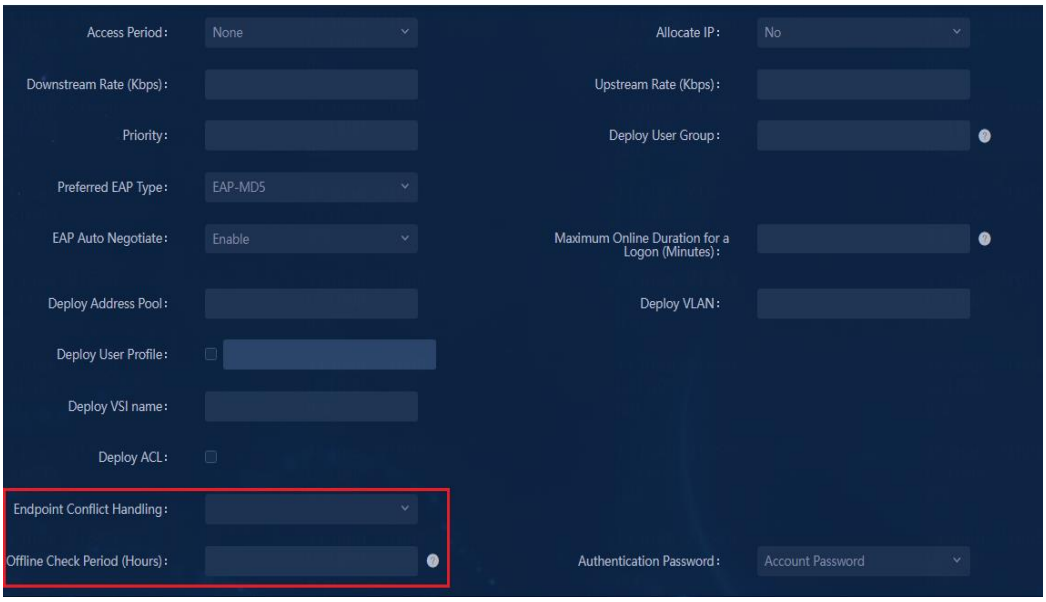
- **Authorization Information**: 通常、デフォルト値を使用します。

  次のパラメーターの設定に注意してください。

  - **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。
  - **Offline Check Period(Hours)**: このパラメーターを設定して、スイッチが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に、パケットをアクティブに送信しないプリンタなどのダムエンドポイントをログオフしないようにします。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。このパラメーターは 0～596523 の範囲の整数です。0 に設定すると、エンドポイントはオフラインになりません。空に設定すると、オフラインチェック期間は 5 分になります。

  一貫性のないエンドポイント情報を処理する方法:

  - **Log Conflict and Continue Authentication**: ユーザーが同じ MAC アドレスを使用しているが、異なるエンドポイントを使用してオンラインになる場合は、ログを記録し、ユーザーが認証を通過してオンラインになることを許可します。
  - **Reject Authentication**: ユーザーが同じ MAC アドレスを使用しているが、異なるエンドポイントを使用してオンラインになる場合、ユーザーのオンライン要求を拒否します。
  - **Deploy Blackhole MAC**: MAC アドレスの偽造を防止するために使用されます。ユーザーが同じ MAC アドレスを使用しているが、異なるエンドポイントを使用してオンラインになる場合は、ユーザーのオンライン要求を禁止し、MAC 認証のサイレント MAC アドレスリストに MAC アドレスを発行します。



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。

```
<leaf-1>display mac-authentication connection
Total connections: 1
Chassis ID: 1
Slot ID: 4
User MAC address: 0000-0000-0010
Access interface: Ten-GigabitEthernet1/4/0/2
Username: 000000000010
User access state: Successful
Authentication domain: hz1
IPv4 address: 20.0.0.2
Initial VLAN: 149
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi4
Authorization ACL ID: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 86400 sec
```

- **認証バインド情報:**

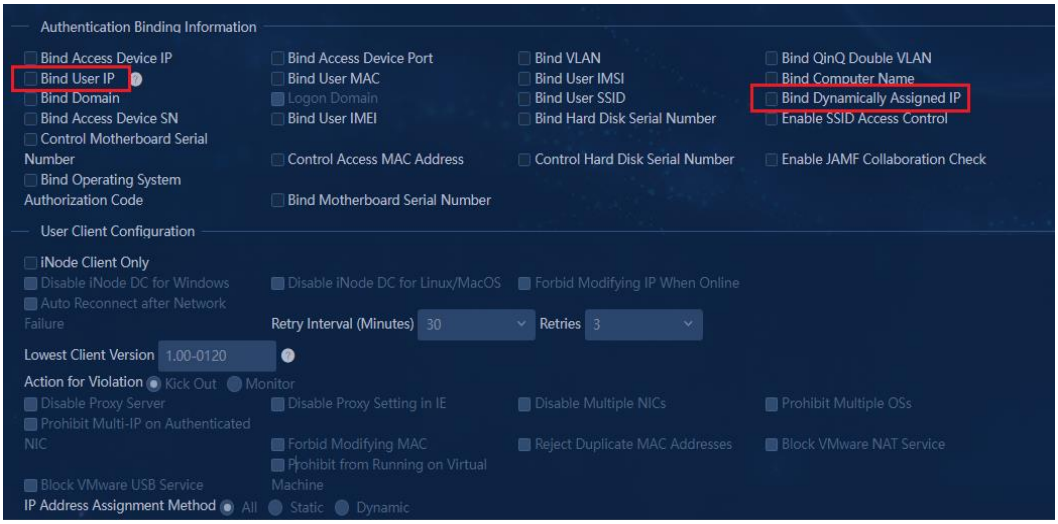
  次のパラメーターに注意してください。

  - **Bind User IP**: オンラインエンドポイントをそのスタティック IP アドレスにバインドするには、このオプションを選択します。これを選択すると、エンドポイントデバイスは、デバイスがオンラインになった後に、バインドされたスタティック IP アドレスをユーザーの詳細情報に記録します。
  - **Bind Dynamically Assigned IP**: エンドポイントが DHCP サーバーを介して IP アドレスを取得する場合は、このオプションを選択します。エンドポイントが初めてオンラインになったときに、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をバインドするには、このオプションを選択します。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。

  ⚠ 警告!

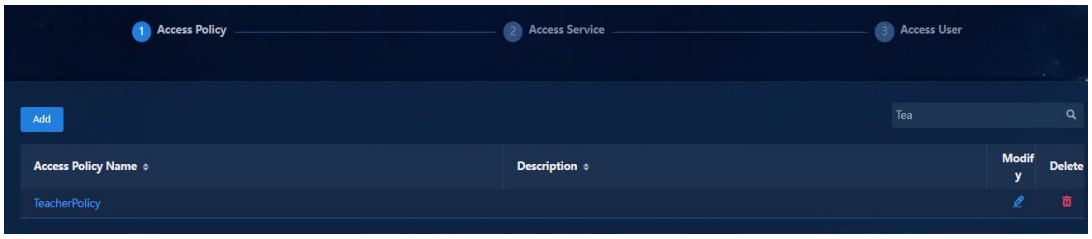
  Bind User IP パラメーターと Bind Dynamically Assigned IP パラメーターを同時に選択することはできません。

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



3. パラメーターの設定後、**OK** をクリックして構成を保存します。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、**Add** をクリックし、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。

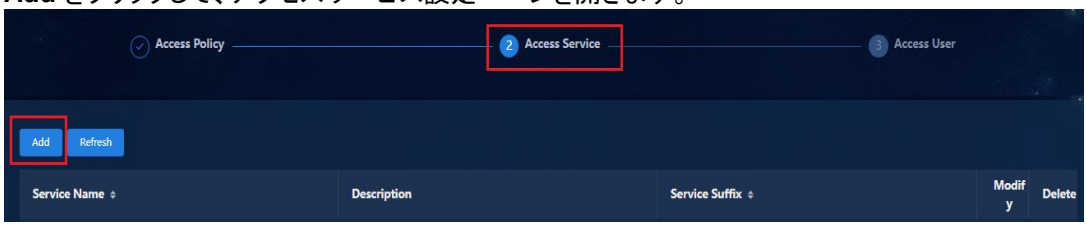
アクセスサービスの設定

アクセスサービスの設定には、次の方法を使用できます。

- **Using the campus wizard**: **Guide** > **Campus Wizard** > **User Onboarding Plan** ページに移動し、**Step 2 Access Service** でアクセスサービスを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: アクセスサービスを設定するには、**Automation** > **User** > **Access Service** > **Access Service** ページに移動します。

アクセスサービスを設定するには、次の手順を実行します。

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。



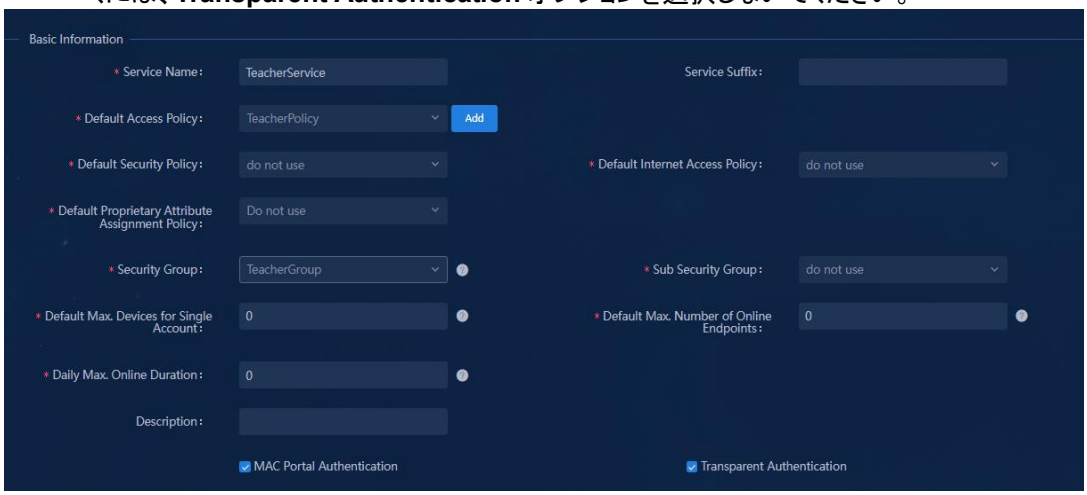
2. 次のパラメーターを設定します。

   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、他のパラメーターにはデフォルト設定を使用します。次に、**OK** をクリックして設定を保存します。

- **基本情報:**

  パラメーターの説明:

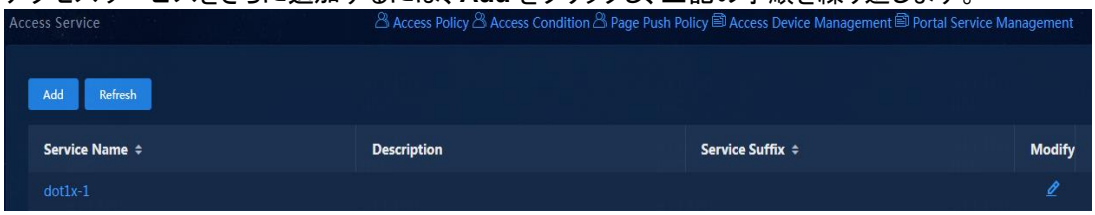
  - **Default Access Policy**: デフォルトでは、すべてのユーザーがオンラインになれないことを示す **Access Forbidden** です。ユーザーがオンラインになることを許可するには、デフォルトのアクセスポリシーを構成する必要があります。**Add** をクリックすると、新しいデフォルトのアクセスポリシーを追加できます。
  - **Security Group**: このパラメーターは設定する必要があります。『Configuring access networks』で作成されたセキュリティグループがドロップダウンリストに表示されます。
  - **Sub Security Group**: IP ベースのポリシーモードでは、デフォルトの do not use 設定を使用します。
  - **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。Transparent Authentication オプションはオプションです。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**: 必要に応じてアクセスシナリオを設定します。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設定すると、追加されたアクセスサービスを表示できます。

   アクセスサービスをさらに追加するには、**Add** をクリックし、上記の手順を繰り返します。



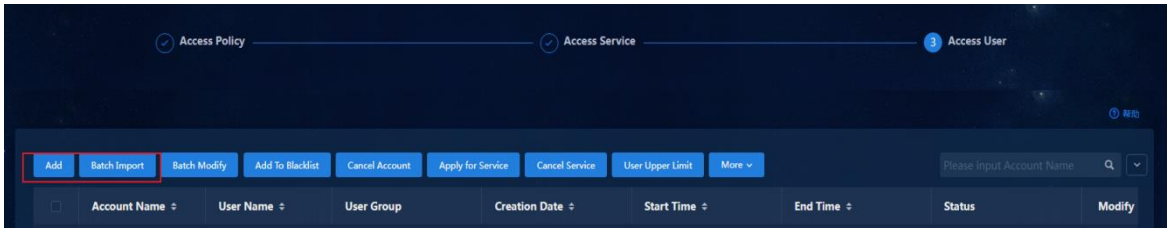
4. アクセスサービスを設定したら、**Next** をクリックしてアクセスユーザーを設定します。

アクセスユーザーの管理

アクセスユーザーの設定には、次の方法を使用できます。

- **Using the campus wizard**: **uide** > **Campus Wizard** > **User Onboarding Plan** ページに移動し、**Step 3 Access User** でアクセスユーザーを設定します。このセクションでは、この方法を使用します。
- **Not using the campus wizard**: **Automation** > **User** > **Access User** ページに移動して、アクセスユーザーを設定します。

アクセスユーザーを手動で追加するか、ユーザーをインポートできます。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。自動デバイスデプロイ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、次のパラメーターを設定します。
   - **Basic Information** : **User Name** および **Identity Numbe**r を指定します。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。

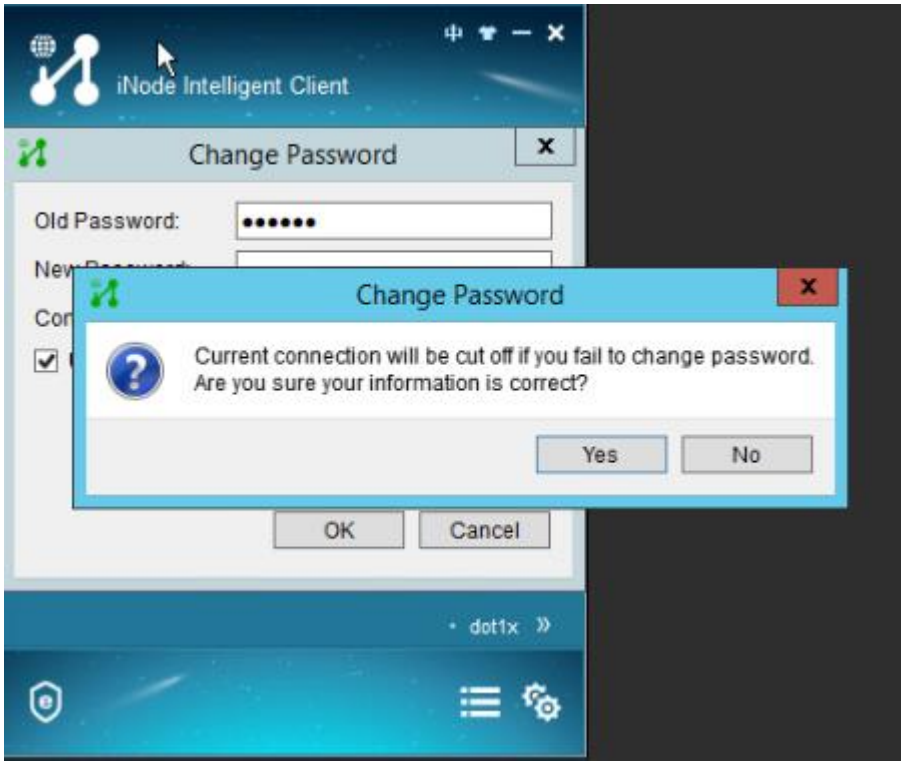
   - **Access Information**: アカウント名とパスワードを入力します。その他のパラメーターについては、デフォルト値を使用できます。
     - **Max. Idle Time**: デフォルトでは空になっています。これは、セッションがタイムアウトしないことを示します。
     - **Max. Concurrent Logins**: デフォルト値は 1 です。最大値は 255 です。このパラメーターは、ログインに同じアカウントを使用するエンドポイントの数を指定します。詳細は、『Setting the maximum number of online endpoints 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、**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した後、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。

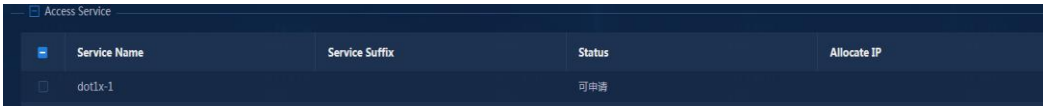
⚠ **警告!**

Modify Password at Next Login は 1 回限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。

次の図に示すように、**Modify Password at Next Login** を選択すると、ユーザーはパスワードを編集するためのページに入ります。パスワードが正常に編集された後、ユーザーは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。



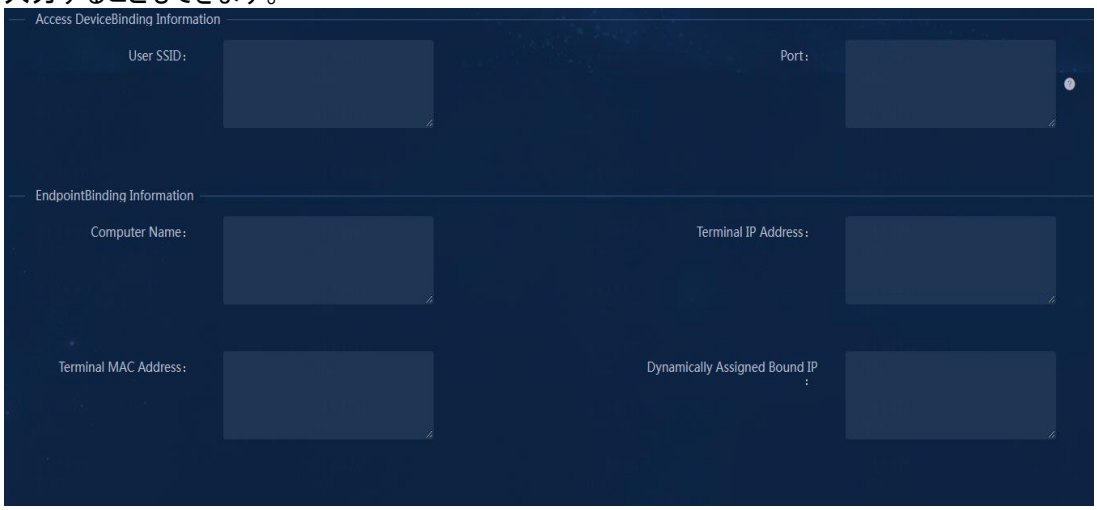
- **Access Service**:各アクセスユーザーは、アクセスサービスにバインドされている必要があります。認証に合格すると、ユーザーはアクセスサービスのセキュリティグループ内のネットワークリソースにアクセスできます。



- **EndpointBinding 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。

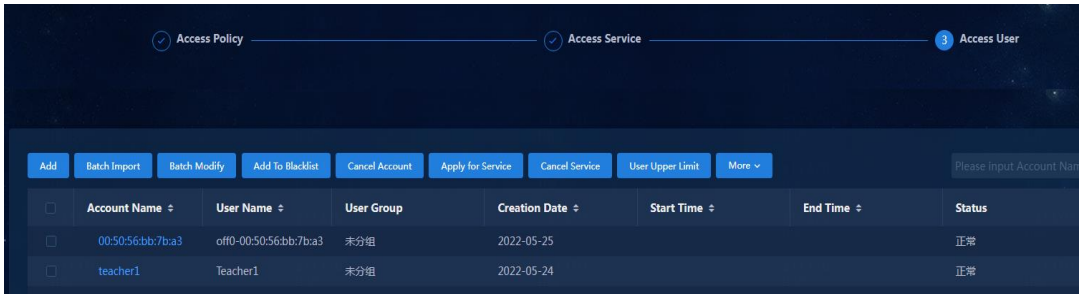
システムは、アクセスサービスとアクセスポリシーの設定に基づいて、バインディング情報を自動的に入力することもできます。



⚠ **警告!**

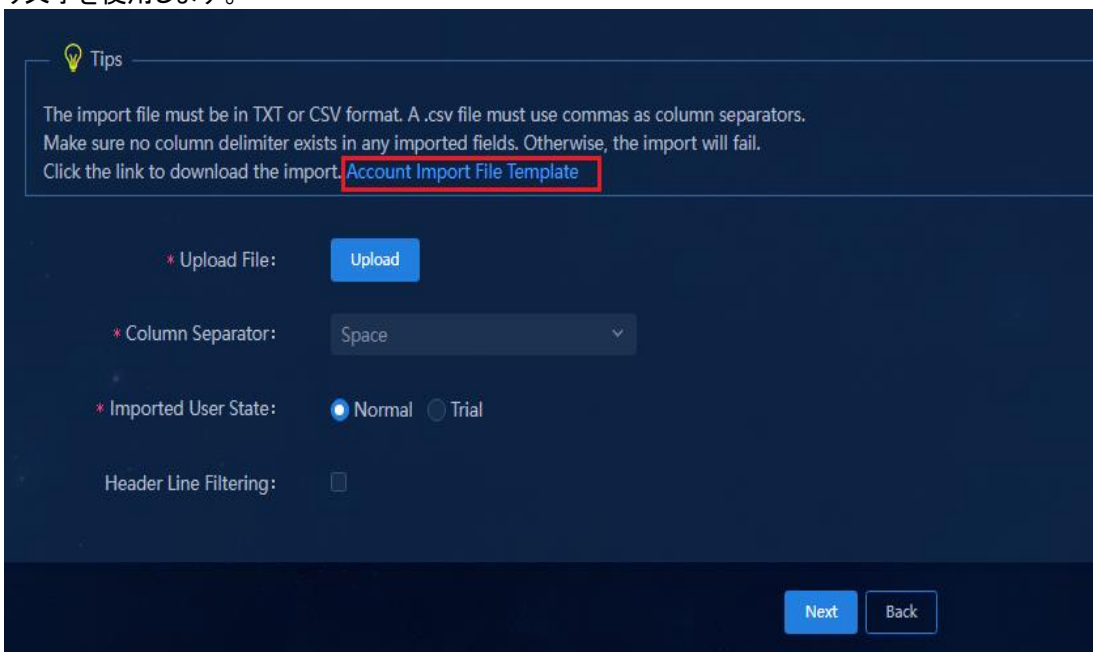
Endpoint Binding Information エリアで設定した IP アドレスは『Configuring access policies』の **Bind User IP** で使用する必要があります。**Bind User IP** を選択しない場合、**Endpoint Binding Information** エリアで指定した IP アドレスは有効になりません。

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



ユーザーの一括インポート

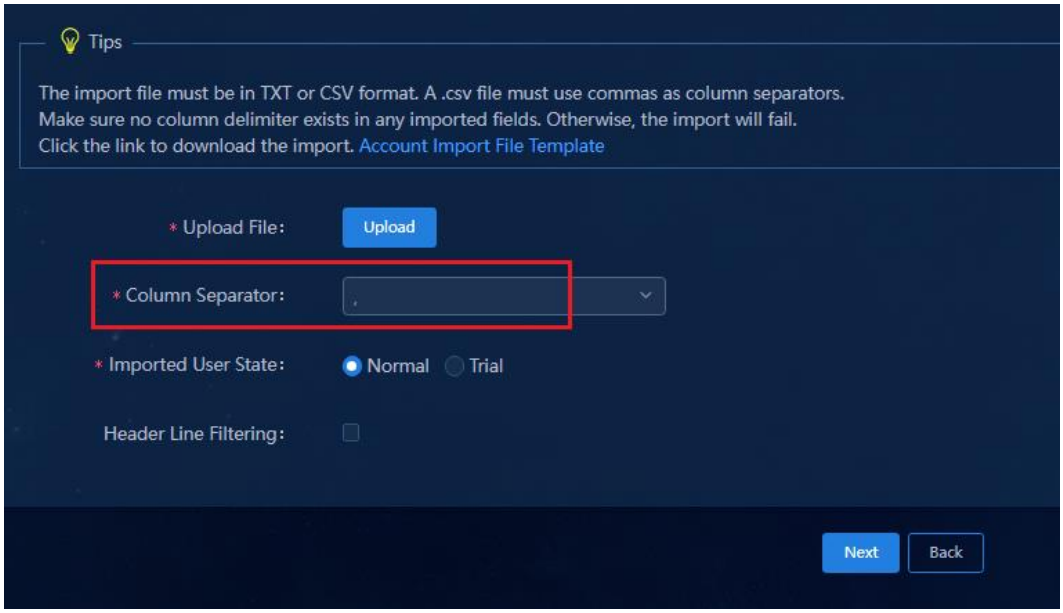
1. **Access User** タブで、**Batch Import** をクリックし、**Account Import File Template** リンクをクリックしてテンプレートをダウンロードします。列を区切るには、Tab キーを使用するか、コンマ(,)などの区切り文字を使用します。



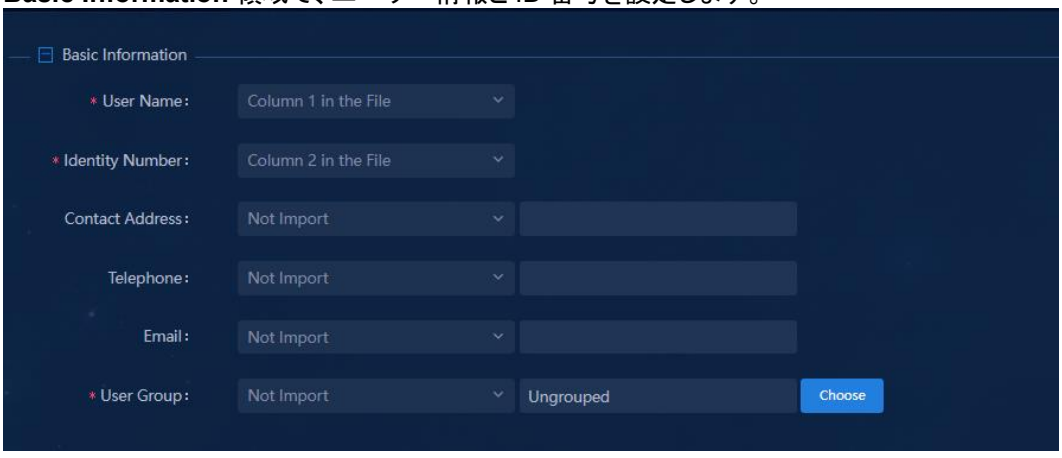
この例では、次の図に示すように、カラムはカンマ(,)で区切られています。

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

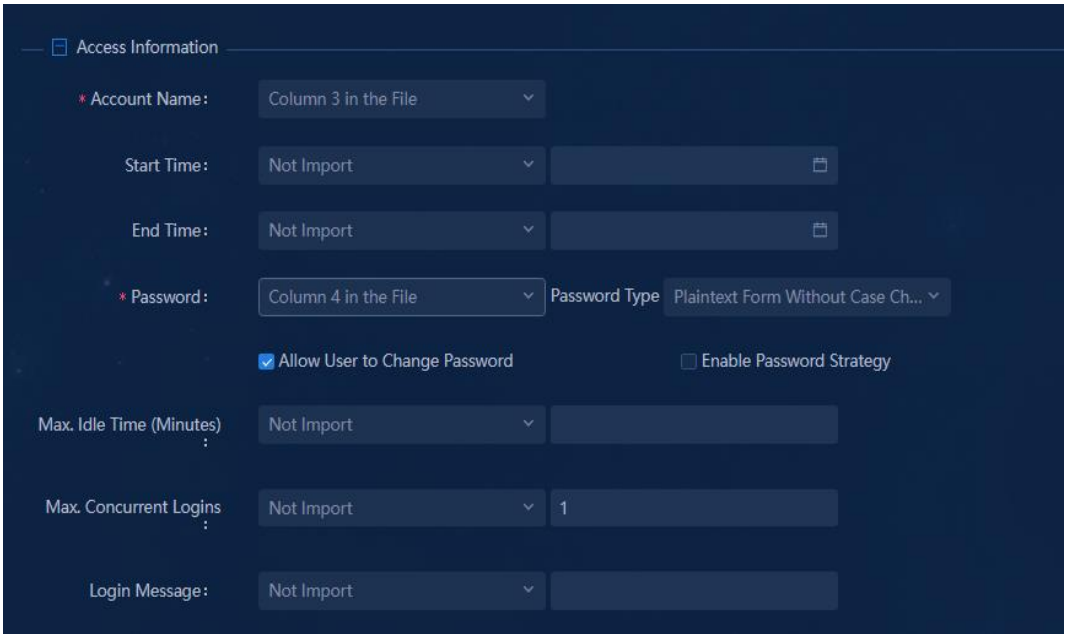
2. 次の図に示すように、**Upload** をクリックし、ファイルを選択し、区切り文字を選択して、**Imported User State** で **Normal** を選択します。



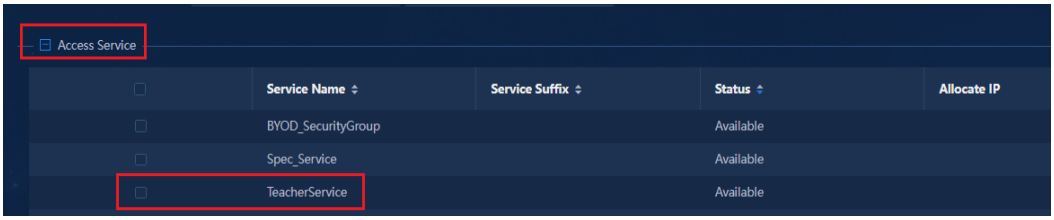
3. **Next** をクリックします。
   - **Basic Information** 領域で、ユーザー情報と ID 番号を設定します。



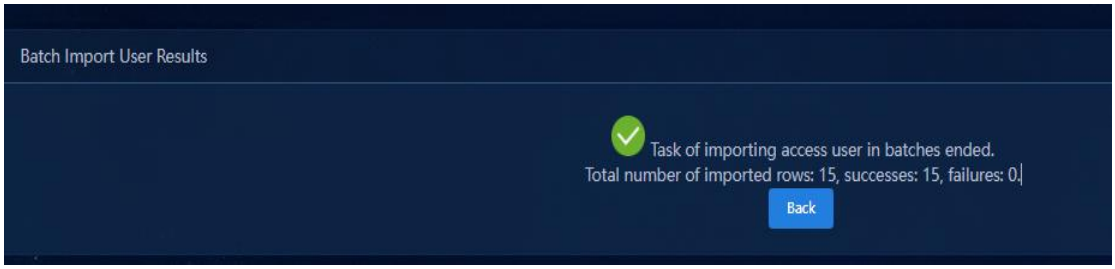
- 必要に応じてユーザーグループを選択します。デフォルト値は **Ungrouped** です。
- **Access Information** 領域で、**Account Name** と **Password** を設定します。パスワードはファイルから選択することも、直接入力することもできます。パスワードを直接入力すると、すべてのユーザーが同じパスワードを使用します。



- **Access Service** エリアでアクセスサービスを選択します。これは必須の操作です。



4. ユーザーを一括インポートするには、OK をクリックします。



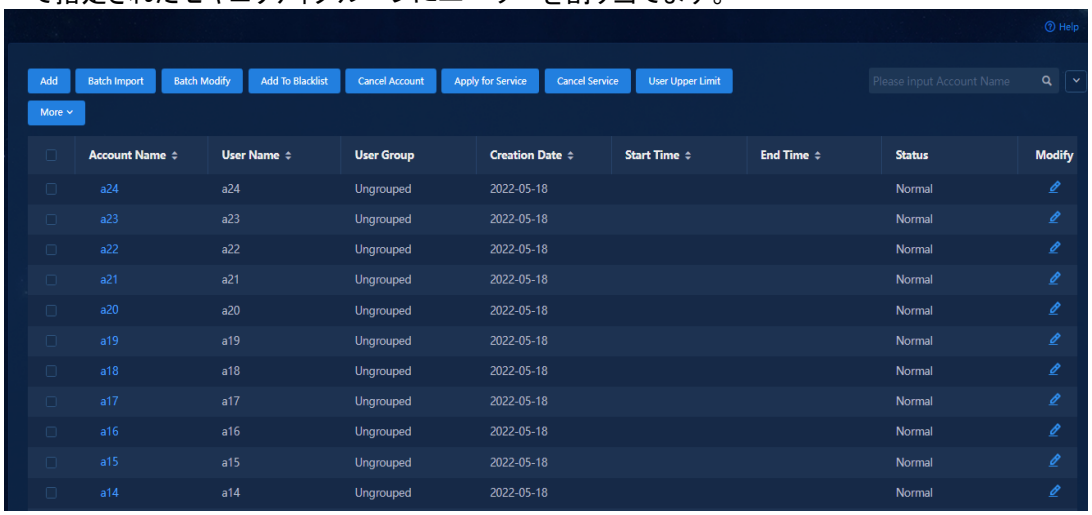
5. ユーザーが正常にインポートされると、インポートされたユーザーを **Access User** ページで表示できます。

アクセスシナリオの管理(オプション)

1. アクセスシナリオを追加するには、**Automation** > **User** > **Access Service** ページに移動します。
   - **Add** をクリックして、**Add Access Scenario** ページを開きます。**Access Scenario List** 領域で **Add** をクリックし、アクセスシナリオをここに追加

- サービス名に対応する **Modify** アイコンをクリックします。**Access Scenario List** 領域で **Add** をクリックし、アクセスシナリオをここに追加します。

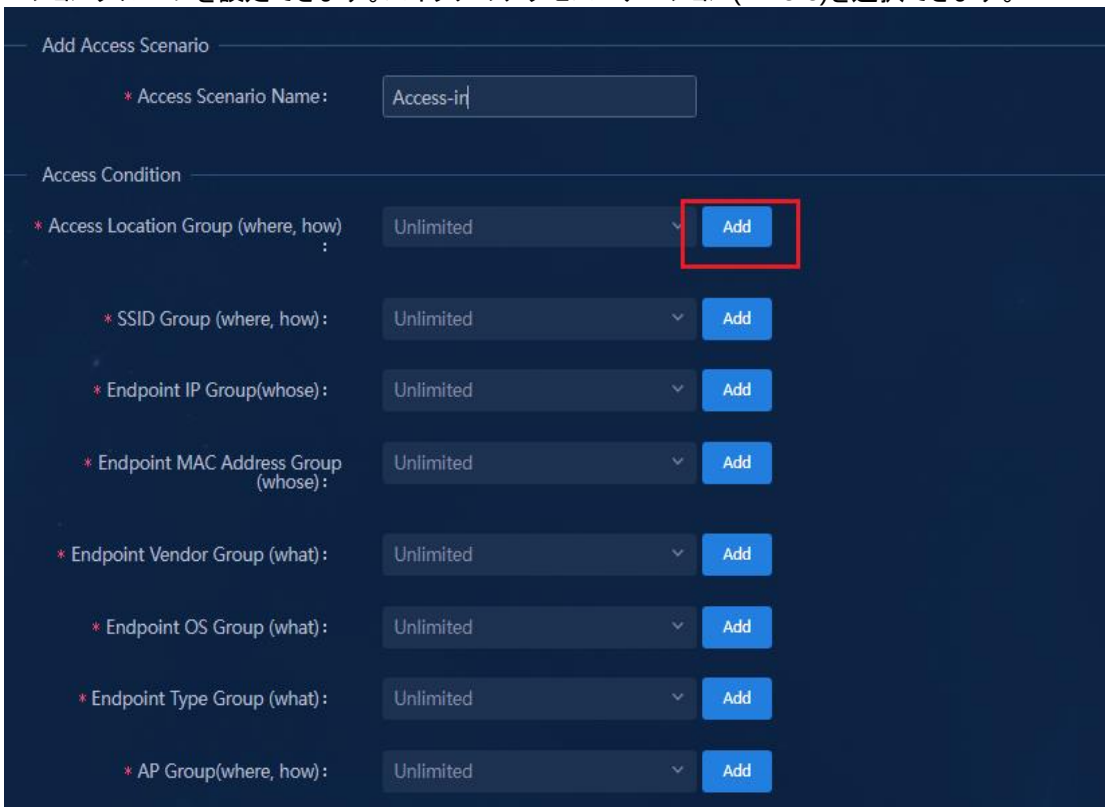
アクセスシナリオが構成されている場合、ユーザーがオンラインになると、システムは構成されたアクセスシナリオとユーザーを照合し、一致したシナリオで指定されたセキュリティグループにユーザーを割り当てます。ユーザーに一致するものが見つからない場合、システムはデフォルトのアクセスポリシーで指定されたセキュリティグループにユーザーを割り当てます。



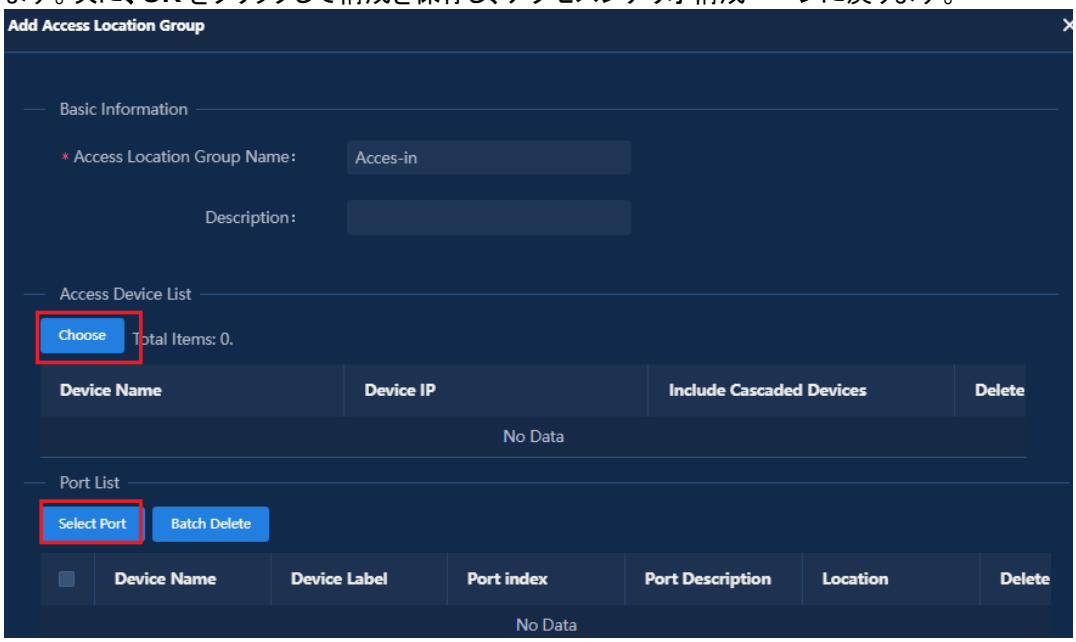
2. **Access Scenario** 設定ページで、次の図に示すように 5W1H を設定します。

『誰が』、『誰の』、『何を』、『いつ』、『どこで』および『どのように』(5W1H)に基づくアクセス条件は、複数のシナリオをカバーします。個々の需要を満たすために、必要に応じてシナリオをカスタマイズできます。

たとえば、**Access Location Group(where, how)**パラメーターの **Add** をクリックして、アクセスロケーショングループを設定できます。スイッチのアクセスロケーション(Where)を選択できます。

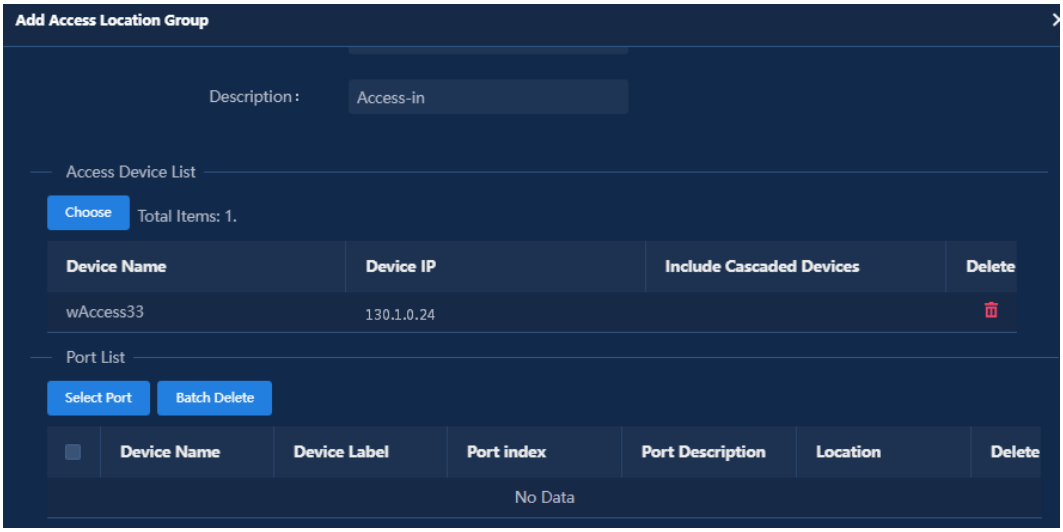


3. **Add Access Location Group** ページで、アクセスデバイスまたはアクセスインターフェイスを選択します。次に、**OK** をクリックして構成を保存し、アクセスシナリオ構成ページに戻ります。



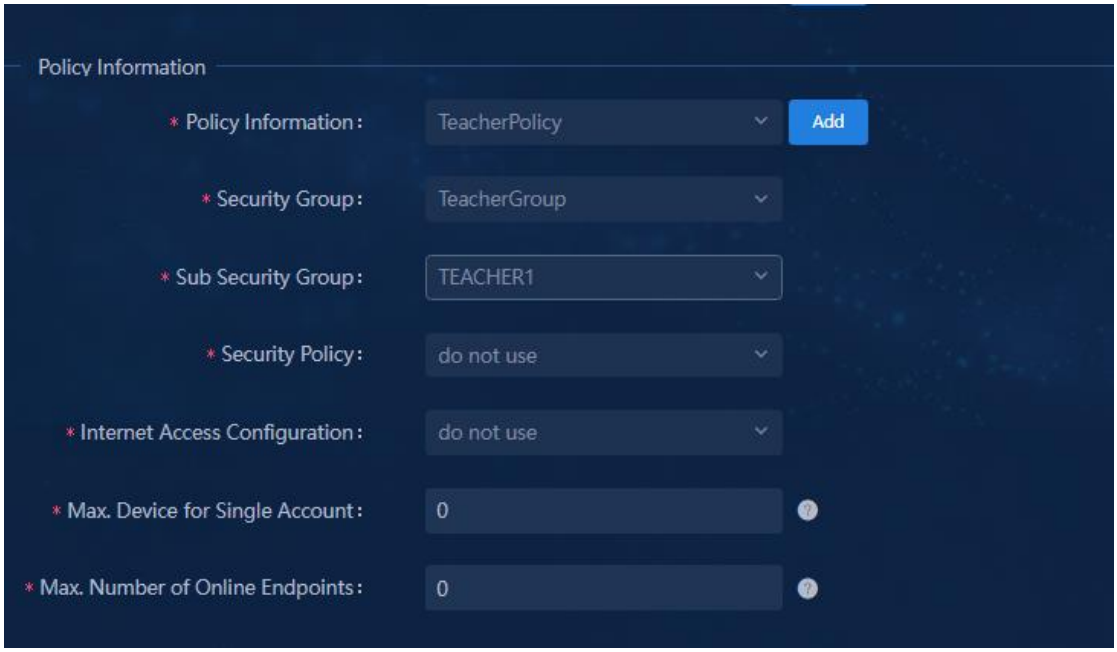
アクセスデバイスまたはアクセスインターフェイスの設定の説明:

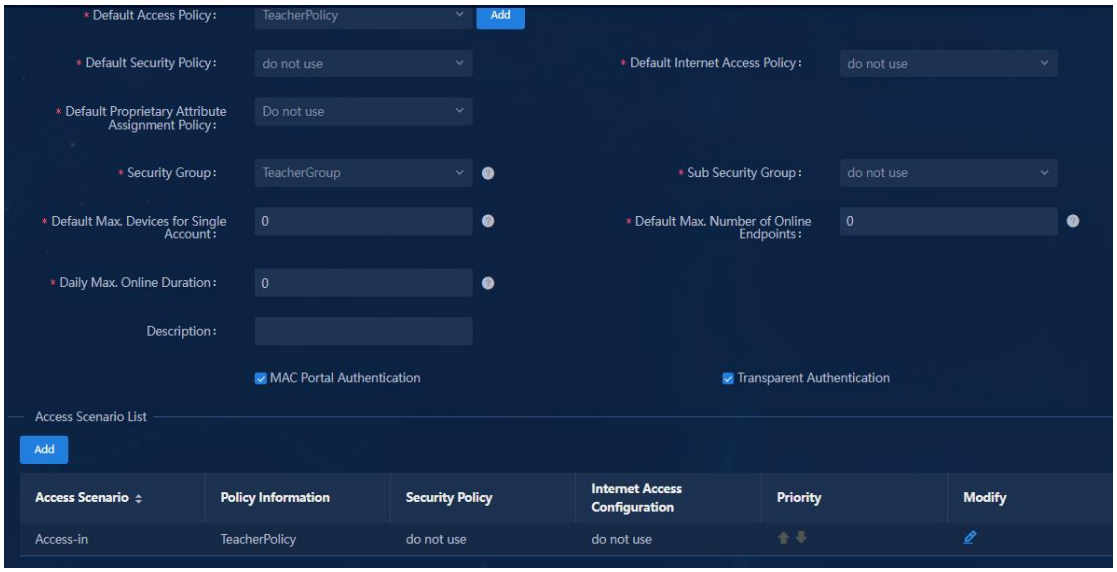
- アクセスデバイス:リーフデバイス、アクセスデバイスまたはカスケードアクセスデバイスを選択できます。リーフデバイスを選択するときに、カスケードアクセスデバイスを含めるかどうかを選択できます。



- アクセスインターフェイス:リーフ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。逆の場合も同様です。

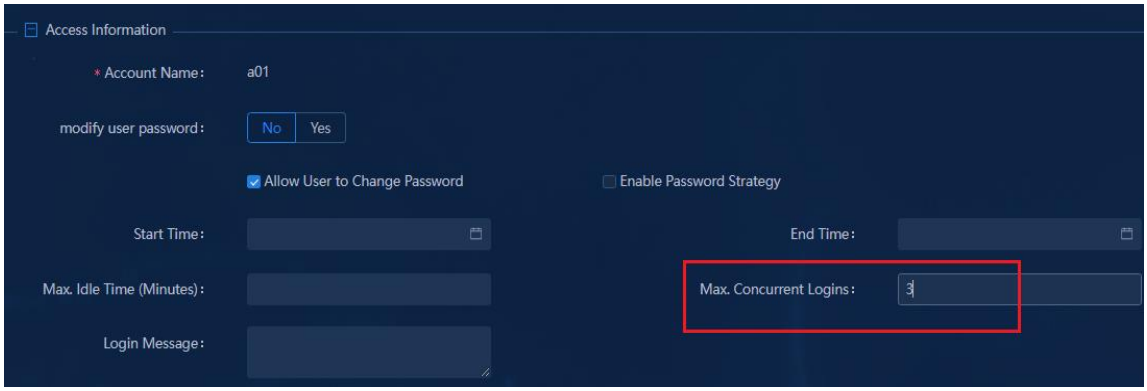
4. アクセスシナリオの構成ページで、アクセスポリシーパラメーターを構成し、**OK** をクリックしてアクセスシナリオの構成を終了します。構成したアクセスシナリオが **Access Scenario List** に表示されます。



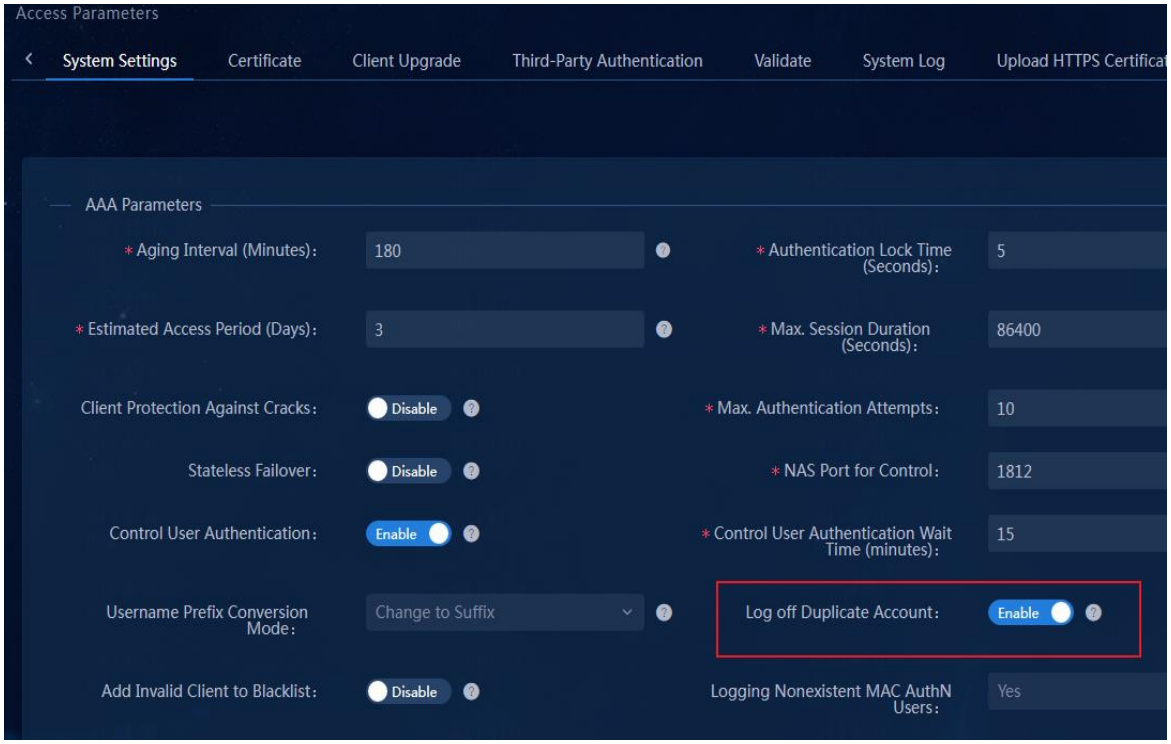


アカウントでサポートされるオンラインエンドポイントの最大数の設定

Max. Concurrent Logins パラメーターは、1 つのアカウントのオンラインエンドポイントの数を制限するために使用されます。このパラメーターを構成するには、**Automation** > **User** > **Access User** > **All Access Users** ページにナビゲートします。次の図に示すように、アカウント **a01** では、3 つのエンドポイントを同時にログインできます。



Automation > **User** > **Access Parameters** > **System Settings** ページに移動して、**Log Off Duplicate Account** パラメーターを設定し、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を制御することもできます。アイコンをクリックし、次のように設定ページに入ります。



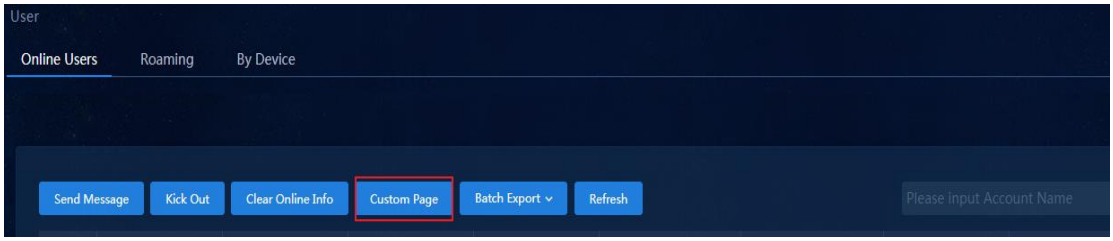
Log Off Duplicate Account パラメーターは、有効または無効にできます。デフォルトでは **Enable** に設定されており、**Max. Concurrent Logins** パラメーターの値が **1** の場合にのみ有効になります。

- **Log Off Duplicate Account** パラメーターを **Enable** に設定すると、次のようになります。
  - **Max. Concurrent Logins** パラメーターが 1 に設定されている場合、新しいエンドポイントがそのアカウントを使用してオンラインになると、現在のエンドポイントは強制的にログオフされます。
  - **Max. Concurrent Logins** パラメーターが 1 より大きい値に設定されている場合、新しいエンドポイントがアカウントを使用してオンラインになったときに、現在のエンドポイントが強制的にログオフされることはありません。
- **Log Off Duplicate Account** パラメーターを **Disable**』に設定した場合は、次のようになります。

  Max. Concurrent Logins パラメーターが 1 に設定されている場合、現在のエンドポイントがログオフするまで、エンドポイントはそのアカウントを使用してオンラインになることはできません。

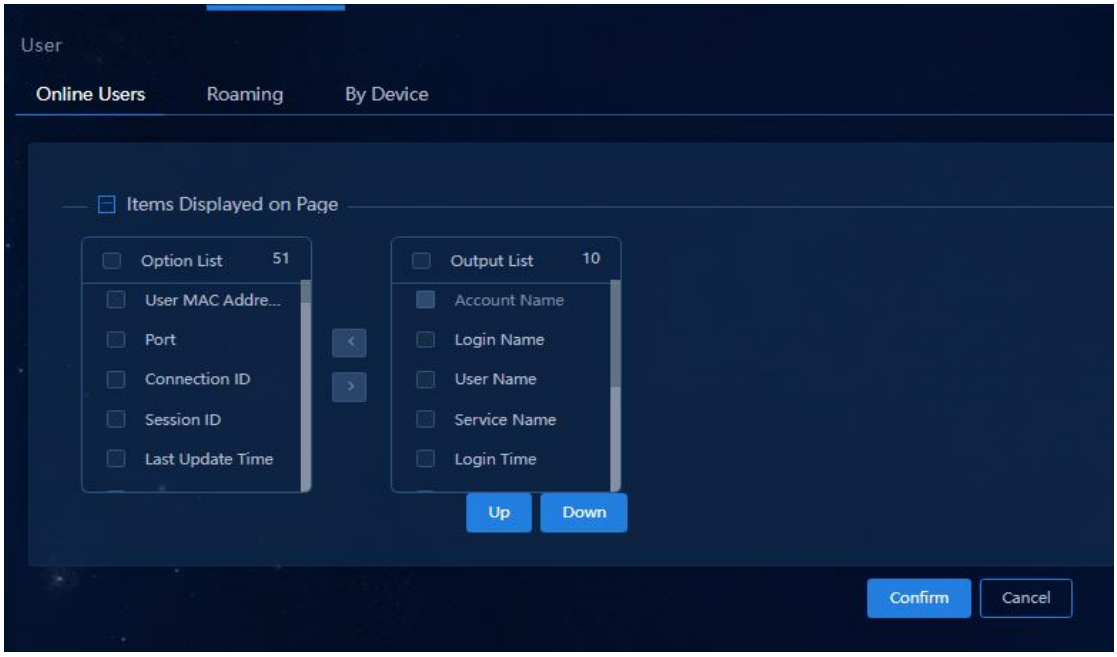
オンラインユーザーの管理

1. **Monitor** > **Monitor List** > **Online User** > **Local** ページに移動すると、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すると、メッセージの送信、強制ログアウト、オンライン情報のクリア、再認証、ページのカスタマイズ、一括エクスポート、詳細情報の表示、ログの収集、ブラックリストの設定など、オンラインユーザーを管理できます。



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。

   Custom Page をクリックします。オンラインユーザーリストのフィールドを表示するには、**Option List** でフィールドを選択し、›ボタンをクリックします。オンラインユーザーリストのフィールドを非表示にするには、出力リストでフィールドを選択し、‹ボタンをクリックします。



ユーザー認証とアクセス

認証に合格してオンラインになる前に、『Configuring AD-Campus』の説明に従って基本設定を完了する必要があります。設定には、次のカテゴリが含まれます。

- 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)。
- 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)。
- リーフデバイスグループへのデバイスの割り当て、およびリーフダウンリンクインターフェイスグループへのインターフェイスの割り当て。
- 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、アクセスポリシー、およびアクセスユーザーの設定。

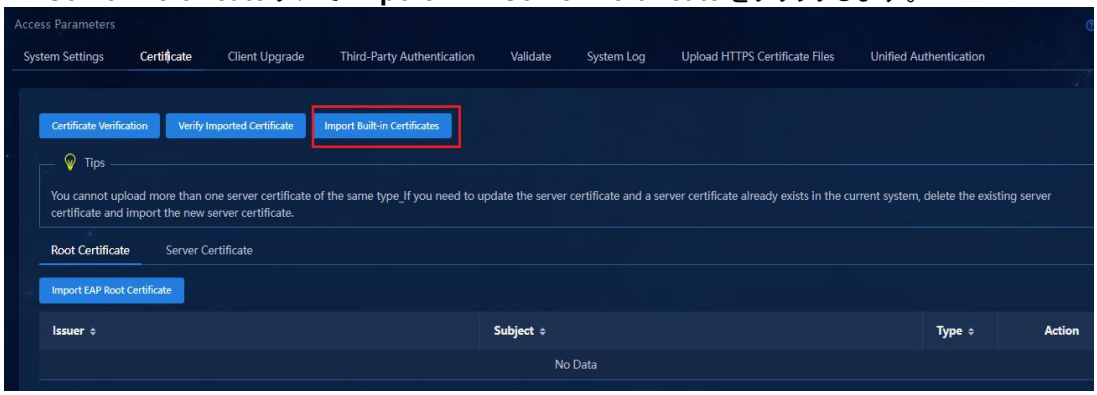
802.1X認証の設定

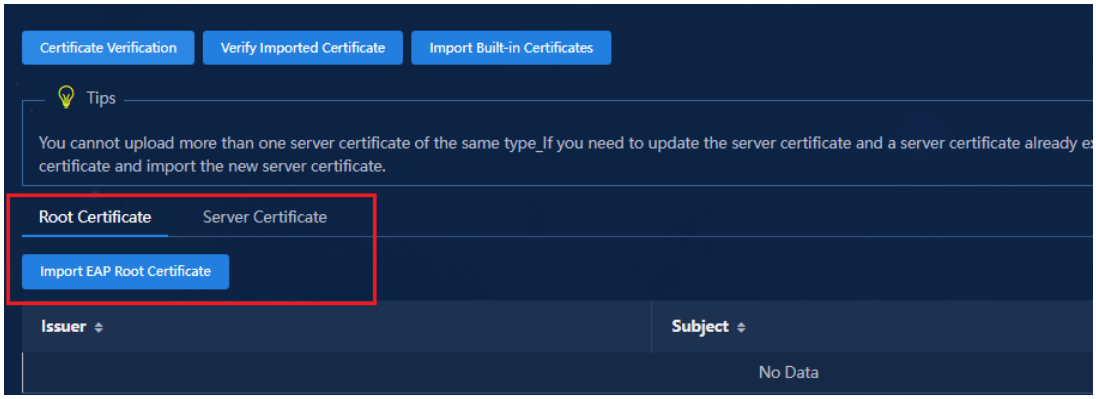
証明書のインストール

注:

- H3C iNode クライアントを使用して 802.1X 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. H3C 組み込み証明書をインポートするには、次の図に示すように、**Automation** > **User** > **Service Parameters** > **Access Parameters** ページに移動し、**Import Built-in Certificates** をクリックします。
2. 組み込み証明書をインポートした後、非 H3C iNode クライアントを使用して 802.1X 認証を正常に開始できます。
3. 顧客から提供された証明書をインポートする手順は、次のとおりです。
   - **Root Certificate** タブで、**Import EAP Root Certificate** をクリックします。
   - **Server Certificate** タブで **Import EAP Server Certificate** をクリックします。



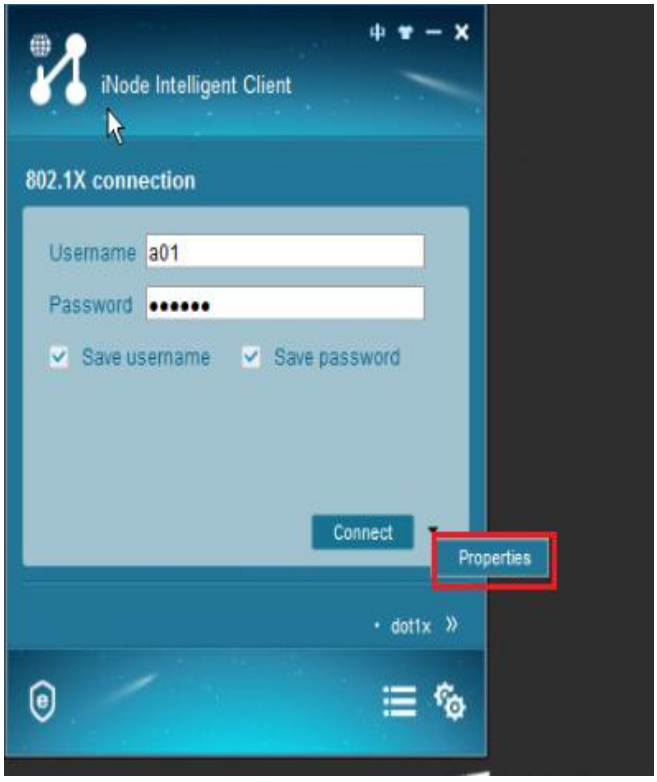


ユーザー認証

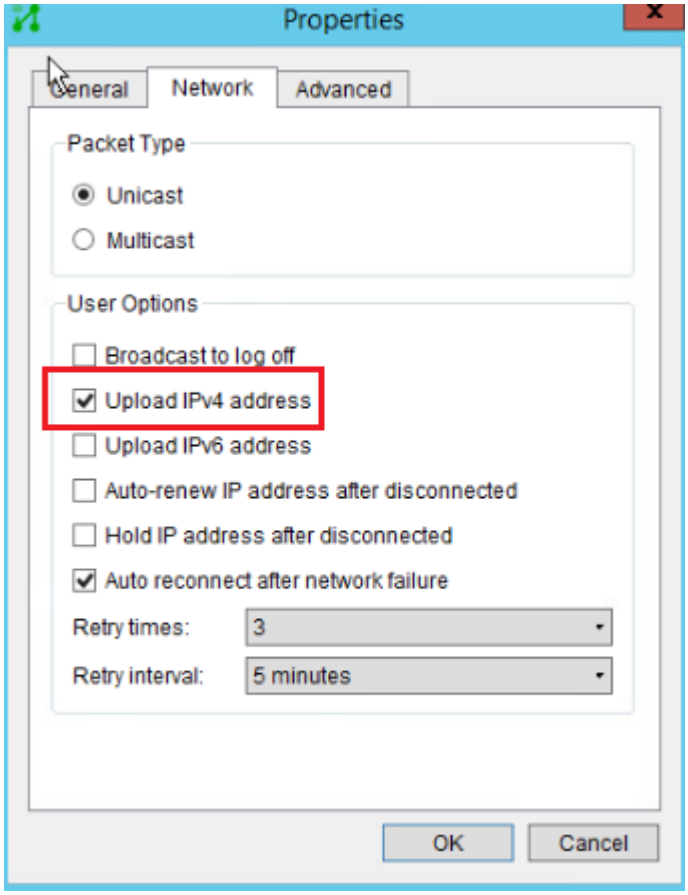
iNode クライアント

上記の設定が完了したら、iNode クライアントを介してオンラインになるための認証を実行できます。

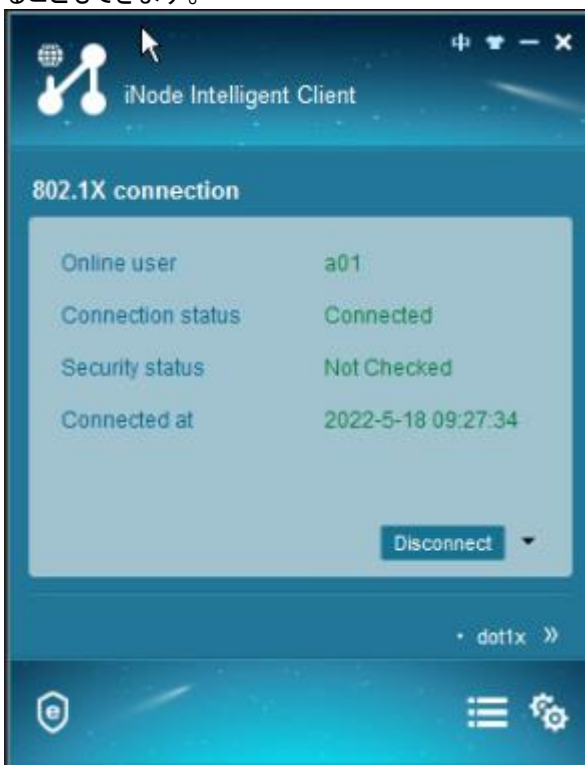
1. iNode クライアントを起動し、**Access User** page ページで作成またはインポートしたユーザー名とパスワードを入力します。

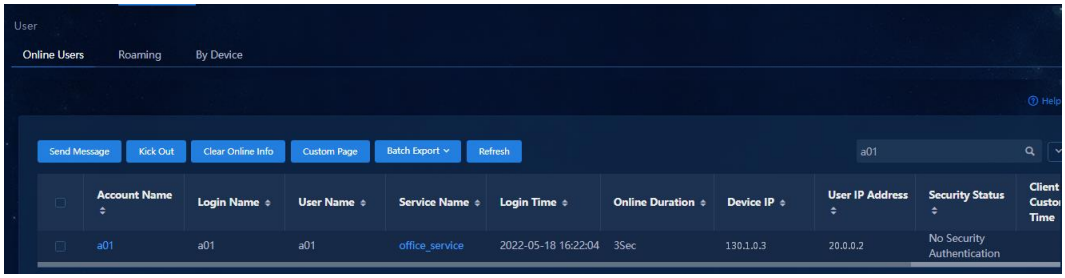


2. **Properties** パラメーターを構成します。**Connect** の横にある逆三角形をクリックし、**Properties** をクリックします。**Properties** ダイアログボックスで、次のパラメーターを構成します。
   - 認証をトリガーするパケットタイプとして **Unicast** または **Multicast** を選択します。
   - クライアントが静的 IP アドレスを使用する場合は、**Upload IPv4 address** を選択します。



3. **Connect** をクリックし、ユーザーがエンドポイント PC 上のネットワークに接続できることを確認します。**Monitor** > **Monitor List** > **User** > **Online Users** ページで、オンラインユーザー情報を表示することもできます。

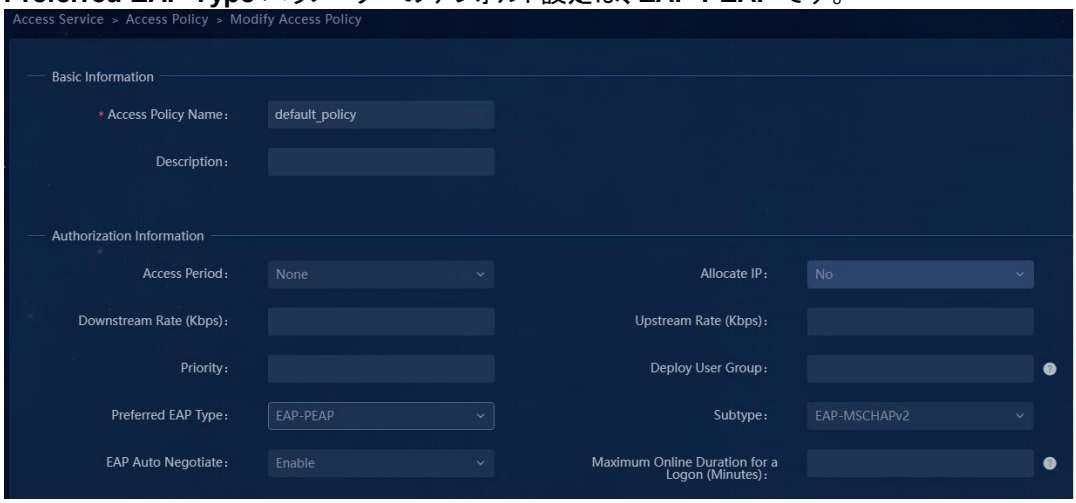




非 H3C iNode クライアント

1. 802.1X デバイスポリシーテンプレートで、認証方式を EAP に設定します。詳細については、『Configuring a device policy template of the 802.1X type』を参照してください。

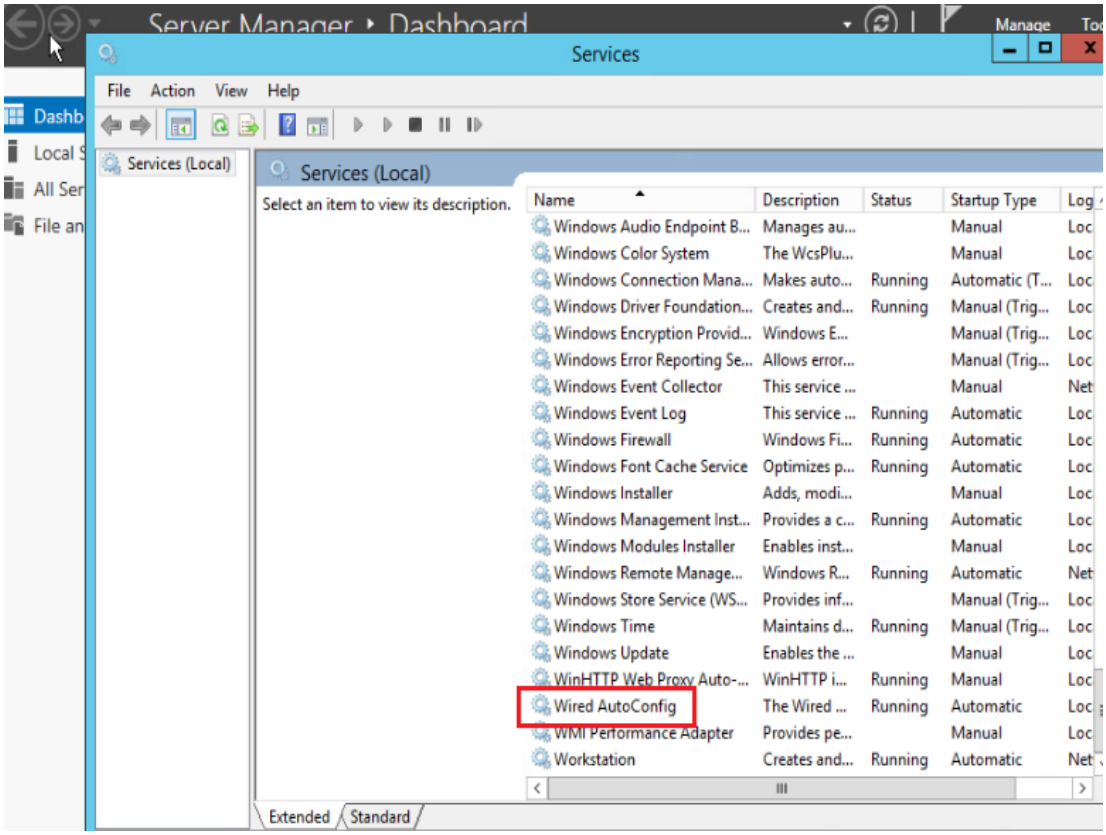
   Preferred EAP Type パラメーターのデフォルト設定は、**EAP-PEAP** です。



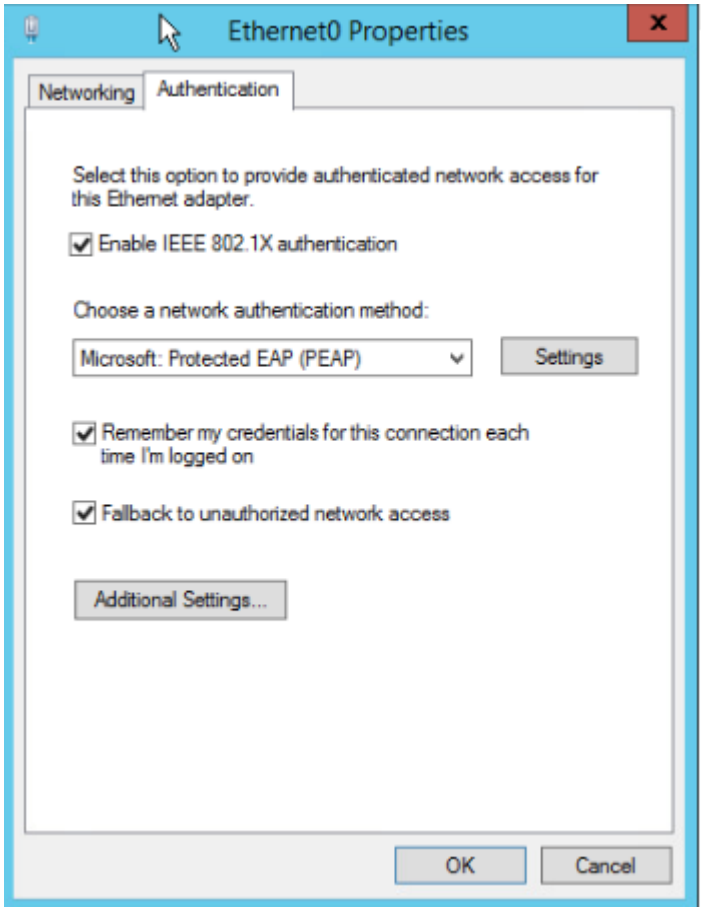
2. リーフダウンリンクインターフェイスでハンドシェイク機能をディセーブルにします。詳細については、『Configuring a user-defined policy template』を参照してください。

```
#
interface Bridge-Aggregation1024
 port link-type trunk
 port trunk permit vlan1 101 to 3000 4094
 link-aggregation mode dynamic
 mac-based ac
 dot1x
 undo dot1x handshake                          //Disable the handshake function.
 undo dot1x multicast-trigger
#
```

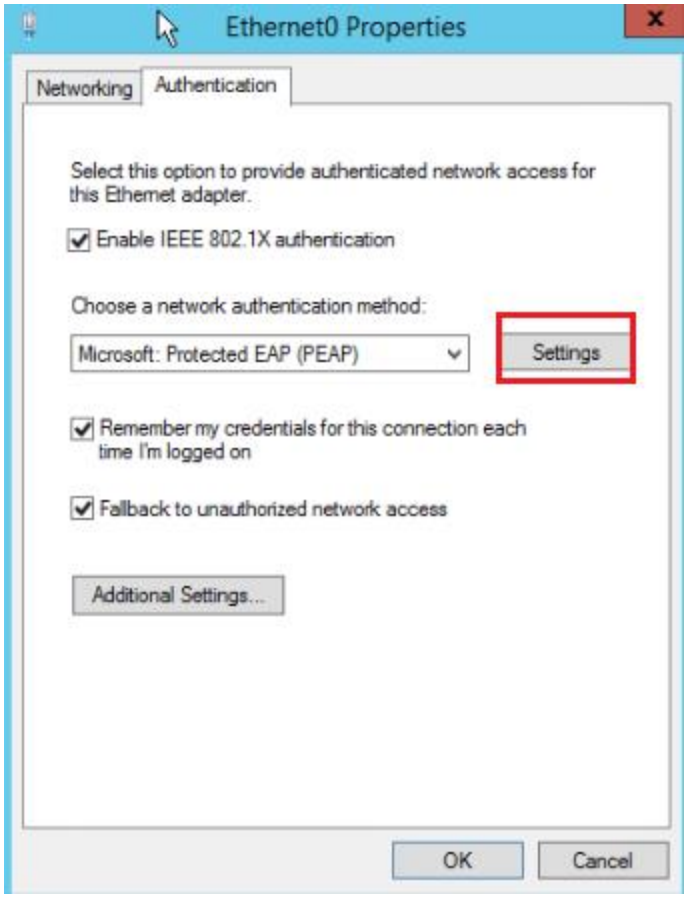
3. クライアントを設定し、**Services** で **Wired AutoConfig** サービスを有効にします。

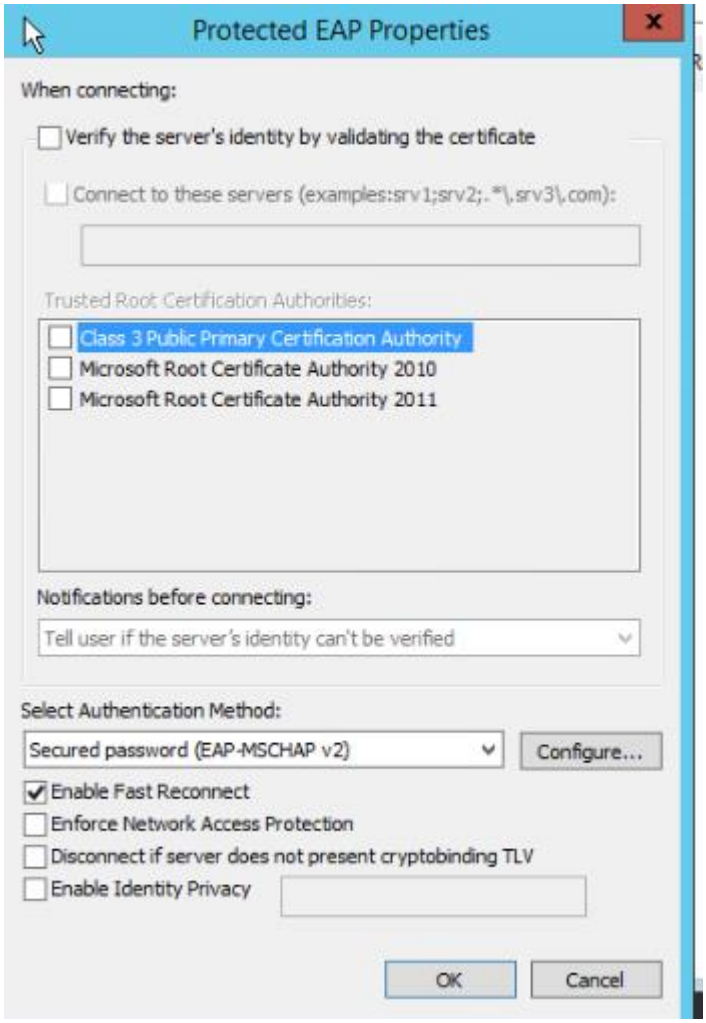


4. **Network Adapter** > **Etherbet0 Properties** > **Authentication** ページに移動し、**Enable IEEE 802.1X authentication** オプションと **Fallback to unauthorized network access** オプションを選択します。

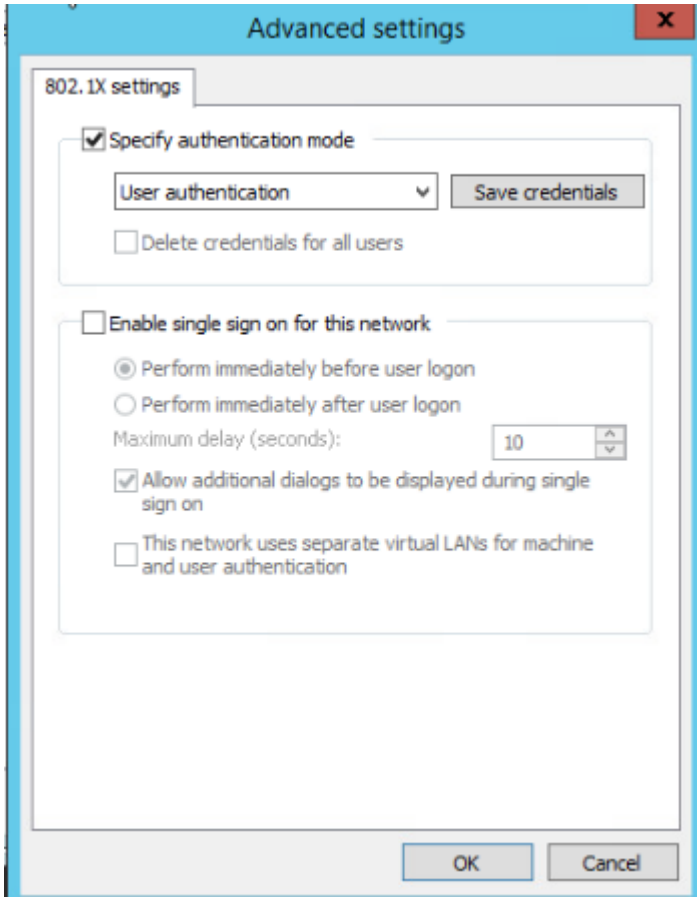


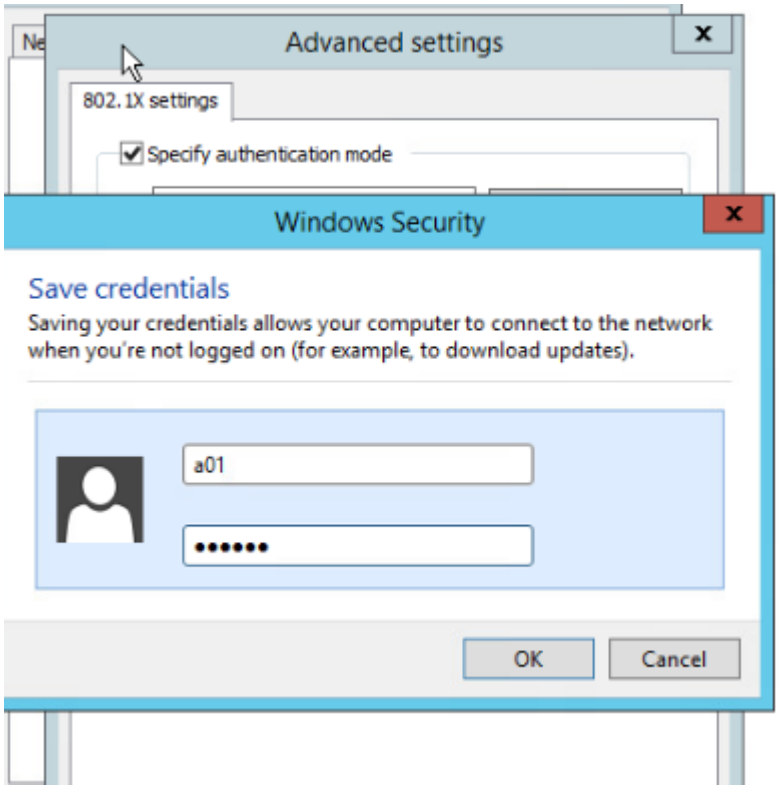
5. **Network Adapter** > **Etherbet0 Properties** > **Authentication** > **Settings** ページに移動し、**Verify the server's identity by validating the certificate** オプションをクリアします。その他のパラメーターにはデフォルト値を使用します。


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



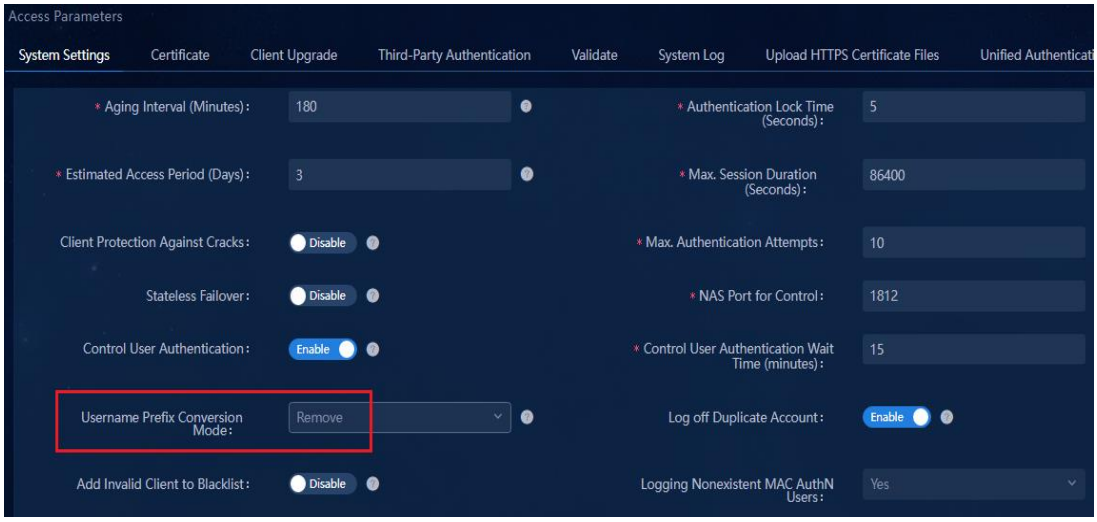
6. **Network Adapter** > **Etherbet0 Properties** > **Authentication** > **Advanced Settings** ページに移動し、**Specify authentication mode** オプションを選択し、ドロップダウンリストボックスで User authentication を選択して、**Save credentials** をクリックします。ポップアップページで、ユーザー名とパスワードを入力します。





7. **OK** をクリックすると、ユーザーが正常に認証されます。

8. 一部のエンドポイントにはプレフィクス情報があり、システムはユーザーが存在しないことを示すため、認証を通過できない場合があります。このような場合は、サフィックスを持つドメインを追加できます。詳細については、『Configuring a device policy template of the AAA type』を参照してください。さらに、**Automation>User>Service Parameters>Access Parameters>System Settings** ページに移動して、**Username Prefix Conversion Mode** を **Remove** に変更できます。



MACポータル認証の設定

> ⚠ **警告!**
>
> MAC ポータル認証ページにアクセスするには、エンドポイントで Google Chrome ブラウザを使用します。

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。

MAC ポータル認証には、次の段階があります。

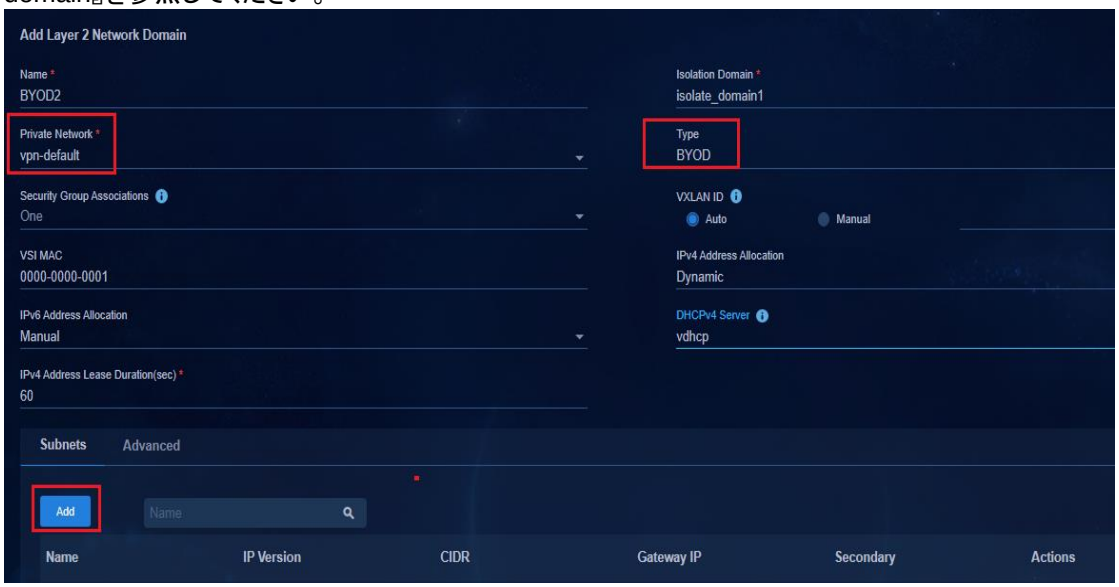
- **First stage**: ユーザーのエンドポイントがアクセススイッチのポートに接続され、ポートが起動すると、エンドポイントは MAC アドレスを含むパケットを送信して MAC 認証をトリガーします。スイッチはユーザーを BYOD 匿名ユーザーとして識別し、ユーザーを BYOD セキュリティグループに割り当てます。ユーザーエンドポイントは、セキュリティグループに指定されたサブネットから IP アドレスを取得します。
- **Second stage**: ユーザーが Web ページを開くと、アクセススイッチはそれを MAC ポータル認証ページにリダイレクトします。ページで、ユーザー名とパスワードを入力します。ユーザーが正常にログインした後、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 サーバー上の BYOD セキュリティグループ内の 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、第 1 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。ユーザーがプッシュされた Web ページにユーザー名とパスワードを入力してログインすると、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。第 1 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。

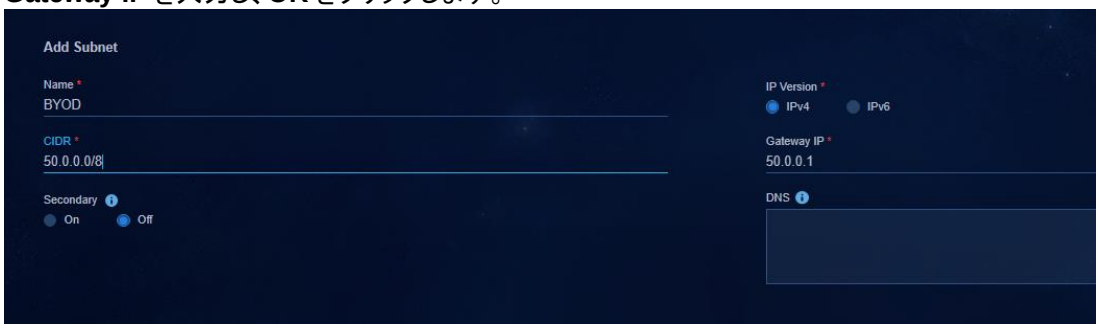
BYOD セキュリティグループの作成

SeerEngine キャンパスで BYOD セキュリティグループを設定するには、次の手順を実行します。

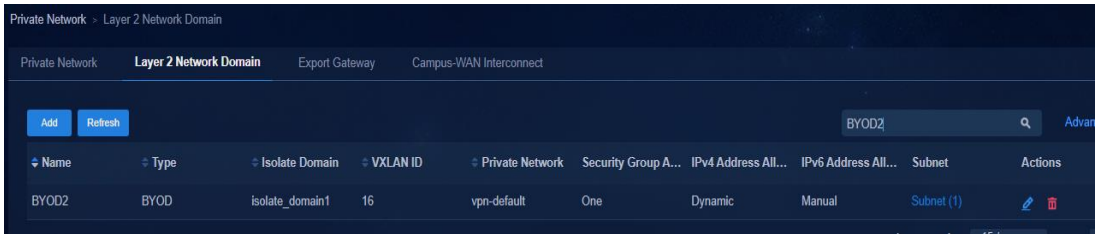
1. **Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動し、Add をクリックします。**Add Layer 2 Network Domain** ページで、Private Network フィールドで vpn-default を選択し、Type フィールドで BYOD を選択します。BYOD アドレスプールの IP アドレスのデフォルトのリース時間は 1 分です。リース時間は 30 秒以上にすることをお勧めします。必要に応じてリース時間を調整できます。BYOD セキュリティグループには H3C vDHCP サーバーを選択する必要があります。その他のパラメーターの説明については、『Creating a Layer 2 network domain』を参照してください。



2. サブネットタブで、**Add** をクリックします。**Add subnet** ページで、**Name**、**IP version**、**CIDR**、および **Gateway IP** を入力し、**OK** をクリックします。

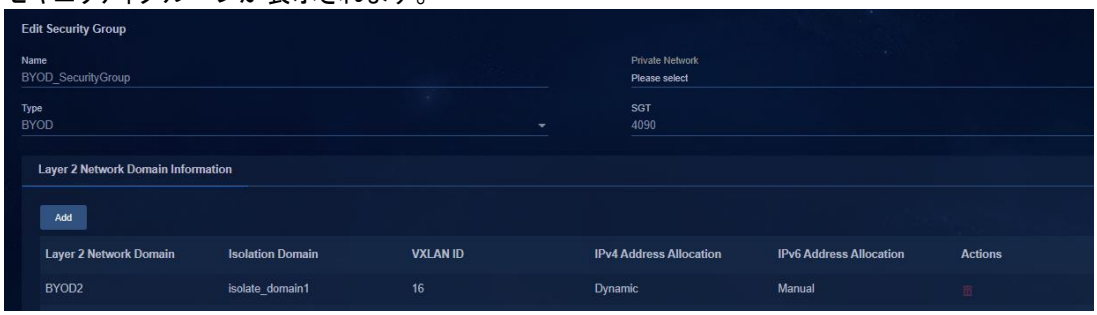


3. システムが **Add Layer 2 Network Domain** ページに戻ったら、**OK** をクリックします。その後、Layer 2 network domain リストに新しい BYOD レイヤー2 ネットワークドメインを表示できます。



4. BYOD レイヤー2 ネットワークドメインを追加したら、**Automation** > **Campus Network** > **Security Group** > **User Security Group** ページに移動し、**Add** をクリックします。**Add Security Group** ペ

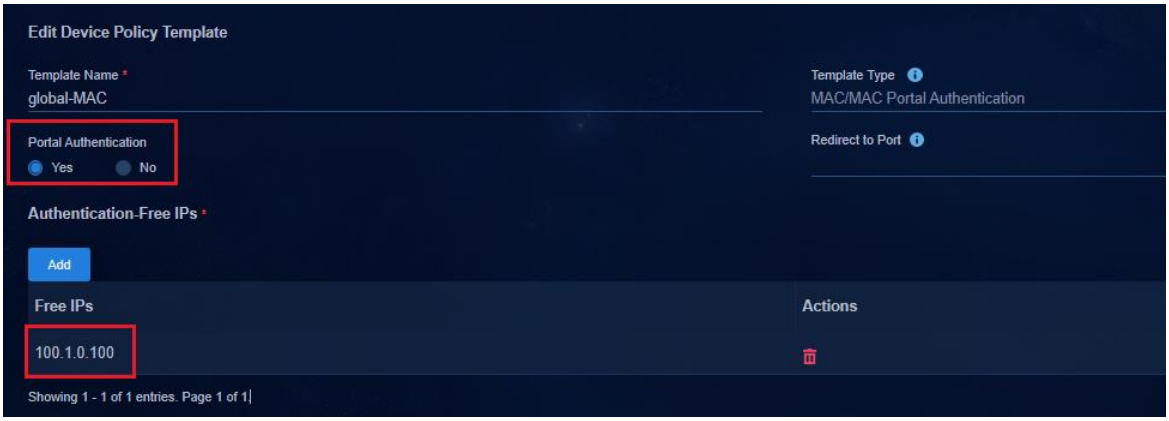
ージで、Type フィールドで BYOD を選択し、**Private Network** フィールドで **vpn-default** を選択します。**Layer 2 Network Domain Information** 領域で、Add をクリックして、前に追加した BYOD レイヤー2 ネットワークドメインを追加します。OK をクリックすると、セキュリティグループリストに BYOD セキュリティグループが表示されます。



ACL 3001 の設定

ACL 3001 は Configuring 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 **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、ACL 3001 がデバイスグループ内のデバイスに展開されます。コントローラー上で空き IP を追加、変更、または削除すると、コントローラーは変更をデバイスに展開します。



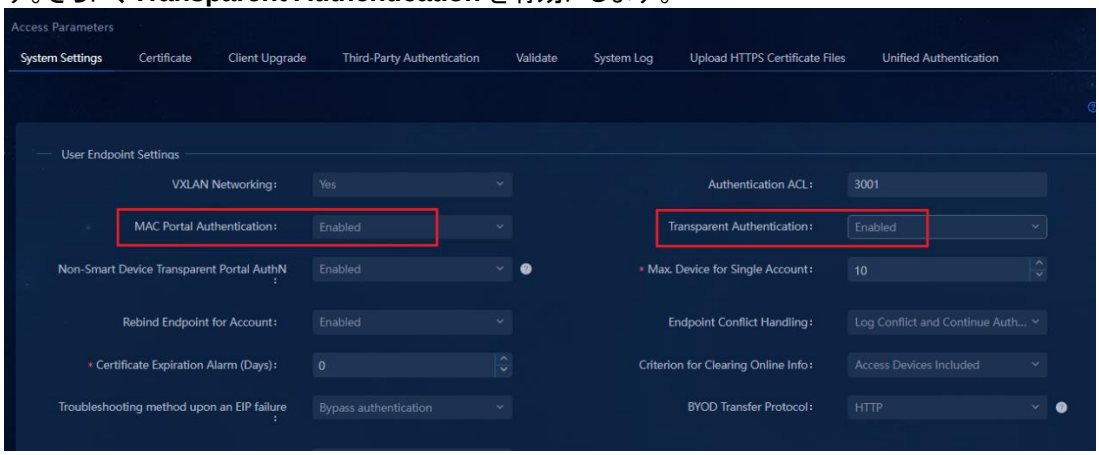
ACL ポリシーは、デバイスグループポリシー設定に従って展開されます。

```
#
<Leaf1>display acl all
Advanced IPv4 ACL 3001, 2 rules,
SDN_ACL_AUTH
ACL's step is 5, start ID is 0
 rule 0 permit udp destination-port eq dns
 rule 1 permit ip destination 100.1.0.100 0
#
```

MAC ポータル認証の有効化

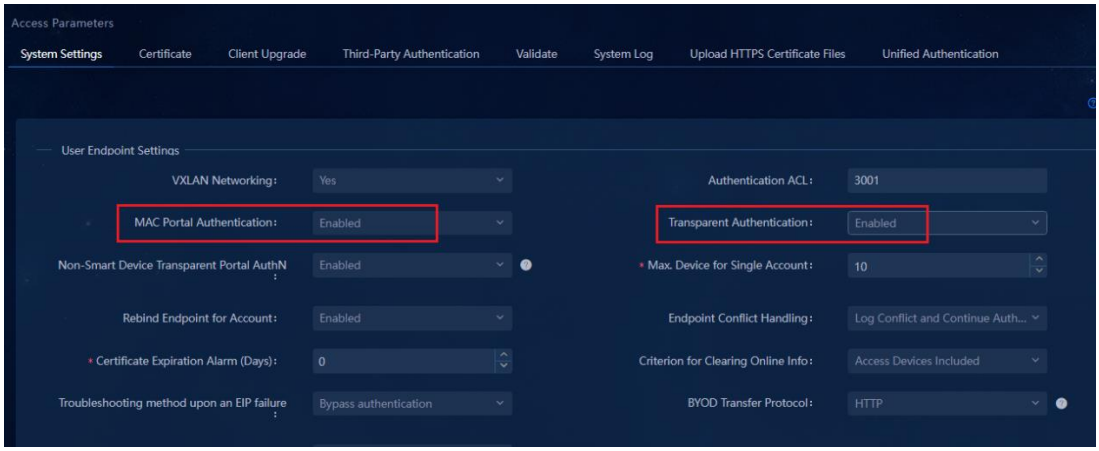
1. EIA に対して MAC ポータル認証を有効にするには、**Automation** > **User** > **Service Parameters** > **Access Parameters** > **System Settings** ページに移動し、**User Endpoint Settings** という名前のテンプレートに対応するアイコンをクリックします。**User Endpoint Settings** 領域で、**MAC**

Portal Authentication フィールドの **Enabled** を選択して、**MAC Portal Fast Configuration** ページを開きます。MAC ポータル認証が有効になっている場合は、まず無効にしてから再度有効にします。さらに、**Transparent Authentication** を有効にします。

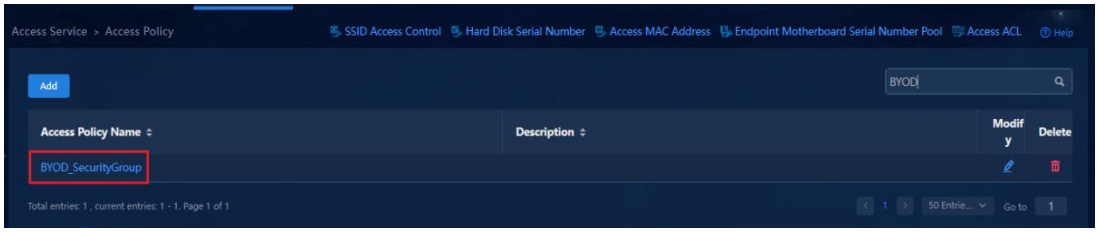


2. **MAC Portal Fast Configuration** ページで、**OK** をクリックします。

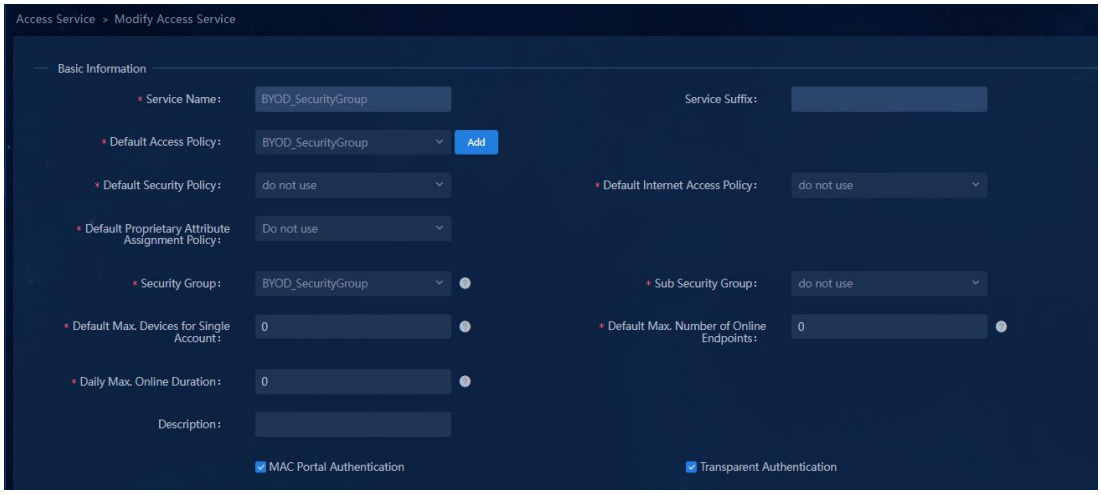
次のような一連の設定が自動的に作成されます。



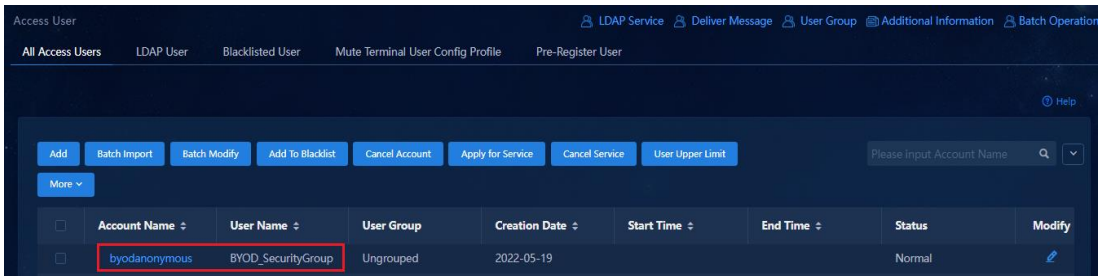
自動的に作成されたアクセスポリシー:



自動的に作成されたアクセスサービス、関連するアクセスポリシー、およびセキュリティグループ:

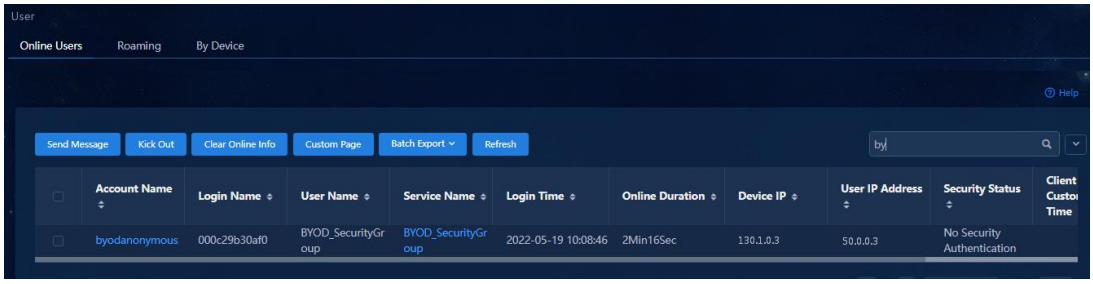


自動的に作成された BYOD ユーザー:



MAC ポータル認証の開始

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 byodanonymous を使用してログインします。ユーザーが BYOD 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 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。



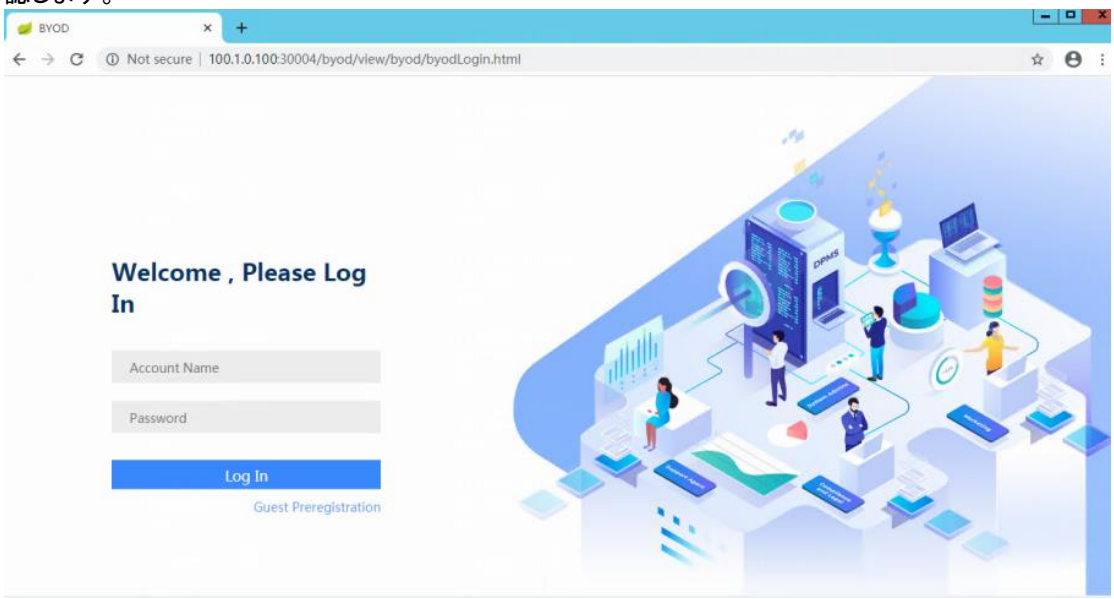
アクセススイッチ(オーセンティケータとして機能)で、次のようにオンライン MAC 認証ユーザー情報を表示します。

```
<Leaf1>display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 000c-29b2-2f11
Access interface: Bridge-Aggregation1024
Username: 000c29b22f11
User access state: Successful
Authentication domain: isp
IPv4 address: 50.0.0.2
```

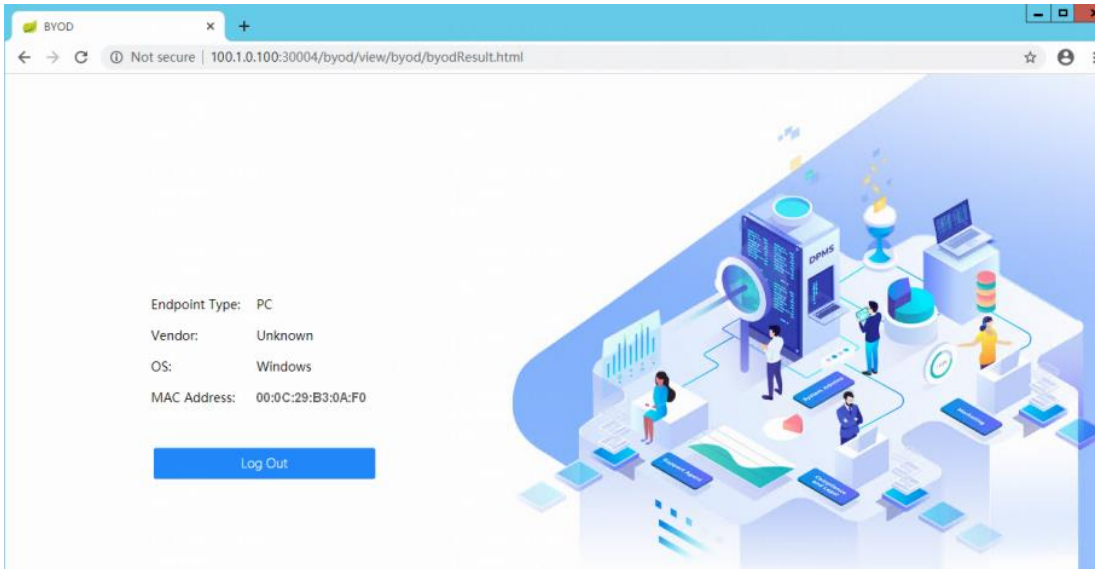
```
IPv4 address source: IP Source Guard
Initial VLAN: 111
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi5
Authorization ACL number/name: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: http://100.1.0.100:30004/byod/index.html?usermac=%m&userip=
%c&userurl=%o&original=%o
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 sec
Online from: 2020/10/20 11:38:07
Online duration: 0h 19m 53s
Port-down keep online: Disabled (offline)
```

2. ユーザーの PC で Web ブラウザを開き、1. 1. 1. 1 などの 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を自動的に開きます。ユーザーがリダイレクションページへのアクセスにドメイン名を使用する場合、次の制限があります。
   - ユーザーが DHCP を通じて IP アドレスを取得する場合は、隔離ドメインまたはレイヤー2 ネットワークドメインページで DNS サーバーIP を設定する必要があります。
   - ユーザーが静的 IP アドレスを使用する場合は、DNS サーバーIP をユーザーに対して手動で設定する必要があります。

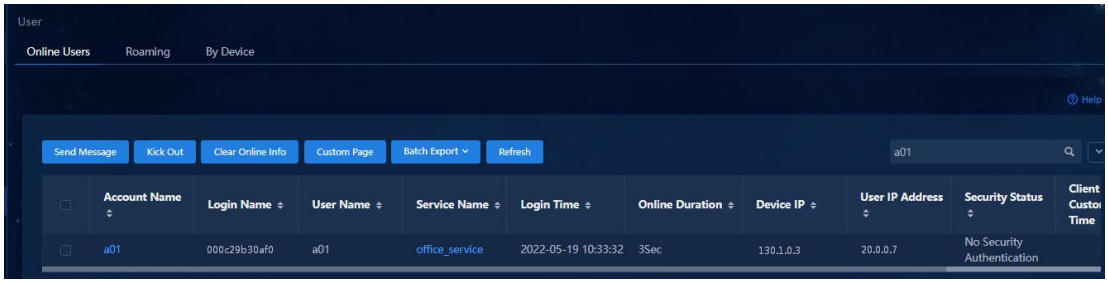
   さらに、スパインデバイスとリーフデバイスが DNS サーバーに到達するルートを持っていることを確認します。



3. 正しいアカウント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。



MAC 認証ユーザー情報がアクセスデバイスに表示されます。

```
<leaf10510> dis mac-authentication connection user-name 000c29b22f11
Total connections: 1
Chassis ID: 2
Slot ID: 10
User MAC address: 000c-29b2-2f11
Access interface: Bridge-Aggregation1024
Username: 000c29b22f11
User access state: Successful
Authentication domain: hz1
IPv4 address: 20.0.0.7
IPv6 address: FE80::18AD:C0E3:497B:84BA
IPv4 address source: IP Source Guard
IPv6 address source: User packet
Initial VLAN: 120
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization dynamic ACL 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: 2021/08/24 10:36:48
Online duration: 0h 2m 5s
Port-down keep online: Disabled (offline)
```

MAC認証の設定

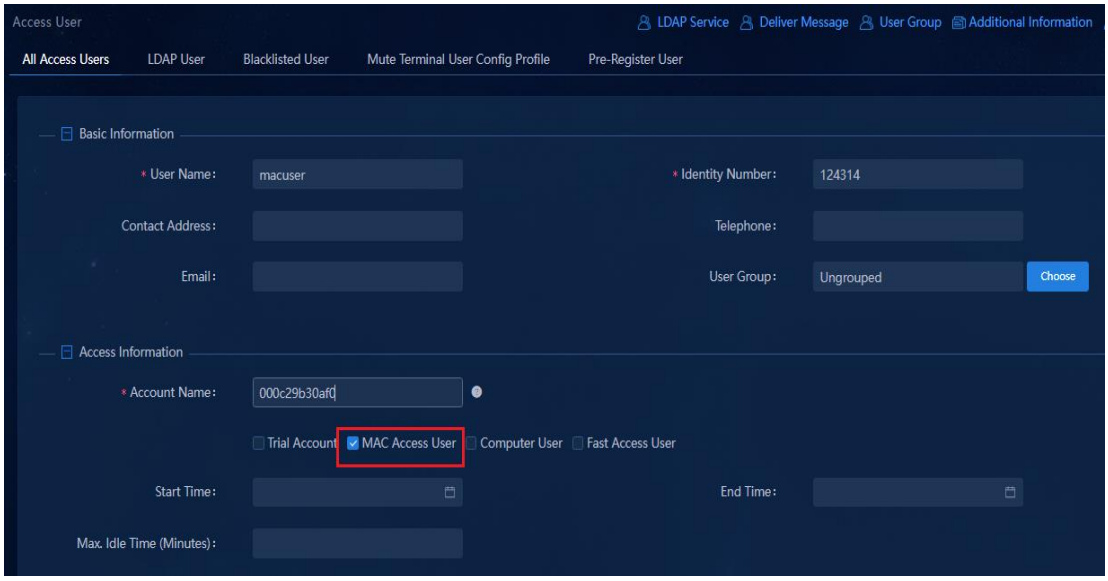
MAC 認証は主に、ユーザーがクライアントを持たず、エンドポイント MAC アドレスを介して直接オンラインになるように認証をトリガーするシナリオに適用されます。

MAC 認証ユーザーの設定

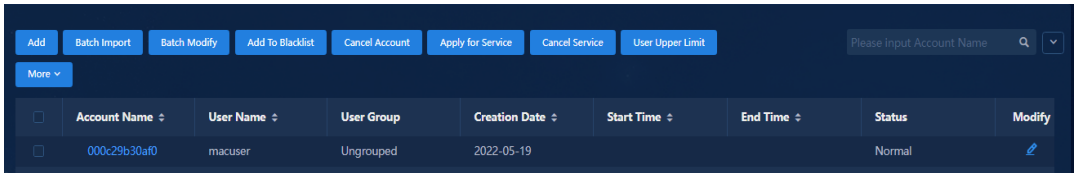
MAC 認証ユーザーを設定するには、**Automation** > **User** > **Access User** ページに移動し、**Add** をクリックしてアクセスユーザーを手動で追加するか、アクセスユーザーを一括でインポートします。

アクセスユーザーを手動で追加する

1. **Access User** ページで **Add** をクリックします。**Access Information** 領域でアカウント名を入力し、**MAC Access User** オプションを選択します。次に、サーバーによってユーザーのパスワードが自動的に構成されます。アカウント名は、次の図に示すように xxxxxxxxxxxx の形式の MAC アドレスです。

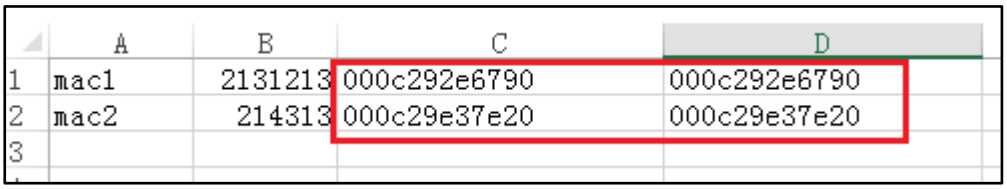


2. ユーザーのアクセスサービスを選択し、**OK** をクリックします。



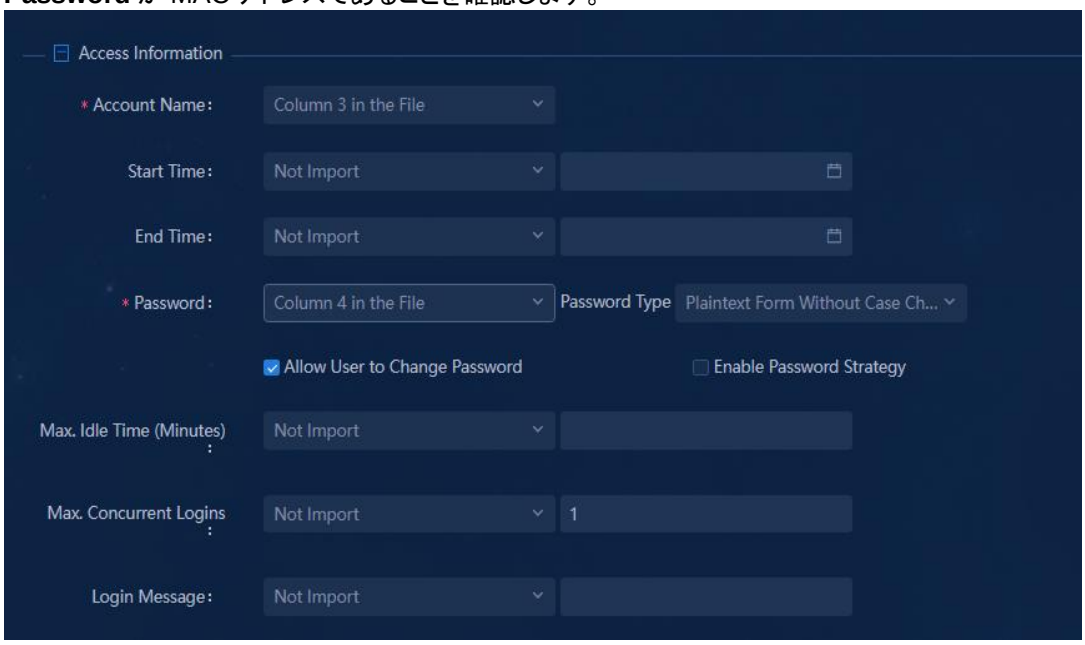
アクセスユーザーの一括インポート

1. **Access User** ページで、**Batch Import** をクリックします。**Tips marvel** 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。ダウンロードしたテンプレートに従って、インポートするアクセスユーザーの情報を入力します。
2. **Upload** をクリックし、アップロードするファイルを選択します。ファイル内のユーザー名とパスワードは、次の図に示すように、xxxxxxxxxxxx 形式の MAC アドレスである必要があります。

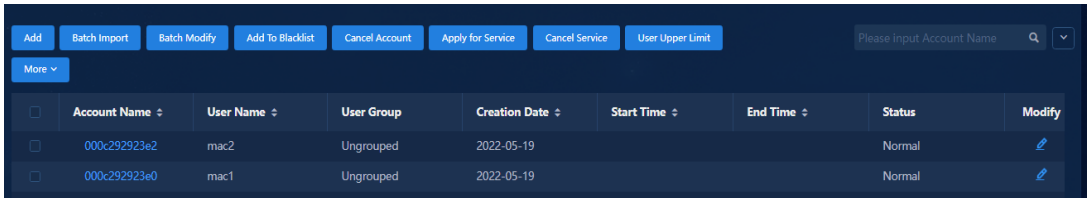


	A	B	C	D
1	mac1	2131213	000c292e6790	000c292e6790
2	mac2	214313	000c29e37e20	000c29e37e20
3				

3. ファイルをアップロードしたら、ファイルで使用されているカラム区切り文字を選択し、**Next** をクリックしてアクセスユーザー設定ページを開きます。**Access Information** 領域の **Account Name** と **Password** が MAC アドレスであることを確認します。

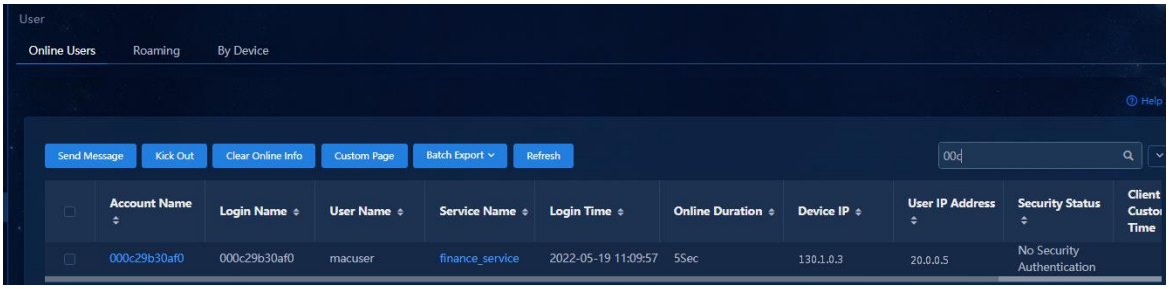


4. アクセスサービスを選択し、**OK** をクリックします。2 人の新しいユーザーが正常にインポートされたことが表示されます。



MAC 認証の設定

PC に接続しているスイッチ上のポートがアップになると、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、**Monitor** > **Monitor List** > **User** > **Online Users** ページで、MAC 認証済みオンラインユーザーに関する情報を表示できます。

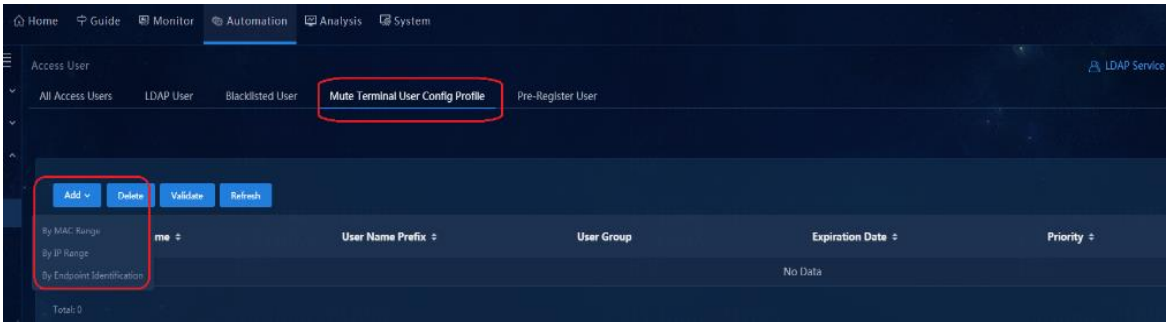


ブロードバンドIoTサービスの設定

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、ユーザーは認証のためにユーザー名とパスワードを手動で入力する必要はなく、直接オンラインになります。

現在、MAC アドレス範囲、IP アドレス範囲、およびエンドポイント ID の 3 つのコンフィギュレーションモードを使用できます。

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 アドレスの範囲を設定します。リーフ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*****コマンドを実行します。インターフェイスポリシーテンプレートで **Include User IP Addresses in MAC Authentication Requests** をイネーブルにする方法については、『Configuring an interface policy template of the MAC/MAC portal authentication type』を参照してください。
- **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。

⚠ 警告!

- 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。プライオリティ値は 0～n の値に設定できます。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** 認証の場合と、**Bind User IP** 認証がアクセスポリシーで設定されている場合にだけ使用します。それ以外のユーザー認証の場合は、このコマンドを使用しないでください。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、コントローラーは ARP スヌーピング設定を発行して、スタティック IP アドレスを EIA に配信します。

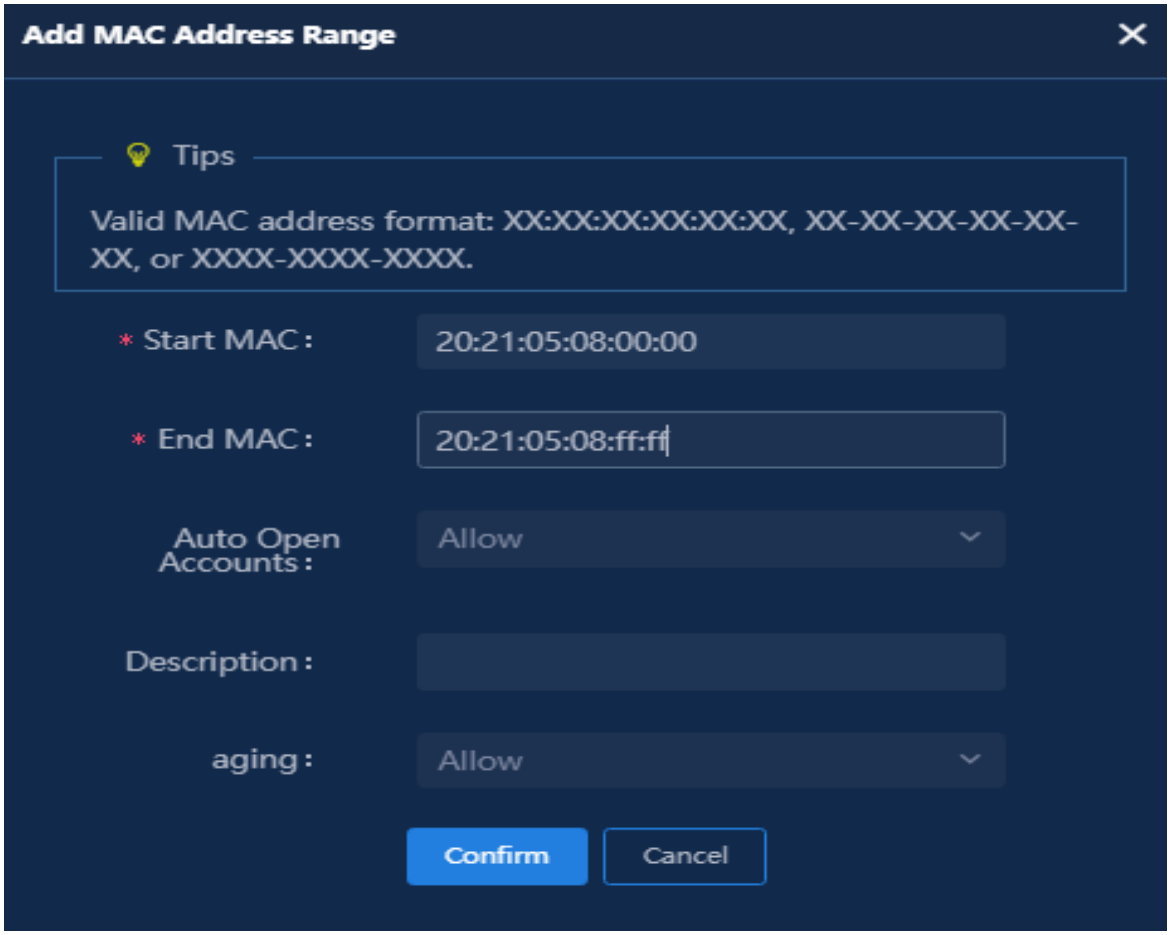
MAC アドレス範囲に基づく高速オンライン

Mute Terminal User Config Profile ページで、**Add** をクリックし、**By MAC Range** を選択します。ポップアップページで、プロファイル名とユーザー名プレフィクスを入力します。このページの **Basic Information** 領域の Priority パラメーターは、0～999 の値に設定できます。デフォルト値は 0 です。値が小さいほど、プライオリティが高くなります。

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。

アクセスユーザーを手動で追加する

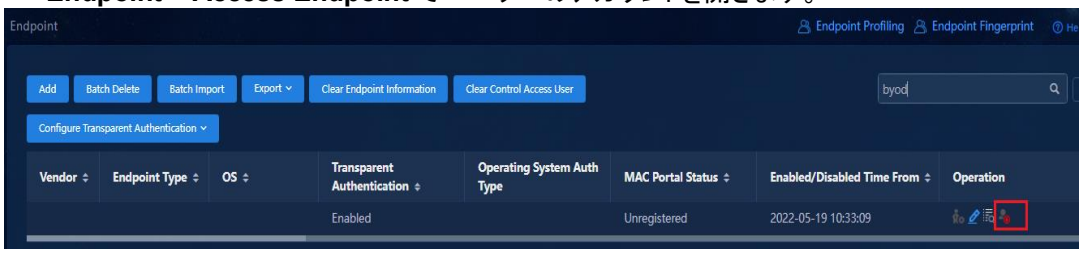
Add をクリックして、**Add MAC Address Range** ページを開きます。MAC アドレス範囲を入力し、OK をクリックします。複数の MAC アドレス範囲を追加できます。各アドレス範囲は、要件に従って構成できます。



Add MAC Address Range ページのパラメーターの説明:

- **Auto Open Accounts**: **Allow** または **Deny** に設定できます。

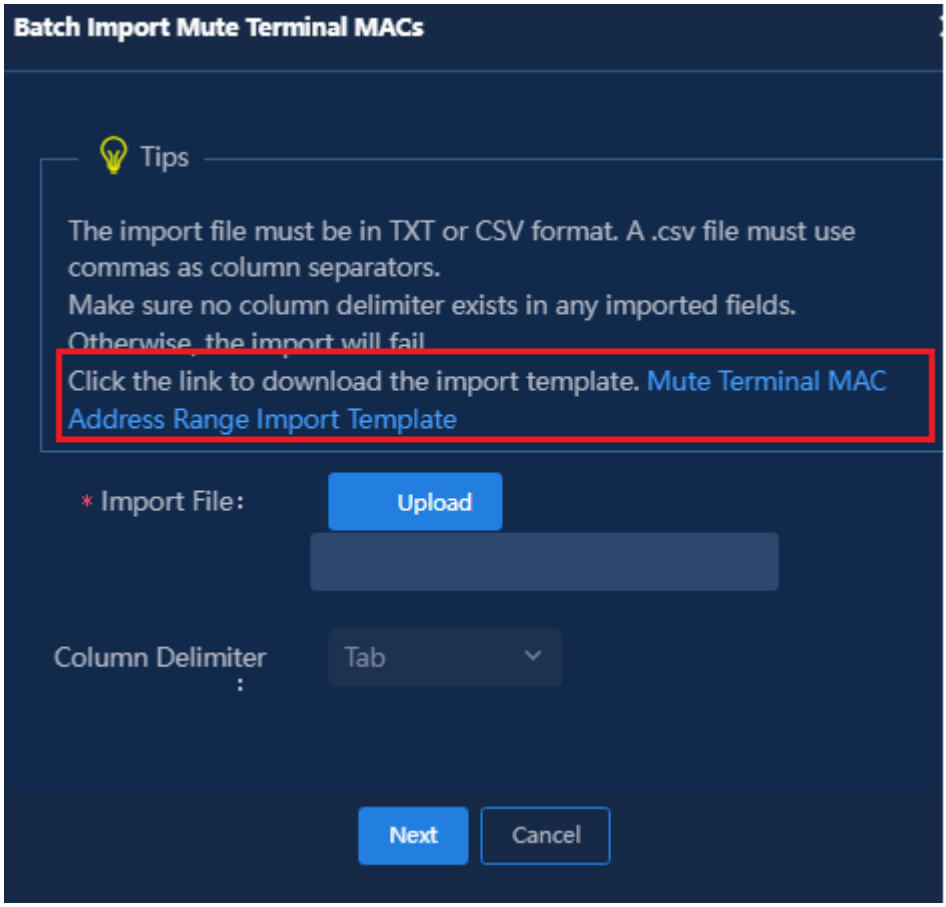
- **Allow**: エンドポイントが MAC アドレス範囲と一致する場合、システムはユーザーを認証するアカウントを自動的に作成し、認証されたユーザーを対応するセキュリティグループに追加し、ユーザーの IP アドレスを取得します。
- **Deny**: アカウントは自動的に作成されません。認証されたユーザーは、MAC ポータル認証をトリガーして、BYOD セキュリティグループに入ります。管理者は、**Monitor** > **Monitor List** > **Endpoint** > **Access Endpoint** でユーザーのアカウントを開きます。



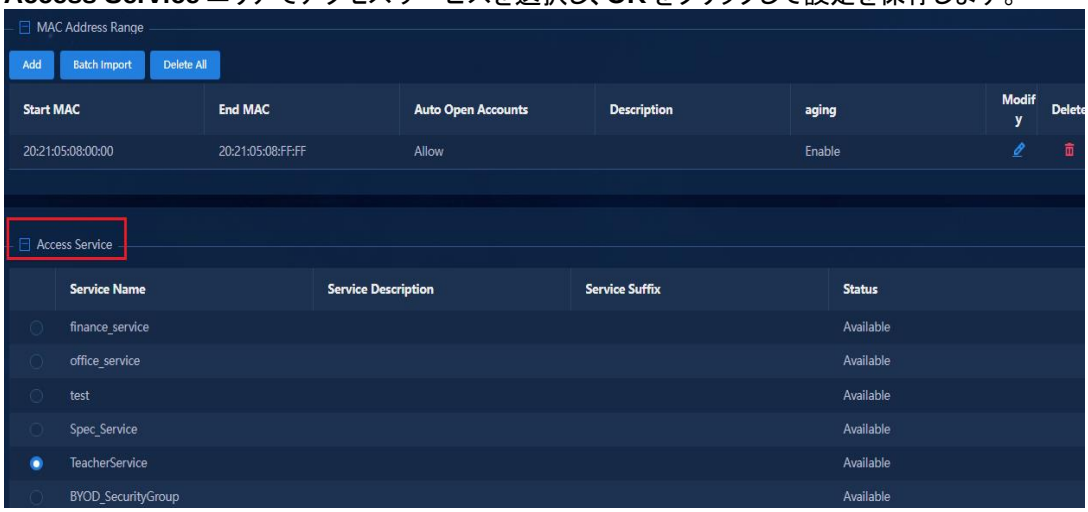
- **aging**: **Allow** または **Prohibit** に設定できます。
  - **Allow**: EIA は、トラフィックがなく、NAS がリブートし、NAS ポートがダウンした場合に、認証されたミュートエンドポイントがタイムアウト後にオフラインになることを許可します。
  - **Prohibit**: トラフィックがなく、NAS がリブートし、NAS ポートがダウンしている場合、EIA はミュートエンドポイントのエージングを許可せず、EIA 上のミュートエンドポイントはオンラインのままになります。リーフデバイスが回復すると、EIA からのオンライン情報を要求して、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。

アクセスユーザーの一括インポート

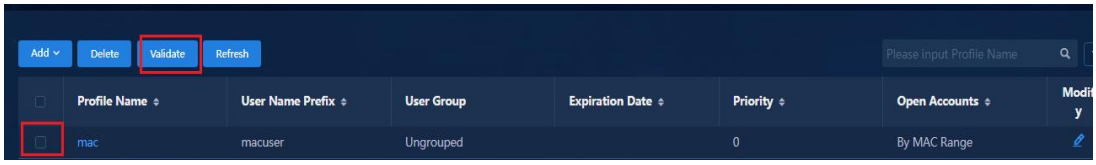
1. **Batch Import** をクリックして、**Batch Import Mute Terminal MACs** ページを開きます。バッチインポート用のインポートテンプレートをダウンロードできます。**Mute Terminal MAC Address Range Import Template** リンクをクリックして、インポートテンプレートをダウンロードします。ダウンロードしたテンプレートに従って、インポートする MAC アドレス範囲を入力します。テンプレートの形式は次のとおりです。



2. **Upload** をクリックし、アップロードするファイルを選択します。次に、ファイルで使用する列デリミタを選択し、**Next** をクリックします。**Batch Import Mute Terminal MACs** ページでパラメーターを設定し、**OK** をクリックします。このページのパラメーター設定の詳細は、『Manually adding an access user』を参照してください。
3. **Access Service** エリアでアクセスサービスを選択し、**OK** 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 分以内)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。

⚠ **警告!**

手動の **Validate** 操作では、一度に約 2000 個の MAC アドレスを有効にできます。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。

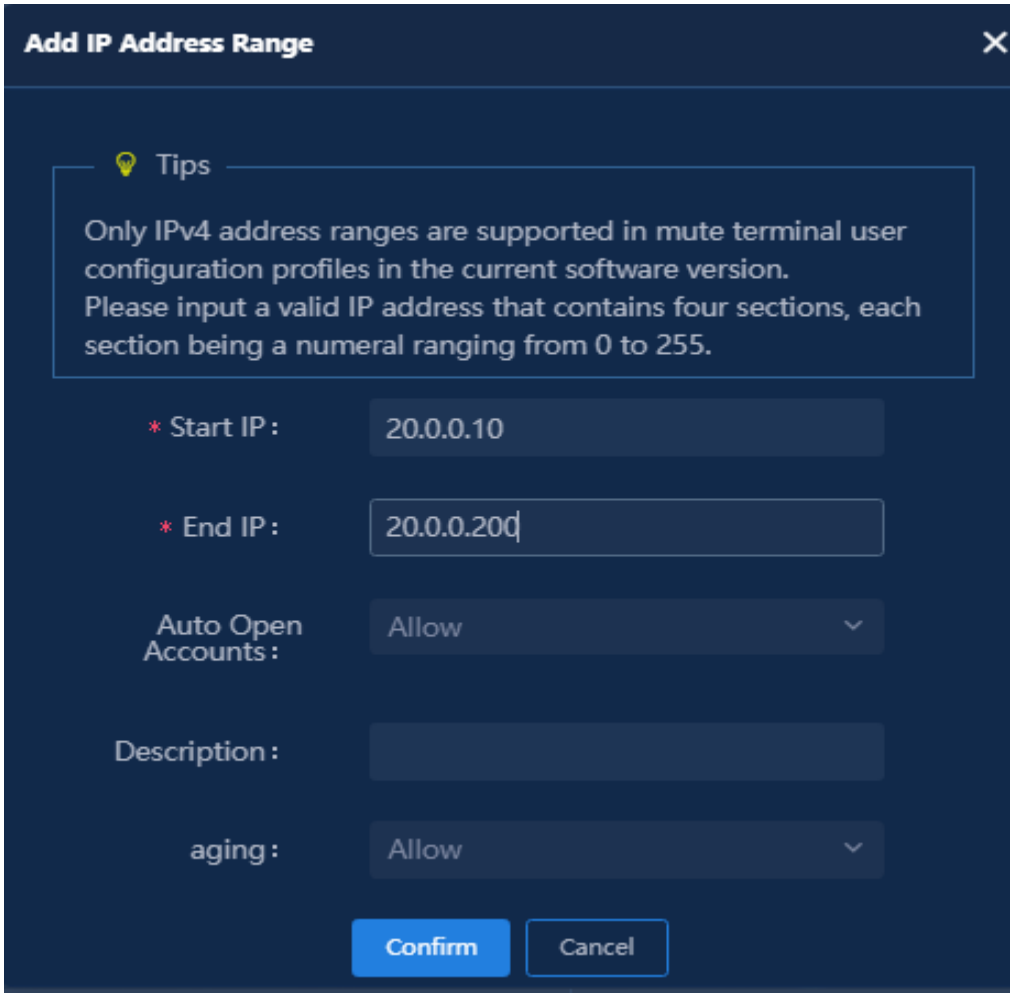
IP アドレス範囲に基づいた高速オンライン

Mute Terminal User Config Profile ページで、**Add** をクリックし、**By IP Range** を選択します。このページの **Basic Information** 領域にある **Priority** パラメーターには、0～999 の値を設定できます。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、異なっている必要があります。

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。

アクセスユーザーを手動で追加する

IP Address Range 領域で、**Add** をクリックして **Add IP Address Range** ページを開きます。このページでパラメーターを構成し、**OK** をクリックして構成を保存します。

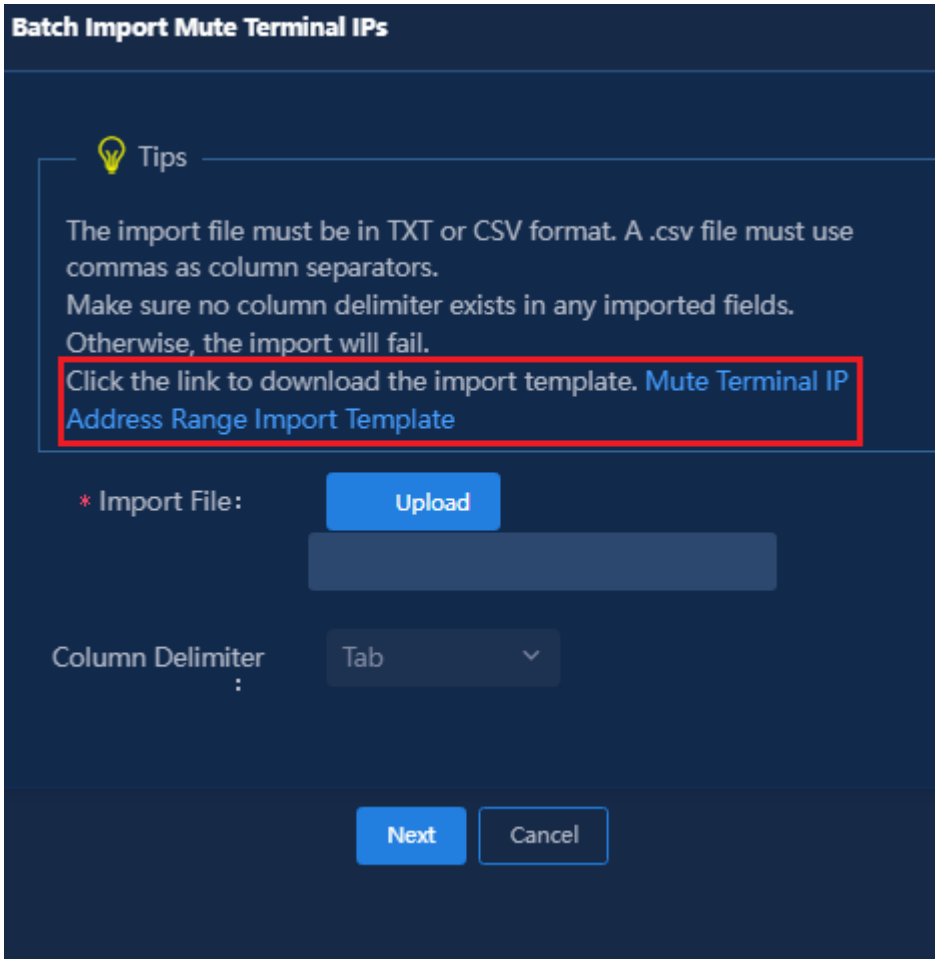


⚠ 警告!

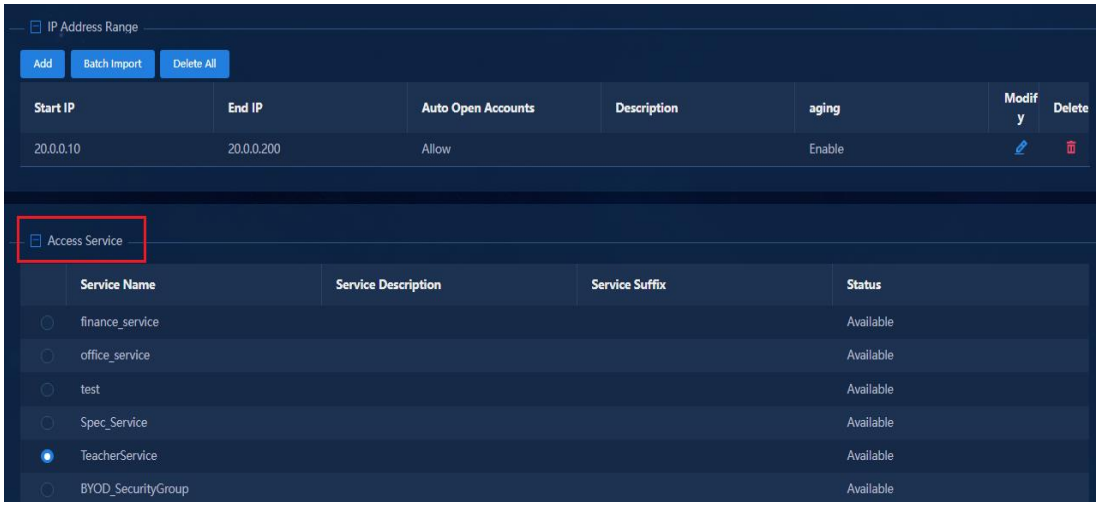
- 入力する IP 範囲は、**Access Service** で設定されたセキュリティグループのサブネットと同じである必要があります。セキュリティグループのサブネットを表示するには、SeerEngine キャンパスにログインし、**Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動して、Subnet カラムのサブネットリンクをクリックします。
- 複数の IP アドレス範囲を追加できます。各 IP アドレス範囲のパラメーターは、必要に応じて設定できます。

アクセスユーザーの一括インポート

1. **Batch Import** をクリックします。バッチインポート用のインポートテンプレートをダウンロードできます。**Mute Terminal IP 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 IP アドレス範囲を入力します。テンプレートの形式は次のとおりです。



2. **Upload** をクリックし、アップロードするファイルを選択します。次に、ファイルで使用する列デリミタを選択し、**Next** をクリックします。**Batch Import Mute Terminal MACs** ページでパラメーターを設定し、**OK** をクリックします。このページのパラメーター設定の詳細は、『』を参照してください。
3. このページでアクセスサービスを選択し、**OK** 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 分以内)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*****コマンドをリーフデバイスのダウンリンクインターフェイスに展開します。スタティック IP アドレスを使用するクライアントが認証をトリガーし、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*****コマンドについて:

   - **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認証をトリガーします。
   - **exclude-ip acl***: ACL の指定された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。

   次のコマンドがリーフデバイスに展開されます。

   #アドレス fe80 に一致する ACL を作成します。

   ```
   acl ipv6 basic 2000
   rule deny source fe80:0::0:0 16
   #
   ```

   #mac-authentication carry user-ip コマンドをリーフダウンリンクインターフェイスに展開します。

   ```
   interface gigabitethernet 1/0/1
   mac-authentication carry user-ip exclude-ip acl 2000
   #
   ```

⚠ 警告!

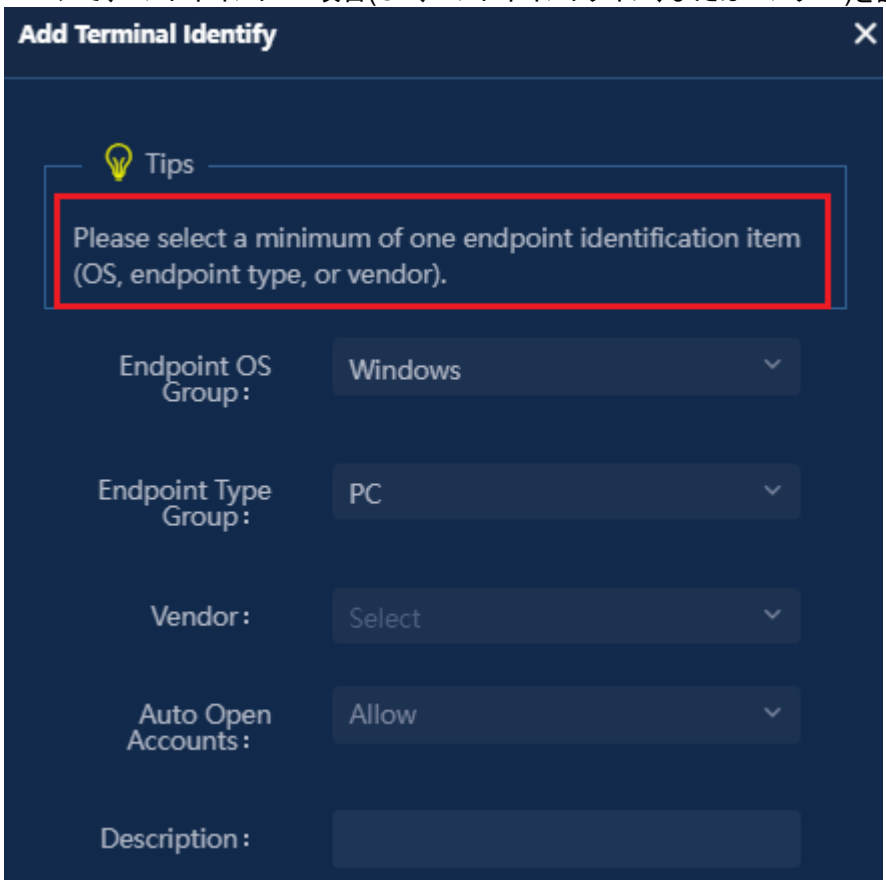
- 現在の AD-Campus ソリューションでは、fe80 で始まる IPv6 リンクローカルアドレスをフィルタリングするには、**mac-authentication carry user-ip exclude-ip acl***コマンドが必要です。
- エンドポイントユーザーがスタティック IP アドレスを使用してにアクセスする場合、ユーザーパケットで伝送される IP アドレスは、ユーザーの実際の IP アドレスではない場合があります。たとえば、IPv4 スタティックアドレスネットワーキングでは、ユーザーパケットで伝送される IP アドレスは、fe80 で始まる IPv6 リンクローカルアドレスです。**mac-authentication carry user-ip** コマンドが使用された後、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 認証要求を開始します。これにより、サーバーは誤った IP アドレスをユーザーにバインドするか、ユーザーを正しい IP および MAC アドレスバインディングと照合できなくなります。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 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

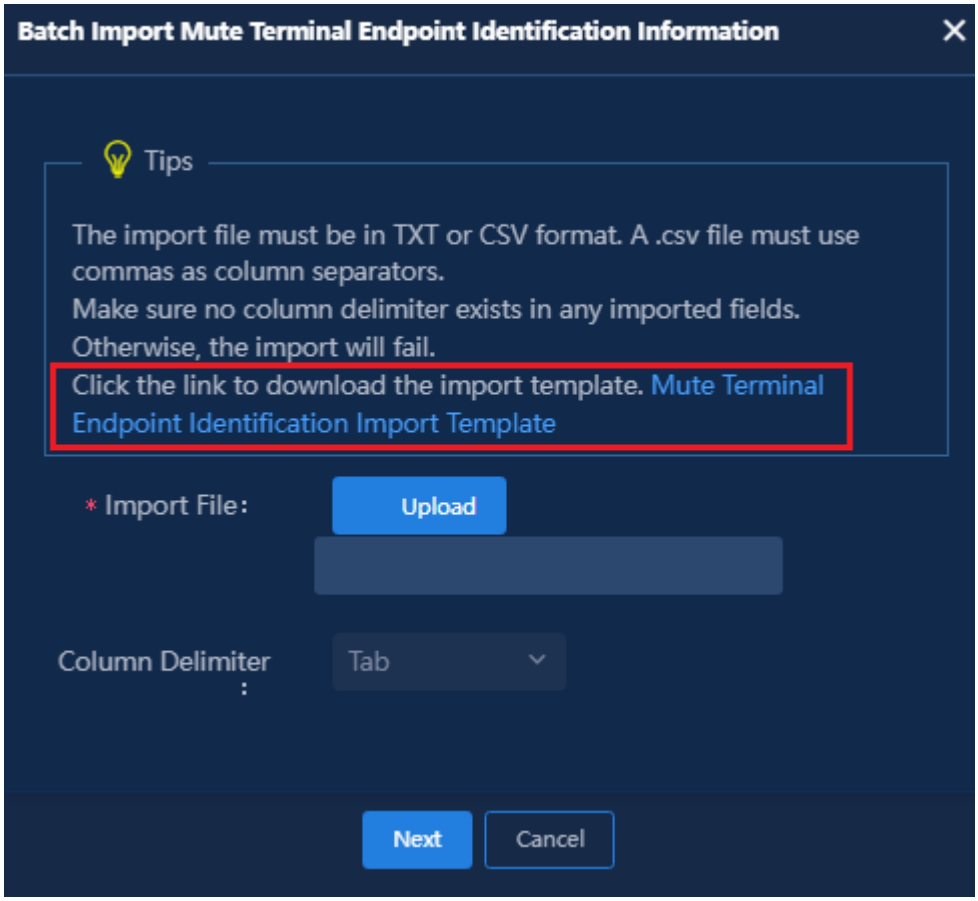
Mute Terminal User Config Profile ページで、**Add** をクリックし、**By Endpoint Identification** を選択します。

エンドポイント識別項目は、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。その他のパラメーターの設定については、『Fast online based on MAC address ranges』を参照してください。

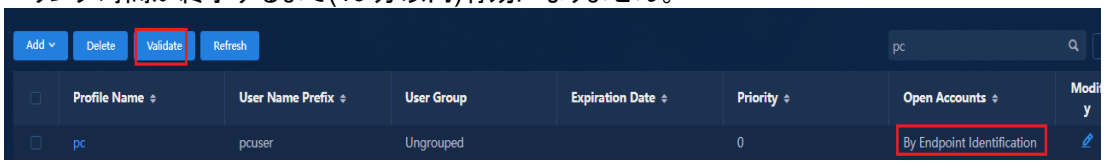
- エンドポイント ID エントリーを手動で追加するには、**Add** をクリックします。**Add Terminal Identity** ページで、エンドポイント ID 項目(OS、エンドポイントタイプ、またはベンダー)を設定します。



- エンドポイント ID エントリーを一括でインポートするには、**Mute Terminal Endpoint Identification 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。インポートテンプレートの形式は次のとおりです。



- 構成が完了したら、**Validate** をクリックします。**Validate** をクリックしない場合、構成はシステムのポーリング時間が終了するまで(10 分以内)有効になりません。

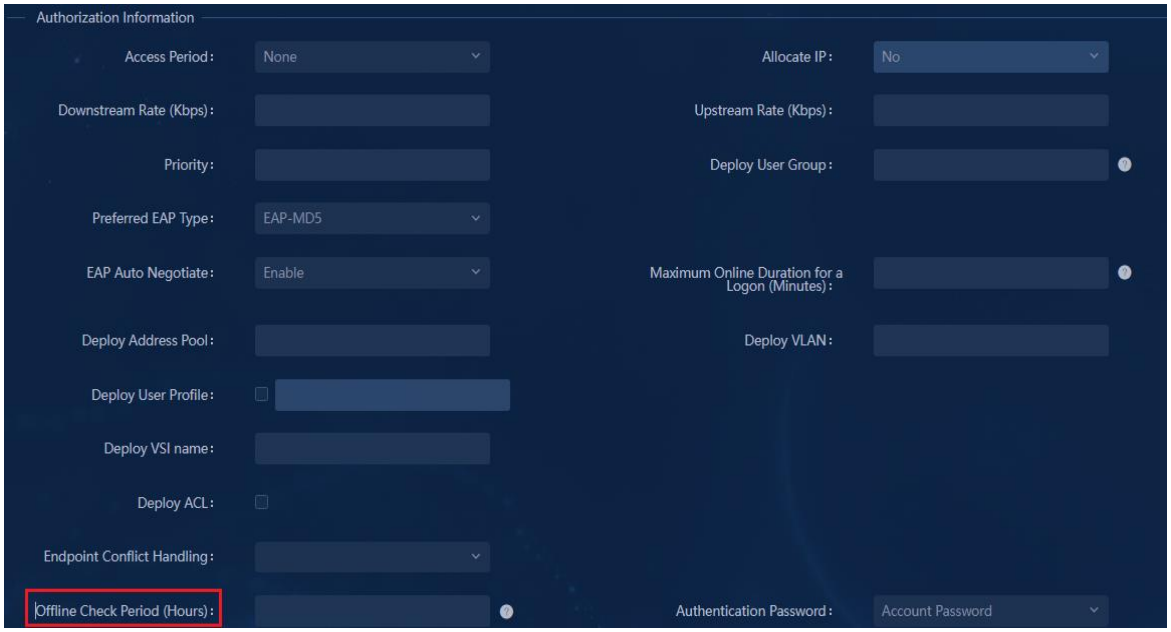


エンドポイントデバイスからのトラフィックによって認証がトリガーされます。システムは、エンドポイントのフィンガープリントをエンドポイント ID エントリーと照合します。一致するものが見つかった場合、システムは自動的にユーザーカウントを作成し、認証されたユーザーを対応するセキュリティグループに追加します。

ブロードバンド IoT エンドポイントを長期にわたってオンライン状態に維持する

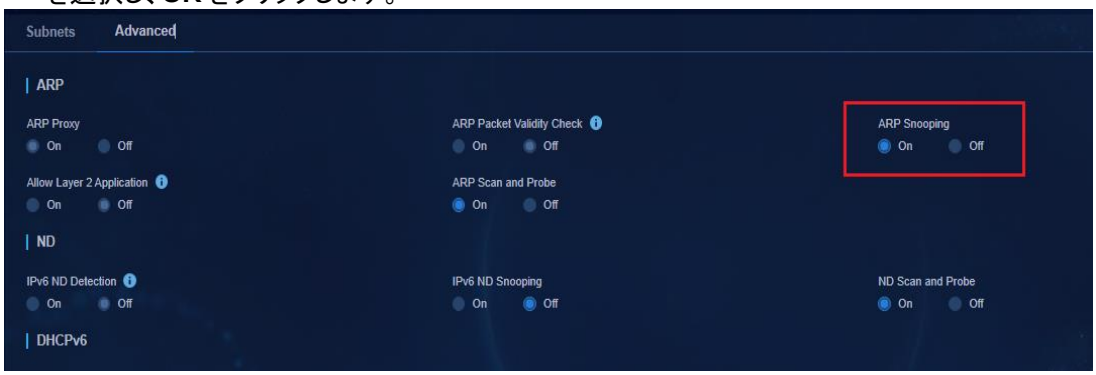
IoT エンドポイントを長期間オンライン状態に維持するには、ARP/ND スヌーピングとともにオフラインチェック期間(時間)を使用し、ARP/ND エントリーの経過時間の 30 秒前にキープアライブをトリガーします。ブロードバンド IoT エンドポイントを 1～2 回のオフラインチェック期間にわたってオンライン状態に維持するには、EIA のアクセスポリシーで **Offline Check Period(Hours)**を設定するだけです。設定は次のとおりです。

Automation > **User** > **Access Service** > **Access Policy** ページに移動し、Edit アイコンをクリックして、**Authorization Information** 領域の **Offline Check Period(Hours)**を変更します。推奨値は 24 時間です。



ブロードバンド IoT エンドポイントを常にオンライン状態に維持するには、次のいずれかの方法を選択します。

- 方法 1: オフラインチェック期間を 0 に設定し、オフラインチェックを無効にします。エンドポイントは長期間トラフィックがない状態でエージングしていません。
- 方法 2: オフラインチェック期間を 0 に設定することに加えて、SeerEngine キャンパスコントローラーで ARP スヌーピングをイネーブルにし、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します。この方法は、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できます。ARP スヌーピングをイネーブルにするには、次のようにします。
  a. **Automation** > **Campus Network** > **Private Network** > **Layer 2 Network Domain** ページに移動し、ターゲットレイヤー2 ネットワークドメインの **Edit** アイコンをクリックします。
  b. **Edit Layer 2 Network Domain** ページの **Advanced** タブで、**ARP Snooping** フィールドの **On** を選択し、**OK** をクリックします。



arp snooping enable コマンドがリーフデバイスに展開されます。

```
#
vsi vsi3
 description SDN_VSI_3
 gateway vsi-interface 3
 statistics enable
 arp snooping enable        //Command deployed by the controller.
 flooding disable all all-direction
```

```
 vxlan 3
 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、ARP エージングタイマーよりも長いオフラインチェック期間(3600 秒など)を参照します。

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

⚠ **警告!**

mac-authentication offline-detect mac-address xxxx-xxxx-xxxx timer xxxx check-arp-or-nd-snooping コマンドは、認証エンドポイントデバイスごとに使用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。このコマンドを使用せずに、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。

認証不要インターフェイスの設定

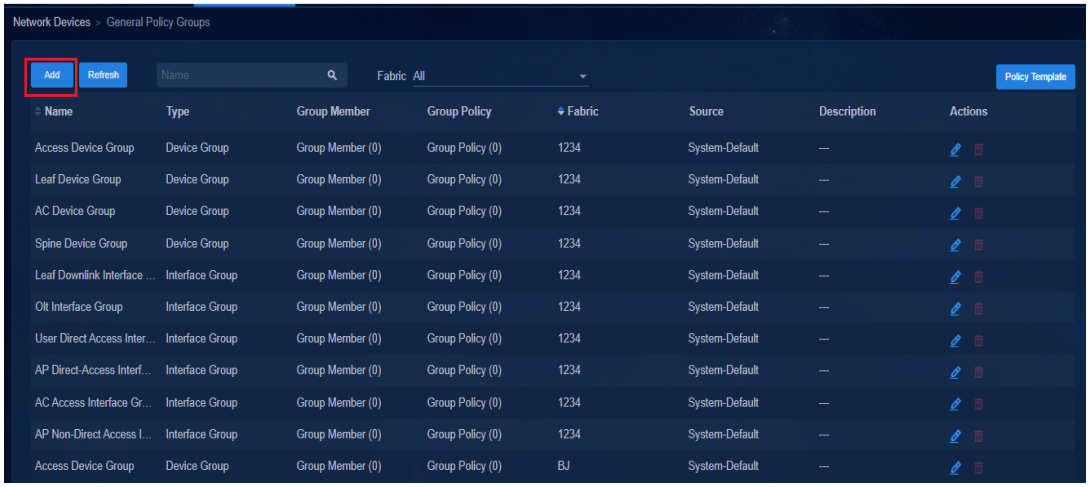
コントローラーには、認証不要のインターフェイスを設定できます。認証不要のインターフェイスからオンラインになったユーザーは、認証なしで set セキュリティグループに直接参加して、IP アドレスを取得し、セキュリティグループの対応するネットワークリソースにアクセスできます。

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。

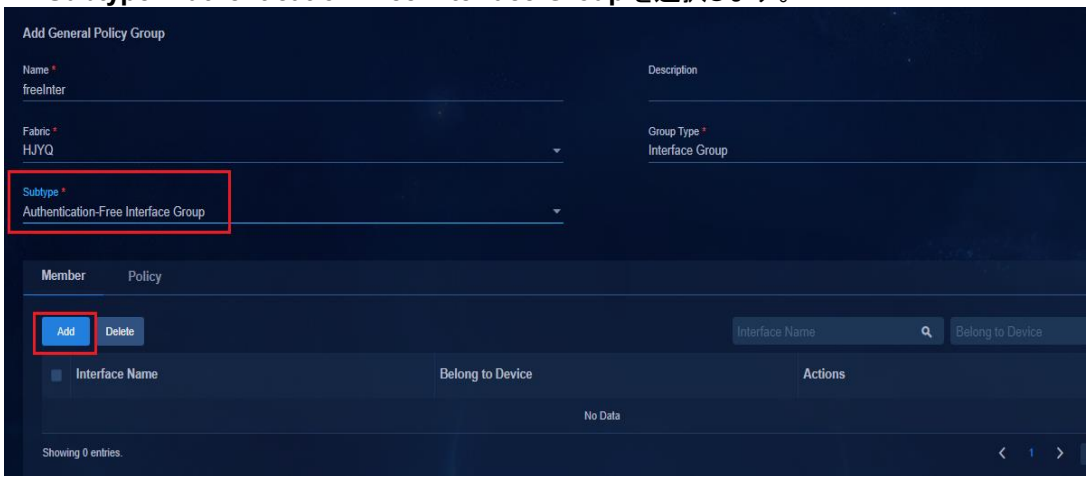
認証不要インターフェイスグループの追加

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手動で設定する必要があります。

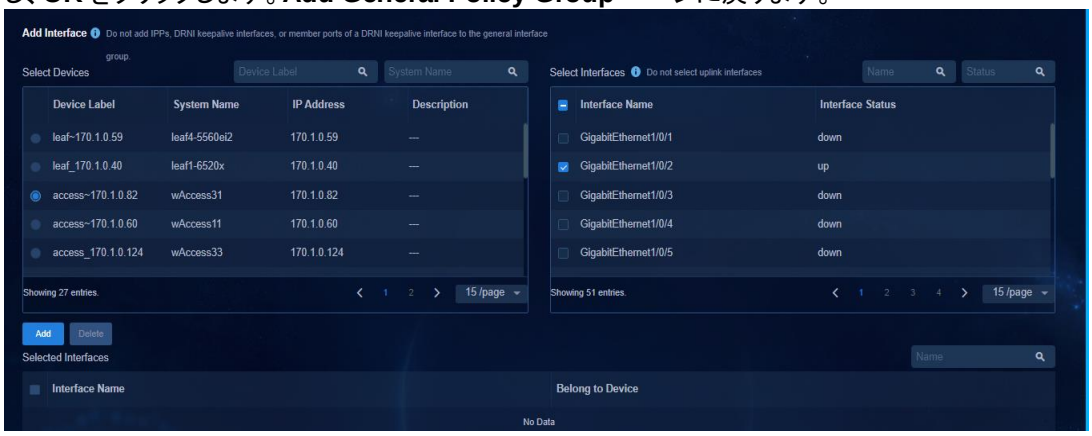
1. **Automation** > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Add** をクリックします。



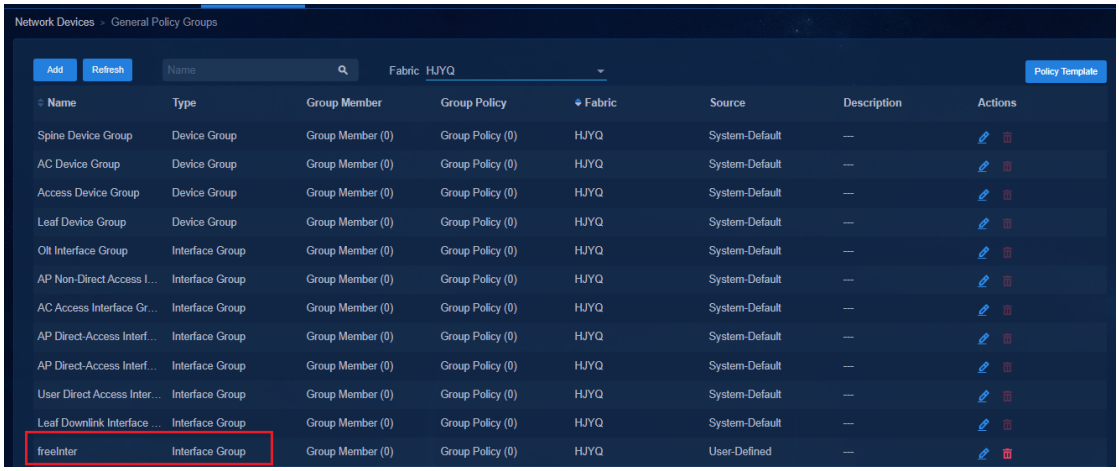
2. 次の図に示すように、認証不要のインターフェイスグループを作成し、グループのメンバーを選択します。
   - **Group Type**: **Interface Group** を選択します。
   - **Subtype**: **Authentication-Free Interface Group** を選択します。



3. **Add General Policy Group** ページの **Member** タブで、**Add** をクリックします。**Add Interface** ページで、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 Selected Interface リストに追加し、**OK** をクリックします。**Add General Policy Group** 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。**General Policy Groups** リストで、認証フリーインターフェイスグループを表示できます。



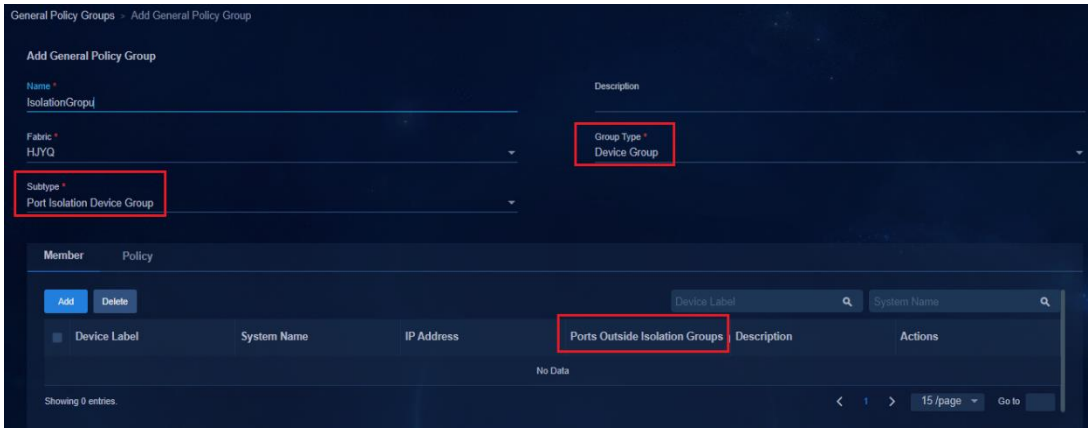
隔離ポートデバイスグループの追加

⚠ 警告!

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にある場合、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する必要があります。マルチレベルカスケードアクセスデバイスの場合、ポート隔離デバイスグループに追加する必要があるのは、認証不要インターフェイスグループ内にインターフェイスを持つアクセスデバイスだけです。

認証フリーインターフェイスがリーフデバイス上のインターフェイスである場合は、この作業を省略します。

1. **Automation** > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Add** をクリックします。
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。
3. **Member** タブで **Add** をクリックし、認証不要インターフェイスグループが設定されているアクセスデバイスを選択します。
   - **Ports Outside Isolation Groups**: アクセスデバイスをリーフ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。マルチレベルカスケードアクセスデバイスの場合、上位レベルのアクセスデバイスを下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は、隔離グループ外のポートに追加する必要があります。



4. 設定を展開してデバイスにアクセスします。

   隔離ポートグループをグローバルに展開します。

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

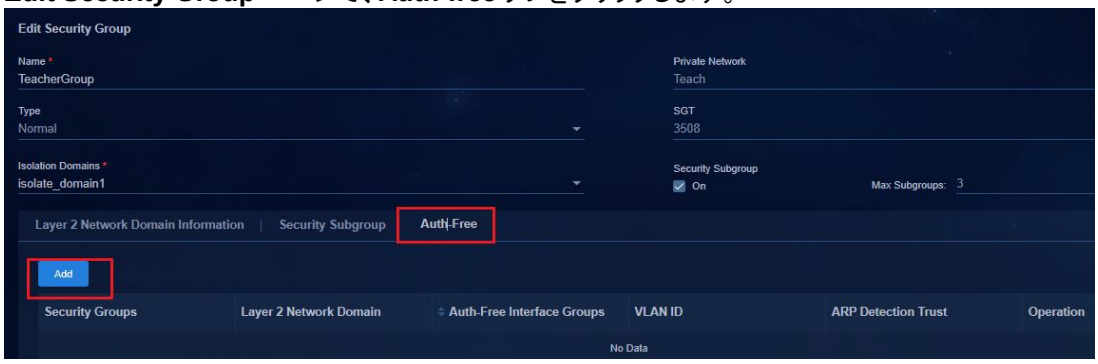
   アクセスデバイスのインターフェイスに対して port-isolate enable group 1 コマンドを発行します(隔離グループ外のポートを除く)。

   ```
   #
   interface GigabitEthernet1/0/1
    port link-mode bridge
    port access vlan 101
    port-isolate enable group 1
    stp edged-port
    poe enable
   #
   ```

認証不要のインターフェイスグループへのセキュリティグループのバインド

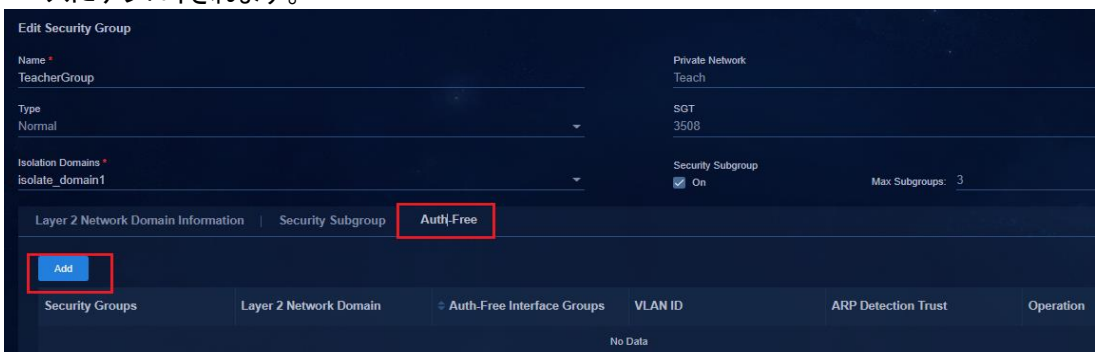
Automation > **Campus Network** > **Security Group** ページに移動し、セキュリティグループの対応する **Actions** カラムで **Edit** アイコンをクリックします。

1. **Edit Security Group** ページで、**Auth-free** タブをクリックします。



2. このページで **Auth-free Interface Groups** を選択します。

   - **ARP Detection Trust:** デフォルトでは有効になっています。このパラメーターを有効にすると、ARP 検出の信頼構成が、認証不要サービスによって発行されたイーサネットサービスインスタンスにデプロイされます。



デバイスに展開された設定

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。

- 認証不要インターフェイスグループのメンバーがアクセスデバイス上のインターフェイスである場合は、次のようにします。

  #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で、イーサネットサービスインスタンス 4051 を設定します。

```
#
interface Ten-GigabitEthernet1/2/0/13
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094

 port-security free-vlan 1 4051 4094
 #
 service-instance 4051
encapsulation s-vid 4051
 xconnect vsi vsi3
 arp detection trust
#
return
#
```

  アクセスデバイスの認証不要インターフェイスでスタティック VLAN を設定します。

```
interface GigabitEthernet1/0/49
 port access vlan 4051
 stp edged-port
#
```

- 認証不要インターフェイスグループのメンバーがリーフデバイス上のインターフェイスである場合は、次の手順を実行します。

  # リーフデバイスの認証不要インターフェイスで、イーサネットサービスインスタンス 4051 を設定します。

```
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 vsi3
  arp detection trust
#
return
#
```

ゲストがオンラインであるか、認証がオンラインで失敗しました

⚠ 警告!

- ゲストオンラインおよび認証失敗オンラインをサポートするのは、802.1X 認証だけです。
- ゲスト機能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。
- ゲストオンライン認証と MAC ポータル認証は相互に排他的です。

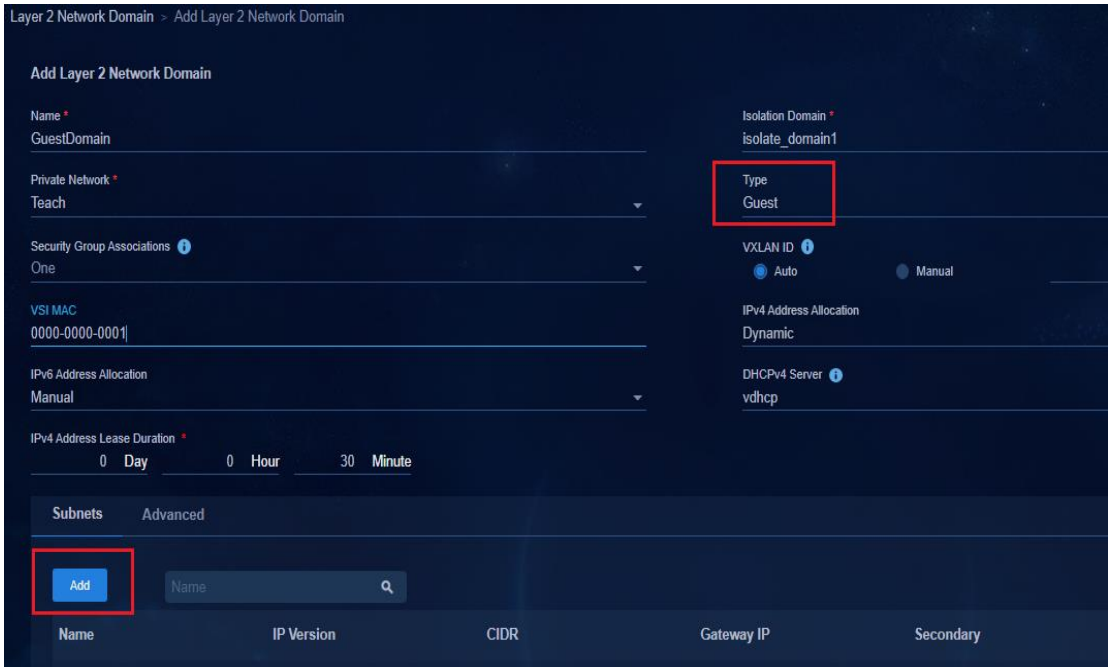
ゲストオンライン

Guest online を使用すると、認証サーバーを設定しなくても、ユーザーがオンラインになったときにゲストタイプのセキュリティグループにアクセスできます。

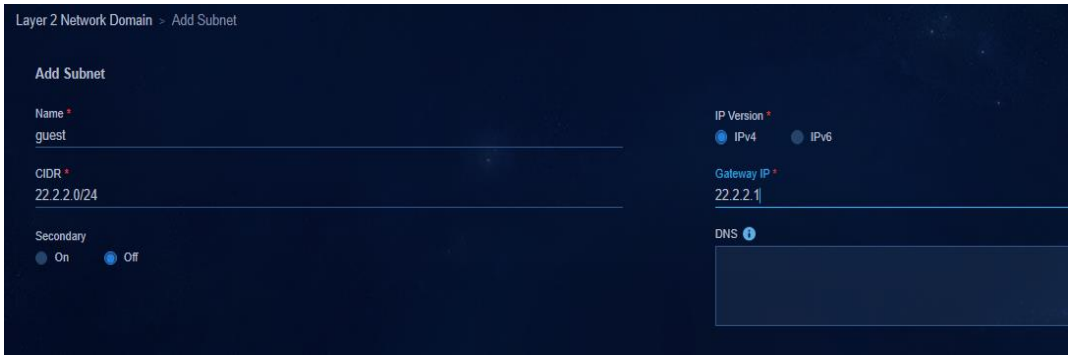
ゲストタイプのレイヤー2 ネットワークドメインの作成

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

1. **Add** をクリックして **Add Layer 2 Network Domain** ページを開き、次のパラメーターを設定します。
   - **Private Network**: プライベートネットワークを選択します。
   - **Type**: **Guest** を選択します。
   - **IPv4 Address Allocation**: **Dynamic** を選択します。
   - **DHCPv4 Server**: DHCPv4 サーバーを選択します。
   - **IPv4 Address Lease Duration**: デフォルトでは 30 分に設定されています。



2. **Subnets** タブで、**Add** をクリックします。**Add Subnet** ページで、**IP Version** を選択し、**CIDR** と **Gateway IP** を設定します。

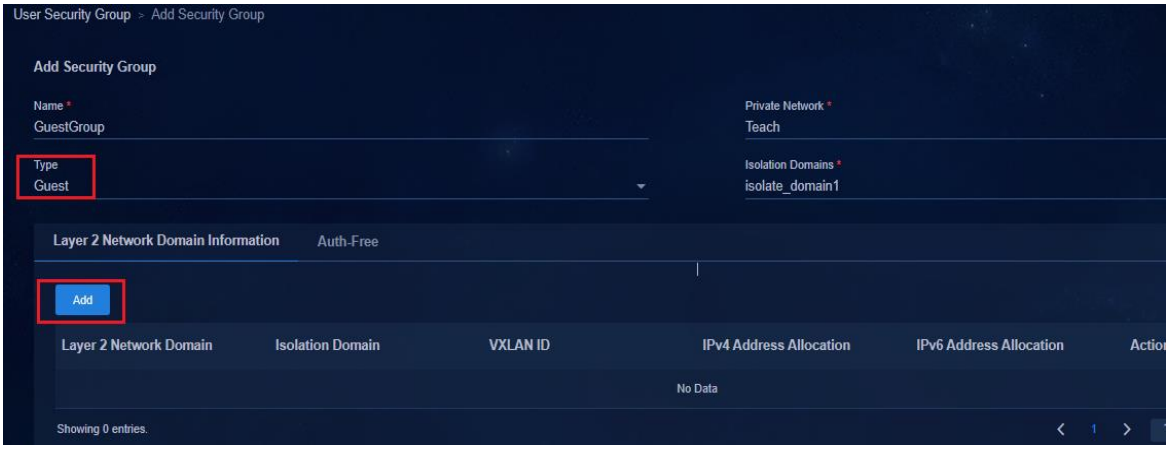


3. **OK** をクリックすると、**Add Layer 2 Network Domain** ページに戻ります。次に、**OK** をクリックします。

ゲストタイプのセキュリティグループを作成する

Automation > **Security Group** > **User Security Group** ページに移動し、**Add** をクリックして **Add Security Group** ページを開きます。

1 つの分離ドメインに対して 1 つのゲストタイプのセキュリティグループを構成します。分離ドメインに複数のファブリックが含まれる場合、ゲストタイプのセキュリティグループはすべてのファブリックで共有されます。**Type** に **Guest** を選択します。**Layer 2 Network Domain Information** タブをクリックし、**Add** をクリックします。**Add Layer 2 Network Domain** ページで、前に構成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



ポリシーテンプレートでのゲストアクセスのイネーブル化

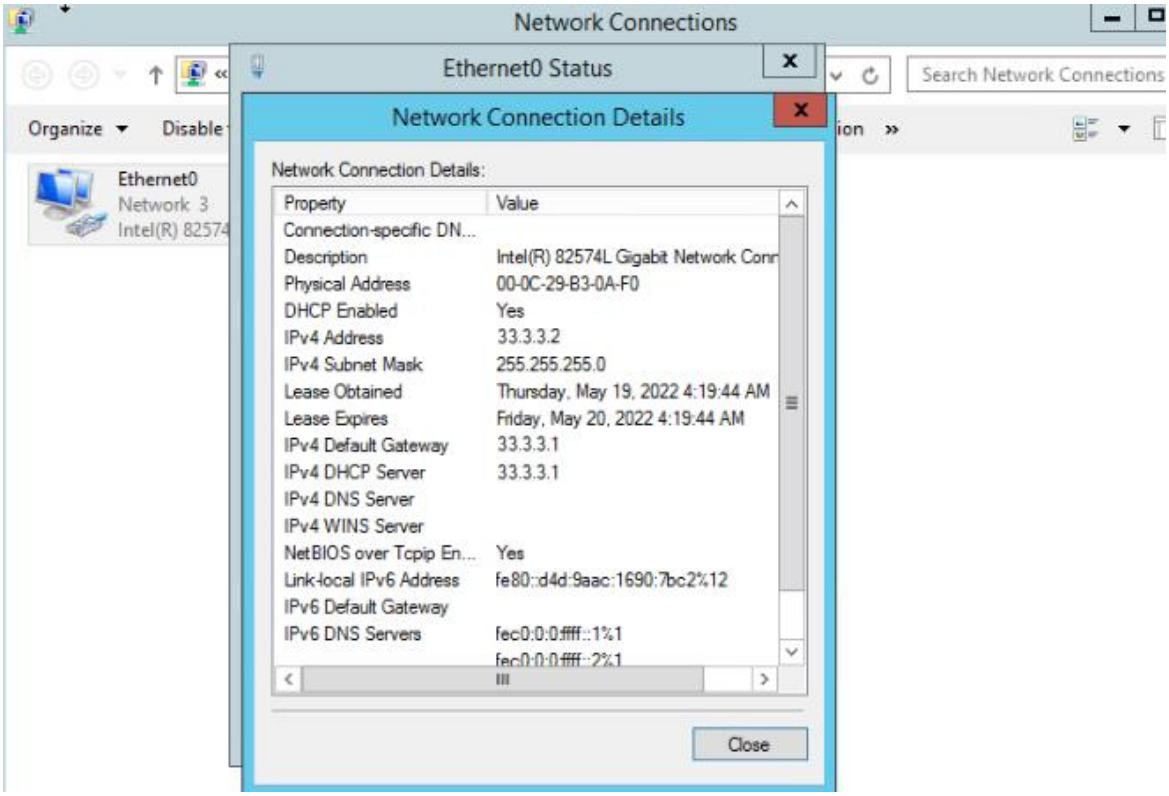
『Configuring an interface policy template of the 802.1X type』で **Guest Access** を有効にします。

この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適用すると、次の設定が展開されます。

```
[leaf105102-Ten-GigabitEthernet1/0/0/14]display this
#
interface Ten-GigabitEthernet1/0/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094
 stp tc-restriction
 mac-based ac
 dot1x
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x guest-vsi vsi10
 port-security free-vlan 1 4094
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
Return
```

オンラインになるユーザーの認証

ユーザーの PC がネットワークに接続されている場合、ユーザーは IP アドレスを取得して、ゲストタイプのセキュリティグループによって指定された特定のリソースにアクセスできます。



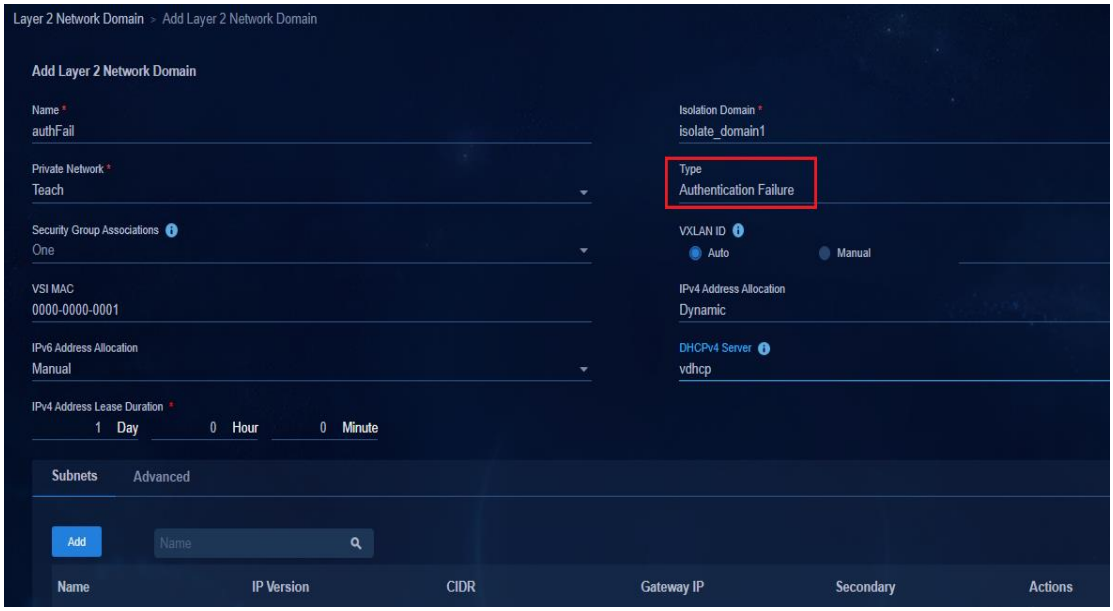
認証に失敗したユーザーがオンラインになることを許可する

このモードは、認証が失敗した場合に使用されます。ユーザーが 802.1X 認証に合格しなかった場合でも、ユーザーはオンラインになり、**Authentication Failure** タイプの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。

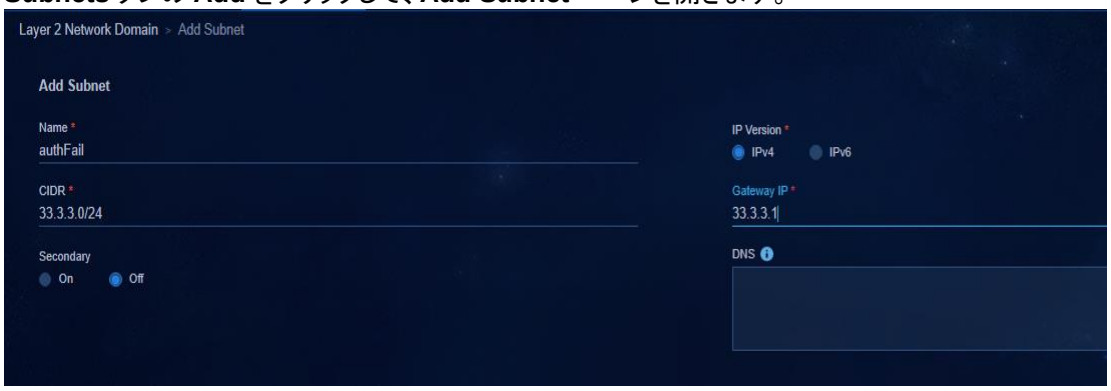
認証失敗レイヤー2 ネットワークドメインの作成

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

1. **Add** をクリックして **Add Layer 2 Network Domain** ページを開き、次のパラメーターを設定します。
   - **Private Network**: プライベートネットワークを選択します。
   - **Type**: **Authentication Failure** を選択します。
   - **IPv4 Address Allocation**: **Dynamic** を選択します。
   - **DHCPv4 Server**: DHCPv4 サーバーを選択します。
   - **IPv4 Address Lease Duration**: デフォルトでは 1 日に設定されています。



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

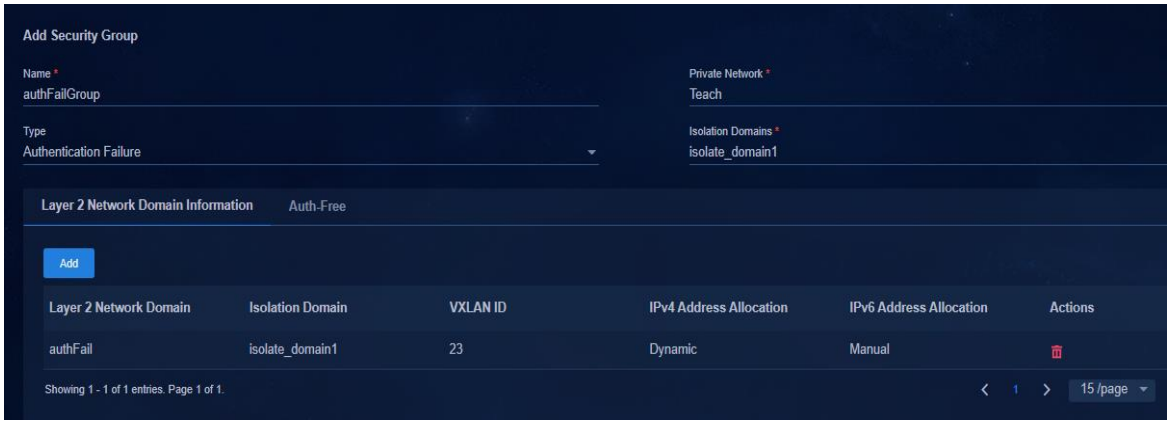


3. **OK** をクリックすると、**Add Layer 2 Network Domain** ページに戻ります。次に、**OK** をクリックします。

認証失敗セキュリティグループの作成

Automation > **Security Group** > **User Security Group** ページに移動し、**Add** をクリックして **Add Security Group** ページを開きます。

1 つの分離ドメインに対して 1 つの認証失敗セキュリティグループを構成します。分離ドメインに複数のファブリックが含まれる場合、認証失敗セキュリティグループはすべてのファブリックで共有されます。**Type** で **Authentication Failure** を選択します。**Layer 2 Network Domain Information** タブをクリックし、**Add** をクリックします。**Add Layer 2 Network Domain** ページで、前に構成した認証失敗レイヤー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での認証失敗時のアクセスの使用可能化

『Configuring an interface policy template of the 802.1X type』の **Access on Authentication Failure** を有効にする

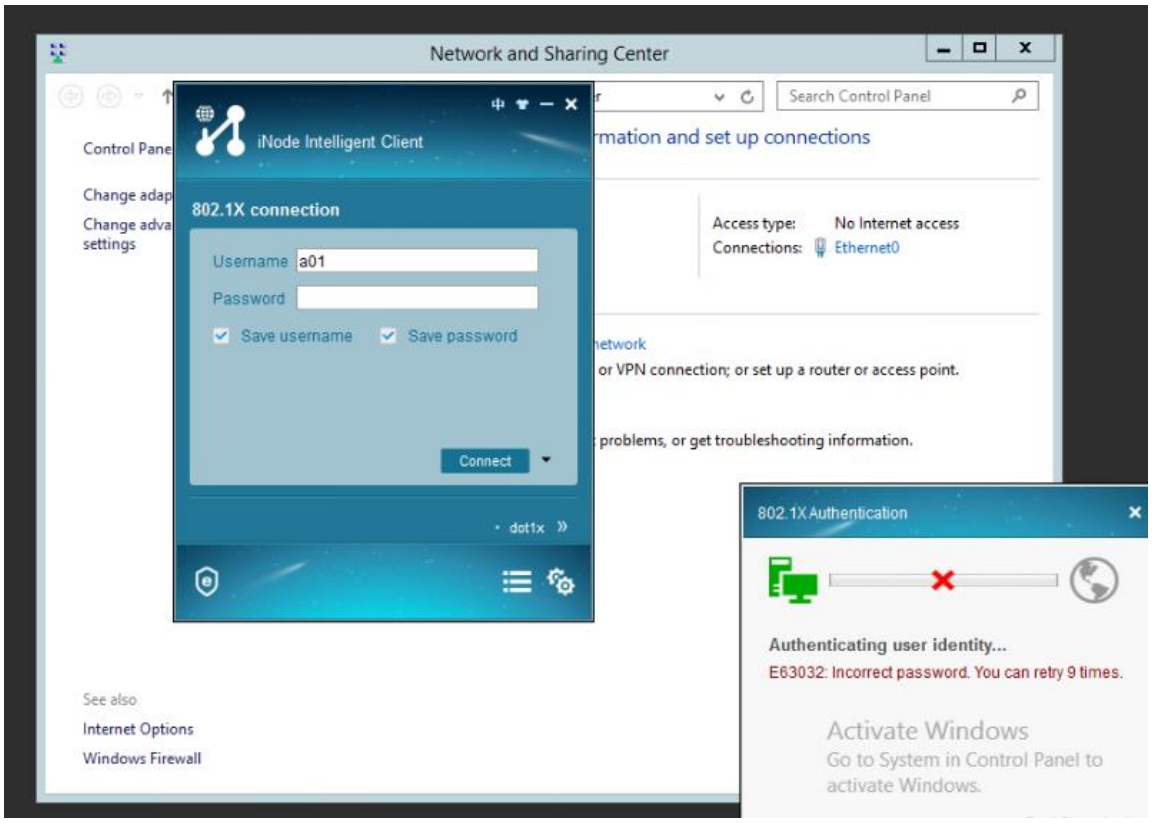
このポリシーテンプレートをリーフダウンリンクインターフェイスグループに適用すると、次の設定が展開されます。

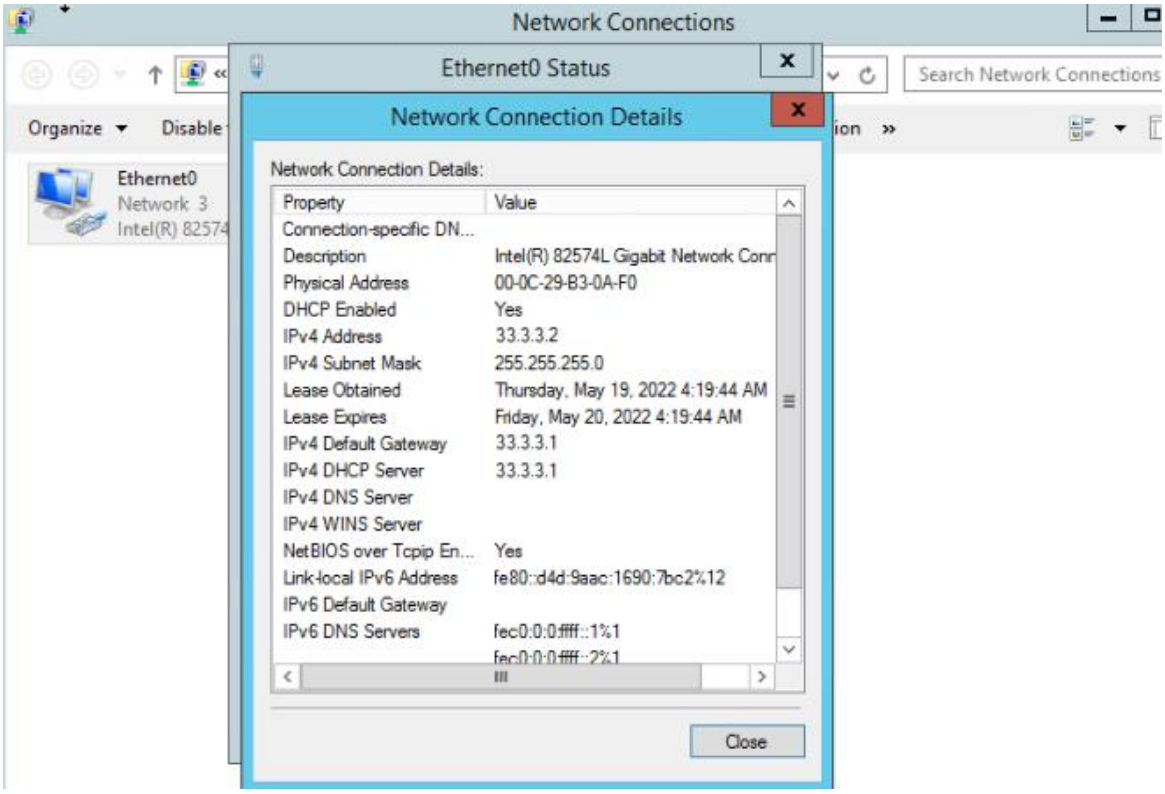
```
[leaf105102-Ten-GigabitEthernet1/0/0/14]display this
#
interface Ten-GigabitEthernet1/0/0/14
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094
 stp tc-restriction
 mac-based ac
 dot1x
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x guest-vsi vsi10
```

```
 dot1x auth-fail vsi vsi12
 dot1x critical vsi vsi11
 dot1x critical eapol
 port-security free-vlan 1 4094
 #
 service-instance 4094
  encapsulation s-vid 4094
  xconnect vsi vxlan4094
#
```

オンラインになるユーザーの認証

ユーザーの PC で 802.1X 認証に失敗した場合、ユーザーは認証失敗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。





ゲストサービス

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、アクセス権が制限されています。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現し、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。

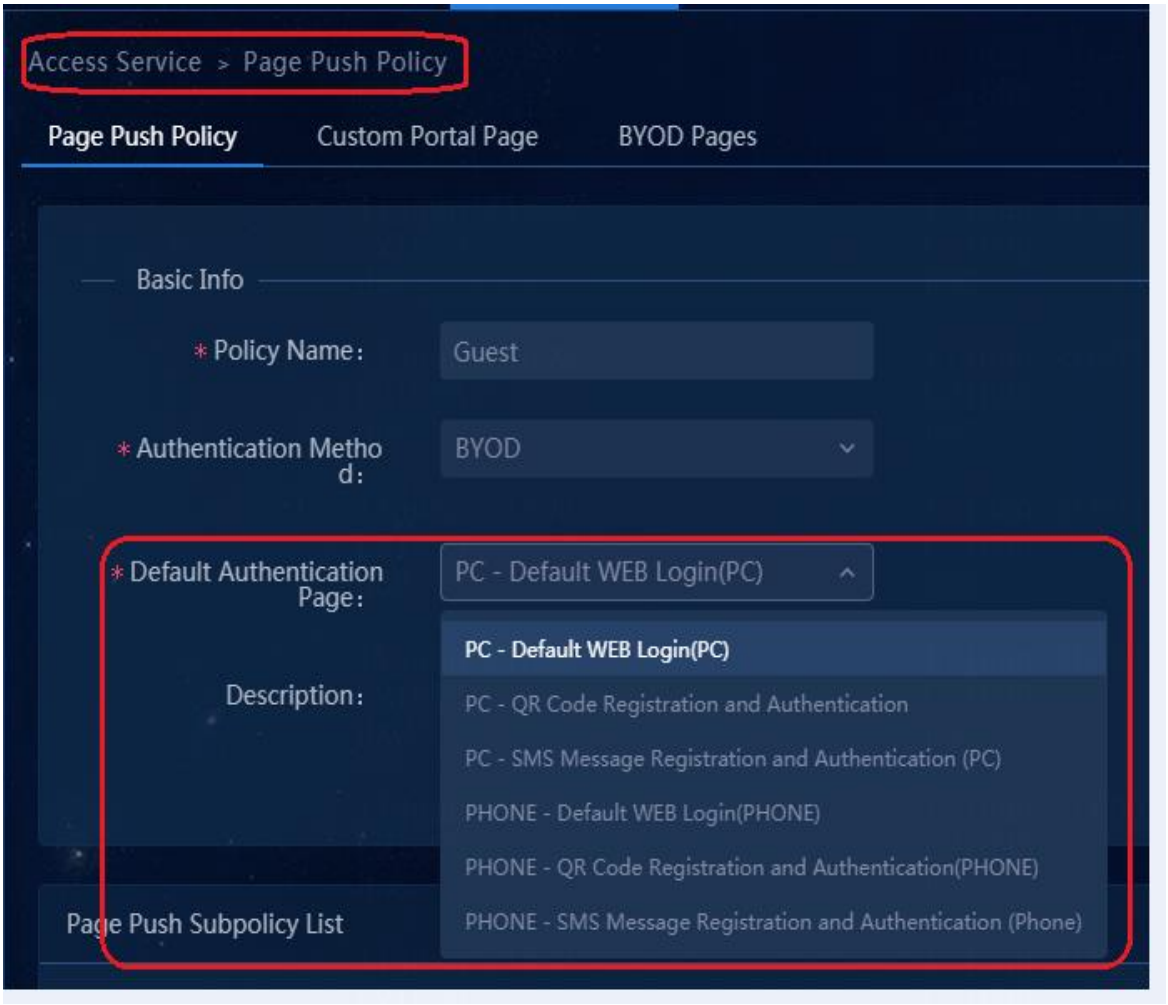
ゲストでは、次の図に示すように、次のページプッシュ方式を使用できます。

- PC の場合: デフォルトの WEB ログイン(PC)、QR コードの登録と認証(PC)、および SMS メッセージの登録と認証(PC)。
- 電話機の場合: デフォルトの WEB ログイン(電話機)、QR コード登録および認証(電話機)、および SMS メッセージ登録および認証(電話機)。

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。

ゲストユーザーが QR コードをスキャンしてログインすると、ゲストユーザーは管理者が設定した QR コードをスキャンしてログインし、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。



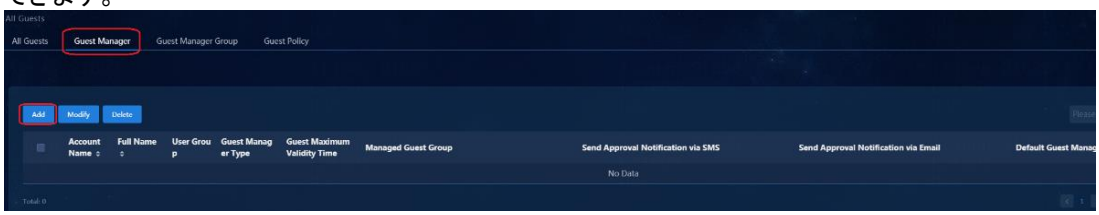
次の情報では、**PC - Default Web Login** 方式を紹介します。ゲストは **Guest Auto-Registration**.に設定されています。つまり、管理者が手動で承認しなくても、事前登録後にゲストは自動的にオンラインになります。

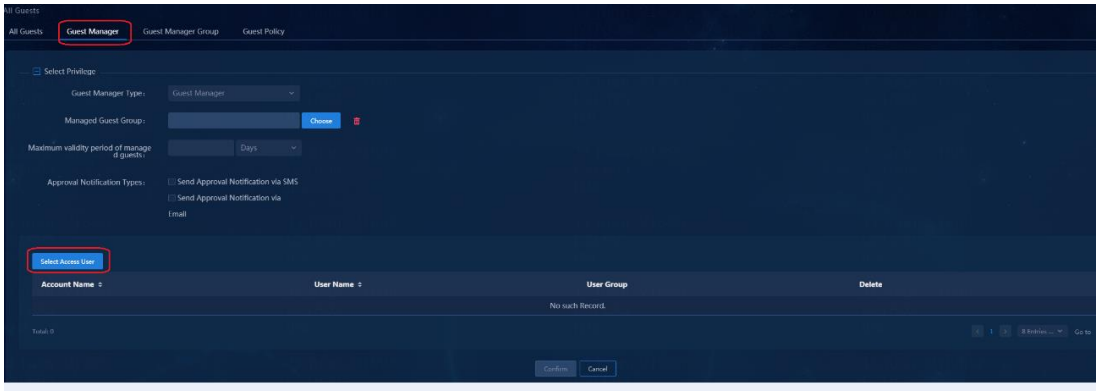
ゲスト管理の設定

ゲストマネージャーの設定

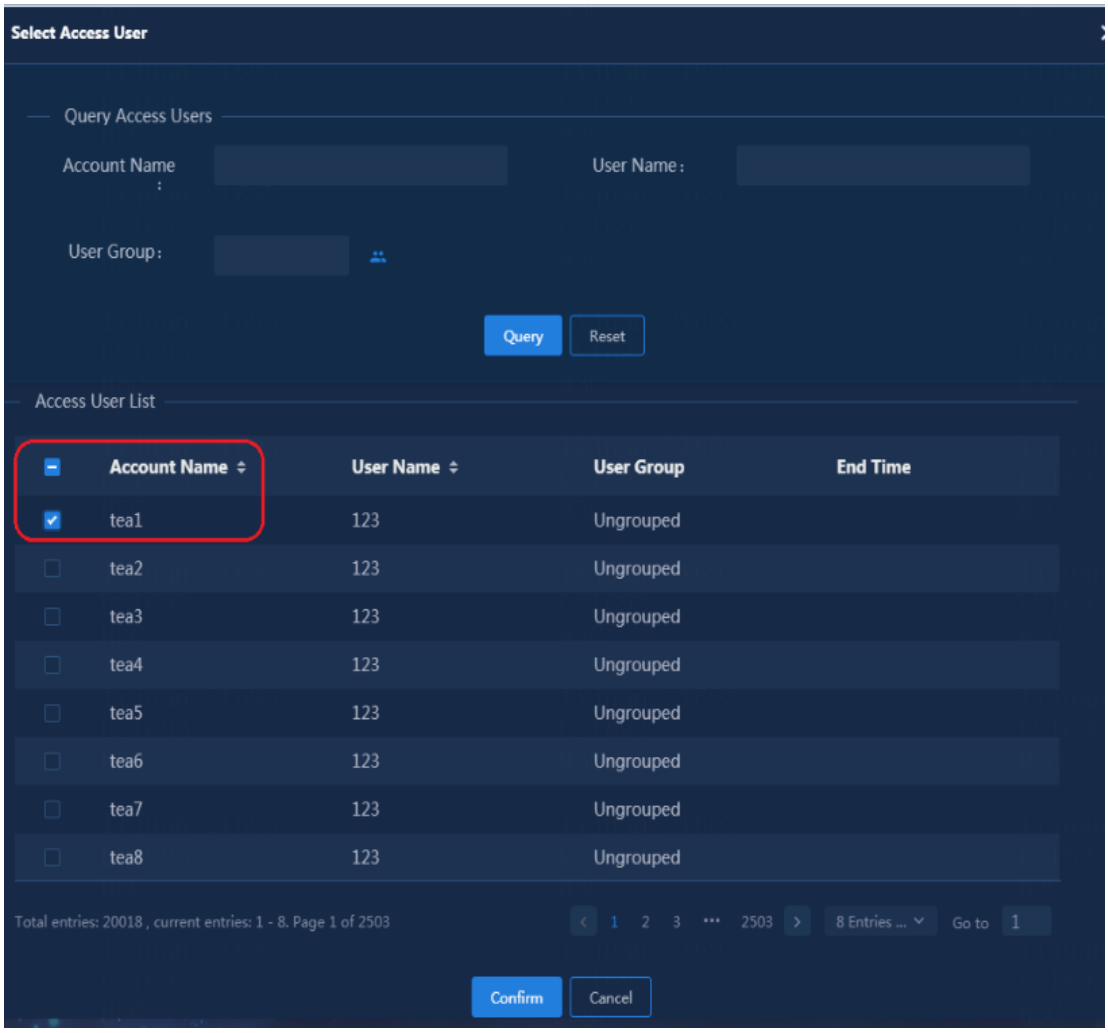
Automation > **User** > **Guest User** ページに移動し、**Guest Manager** タブをクリックします。

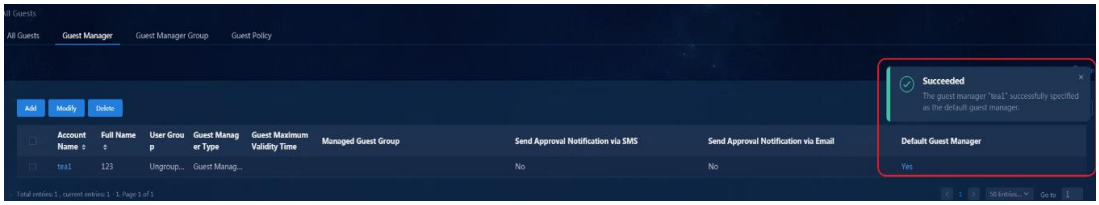
1. **Guest Manager** ページで、**Add** をクリックして、ゲストマネージャーを追加するためのページを開きます。**Select Access User** をクリックして、**Select Access User** ページを開きます。すべてのアクセスユーザー情報を表示できます。ゲストマネージャーは、アクセスユーザーから選択されます。1 つのゲストに 1 つのゲストマネージャーが必要です。デフォルトのゲストマネージャーを設定することもできます。





2. アクセスユーザーを選択し、**OK** をクリックします。**Add Guest Manager** ページに戻ります。**OK** をクリックすると、**Guest Manager** ページに戻ります。ゲストがゲストマネージャーリストに表示されます。**Default Guest Manager** 列で **Yes** または **No** をクリックして、デフォルトのゲストマネージャー機能を構成できます。**Yes** の値は、アクセスユーザーがデフォルトのゲストマネージャーであることを



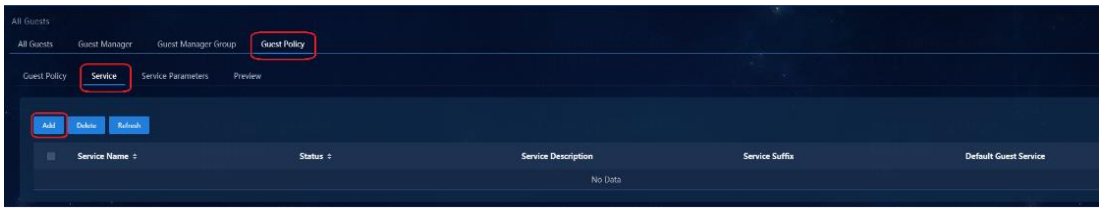


ゲストサービスの設定

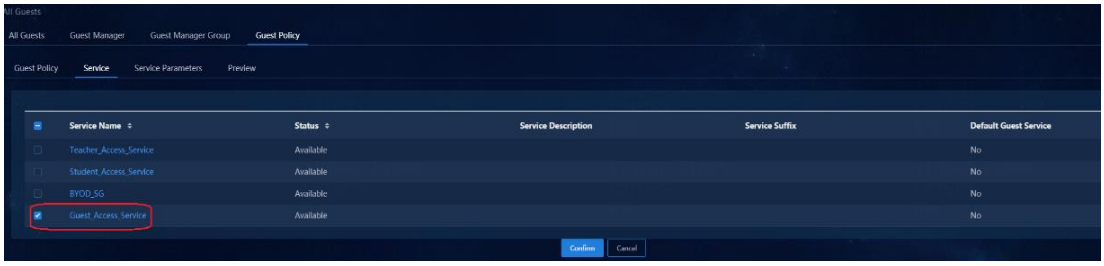
ストサービスを追加する前に、レイヤー2 ネットワークドメイン、セキュリティグループ、アクセスポリシー、およびゲストサービスに対応するアクセスサービスを作成する必要があります。設定の詳細については、『Creating a Layer 2 network domain』、『Configuring security group』、『Configuring access policies』、および『Configuring access services』を参照してください。たとえば、**Guest Security Group** を設定し、対応するアクセスポリシーを設定してから、**Guest Security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

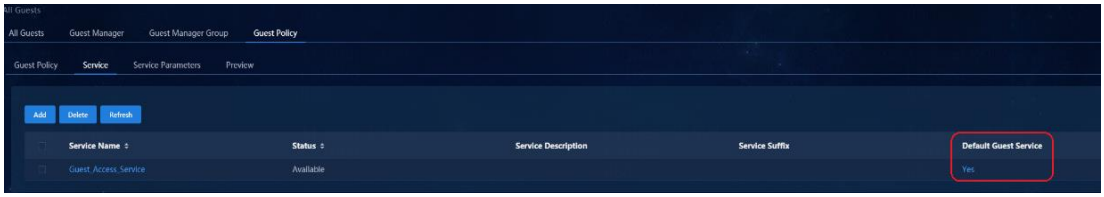
ゲストサービスを設定するには、次の手順を実行します。

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. Guest ページで、1 つ以上のゲストサービスを選択し、**OK** をクリックします。開いたページで、**Back** をクリックして **Service** ページに戻ります。**Default Guest Service** 列で、**Yes** または **No** をクリックしてデフォルトゲストサービスを構成します。ゲストサービスリストにデフォルトゲストサービスが存在する必要があることに注意してください。

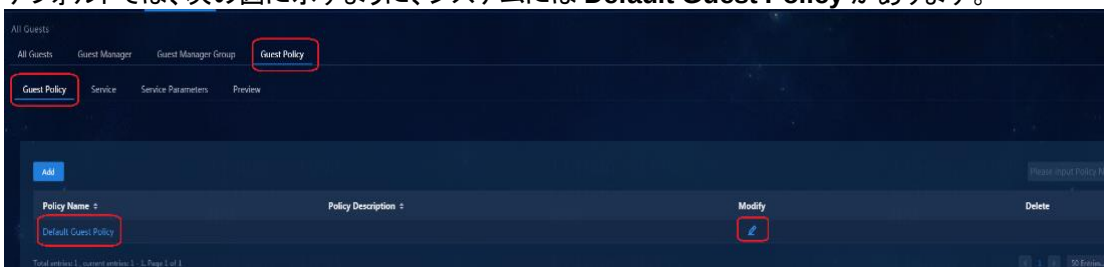




ゲストポリシーの設定

Automation > **User** > **Guest User** > **Guest Policy** > **Guest Policy** ページに移動します。

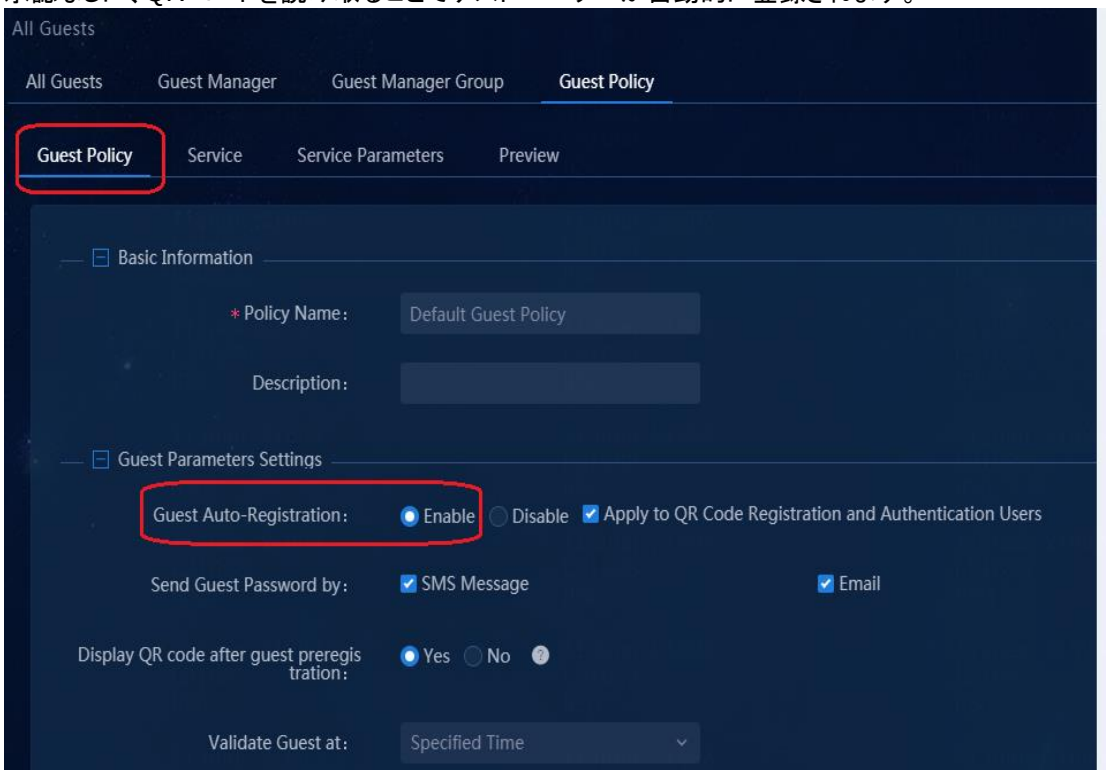
1. デフォルトでは、次の図に示すように、システムには **Default Guest Policy** があります。



2. **Edit** アイコンをクリックして、ポリシーを変更します。

Guest Auto-Registration を **Enable** に設定します。これは、ゲストユーザーが事前登録の完了後に自動的にオンラインになることを示します。この機能が無効になっている場合、ゲストユーザーはゲストマネージャーの承認後にのみオンラインになることができます。

Guest Auto-Registration を **Enable** に設定した後、**Apply to QR Code Registration and Authentication Users** チェックボックスを選択します。この場合、『Configuring a page push policy』で **QR Code Registration and Authentication** が設定されていると、ゲストマネージャーの承認なしに、QR コードを読み取ることでゲストユーザーが自動的に登録されます。



3. **OK** をクリックして設定を完了します。

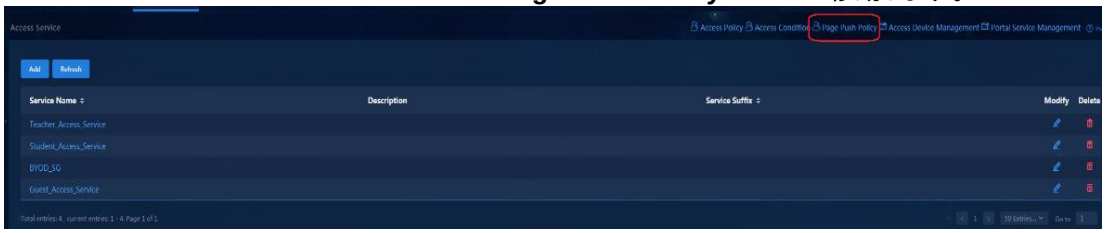
ゲストサービスパラメーターの設定

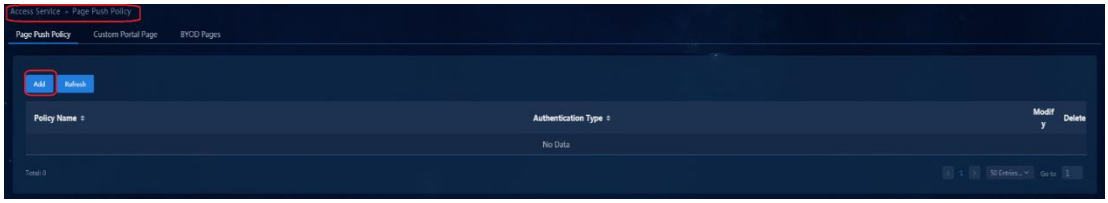
Automation > **User** > **Guest User** > **Guest Policy** > **Service Parameters** ページに移動します。

デフォルト設定を使用するか、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。詳細については、『Guest online』を参照してください。

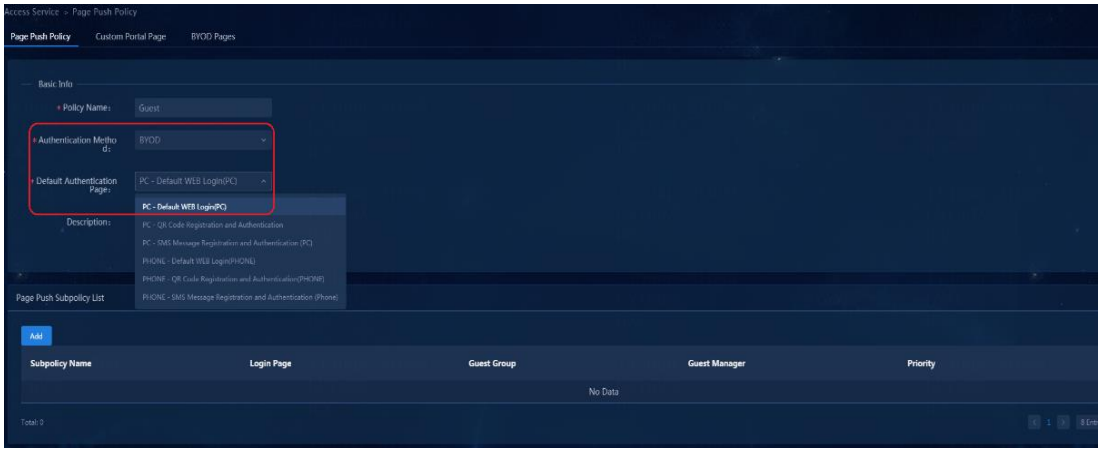
ページプッシュポリシーの設定

1. **Automation** > **User** > **Access Service** > **Page Push Policy** ページに移動します。





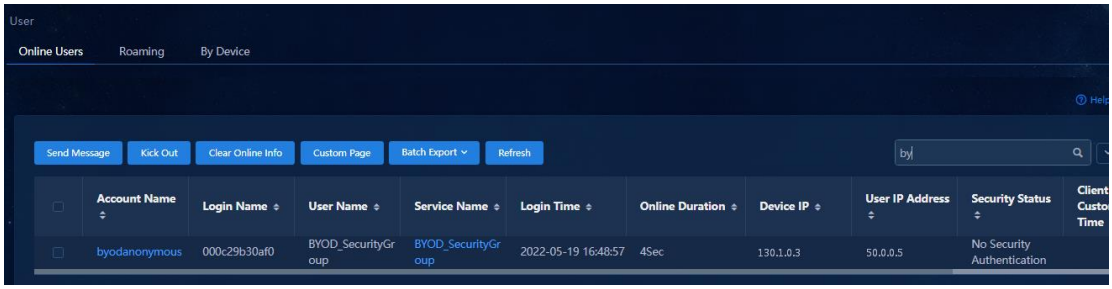
2. **Add** をクリックし、ポップアップページで次のパラメーターを設定します。
   - **Authentication Method**: **BYOD** を選択します。
   - **Default Authentication Page**:デフォルトでは **PC-Default WEB Login(PC)**で、Web ページを介したログインを示します。必要に応じて認証方法を設定できます。
3. 設定後、**OK** をクリックして構成を保存します。**Page Push Policy List** で新しいプッシュポリシーを表示できます。



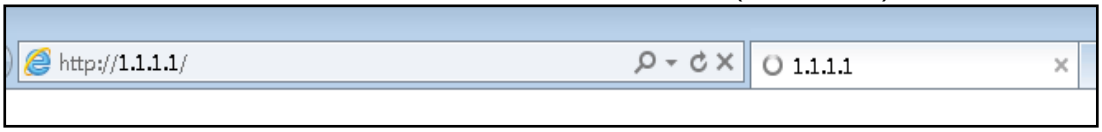
ゲストオンライン

ユーザー認証とアクセス

1. 認証デバイスポートが起動すると、MAC 認証がトリガーされます。ゲストは匿名アカウント(**byodanonymous** という名前)を使用してオンラインになります。ゲストは、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 IP アドレスを取得します。匿名アカウントは、**Monitor** > **Monitor List** > **User** > **Online Users** ページで確認できます。

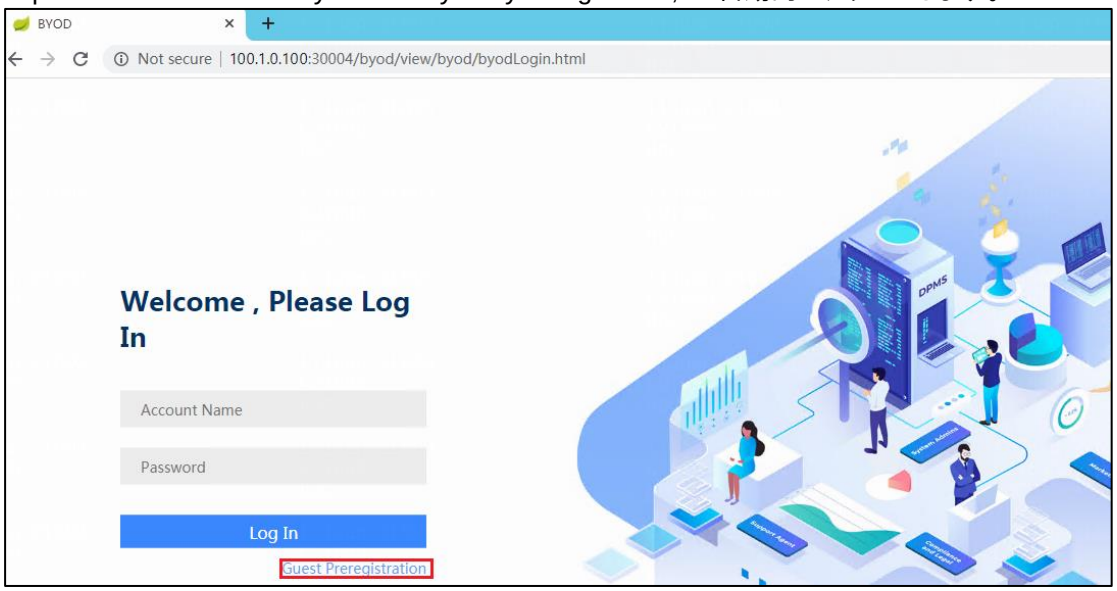


2. クライアントで Web ページを開いた後、1.1.1.1 などの IP アドレス(任意の URL)を入力します。



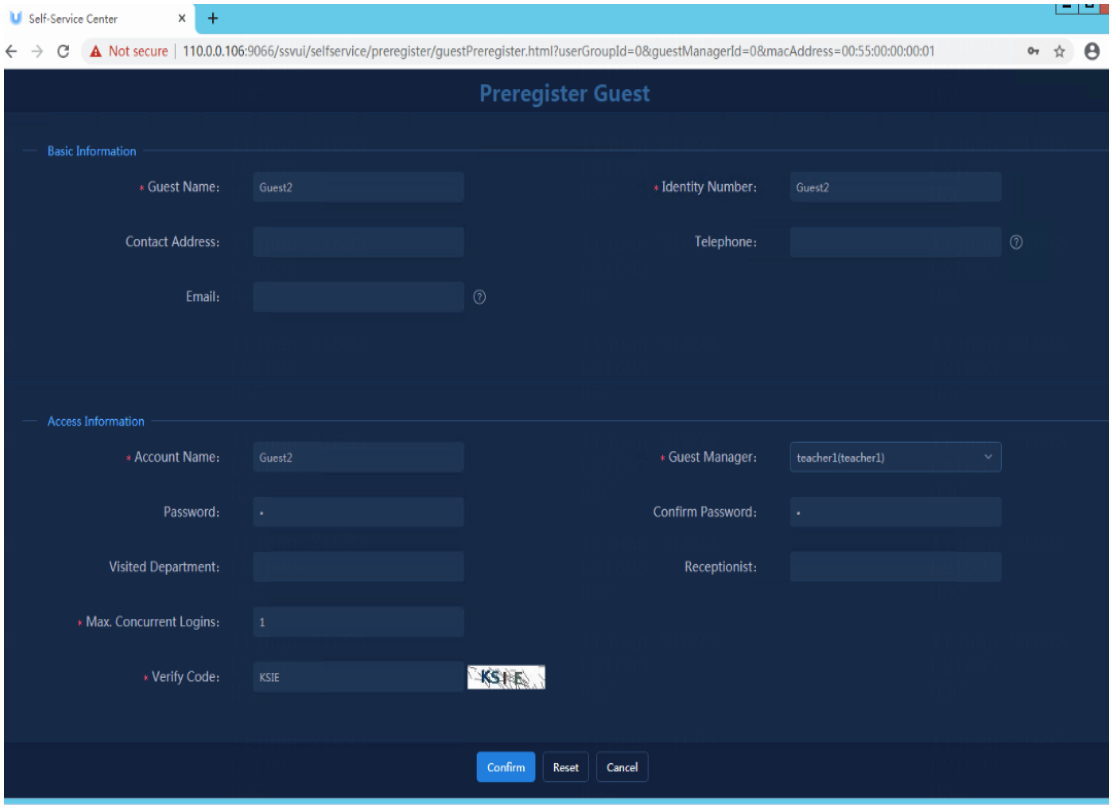
既定の Web ページ

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、次の図に示すように、BYOD のデフォルトページである http://100.1.0.100:30004/byod/view/byod/byodLogin.html，に自動的にアクセスします。

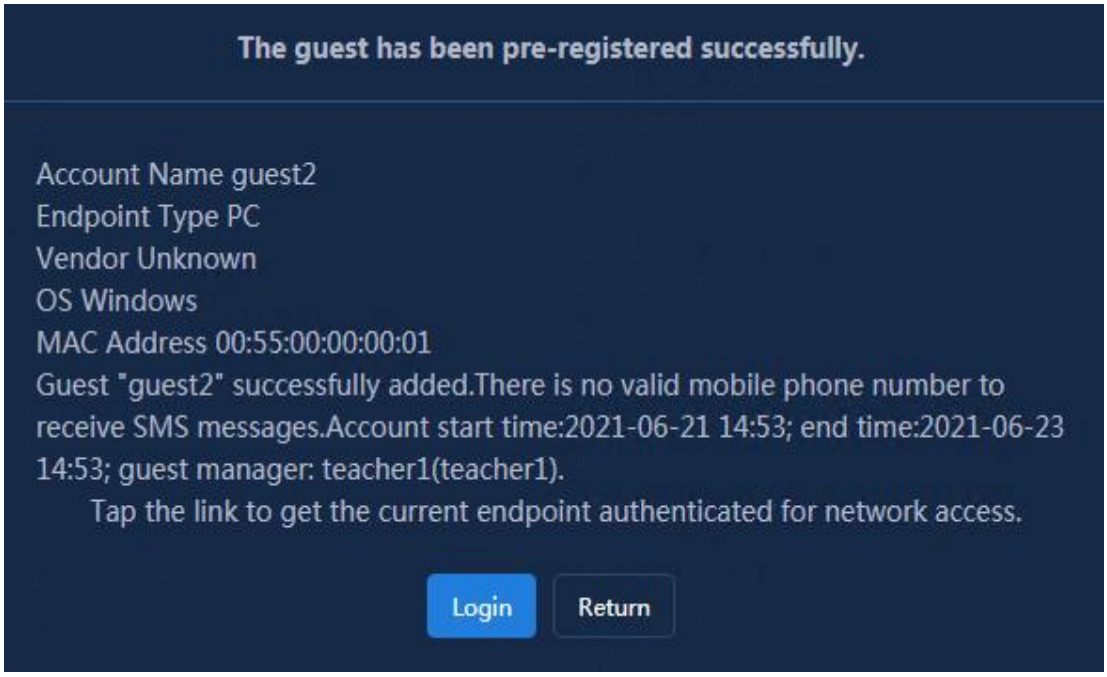


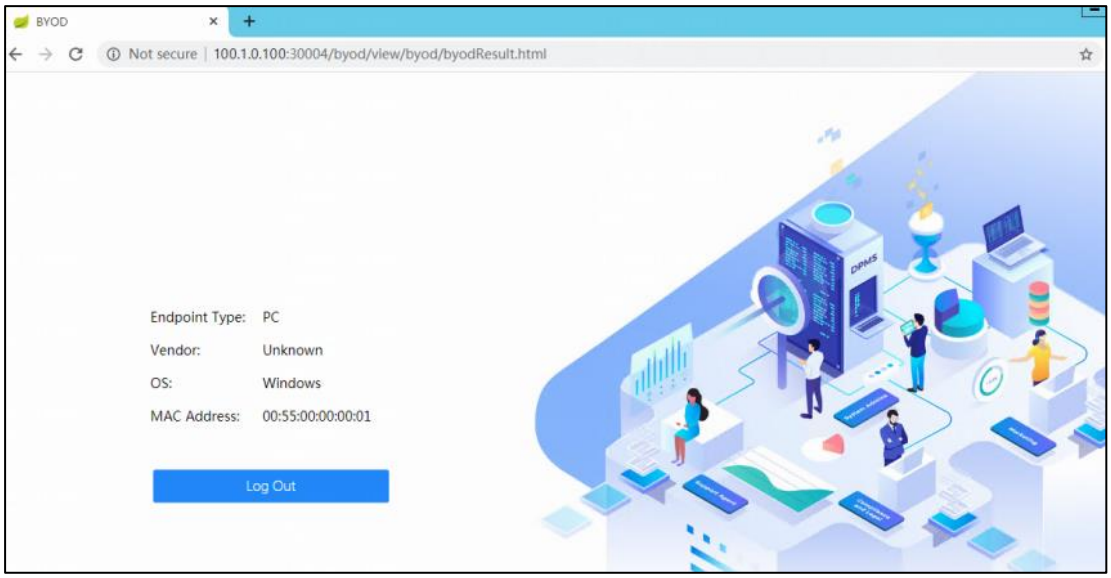
2. **Guest Preregistration** をクリックして次のページを開き、**Account Name**、**Identity Number**、**Verify Code**、および **Guest Manager** など、*印の付いた必須フィールドに入力します。**OK** をクリックして事前登録を完了します。

ゲストマネージャーは、前に設定したデフォルトのマネージャーです。パスワードが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。

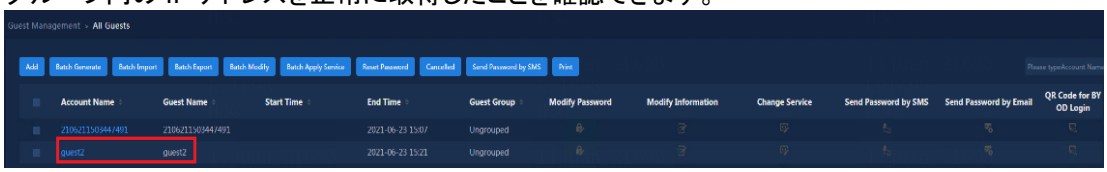


3. 登録に成功すると、登録結果の情報が表示されます。Login をクリックして直接ログインし、**Back** をクリックして BYOD ログインページに移動します。登録済アカウントおよびパスワード(**fa1/123456**)を入力してログインすることもできます。

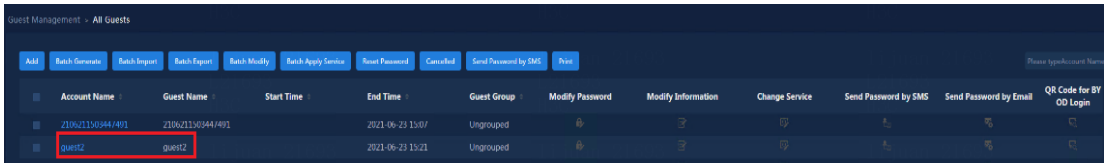




4. **Monitor** > **Monitor List** > **User** > **Online Users** ページに移動します。ゲストがゲストセキュリティグループ内の IP アドレスを正常に取得したことを確認できます。

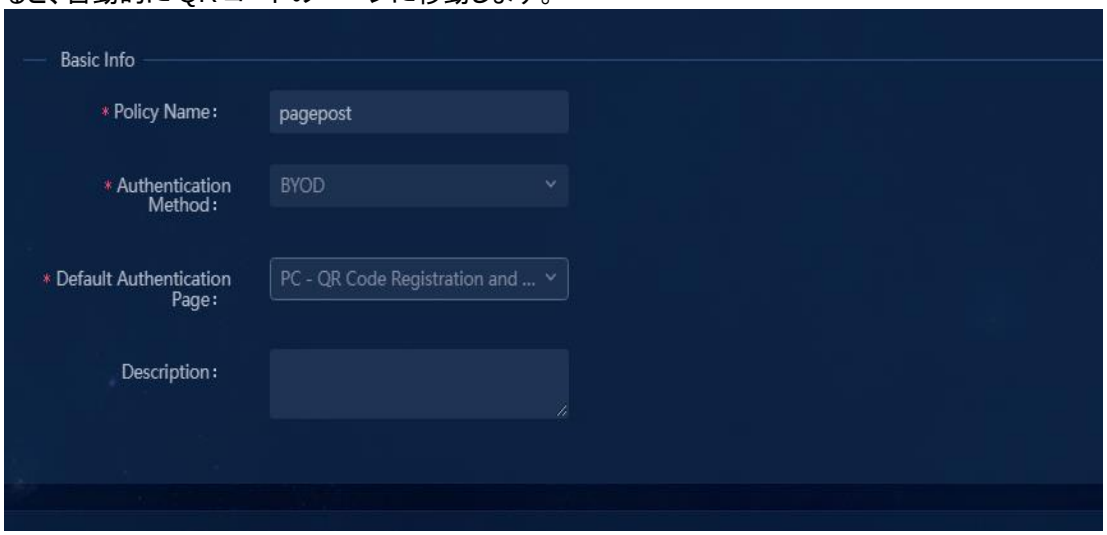


5. **Automation** > **User** > **Guest User** > **All Guests** ページにナビゲートします。新しく登録されたゲストユーザーが表示されます。アカウント名をクリックして、登録されたゲストユーザーの詳細を表示します。

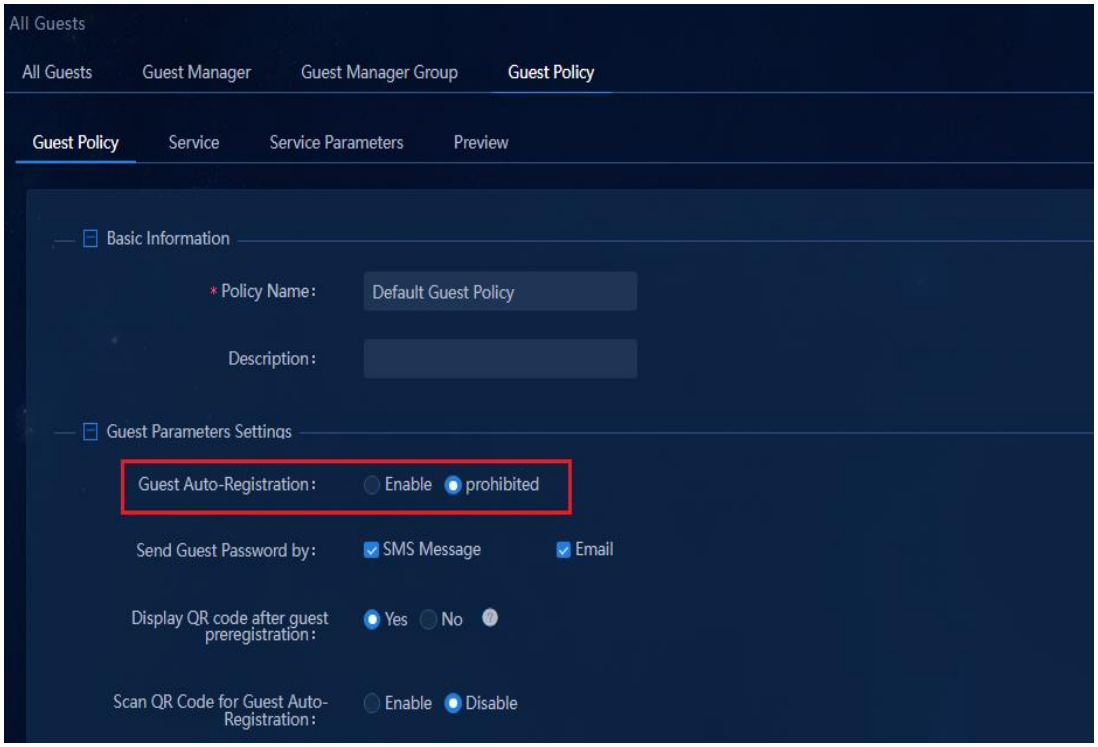


QR コード登録認証

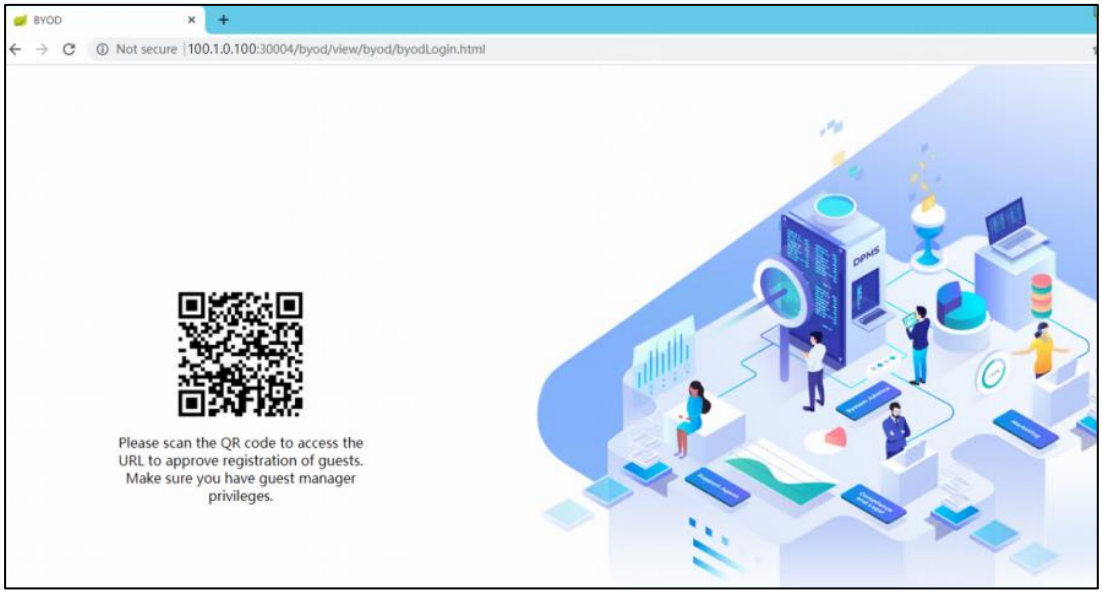
1. 『Configuring a page push policy』で **PC - QR Code Registration and Authentication** を選択すると、自動的に QR コードのページに移動します。



2. 『Configuring a guest policy』の **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ーによって承認される必要があります。

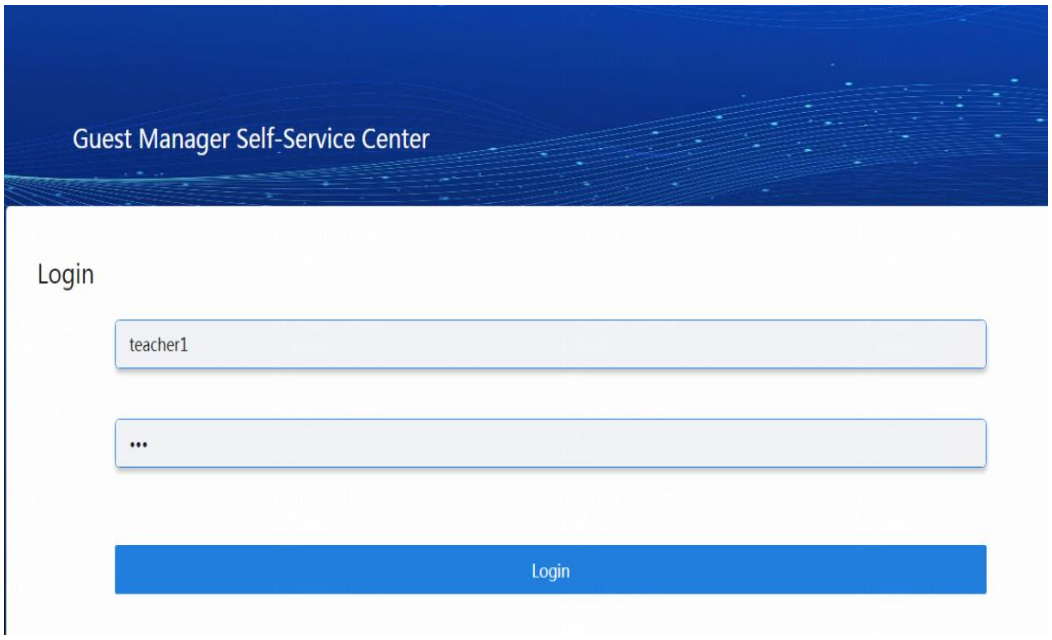


3. クライアント PC 認証ポートが起動し、BYOD セキュリティグループにアクセスしたら、クライアント PC の Google Chrome で任意の IP アドレスを入力します。次の図に示すように、QR コードページが開きます。

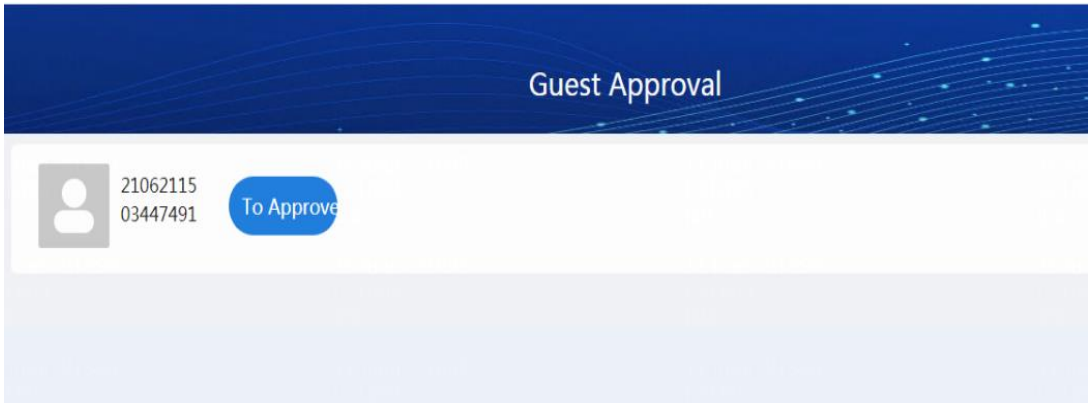


4. ゲストマネージャーは、このゲストの PC 上の QR コードを電話でスキャンできます。**Continue** をクリックして Web にアクセスします。

   電話機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 PC に手動で入力し、**Enter** キーを押します。次のページが開きます。ゲストマネージャーカウントを使用してログインします。

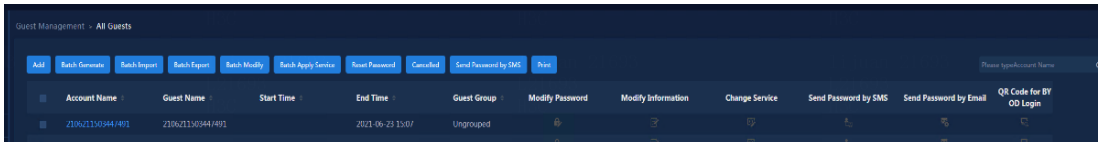


5. ログイン後、次のページが開きます。次に示すアカウントは、ゲストに与えられたアカウントです。ゲストマネージャーは **To Approve** をクリックします。



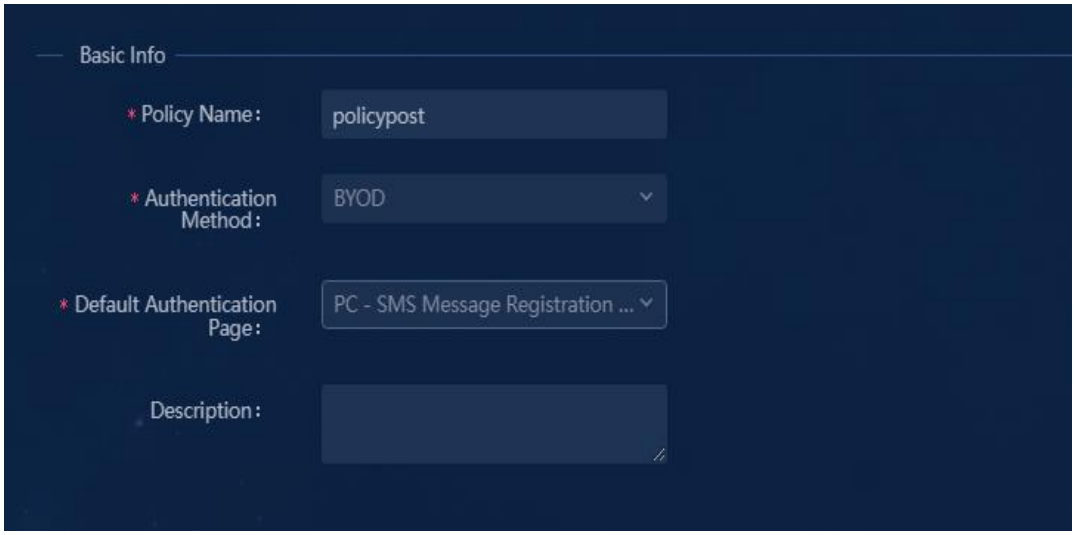
6. 承認ページが開いたら、**Accept** をクリックしてゲストアカウントを登録します。ユーザーの Web ページがジャンプして、登録が成功したことを示すページが表示されます。

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 User** > **All Guests** ページに移動します。ユーザーがゲストアクセスグループにログインし、**Guest Access Group** 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。



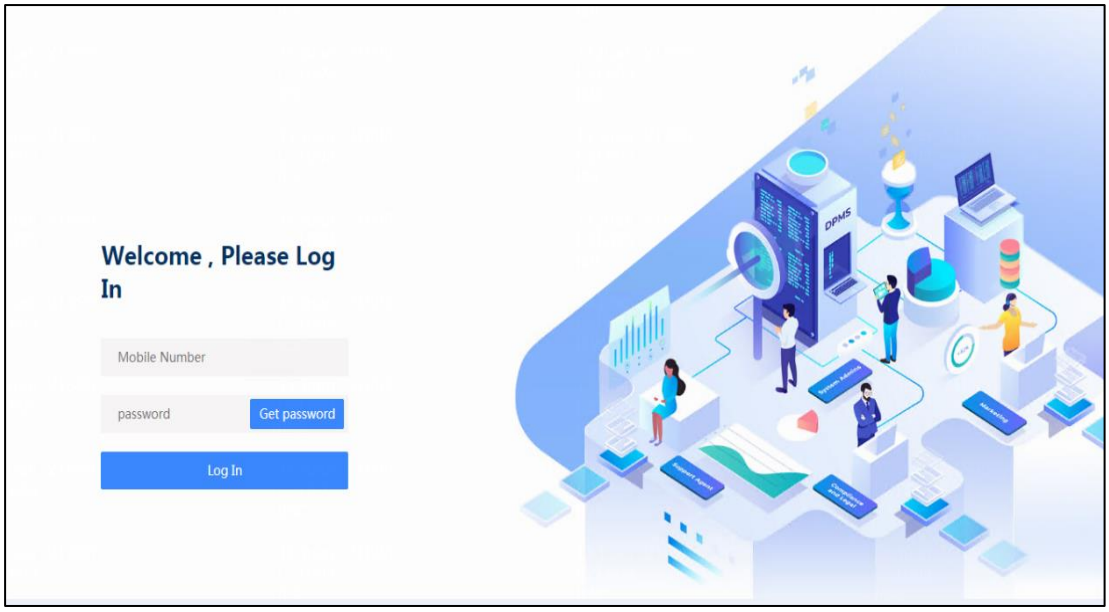
ショートメッセージ登録認証画面

1. 『Configuring a page push policy』で **PC - SMS Message Registration and Authentication** を選択すると、ユーザーの PC は自動的にデフォルトの SMS ページにジャンプします。



2. クライアント PC 認証ポートが起動し、BYOD アクセスグループに参加したら、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。次のページが開きます。

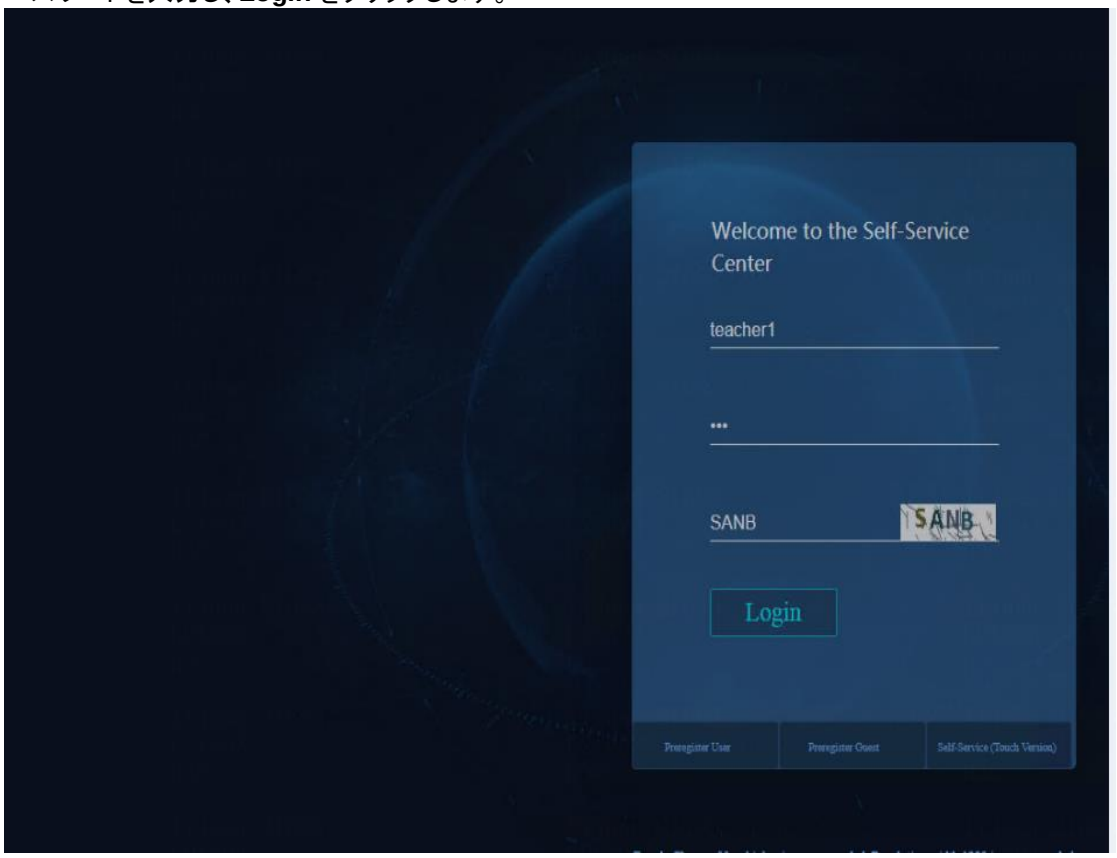
   対応する SMS モデムまたは SMS ゲートウェイがある場合は、電話番号を入力し、パスワードを取得してログインできます。



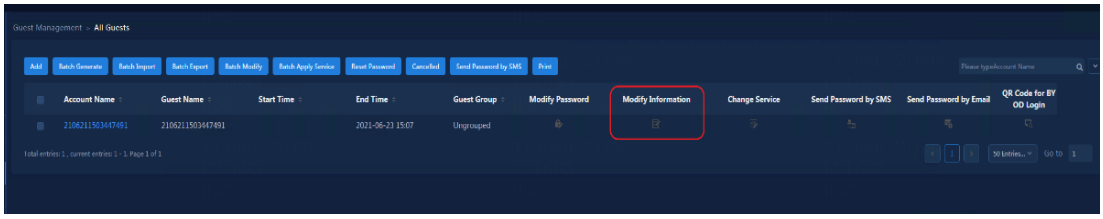
QR コードを読み取ってログインする

ゲストマネージャー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。

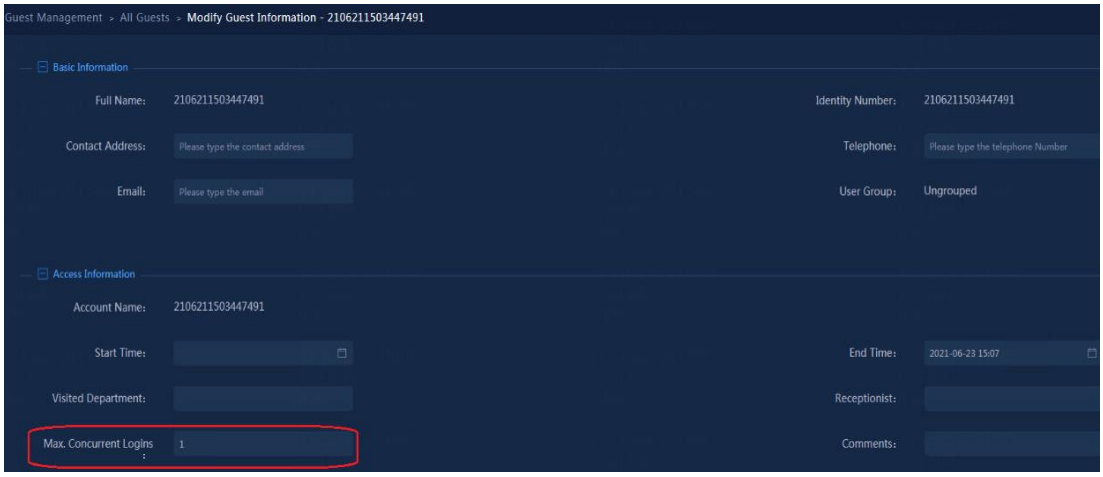
1. ゲストマネージャーは、EIA サーバーhttp://100.1.0.100:9066/ssvui/login.html の IP アドレスをブラウザに入力して、**Self-Service Center** ページにログインします。ゲストマネージャーのユーザー名とパスワードを入力し、**Login** をクリックします。



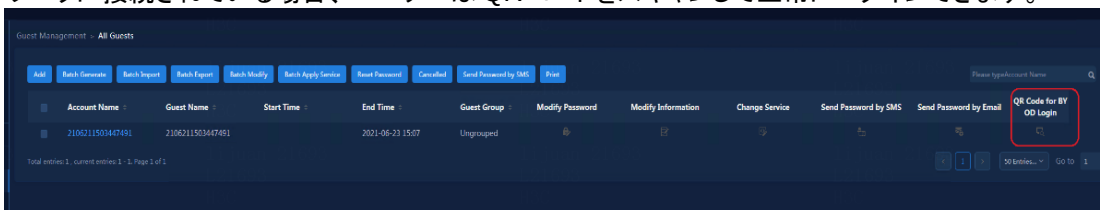
2. **Self-Service Center** にログインした後、**Guest User** > **All guests** を選択します。ゲスト情報が表示されます。



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、アイコン をクリックして **Max. Concurrent Logins** パラメーターを変更します。必要に応じて QR コードの読み取り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** を設定した後、**QR Code for BYOD Login** 列のポータル認証 QR コードの アイコンをクリックして、QR コードページを開きます。ユーザーのエンドポイントが内部ネットワークに接続されている場合、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。

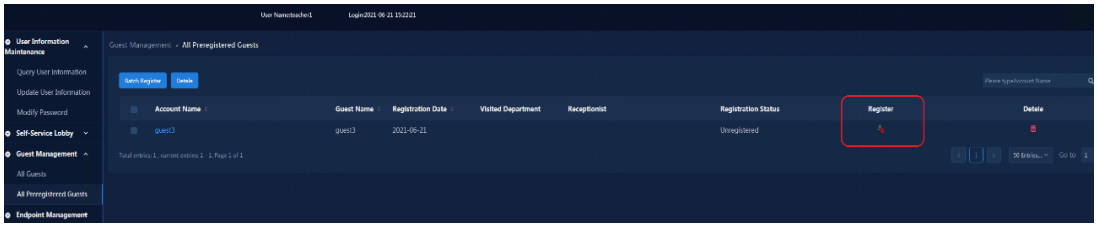


5. WeChat を使用してゲスト QR コードをスキャンしてログインを完了する場合は、BYOD セキュリティグループアドレスが外部ネットワークに接続できないときに、次の操作を実行します。
   a. ゲストの電話が外部ネットワークに接続されている場合は、WeChat を使用してゲストマネージャーによって生成された QR コードをスキャンし、QR コード内の URL を取得します。
   b. 受信した URL をパソコンに入力してログインします。

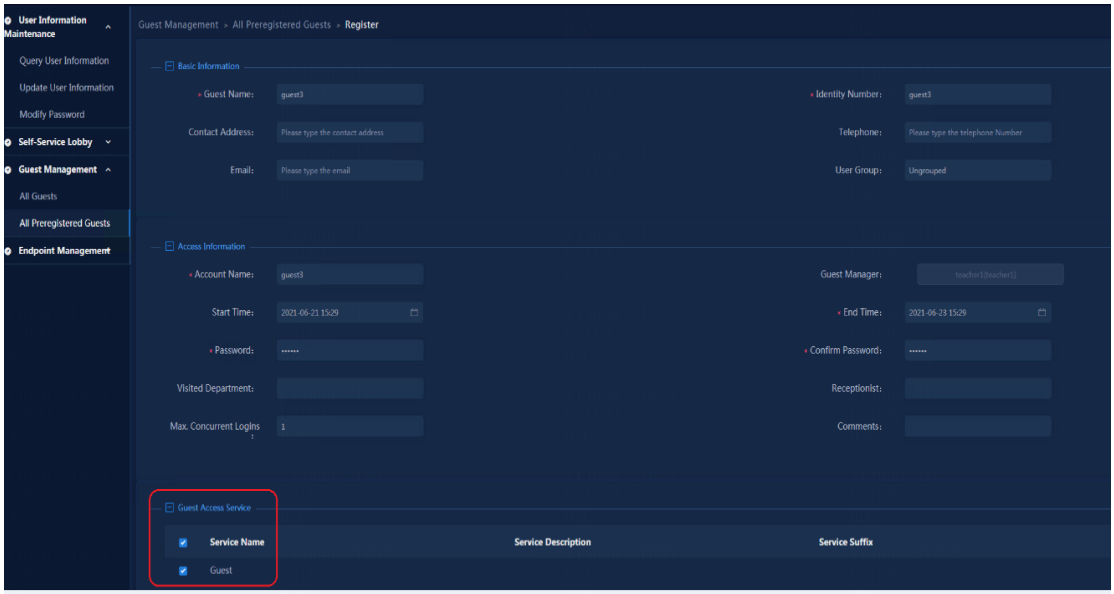
ゲストの承認

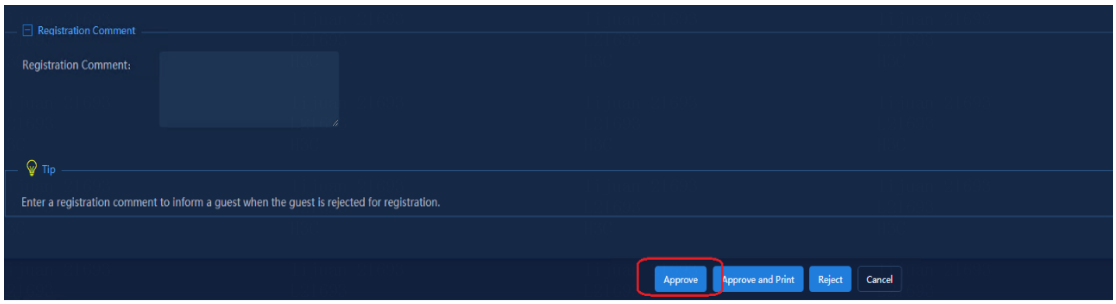
『Configuring a guest policy』で **Guest Auto-Registration** が **Disable** に設定されている場合、ゲストはゲストマネージャーによって承認される必要があります。ゲストは承認後に公式ゲストユーザーになることができます。

1. ゲストマネージャーは、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。ゲストマネージャーのユーザー名とパスワードを入力し、**Login** をクリックします。
2. **Guest User** > **All Preregistered guests** を選択して、承認待ちのすべてのゲストユーザーを照会します。承認のアイコンをクリックします。

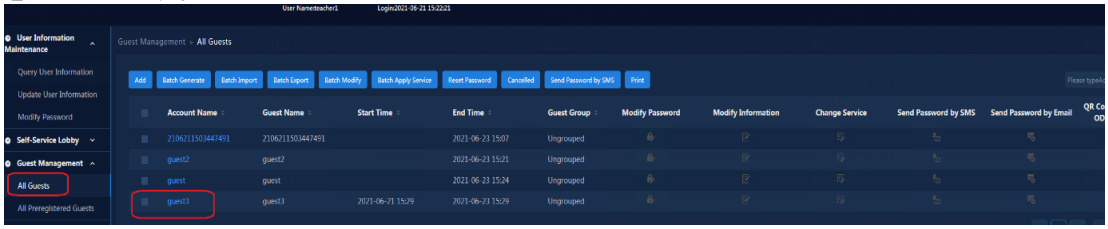


承認時に、ゲストのアクセスユーザーを変更できます。『Configuring a guest service』で構成されているすべてのアクセスサービスが一覧表示されます。**Approve** をクリックします。





3. 承認後、**Automation** > **Users** > **Guest Users** > **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。



権限とドメインの管理

概要

キャンパスコントローラーは、権限とドメイン管理機能をサポートしています。主に、オペレーターがコントローラーにログインした後に、ロール属性に従ってコントローラーがオペレーターに付与する機能権限を指します。多くの機能が含まれます。このセクションでは、主に分離ドメインとファブリック関連の設定について説明します。

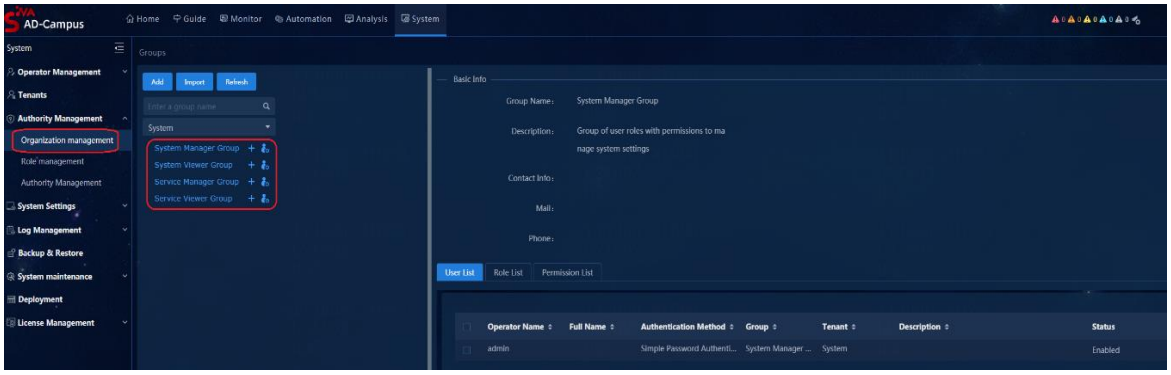
基本概念

グループ

システムには、演算子を階層的に管理するためのグループが用意されています。グループには、グループ内の演算子の権限を制御する演算子ロールを構成できます。システムには、4 つのデフォルトグループが事前に構成されています。必要に応じてグループを作成することもできます。

- システムマネージャーグループ:システム設定を管理する権限を持つユーザーロールのグループ。
- **System Viewer Group**: システム設定を表示する権限を持つユーザーロールのグループ。
- **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ロールのグループ。
- **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ロールのグループ。

グループを表示するには、**System** > **Authority Management** > **Organization Management** ページにナビゲートします。



⚠ 警告!

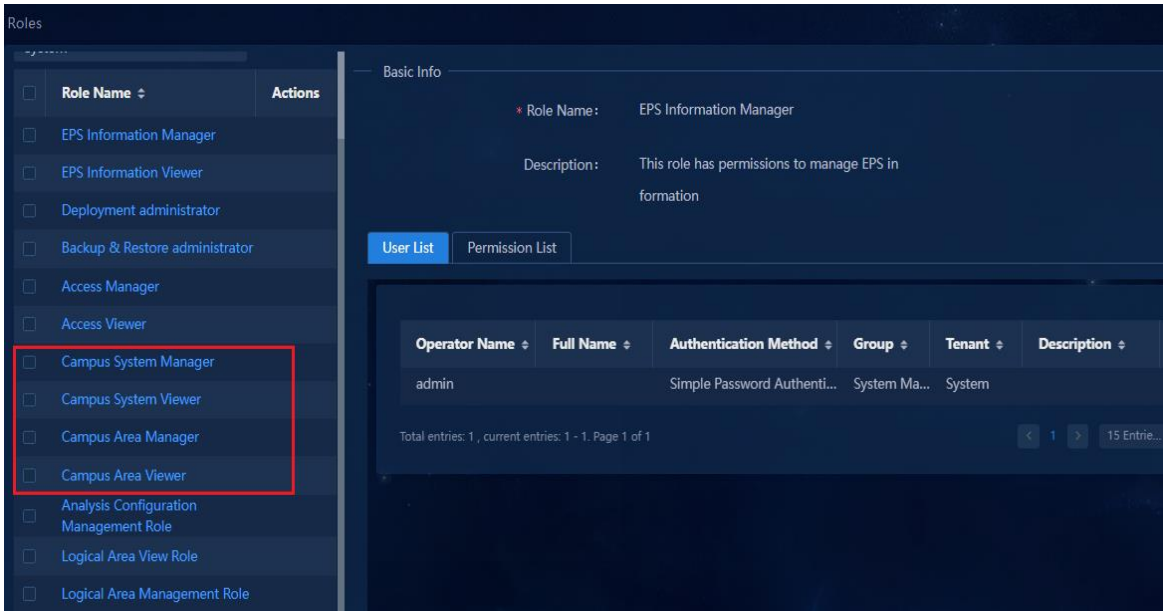
- オペレーターによって使用されているグループは削除できません。
- グループの名前は変更できません。
- 既に存在するグループは追加できません。
- 最大 10 レベルのサブグループを作成できます。
- パフォーマンスの制限により、最大 7 レベルのグループをインポートできます。

ロール

ロールは、ユーザータイプに対する一連の権限を定義します。ロールベースの権限制御が採用されているため、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。デフォルトでは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。

- **Campus System Manager**: キャンパスネットワークの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。

ロールを表示するには、**System** > **Authority Management** > **Roles** ページに移動します。



⚠ 警告!

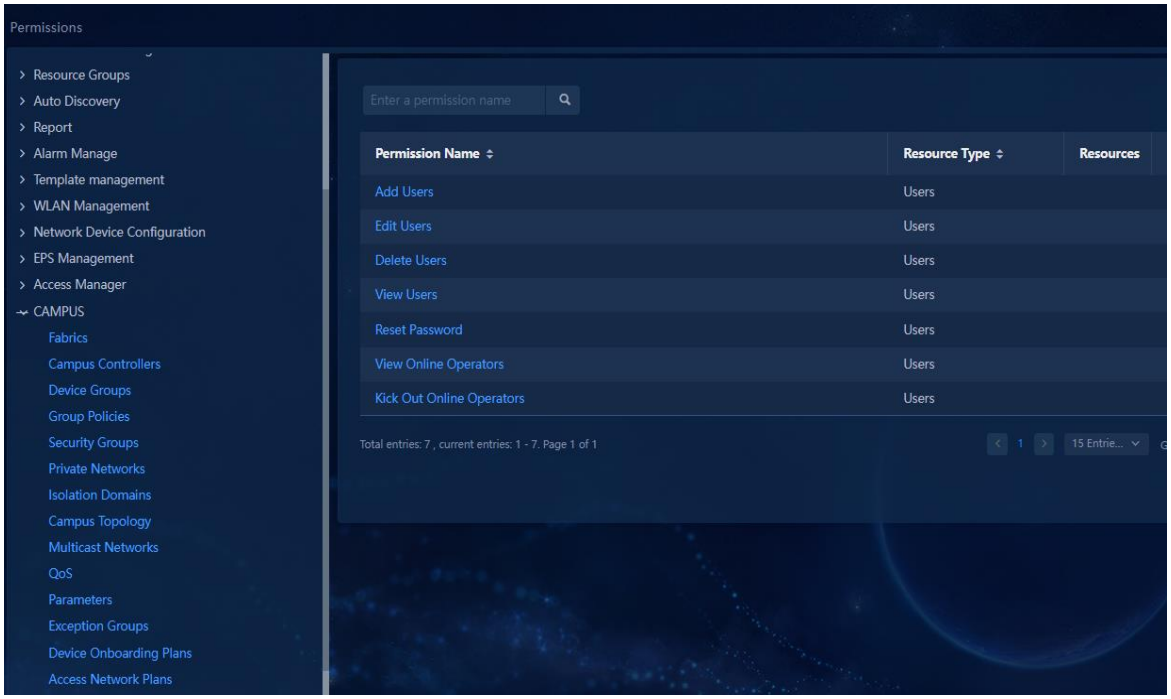
- キャンパスエリアロールには、デフォルトでは分離ドメインまたはファブリックの権限が含まれていないため、必要に応じてエリア権限を手動で追加する必要があります。
- 既に存在するロールは追加できません。
- ロールを削除した後、削除したロールと同じ名前でロールを再追加できます。
- ロールの削除には注意が必要です。ロールを削除すると、そのロールを持つユーザーはそのロールの権限を持たなくなります。

アクセス権

権限は、リソースタイプに対して許可された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。デフォルトでは、一連の権限が提供されます。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の権限には、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含まれます。

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、エリアマネージャーは、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。

権限を表示するには、**System** > **Authority Management** > **Permissions** ページに移動します。



⚠ **警告!**

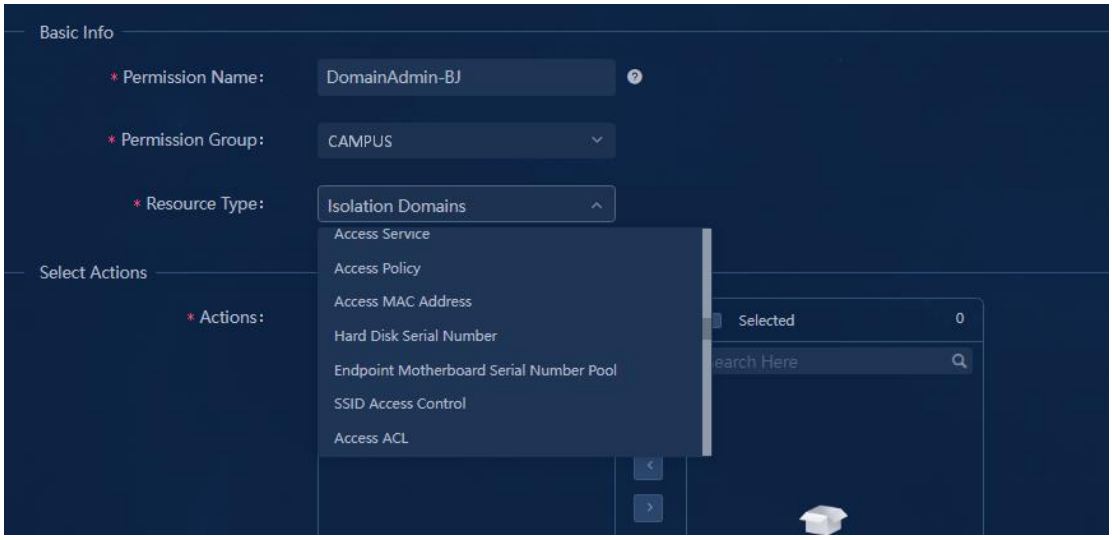
- admin オペレーターはスーパー管理者であり、デフォルトですべての権限を持っています。
- 権限の変更時に名前を変更することはできません。
- 既に存在するアクセス許可は追加できません。
- 表示権限のないデータを変更または削除する権限がある場合、そのデータはページに表示されません。
- リソースデータの一部のみがアクセス許可に指定されている場合、そのアクセス許可では、ユーザーが他のデータを表示、変更、または削除することはできません。
- 権限の削除には注意が必要です。権限を削除すると、その権限を持つユーザーは、対応する操作権限またはデータ権限を持たなくなります。

アクセス許可とドメインの構成

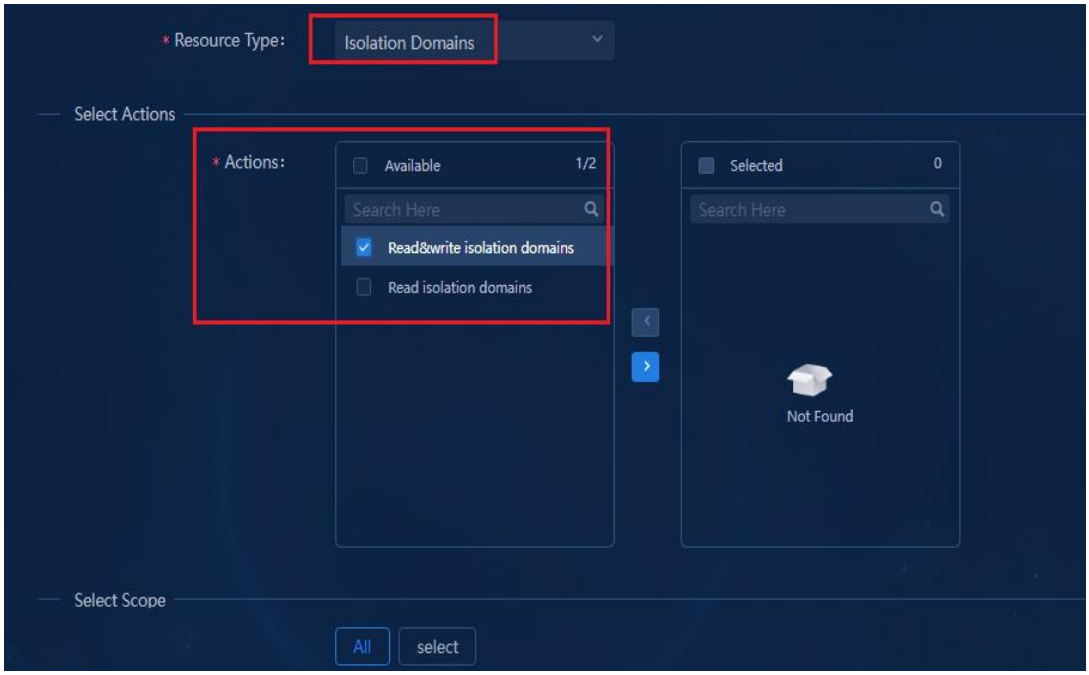
権限の追加

エリアマネージャーのサブ権限の追加

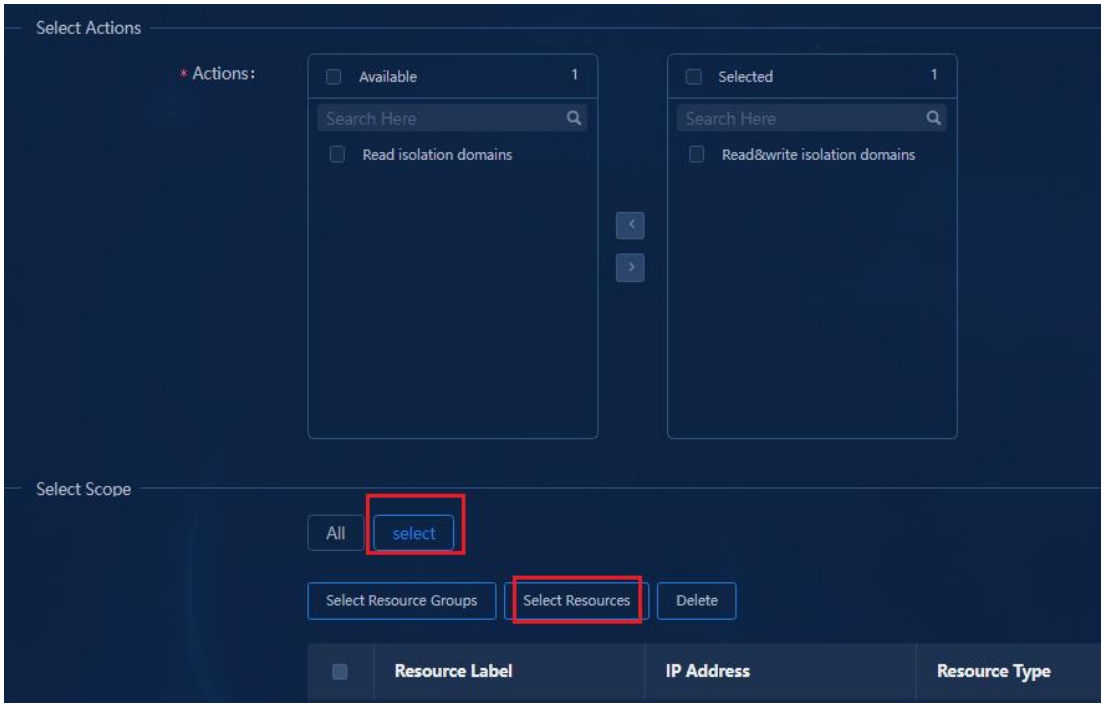
1. **System** > **Authority Management** > **Permissions** ページに移動して、追加 **Add** をクリックします。権限名を入力し、権限グループとして **CAMPUS** を選択し、リソースタイプとして **Isolated Domain** を選択します(名前を入力して、目的のリソースタイプをフィルタリングできます)。

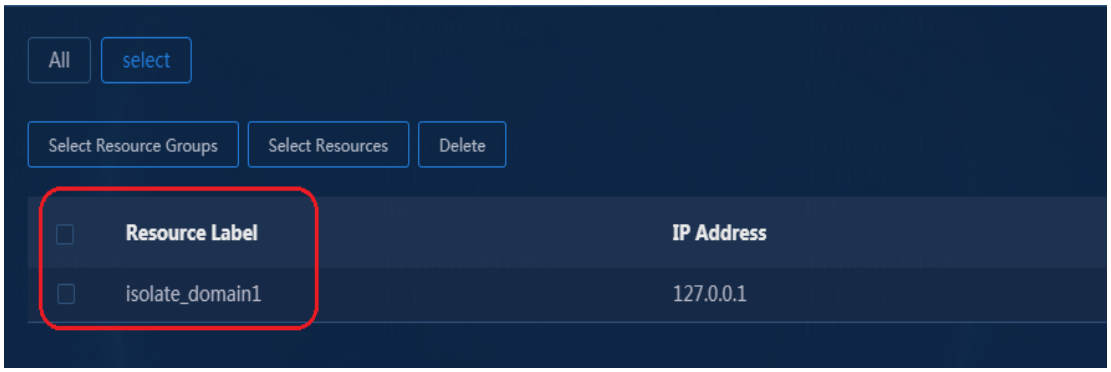


2. **Select Actions** 領域で、**Read&write isolation domains**(エリアマネージャーの場合)または Read isolation domains(エリアビューアの場合)チェックボックスを選択します。次に、›アイコンをクリックして **Selected** リストに追加します。



3. **Select Scope** で、**All** または **select** を選択します。このセクションでは、例として **select** を選択します。**Select Resources** を選択します。表示されたダイアログボックスで、対応する分離ドメインを選択し、**select** をクリックします。

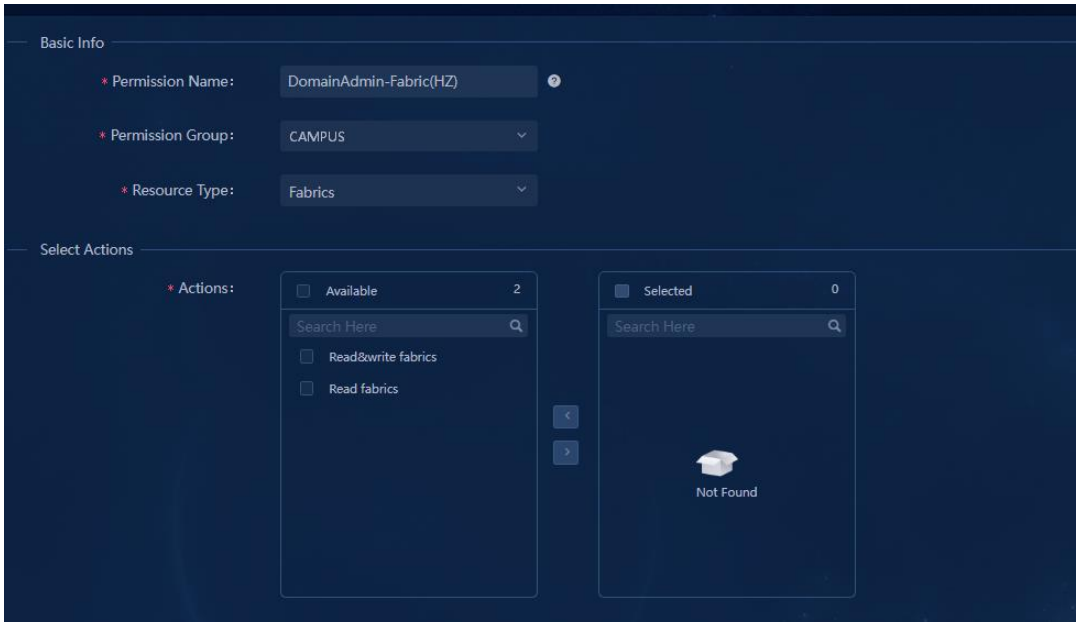




4. **OK** をクリックします。エリアマネージャーのサブ権限が **Isolation Domains** 権限の下に追加されます(パス: **System** > **Permissions** > **CAMPUS** > **Isolation Domains**)。

ファブリック下のエリアオペレーターに対するサブ権限の追加

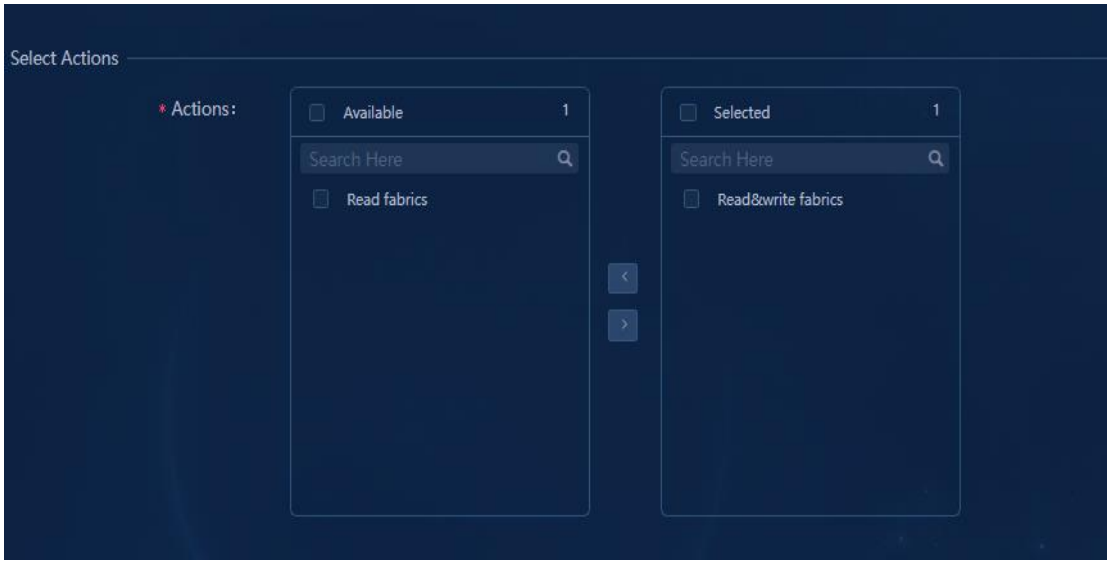
1. **System** > **Authority Management** > **Permissions** ページに移動し、**Add** をクリックします。Permission Name を入力し、**Permission Group** として **CAMPUS** を選択し、**Resource Type** として **Fabrics** を選択します。



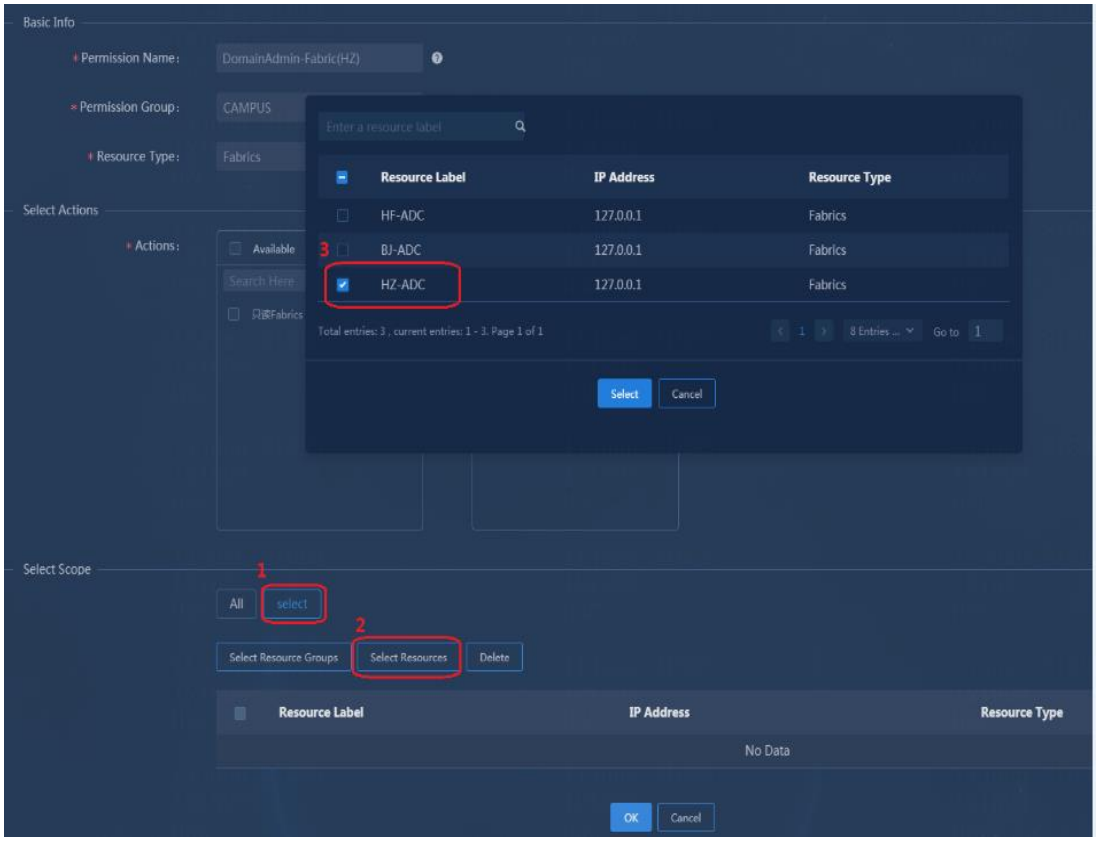
⚠ 警告!

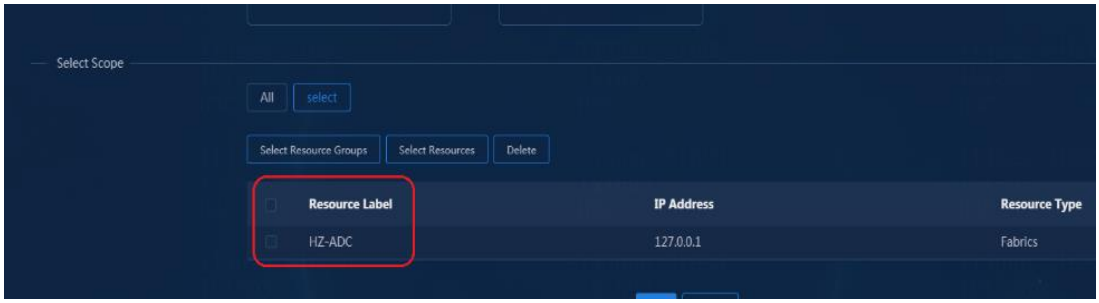
キャンパスコントローラーと DC コントローラーの両方が配置されている場合、2 つのファブリック権限があります。スコープ構成を許可する権限は、キャンパスのファブリック権限です。

2. **Select Actions** 領域で、**Read&Write Fabrics**(エリアマネージャーの場合)または **Read fabrics**(エリアビューアの場合)チェックボックスを選択します。次に、›アイコンをクリックして **Selected** リストに追加します。

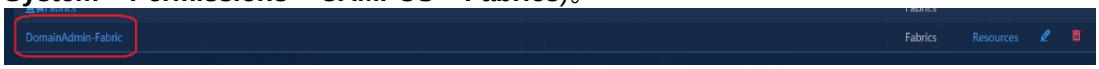


3. **Select Scope** 領域で、**All** または **select** を選択します。このセクションでは、例として **select** を選択します。Select Resources を選択します。表示されたダイアログボックスで、対応するファブリックを選択し、**Select** をクリックします。



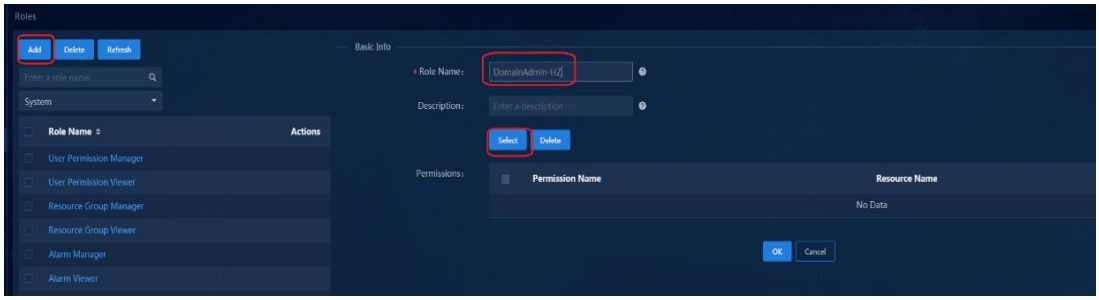


4. **OK** をクリックします。エリアマネージャーのサブ権限が **Fabrics** 権限の下に追加されます(パス: **System** > **Permissions** > **CAMPUS** > **Fabrics**)。

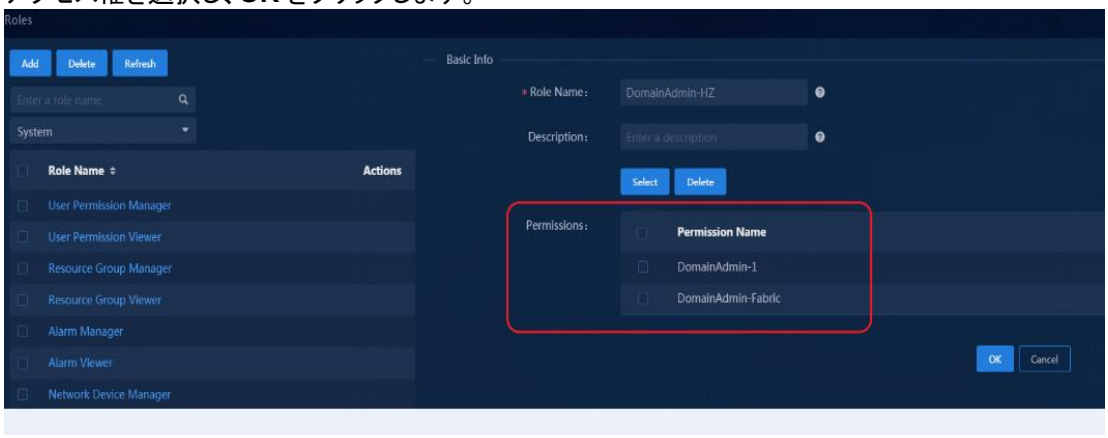


ユーザー定義の役割の追加

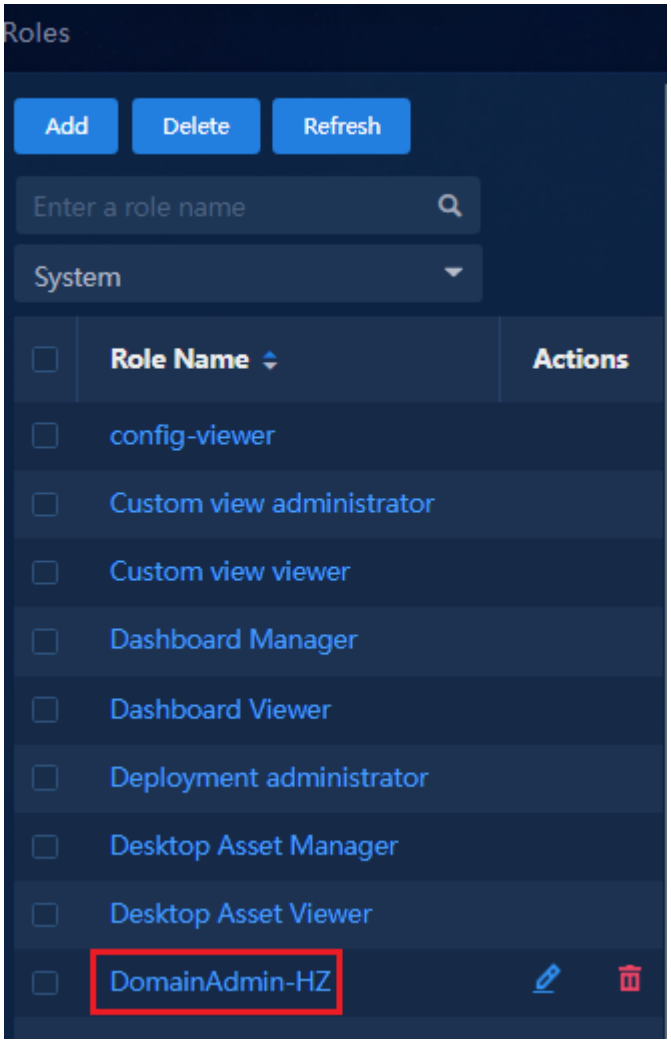
1. **System** > **Authority Management** > **Roles** ページにナビゲートし、**Add** をクリックしてロール名を入力します。ロールの権限を選択するには、**Select** をクリックします。権限フィルタがサポートされています。権限名を入力して、必要な権限を取得できます。



2. 『Adding a permission』に追加したアクセス権の名前を入力し、**Search** アイコンをクリックします。アクセス権を選択し、**OK** をクリックします。

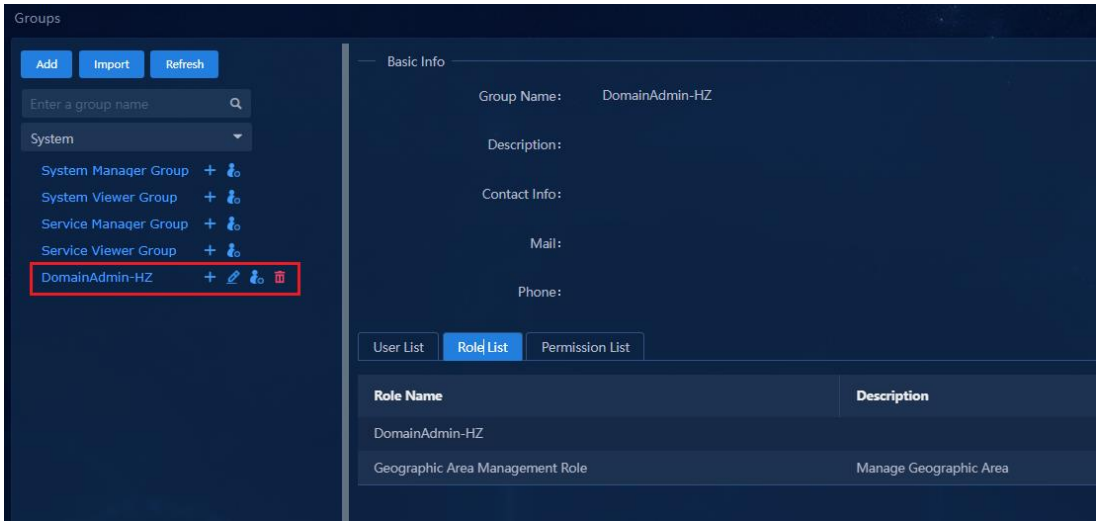


3. **OK** をクリックして、エリアロールの追加を完了します。追加したエリアロールは、**System** > **Authority Management** > **Roles** ページに表示されます。



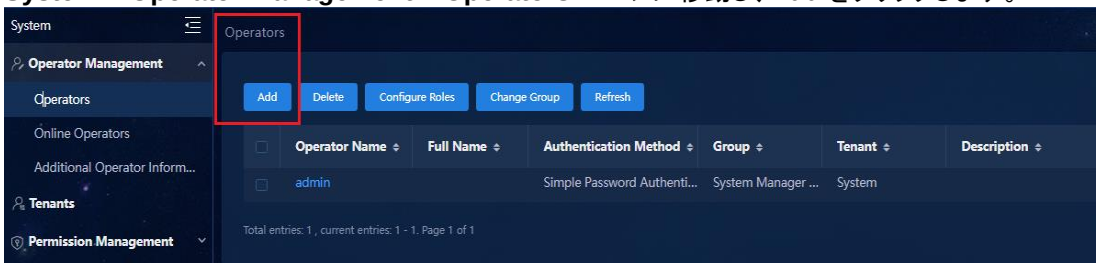
ユーザー定義グループの追加

1. **System** > **Authority Management** > **Groups** ページに移動し、**Add** をクリックします。グループ名、メール、および連絡先情報を入力します。
2. 『Adding user-defined roles』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。追加したエリアグループは、**System** > **Authority Management** > **Group** ページで表示できます。

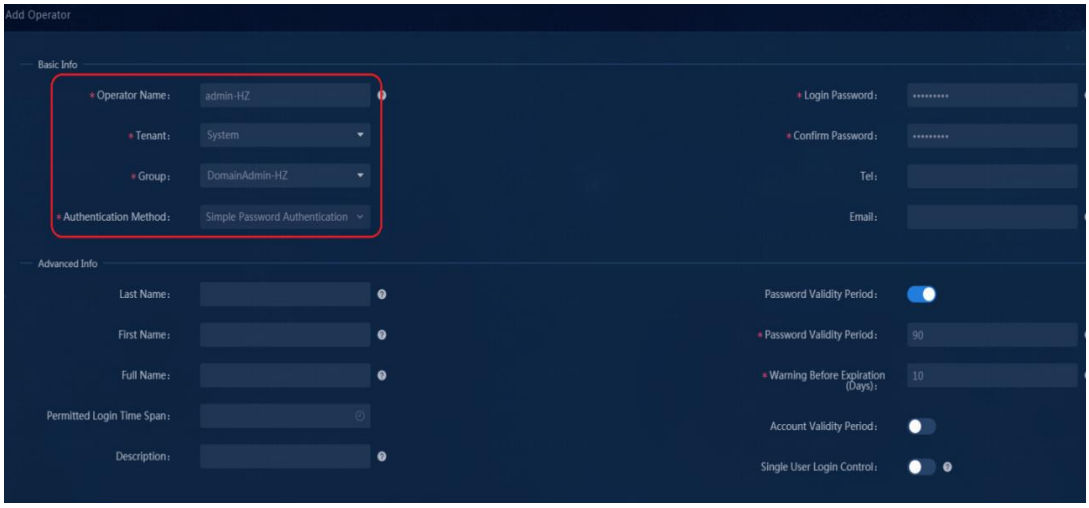


演算子の追加

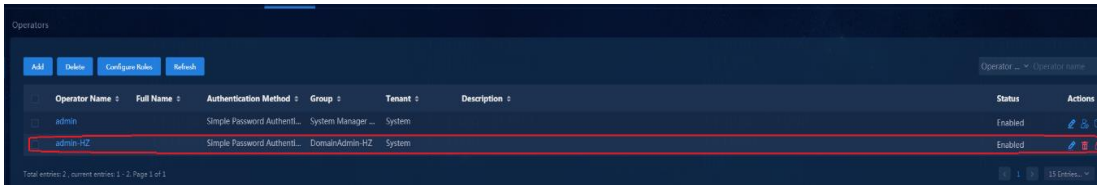
1. **System** > **Operator Management** > **Operators** ページに移動し、**Add** をクリックします。



2. 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『Adding user-defined groups』で追加されたグループを選択します。認証方法として **Simple Password Authentication** を選択し、ログインパスワードを入力します。パスワードは、複雑さの要件を満たす必要があります。つまり、パスワードは、数字、大文字、小文字、特殊文字 (!"#$%&'()*+,-./:;^`<=>?@{}_~)およびスペースを含む 8 から 30 文字の文字列である必要があります。パスワードには、オペレーターユーザー名またはオペレーターユーザー名の逆順の文字を含めることはできません。パスワードの先頭または末尾にスペースを使用することはできません。



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

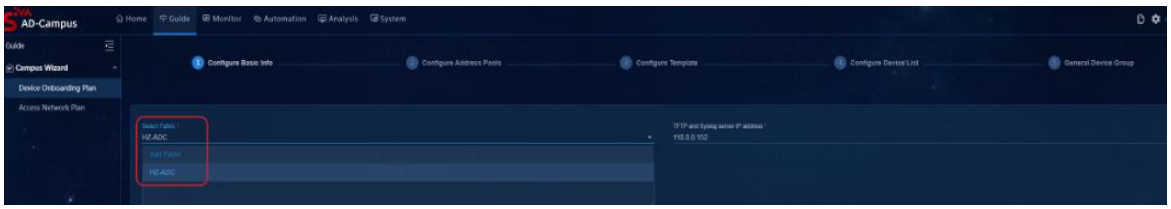
『演算子の追加』で追加されたオペレーターを使用してコントローラー管理ページにログインし、オペレーターに設定された権限があるかどうかを確認します。

⚠ 警告!

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。

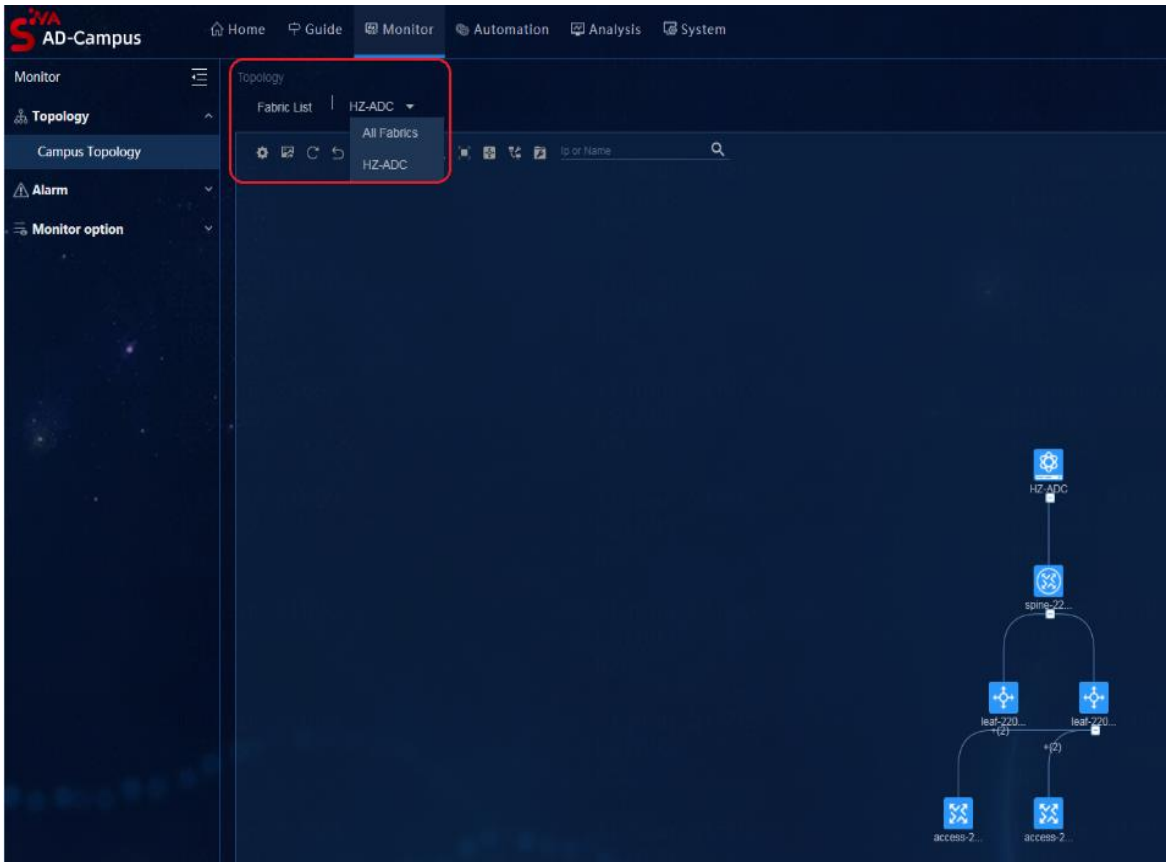
Wizard > Campus Wizard > Device Onboarding Plan

デバイスオンボーディング構成に使用可能なファブリックは、認可されたファブリックのみです。対応するアドレスプール構成およびロールテンプレートを表示できます。他のファブリックに関する情報を選択または表示することはできません。



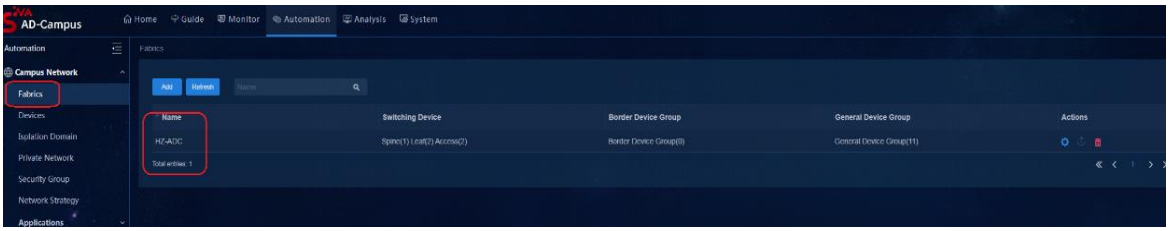
Monitor > Topology > Campus Topology

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を表示できますが、他のファブリックのトポロジ情報は表示できません。



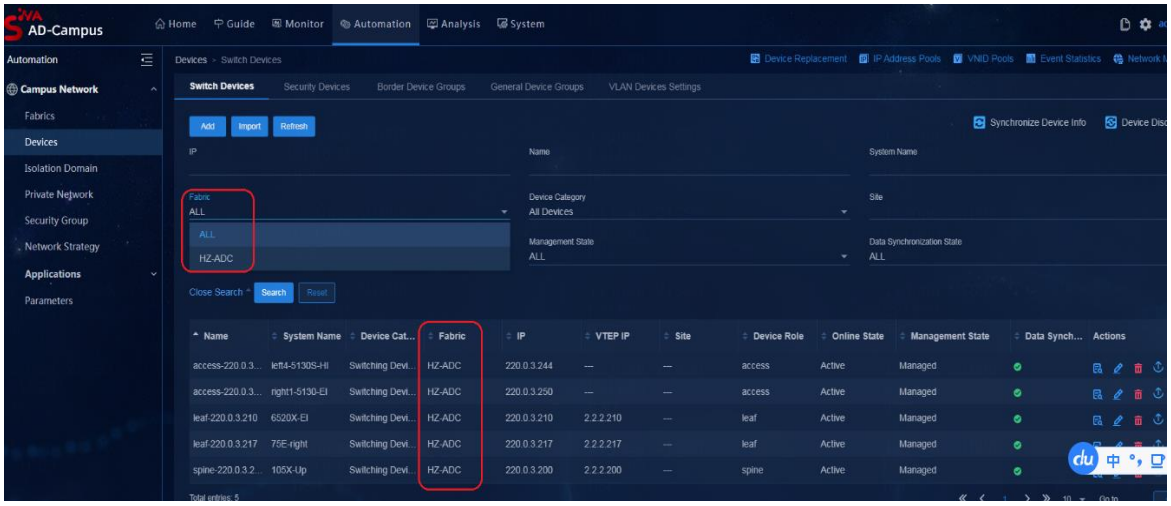
Automation>Campus Network>Fabrics の順に選択

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



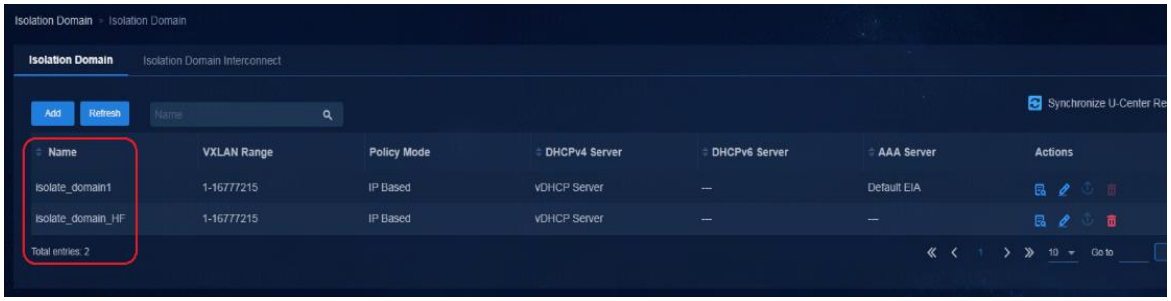
Automation>Campus Network>Devices>Switch Devices

許可されたファブリック内のデバイスだけを表示および変更できます。他のファブリックのデバイス情報は表示できません。

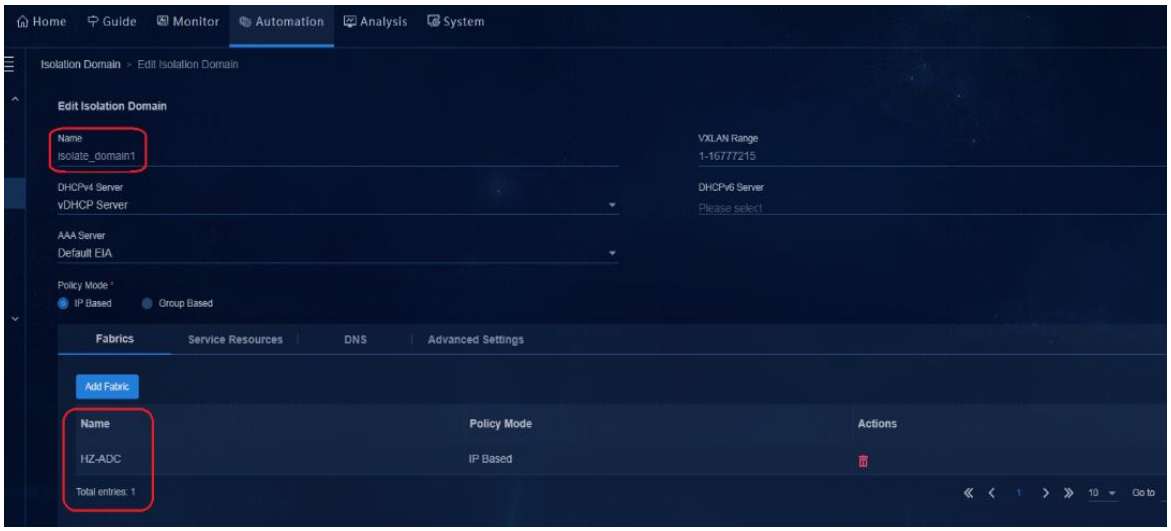


Automation > Campus Network > Isolation Domain > Isolation Domain

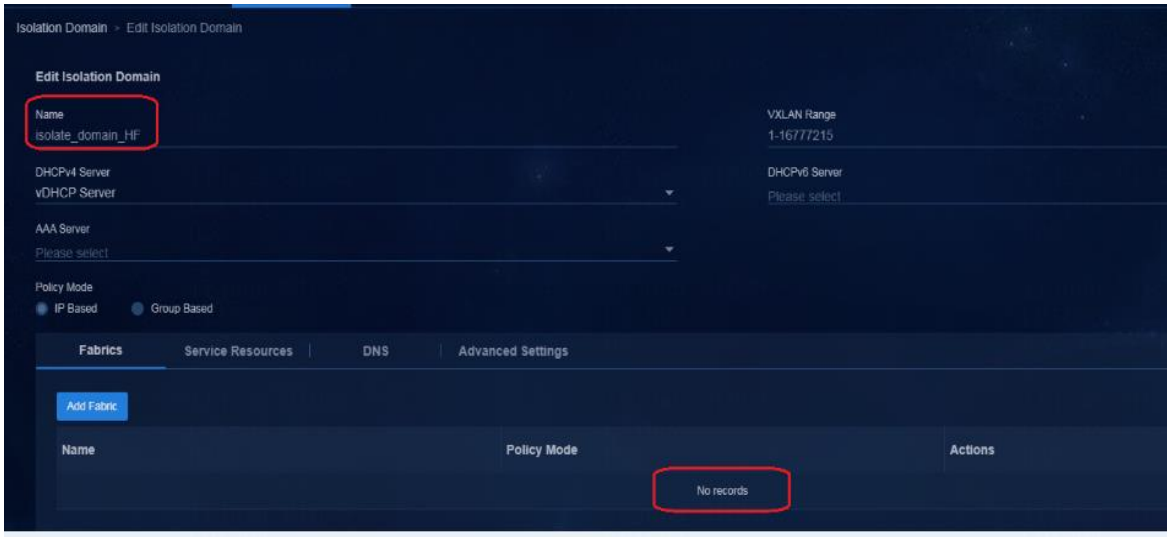
デフォルトでは、すべての分離ドメインを表示できます。



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。



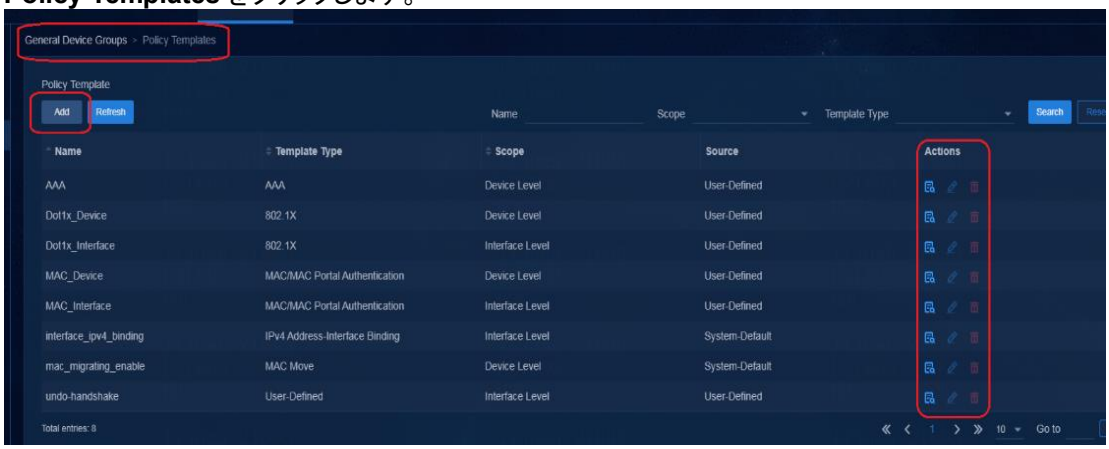
他の分離ドメインにバインドされているファブリックは表示できません。



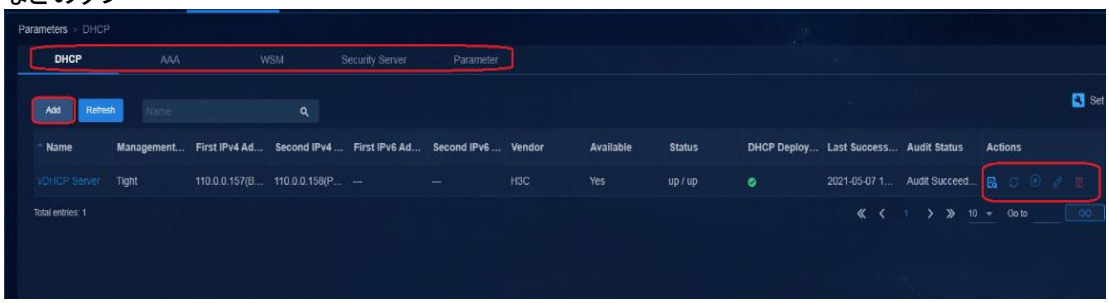
公的資源

一部のパブリックリソースは、オペレーターに対するエリア権限の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ーには、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。主に次のインターフェイスが関係します。

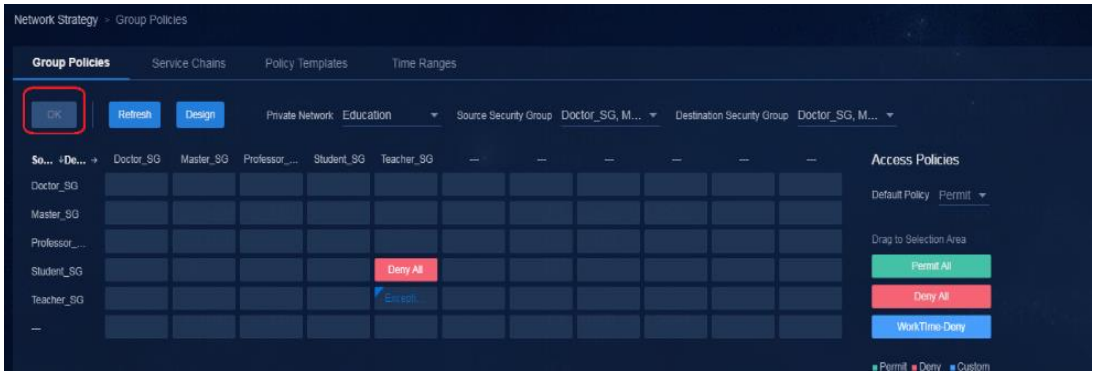
- **Automation** > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Policy Templates** をクリックします。



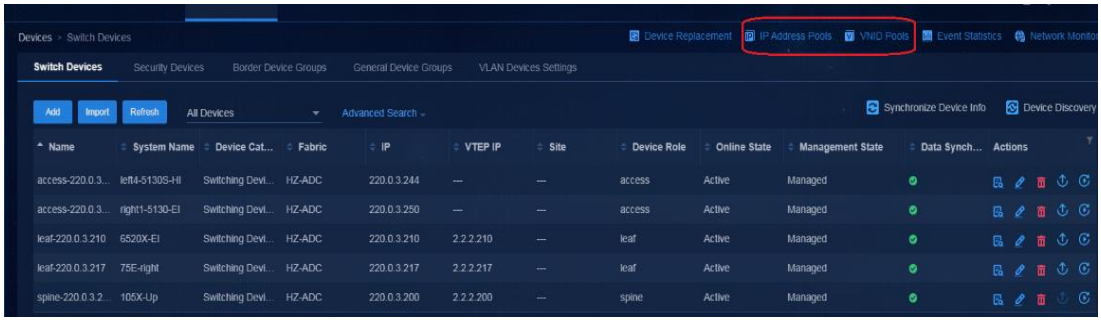
- **Automation** > **Campus Network** > **Network Parameters** ページの **DHCP**、**AAA**、**Parameter** などのタブ



- **Automation** > **Campus Network** > **Network Strategy** ページの **Group Policies** タブ、**Service Chains** タブ、**Policy Templates** タブ、および **Time Ranges** タブ



- **Automation > Campus Network > Devices** ページの **Device Replacement**、**IP Address Pools**、**VNID Pools** などのパラメーター。



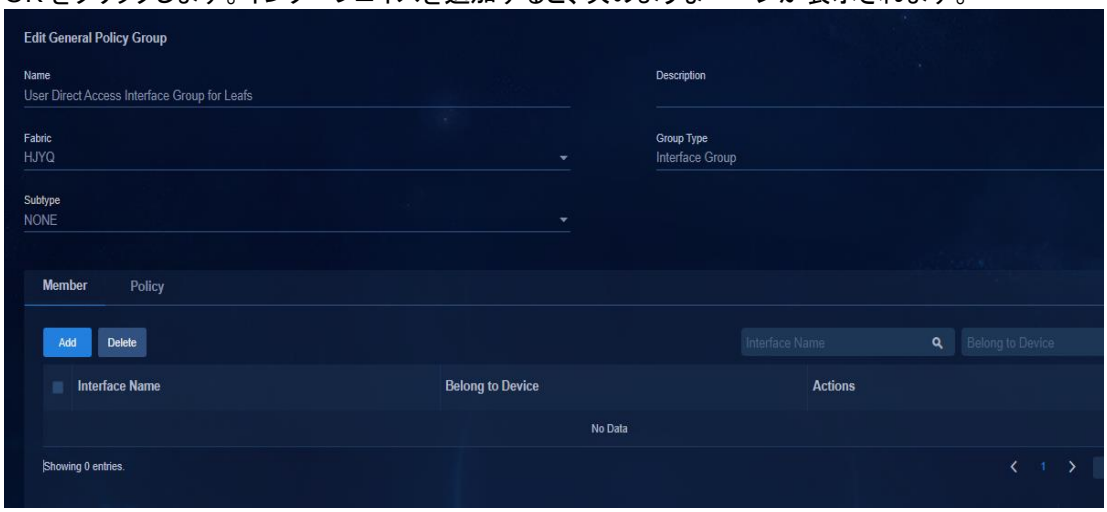
リーフデバイスに直接接続されたエンドポイントの設定

リーフインターフェイスは、デバイスにアクセスするだけでなく、エンドポイントにも直接接続できます。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認証され、オンラインになります。

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** > **Devices** > **General Device Groups** ページに移動し、**User Direct Connection-Leaf Interface Group** という名前のグループに対応する **Edit** アイコンをクリックして、**Edit General Policy Group** ページを開きます。

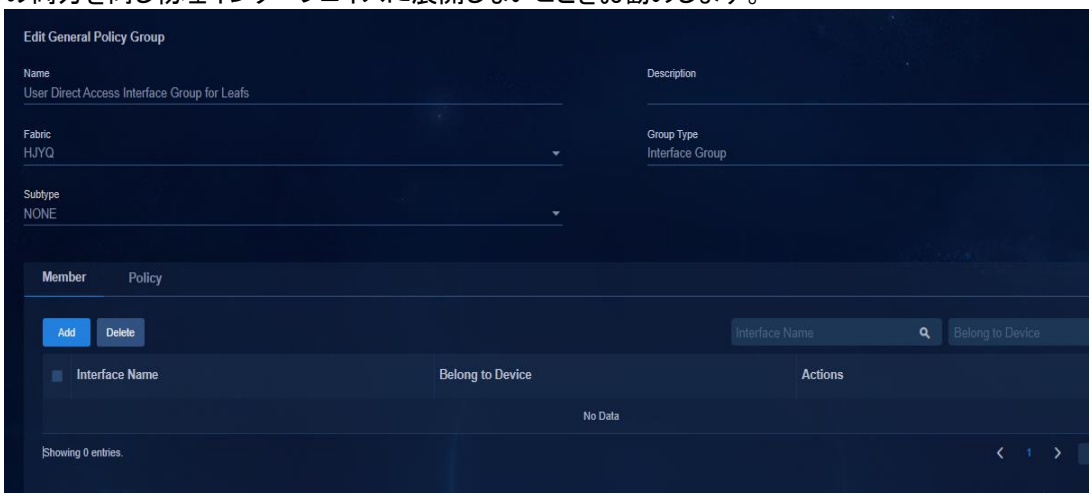
2. **Member** タブで、**Add** をクリックします。リーフデバイスのエンドポイントに接続されているインターフェイスを選択します。**Add** をクリックして、選択したインターフェイスリストにインターフェイスを追加し、OK をクリックします。インターフェイスを追加すると、次のようなページが表示されます。



3. **OK** をクリックして、メンバーの追加を完了します。

インターフェイスグループへのポリシーの展開

1. **Automation** > **Campus Network** > **Devices** > **General Device Groups** ページに移動し、**Add** をクリックして、『Configuring a policy template』で設定したポリシーテンプレートを選択し、グループポリシーに追加します。実際の状況に応じて、802.1X 認証テンプレートまたは MAC/MAC ポータル認証テンプレートを展開できます。802.1X 認証テンプレートと MAC/MAC ポータル認証テンプレートの両方を同じ物理インターフェイスに展開しないことをお勧めします。



2. リーフデバイスに展開される設定は、次のとおりです。

   802.1X 認証テンプレートまたは MAC/MAC ポータル認証テンプレートを、実際の状況に応じてインターフェイスに展開します。選択できるテンプレートは 1 つだけです。この例では、MAC/MAC ポータル認証テンプレートが展開されます。

```
[Leaf11-Ten-GigabitEthernet5/0/22]display this //Interface directly connected to endpoints.
#
interface Ten-GigabitEthernet5/0/22
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1
 mac-based ac
 mac-authentication
 mac-authentication domain isp
 mac-authentication parallel-with-dot1x
 mac-authentication critical vsi vsi167 url-user-logoff
#
```

3. 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。

ユーザークリティカルなソリューションの構成

⚠ **警告!**

- EAD 機能を使用しない場合は、**Enable Policy Server** オプションを選択しないことをお薦めします。デフォルトでは、このパラメーターが選択されています。このオプションを選択すると、iNode クライアントを使用するオンライン 802.1X 認証ユーザーのエスケープ時間が 3 ハートビート間隔を超えた後、ユーザーは自動的にオフラインになります。
- **Automation** > **User** > **Access Parameters** > **Policy Server Parameters** ページで、ユーザークリティカルソリューションを設定します。

重要なレイヤー2ネットワークドメインの作成

クリティカルスキームは主に、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クリティカルセキュリティグループです。

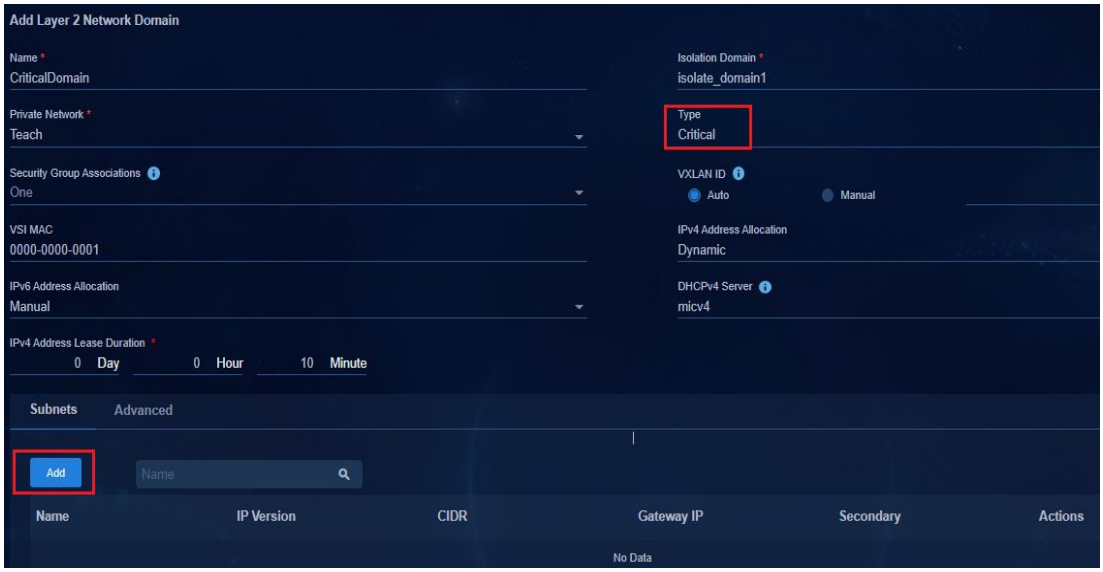
重要なサービスを構成する場合、重要なサービスに対して DHCP サーバーを設定する必要があり、重要なセキュリティグループに対応するサブネットが DHCP サーバーに配信されます。H3C DHCP サーバーまたはサードパーティの DHCP サーバーを使用できます。

⚠ **警告!**

- 分離ドメインでは、重要なセキュリティグループを 1 つだけ構成できます。
- クリティカルセキュリティグループはプライベートネットワークで設定する必要があり、VPN インスタンス **vpn-default** でクリティカルセキュリティグループを設定することはサポートされていません。
- ベストプラクティスとして、重要な DHCP サーバーを、EIA サーバー、BYOD DHCP サーバー、およびサービス DHCP サーバーとは別のサーバーに設定します。重要なサーバーとネットワークデバイスが相互に到達できることを確認します。

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 **Add Layer 2 Network Domain** ページを開き、次のパラメーターを設定します。
   - **Private Network**: プライベートネットワークを選択します。**vpn-default** は選択できません。
   - **Type**: **Critical** を選択します。
   - **IPv4 Address Allocation**: **Dynamic** を選択します。
   - **DHCP Server**: 重要な DHCP サーバーを選択します。重要な DHCP サーバー構成の詳細については、『Configuring the critical DHCP server』を参照してください。
   - **IPv4 Address Lease Duration**: デフォルトでは 10 分に設定されています。



2. **Subnets** タブで、**Add** をクリックします。表示されたページで、**Name** と **CIDR** を設定し、**OK** をクリックします。レイヤー2 ネットワークドメインページに戻ります。
3. **OK** をクリックすると、**Layer 2 Network Domain** ページに新しい重要なレイヤー2 ネットワークドメインが表示されます。

リーフデバイスに展開された設定:

#リーフデバイスの VSI インターフェイスを展開する DHCP サーバーの IP アドレスは、重要な DHCP サーバーの IP アドレスです。

```
#
interface Vsi-interface167       //The VSI interface number corresponds to the VXLAN ID in the Layer 2 network domain ID.
 description SDN_VSI_Interface_167
ip binding vpn-instance Teach
ip address 40.0.0.1 255.255.0.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 dhcp select relay proxy
 dhcp relay information circuit-id vxlan-port
 dhcp relay information enable
 dhcp relay server-address 192.168.2.210
 dhcp relay source-address interface Vsi-interface4094
 dhcp relay request-from-tunnel discard
#
```

重要なセキュリティグループの作成

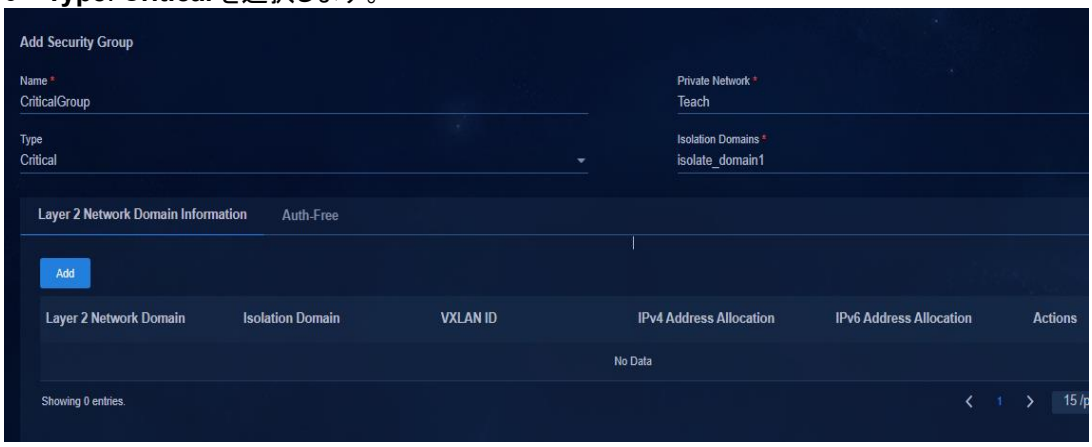
注:

分離ドメインに構成できるクリティカルセキュリティグループは 1 つのみです。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 つのクリティカルセキュリティグループを共有します。

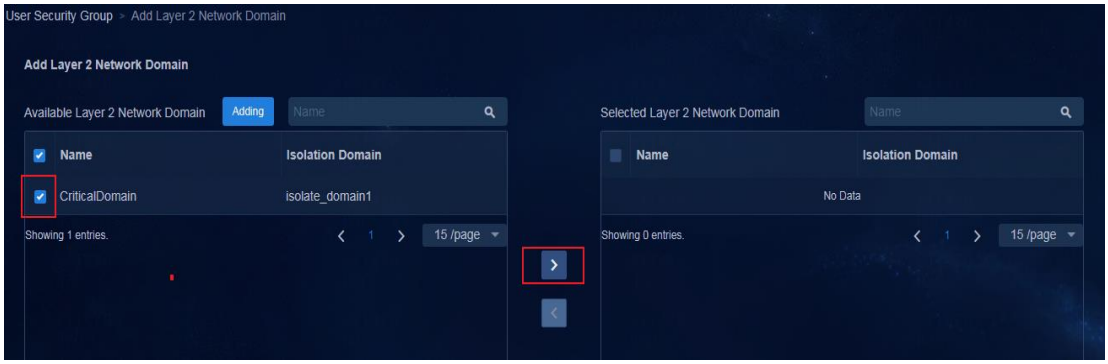
Automation > **Campus Network** > **Security Group** > **User Security Group** ページに移動します。

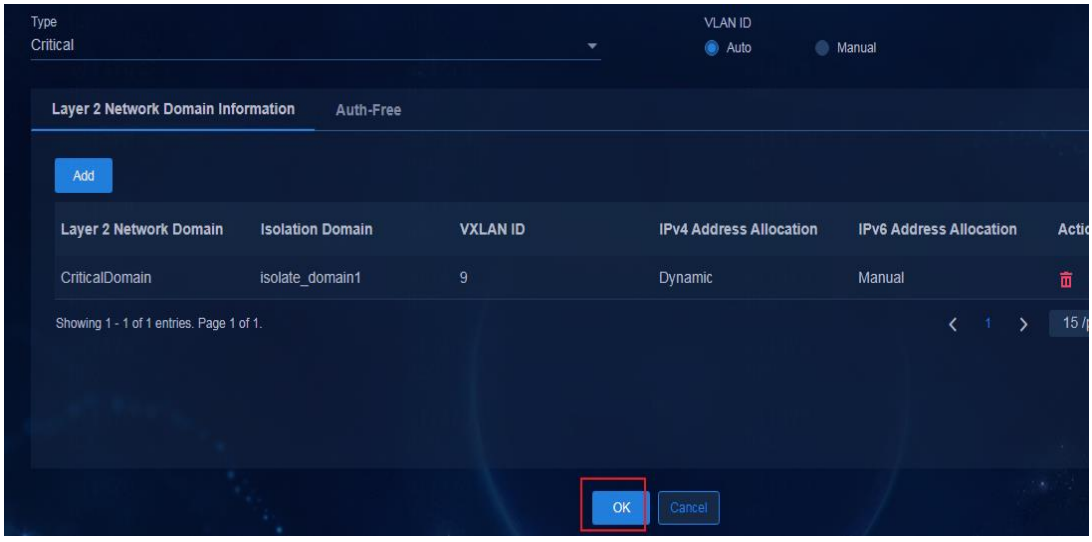
1. **Add** をクリックし、次のパラメーターを設定します。
   - **Private Network**: プライベートネットワークを選択します。

- **Type**: **Critical** を選択します。

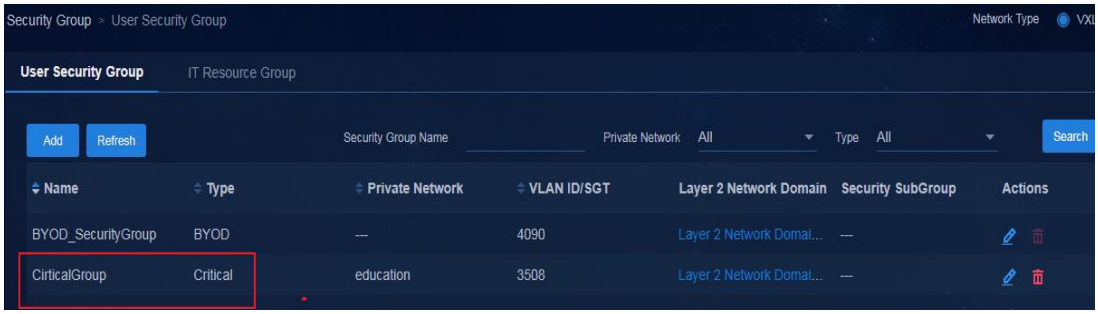


2. **Layer 2 Network Domain Information** タブを選択し、**Add** をクリックします。**Add Layer 2 Network Domain** ページで、設定済みのクリティカルドメインを選択し、> アイコンをクリックして、設定済みのクリティカルレイヤー2 ネットワークドメインを **Selected Layer 2 Network Domain** リストに追加します。**OK** をクリックして設定を保存します。





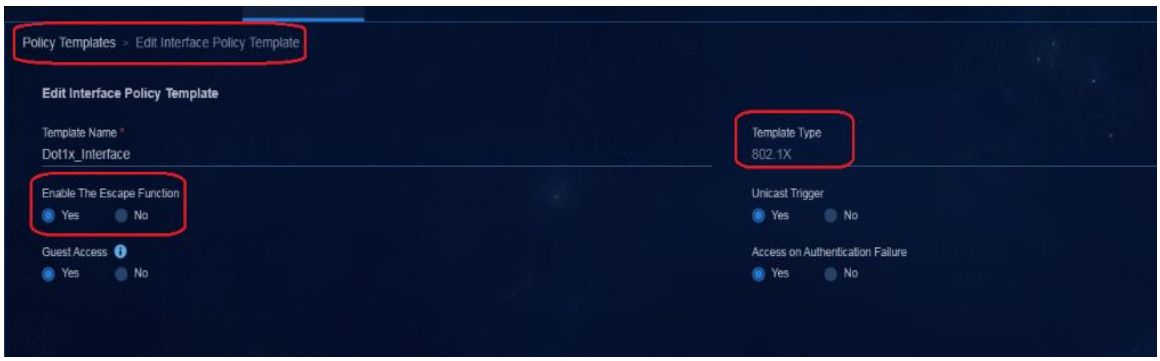
3. **OK** をクリックすると、**User Security Group** ページに新しいクリティカルセキュリティグループが表示されます。

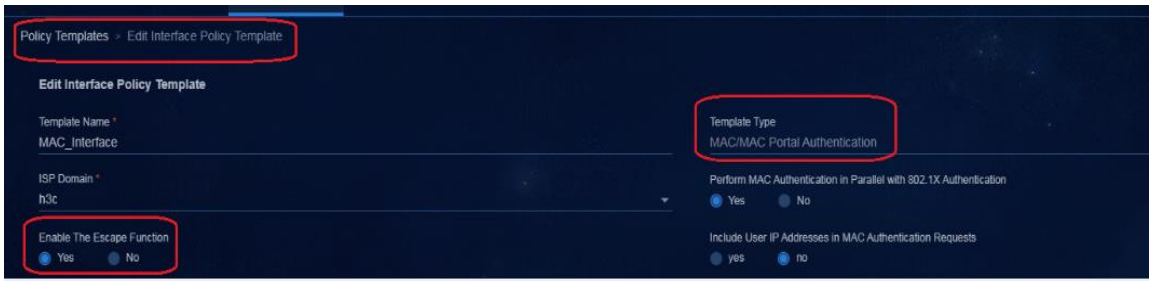


ポリシーテンプレートの設定

クリティカル機能を有効にするには、ポリシーテンプレートでクリティカル機能を設定し、リーフデバイスインターフェイスグループにポリシーテンプレートを適用する必要があります。詳しくは、『Configuring an interface policy template of the 802.1X type』および『Configuring an interface policy template of the MAC/MAC portal authentication type』を参照してください。

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





ポリシーテンプレートを使用してリーフダウンリンクインターフェイスグループが設定されると、コントローラーは重要な VSI 関連の設定をリーフダウンリンクインターフェイスに展開します。

```
#
interface Bridge-Aggregation1023
 port link-type trunk
 port trunk permit vlan 1 101 to 3000 4094
 link-aggregation mode dynamic
 stp tc-restriction
 mac-based ac
 dot1x
 undo dot1x handshake
```

```
undo dot1x multicast-trigger
dot1x unicast-trigger
dot1x critical vsi vsi167
dot1x critical eapol
mac-authentication
mac-authentication domain isp
mac-authentication parallel-with-dot1x
mac-authentication critical vsi vsi167 url-user-logoff
port-security free-vlan 1 4094
#
service-instance 4094
 encapsulation s-vid 4094
 xconnect vsi vxlan4094
#
```

重要なITリソースへのアクセス設定

クリティカルセキュリティグループは、プライベートネットワーク vpn-default に設定できません。異なる分離ドメインに構成されたクリティカルセキュリティグループは異なります。ベストプラクティスとして、複数のプライベートネットワークからアクセスされる 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デプロイします。次に、プライベートネットワーク内の IT リソースグループを構成し、クリティカルセキュリティグループおよび IT リソースグループにアクセスする権限を構成します。

デフォルトでは、プライベートネットワークは vpn-default プライベートネットワークと通信でき、vpn-default に対する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が Permit または Deny に設定されているかどうかにかかわらず、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てから、重要なセキュリティグループが特定の IT リソースグループにアクセスできないようにアクセスポリシーを構成する必要があります。このためには、IT リソースグループに対して拒否モードのグループポリシーを展開します。

重要なDHCPサーバーの設定

クリティカルセキュリティグループを設定する場合は、クリティカル DHCP サーバーを指定する必要があります。

- 分離ドメインに構成されている DHCP サーバーが Microsoft DHCP サーバーである場合は、そのサーバーを重要な DHCP サーバーとして使用できます。
- 隔離ドメインに構成されている DHCP サーバーが H3C vDHCP サーバーである場合は、新しい DHCP サーバーを重要な DHCP サーバーとして構築する必要があります。

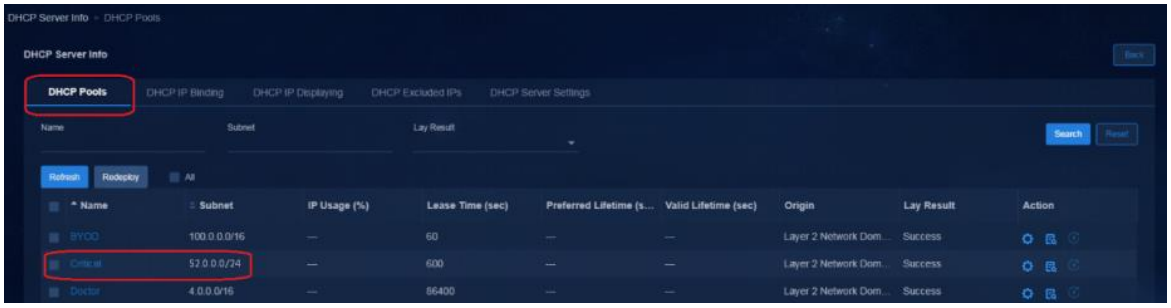
重要な DHCP サーバーの設定は次のとおりです。

- 重要な DHCP サーバーが H3C vDHCP サーバーである場合、認証設定は必要ありません。『Creating a critical Layer 2 network domain』の場合は、vDHCP を直接選択します。
- 重要な DHCP サーバーが Microsoft DHCP サーバーである場合は、VXLAN 4094 アドレスプールを設定する必要があります。

Microsoft の密結合 DHCP サーバーの構成

Microsoft DHCP サーバーを重要な DHCP サーバーとして使用する場合は、VXLAN 4094 アドレスプールを構成する必要があります。VXLAN 4094 アドレスプールの構成については、『Adding a Microsoft DHCP server』を参照してください。

重要なセキュリティグループが作成されると、次の図に示すように、選択した重要な DHCP サーバーに重要なサービスのアドレスプールが作成されます。



⚠ 警告!

分離ドメインに複数のファブリックがある場合は、複数のファブリックに対して VXLAN 4094 アドレスプールを設定する必要があります。

Microsoft の疎結合 DHCP サーバーの構成

疎結合モードでは、SeerEngine キャンパスコントローラーは DHCP サーバーに設定を展開しません。DHCP サーバー上の重要なセキュリティグループ内のサブネットを含むアドレスプールを手動で作成する必要があります。

VLAN 4094 のスコープの作成

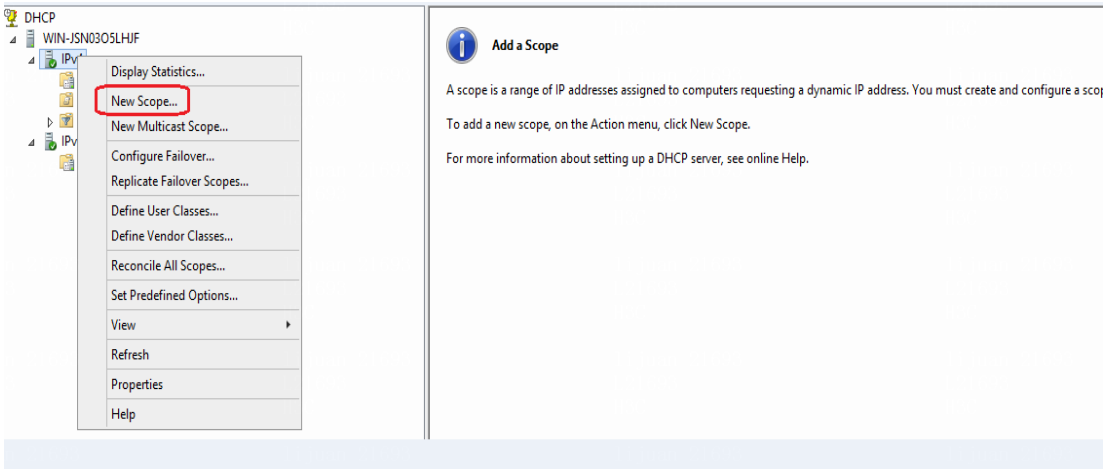
Microsoft DHCP サーバーで、VLAN 4094 のスコープを手動で設定します。

このアドレススコープを構成する目的は、後で作成される重要なセキュリティグループの IP アドレスプールからユーザーが IP アドレスを取得できるようにすることです。VLAN 4094 スコープを構成する必要があります。構成しない場合、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。

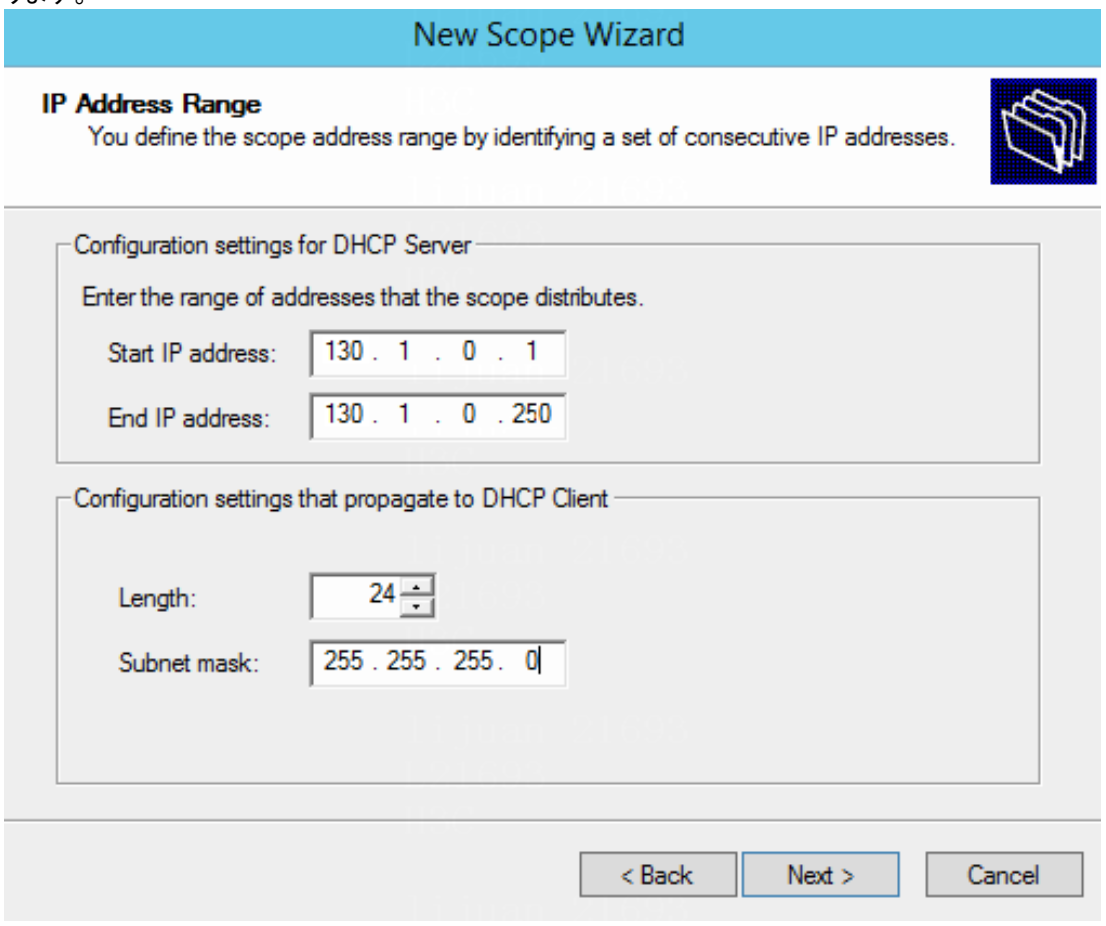
⚠ 警告!

分離ドメインに複数のファブリックがある場合は、複数のファブリックに対して VXLAN 4094 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** を選択し、**New Scope Wizard** ページを開きます。**Next** をクリックして名前を入力します。

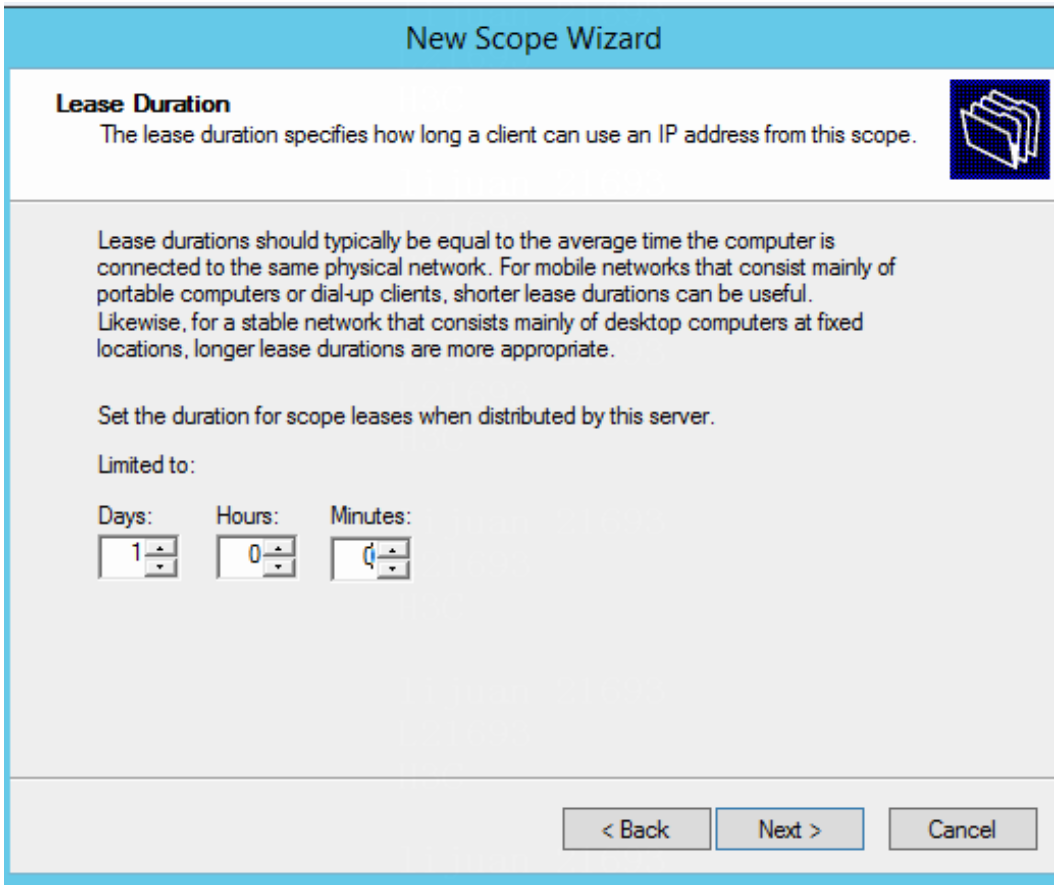


2. **Next** をクリックして、**IP Address Range** ページにアクセスします。IP アドレスセグメントを入力します。これは、デバイス上の VXLAN 4094/VLAN 4094 の IP アドレスセグメントと同じである必要があります。

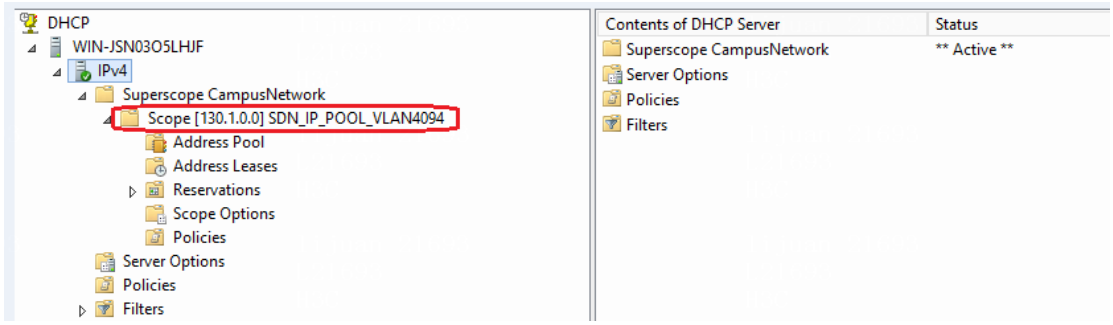


3. **Next** をクリックします。開いたページで、除外する IP アドレス範囲を入力します。この手順はオプションです。設定できるのはゲートウェイ IP のみです。**Add** をクリックして、アドレスをリストに追加します。

4. **Next** をクリックします。リース期間を 1 日に設定します。

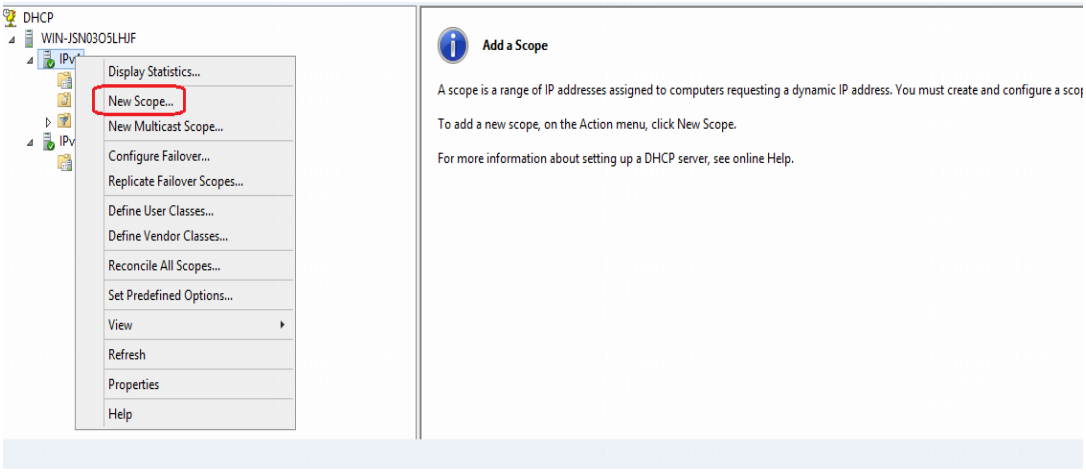


5. **Next** を続けてクリックします。ここで説明していないパラメーターについては、**Next** をクリックします。**Activate Scope** ページで、**Yes, I am activating the scope now** を選択
6. **Next** をクリックし、**Finish** をクリックします。設定が完了すると、VLAN 4094 スコープは次のように設定されます。

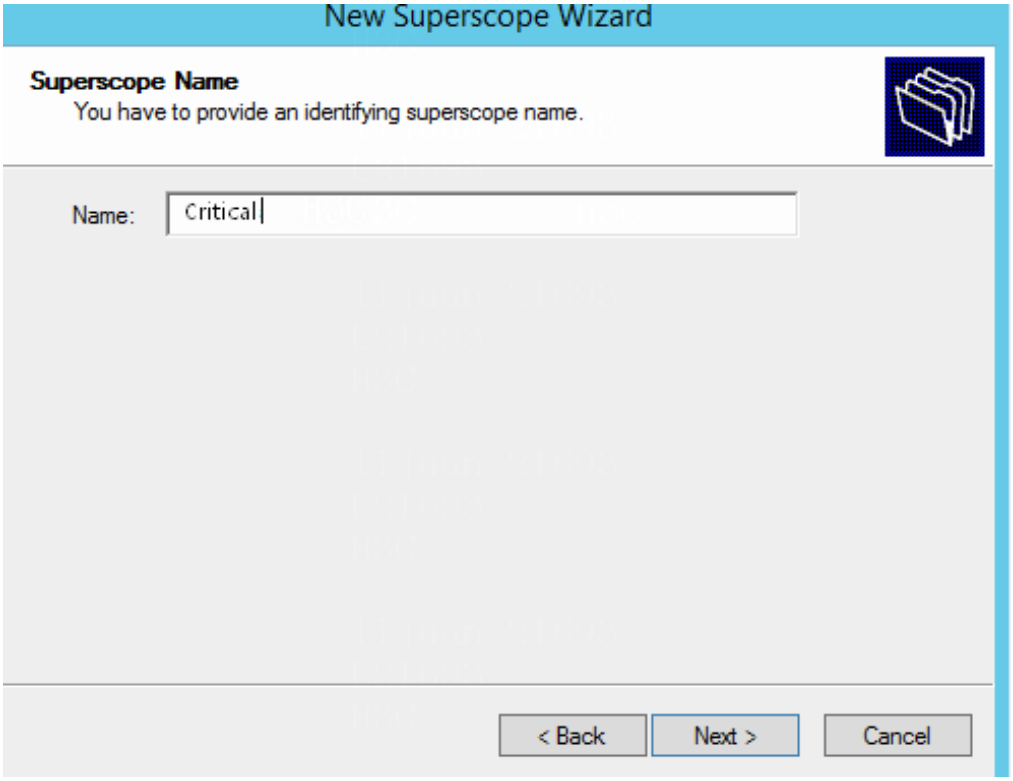


重要なセキュリティグループスコープを作成する

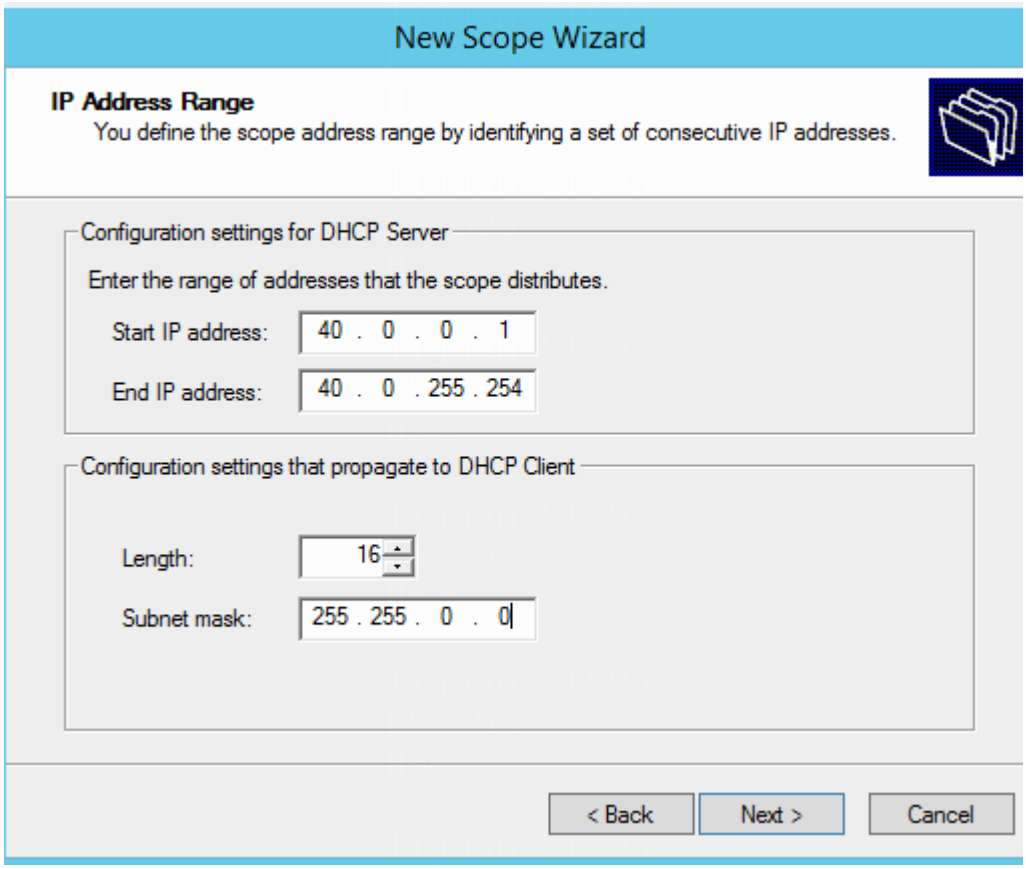
1. Microsoft DHCP サーバーで右クリックし、**New Scope** を選択して、**New Scope Wizard** ページを開きます。



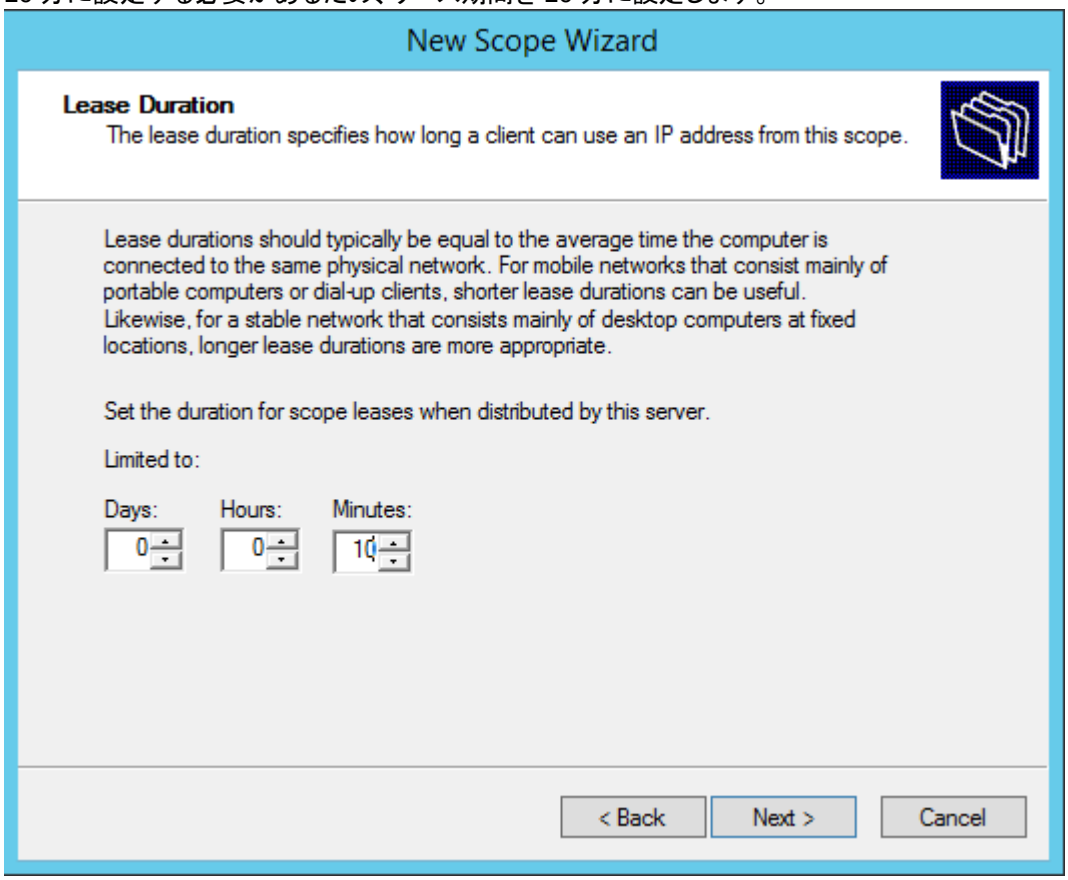
2. 名前を入力して、重要なセキュリティグループを作成します。



3. **Next** をクリックして、**IP Address Range** ページにアクセスします。『Creating a critical security group』で設定したサブネットセグメントと同じ IP 範囲を入力してください。

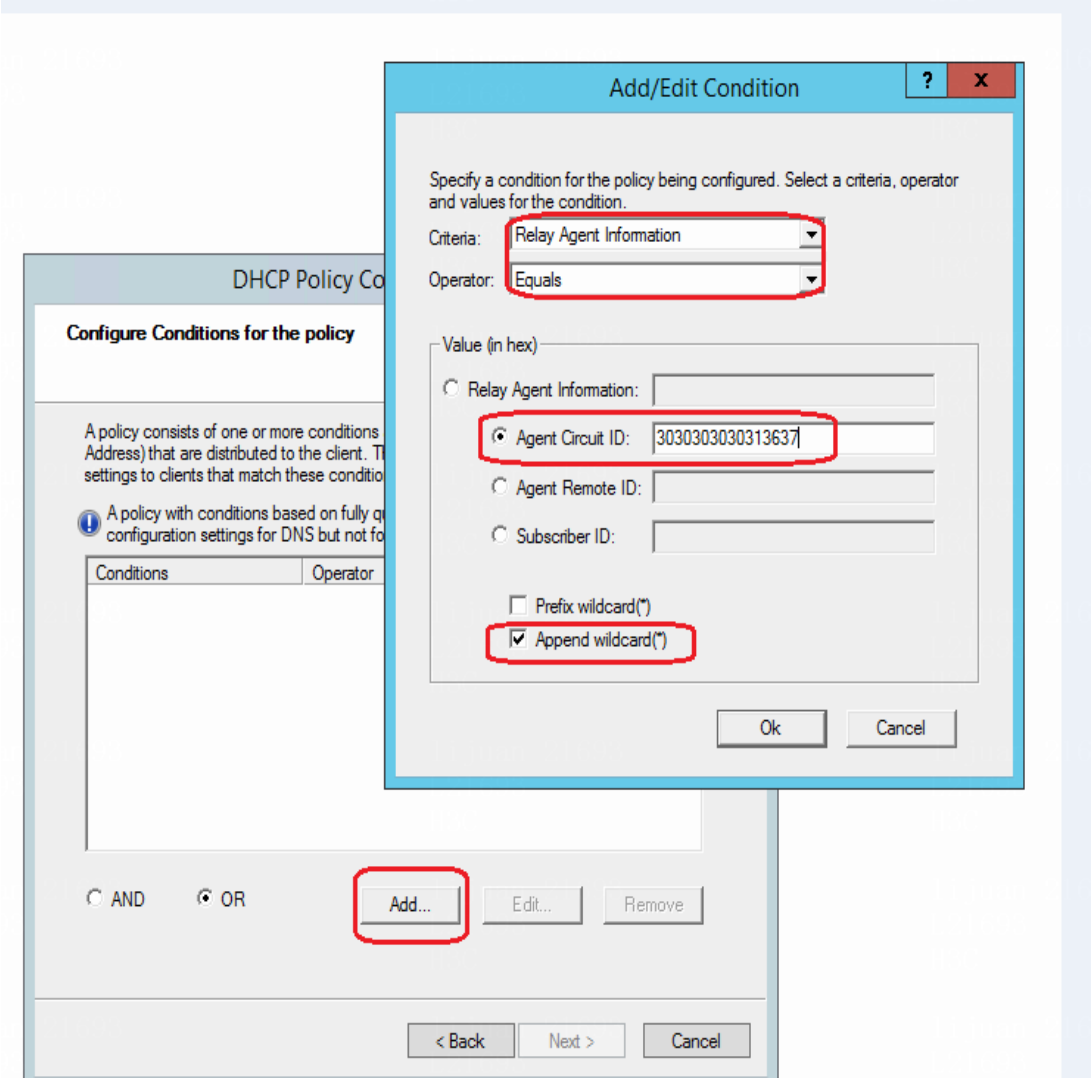


4. **Next** をクリックして、**Lease Duration** ページにアクセスします。重要なソリューションのリース期間を 10 分に設定する必要があるため、リース期間を 10 分に設定します。

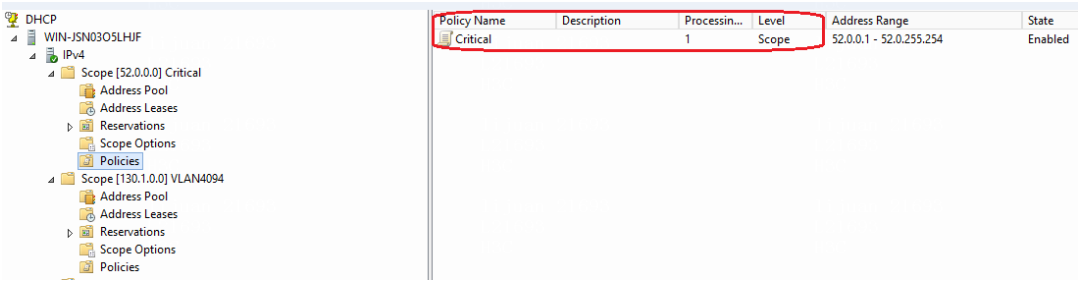


5. 設定が完了するまで、**Next** をクリックします。

6. スコープのポリシーを設定します。その他の設定は、VLAN 4094 のスコープポリシー設定と同じです。そのため、ここでは詳細を説明しません。
7. **Policies** を右クリックし、**Add** を選択してポリシー名を入力します。**Next** をクリックして、**Configure Conditions for the policy** ページにアクセスします。
8. **Add** をクリックして、**Add Condition/ Edit Condition** ページにアクセスします。**Relay Agent Information** を選択します。**Operator** を **Equal** に設定します。リレーエージェントの値は ASCII コードで、30303030 で始まり、VXLAN ID の 30313637 が続きます。これは、VXLAN ID が 167 であることを示し、*が続きます。*はワイルドカードで、任意の値に一致します。VXLAN ID 値は、クリティカルセキュリティグループの VXLAN ID 値です。

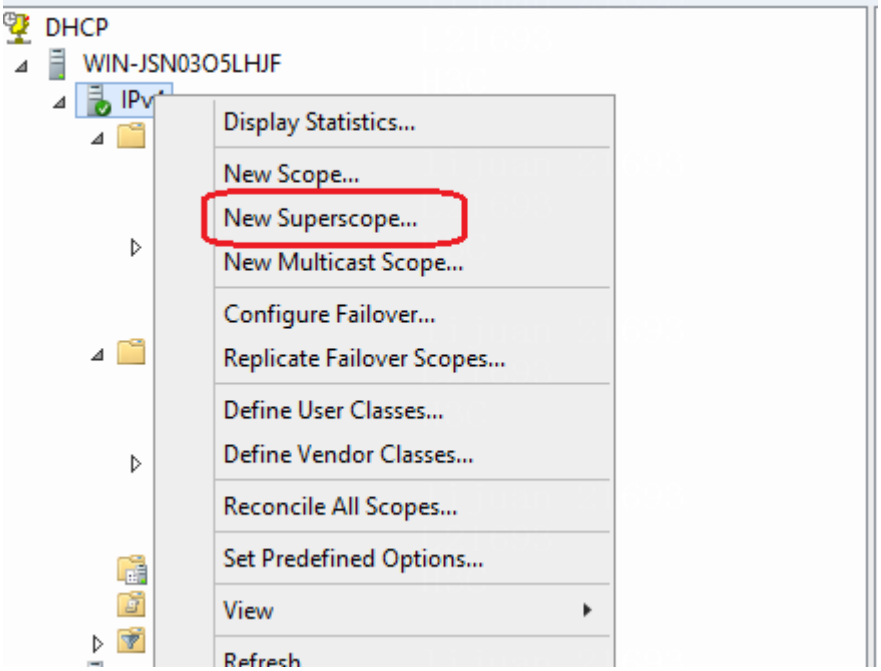


9. **OK** をクリックして設定を保存します。次に、**Next** をクリックしてポリシー構成設定ページにアクセスします。Configure IP address ranges for the policy パラメーターを **No** に設定します。
10. **Next** をクリックして **Summary** ページにアクセスします。Finish をクリックします。構成が完了すると、次のようなページが表示されます。

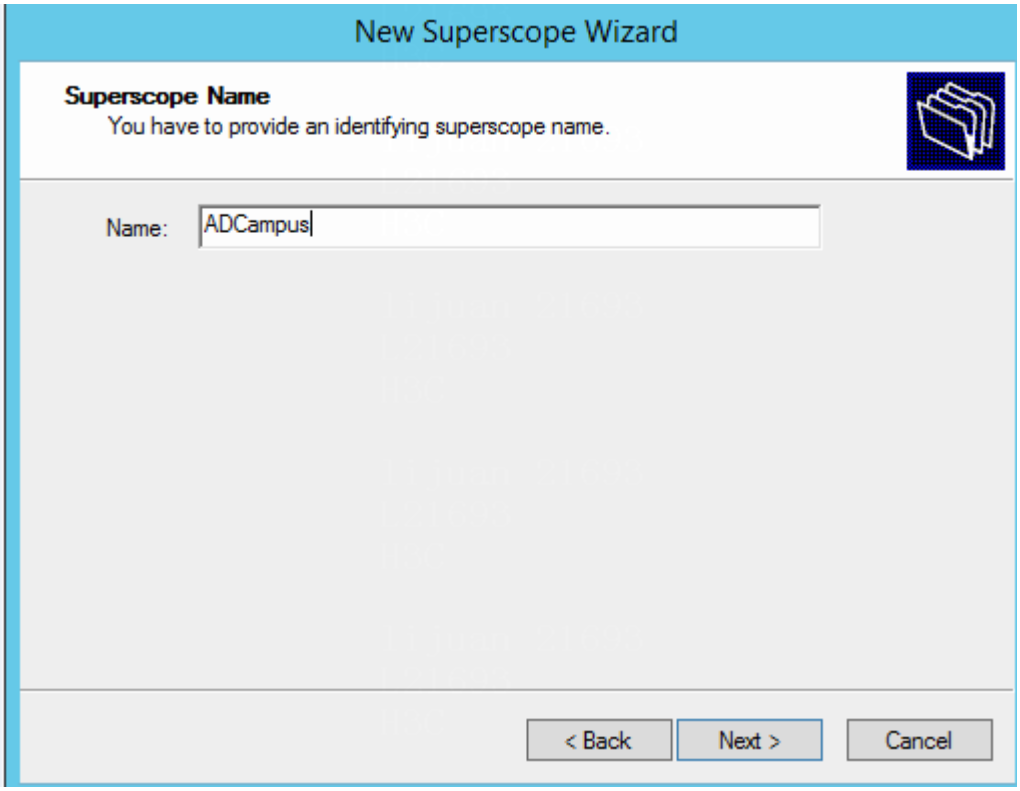


スーパースコープの作成

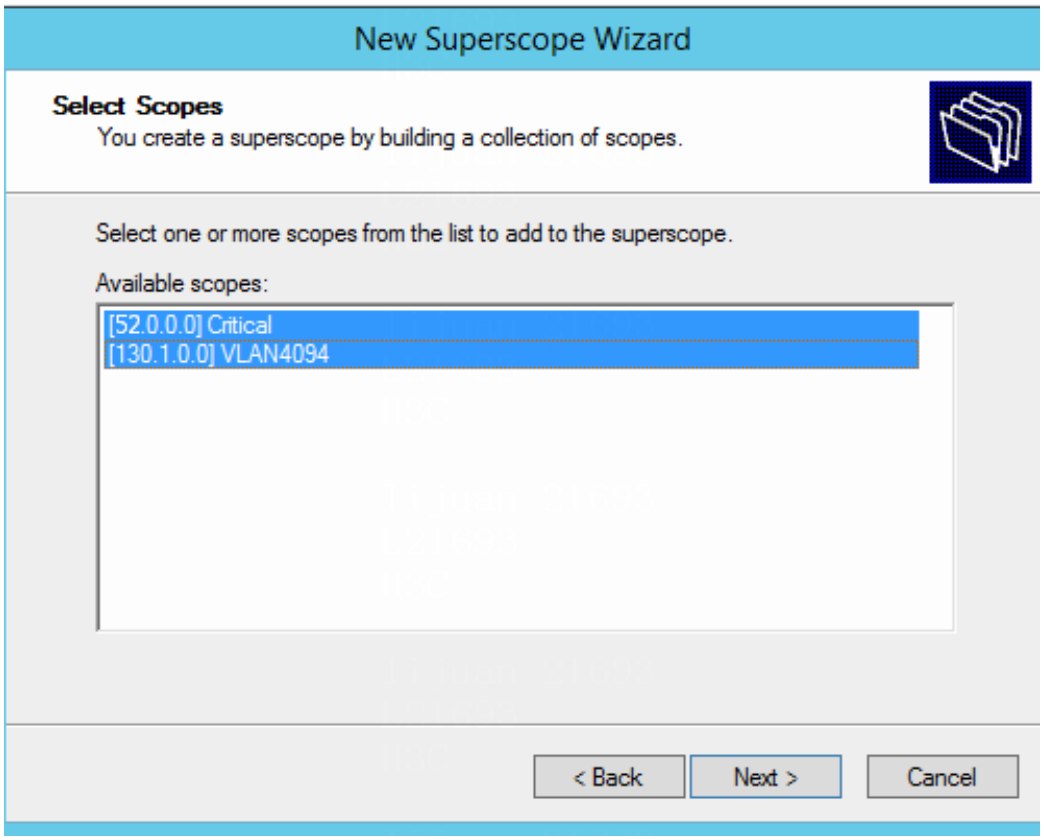
1. 右クリックして **New Superscope** を選択し、**New Superscope Wizard** ページを開きます。



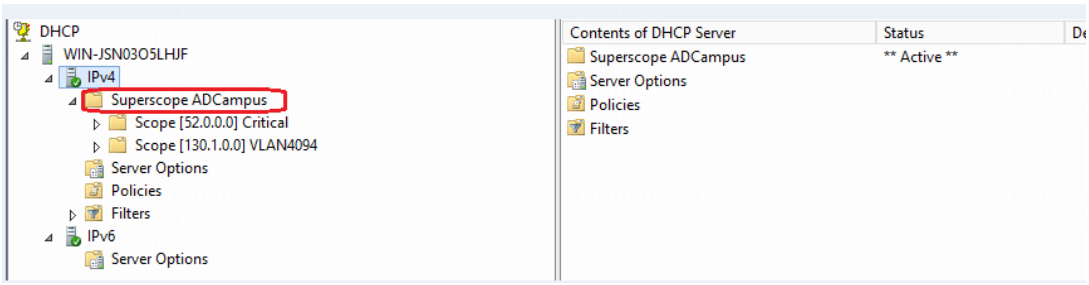
2. **Next** をクリックし、名前を入力します。



3. **Next** をクリックして、**Select Scopes** ページにアクセスします。前に作成した **Critical** セキュリティグループスコープと **VLAN4094** スコープをクリックします。



4. **Next** をクリックして、スーパースコープの構成を完了します。これで、スーパースコープには、前に作成した **Critical** セキュリティグループスコープと **VLAN4094** スコープがすでに含まれていることがわかります。



5. 重要なソリューションのすべての構成が完了しました。将来、EIA サーバーに障害が発生した場合、ユーザーは自動的に重要な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重要なセキュリティグループから IP アドレスを取得します。

IT リソースグループ

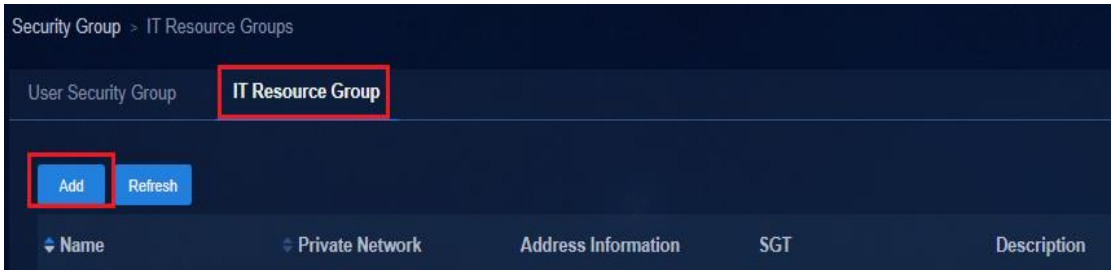
ITリソースグループの作成

IT リソースグループには、セキュリティグループユーザーがアクセスできるネットワークリソースが含まれています。セキュリティグループユーザーの IT リソースグループ内のサーバーリソースへのアクセスは、アクセスポリシーを展開することで制御できます。

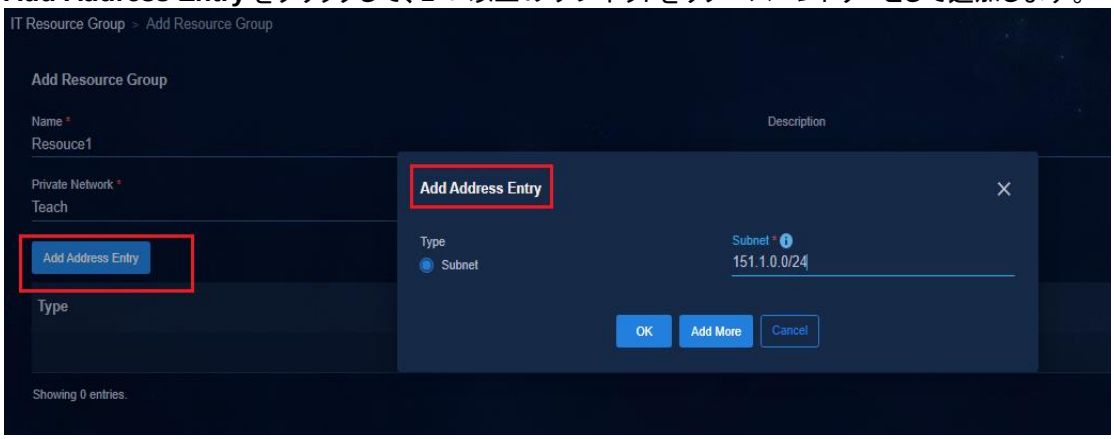
⚠ 警告!

IP アドレスエントリーの数は、IT リソースグループに制限されません。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薦めします。

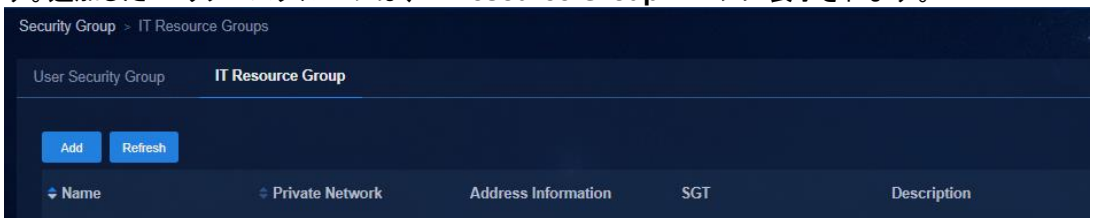
1. **Automation** > **Campus Network** > **Security Group** > **IT Resource Group** ページに移動します。



2. **Add** をクリックし、名前を入力して、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、**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。



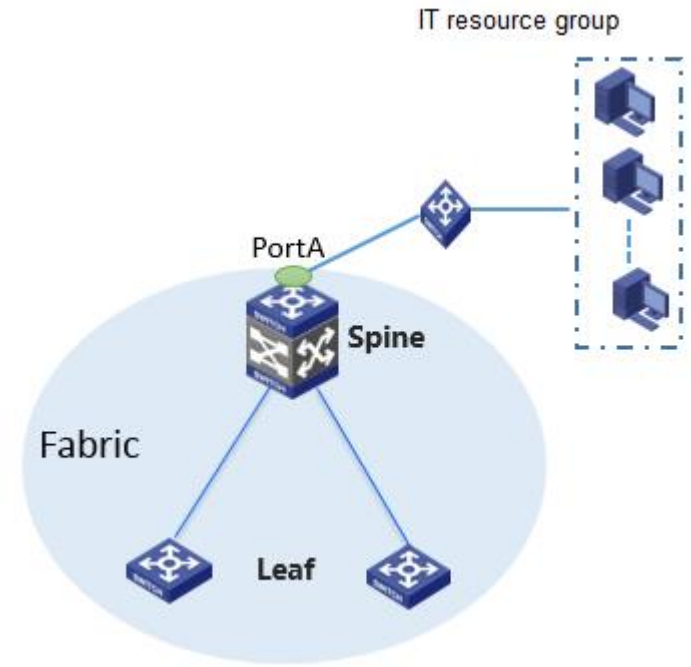
3. **OK** をクリックすると、**Add Resource Group** ページに戻ります。**OK** をクリックして構成を保存します。追加した IT リソースグループは、**IT Resource Group** ページに表示されます。



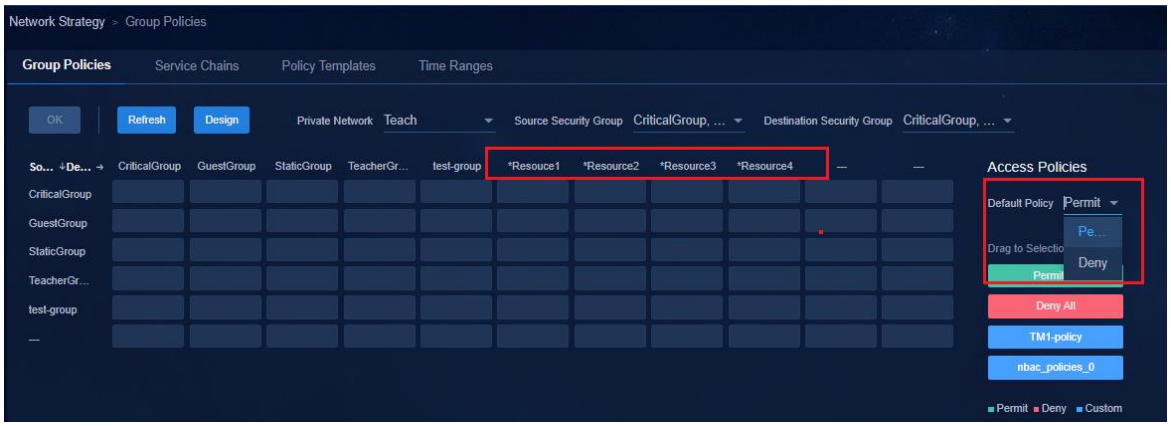
ITリソースグループへのアクセス

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、次の図に示すように、特にネットワーク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** ページで、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** を選択した場合、プライベートネットワーク内のすべてのユーザーは、グループポリシーを構成しなくても、IT リソースグループ内のリソースにアクセスできます。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ポリシーを構成します。
- **Deny** を選択すると、既定では、プライベートネットワーク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なくなります。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、グループ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既定のアクセスポリシー(許可または拒否)に関係なく、IT リソースグループと通信できます。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、拒否モードのグループポリシーを構成して展開します。

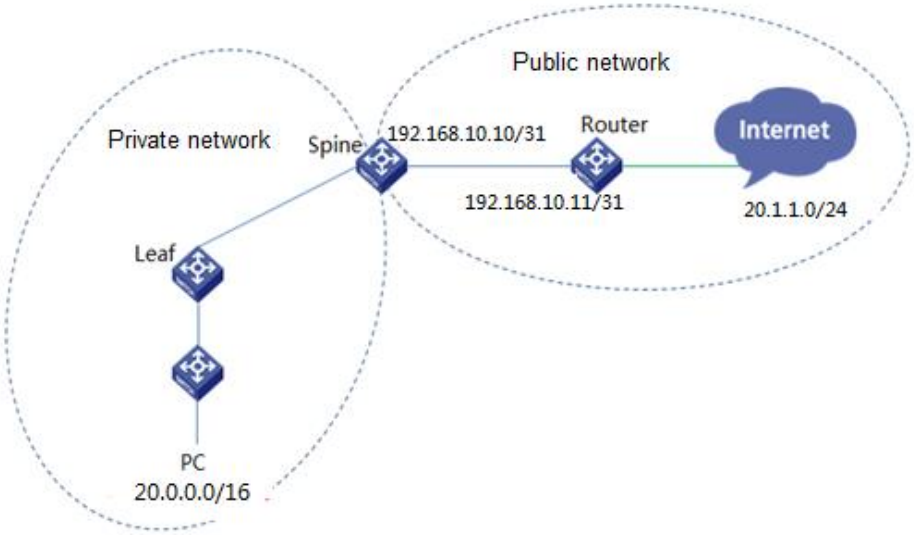
境界デバイスを介した外部ネットワークへのアクセス(シングルスパイン)

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。

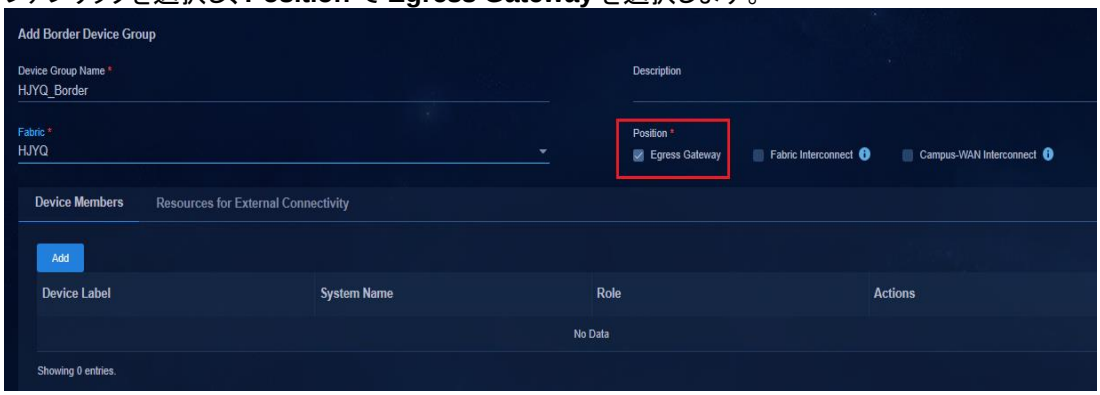
キャンパスネットワークには、1 つまたは複数の VRF を設定できます。この項では、教育ネットワークを例に取り、プライベートネットワーク内のユーザーPC(20.0.0.3)が外部ネットワーク(20.1.1.0/24)にアクセスできるようにするための、コントローラーを介したルート設定と展開について説明します。



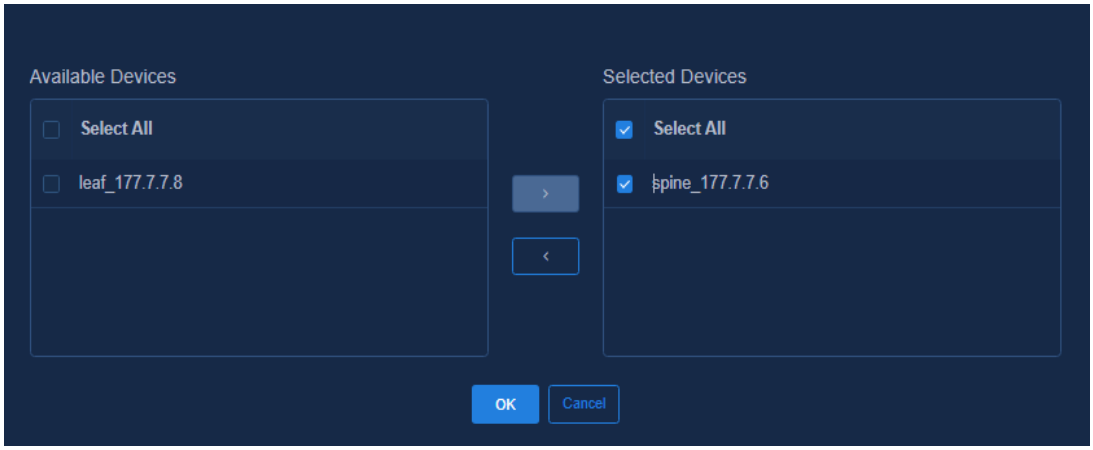
境界デバイスグループの作成

ボーダーデバイスグループを追加するには、**Automation** > **Campus Network** > **Devices** > **Border Device Groups** ページに移動し、**Add** をクリックします。

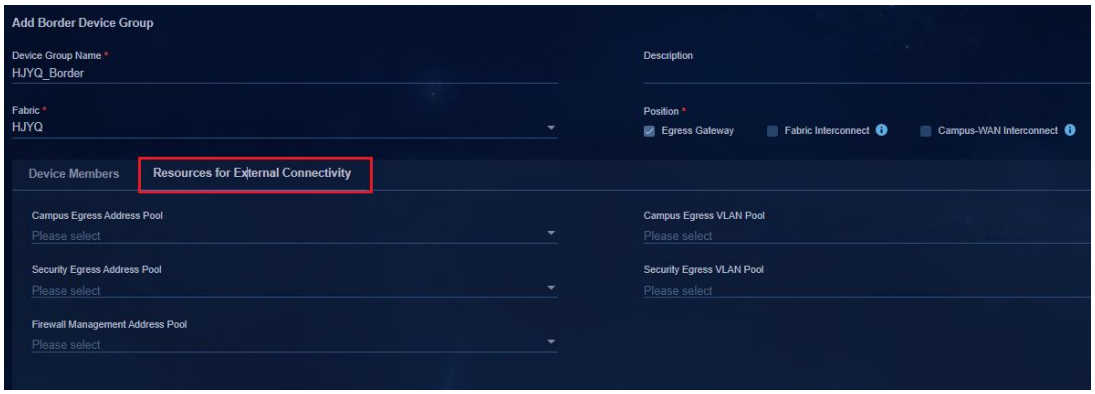
1. ファブリックを選択し、**Position** で **Egress Gateway** を選択します。



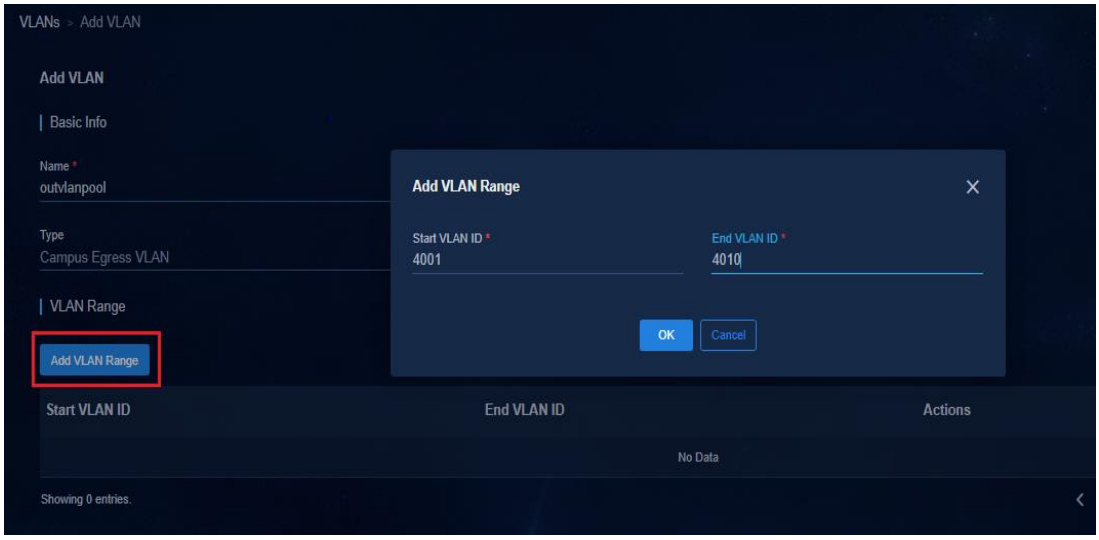
2. **Device Members** タブで、**Add** をクリックします。境界デバイスとしてスパインデバイスまたはリーフデバイスを選択できます。境界デバイスとしてスパインデバイスを選択する例を考えてみます。



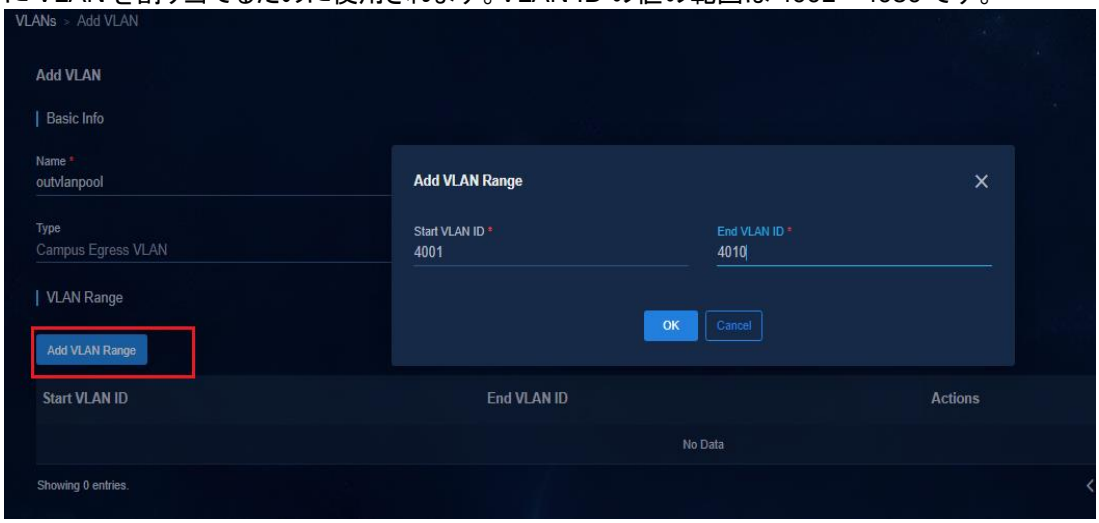
3. 出力ネットワークリソースを設定するには、**Resources for External Connectivity** タブをクリックします。ネットワークリソースの自動割り当てに使用されるアドレスプールと VLAN プールを指定できます。キャンパスが外部ネットワークと通信するときのリソース割り当てには、**Campus Egress Address Pool** 設定と **Campus Egress VLAN Pool** 設定をペアで設定する必要があります。これらの設定を設定しない場合は、『Adding a private network (optional)』で出力ゲートウェイメンバーを追加するときに、**Manual Configuration for Egress Network Resource Allocation Mode** を選択する必要があります。ファイアウォールネットワークリソース割り当ての設定には、**Security Egress Address Pool**、**Security Egress VLAN Pool**、および **Firewall Management Address Pool** 設定が使用されます。詳細については、『AD-Campus 6.2 Security Convergence Configuration Guide』を参照してください。この項では、キャンパス出力ゲートウェイリソースの設定についてのみ



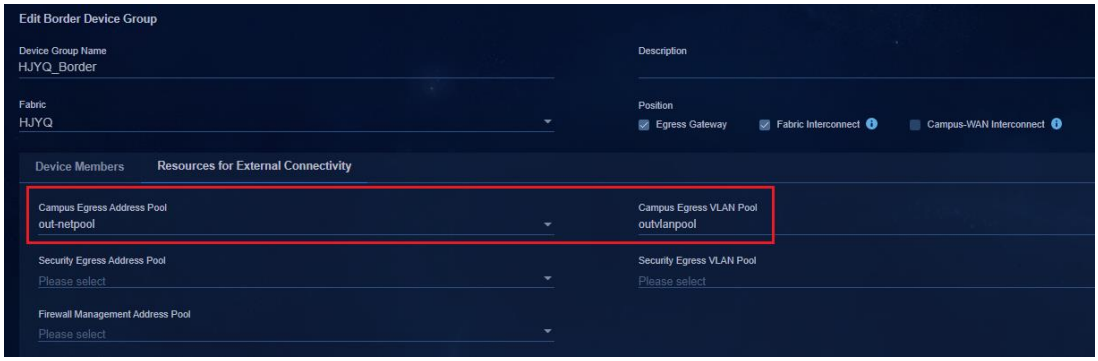
4. **Campus Egress Address Pool** をクリックし、既存のアドレスプールを選択するか、新しいアドレスプールを作成します。新しいキャンパス出力アドレスプールの作成を選択した場合、このキャンパス出力アドレスプールは、ローカルおよびリモート IP アドレスを出力ネットワークリソースに割り当てるために使用され、IPv4 アドレスと IPv6 アドレスの両方をサポートします。



5. **Campus Egress VLAN Pool** をクリックして、既存の VLAN プールを選択するか、新しい VLAN プールを作成します。新しいキャンパス出力 VLAN プールの作成を選択した場合、このキャンパス出力 VLAN プールは、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使用されます。VLAN ID の値の範囲は 4001～4050 です。

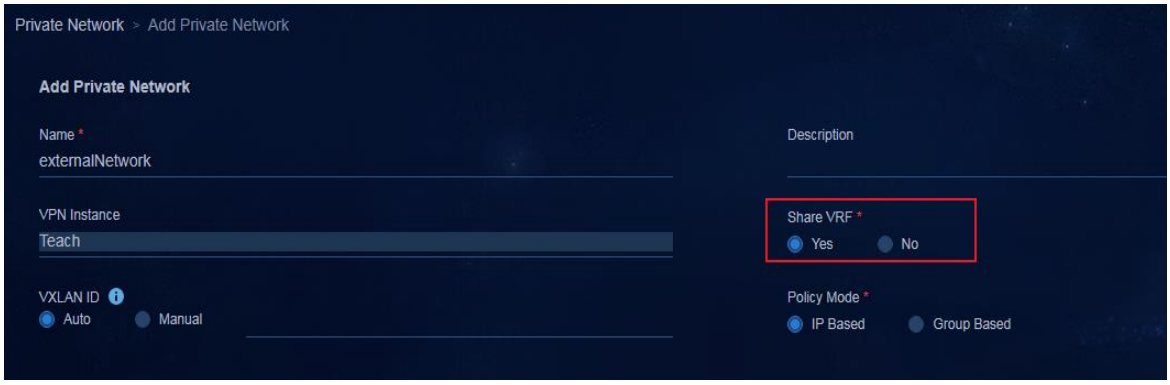


6. 出力ネットワークリソースの設定が完了したら、**OK** をクリックします。その後、作成した境界デバイスグループを境界デバイスグループリストに表示できます。



プライベートネットワークの追加(オプション)

出力ゲートウェイのプライベートネットワークを追加するときに、VRF 共有をイネーブルにします。VRF 共有をイネーブルにするには、**Automation** > **Campus Network** > **Private Network** ページに移動し、**Share VRF** を **Yes** に設定します。



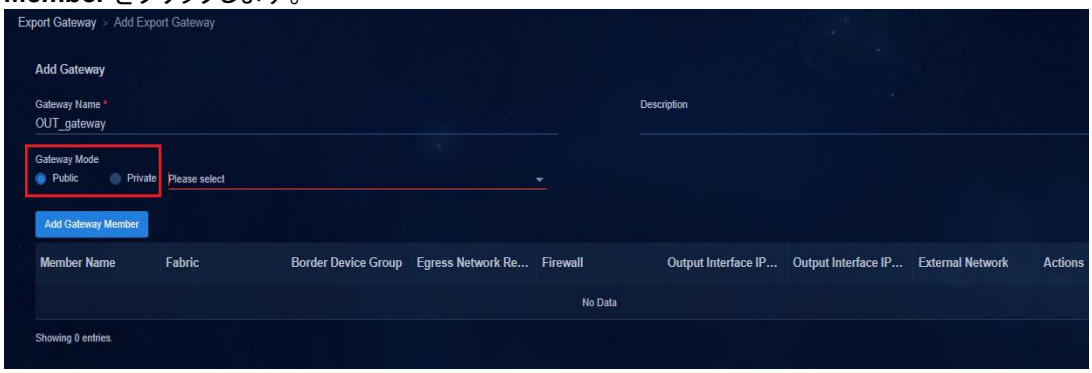
出力ゲートウェイの追加

出力ゲートウェイを追加する場合は、必要に応じてゲートウェイモードを選択します。パブリックゲートウェイを選択する場合は、VRF を指定する必要があります。ゲートウェイメンバーを追加する場合は、以前に作成したボーダーデバイスグループを選択します。

- **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。パブリックゲートウェイが設定されている場合は、『Adding a private network (optional)』でパブリックゲートウェイが使用するネットワークを選択するか、パブリックゲートウェイの VRF を手動で追加できます。
- **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だけで使用できます。

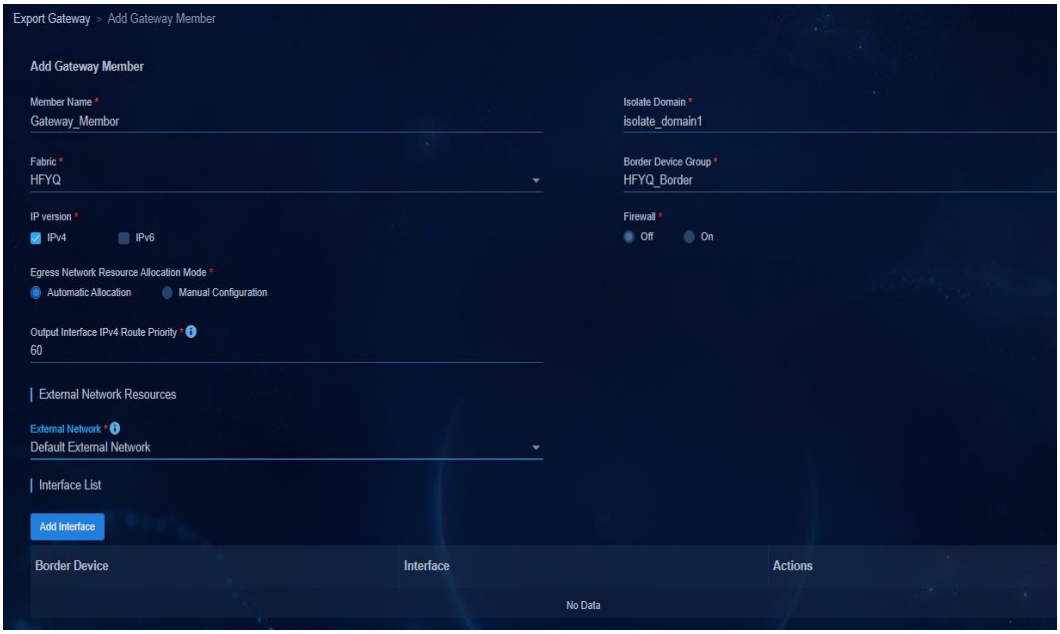
Automation > **Campus Network** > **Private Network** > **Export Gateway** ページに移動します。

1. **Add** をクリックして **Add Gateway** ページを開き、**Gateway Mode** を構成します。**Add Gateway Member** をクリックします。

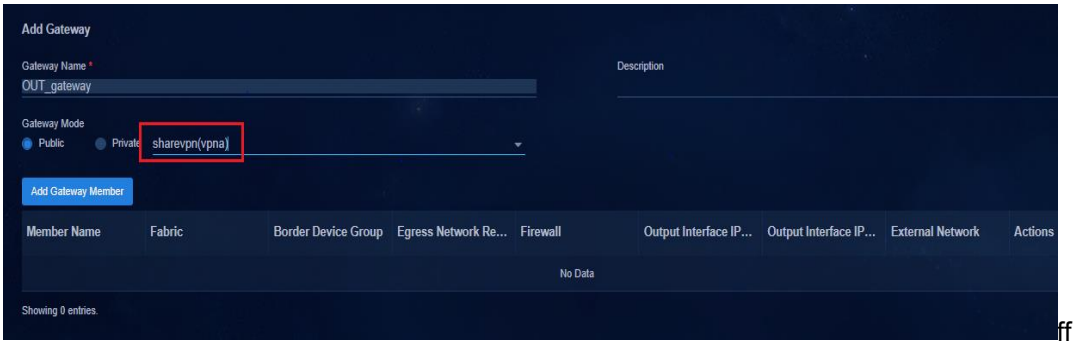


2. 表示されたページで、**Isolation Domain**, **Fabric**, **Border Device Group** および **IP version**,を選択し、**Egress Network Resource Allocation Mode を Automatic Allocation** または **Manual Allocation** に設定します。**Output Interface IPv4 Route Priority** のデフォルト値は 60 に設定されています。必要に応じて設定できます。値が小さいほど、優先度が高くなります。

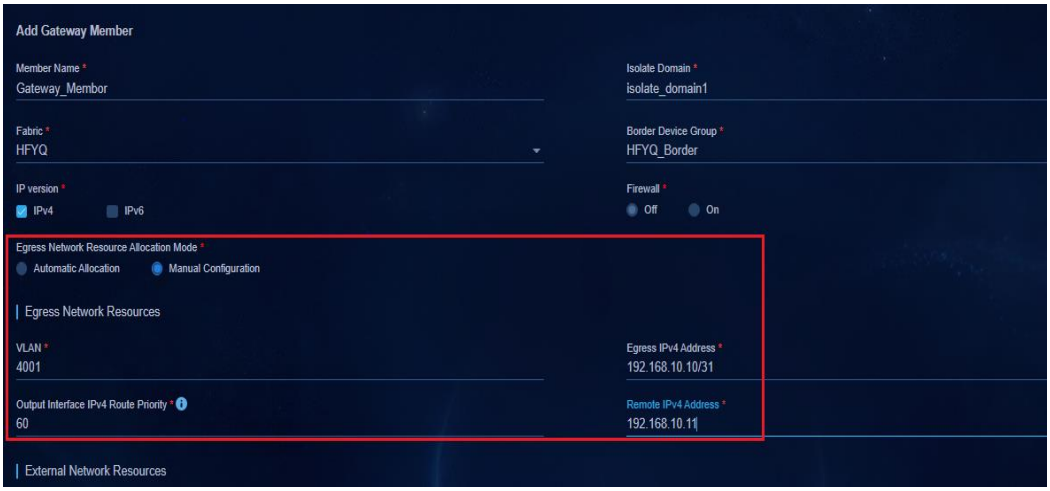
   - **Automatic Allocation** を選択すると、『Creating a border device group』で設定されている設定に従って、VLAN、出力ネットワークセグメント、およびリモートネットワークセグメントがボーダーデバイスに自動的に割り当てられます。



   - **Manual Configuration** を選択する場合は、境界デバイスと出力ネットワークを選択し、**VLAN**, **Egress IPv4 Address**,、およびリモート IPv4 アドレスを手動で設定する必要があります。**Remote IPv4 Address** は、出力 IPv4 アドレスと同じネットワークセグメントにある必要があります。



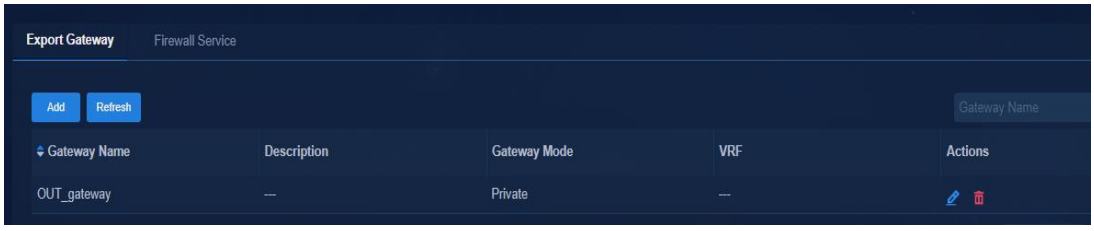
ff



- 外部ネットワークリソースを選択します。出力ネットワークがアクセスできるリソースを指定できます。
- インターフェイスを選択します。出力インターフェイスは、ボーダーデバイスを外部ルートデバイスに接続するインターフェイスです。

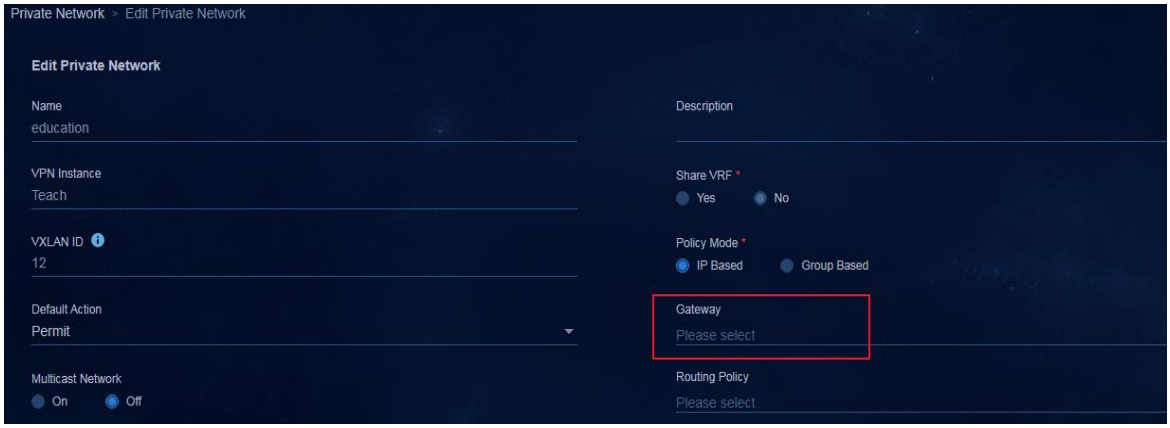
3. **OK** をクリックすると、**Add Gateway** ページに戻ります。ゲートウェイメンバーの Actions 列にある **Details** アイコンをクリックして、ボーダーデバイスと外部デバイス間の通信に関する VLAN およびネットワークセグメント情報を表示します。

4. **OK** をクリックして設定を保存します。次に、作成した出力ゲートウェイを **Export Gateway** リストに表示できます。



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

Automation > **Campus Network** > **Private Network** > **Private Network** ページに移動し、プライベートネットワークの **Actions** カラムにある **Edit** アイコンをクリックします。外部ネットワークと通信する必要があ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。



デバイスに展開された出力ゲートウェイ設定の表示

スパインデバイス上のコントローラー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。

パブリックゲートウェイモード用に展開された設定

- VLAN 設定:

```
#
vlan 4001
#
```

- VLAN インターフェイス設定:

```
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance VPN1      //Instance name of the public gateway.
 ip address 192.168.10.10 255,255,255,254
#
```

- VPN インスタンス設定:

```
#
ip vpn-instance VPN1
 description SDN_VRF_fc248f21-f522-42b0-9882-cea78ee24a1dVPN1
 #
 address-family ipv4
  route-replicate from vpn-instance Teach protocol direct
  route-replicate from vpn-instance Teach protocol bgp 100
#
```

- 出力ゲートウェイの VPN インスタンスのルート再配布設定。

```
#
bgp 100
#
 ip vpn-instance Teach
  #
  address-family ipv4 unicast
   default-route imported
   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
#
```

- スタティックルート設定(ネクストホップとしてリモート VLAN インターフェイス 4001 のアドレスを使用):

```
#
ip route-static vpn-instance Teach 0.0.0.0 0 vpn-instance VPN1 192.168.10.11 de
scription SDN_ROUTE
#
```

プライベートゲートウェイモード用に展開された設定

- キャンパス出力 VLAN:

```
#
vlan 4001
#
```

- ACL ルール設定:

```
#
acl advanced name SDN_ACL_SC_PERMIT_ALL
 description SDN_ACL_SC_PERMIT_ALL
 rule 0 permit ip
#
```

- キャンパス出力 VLAN に基づく PBR ポリシー設定:

```
#
policy-based-route SDN_SC_VLAN_4001 permit node 65535
 if-match acl name SDN_ACL_SC_PERMIT_ALL
#
```

- VLAN インターフェイス設定:

```
#
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance Teach
 ip address 192.168.10.10 255,255,255,254
 ip policy-based-route SDN_SC_VLAN_4001        Apply the PBR policy.
#
```

- BGP へのデフォルトおよびスタティックルートの再配布:

```
#
bgp 100
 non-stop-routing
```

```
 router-id 200.1.1.254
 peer 200.1.1.251 as-number 100
 peer 200.1.1.251 connect-interface LoopBack0
 peer 200.1.1.252 as-number 100
 peer 200.1.1.252 connect-interface LoopBack0
#
 address-family l2vpn evpn
  peer 200.1.1.251 enable
  peer 200.1.1.251 reflect-client
  peer 200.1.1.252 enable
  peer 200.1.1.252 next-hop-local
  peer 200.1.1.252 reflect-client

 #
 ip vpn-instance Teach
  #
  address-family ipv4 unicast
   default-route imported
   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
   network 40.0.0.0 255.255.0.0
   network 40.0.0.1 255.255.255.255
  #
---- More ----
#
```

- スタティックルート設定(ネクストホップとしてリモート VLAN インターフェイス 4001 のアドレスを使用):

```
ip route-static vpn-instance Teach 0.0.0.0 0 192.168.10.11 description SDN_ROUTE
```

境界デバイス上の外部ネットワークに接続されたインターフェイスに展開された設定

```
#
interface Ten-GigabitEthernet2/2/0/36
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
#
```

境界デバイスに接続されたL3デバイスの手動設定

```
#
vlan 4001       //VLAN in egress gateway details.
#
#
```

```
interface Ten-GigabitEthernet1/0/9
port link-type trunk
port trunk permit vlan 4001
#
```
Configure an IP address for communicating with the border device. //Remote IPv4 address in egress gateway details.
```
interface Vlan-interface 4001
ip address 192.168.10.11 255.255.0.0
#
```
Configure a default route to interoperate with the private network and the next hop is the gateway address of the external network.
```
ip route-static 0.0.0.0 0 20.1.1.1
#
```
The route from the public network to the private network needs to be configured for each network segment that communicates with the public network, and the next hop is the border device.
```
#
ip route-static 20.0.0.0 16 192.168.10.10
ip route-static 30.0.0.0 16 192.168.10.10
#
```

ボーダーデバイスと外部ルートデバイスの関連付け(デュアルボーダー)

現在のバージョンでは、コントローラーはデュアルボーダー出力の自動展開をサポートしていません。2 つのボーダーデバイスを手動で設定する必要があります。この項では、デュアルボーダーデバイスの設定について説明します。

border 1の設定

- パブリック出力用の VPN 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  //Replicate the VPN routes and repeat this command if multiple private networks exist.
  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の出力と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    //Bind VPNa of the public gateway.
 ip address 192.168.10.10 255,255,255,250
#
```

- L3 デバイスに接続されているインターフェイスを VLAN 4001 に割り当てます。

```
#
interface Ten-GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 4001
#
```

- ルートをインポートするように BGP を設定します。

```
#
bgp 100
#
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   default-route imported     //Import default routes.
   preference 240 240 130
   import-route static  //Import static routes.
   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    //Bind VPNa of the public gateway.
 ip address 192.168.10.12 255,255,255,250
#
```

- 他の境界デバイスに接続されているインターフェイスを VLAN 4002 に割り当てます。

```
#
interface Ten-GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 4002
#
```

- NQA と追跡の設定を行います。

#NQA オペレーション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  //admin is the username and configure it the same as the username configured when a local user is created.
type icmp-echo
destination ip 192.168.10.11  //The destination IP is the IP address of VLAN-interface 4001 on the L3 device.
frequency 100
reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna  //VPN bound to VLAN-interface 4001.
#
# Enable the NQA operation.
nqa schedule admin border1 start-time now lifetime forever
#
# Associate an NQA operation with the links between border devices.
nqa entry admin border2  //admin is the username and configure it the same as the username configured when a local user is created.
type icmp-echo
destination ip 192.168.11.11  //The destination IP is the IP address of VLAN-interface 4002 on the L3 device.
frequency 100
reaction 2 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna  //VPN bound to VLAN-interface 4002.
#
# Enable the NQA operation.
nqa schedule admin border2 start-time now lifetime forever
#
# Configure track-NQA collaboration.
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 vpn1 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、トラックエントリーをスタティックルートに関連付けます。

```
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.10.11 track
1
#
# Configure a backup static route from VPN vpn1 to the public network. The next hop of the backup route is border 2.
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.11.11 track
2 preference 61
#
# Configure a static route to forward the packets from border 2 to border 1 to the public network.
ip route-static vpn-instance vpna 0.0.0.0 0 192.168.10.11
#
```

border 2の設定

- 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  //Replicate the routes of VPN vpn1.
  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    //Bind VPNa of the public gateway.
 ip address 192.168.11.10 255,255,255,250
#
```

- L3 デバイスに接続されているインターフェイスを VLAN 4002 に割り当てます。

```
#
interface Ten-GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 4002
#
```

- ルートをインポートするように BGP を設定します。

```
#
bgp 100
```

```
#
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   default-route imported     //Import default routes.
   preference 240 240 130
   import-route static   //Import static routes.
   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 4001 を設定します。

```
#
interface Vlan-interface4001
 description to_border1_Interface_4001
 ip binding vpn-instance VPNa    //Bind VPNa of the public gateway.
 ip address 192.168.10.12 255,255,255,250
#
```

- 他の境界デバイスに接続されているインターフェイスを VLAN 3 に割り当てます。

```
#
interface Ten-GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 4001
#
```

- NQA と追跡の設定を行います。

#NQA オペレーション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  //admin is the username and configure it the same as the username configured when a local user is created.
type icmp-echo
destination ip 192.168.11.11  //The destination IP is the IP address of VLAN-interface 4002 on the L3 device.
frequency 100
reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
vpn-instance vpna  //VPN bound to VLAN-interface 4002.
#
# Enable the NQA operation.
nqa schedule admin border2 start-time now lifetime forever
#
# Associate an NQA operation with the links between border devices.
nqa entry admin border1 //admin is the username and configure it the same as the username configured when a local user is created.
type icmp-echo
destination ip 192.168.10.11  //The destination IP is the IP address of VLAN-interface 4001 on the L3 device.
frequency 100
```

```
reaction 2 checked-element probe-fail threshold-type consecutive 3 action-type
trigger-only
vpn-instance vpna  //VPN bound to VLAN-interface 4001.
#
# Enable the NQA operation.
nqa schedule admin border1 start-time now lifetime forever
#
# Configure track-NQA collaboration.
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 vpn1 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、トラックエントリーをスタティックルートに関連付けます。

```
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.11.11 track
1
#
# Configure a backup static route from VPN vpn1 to the public network. The next hop of the backup route is border 2.
ip route-static vpn-instance vpn1 0.0.0.0 0 vpn-instance vpna 192.168.10.11 track
2 preference 61
#
# Configure a static route to forward the packets from border 1 to border 2 to the public network.
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デバイスの設定

- 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 に接続されているインターフェイスを VLAN 4001 に割り当てます。

```
#
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を VLAN 4002 に割り当てます。

```
#
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。

#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。ネクストホップはパブリックネットワークゲートウェイです。

```
ip route-static 0.0.0.0 0 21.1.0.1
#
```

Configure static routes from the public network to each private network that will communicate with the public network. The next hops of these routes are border 1 and border 2.

```
#
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
#
```

マルチキャスト設定

コントローラーとデバイスの両方が、レイヤー2 マルチキャストとレイヤー3 マルチキャストの設定をサポートしています。これにより、単一ポイントから複数ポイントへのトラフィックの伝送が可能になります。

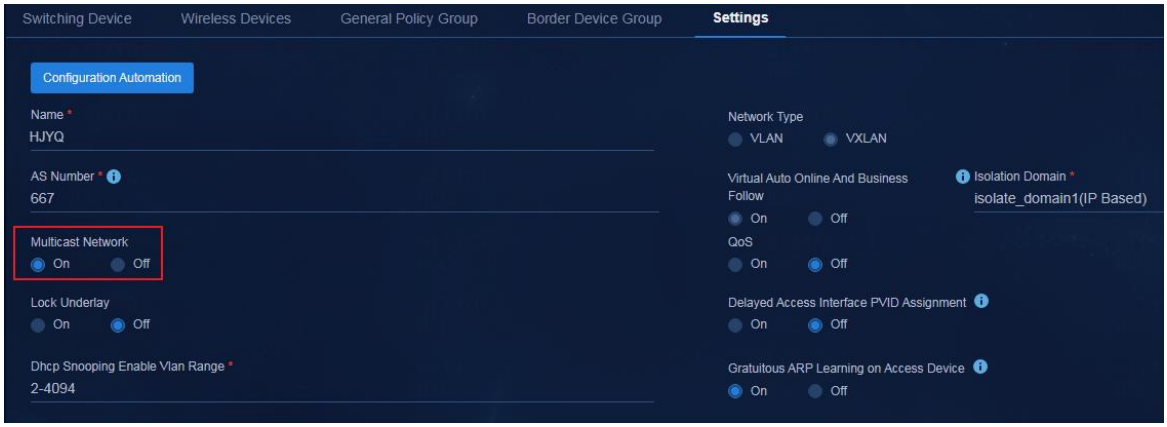
マルチキャストサービスコンフィギュレーション

レイヤー2 マルチキャスト

レイヤー2 マルチキャストのグローバルなイネーブル化

レイヤー2 マルチキャストネットワークを設定するには、マルチキャストをグローバルにイネーブルにし、**Multicast Network** を **On** に設定する必要があります。

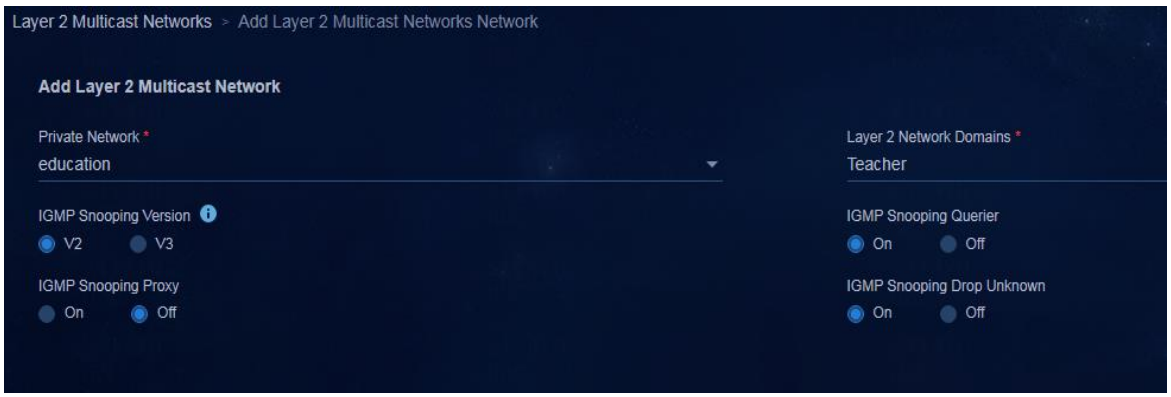
Automation > **Campus Network** > **Fabrics** ページに移動し、ファブリックの **Actions** カラムにある Settings アイコンをクリックします。**Settings** タブをクリックし、Multicast Network で **On** を選択し、**OK** をクリックして設定を保存します。次に、IGMP スヌーピング設定がファブリック内のスパインデバイスとリーフデバイスにグローバルに展開されます。



マルチキャストサービスの設定

必要に応じて、マルチキャストサービスを設定できます。

Automation > **Campus Network** > **Application Policy** > **Multicast** > **Layer 2 Multicast** ページに移動し、**Add** をクリックします。次に、必要に応じてマルチキャストサービスを設定します。



パラメーター:

- **Private Network**: マルチキャストをイネーブルにする必要があるプライベートネットワークを選択します。
- **Layer 2 Network Domain**: マルチキャストをイネーブルにする必要があるレイヤー2 ネットワークドメインを選択します。マルチキャストがイネーブルの場合、IGMP スヌーピングはレイヤー2 ネットワークドメインの対応する VSI で自動的にイネーブルになります。
- **IGMP Snooping Version**: IGMP スヌーピングバージョンを選択します。
- **IGMP Snooping Querier**:この機能をイネーブルにすると、スパインデバイスのレイヤー2 ネットワークドメインに対応する VSI でクエリア機能が自動的に設定されます。実際の環境に別のレイヤー3 マルチキャストデバイスまたはクエリアがある場合、この機能はオプションです。
- **IGMP Snooping Proxy**: リーフデバイスで IGMP スヌーピングプロキシをイネーブルにして、ダウンストリームホストに代わってレポートを送信し、アップストリームデバイスにパケットを残します。この機能により、アップストリームデバイスで受信される IGMP レポートおよび Leave パケットの数を減らすことができます。
- **IGMP Snooping Drop Unknown**: この機能により、レイヤー2 デバイスは、不明なマルチキャストデータパケットを VXLAN でフラッディングするのではなく、ルータポートにだけ転送できます。デバイスにルータポートがない場合、不明なマルチキャストデータパケットはドロップされます。

VSI の設定は、次の方法で表示できます。

```
[Leaf7503-vsi-vsi3]display this
#
vsi vsi3
 description SDN_VSI_3
 gateway vsi-interface 3
 statistics enable
 ipv6 nd snooping enable global
 ipv6 nd snooping enable link-local
 flooding disable all all-direction
 vxlan 3
 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
 igmp-snooping enable
 igmp-snooping drop-unknown     //Discard unknown multicast data packets.
 dhcp snooping binding record
 ipv6 dhcp snooping binding record
#
```

スパインデバイスでの AC インターフェイスの設定

スパインデバイスが出力ルータに接続し、マルチキャストパケットが VLAN を介して VXLAN にマッピングされるインターフェイスで、スタティック AC を設定します。

1. レイヤー2 ネットワークドメインを設定したら、**Automation** > **Campus Network** > **Fabrics** ページに移動し、ファブリックの **Actions** カラムにある **Settings** アイコンをクリックします。
2. **General Policy Groups** タブをクリックし、**AP Non-Direct Access Interface Group for Leafs** の **Actions** カラムにある **Edit** アイコンをクリックします。

3. **Member** タブを選択し、**Add** をクリックして、**AP Non-Direct Access Interface Group for Leaf** にインターフェイスを追加します。コントローラーは、セキュリティグループに対応するイーサネットサービスインスタンスを自動的に配信します。

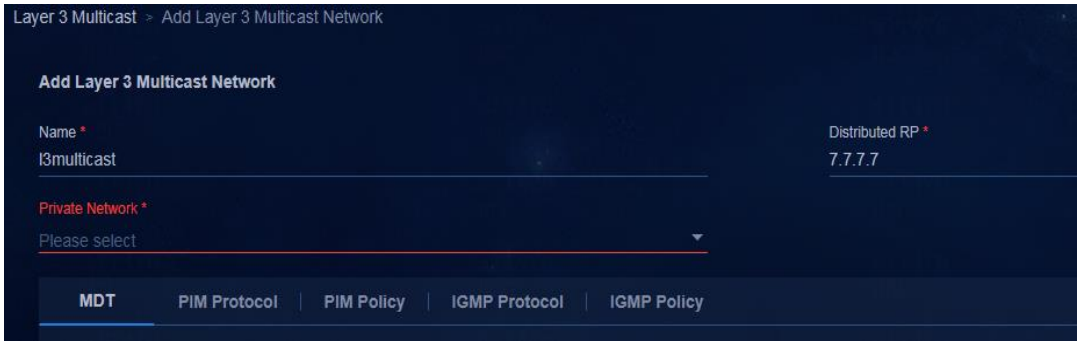
設定が完了し、エンドポイントがマルチキャストグループに加入すると、エンドポイントはマルチキャスト送信元からのマルチキャストトラフィックを正常に受信できます。

レイヤー3 マルチキャスト

プライベートネットワークをレイヤー3 マルチキャストネットワークにバインドし、RP アドレス、MDT、PIM プロトコルとポリシー、および IGMP プロトコルとポリシーを設定することで、レイヤー3 マルチキャストトラフィックを同じ VPN で交換できます。

レイヤー3 マルチキャストは、レイヤー2 マルチキャストに基づいています。次の設定が必要です。

1. **Automation** > **Campus Network** > **Application Policy** > **Multicast** > **Layer 3 Multicast** ページに移動します。
2. **Add** をクリックし、次のパラメーターを設定します。
   - **Name**: レイヤー3 マルチキャストネットワークの名前を入力します。
   - **Distributed RP**: EVPN VXLAN ネットワーキングでは、マルチキャストが PIM-SM モードを採用している場合、ネットワーク内の各リーフデバイスは、マルチキャストデータ転送用のプライベートネットワークの RP として機能します。
   - **Private Network**: 設定を展開するプライベートネットワークをバインドします。



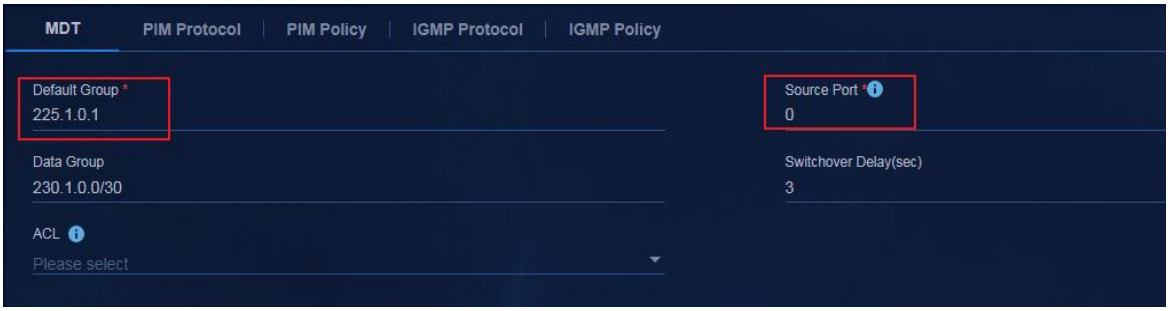
次の設定がリーフデバイスに展開されたことを確認できます。

```
#
pim vpn-instance Teach      //Corresponding private network instance.
 c-bsr 7.7.7.7
 c-rp 7.7.7.7
#
```

MDT タブ

MDT タブでは、デフォルトグループ、送信元ポート、データグループなどのパラメーターを指定できます。データグループマスクの値の範囲は、デバイスモデルによって異なります。

- **Default Group**: デフォルトグループは、パブリックネットワーク上のマルチキャスト VPN によって割り当てられた独立したマルチキャストグループであり、パブリックネットワーク上でプライベートマルチキャストデータの送信を実現するために使用されます。
- **Source Port**: MVXLAN 送信元インターフェイスを指定します。MVXLAN 送信元インターフェイスは、BGP ピア関係を確立するために使用される送信元インターフェイスと同じである必要があります。そうでない場合、正しいルーティング情報を取得できません。現在、指定できるのはループバックインターフェイスだけです。
- **Data Group**: このパラメーターが設定されている場合、デバイスはデータグループから最も参照されていないアドレスを選択してデフォルトグループを置き換え、パブリックネットワーク上でプライベートマルチキャストデータの送信をイネーブルにします。
- **ACL**: データグループが構成されている場合にのみ構成します。ACL が構成されている場合、ACL に一致するトラフィックのみがデータグループを使用してパブリックネットワーク上で送信されます。ACL に一致しないトラフィックは、デフォルトグループを使用してパブリックネットワーク上で送信されます。
- **SwitchOver Delay(sec)**: デフォルトグループからデータグループへの切り替えの遅延時間。データグループが設定されている場合にだけ設定できます。



デバイスでは、次の設定を表示できます。

```
[Spine10510]multicast-vpn vxlan vpn-instance Teach mode mdt
[Spine10510-mvxlan-vpn-instance-Teach]dis this
#
multicast-vpn vxlan vpn-instance Teach mode mdt  //
  address-family ipv4
  source LoopBack0                      //Source interface.
  default-group 225.1.0.1                 //Default group IP.
data-group 230.1.0.0 255.255.255.252 name SDN_ACL_MULTICAST_test //Deployed only when the data group and ACL have been configured.
data-delay 3
#
```

PIM protocol タブ

- **Protocol Type**: オプションには、**PIM-SM** および **PIM-SSM** が含まれます。

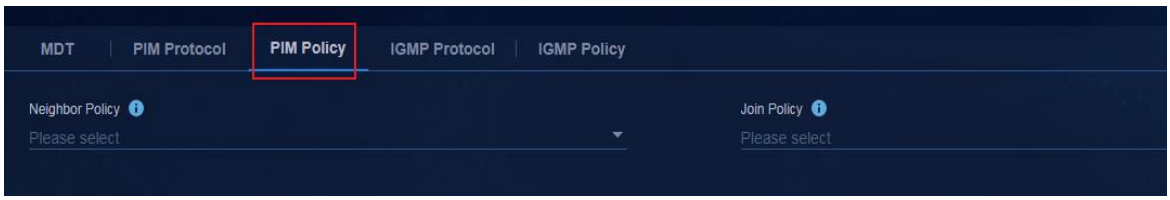
- **Hello Interval(sec)**: このパラメーターを設定すると、デバイス上で PIM プロトコルを実行している各インターフェイスは、このセグメント内のすべての PIM デバイスに hello パケットを定期的に送信して、PIM ネイバーを検出し、デバイス間の PIM ネイバー関係を維持します。

デバイスでは、次の設定を表示できます。

```
[Leaf7503]int Vsi-interface 3       //The VSI interface enabled in the Layer 2 network domain.
[Leaf7503-Vsi-interface3]dis th
#
interface Vsi-interface3
 description SDN_VSI_Interface_3
 ip binding vpn-instance Teach
 ip address 20.0.0.1 255.255.0.0
 pim sm                                          //Protocol mode.
 pim hello-option holdtime 105
 pim hello-option lan-delay 500
 pim hello-option override-interval 2500
 pim holdtime join-prune 210
 pim timer hello 30                              //Hello packet sending frequency.
 pim timer join-prune 60
 pim distributed-dr
#
```

PIM policy タブ

- **Neighbor Policy**: ネイバーポリシーを設定することで、PIM ドメインのセキュリティと通常のトラフィック転送を確保します。
- **Join Policy**: Join policy を設定することで、不正なデバイスが PIM ドメインに加入するのを防ぐことができます。



IGMP プロトコルタブ

- **IGMP Version**: IGMP プロトコルには、IGMPv1、IGMPv2、および IGMPv3 の 3 つのバージョンがあります。
- **SSM Mapping**: IGMPv1 および IGMPv2 を使用する PIM-SSM モードが選択されている場合、IGMPv1 および IGMPv2 はマルチキャストグループに加入するマルチキャストレシーバをサポートし

ないため、完全な PIM-SSM モードマルチキャスト転送を実現するには、デバイス上で SSM スタティックマッピングルールを設定する必要があります。

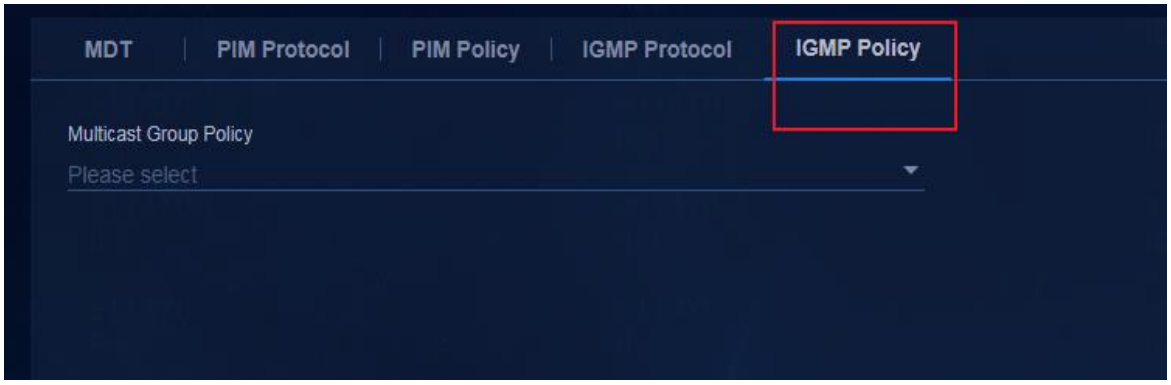
- **Querier's Robustness Variable**: クエリアのロバスト性変数は、起こり得るネットワークパケット損失を補償するために設定されたパケット再送信の数である。

マルチキャストネットワークがイネーブルになっている VSI インターフェイスでは、次の設定を表示できます。

```
[Leaf7503]int Vsi-interface 3      //The VSI interface enabled with multicast in the Layer 2 network domain.
[Leaf7503-Vsi-interface3]display this
#
interface Vsi-interface3
 description SDN_VSI_Interface_3
 ip binding vpn-instance Teach
 ip address 20.0.0.1 255.255.0.0
 pim sm
 pim hello-option holdtime 105
 pim hello-option lan-delay 500
 pim hello-option override-interval 2500
 pim holdtime join-prune 210
 pim timer hello 30
 pim timer join-prune 60
 pim distributed-dr
igmp enable
 igmp other-querier-present-interval 255
 igmp query-interval 125
 igmp max-response-time 10
 igmp robust-count 2
 igmp last-member-query-interval 1
#
```

IGMP policy タブ

Multicast Group Policy: インターフェイス上でマルチキャストグループフィルタを設定して、そのインターフェイス上のホストが加入できるマルチキャストグループを制限します。



プロトコル固有のマルチキャストパケットフィルタリング

特定のプロトコルマルチキャストパケットがデバイスに与えるトラフィックへの影響を回避するには、デバイス上の特定のマルチキャストグループアドレスを除外します。

```
#
acl number 3000
rule 0 deny ip destination 239.255.255.250 0
rule 5 permit ip
#
# Configure a source policy in PIM view.
#
pim vpn-instance Teach
source-policy 3000
#
```

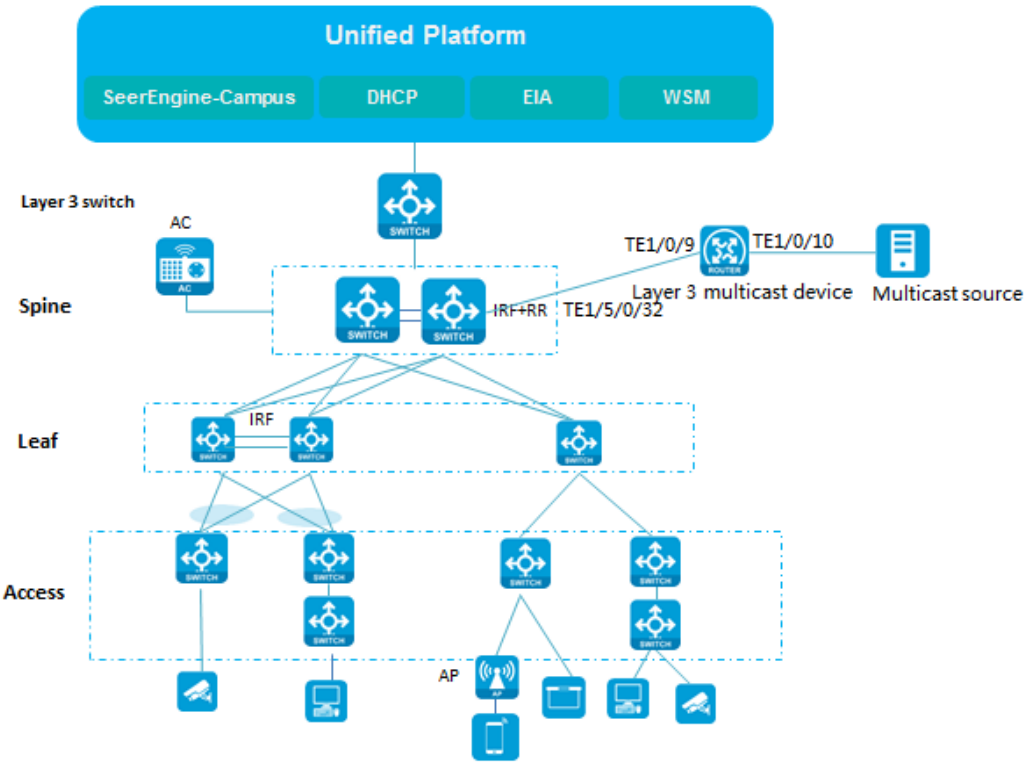
上記のすべての設定が完了すると、レイヤー3 マルチキャストトラフィックを同じ VPN インスタンスで送信できます。

警告!

1 つのレイヤー3 マルチキャストネットワークにバインドできるプライベートネットワークは 1 つだけです。

スパインがルータ経由でマルチキャスト送信元に接続されている場合のマルチキャストサービスの設定

マルチキャスト送信元が外部ルータを介してスパインに接続されている場合、次の図に示すように、レイヤー3 マルチキャストトラフィックを送信するように外部ルータを設定する必要があります。



出力ゲートウェイの設定

マルチキャストサービスに関連する設定を行う前に、出力ゲートウェイを設定する必要があります。出力ゲートウェイの設定については、『Creating a border device group』、『Adding an egress gateway』、および『Viewing egress gateway configuration deployed to device』を参照してください。レイヤー3 マルチキャストデバイスは、ボーダーデバイスに接続された外部ルートデバイスとして機能します。

⚠ 警告!

マルチキャストシナリオで出力ゲートウェイを使用する場合は、エクスクルーシブゲートウェイを選択します。

境界と外部ネットワーク間の接続のためのインターフェイスの手動設定

```
#
interface Ten-GigabitEthernet2/2/0/36
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all  //Configuration deployed when the output interface is configured in the egress gateway.
#

#
```

```
interface Vlan-interface4001
 description SDN_VLAN_Interface_4001
 ip binding vpn-instance Teach
 ip address 192.168.10.10 255,255,255,254
 pim sm      //Enable PIM SM manually on the VLAN interface.
 ip policy-based-route SDN_SC_VLAN_4001
#
#
pim vpn-instance Teach
 static-rp 192.168.10.11   //Manually configure a static RP and the address is the IP address of VLAN-interface 4001 on the L3 multicast device.
#
```

境界デバイスに接続されたレイヤー3 マルチキャストデバイスでの手動設定

```
#
vlan 4001      //VLAN in egress gateway details.
#
# Configure an IP address for communicating with the border device. //Remote IPv4 address in egress gateway details.
interface Vlan-interface 4001
ip address 192.168.10.11 255,255,255,254
pim sm
#
```

Configure a default route to interoperate with the private network.

`ip route-static 0.0.0.0 0 192.168.10.10 //`The next hop is the address of the egress local IPv4 in the egress gateway details.

Egress routers (devices supporting Layer 3 multicast) are globally configured with multicast routing:

```
#
multicast routing
#
```

Enable IGMP and PIM (PIM SM or PIM DM) on the VLAN interface. Take PIM SM as an example:

```
#
vlan 10
#
#
interface Vlan-interface10                //VLAN interconnecting with the multicast source.
 ip address 10.1.0.1 255.255.255.0
 pim sm                                   //Or PIM DM.
#
#
#
```

Globally specify the RP address and configure the RPF check:

```
#
pim
 static-rp 192.168.10.11
#
#
```

```
ip rpf-route-static 201.0.0.0 16 192.168.10.11
ip rpf-route-static 202.0.0.0 16 192.168.10.11      //Configure multicast static routes. Otherwise, RPF check failure might cause the multicast forwarding table to fail to be established. The addresses 201.0.0.0 and 202.0.0.0 are the user service segments, and 192.168.10.11 is the address of VLAN-interface 4001.

#
```

Configurations related to the multicast source interconnect interface and spine interconnect interface:

```
#
interface Ten-GigabitEthernet1/0/9        //Interface connected to the spine.
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4001
#
interface Ten-GigabitEthernet1/0/10          //Interface connected to the multicast source.
 port link-mode bridge
 port access vlan 10
#
```

QoS

QoS とは,Quality of Service の略であり,ネットワークのリソースは常に有限であり,あるサービスの品質を確保するためには,他のサービスの QoS との間で妥協が必要となる場合があります.そのため,ネットワーク管理者は,ネットワークのリソースを効率的に利用できるように,サービスの特性に応じてネットワークのリソースを合理的に計画し,割り当てる必要があります.

ユーザーは、QoS ポリシーを設定することで、ネットワークリソースの割り当てを制御できます。このポリシーは、次のもので構成されます。

- Class: パケットを識別するための規則を定義します。
- Traffic behavior: クラスによって識別されたパケットに対して実行される QoS アクションのセットを定義します。

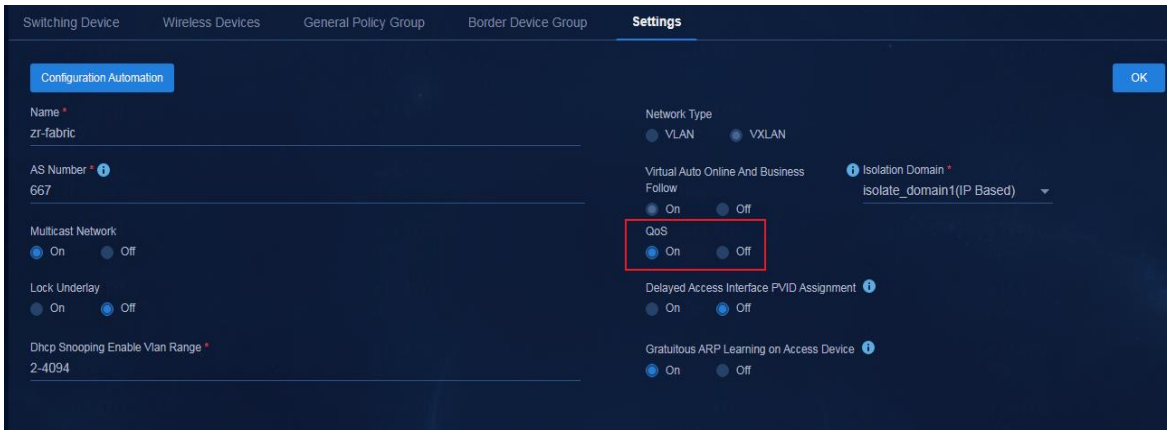
クラスをトラフィック動作に関連付けることにより、QoS ポリシーは、分類ルールに一致するパケットに対して、トラフィック動作で定義されたアクションを実行します。

⚠ 警告!

- 現在のソフトウェアバージョンでは、S5560X スイッチシリーズと S6520X スイッチシリーズは、QoS ポリシーとグループポリシーの同時使用をサポートしていません。
- 現在、QoS は東西のトラフィック制御をサポートしていません。
- S5130EI および S5130HI スイッチは、QoS ベースの DSCP リマークをサポートしていません。

QoSのグローバルなイネーブル化

ファブリックで QoS をイネーブルにするには **Automation** > **Campus Network** > **Fabrics** ページに移動し、ファブリックの **Actions** カラムで **Settings** アイコンをクリックします。**Settings** タブをクリックし、**QoS** パラメーターを **On** に設定し、**OK** をクリックして設定を保存します。



次のコマンドは、ファブリック内のすべてのデバイスに展開されます。

- スパインおよびリーフデバイスにグローバルに展開されたコマンド:

  ```
  #
  qos trust tunnel-dscp
  #
  ```

- スパイン、リーフ、およびアクセスデバイスの相互接続されていないインターフェイスに展開されるコマンド:

  ```
  #
  ```

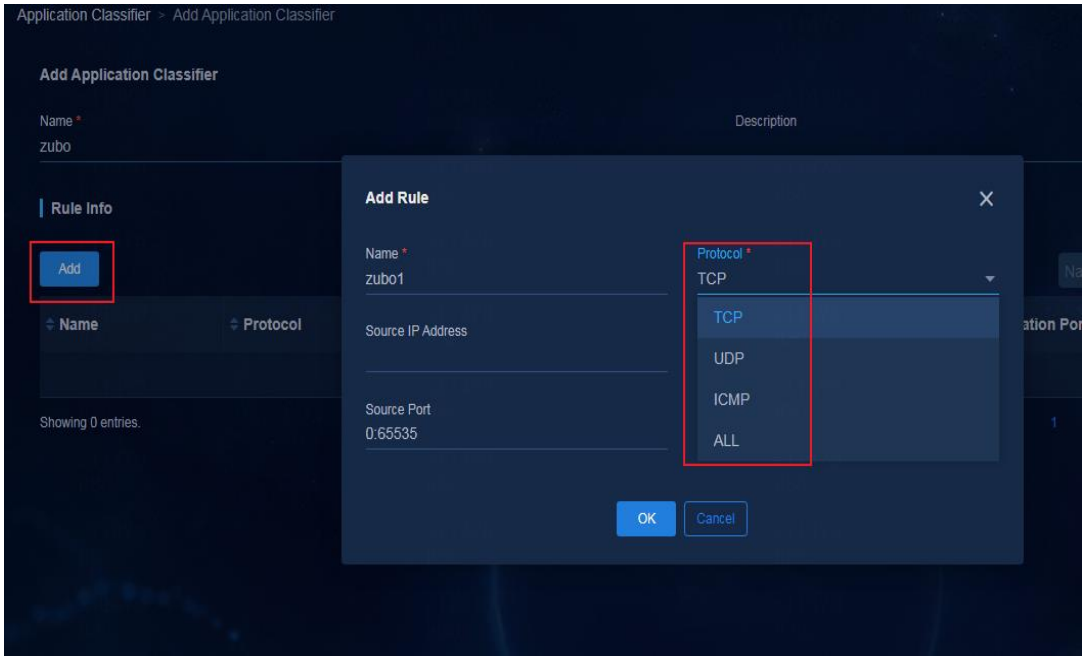
```
qos priority dscp 0
#
```

- スパイン、リーフ、およびアクセスデバイスの相互接続されたインターフェイスに展開されるコマンド:

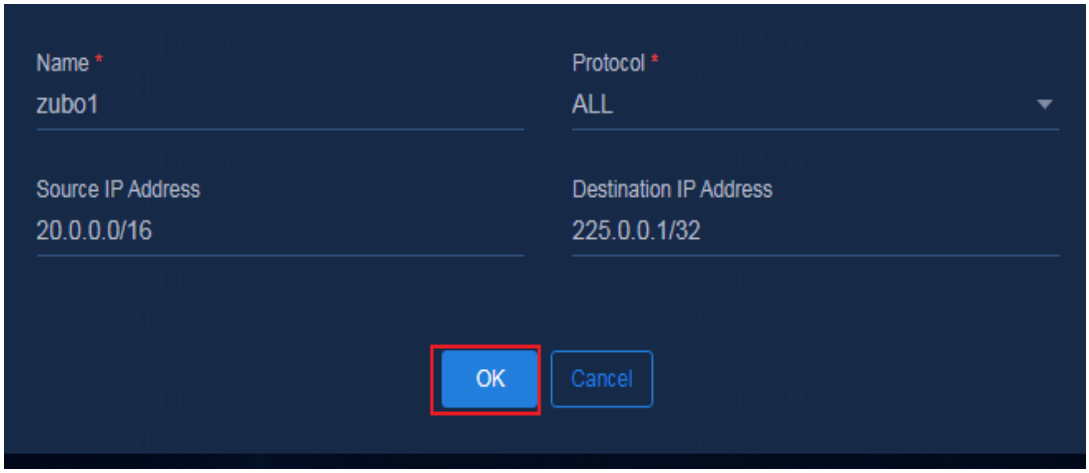
```
#
qos trust dscp
 qos wrr weight
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
#
```

アプリケーション分類子の追加

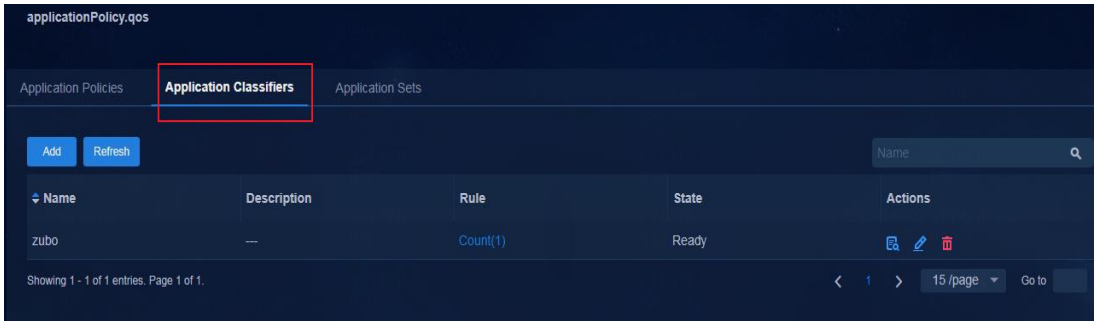
1. **Automation** > **Campus Network** > **Applications** > **QoS** > **Application Classifiers** ページに移動し、**Add** をクリックします。
2. アプリケーション分類子の名前を入力し、**Add** をクリックして、アプリケーション分類子に対応するルール情報を構成します。**Name**、**Protocol**、**Source IP Address**、**Destination IP Address**、**Source Port** および **Destination Port** のパラメーターを構成します。このルールに一致するすべてのパケットは、自動的に 1 つのクラスとして分類されます。



3. 次の規則を例にとると、送信元 IP セグメント 20.0.0.0/16 と宛先 IP セグメント 225.0.0.1/32 に一致するすべてのパケットは、自動的に 1 つのクラスとして分類されます。



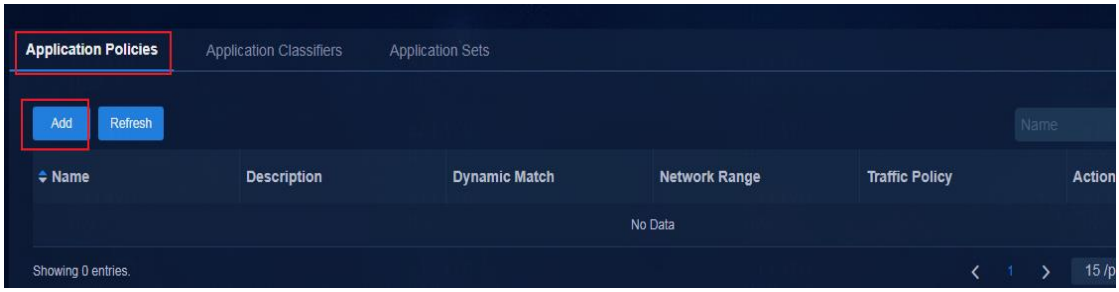
4. **OK** をクリックして、**Add Application Classifier** ページに戻ります。**OK** をクリックして構成を保存し、アプリケーション分類子リストに戻ります。構成したアプリケーション分類子を表示できます。アプリケーション分類子の状態は、参照されていない場合は **Ready** です。また、アプリケーション分類子を表示、編集または削除できます。



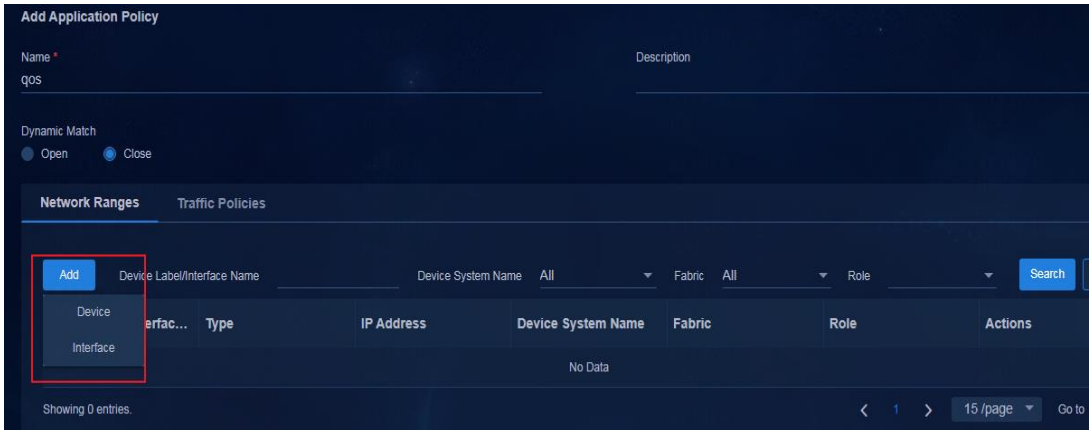
アプリケーションポリシーの追加

アプリケーション分類子を設定したら、アプリケーションポリシーを設定して、アプリケーション分類子に対して実行するアクションを決定する必要があります。

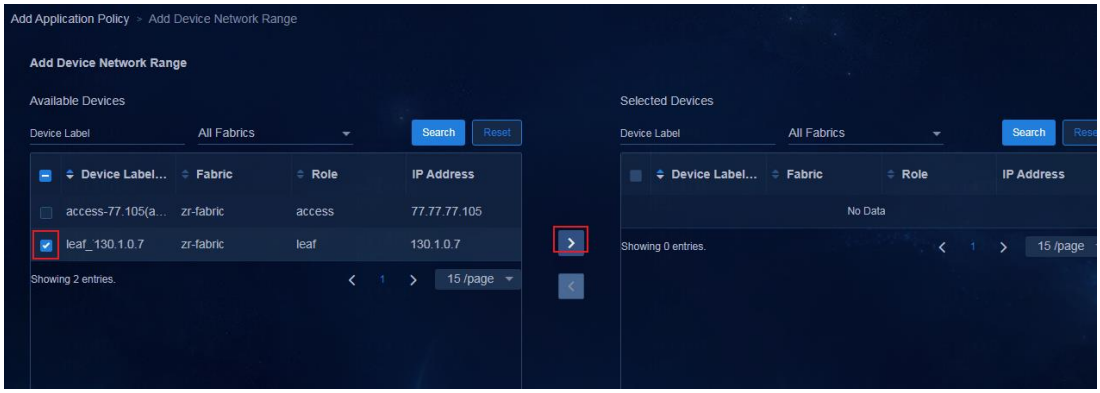
1. **Automation** > **Campus Network** > **Applications** > **QoS** > **Application Policies** ページに移動し、**Add** をクリックします。



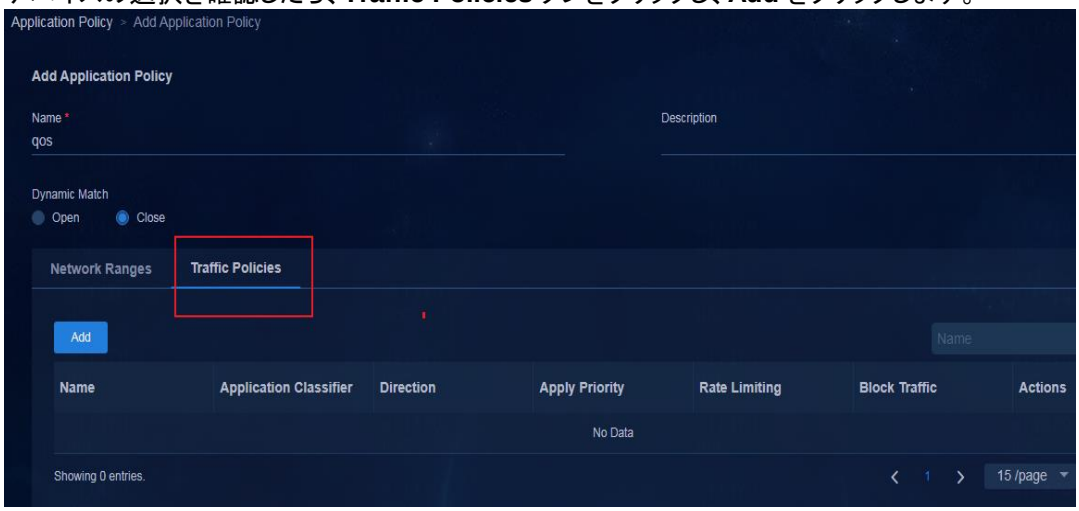
2. ポリシー名を入力すると、**Dynamic Match** 設定を開いたり閉じたりできます。ポリシー名を開くと、アプリケーションセットに対応するパケットが自動的に識別され、トラフィック保証ポリシーが実行されるため、**Network Range** を構成する必要はありません。デフォルトでは **Close** に設定されています。次に、Network Range タブで **Add** をクリックすると、ポップアップドロップダウンボックスで **Device** または **Interface** を選択できます。



3. デバイスまたはインターフェイスの選択ページでは、アプリケーションポリシーが展開されるデバイスまたはインターフェイスを選択できます。ポリシーが適用されるデバイスまたはインターフェイスだけがアプリケーション分類子と一致し、ポリシーアクションを実行します。



4. デバイスの選択を確認したら、**Traffic Policies** タブをクリックし、**Add** をクリックします。



このページのパラメーター:

- **Name**: 既存のトラフィックポリシーとは異なるポリシー名を入力します。
- **Application Classifier**: トラフィックポリシーを実装するアプリケーション分類子を選択します。
- **Direction**: オプションには **IN**、**OUT**、**BOTH** があり、それぞれインバウンド方向、アウトバウンド方向およびインバウンド方向とアウトバウンド方向の両方を示します。**IN** を選択してパケットを分類し、インバウンド方向で一致するパケットに対してアクションを実行することをお薦めします。

⚠ **警告!**

現在のソリューションでは、着信方向で一致するパケットに対して QoS ポリシーを設定する必要があります。

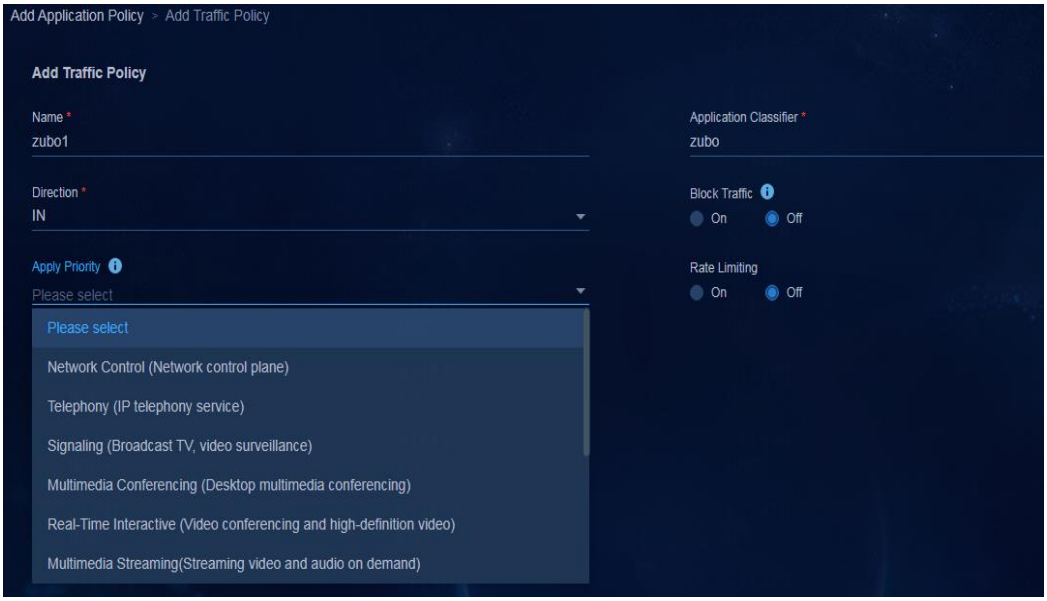
- **Block Traffic**: デフォルトでは、**Off** に設定されています。イネーブルの場合、一致したアプリケーション分類子のトラフィックはブロックされ、アプリケーションプライオリティおよびトラフィックレート制限は設定できません。
- **Apply Priority**: 優先度はアプリケーションによって異なります。デバイスは、パケットの優先度に従って異なるキューにパケットを送信します。通常、キューは 8 つ(0～7)あります。SP 方式では、値が大きいほど優先度が高くなります。デバイスは、優先度の高いものから低いものへパケットを送信します。つまり、優先度の高いキューが空の場合は、優先度の低いキューにパケットを送信します。WRR 方式では、各優先度キューに重みが割り当てられます。デバイスは、その重みに従って各キューをポーリングします。

  次の表に、異なるアプリケーションのキュー値を示します。キュー6 と 7 は予約されています。

  Table 5 アプリケーションの優先度

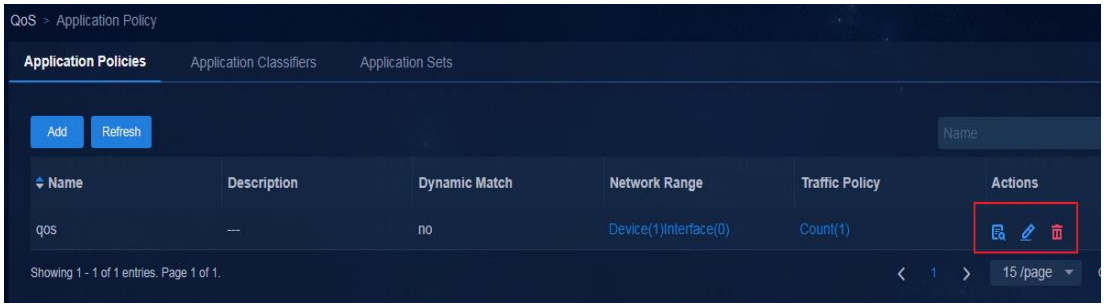
アプリケーション名	キュー
ネットワークコントロール(ネットワークコントロールプレーン)	5
テレフォニー(IPテレフォニーサービス)	5
シグナリング(ブロードキャストTV、ビデオ監視)	5
マルチメディア会議(デスクトップマルチメディア会議)	4
リアルタイムインタラクティブ(ビデオ会議および高品位ビデオ)	4
マルチメディアストリーミング(ビデオおよびオーディオのオンデマンドストリーミング)	3
ブロードキャストビデオ(テレビ放送およびライブイベント)	3
低遅延データ(クライアント/サーバートランザクション Webベースのオーダー)	1
OAM(OAMおよびP)	1
高スループットデータ(ストアアンドフォワードアプリケーション)	0
標準(差別化されていないアプリケーション)	2
低優先度データ(帯域幅保証のないフロー)	0

特定のトラフィックに対して特定のプライオリティでスケジューリングする必要がある場合は、次の図に従って設定を実行します。トラフィックに対応するアプリケーション分類子を選択します。方向には **IN** を選択し、アプリケーションプライオリティには Network Control(ネットワークコントロールプレーン)を選択します。

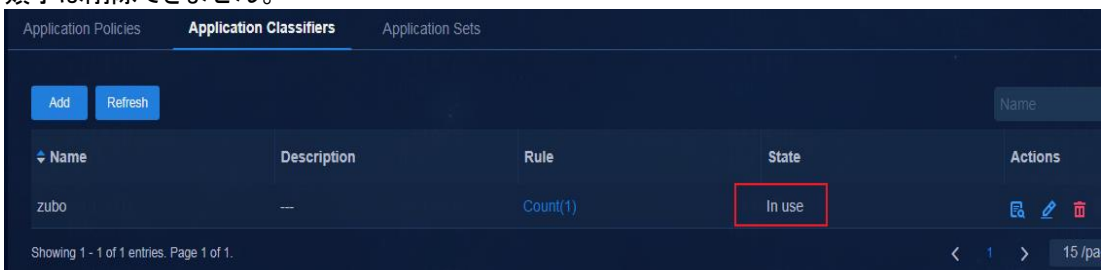


- **Rate Limiting**: パラメーターは、トラフィックのレート制限を設定します。デフォルトでは、**Off** に設定されています。必要に応じて有効にできます。レート制限を有効にする場合は、次のようなトラフィックポリシングパラメーターを設定する必要があります。
  - **CIR(kbit/s)**: 認定情報レートを示します。これは kbps 単位の平均トラフィックレートです。
  - **PIR(kbit/s)**: ピーク情報レートを kbps 単位で示します。PIR と CIR の単位は同じである必要があります。
  - **CBS(Byte)**: バイト単位の認定バーストサイズ。
  - **EBS(Byte)**: 超過バーストサイズ(バイト単位)。

5. **OK** をクリックして **Add Application Policy** ページに戻り、もう一度 OK をクリックして **Application Policy** ページに戻ります。リストに追加したアプリケーションポリシーを表示できます。ポリシーを表示、編集または削除できます。



6. アプリケーション分類子タブをクリックすると、アプリケーションポリシーで参照されているアプリケーション分類子の状態が使用中に切り替わっていることがわかります。**In use** 状態のアプリケーション分類子は削除できません。



デバイスに展開された設定の表示

- 設定がデバイスに展開されている場合、デバイスで次のコマンドを表示できます。

```
<Leaf>dis current-configuration | in traffic
traffic classifier SDN4_UEF4NPODIEGU5HZQU2XL4E2MGY operator and
traffic behavior SDN_TOEWO6M6MOKCVBHITHF3TWSGPE

<Leaf>dis current-configuration | begin traffic
traffic classifier SDN4_UEF4NPODIEGU5HZQU2XL4E2MGY operator and     //Traffic classifier.
 if-match acl name SDN_SP_ACL_UEF4NPODIEGU5HZQU2XL4E2MGY
#
traffic behavior SDN_TOEWO6M6MOKCVBHITHF3TWSGPE     //Traffic behavior.
 remark dscp ef
 remark dot1p 5
 car cir 800 cbs 50176 pir 800 ebs 50176 green pass red discard yellow pass
//Deployed when rate limiting is configured.
#
qos policy SDN_IN_qos
 classifier SDN4_UEF4NPODIEGU5HZQU2XL4E2MGY behavior SDN_TOEWO6M6MOKCVBHITHF3TWS
GPE
#
```

- 設定がインターフェイスに展開されている場合、インターフェイスで次のコマンドを表示できます。

```
[Leaf]interface Ten-GigabitEthernet1/2/0/16
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3504 3508 4002
```

```
 qos apply policy SDN_OUT_test outbound
```
(If select **BOTH** for direction in the traffic policy, two application policies will be deployed.)

```
#
return
[Leaf-Ten-GigabitEthernet1/2/0/16]
```

//Label the packets that match the policy and add the packets to the queue specified in the policy at the outbound direction.

//

```
<Leaf11>display qos queue-statistics interface Ten-GigabitEthernet 5/0/4 outband
Interface: Ten-GigabitEthernet5/0/4          //Packet  outbound interface.
 Direction: outbound
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 189 packets, 56511 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 4
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 5
  Forwarded: 64728993 packets, 4265970097 bytes, 1503210 pps, 769643520 bps
  Dropped: 64671339 packets, 4261944441 bytes
  Current queue length: 0 packets
---- More ----
 Queue 6
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 7
  Forwarded: 1 packets, 149 bytes, 0 pps, 0 bps
```

リーフアクセスネットワークモデルの制約事項とガイドライン

シングルリーフシナリオ

シングルリーフのシナリオでは、ネットワーク全体に 1 つのリーフデバイスのみが存在します。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デバイスに接続されます。SeerEngine キャンパスや DHCP サーバーなどのサーバーも、このリーフデバイス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。このリーフデバイスのリーフ構成は、従来のリーフ構成とは異なります。この項では、異なる設定についてのみ説明します。その他の設定の詳細は、前の章で説明した標準ネットワークモデルとその構成を参照してください。

- 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 DHCP スヌーピングがイネーブルになっていないため)、DHCP サーバーに接続されているイーサネットサービスインスタンスを DHCP スヌーピングの信頼できるポートとして指定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
#
```

- ネットワークにはリーフデバイスが 1 つしか存在しないため、リーフデバイスの BGP ピアを確立する必要はありません。ただし、カスタムプライベートネットワークが存在する場合は、VPN 間ルート再配布を設定する必要があります。次の方法を使用できます。
  - 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  //Import the direct routes in VPN instance vpn1 to VPN instance vpn-default. Repeat this command if multiple VPN instances exist.
 #
 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
//You only need to import the direct routes in VPN instance vpn-default. Configure similar settings If communication to other VPN instances is required.
 #
 address-family evpn
  vpn-target 1:1 1:4 import-extcommunity
  vpn-target 1:4 export-extcommunity
 #
```

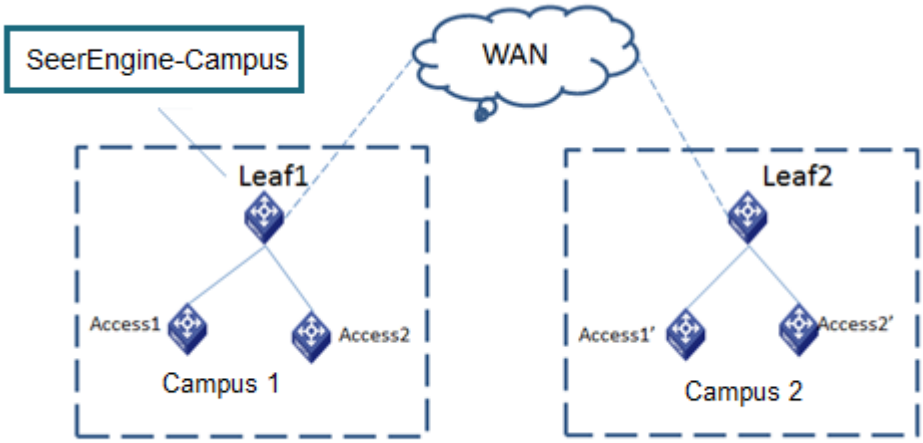
- リーフデバイスで、次のスパニングツリー設定を行います。

```
#
stp ignored vlan 2 to 4094
stp global enable
stp root primary
#
# On the leaf downlink interfaces, enable TC-BPDU transmission restriction.
stp tc-restriction
#
```

マルチリーフ シナリオ

マルチリーフのシナリオは、複数のキャンパスがあるネットワークに存在します。このシナリオでは、SeerEngine キャンパスなどのサーバーに接続されているコアデバイス(RR としても機能)もリーフデバイスグループに追加する必要があります。他のリーフデバイスでリーフ設定を構成するのと同じ方法で、コアデバイスでリーフ設定を構成します。

ネットワークで機能が正常に実行されるようにするには、すべてのリーフデバイスに構成を追加する必要があります。この項では、追加の構成についてのみ説明します。その他の設定については、前の章で説明した標準ネットワークモデルとその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          //Configure the ARP proxy.
#
```

追加の設定は次のとおりです。

- 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 DHCP スヌーピングがイネーブルになっていません)、DHCP サーバーに接続されているイーサネットサービスインスタンスを DHCP スヌーピングの信頼できるポートとして指定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
  #
  ```

- エンドポイント(カスタム VPN インスタンス)は、サーバーに接続されたコアデバイス上に存在する場合があります。エンドポイントは、VPN インスタンス vpn-default 内のサーバーまたは外部ネットワークと通信する必要があります。サーバーに接続されたコアデバイス上の VPN インスタンスに直接ルートをインポートするように BGP を設定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
#
```

- 各リーフデバイスに次の設定を追加します。

```
#
stp ignored vlan 2 to 4094
stp global enable
stp root primary
#
# On the leaf downlink interfaces, enable TC-BPDU transmission restriction.
stp tc-restriction
#
```

冗長デュアルスパインアップリンクの設定

Figure 1 冗長デュアルスパインアップリンクを配置して、スパインデバイスの冗長性保護とトラフィックロードバランシングを実現します。に、冗長デュアルスパインアップリンクのネットワークダイアグラムを示します。

Figure 1 冗長デュアルスパインアップリンク

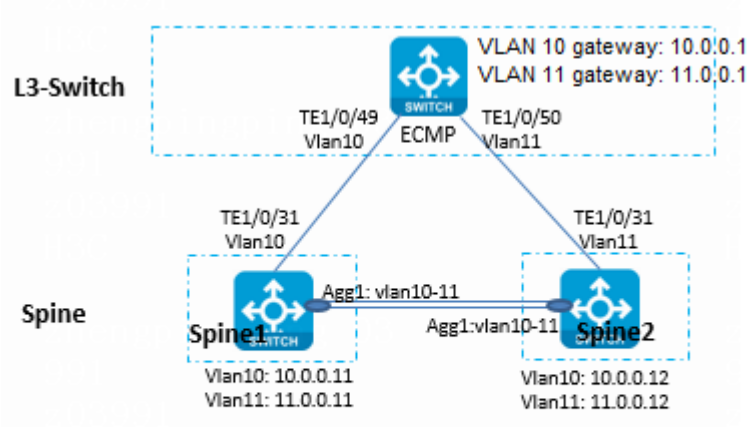


Table 6 スパインデバイスをレイヤー3 スイッチに接続するインターフェイスの IP プランニング

デバイス	インターフェイス	IP アドレス	接続されているデバイス	接続されたインターフェイス	IP アドレス
Spine1	TE2/0/31	10.0.0.11	レイヤー3スイッチ	TE1/0/49日	10.0.0.1
Spine 2	TE2/0/31	11.0.0.12	レイヤー3スイッチ	TE1/0/50日	11.0.0.1
Spine 1	Aggr1(VLAN 10およびVLAN 11)	10.0.0.11 11.0.0.11	Spine 2	Aggr1(VLAN 10およびVLAN 11)	10.0.0.12 11.0.0.12

冗長デュアルスパインアップリンクは、レイヤー3 スイッチに接続されます。レイヤー3 スイッチ上のデュアルスパインデバイスを宛先とするデフォルトの ECMP ルートを設定できます。このセクションでは、冗長デュアルスパインアップリンクの展開に必要な特別な設定についてのみ説明します。その他の設定については、『Manual incorporation』を参照してください。

レイヤー3スイッチの設定

#VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
# Configure the spanning tree feature.
#
stp global enable
```

```
#
# Enable VLAN Ignore for VLAN 10 and VLAN 11. The VLANs are connected to the spine devices.
stp ignored vlan 10 to 11
#
# Configure VLAN-interface 10 and VLAN-interface 11.
#
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
#
# Assign the interface connected to Spine 1 to VLAN 10.
#
interface Ten-GigabitEthernet1/0/49
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10  //Determine whether to add the interface to VLAN 1 according to the actual networking.
#
# Assign the interface connected to Spine 2 to VLAN 11.
#
interface Ten-GigabitEthernet1/0/50
 port link-mode bridge
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 11   // Determine whether to add the interface to VLAN 1 according to the actual networking.
#
# Configure track.
#
track 1 interface Ten-GigabitEthernet1/0/49 physical
track 2 interface Ten-GigabitEthernet1/0/50 physical
#
# Configure two default routes with the next hops being the IP addresses of Spine 1 and Spine 2.
#
 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
#
# Add 32-bit host routes destined for the spine devices. The routes protect traffic forwarding in case of inter-spine link failures or spine device failures.
#
ip route-static 130.1.0.101 32 10.0.0.11  //130.1.0.101 is the address of VSI-interface 4094 on Spine 1.
 ip route-static 130.1.0.102 32 11.0.0.12  //130.1.0.102 is the address of VSI-interface 4094 on Spine 2.
#
```

Spine 1のレイヤー3スイッチへの接続

#スパニングツリーの設定を行います。

```
#
stp instance 0 root primary
 stp ignored vlan 2 to 4094
 stp global enable
#
```

Create VLAN 10.

```
#
vlan 10
#
```

Configure VLAN-interface 10 and associate VPN instance **vpn-default** with the VLAN interface.

```
#
interface Vlan-interface10
 ip binding vpn-instance vpn-default
 ip address 10.0.0.11 255.255.255.0
#
```

Assign the interface connected to the Layer 3 switch to VLAN 10.

```
#
interface Ten-GigabitEthernet1/0/31
 port link-mode bridge
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 10  // Determine whether to add the interface to VLAN 1 according to the actual networking.
#
```

Configure static routes destined for servers with the next hops being the IP address of the Layer 3 switch.

```
#
 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
#
```

Spine 2のレイヤー3スイッチへの接続

#スパニングツリーの設定を行います。

```
#
stp instance 0 root secondary
 stp ignored vlan 2 to 4094
 stp global enable
#
```

Create VLAN 11.

```
#
vlan 11
#
```

Configure VLAN-interface 11 and associate VPN instance **vpn-default** with the VLAN interface.

```
#
interface Vlan-interface11
```

```
 ip binding vpn-instance vpn-default
 ip address 11.0.0.12 255.255.255.0
#
# Assign the interface connected to the Layer 3 switch to VLAN 11.
#
interface Ten-GigabitEthernet1/0/31
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11  // Determine whether to add the interface to VLAN 1 according to the actual networking.
#
# Configure static routes destined for servers with the next hops being the IP address of the Layer 3 switch.
#
 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
#
```

Spine 1とSpine 2の接続

Spine 1 の設定

#高速リルートを設定します。

```
#
ip route-static fast-reroute auto
#
# Create VLAN 11.
#
vlan 11
#
# Create VLAN-interface 11.
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 11.0.0.11 255.255.255.0
#
# Create VLAN 3 for communicating with the underlay network.
#
vlan 3
#
# Create VLAN-interface 3.
#
interface Vlan-interface3
 ip address 3.0.0.1 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
# Create an aggregation group.
#
```

```
interface Bridge-Aggregation1
 link-aggregation mode dynamic
#
```
Add interfaces to the aggregation group.
```
#
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
#
```
Add the aggregate interface to VLAN 10, VLAN 11, and VLAN 3.
```
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1   // Determine whether to add the interface to VLAN 1 according to the actual networking.
 port trunk permit vlan 3 10 to 11
 link-aggregation mode dynamic
#
```
//Since fast rerouting has been configured, the following NQA-track collaboration configuration is optional.
Configure track for quick inter-leaf link failure detection and link switchover.
```
#
track 1 interface Bridge-Aggregation1 physical
#
```
Configure a static route destined for VXLAN 4094 on Spine 2 (with the next hop being the IP address of VLAN-interface 10 or VLAN-interface 11).
```
#
ip route-static vpn-instance vpn-default 130.1.0.102 32 11.0.0.12 track 1
#
```
Configure NQA-track collaboration and static routes destined for the server cluster. The next hops of the static routes are the gateway IP addresses of VLAN 10 and VLAN 11 on the Layer 3 switch. Associate the static routes with track entries for quick link failure detection and link switchover.
```
#
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
//Configuration of static routes when NQA-track collaboration is not configured.
#
 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
#
#
# Configure BGP to import static routes to VPN instance vpn-default.
#
bgp 100
#
 ip vpn-instance vpn-default
  #
  address-family ipv4 unicast
   import-route direct
   import-route static
 #
```

Spine 2 の設定

```
#高速リルートを設定します。
#
ip route-static fast-reroute auto
#
# Create VLAN 10.
#
vlan 10
#
# Create VLAN-interface 10.
#
interface Vlan-interface11
 ip binding vpn-instance vpn-default
 ip address 10.0.0.12 255.255.255.0
#
# Create VLAN 3 for communicating with the underlay network.
```

```
#
vlan 3
#
# Create VLAN-interface 3.
#
interface Vlan-interface3
 ip address 3.0.0.2 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
# Create an aggregation group.
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
#
# Add interfaces to the aggregation group.
#
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
#
# Add the aggregate interface to VLAN 10, VLAN 11, and VLAN 3.
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1   // Determine whether to add the interface to VLAN 1 according to the actual networking.
 port trunk permit vlan 3 10 to 11
 link-aggregation mode dynamic
#
//Since fast rerouting has been configured, the following NQA-track collaboration configuration is optional.
# Configure track for quick inter-leaf link failure detection and link switchover.
#
track 1 interface Bridge-Aggregation1 physical
#
# Configure a static route destined for VXLAN 4094 on Spine 1 (with the next hop being the IP address of VLAN-interface 10 or VLAN-interface 11).
#
ip route-static vpn-instance vpn-default 130.1.0.101 32 11.0.0.11 track 1
#
# Configure NQA-track collaboration and static routes destined for the server cluster. The next hops of the static routes are the gateway IP addresses of VLAN 10 and VLAN 11 on the Layer 3 switch. Associate the static routes with track entries for quick link failure detection and link switchover.
#
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
#
//Configuration of static routes when NQA-track collaboration is not configured.
#
 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
#
# Configure BGP to import static routes to VPN instance vpn-default.
#
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の設定

リーフデバイス上のサーバーネットワークセグメントを宛先とする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のスタティックルートの設定

#アクセスデバイス上のサーバーを宛先とする 2 つのスタティックルートを設定し、スパインデバイス上の VXLAN 4094 アドレスをゲートウェイアドレスとして指定します。

```
#
ip route-static 100.1.0.0 24 130.1.0.101    //VXLAN 4094 address of Spine 1.
ip route-static 100.1.0.0 24 130.1.0.102    //VXLAN 4094 address of Spine 2.
ip route-static 110.1.0.0 24 130.1.0.101
ip route-static 110.1.0.0 24 130.1.0.102
#
```

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、コントローラーはリーフデバイスに対してのみ DRNI 設定をサポートしています。スパインデバイスの DRNI は手動で設定する必要があります。

この章では、スパインデバイスでのデュアルスパインシナリオに必要な特別な設定についてのみ説明します。その他の設定については、『Manual incorporation』を参照してください。

レイヤー3スイッチの設定

#VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
# Configure VLAN-interface 10 and VLAN-interface 11.
#
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
#
# Assign the interface connected to Spine 1 to VLAN 10.
#
interface Ten-GigabitEthernet1/0/25
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10  // Determine whether to add the interface to VLAN 1 according to the actual networking. If not required, execute the undo permit vlan 1 command to remove the interface from VLAN 1.
#
# Assign the interface connected to Spine 2 to VLAN 11.
#
interface Ten-GigabitEthernet1/0/26
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 11   // Determine whether to add the interface to VLAN 1 according to the actual networking. If not required, execute the undo permit vlan 1 command to remove the interface from VLAN 1.
#
# Configure track.
#
track 1 interface Ten-GigabitEthernet1/0/25 physical
track 2 interface Ten-GigabitEthernet1/0/26 physical
#
# Configure two default routes with the next hops being the IP addresses of Spine 1 and Spine 2.
#
 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
#
```

Spine 1のレイヤー3スイッチへの接続

#VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
```

Configure VLAN-interface 10 and VLAN-interface 11, and associate VPN instance **vpn-default** with the VLAN interfaces.

```
#
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
#
```

Assign the interface connected to the Layer 3 switch to VLAN 10.

```
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10  // Determine whether to add the interface to VLAN 1 according to the actual networking. If not required, execute the undo permit vlan 1 command to remove the interface from VLAN 1.
#
```

Configure NQA-track collaboration and static routes destined for the server cluster. The next hops of the static routes are the gateway IP addresses of VLAN 10 and VLAN 11 on the Layer 3 switch. Associate the static routes with track entries for quick link failure detection and link switchover.

```
#
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
#
```

Spine 2のレイヤー3スイッチへの接続

#VLAN 10 と VLAN 11 を作成します。

```
#
vlan 10 to 11
#
```

Configure VLAN-interface 10 and VLAN-interface 11, and associate VPN instance **vpn-default** with the VLAN interfaces.

```
#
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
#
```

Assign the interface connected to the Layer 3 switch to VLAN 11.

```
#
interface Ten-GigabitEthernet2/0/31
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 11  // Determine whether to add the interface to VLAN 1 according to the actual networking. If not required, execute the undo permit vlan 1 command to remove the interface from VLAN 1.
#
```

Configure NQA-track collaboration and static routes destined for the server cluster. The next hops of the static routes are the gateway IP addresses of VLAN 10 and VLAN 11 on the Layer 3 switch. Associate the static routes with track entries for quick link failure detection and link switchover.

```
#
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
#
```

Spine 1でのDRNIの設定

#OSPF の高速リルーティングを設定します。

```
#
ospf 1 router-id 200.1.1.254  //Specify a unique router ID. The IP address of Loopback 0 is specified.
 non-stop-routing
fast-reroute lfa
 area 0.0.0.0
#
```

Configure Loopback 2. Spine 1 and Spine 2 use the same IP address for Loopback 2.

```
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
#
```

Create VLAN 2 and configure VLAN-interface 2. Spine 1 and Spine 2 use different IP addresses for the VLAN interface. VLAN 2 is used to synchronize underlay routes between the two DR member devices.

```
#
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
#
```

Configure the MAC address of VSI-interface 4094. Spine 1 and Spine 2 use the same MAC address for the VSI interface.

```
#
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
#
```
Configure loop detection to eliminate loops in VSI **vxlan4094**.
```
#
vsi vxlan4094
 loopback-detection action block
 loopback-detection enable vlan 4094
    #
```
Configure EVPN distributed relay. The configurations on Spine 1 and Spine 2 are the same.
```
#
l2vpn drni peer-link ac-match-rule vxlan-mapping
evpn drni group 99.99.0.10    //Specify the IP address of Loopback 2 as the virtual VTEP address. The device will be reactivated.
evpn global-mac 0001-0001-0004  //MAC addresses on Spine 1 and Spine 2 are the same.
#
#
 vxlan default-decapsulation source interface LoopBack0
#
```
Enable the device to replace the next hop in advertised BGP EVPN routes with the virtual VTEP address.
```
#
bgp 1
address-family l2vpn evpn
nexthop evpn-drni group-address
#
```
Configure the keepalive interface (a Layer 3 interface that can be a logical interface or a physical interface).
```
#
ip vpn-instance DRNI_KeepAlive       //Configure the exclusive VPN instance for keepalive.
#
#
interface FortyGigE3/0/33
 port link-mode route
 ip binding vpn-instance DRNI_KeepAlive    //Bind a VPN instance.
 ip address 192.168.0.1 255.255.255.252      //Configure address mask 30. Specify different IP addresses for the keepalive interfaces on Spine 1 and Spine 2.
#
```
Specify the destination and source IP addresses of keepalive packets.
```
#
drni keepalive ip destination 192.168.0.2 source 192.168.0.1 vpn-instance
DRNI_KeepAlive
#
```
Configure the DR system parameters. Configure the same system MAC and different system numbers for devices in a DR system.
```
#
drni restore-delay 180
drni system-mac 542b-de08-8200
drni system-number 1
drni system-priority 10
#
```

Configure an IPP (it must be a layer 2 aggregate interface).

```
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4094                    //The PVID must be 4094.
 link-aggregation mode dynamic
 port drni intra-portal-port 1                //Configure the IPP.
 undo mac-address static source-check enable  //Disable source MAC address check.
#
#
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
#
```

Configure DRNI MAD.

```
#
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
#
```

Set the MAC entry aging timer to a value no less than 20 minutes.

```
#
mac-address timer aging 1560
#
```

Disable source MAC address check on the interface connected to leaf devices.

```
#
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
#
```

Enable DR system auto-recovery and specify a reload delay time. To avoid incorrect role preemption, make sure the reload delay time is longer than the amount of time required for the device to restart.

```
drni auto-recovery reload-delay delay-value 600
#
```

Spine 2でのDRNIの設定

#OSPF の高速リルーティングを設定します。

```
#
ospf 1 router-id 200.1.1.253  // Specify a unique router ID. The IP address of Loopback 0 is specified.
 non-stop-routing
fast-reroute lfa
 area 0.0.0.0
#
```

Configure Loopback 2. Spine 1 and Spine 2 use the same IP address for Loopback 2.

```
#
interface LoopBack2
 ip address 99.99.0.10 255,255,255,255
 ospf 1 area 0.0.0.0
#
```

Create VLAN 2 and configure VLAN-interface 2. Spine 1 and Spine 2 use different IP addresses for the VLAN interface.

```
#
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
#
```

Configure the MAC address of VSI-interface 4094. Spine 1 and Spine 2 use the same MAC address for the VSI interface.

```
#
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
#
```

Configure loop detection to eliminate loops in VSI **vxlan4094**.

```
#
vsi vxlan4094
     loopback-detection action block
 loopback-detection enable vlan 4094
#
```

Configure EVPN distributed relay. The configurations on Spine 1 and Spine 2 are the same.

```
#
```

```
l2vpn drni peer-link ac-match-rule vxlan-mapping
evpn drni group 99.99.0.10    // Specify the IP address of Loopback 2 as the virtual VTEP address. The device will be reactivated.
evpn global-mac 0001-0001-0004  // MAC addresses on Spine 1 and Spine 2 are the same.
#
 vxlan default-decapsulation source interface LoopBack0
#
# Enable the device to replace the next hop in advertised BGP EVPN routes with the virtual VTEP address.
#
bgp 1
address-family l2vpn evpn
nexthop evpn-drni group-address
#
# Configure the keepalive interface (a Layer 3 interface that can be a logical interface or a physical interface).
#
ip vpn-instance DRNI_KeepAlive       //Configure the exclusive VPN instance for keepalive.
#
interface FortyGigE3/0/33
 port link-mode route
 ip binding vpn-instance DRNI_KeepAlive    //Bind a VPN instance.
 ip address 192.168.0.2 255.255.255.252      //Configure address mask 30. Specify different IP addresses for the keepalive interfaces on Spine 1 and Spine 2.
#
# Specify the destination and source IP addresses of keepalive packets.
#
drni keepalive ip destination 192.168.0.1 source 192.168.0.2 vpn-instance
DRNI_KeepAlive
#
# Configure the DR system parameters. Configure the same system MAC and different system numbers for devices in a DR system.
#
drni restore-delay 180
drni system-mac 542b-de08-8200
drni system-number 2
drni system-priority 10
#
# Configure an IPP (it must be a layer 2 aggregate interface).
#
interface Bridge-Aggregation1
 description SDN_LAGG
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4094                  // The PVID must be 4094.
 link-aggregation mode dynamic
 port drni intra-portal-port 1                //Configure the IPP.
 undo mac-address static source-check enable  //Disable source MAC address check.
#
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
#
#
```

Configure DRNI MAD.

```
#
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
#
```

Set the MAC entry aging timer to a value no less than 20 minutes.

```
#
mac-address timer aging 1560
#
```

Disable source MAC address check on the interface connected to leaf devices.

```
#
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
#
```

Enable DR system auto-recovery and specify a reload delay time. To avoid incorrect role preemption, make sure the reload delay time is longer than the amount of time required for the device to restart.

```
drni auto-recovery reload-delay delay-value 600
#
```

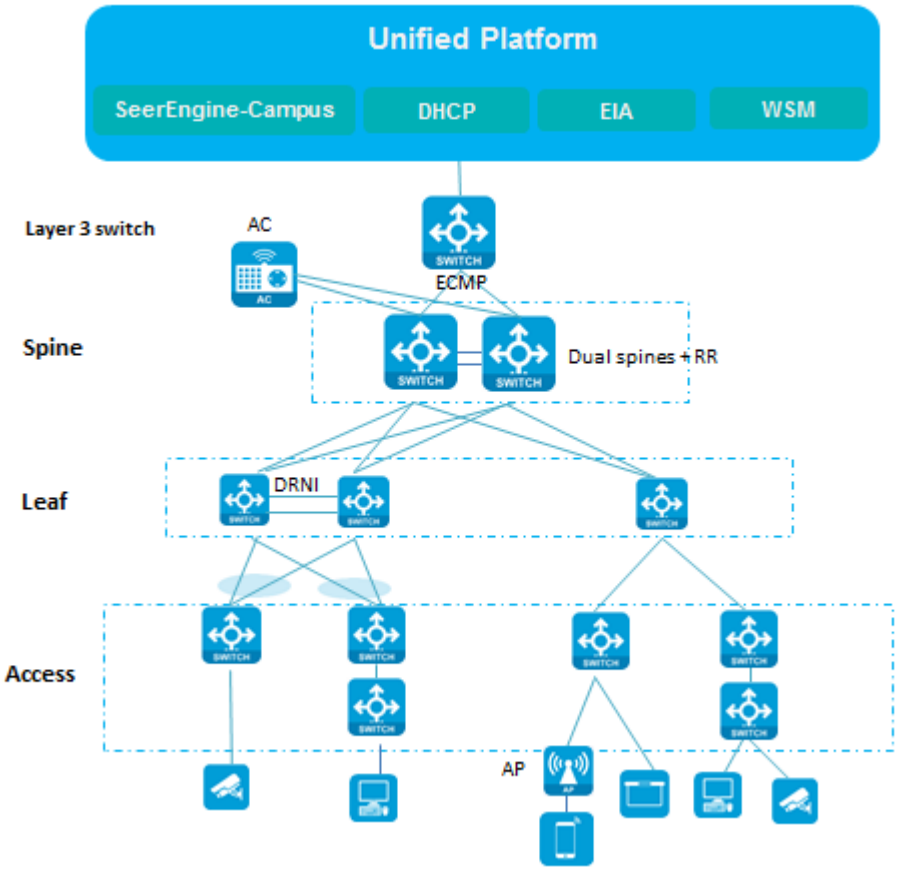
DRNI の設定

DRNIネットワーキング

Distributed Resilient Network Interconnect(DRNI)は、2 つの物理デバイスを集約レベルで 1 つのデバイスに仮想化して、クロスデバイスリンクアグリゲーションを実装するクロスデバイスリンクアグリゲーションテクノロジーである。したがって、デバイスレベルの冗長性保護とトラフィックの負荷分散を提供できる。

AD-Campus ソリューションでは、デバイスの冗長保護とトラフィック負荷分散のために、デバイス上で DRNI を構成して DR システムを形成できます。DRNI のネットワーク図を次の図に示します。

Figure 2 DRNI ネットワーキング



DRシステムの設定

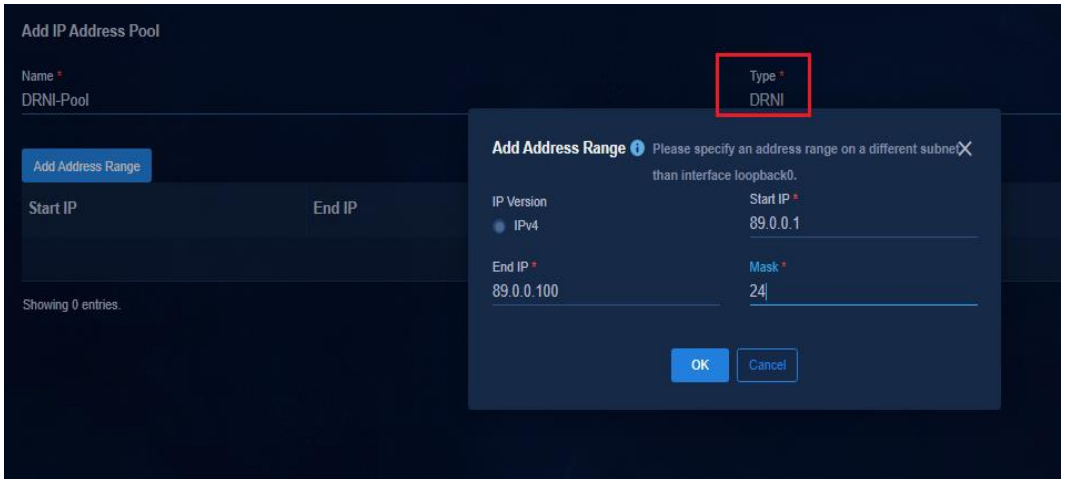
デュアルスパインデバイスの構成については、『Configuring redundant dual-spine uplinks』を参照してください。デュアルスパインデバイスは、コントローラーによって手動で組み込まれます。リーフデバイスがコントローラーによって組み込まれた後、DRNI 設定を構成できます。スパインデバイスとリーフデバイスの組み込みについては、『Configuring AD-Campus』を参照してください。

このセクションでは、リーフデバイスがコントローラーに組み込まれた後の DRNI の設定についてのみ説明します。

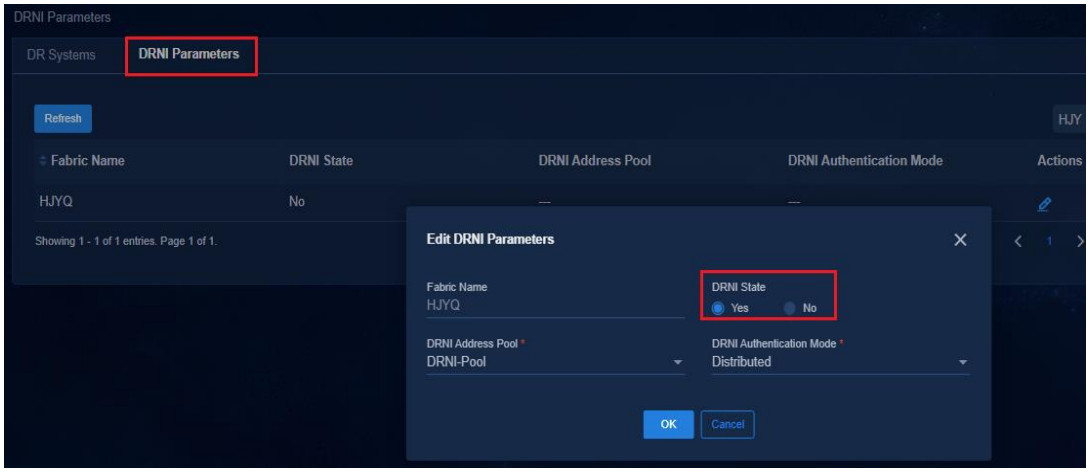
注:

- ファブリックで DRNI をイネーブルにするには、DRNI 仮想 IP 自動割り当てを確認するために、VLAN 4094 アドレスプールをそのファブリックにバインドする必要があります。
- デュアルスパインデバイスは、リーフデバイスと個別の BGP ピア関係を確立する必要があります。設定の詳細については、『Manual incorporation』を参照してください。
- キープアライブリンクと IPL 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 に接続されているインターフェイスが同じレートで動作していることを確認してください。
- 複数の DR システムを同期的に導入しないでください。毎回 1 つの DR システムを導入してください。
- アクセスデバイスに接続されたリーフデバイスが DR システムを形成し、アクセスデバイスが IRF ファブリックを形成し、BFD MAD が IRF ファブリックで設定されている場合は、アクセスデバイスのアップリンクインターフェイスを BFD MAD VLAN から削除します。
- DR システムがリーフデバイスとして使用されているときに、ユーザーがサービスに正しくアクセスできるようにするには、ユーザーがオンラインになる前に DR システムのセットアップが完了していることを確認します。
- DR インターフェイスおよびポータル内ポート(IPP)を展開するには、その DR インターフェイスまたは IPP の **Edit** アイコンをクリックして DR インターフェイスまたは IPP を編集するためのページを開き、対応する物理インターフェイスを追加します。

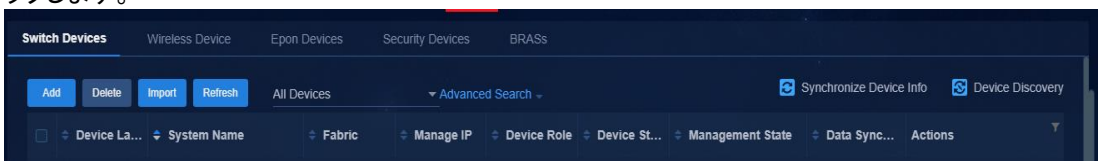
1. **Automation** > **Campus Network** > **Devices** ページに移動し、右上隅にある **IP Address Pools** をクリックします。
2. **Add IP Address Pool** ページで、**Type** として **DRNI** を選択します。
3. DRNI IP アドレスプールは DRNI アドレスを設定し、各 DR システムに 3 つのアドレスを割り当てる必要があります。
   - Loopback 2 のアドレス(2 つのデバイスで同じ):仮想 VTEP アドレスを指定します。
   - VLAN インターフェイス 2 のアドレス(デバイスごとに 1 つ):DR メンバー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** > **Devices** ページに移動し、右上隅の **DRNI** をクリックします。**DRNI Parameters** タブをクリックし、アイコンをクリックして Edit DRNI Parameters ページにアクセスします。
   - **DRNI State**: **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** > **Devices** ページに移動し、**DRNI** をクリックします。**Add** をクリックします。

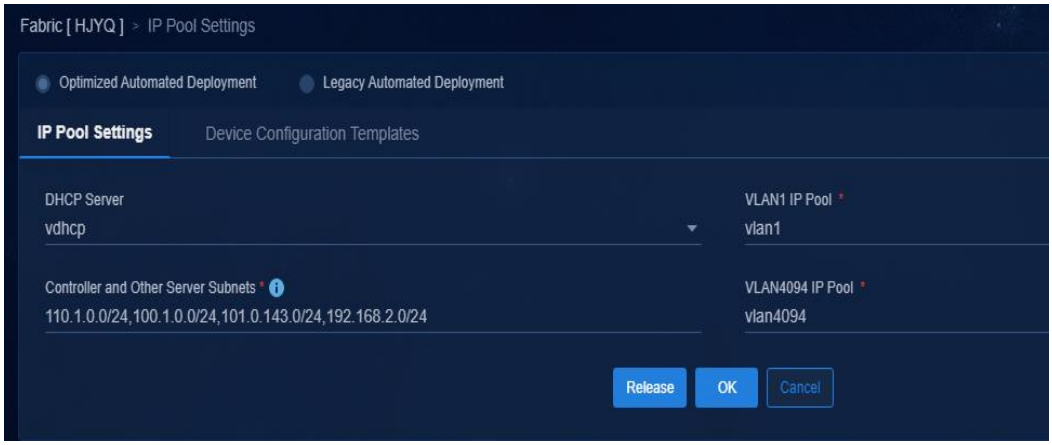


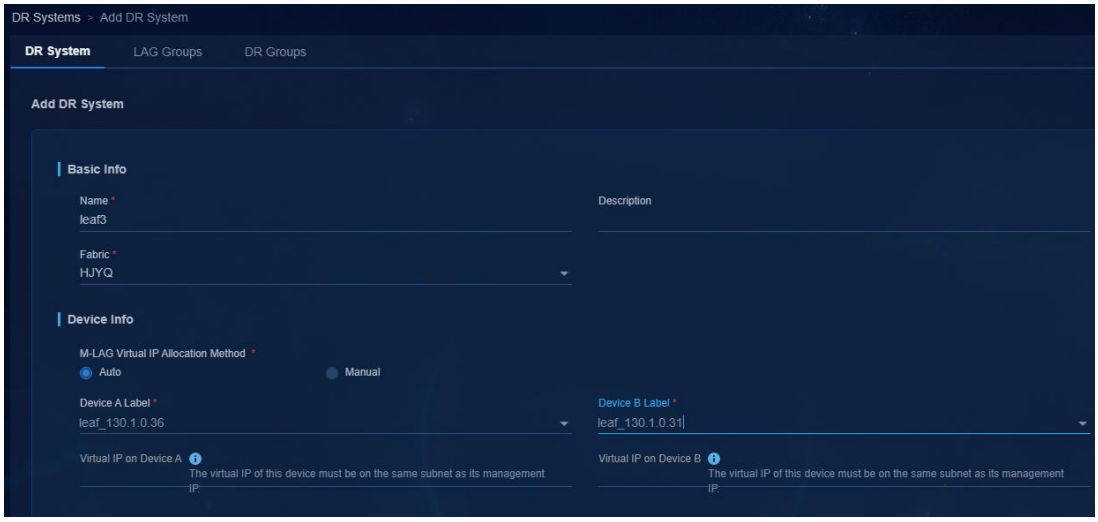
パラメーターについて、次に説明します。

- **Name**: DR システムの名前を入力します。
- **Fabric**: **HJYQ** を選択します。
- **Device A Label/Device B Label**: 各 DR メンバーデバイスのラベルを入力します。
- **DRNI Virtual IP Allocation Method**: デフォルトでは、デバイス管理アドレスプールから自動的に割り当てることができます。手動で割り当てる必要がある場合は、デバイス管理 IP アドレスと同じサブネットの IP アドレスを指定します。IP の競合がないことを確認してください。

  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、自動仮想 IP 割り当て方式が使用されている場合は、**Automation** > **Campus Network** > **Fabrics** s ページに移動する必要があります。**IP Pool Settings** ページで、デバイス上の VXLAN 4094 のサブネットを VLAN 4094 アドレスプールにバインドします。この操作を実行しない場合は、通知メッセージがポップアップ表示されます。

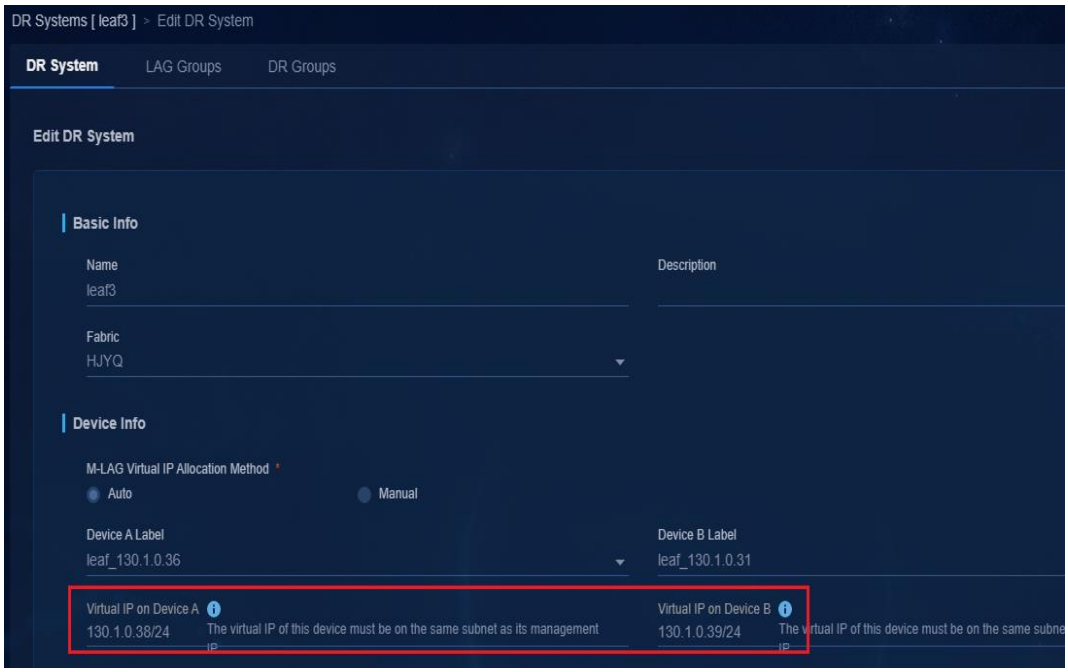
  自動化テンプレートがファブリックに設定されている場合は、自動仮想 IP 割り当て方式を使用するときに、上記の操作を実行する必要はありません。



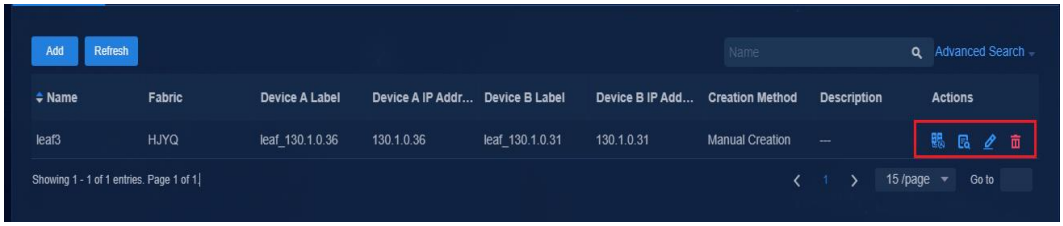


6. コントローラーは自動的に DRNI IPP リンクを作成します。**DR System** タブをクリックして、自動的に設定された仮想 IP アドレスを表示します。

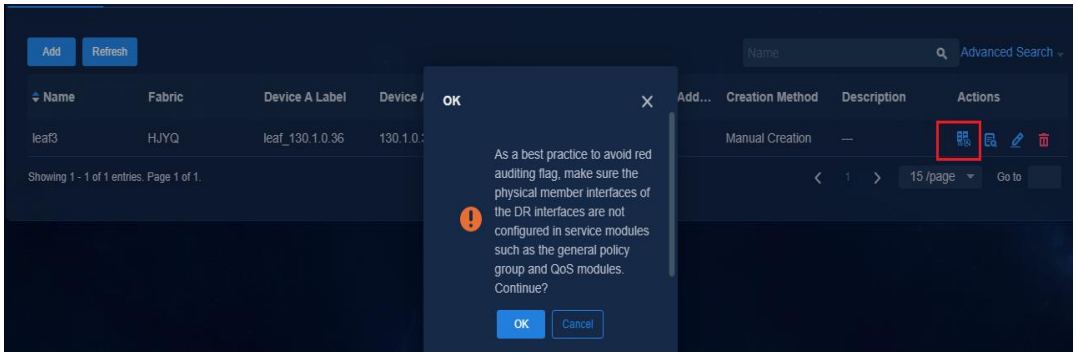
7. DR システムのデプロイ時間は、デバイスモデルによって異なります。デプロイ状態が **Deployed** に変更されるまで待ってから、次の手順に進みます。ベストプラクティスとして、複数の DR システムを同期的にデプロイせず、1 つずつデプロイします。

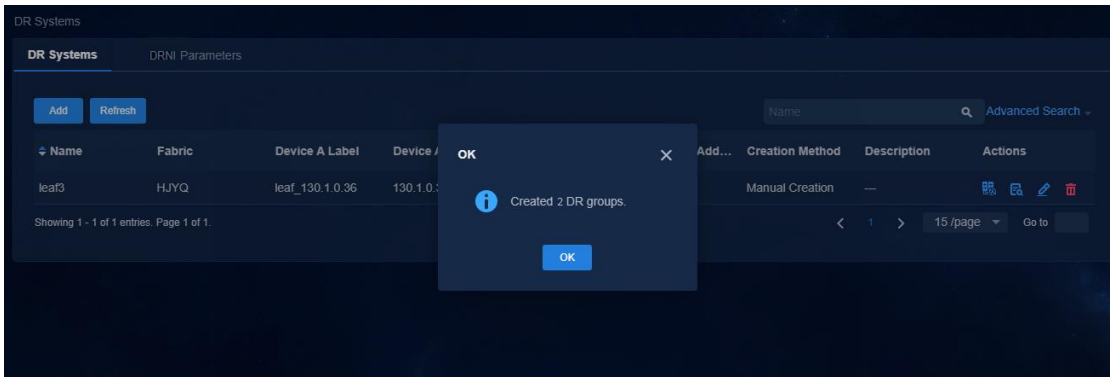


8. **Back** をクリックして **DR System** ページに戻ると、DR システムが正常に作成されたことがわかります。

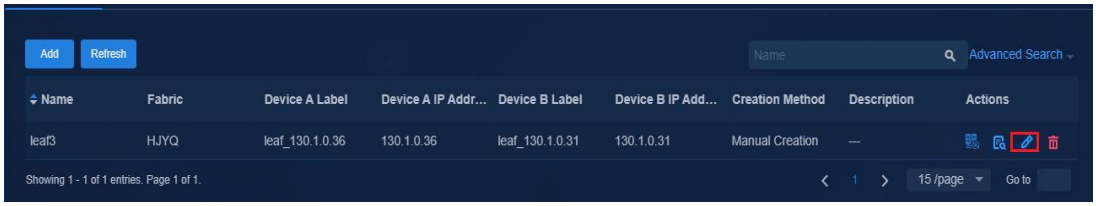


9. アイコンをクリックすると、DR メンバーデバイスは、DR メンバーデバイスとアクセスデバイスを接続するインターフェイスの DR グループを自動的に作成します。
10. DR グループを設定する前に、**Monitor** > **Topology View** > **Campus Topology** に移動して、リーフデバイスとアクセスデバイス間のトポロジリンクがアクティブ化され、正しい状態であることを確認します。

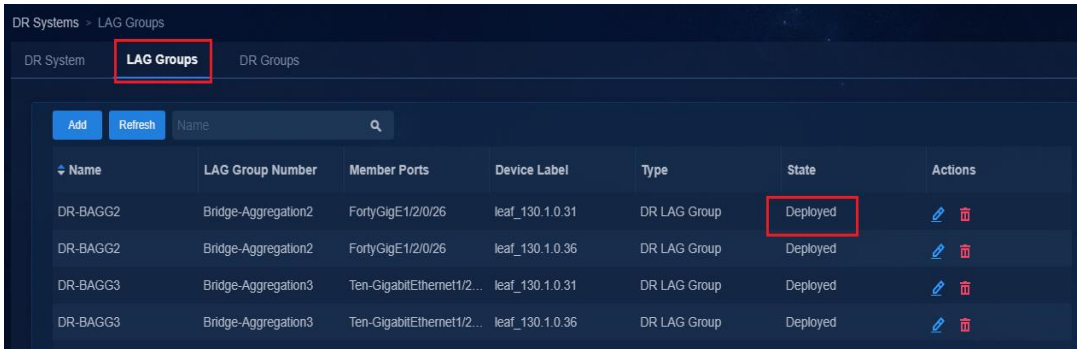




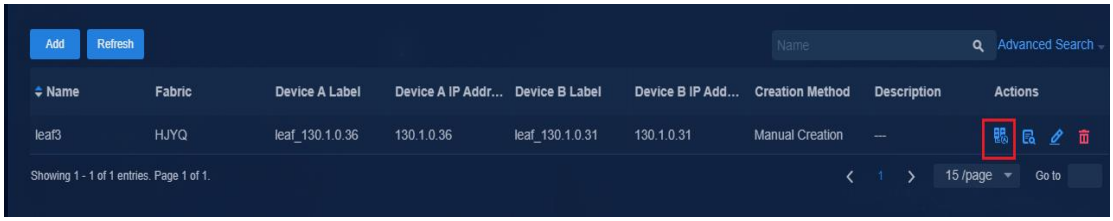
11. 追加した DR システムの **Actions** コラムにあるアイコンをクリックして、DR システム編集ページに入ります。

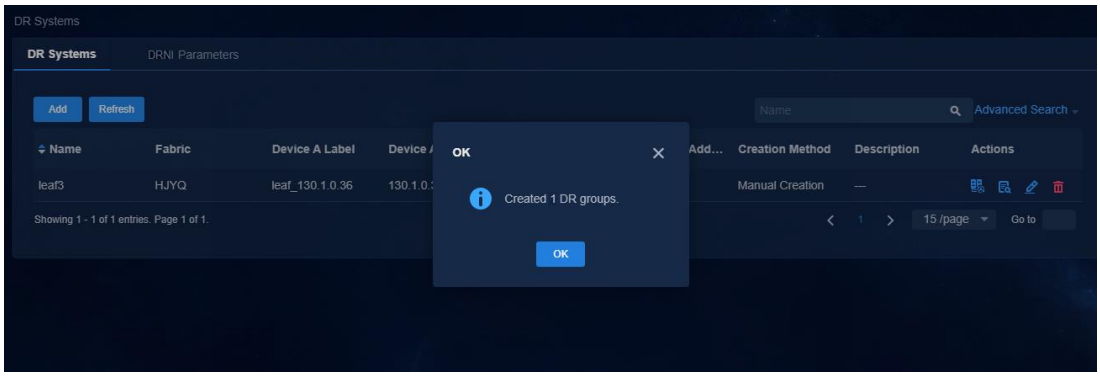


12. **LAG Groups** タブをクリックして、DR グループが自動的に生成されたことを確認します。



13. アクセスデバイスを追加し、アイコンをクリックして DR グループを作成します。





14. DR システムの **Actions** 列のアイコンをクリックして、新しい DR インターフェイスを表示します。

15. DRNI の状態を表示します。

```
<Leaf-S105A> display 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>
```

O&M モニタリング

詳細については、『AD-Campus 6.2 O&M, Monitoring, and Deployment Guide』を参照してください。