Mist Access Assurance 導入ガイド

ジュニパーネットワークス株式会社

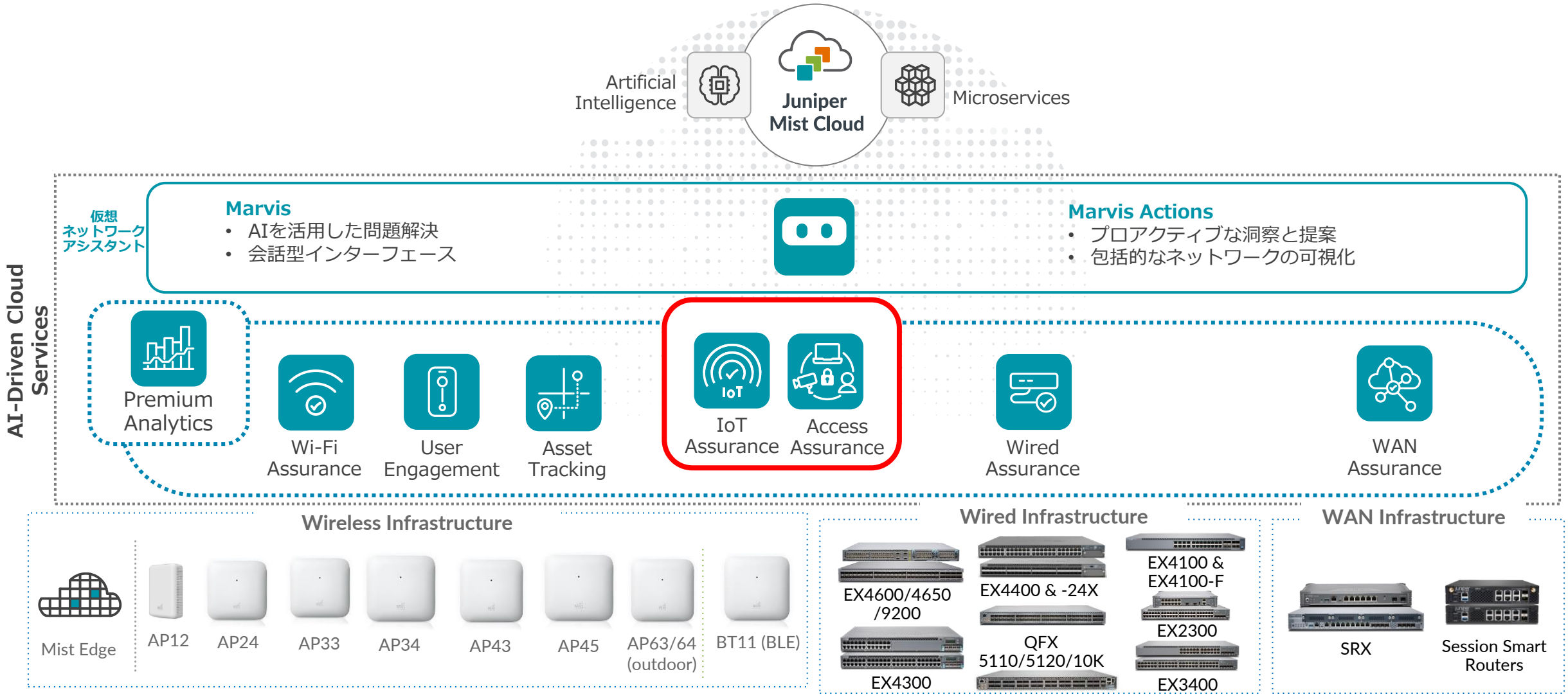
Version 1.0

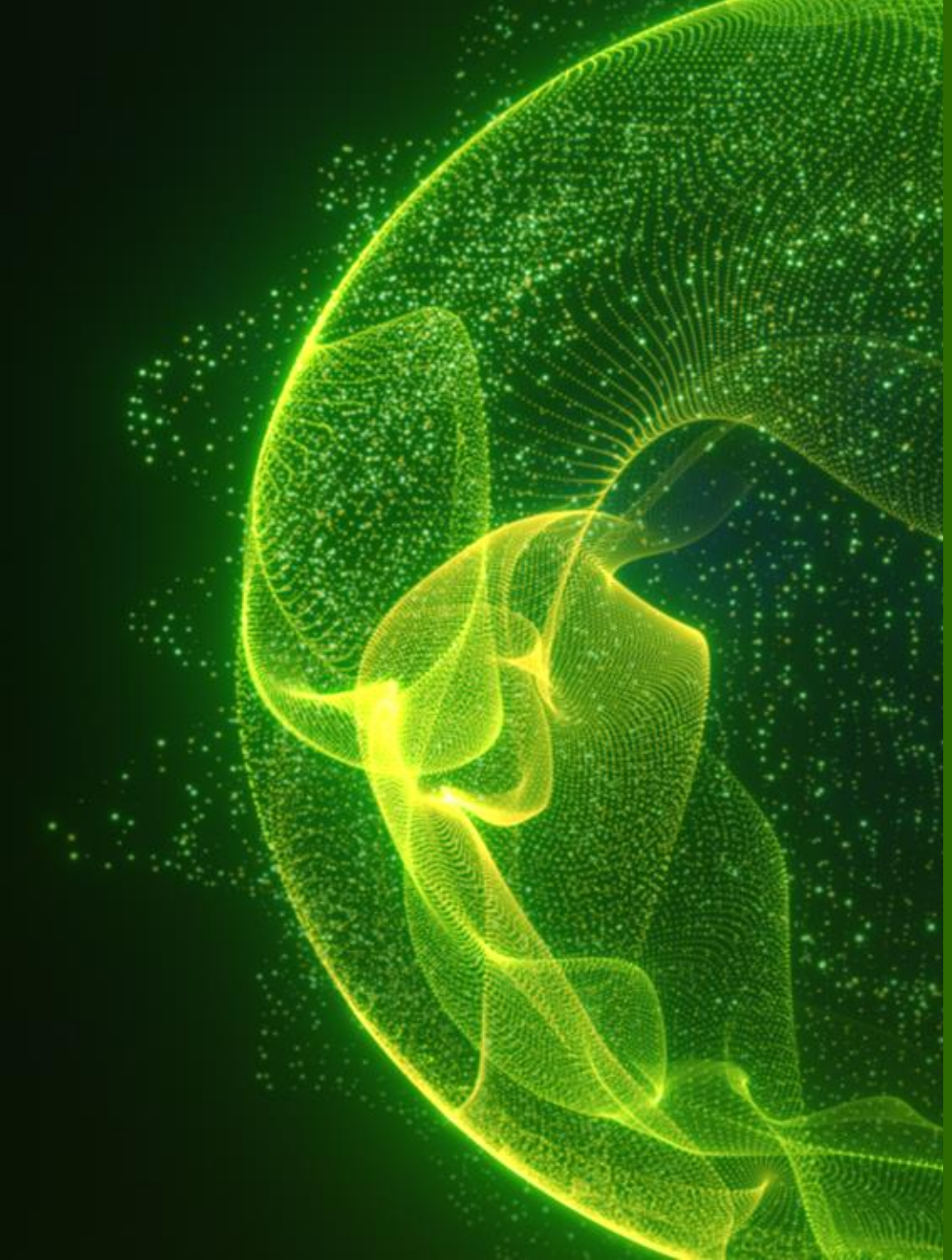
JUNIPer NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、『Mist Access Assurance の導入ガイド 』について説明します
- 手順内容は 2024年10月 時点の Mist Cloud にて確認を実施しております
  実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
  https://www.mist.com/documentation/category/product-updates/
- 設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  Mist Documentation
  Juniper Mist Access Assurance Guide
- 他にも多数の Mist 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html
- **本資料の内容は資料作成時点におけるものであり事前の通告無しに内容を変更する場合があります**
  また本資料に記載された構成や機能を提供することを条件として購入することはできません
- 本資料に記載されている会社名、製品名およびロゴは、各社の商標または登録商標です

Mist – Client to Cloud Full Stack Solutions





Access Assurance / IoT Assurance 購入ガイド

JUNIPER NETWORKS

Access Assurance / IoT Assurance サブスクリプション

ライセンス名：S-CLIENT-S/A-Y

S: Standard
A: Advanced
Y: 契約年数(1年、3年、5年、7年)

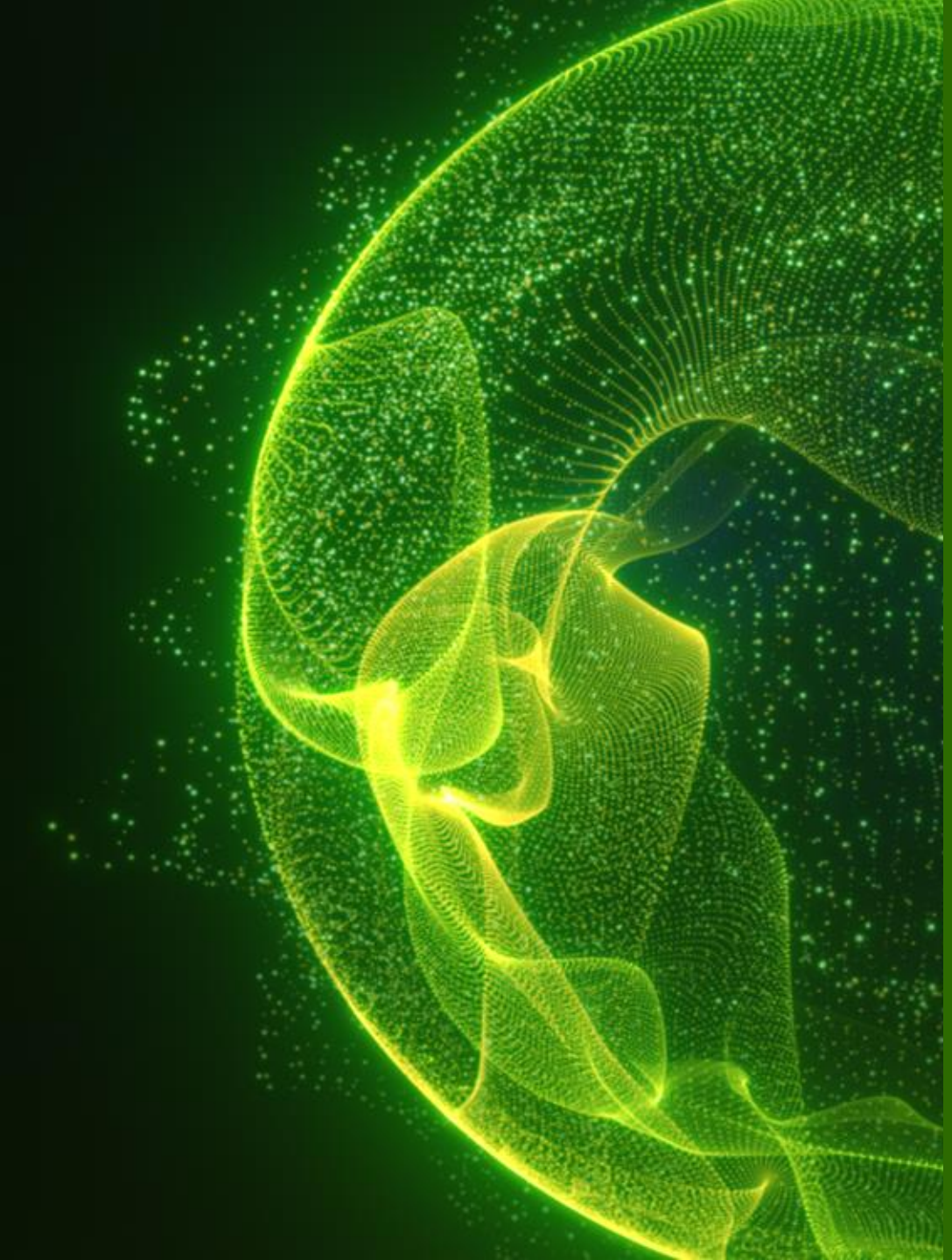
- サブスクリプションは、固有のユーザ/デバイスに紐づくものではなく、アクティブな 1 ユーザ/デバイス毎に消費されます(切断により解放)
- サブスクリプションは、7日間に確認されたアクティブクライアント(同時接続)数の平均に基づいてカウントします

Standard	Advanced
1 ユーザ/デバイス単位のアクティブクライアントに対する標準(Standard) アクセスと IoT Assurance を含みます • EAP-TTLS / EAP-TLS / PEAP-TLS / TEAP / MAB • Cloud PSK / MPSK / Client Onboarding (IoT Assurance)	Standard に加えて下記機能を含みます • UEM / EMM / MDM • ファイアウォール連携 (他社 FW 等との API 連携による動的制御)

型番	説明
S-CLIENT-**S**-1/3/5/7	**Standard** Access & IOT assurance subscription for 1 active client for 1/3/5/7 year
S-CLIENT-**A**-1/3/5/7	**Advanced** Access & IOT assurance subscription for 1 active client for 1/3/5/7 year

※ サードパーティの有線/無線ネットワークインフラストラクチャがある場合は、Mist Edge および機器の台数分のサブスクリプションが必要です

Access Assurance と IoT Assurance は同じ型番で提供されます
IoT Assurance の一部機能は、SUB-MAN (Wi-Fi Assurance) で利用できます



Access Assurance

NAC に求められる要素

認証・認可 (AAA)

802.1X / MAB

ユーザ/デバイスの識別

ユーザ/デバイスの役割の決定

ユーザ ID に基づく VLAN / ポリシーの割り当て

クライアント プロファイリング

パッシブ・フィンガープリント

デバイスタイプ/メーカーの可視化

OS バージョンの可視化

AAA 認証時にデバイスのフィンガープリントを使用

ポスチャ管理

エンドポイントの健全性コンプライアンス
- アンチウイルス
- ファイアウォール
- パッチ/アップデート etc..

エージェントベース/エージェントレス

AAA におけるポスチャコンプライアンス・ステータスの活用

ゼロトラスト ネットワークアクセス

エンドポイントエージェントにより ユーザトラフィックをクラウドに トンネリング

クラウド POP にて
- エンドユーザトラフィックを分類
- ネットワーク・ポリシーを適用

現在の ZTNA は従来の NAC の範囲外でスタンドアローンの概念として存在

クライアント オンボーディング

802.1X(証明書)

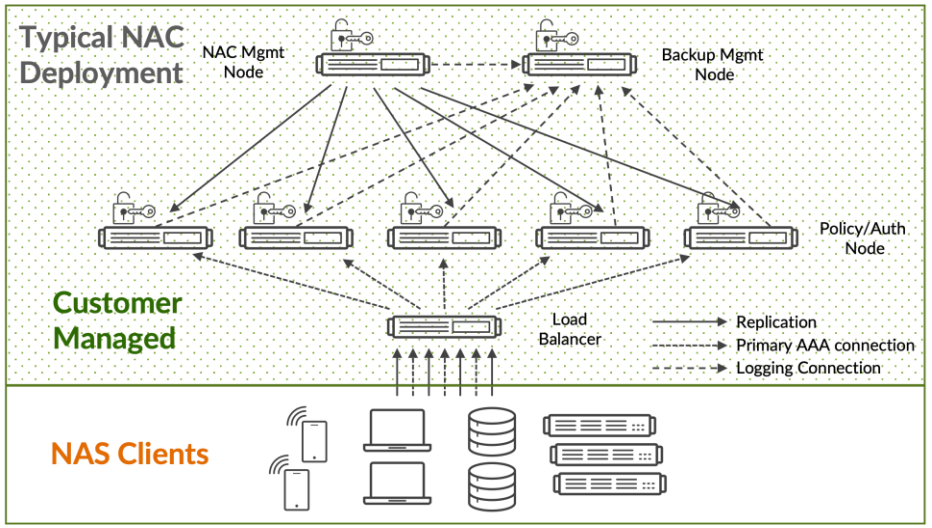
MPSK クレデンシャルを使用した、ポータルベースのアプリベースのエンドユーザデバイスのプロビジョニング

ビルトイン PKI(証明書)インフラ

NAC ソリューションの複雑さ

重要なインフラであり、その必要性は強く認識されているが、多くの課題が山積している
導入・運用・トラブルシュートが複雑になることが多く、安定した NAC の活用には Professional Service や NAC エキスパートが必要になってしまう

ソリューションは複雑かつ脆弱	● サービスの展開と運用に多くの課題 ● 相互運用性により複雑さは飛躍的に増大
トラブルシューティングが複雑	● ログが統合管理されておらず分散 ● エンドツーエンドの不可視性 ● 不十分なインサイト
俊敏性とスケールの欠如	● 従来の LDAP やオンプレでのディレクトリサービス ● オンプレの NAC 機器の拡張には時間が必要
ダウンタイムが必要	● メンテナンス ● 機能アップデート ● セキュリティパッチの適用



現在のNACの複雑さ

1. サービスの冗長性を考慮した設計
2. 高可用性を実現する設計
3. スケールする設計
4. 手動でのスケールアップやスケールダウン
5. サーバハードウェアや仮想マシンの保守
6. アップグレードやセキュリティパッチの適用

Mist Access Assurance はこれらの課題を解決します!!

Mist Access Assurance

Mist AI によって真のクラウドベースのネットワークアクセス制御(NAC) を実現

Juniper Mist Access Assurance は、クラウドベースのセキュアなネットワークアクセス制御(NAC)サービスで、さまざまなデバイスに対する包括的なポリシーフレームワークを提供しますユーザやデバイスの ID に基づいてアクセスを制御し、登録された許可リストにない IoT デバイスにも対応します

- **クラウド ネイティブ アーキテクチャ**
  Network Access Control (NAC)
- **使いやすいアクセスポリシーとワークフロー**
- **冗長性と高可用性**
- **AI を活用し最適化された Day 0/1/2 のオペレーション**

Mist Access Assurance

Mist NAC でできること

AIOps Powered by Mist

ユーザ/デバイスの識別・認証

Identify

Who? What?

- ユーザ
- デバイス ID
- セキュリティポスチャ

Where?

- ロケーション

ポリシー制御

Assign Policy

Micro Segmentation by Identity

ユーザ/デバイスがネットワーク上でどこに属するかを決定し、適切なポリシーを割り当てセグメント化

- VLAN
- Group Based Policy Tag
- Role

サービス状況の確認・検証

Validate Services

Full Stack User Experience

- ユーザは認証されたか？なぜできなかったのか？
- ユーザはどのポリシーに割り当てられたか？
- 認証後のユーザ体験は？

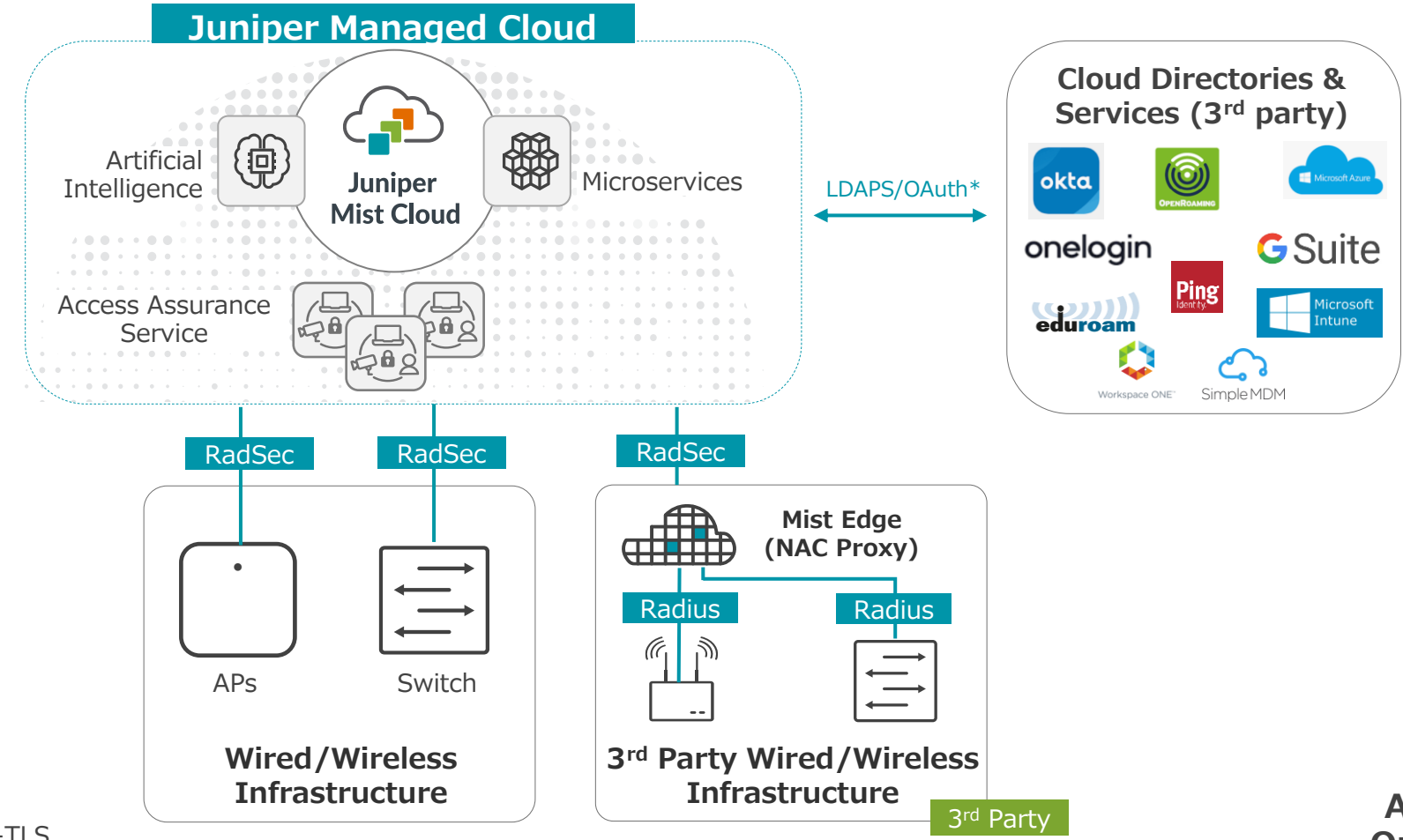
Marvis

- アノマリー検知
- 会話型インタフェースによるトラブルシューティング

Feedback

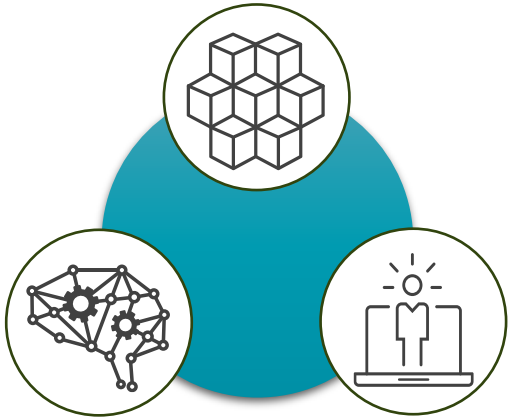
エンドツーエンドのユーザ体感を可視化、ライフサイクルを一元管理可能

Mist Access Assurance



- ✓ EAP-TLS
- ✓ EPA-TTLS(PAP)
- ✓ MAB

Micro-Services based Cloud NAC Offering



AI driven Operations

IT-friendly Day 0-2 operations

Mist Access Assurance

Micro-Services based Cloud NAC Offering

高可用性/高拡張性
定期的・ヒットレスな機能アップグレード
API クロスプラットフォーム統合

AI driven Operations

スタック全体にわたるエンドツーエンドの
ユーザエクスペリエンスの可視性
プロアクティブに問題を検出し迅速に解決

IT-friendly Day 0-2 operations

Wi-Fi / Wired / WAN / NAC にわたる
フルスタックを Mist Cloud で統合管理
シンプルな認証ポリシーとセグメンテーション
エンドツーエンドのネットワークアドミッション制御

Access Assurance 通信・接続要件

Network Types / Communication Requirements

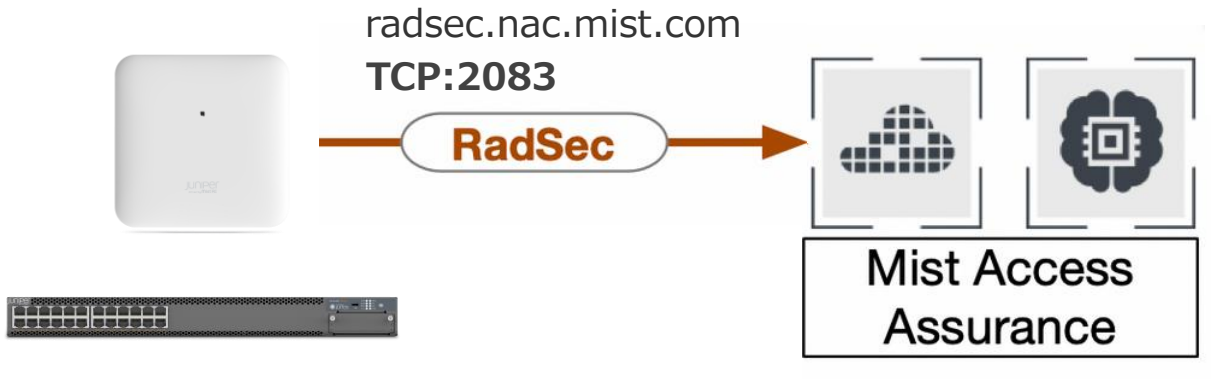
Ports to enable on your firewall
をあわせてご確認ください

Mist AP & EX/QFX

Mist AP
- 0.6.x 以降

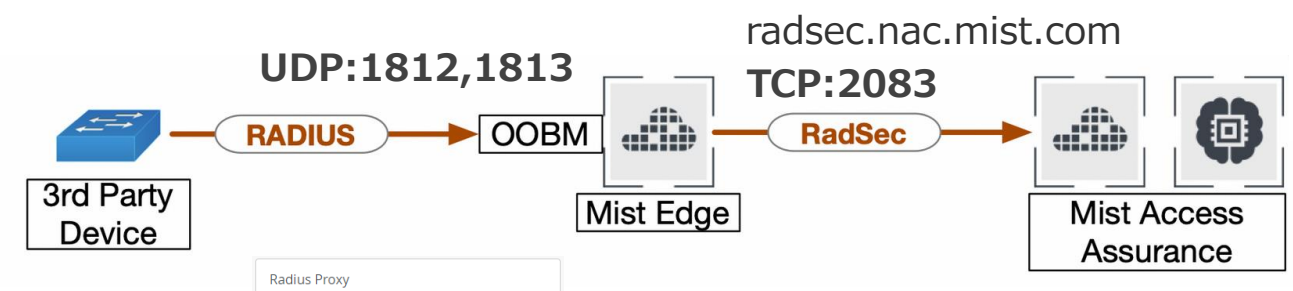
EX/QFX
- 20.4R3-S7 以降
- 21.4R3-S4 以降
- 22.3R3 以降
- 22.4R2 以降
- 23.1R1 以降

Access Assurance
- radsec.nac.mist.com (TCP:2083)

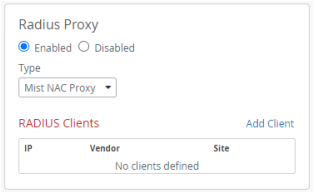


3rd Party Devices

Access Assurance
- radsec.nac.mist.com (TCP:2083)
- Mist Edge(Appliance/VM), ME-VM-OC-PROXY
  - Mist Auth Proxy 専用での利用を推奨
    (Tunterm/OC Proxy 機能との同時利用不可)
  - 冗長性を確保するため複数台の設置を推奨
  - Radius クライアントとして追加が必要
  - Org レベルの認証プロキシとして機能
    (サイト毎の設置不要)
  - 静的 OOBM IP 設定を推奨
    (OOBM IP を Radius サーバとして使用)



Mist Edge Clusters
Add Client



Mist Edge が必要です
Auth Proxy として動作します

Access Assurance - Identity Providers との接続

Integration with Identity Providers

アイデンティティ・プロバイダは、以下のシナリオで使用されます

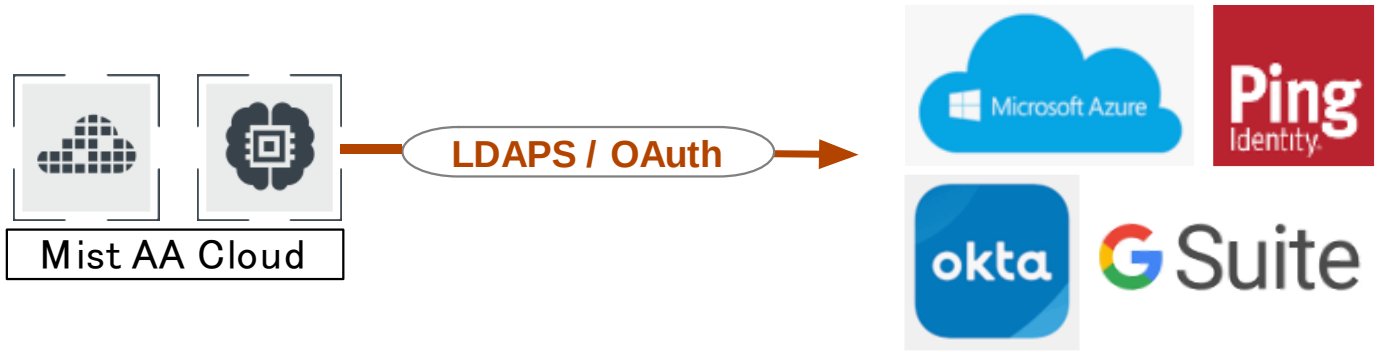
- ユーザ・アカウントのステータスとグループ・メンバーシップの検索 (EAP-TLS ではオプション)
- 証明書の代わりに認証情報を使用したユーザーログイン (EAP-TTLS のみサポート)

Mist Access Assuranceは、クラウドベースのユーザーディレクトリのサポートに重点を置いています

- オンプレミスの Active Directory の場合、Mist AA クラウドからポート 636 経由で LDAPS(Secure LDAP) と直接通信できるようにする必要があります。

LDAPS/OAuth をサポートします

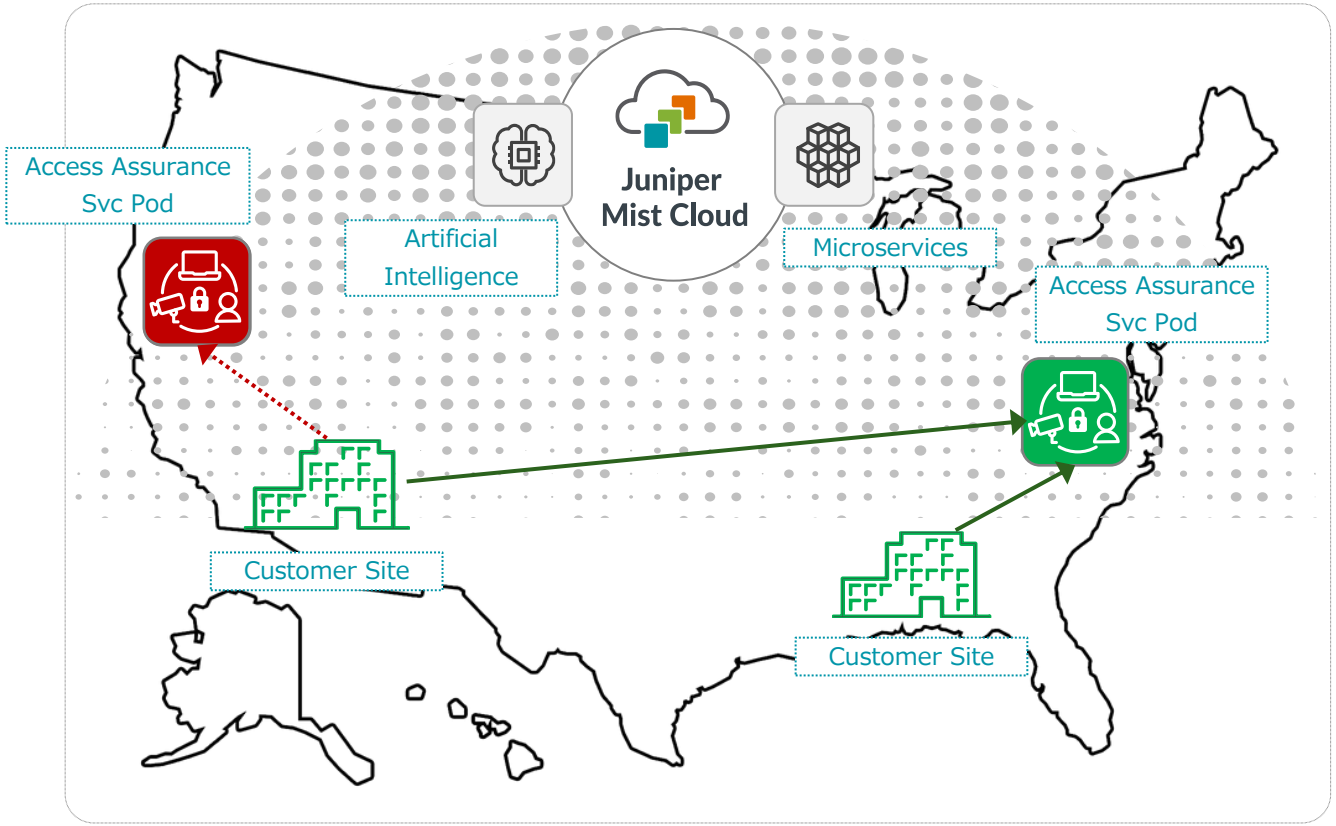
	Azure	Okta	Custom
LDAPS	○	○	○
OAuth	○	○	-



Mist Access Assurance Geo-Affinity

Geo Affinity

- 認証リクエストは、自動的に最寄りの Access Assurance インスタンスに誘導
- PoD の選択は完全に自動化されており特別な設定は不要
- 信頼性の高い冗長化されたネットワークアクセスを提供し、障害時のフェイルオーバーは透過的に動作
- 顧客サイト/デバイスとクラウドインスタンス間の通信はセキュアな RADSEC を使用



主要な認証方式

Auth Type

IEEE802.1X 認証は証明書などのプロビジョニングが必要です
相互認証が行われる EAP-TLS が最も安全な認証方法とされています

802.1X

EAP-TLS — Certificate Base/証明書による認証

- IdPが必須ではなく、必要に応じて使用（アカウントの状態やグループ情報など、ユーザ/デバイス情報をチェックしたい場合）
- 最も安全な認証方法 (証明書は安全なストレージに保存し、適切な管理をします)
- クライアント・デバイスのプロビジョニングが必要(通常、企業では MDM を介して行われる)

User/Device Certificate

EAP-TTLS — Credential Base/ユーザ ID・パスワードによる認証

- 認証にアイデンティティ・プロバイダ（IdP）が必要。
- 802.1XはMFAの場合制限が多く、MITM攻撃を受けやすい。
- Windows11のクレデンシャル・ガードから、パスワード・ベースの認証方法がすべてブロックされるようになった

Username Password

非 802.1X

MAB — MAC アドレスによる認証

- Client Label (MAC アドレス)で端末を識別、活用してスイッチ側でポリシーを適用：VLAN / Role (ダイナミックポートコンフィグで Role を活用)
- API経由で既存のインベントリ管理ソリューションと統合し、各Client ラベルのデバイス登録を自動化
- 代表的なデバイスの種類: プリンター、IP 電話、IoT 有線デバイス

Identity: Device MAC

MPSK — 複数の PSK を作成・管理可能、パスフレーズによる認証

- IoT Assurance を活用して、MPSK(PSK管理・ライフサイクル管理・Client Onboarding) を使用する
- エンドデバイスのサプリカントを透過的にサポート
- PSK をアイデンティティとして使用した一貫性のあるポリシー（VLAN/Role）の適用
- 従来の 802.1X と同様の可視性を実現

Identity: PSK Name

EAP-TTLS の注意点

Considerations for EAP-TTLS

- クレデンシャルベース(username/password)による認証はセキュリティ上の多くの懸念事項があります
  例) MITM、盗用、脆弱なパスワード、使いまわし etc..
- クラウドベースの Identity Providers では、通常認証プロトコルは PAP のみサポートされ、 PEAP-MSCHAPv2 および EAP-TTLS/MSCHAPv2 はサポートされません
- Apple 製品は、username/password の入力時、デフォルトで PEAP-MSCHAPv2 または EAP-TTLS/MSCHAPv2 による認証プロトコルを使用し、PAP は使用することができません
  PAP を使用するためには、 Apple Configurator tool により PAP を有効化したプロファイル作成、端末にインストールする必要があります
  REF: EAP-TTLS – Apple Client Initial Configuration
- Windows 11 では、Credential Guard がデフォルトで有効になり、安全でないプロトコルの使用がブロックされます
  Wi-Fi での MS-CHAPv2 ベースの接続はセキュリティ上の懸念があり、証明書ベースの認証が推奨されています
  REF: Credential Guard を使用するときの考慮事項と既知の問題
- EAP-TTLS は EAP-TLS と比較して認証ステップが多い
  EAP-TLS では、ステップ数が少ないため認証負荷が少ない、使いまわしができずデバイスを特定可能、偽装が難しいなどのメリットがあります

特別の理由がない限り、EAP-TLS が推奨されます

設定フロー

Configuration Flow

STEP 01 | STEP 02 | STEP 03 | STEP 04

EAP-TLS

証明書発行 ※移行も可
- サーバ証明書 ※デフォルト使用時省略可
- クライアント証明書

Mist
- IdP 設定(Optional)

デバイス(PC/モバイル)
- ルート CA 証明書のインポート
- クライアント証明書のインポート
- 有線・無線設定

EAP-TTLS

証明書発行 ※移行も可
- サーバ証明書※デフォルト使用時省略可

Mist
- IdP 設定

デバイス(PC/モバイル)
- ルート CA 証明書のインポート
- 有線・無線設定

MAB

デバイス(プリンタ、IoT etc..)
- MAC アドレスの確認

Wireless

SSID
Security
WAP2/Enterprise(802.1X)
Authentication Servers
Mist Auth
VLAN etc

Wired

Authentication Servers
Mist Auth
Port Profiles
dot1x
MAB
VLAN etc..
Port Configuration
Port ID
Configuration Profile

Auth Policy Labels

AAA Attribute
- VLAN
- Realm
- User Name
- GBP Tag
- Session Timeout
- Custom Vendor Specific Attribute
- Custom Standard Radius Attribute
- Dynamic Wired Port Configuration

Certificate Attribute
- Common Name(CN)
- Subject
- Serial Number
- Issuer
- Subject Alternative Name(SAN)

Client List

SSID

MDM Compliance
- Compliant
- Non Compliant
- Unknown

Client Label

Auth Policies

Auth Type
- EAP-TTLS
- TEAP
- MAB
- PSK
- Admin Auth

Port Types
- Wireless
- Wired

Vendors
- Generic IETF
- Cisco Wireless
- Cisco Wired
- Juniper
- Cisco Meraki
- HPE/Aruba
- Palo Alto

Auth Label ※ユーザ定義

Site/Site Group

+ Optional

Wireless **WxLAN Policy**

Wired **Switch Policy** BETA

Configurations

- Wireless - AP 設定
- Wired - Switch 設定
- Certificate
- Identity Providers
- Auth Policy
- Auth Policy Labels

Wireless - AP 設定

JUNIPER NETWORKS

Wireless - AP 設定

AP 設定概要

Site > WLANs での設定も可能ですが、WLAN Templates での設定が推奨です

[SSID] を設定、[Security] で [WPA2]、[Enterprise(802.1X)] を設定、[Authentication Servers] を [Mist Auth] に設定、環境に応じた [VLAN] 設定をします

WLAN Templates(Organization)

WLANs

SSID	Security	Authentication Servers	VLAN
SSID	**WPA2 > Enterprise(802.1X)**	**Mist Auth**	• Untagged • Tagged • Pool • Dynamic (VLAN Type)

Site Assign

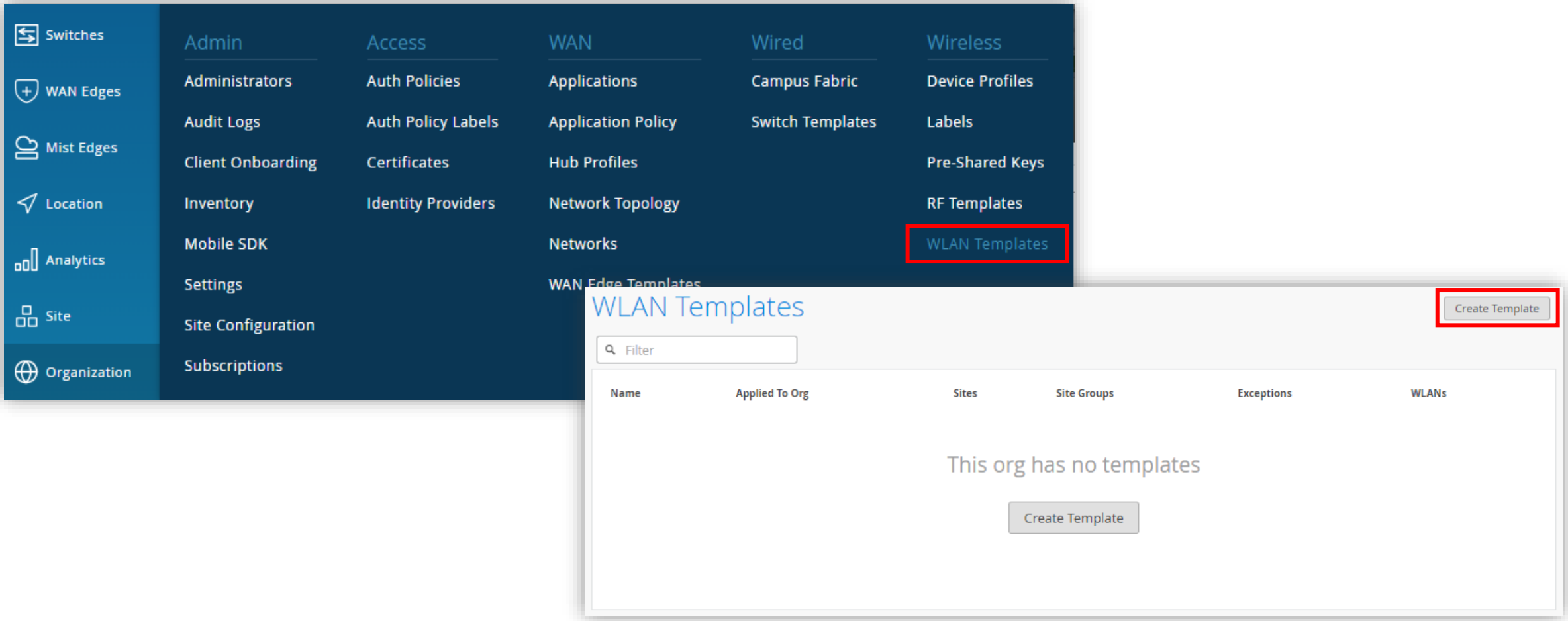
WLANs(Site)

SSID	Security	Authentication Servers	VLAN
SSID	**WPA2 > Enterprise(802.1X)**	**Mist Auth**	• Untagged • Tagged • Pool • Dynamic (VLAN Type)

Wireless - AP 設定

WLAN Templates: Create Template

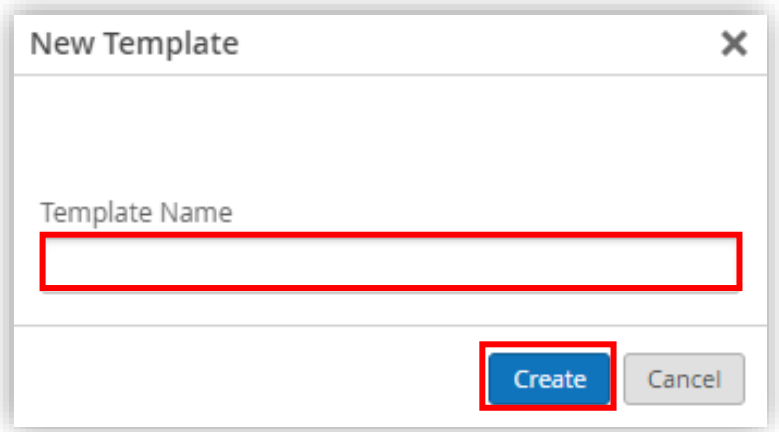
1. [Organization] から [WLAN Templates] をクリックします
2. [Create Template] をクリックします



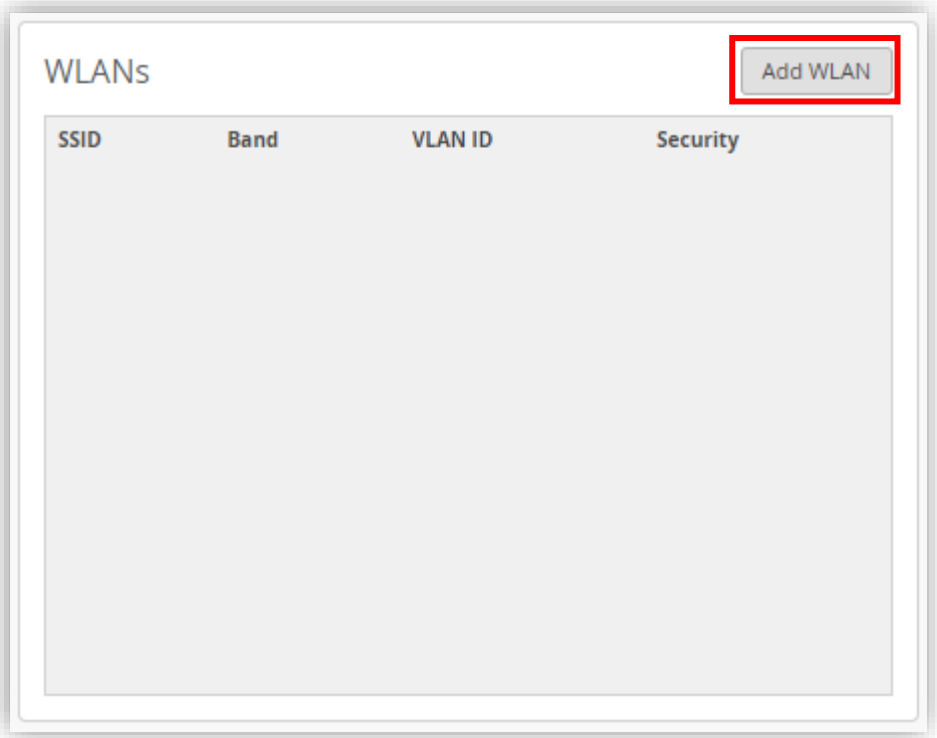
Wireless - AP 設定

WLAN Templates: Add WLAN

3. [Template Name] を設定し、[Create] をクリックします



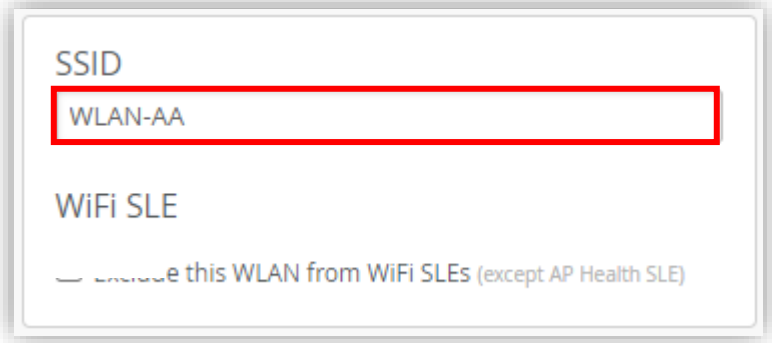
4. [Add WLAN] をクリックします



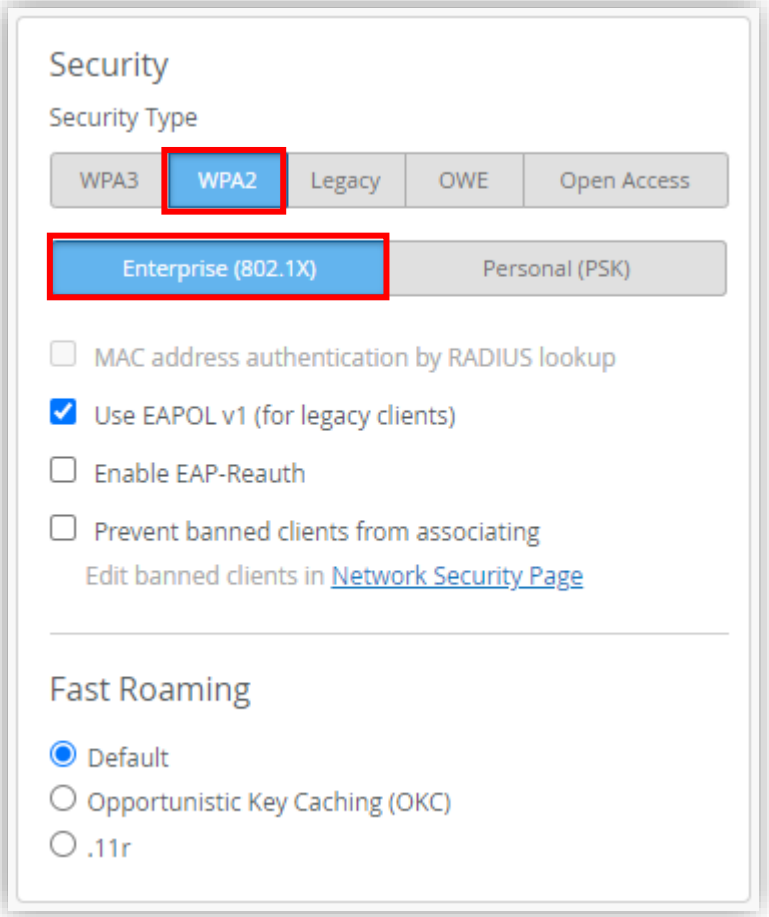
Wireless - AP 設定

WLAN Templates: SSID / Security

5. [SSID] を設定します



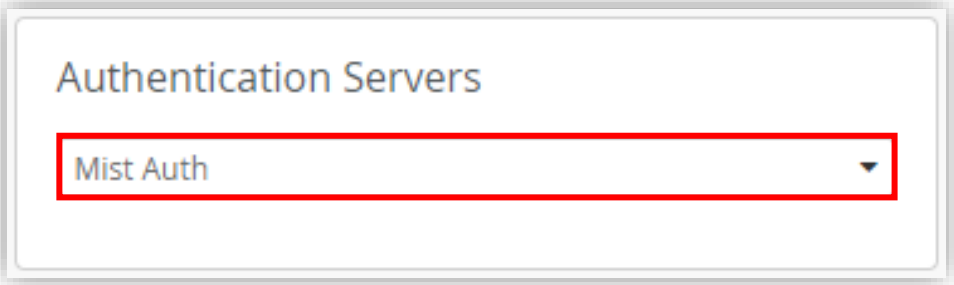
6. [Security] で、[WPA2]、[Enterprise(802.1X)] を選択します



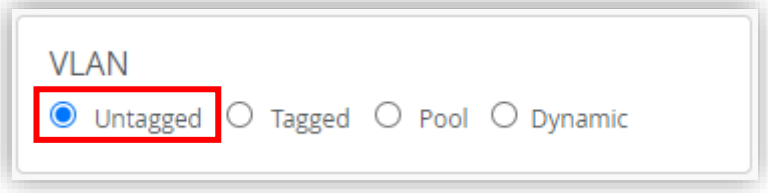
Wireless - AP 設定

WLAN Templates: Authentication Servers / Untagged VLAN

7. [Authentication Servers] で [Mist Auth] を選択します



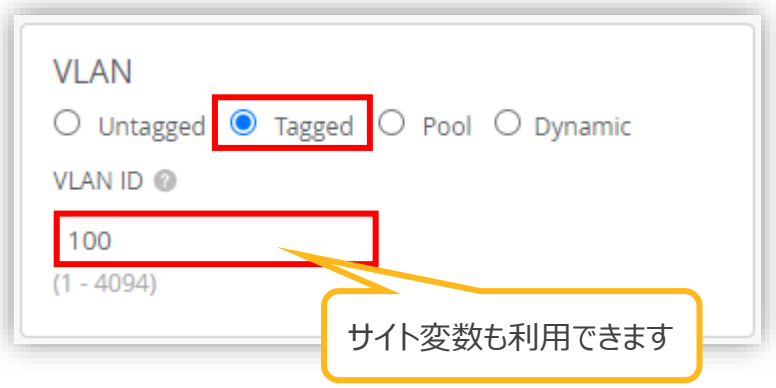
8. (a) Untagged VLAN
[Untagged] を選択します



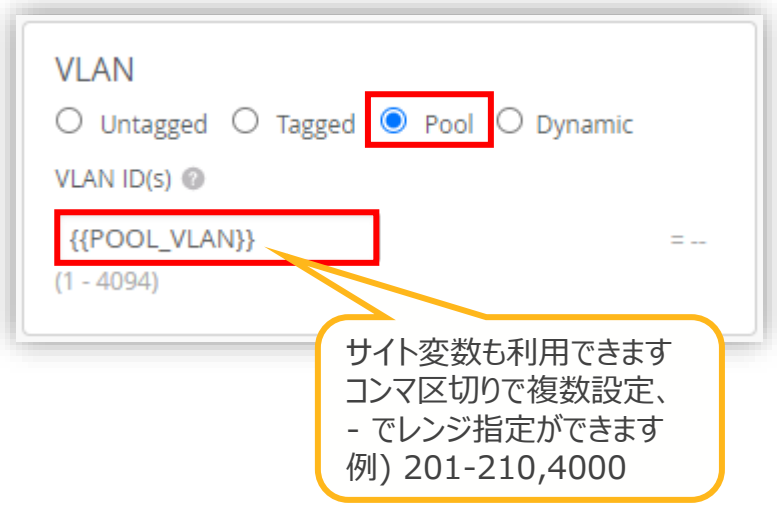
Wireless - AP 設定

WLAN Templates: Tagged VLAN / Pool VLAN

8.(b) Tagged VLAN
[Tagged] を選択し、[VLAN ID] を設定します



8.(c) Pool VLAN
[Pool] を選択し、[VLAN ID(s)] リストを設定します

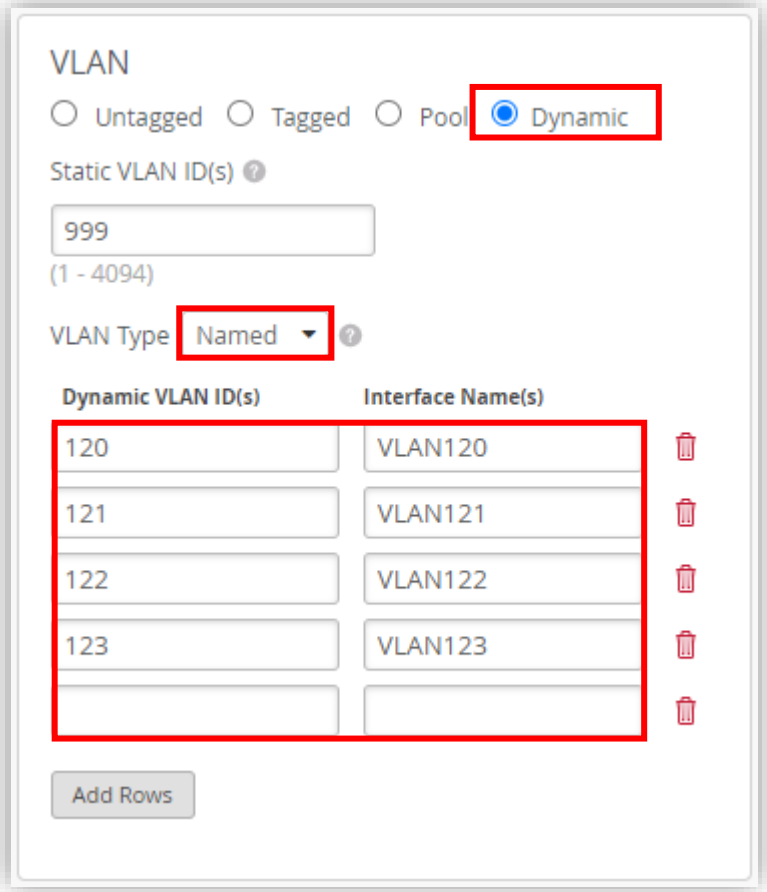


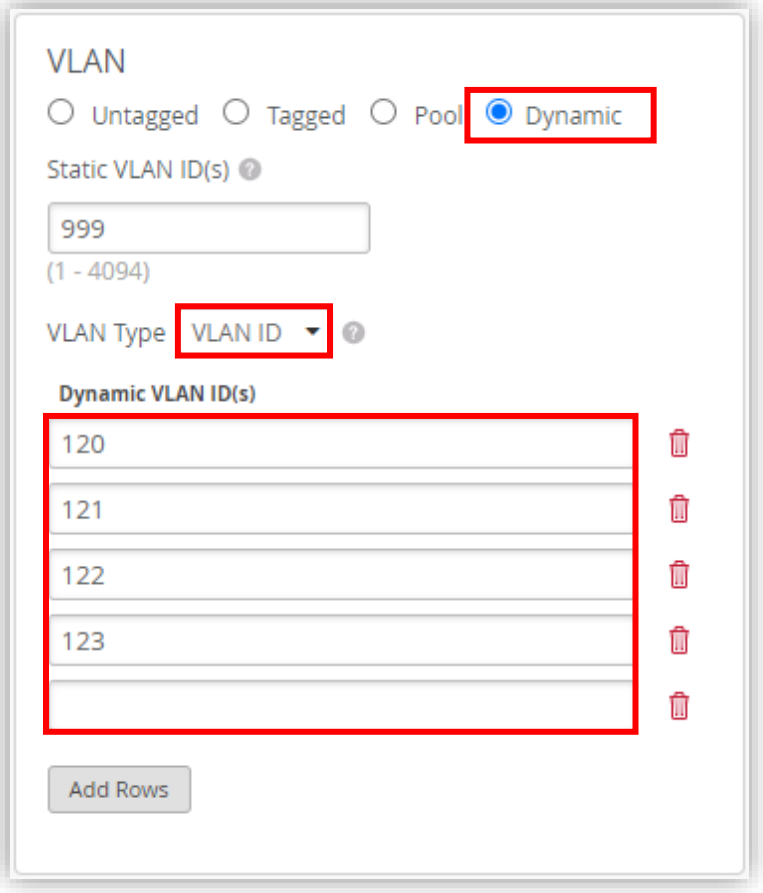
Network は別途設定してください

Wireless - AP 設定

WLAN Templates: Dynamic VLAN

8.(d) Dynamic VLAN
[Dynamic] を選択します





Static VLAN ID(s)

VLAN ID の指定がない場合に所属する VLAN
検疫ネットワークなどを設定します

VLAN Type

Named:
Airespace-Interface-Name または、Tunnel-Private-Group-ID の Radius 属性をサポートし、1 つの VLAN、VLAN プール、またはサイト変数を指定することができます

VLAN ID:
Tunnel-Private-Group-ID の Radius 属性をサポートし、1 つの VLAN、VLAN 範囲、またはサイト変数を指定することができます

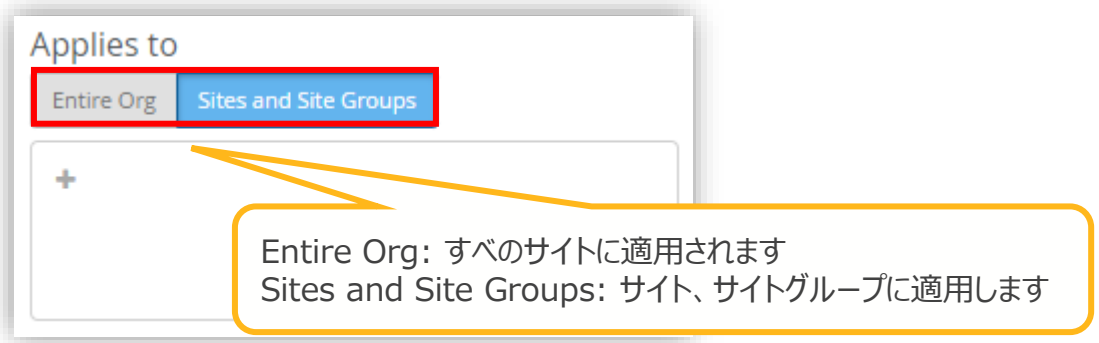
Dynamic VLAN ID(s) を設定します
Named の場合は VLAN 名も入力します

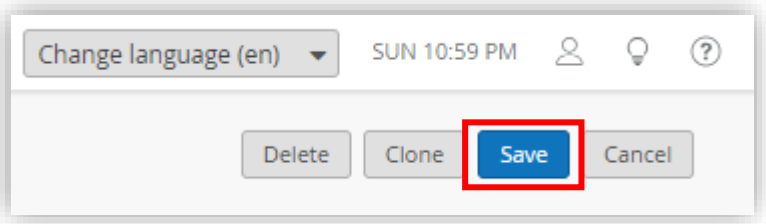
Wireless - AP 設定

WLAN Templates: Create / Applies to / Save

9. [Create] をクリックして、WLAN 設定を完了します

10. WLAN Template を適用するサイトを選択し、[Save] をクリックして、設定を完了します



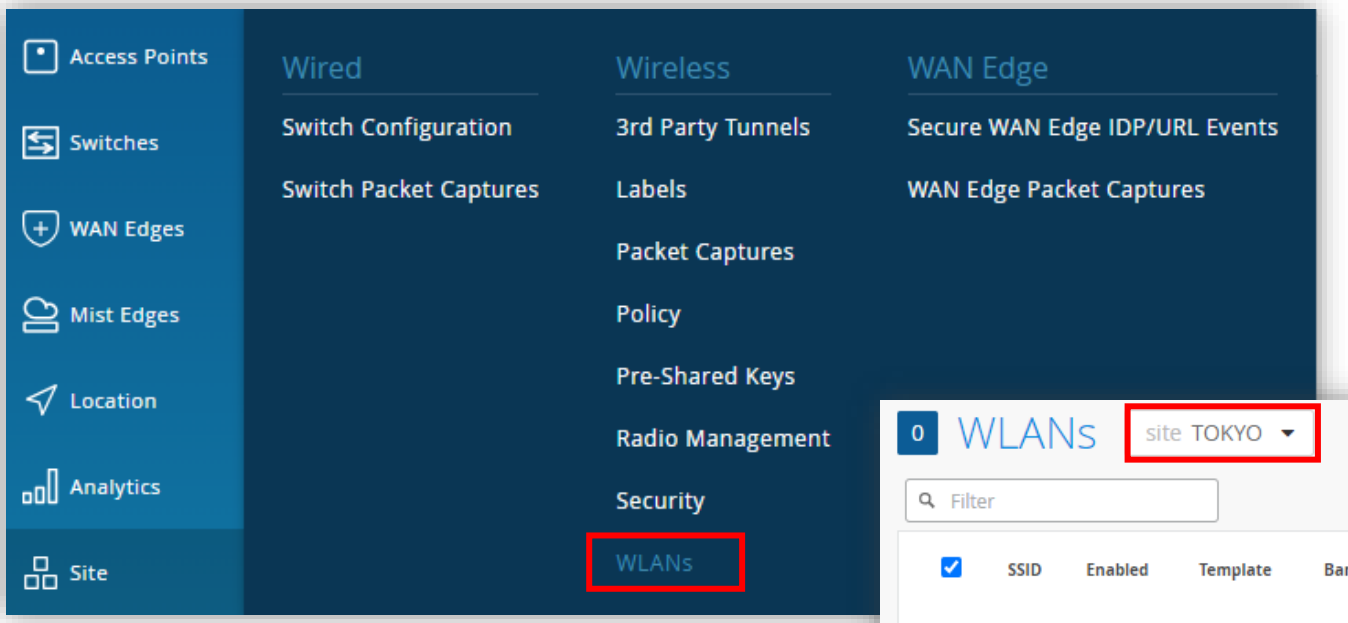


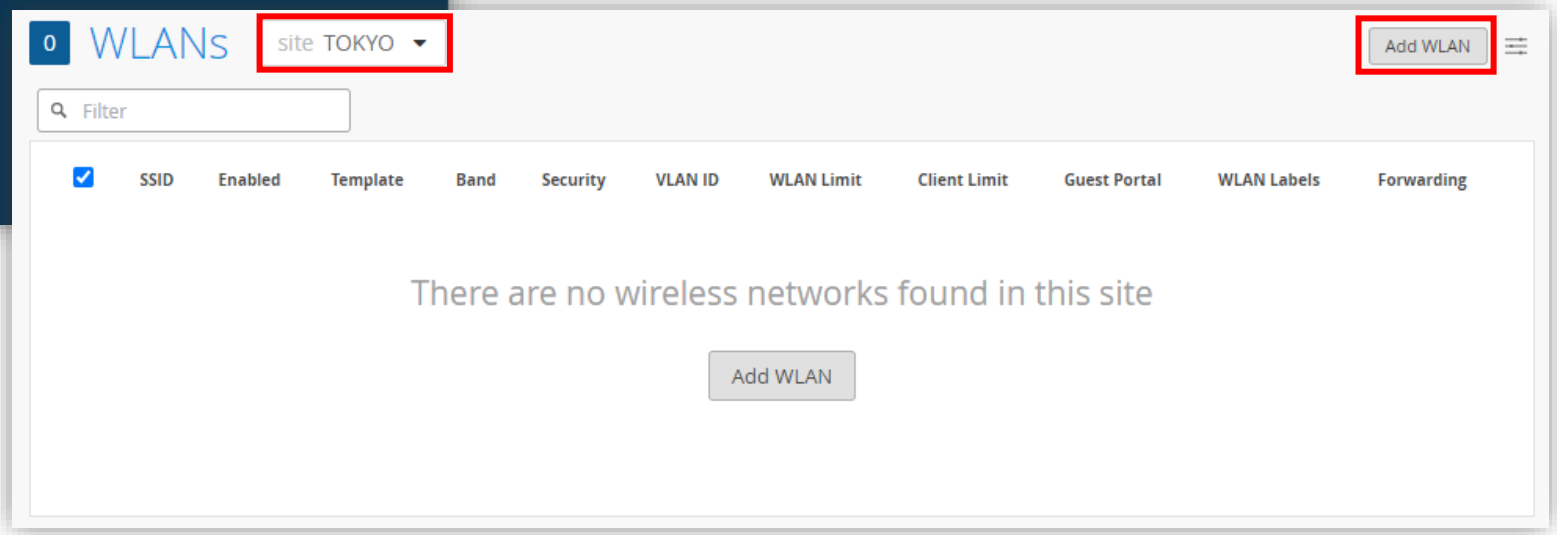
Wireless - AP 設定

WLANs: Add WLAN

WLAN Template を使用しない場合、
Site > WLANs より設定します

1. [Site] から [WLANs] をクリックします
2. [Site] を選択し、[Add WLAN] をクリックします

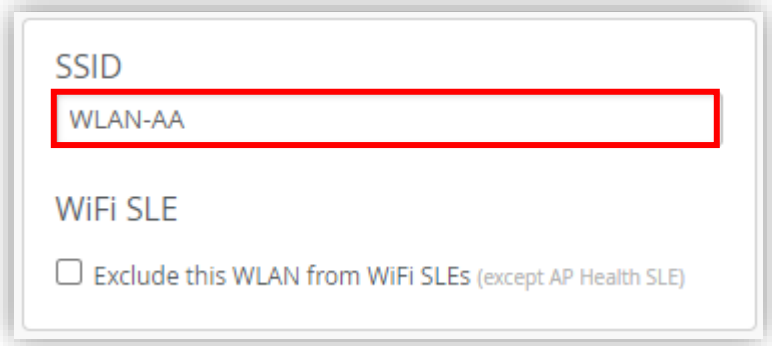




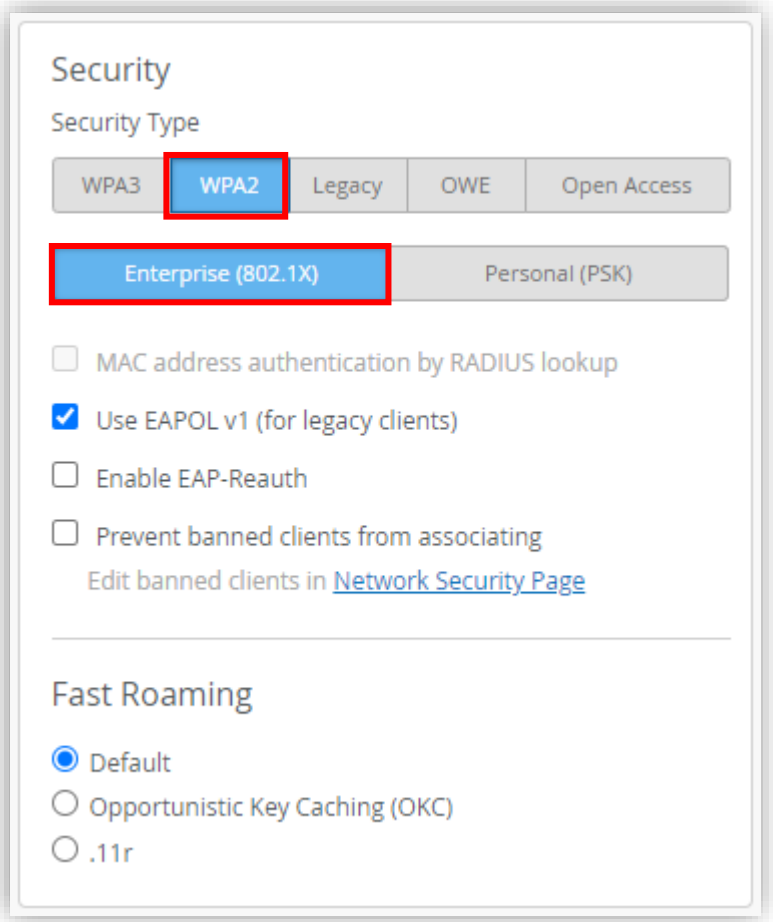
Wireless - AP 設定

WLANs: SSID / Security

3. [SSID] を設定します



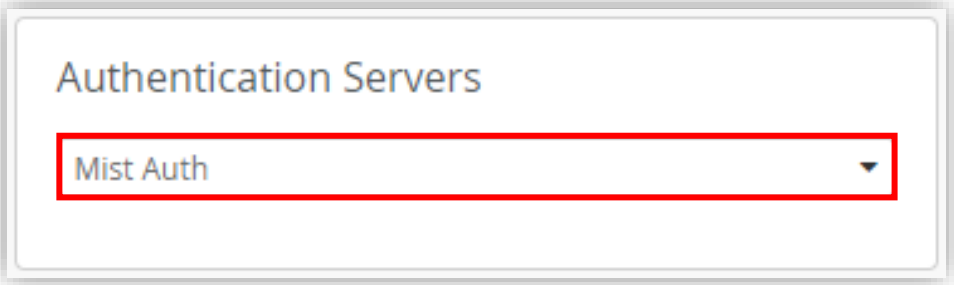
4. [Security] で、[WPA2]、[Enterprise(802.1X)] を選択します



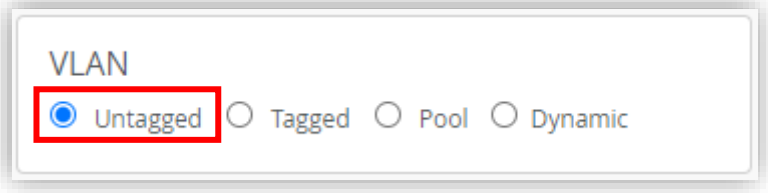
Wireless - AP 設定

WLANs: Authentication Servers / Untagged VLAN

5. [Authentication Servers] で [Mist Auth] を選択します



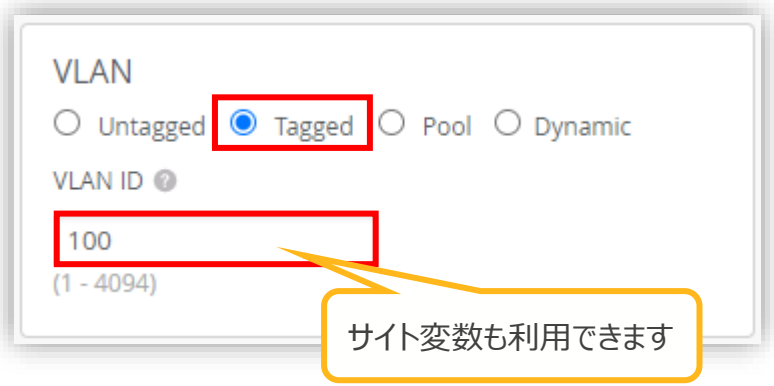
6. (a) Untagged VLAN
[Untagged] を選択します



Wireless - AP 設定

WLANs: Tagged VLAN / Pool VLAN

6.(b) Tagged VLAN
[Tagged] を選択し、[VLAN ID] を設定します



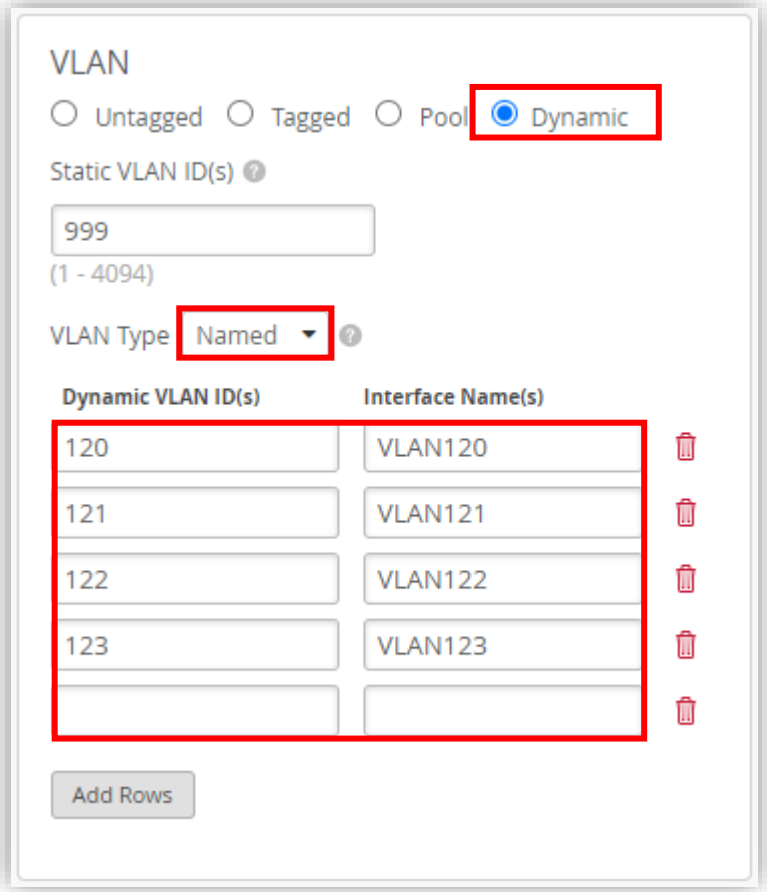
6.(c) Pool VLAN
[Pool] を選択し、[VLAN ID(s)] リストを設定します

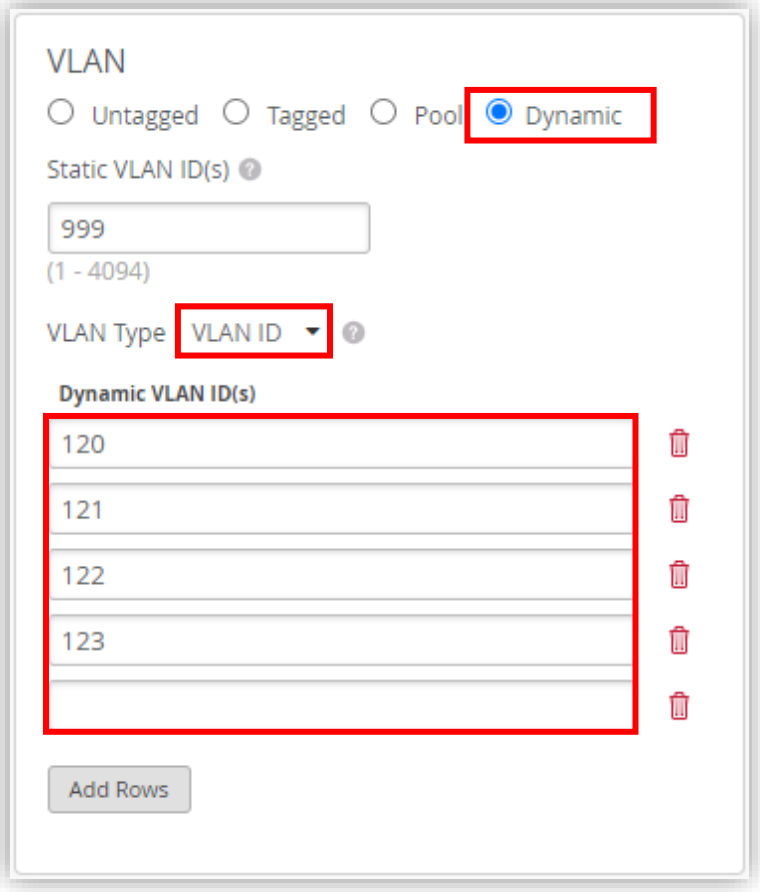
Network は別途設定してください

Wireless - AP 設定

WLANs: Dynamic VLAN

6.(d) Dynamic VLAN
[Dynamic] を選択します





Static VLAN ID(s)

VLAN ID の指定がない場合に所属する VLAN
検疫ネットワークなどを設定します

VLAN Type

Named:
Airespace-Interface-Name または、Tunnel-Private-Group-ID の Radius 属性をサポートし、1 つの VLAN、VLAN プール、またはサイト変数を指定することができます

VLAN ID:
Tunnel-Private-Group-ID の Radius 属性をサポートし、1 つの VLAN、VLAN 範囲、またはサイト変数を指定することができます

Dynamic VLAN ID(s) を設定します
Named の場合は VLAN 名も入力します

Wireless - AP 設定

WLANs: Create

7. [Create] をクリックして、WLAN 設定を完了します

Wired - Switch 設定

JUNIPER NETWORKS

Wired - Switch 設定

Switch Configuration 概要

Switch Configuration(Site)、各 SW でも設定できますが、Switch Templates での設定が推奨です

[Authentication Servers] で [Mist Auth] に設定、[Port Profiles] で IEEE802.1X 認証関連の設定を行い、[Port Configuration] の [Port IDs] でポート指定、[Configuration Profile] に作成したプロファイルを指定します

Switch Templates(Organization)

Switch Configuration(site)

Authentication Servers

- **Mist Auth**
- Source Address

Port Profiles

- **Use dot1x authentication**
- Allow Multiple Supplicants
- Dynamic VLAN
  - Networks
- Mac authentication
  - Mac authentication only
  - Authentication Protocol
- Use Guest Network
  - Guest Network
- Bypass authentication when server is down

Port Configuration

Select Switches Configuration
Info
- Name
- Applies to switch name
- Applies to switch role
- Applies to switch model

Port Config
- Port IDs
- Configuration Profile

Site Assign

Authentication Servers

- **Mist Auth**
- Source Address

Port Profiles

- **Use dot1x authentication**

…省略

Port Configuration

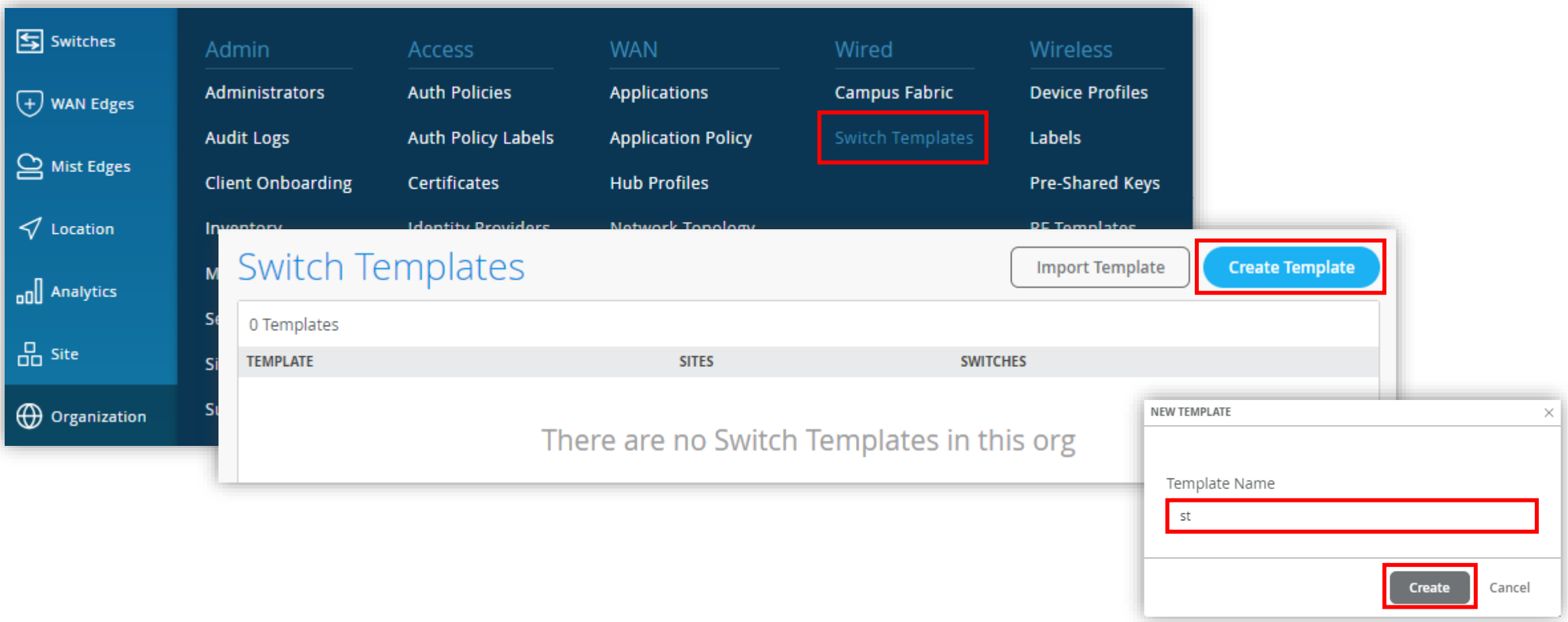
- Port IDs
- Configuration Profile

Switches > {Switch}

Wired - Switch 設定

Switch Templates: Create Template

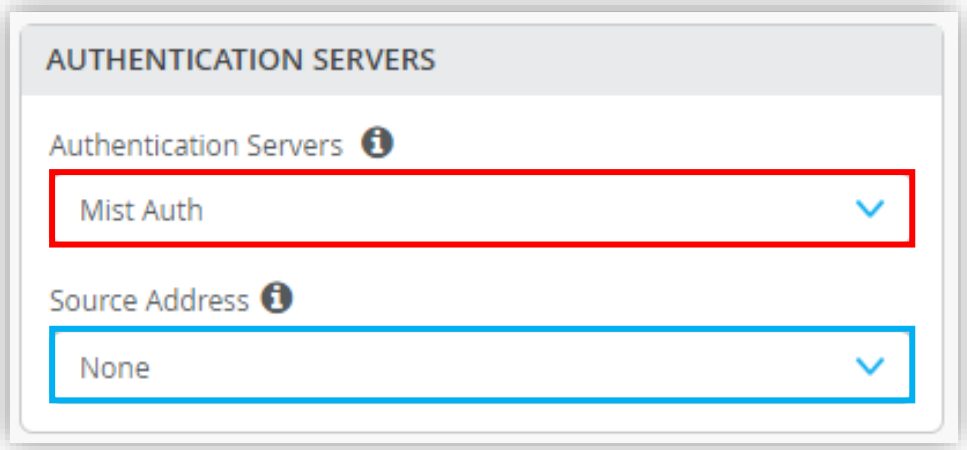
1. [Organization] から、[Switch Templates] をクリックします
2. [Create Template] をクリック、 [Template Name] にテンプレート名を設定、[Create] をクリックします



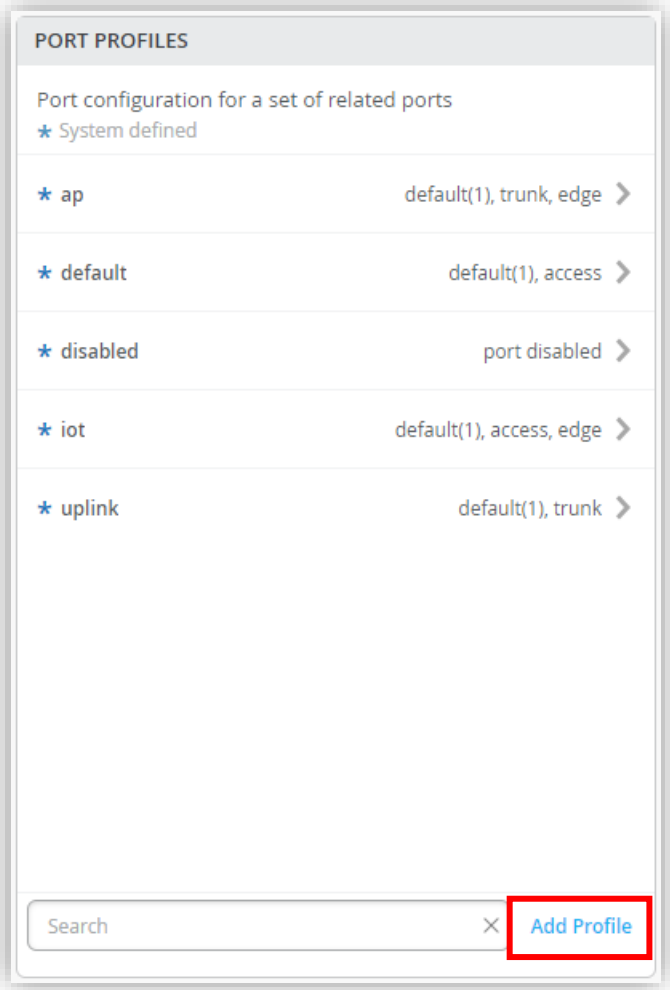
Wired - Switch 設定

Switch Templates: Authentication Servers / Port Profiles

3. [Authentication Servers] で [Mist Auth] を選択します



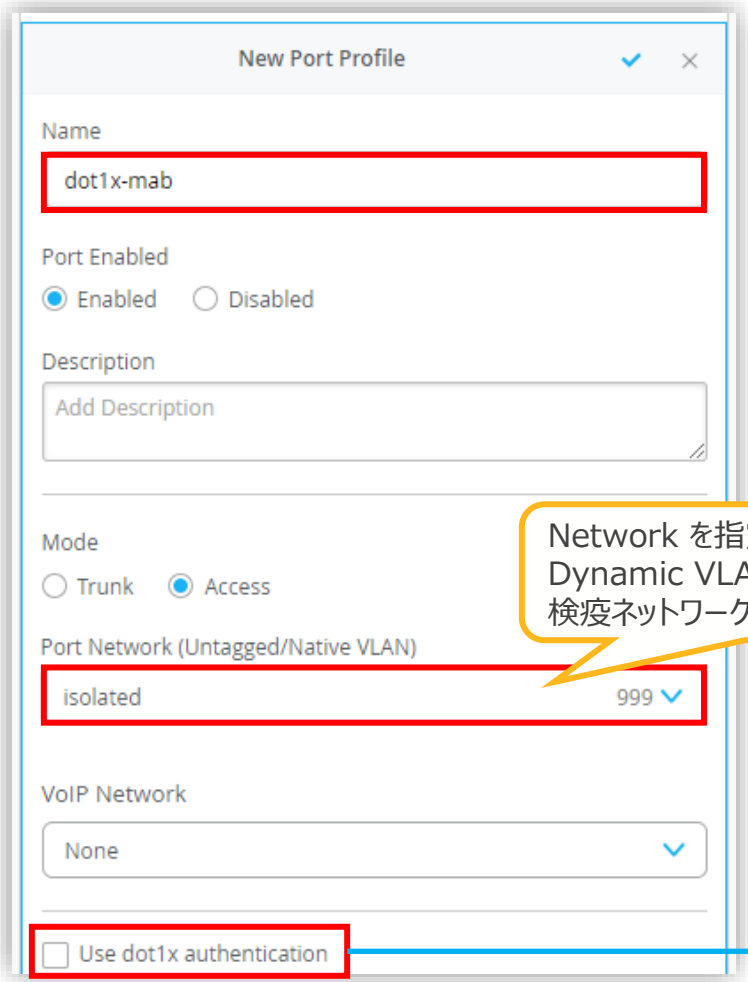
4. [Port Profiles] で [Add Profile] をクリックします



Wired - Switch 設定

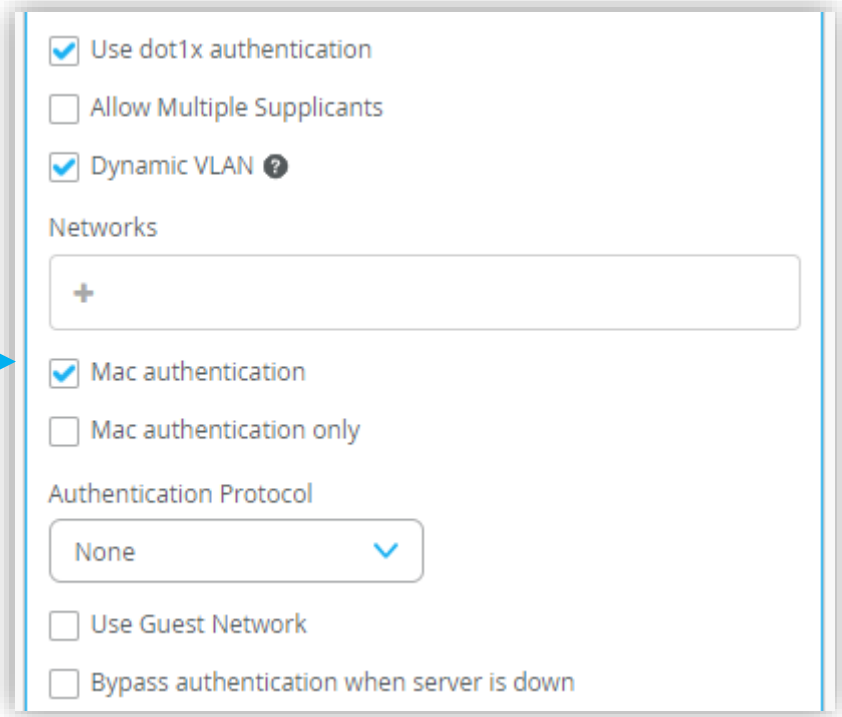
Switch Templates: Port Profiles

5. [Name] を設定し、[Use dot1x authentication] をチェック、必要な項目を設定します



[Name] にプロファイル名を設定します

Network を指定します
Dynamic VLAN を設定する場合は、検疫ネットワークなどを指定します



[Use dot1x authentication] をチェックすると、以降のオプションが表示されます

設定詳細

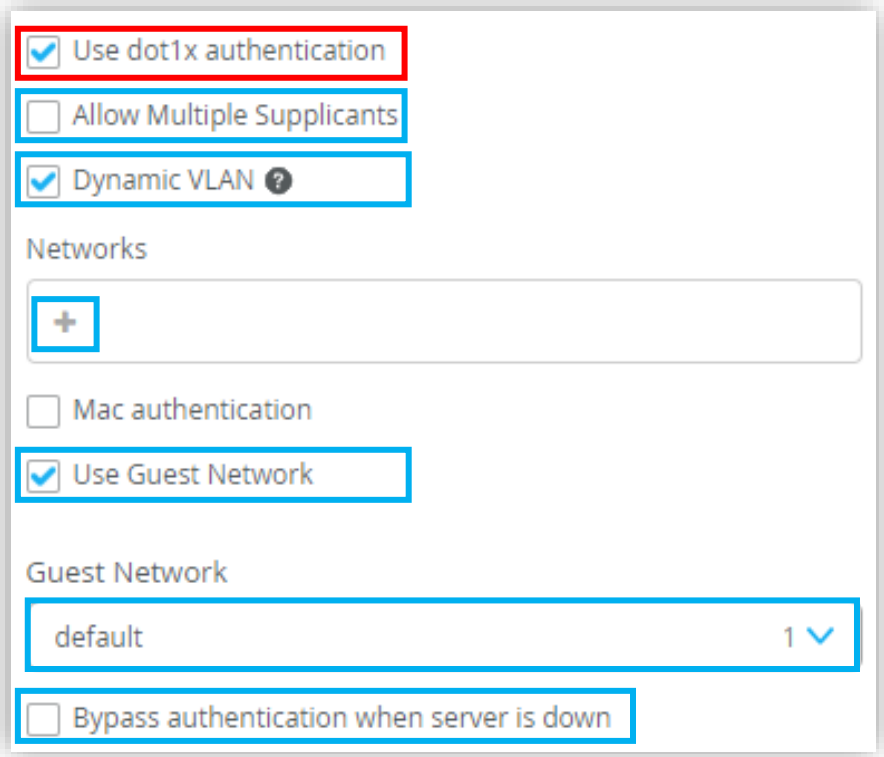
(a) IEEE802.1X 認証

(b) MAB認証

Wired - Switch 設定

Switch Templates: Port Profiles 802.1X

5.(a) 802.1X 認証: [Use dot1x authentication] をチェック(必須)、その他オプションを設定します



[Use dot1x authentication] をチェックします

[Allow Multiple Supplicants] をチェックすると、同一ポートで複数サプリカントが許可されます

動的に VLAN を割り当てる場合、[Dynamic VLAN] をチェックします
[+] から Networks を追加します

Network は別途設定してください

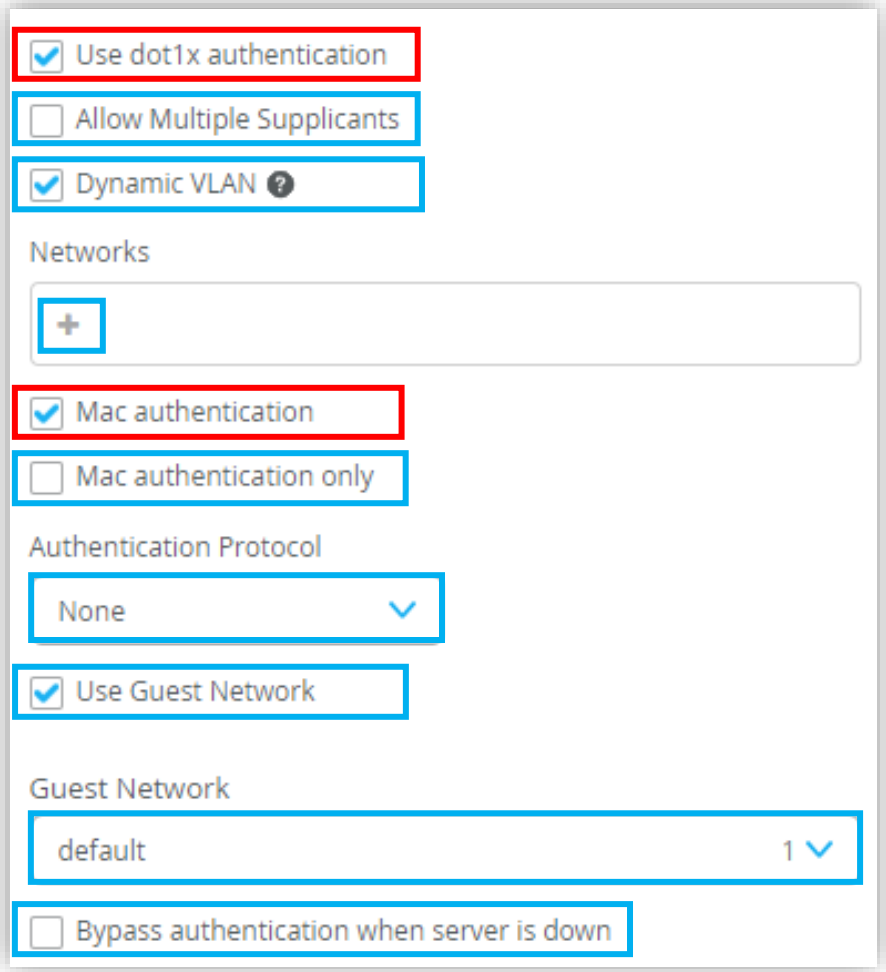
[Use Guest Network] をチェックすると、Guest Network へ認証を行います
[Guest Network] をドロップダウンリストから選択します

[Bypass authentication when server is down] をチェックすると、サーバがダウンしている場合、クライアントは認証なしでネットワークにアクセスできます

Wired - Switch 設定

Switch Templates: Port Profiles MAB

5.(b) MAB 認証: [Use dot1x authentication] と、[Mac authentication] をチェック(必須)、
その他オプションを設定します



[Use dot1x authentication] をチェックします

[Allow Multiple Supplicants] をチェックすると、同一ポートで複数サプリカントが許可されます

[Dynamic VLAN] をチェックして、動的に VLAN を割り当てます
[+] から Networks を追加します

Network は別途設定してください

[Mac authentication] をチェックします
dot1x 認証を試行し失敗すると、MAB での接続を試行(ファールバック) します

[Mac authentication only] をチェックすると、dot1x 認証を試行せずに、
直ちにMAB での接続を試行します

[Authentication Protocol] を指定できます (None/pap/eap-peap/eap-md5)
サプリカントは指定された認証プロトコルで資格情報を提示します

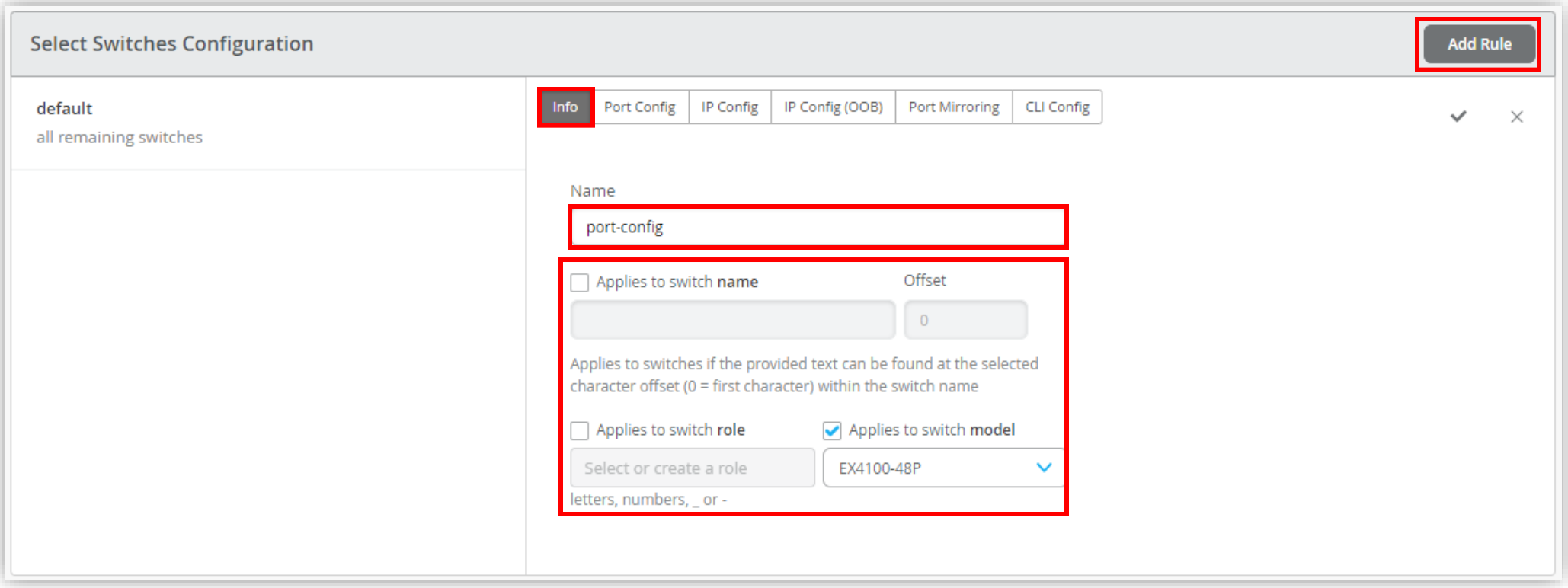
[Use Guest Network] をチェックすると、Guest Network へ認証を行います
[Guest Network] をドロップダウンリストから選択します

[Bypass authentication when server is down] をチェックすると、サーバがダウンしている場合、
クライアントは認証なしでネットワークにアクセスできます

Wired - Switch 設定

Switch Templates: Select Switches Configuration > Port Configuration

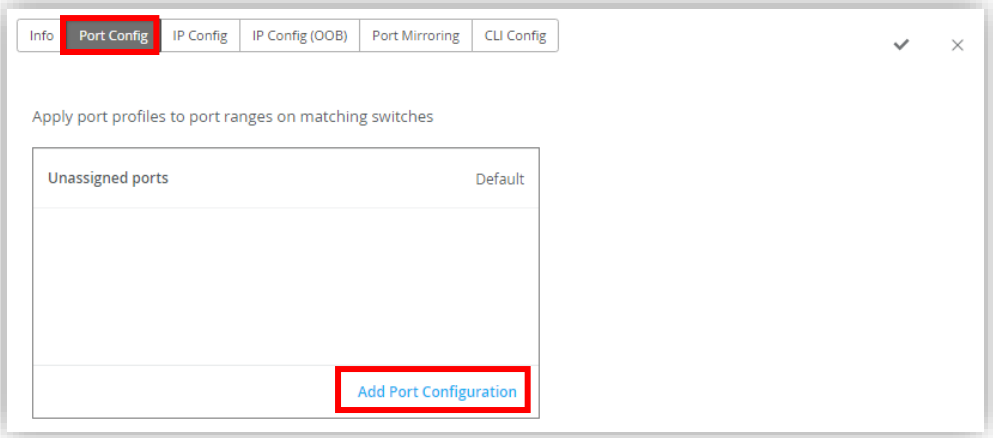
6. [Select Switches Configuration] で [Add Rule] をクリック、[Info] タブで [Name] を設定します
   対象機器を [Applies to name]、[Applies to switch role]、[Applies to switch model] のいずれかで指定します

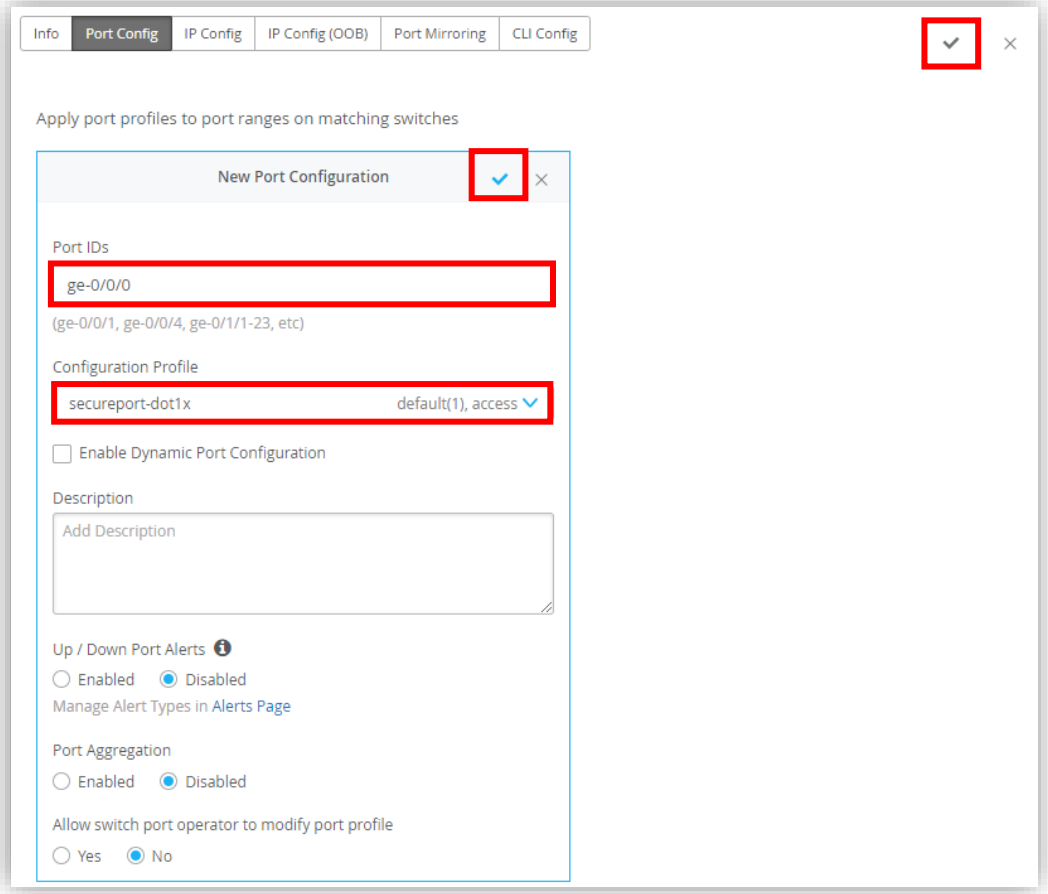


Wired - Switch 設定

Switch Templates: Select Switches Configuration > Port Configuration

7. [Port Config] タブをクリック、[Add Port Configuration] をクリックします
   [Port IDs] で適用するインタフェースを指定、[Configuration Profile] に作成したプロファイルを選択します
   [✓] をクリックして、Port Configuration 設定を完了、[✓] で Rule 設定を完了します

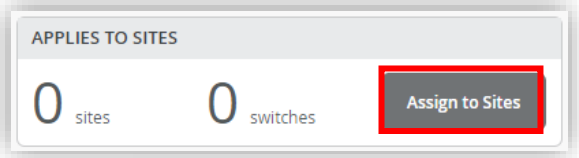


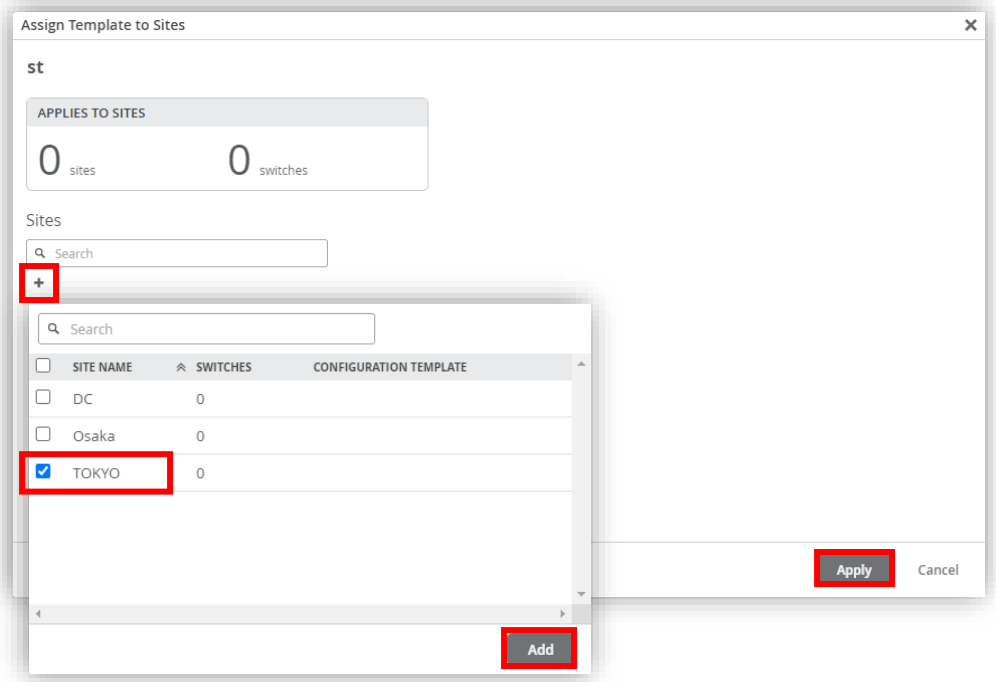


Wired - Switch 設定

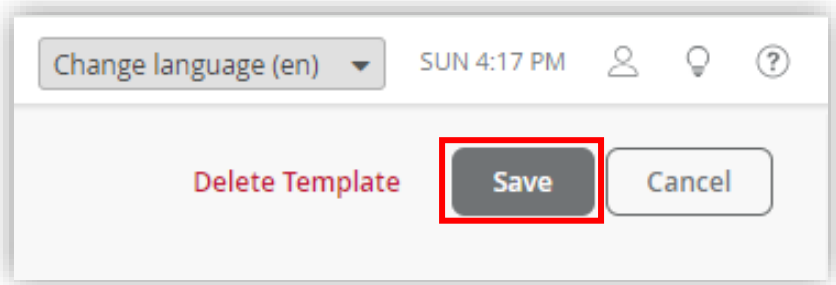
Switch Templates: Assign to Sites / Save

8. [Applies to Sites] で [Assign to Sites] をクリック、[+] からテンプレートを適用するサイトを選択(複数選択可)し、[Add] をクリック、[Apply] をクリックします





9. [Assign to Sites]で Switch Template の設定を完了します



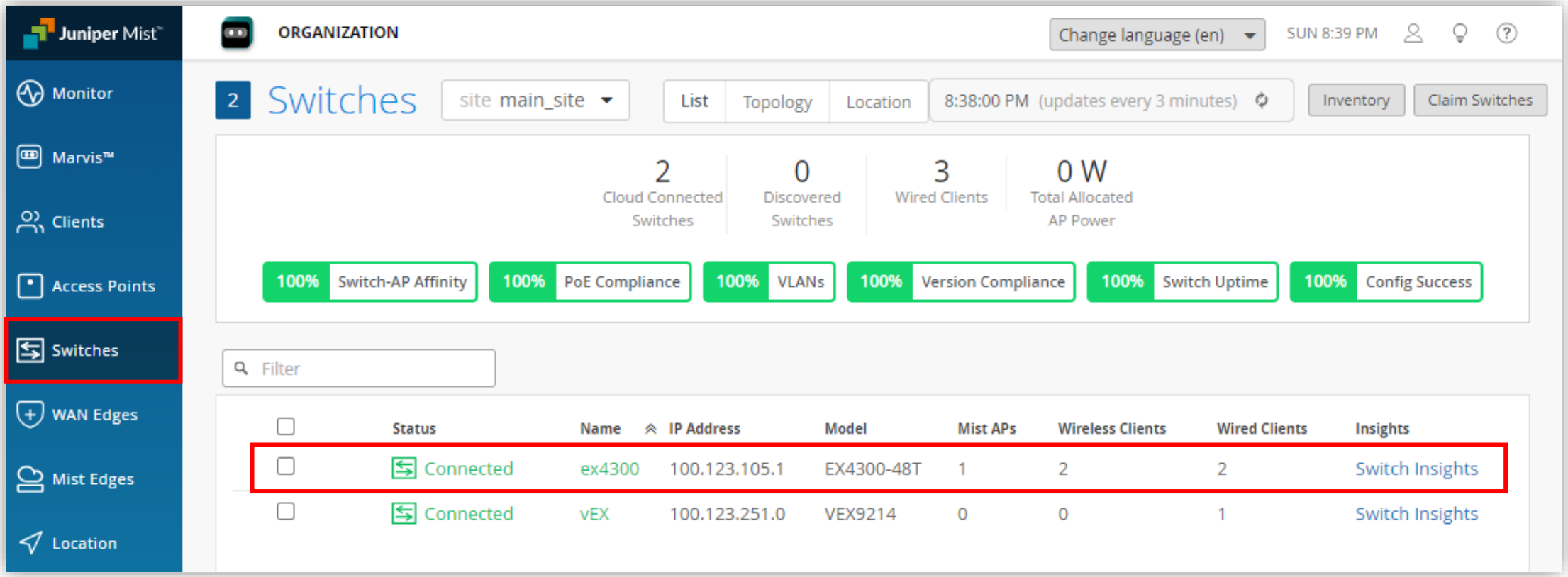
Switch Templates を、サイトにアサインして利用します

Wired - Switch 設定

Per Switch Configuration

Organization > Switch Template、Site > Switch Configuration を使用せずに、スイッチ毎で設定することもできます

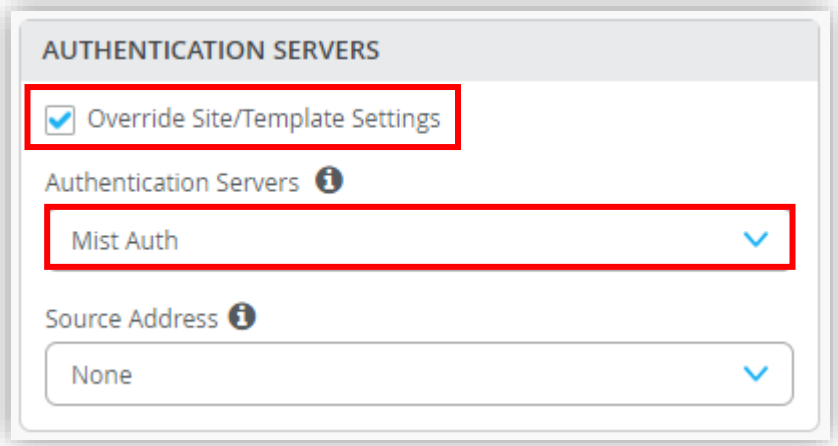
1. [Switches] から、設定する スイッチを選択します



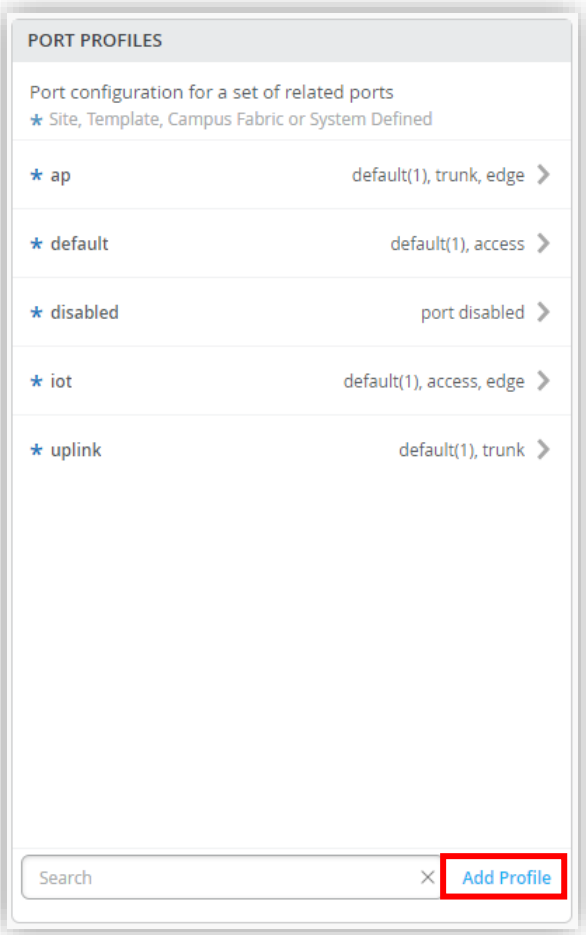
Wired - Switch 設定

Per Switch Configuration

2. [Authentication Server] で [Mist Auth] を選択します



3. [Port Profiles] から [Add Profile] をクリックして、Port Profile を設定します

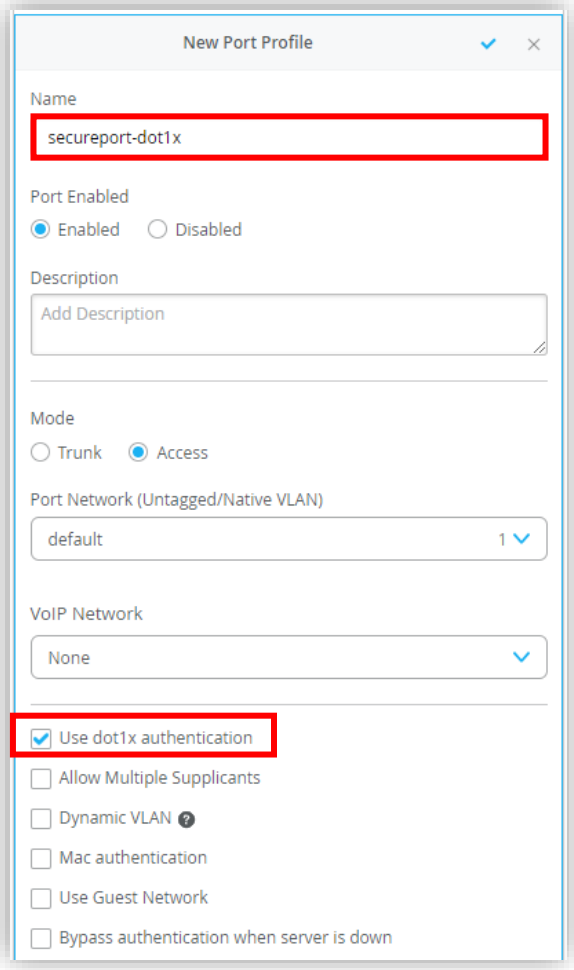


Wired - Switch 設定

Per Switch Configuration

最低限の設定です
その他オプションは、p.40, p.41 参照

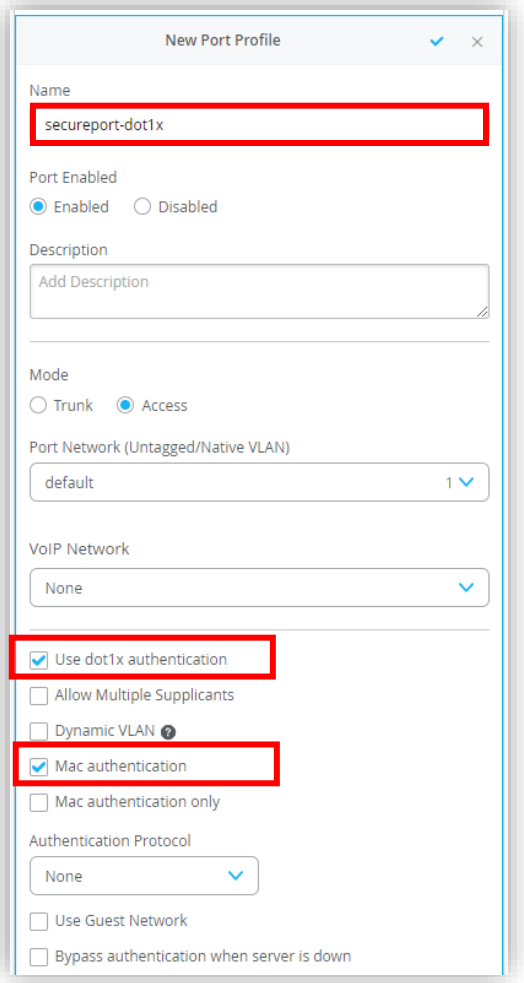
4.(a) Port Profile: 802.1X 認証



[Name] にプロファイル名を設定します

[Use dot1x authentication] をチェックします

4.(b) Port Profile: MAB 認証



[Name] にプロファイル名を設定します

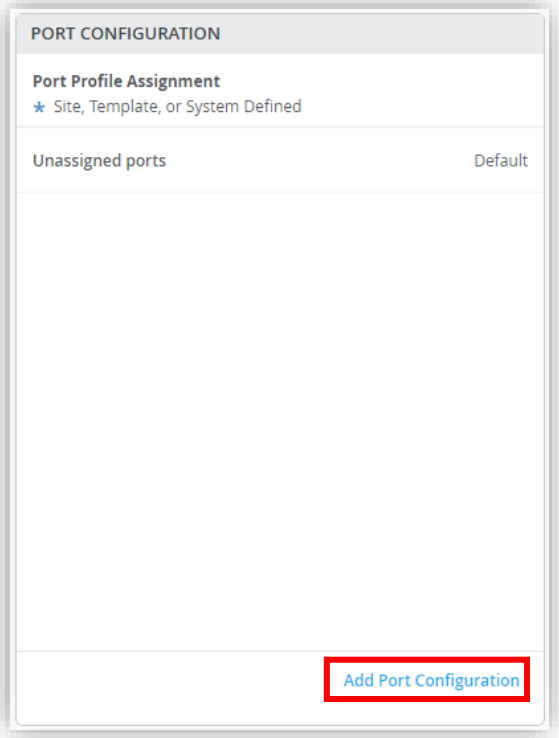
[Use dot1x authentication] をチェックします

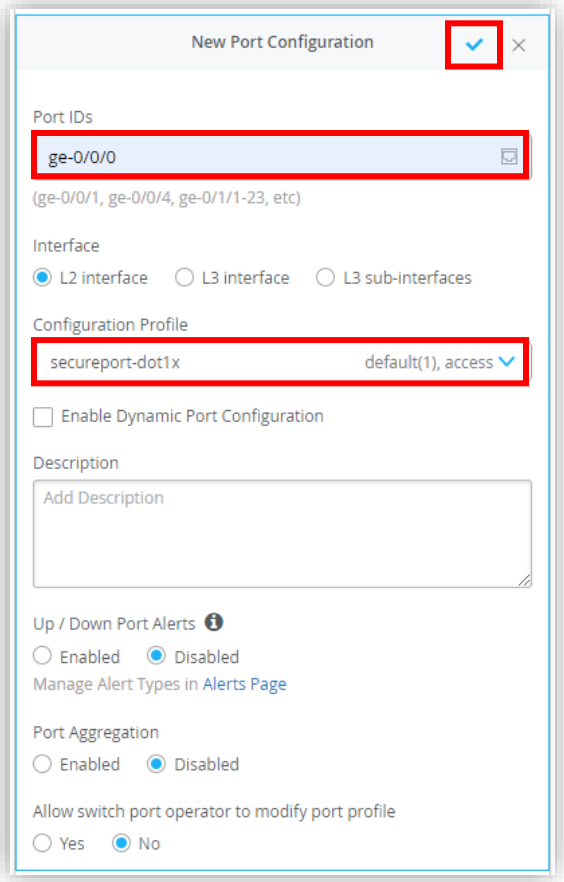
[Mac authentication] をチェックします

Wired - Switch 設定

Per Switch Configuration

5. [Port Configuration] で [Add Port Configuration] をクリックします
   [Port IDs] で適用するインタフェースを指定、[Configuration Profile] に作成したプロファイルを選択します
   [✓] をクリックします





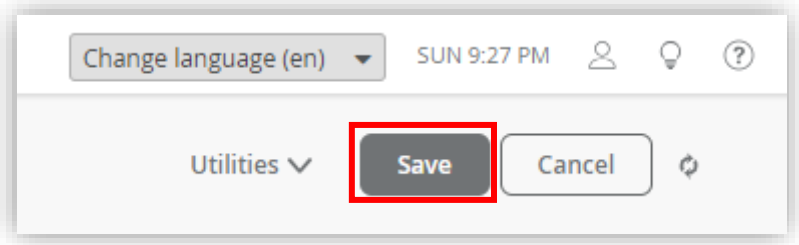
[Port IDs] で適用するインタフェースを指定します

[Configuration Profile] に作成したプロファイルを選択します

Wired - Switch 設定

Per Switch Configuration

6. [Save] で設定を完了します



設定は、下記のいずれでもできます

- **Organization > Switch Templates > {Template}**
- **Site > Switch Configuration > {Site}**
- **Switches > {Switch}**

管理性や拡張性の観点から、Switch Templates での設定が推奨です
Switch Template で Network、Port Profile を設定、個別スイッチで Port Configuration を設定するなど組み合わせて設定することもできます

Certificate

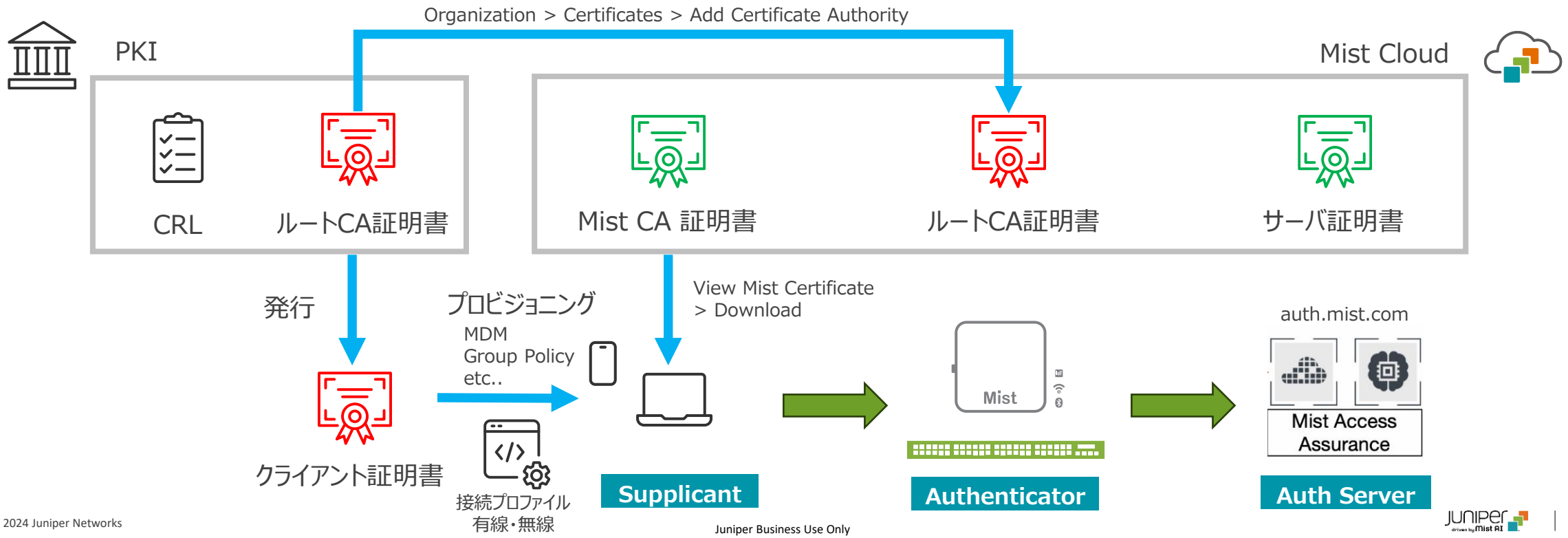
JUNIPER NETWORKS

Certificate

証明書の設定について

- IEEE802.1x 認証では、Server Hello でサーバ証明書が提示され、クライアント側で検証が行われます
- EAP-TLS では、Server Hello に Certificate Request 命令を追加することにより、クライアントにクライアント証明書を要求します。クライアントは証明書を提示し、提示された証明書の検証がサーバ側で行われます

- **Mist はプライベート CA 局として動作し、サーバ証明書(auth.mist.com) を自動で発行します**
- **Mist ではクライアント証明書の発行・配布を行いません**



Certificate

証明書の設定について

クライアントが Access Assurance のサーバ証明書を信頼するためには、以下のどちらかが必要です

1. Mist CA 証明書をクライアントに信頼できる認証局として登録

- Mist CA 証明書をダウンロードします (デフォルトのファイル名: mist-ca.crt)
  Organization > Certificates > View Mist Certificate > Downloads
- クライアントにインストールします

2. クライアントが信頼しているパブリック認証局などにより発行されたサーバ証明書をインポート、デフォルトの Mist 証明書と入れ替え

- Organization > Certificates > Import Custom RADIUS Server Certificate

  下記を入力し、[Save] をクリックします
  - Private Key(秘密鍵)
  - Private Key Password(秘密鍵のパスワード)
  - Signed Certificate(証明書) ※中間証明書を含めます

カスタム X509 証明書の要件

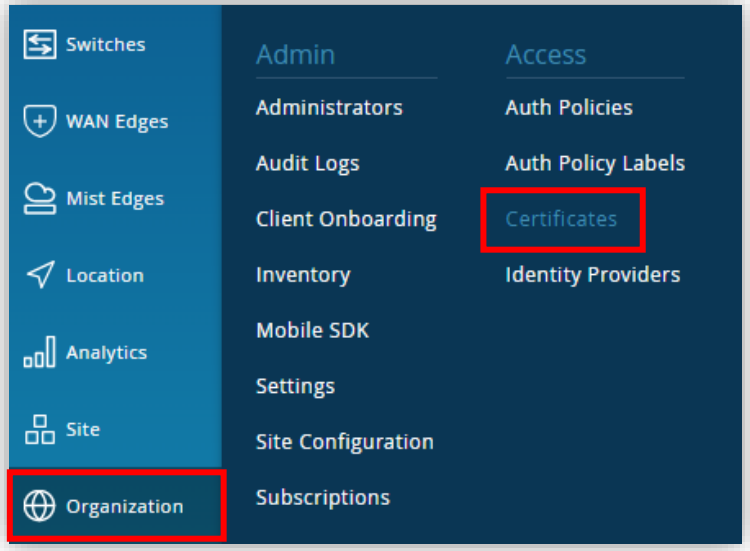
- X509v3 (v1不可)
- CN と SAN を含む証明書を使用できます
- サーバ名がクライアントで証明書検証基準としている場合、SAN にサーバの DNS 名を含めます
- ワイルドカード証明書は使用できません
- TLS web server authentication 拡張属性を含めます (大多数の Android 端末で必要となります)

パブリック/プライベート PKI のいずれの場合も、サーバ/クライアント証明書を検証するため、正しく証明書チェーンを構成する必要があります

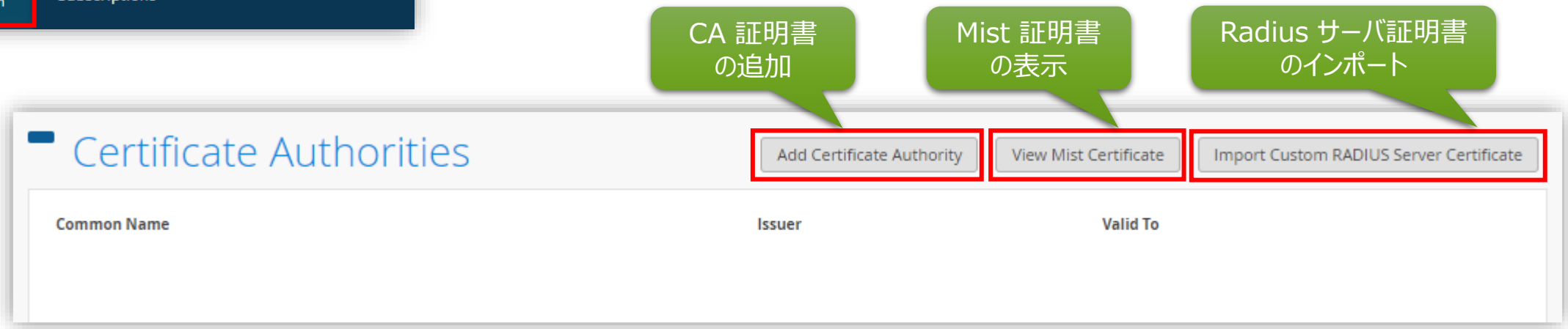
Certificate

設定

[Organization] から [Certificates] をクリックします



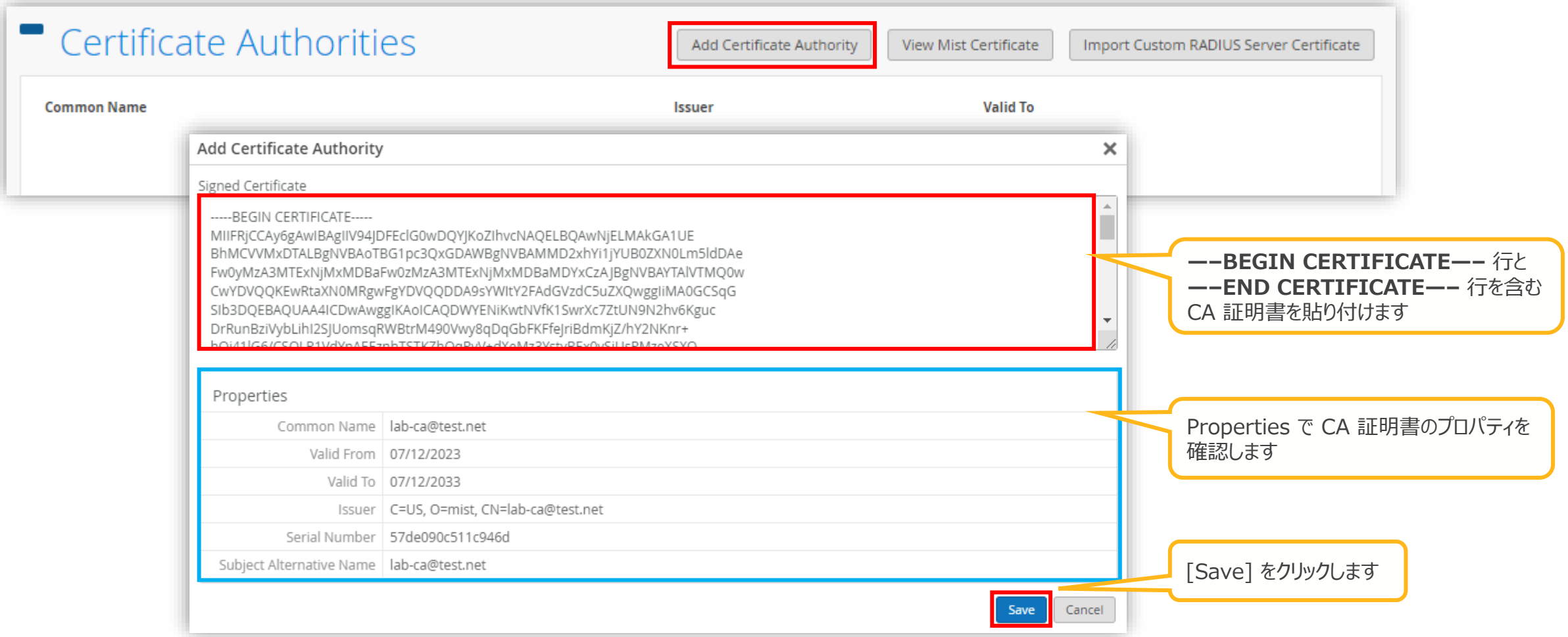
- **Add Certificate Authority (CA 証明書の追加)**
  クライアント証明書認証に使用される CA 証明書を登録します
  クライアントデバイスは、Client Hello でクライアント証明書を提示し、サーバ側の CA 証明書で検証されます
  証明書は同じ CA により署名されている必要があります
- **View Mist Certificate (Mist 証明書の表示)**
  各 Org 毎に固有の Mist CA 認証局により Access Assurance 用のデフォルトサーバ証明書を発行します
  別途設定されていない場合、このデフォルトのサーバ証明書をクライアントに提示します
- **Import Custom RADIUS Certificate (Radius サーバ証明書のインポート)**
  既存のクライアント設定・証明書を変更せずに、発行済みのサーバ証明書を継続利用する場合、既存の証明書(ルート CA 証明書、Radius サーバの公開鍵、および秘密鍵)をインポートします
  カスタム設定がある場合は、デフォルト設定より優先されます



Certificate

Add Certificate Authority

[Add Certificate Authority] をクリックして、[signed Certificate] 欄に CA 証明書を貼り付け、[Save] をクリックします



-----BEGIN CERTIFICATE----- 行と **-----END CERTIFICATE-----** 行を含む CA 証明書を貼り付けます

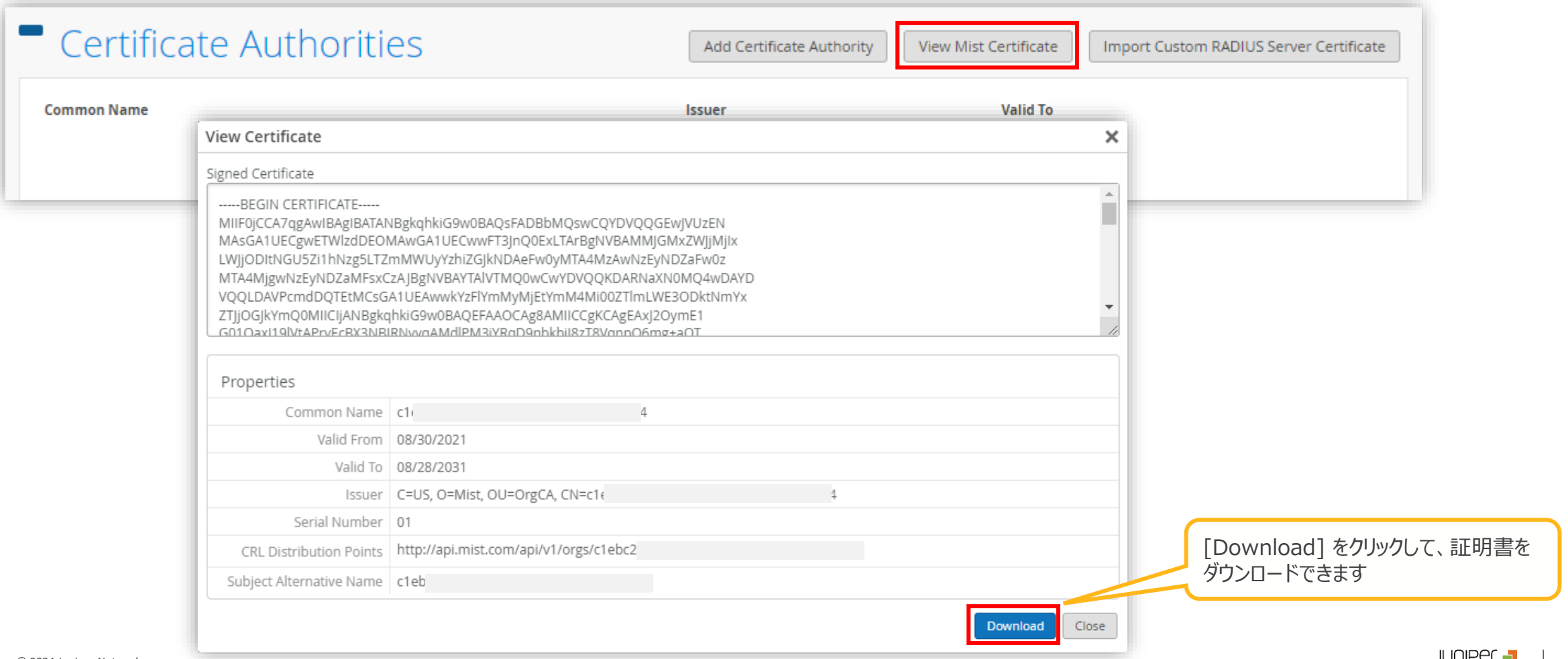
Properties で CA 証明書のプロパティを確認します

[Save] をクリックします

Certificate

View Mist Certificate

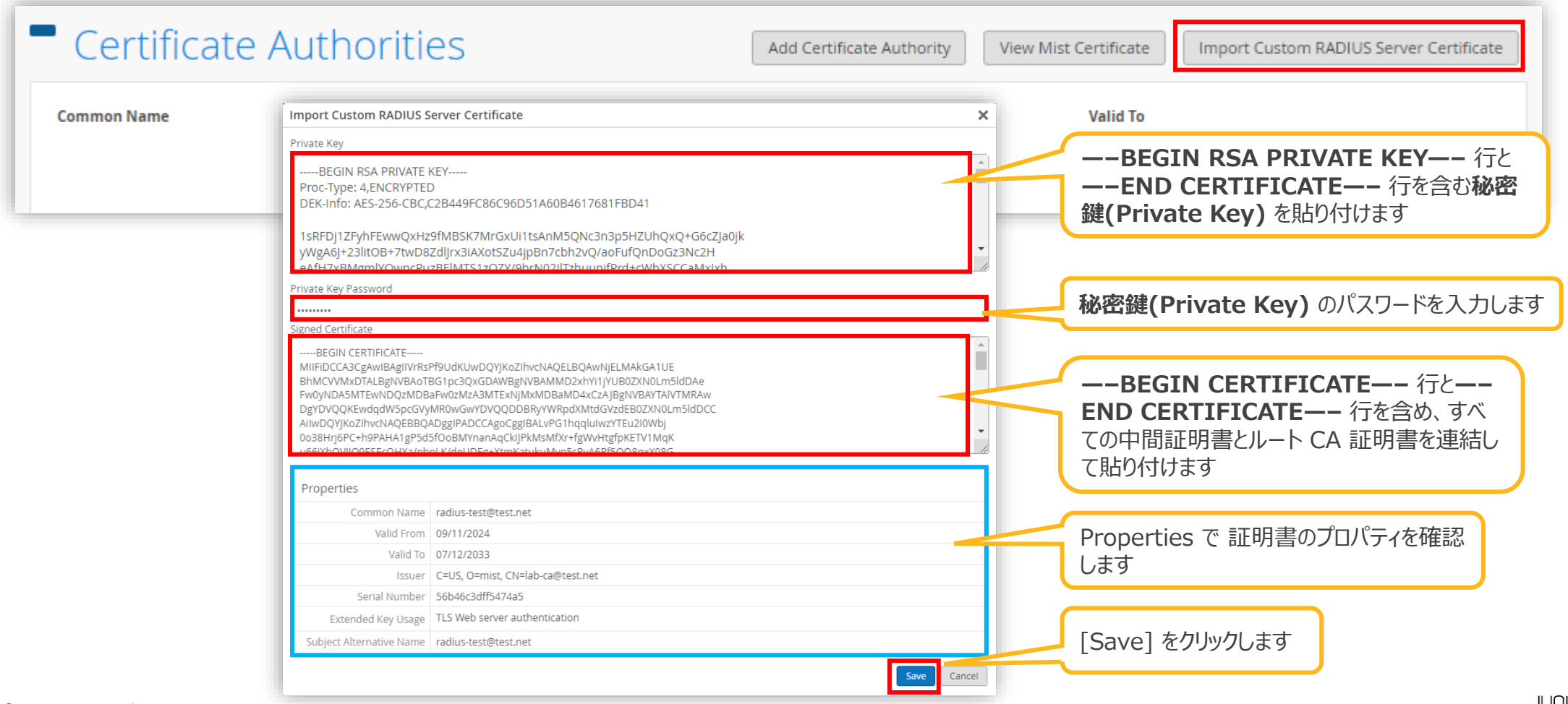
[View Mist Certificate] をクリックして、Mist の CA 証明書を表示します
[Download] よりダウンロードできます



Certificate

Import Custom RADIUS Server Certificate

[Import Custom RADIUS Server Certificate] をクリックし、[Private Key]、[Private Key Password]、[Signed Certificate] を入力し、[Save] をクリックします



--BEGIN RSA PRIVATE KEY-- 行と **--END CERTIFICATE--** 行を含む**秘密鍵(Private Key)** を貼り付けます

秘密鍵(Private Key) のパスワードを入力します

--BEGIN CERTIFICATE-- 行と**--END CERTIFICATE--** 行を含め、すべての中間証明書とルート CA 証明書を連結して貼り付けます

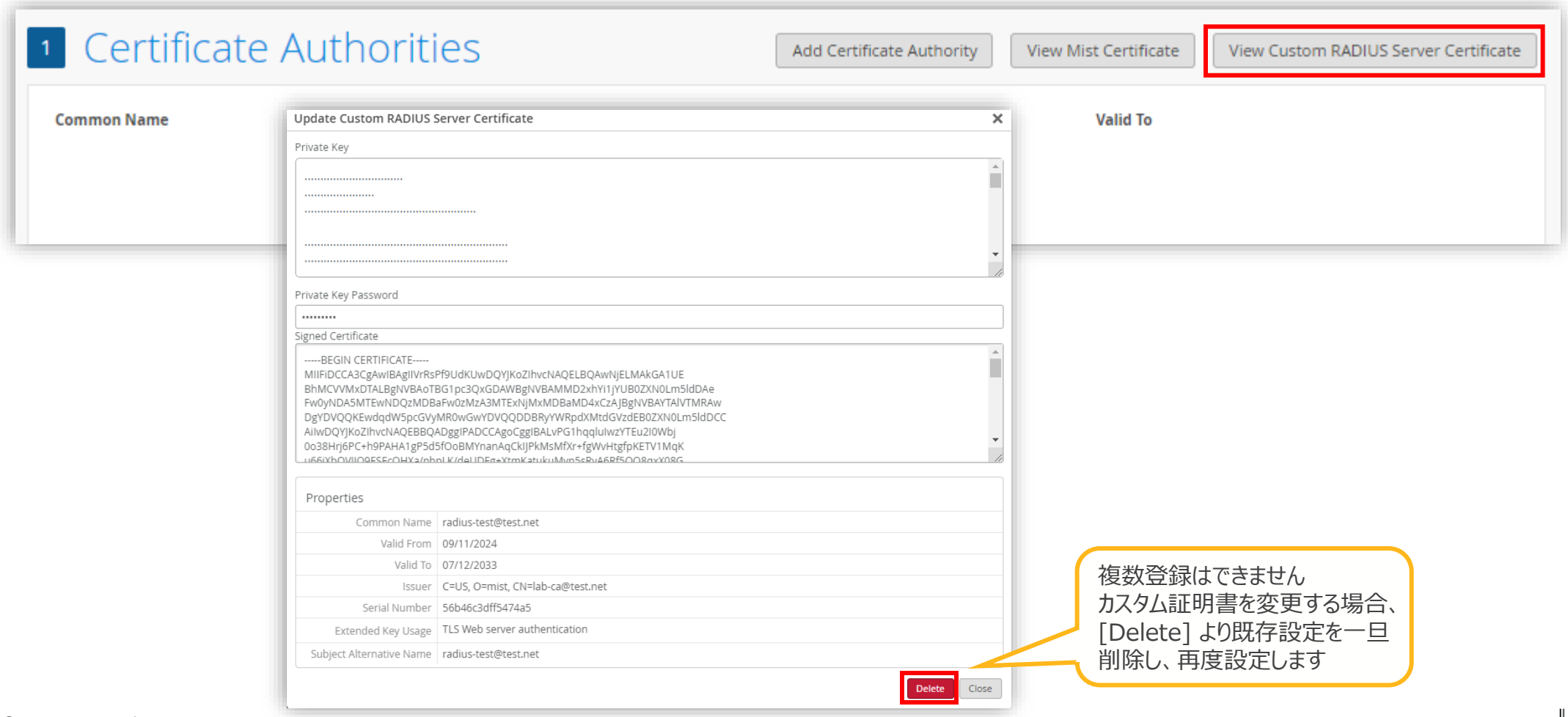
Properties で 証明書のプロパティを確認します

[Save] をクリックします

Certificate

View Custom RADIUS Server Certificate

[View Custom RADIUS Server Certificate] をクリックし、現在登録中のカスタム証明書情報を表示します
複数登録はできません(カスタム証明書を変更する場合、[Delete] より既存設定を一旦削除し、再度設定します)



複数登録はできません
カスタム証明書を変更する場合、
[Delete] より既存設定を一旦
削除し、再度設定します

Identity Providers
Entra ID/OAuth

JUNIPER NETWORKS

Identity Providers

Entra ID(Azure AD)/OAuth Overview

クライアントシークレットの値は作成直後のみ確認できます
忘れずにコピーしてください

Entra ID/OAuth のアプリケーションを登録します

アプリの登録

新規登録 > アプリケーション名を設定 > 登録

アプリケーション(クライアント)ID

ディレクトリ(テナント)ID

証明書またはシークレットの追加

証明書とシークレット

新しいクライアントシークレット

説明

有効期限

クライアントシークレット

認証

パブリッククライアントフローを許可する > 保存

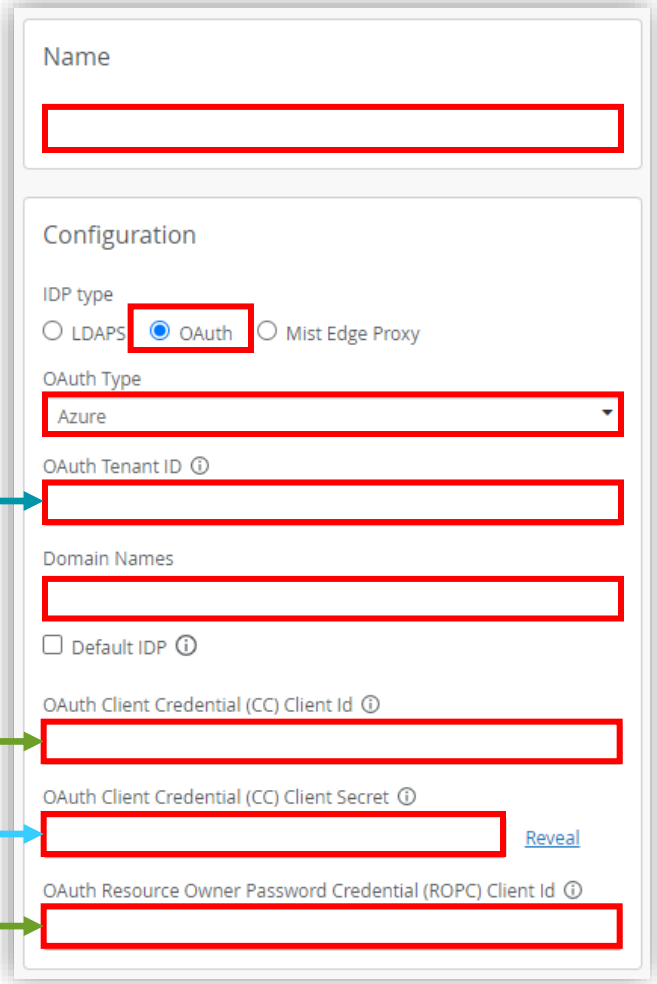
APIのアクセス許可

Microsoft Graph

- User.Read - Delegated
- User.Read.All - Application
- Group.Read.All – Application
- Device.Read.All – Application

ユーザ・グループの追加

Organization > Identity Providers > Add IDP



[Name] を入力します

[OAuth] を選択します

[Azure] を選択します

[OAuth Tenant ID] を入力します

[Domain Names] を入力します

[OAuth Client Credential(CC) Client Id] を入力します

[OAuth Client Credential(CC) Client Secret] を入力します

[OAuth ROPC Client Id] を入力します

Identity Providers

Entra ID アプリの登録

1. Entra ID(旧 Azure Active Directory) にアクセスします
2. [アプリの登録] を選択し、[新規登録] をクリックします

Identity Providers

登録

3. [名前] を入力、[サポートされているアカウントの種類]を選択、[登録] をクリックします

Identity Providers

概要 アプリケーション(クライアント)ID / ディレクトリ(テナント)ID

4. [アプリケーション(クライアント) ID] と[ディレクトリ(テナント) ID] をコピーします
5. [証明書またはシークレットの追加] をクリックします

Identity Providers

証明書とシークレット クライアントシークレットの追加

有効期限は実運用にあわせて適度な期間に設定してください

6. [証明書とシークレット] を選択、 [+新しいクライアントシークレット] をクリックします
   [説明] を入力、[有効期限] を選択し、[追加] をクリックします

Identity Providers

証明書とシークレット クライアントシークレットのコピー

忘れずにコピーしてください

7. クライアントシークレットの [値] をコピーします

Identity Providers

パブリッククライアントフローを許可する

8. [認証] を選択、[パブリッククライントフローを許可する] の項目で [はい] に選択します
   [保存] をクリックします

Identity Providers

API のアクセス許可 Microsoft Graph

9. [API のアクセス許可] を選択、[Microsoft Graph] をクリックします

Identity Providers

API のアクセス許可 アクセス許可の追加

10. アクセス許可を追加します(右表参照)

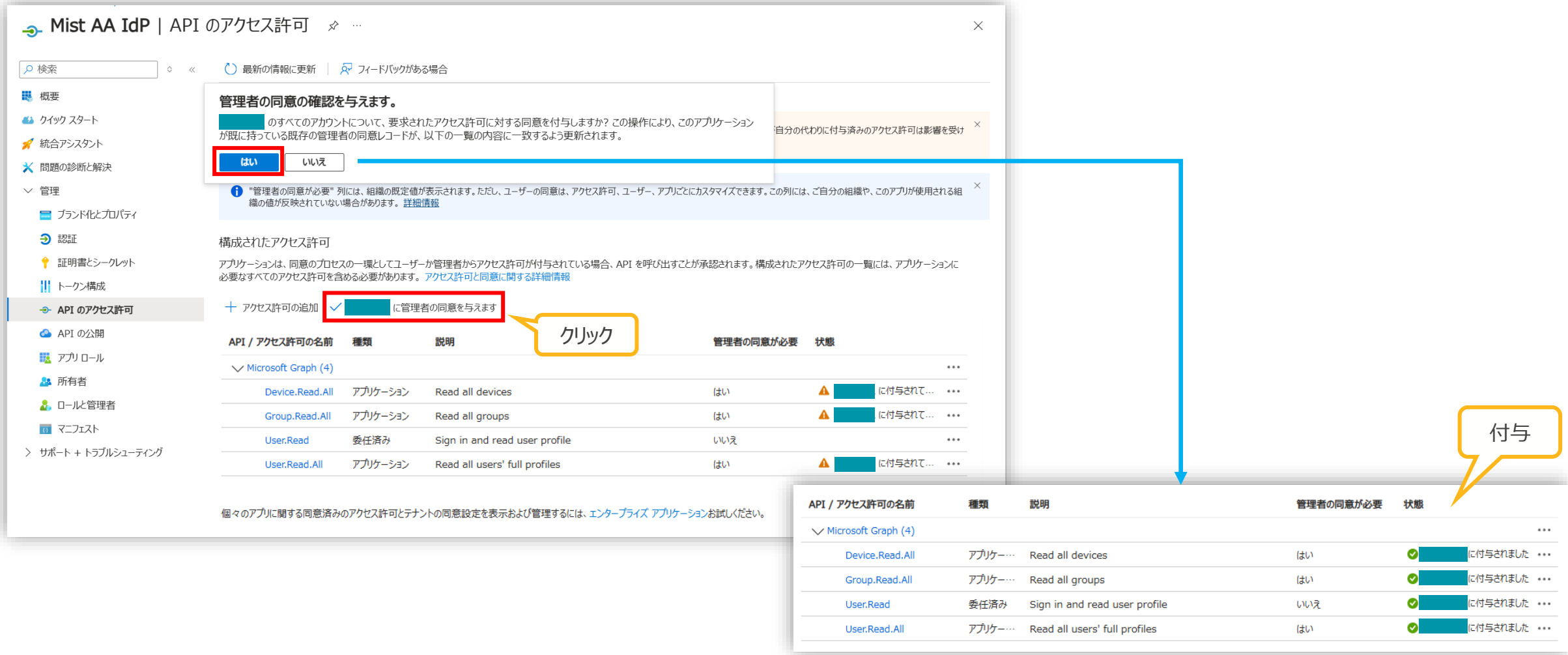
Microsoft Graph	種類
User.Read	委任済み
User.Read.All	アプリケーション
Group.Read.All	アプリケーション
Device.Read.All	アプリケーション

Identity Providers

API のアクセス許可 管理者の同意を与える

Microsoft Graph API を使用して情報をフェッチするために必要なアクセス許可をアプリケーションに付与する必要があります

11. [{テナント名}に管理者の同意を与えます] をクリックし、ポップアップ画面で[はい]をクリックします

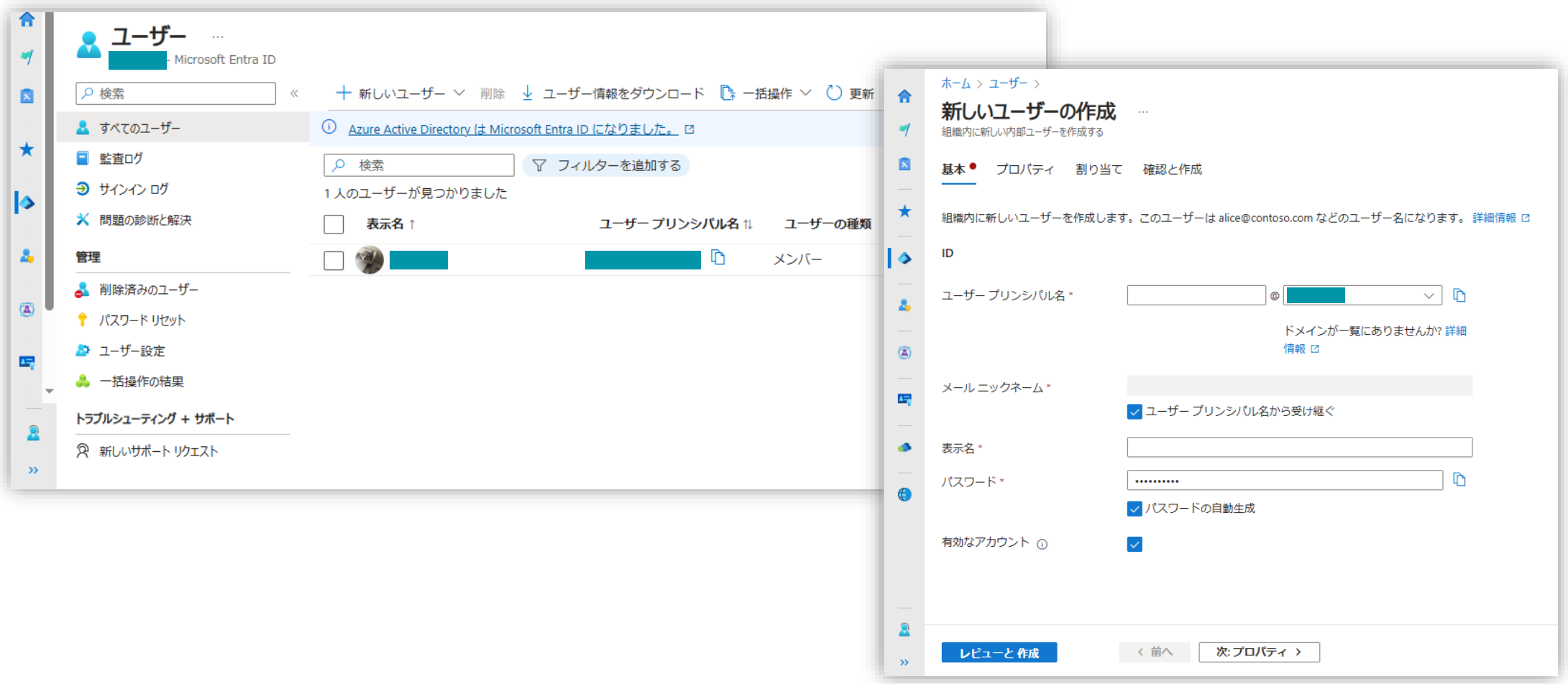


Identity Providers

user/group

User を追加します

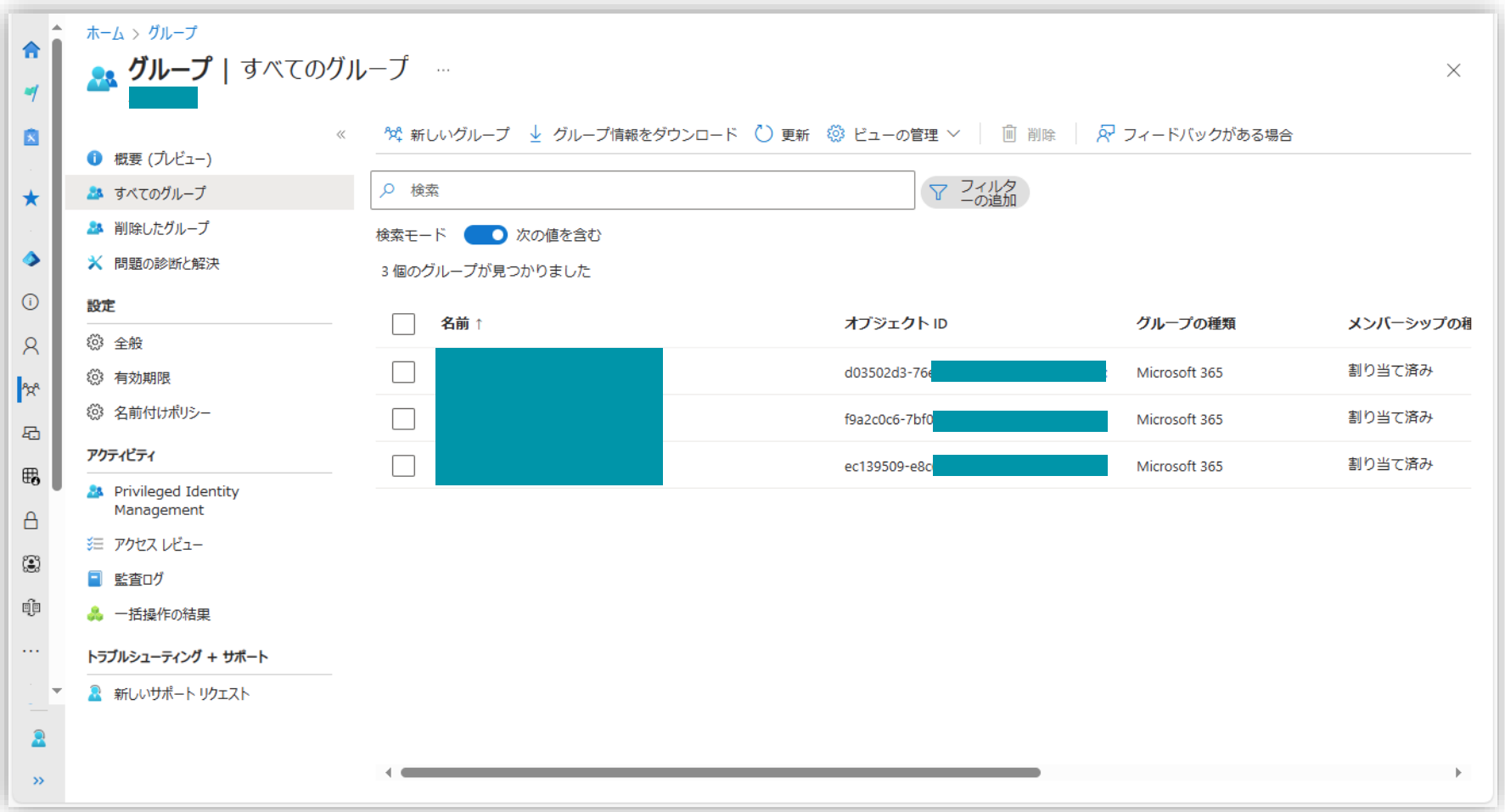
登録したアプリから user/group 情報を参照できるように設定してください(説明は割愛)



Identity Providers

user/group

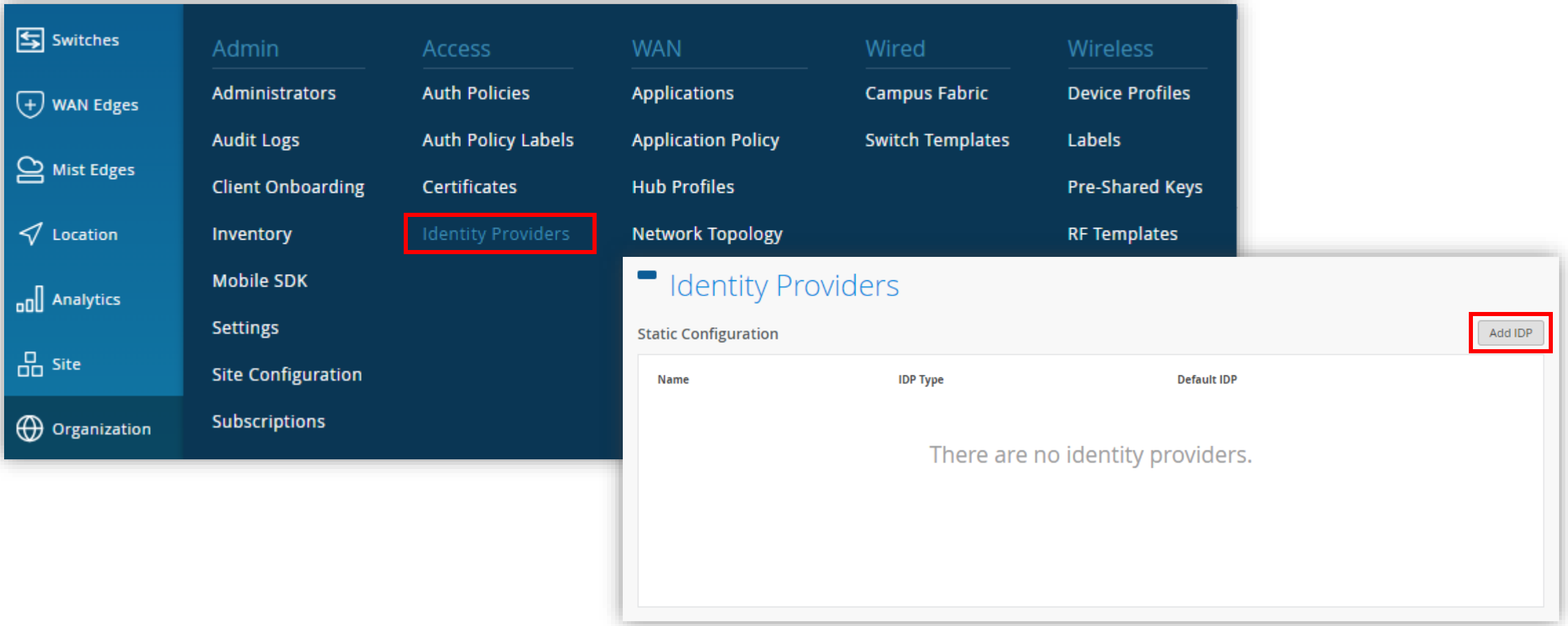
group を追加します



Identity Providers

Add IDP - Entra ID/OAuth

1. [Organization] から [Identity Providers] をクリックします
2. [Add IDP] をクリックします



Identity Providers

Add IDP - Entra ID/OAuth

3. Entra ID に追加したアプリを参照し各項目を設定、[Create] をクリックします

アプリの登録
新規登録 > アプリケーション名を設定 > 登録

アプリケーション(クライアント)ID

ディレクトリ(テナント)ID

証明書またはシークレットの追加

証明書とシークレット

新しいクライアントシークレット

説明

有効期限

クライアントシークレット

認証

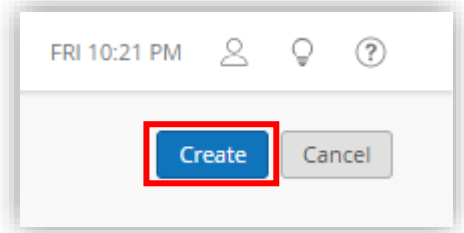
パブリッククライアントフローを許可する > 保存

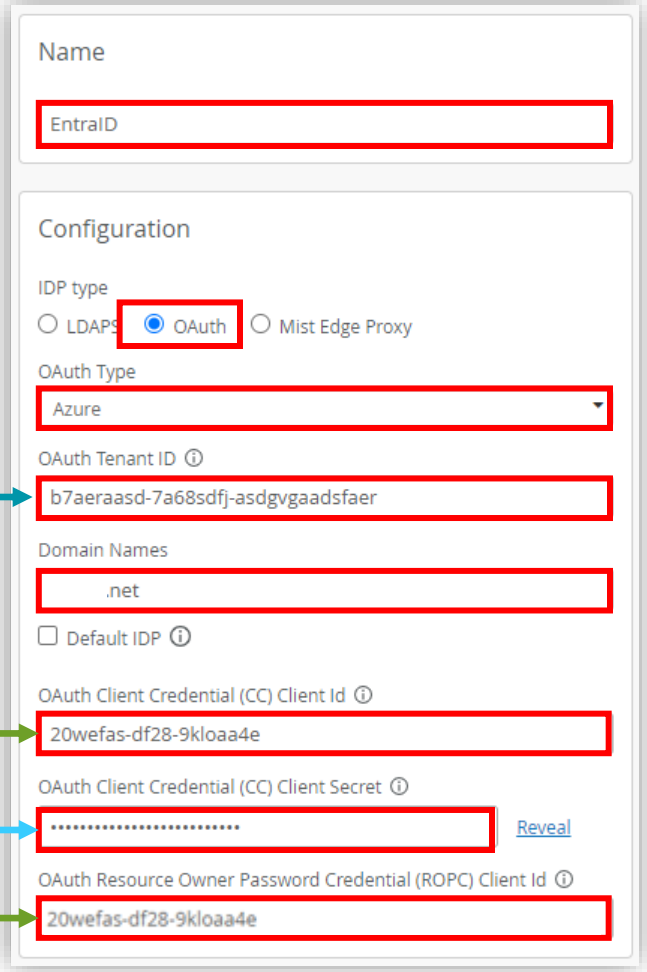
APIのアクセス許可

Microsoft Graph

- User.Read - Delegated
- User.Read.All - Application
- Group.Read.All – Application
- Device.Read.All – Application

ユーザ・グループの追加





[Name] を入力します

[OAuth] を選択します

[Azure] を選択します

[OAuth Tenant ID] を入力します

[Domain Names] を入力します

[OAuth Client Credential(CC) Client Id] を入力します

[OAuth Client Credential(CC) Client Secret] を入力します

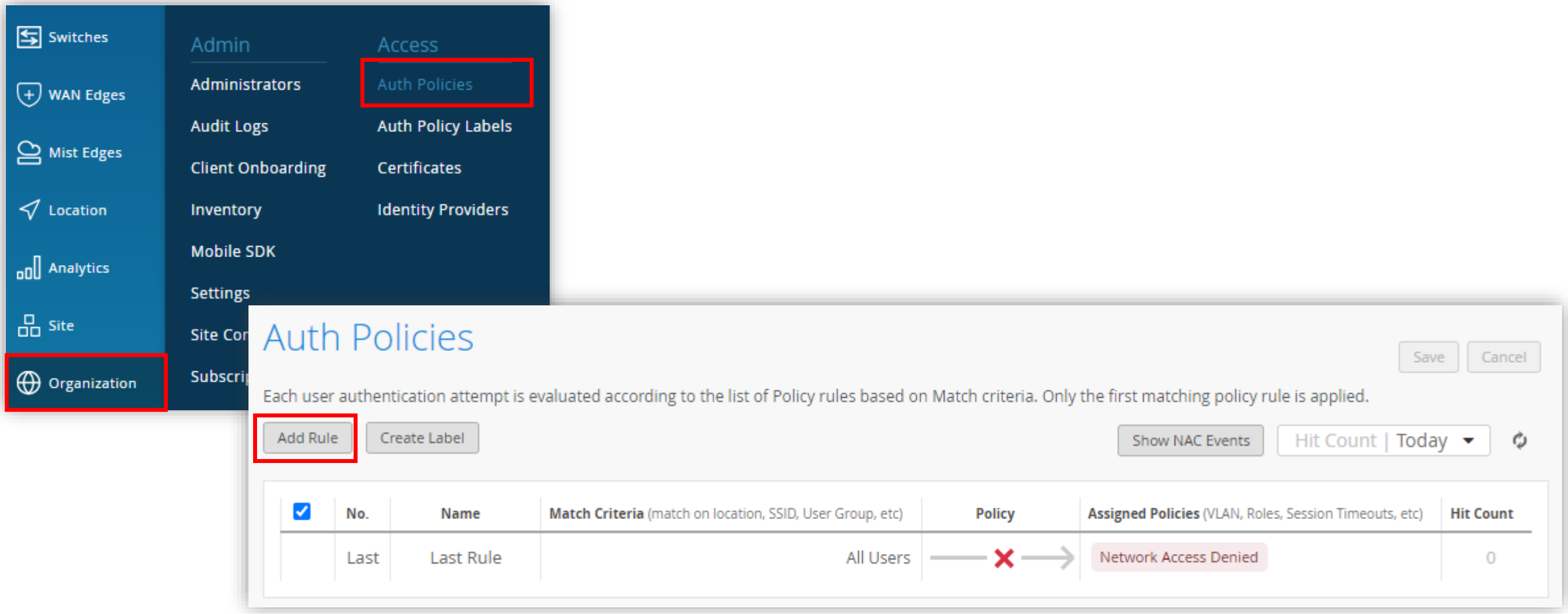
[OAuth ROPC Client Id] を入力します

Auth Policy

Auth Policy

Organization > Auth Policies

[Organization] から [Auth Policy] をクリック、[Add Rule] をクリックします

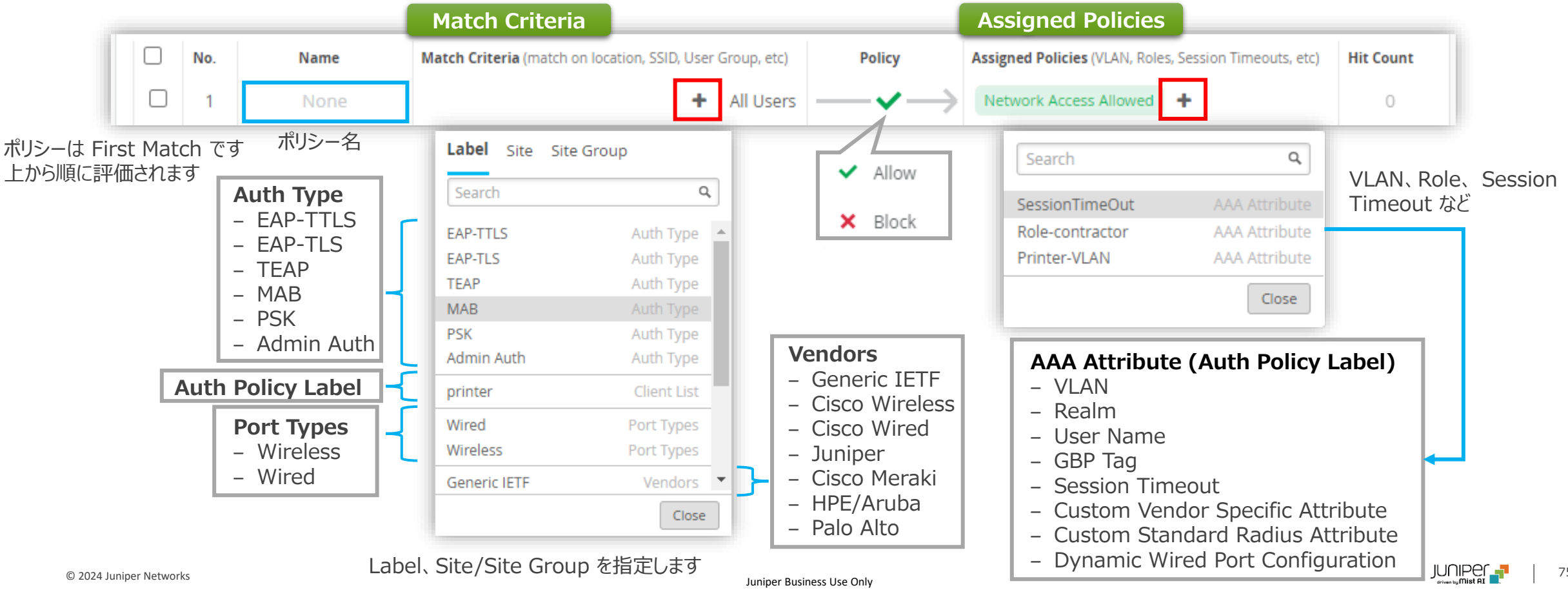


Auth Policy

Organization > Auth Policies

Match Criteria ネットワーク・アプリケーションに認証を要求するユーザ・デバイスを識別します

Assigned Policies ポリシーを満たすユーザ・デバイスに対して、アクセスを許可または拒否するアクションを適用します
加えて、認証ユーザの属性に応じた VLAN、Role、Session Timeout などをパラメータとして付与できます

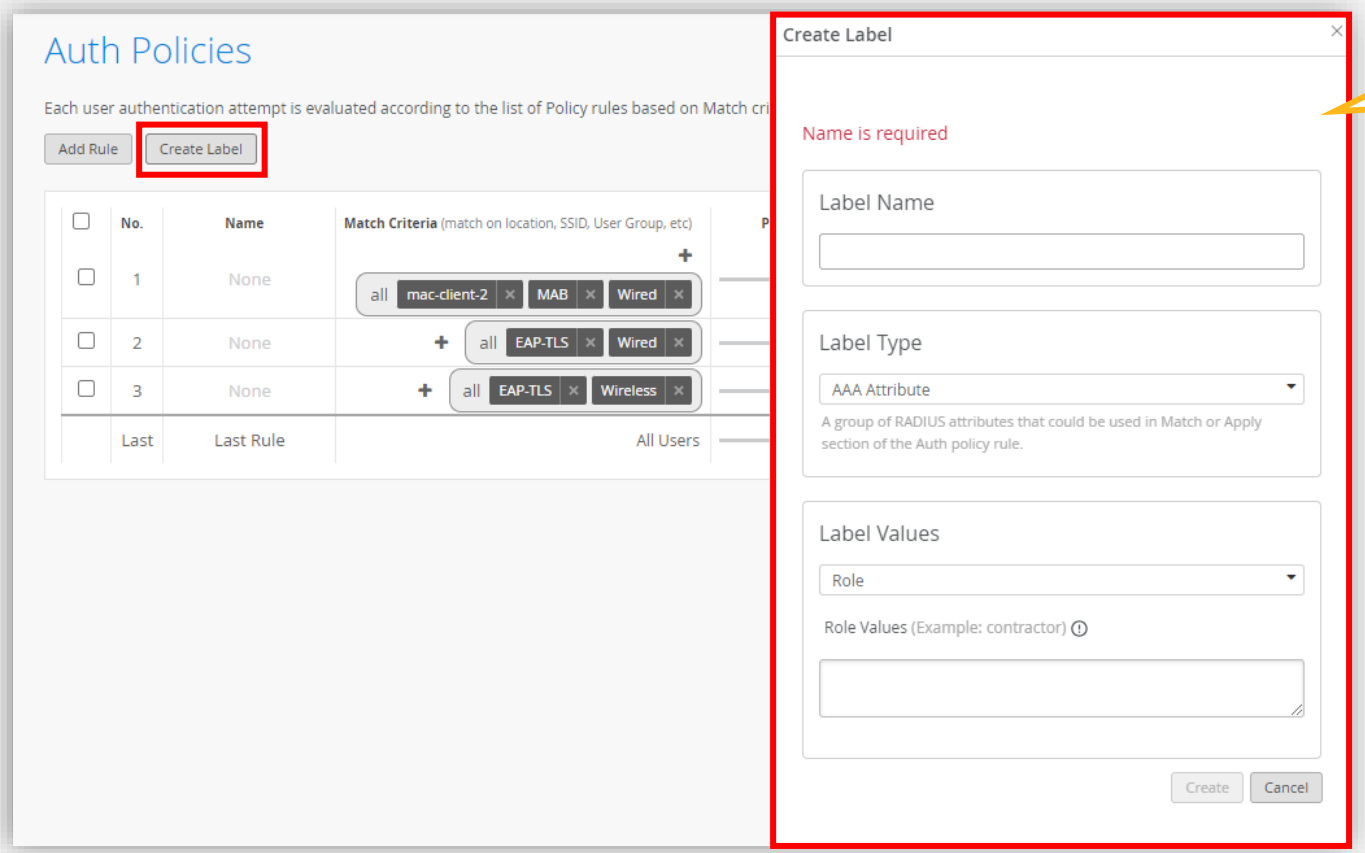


Auth Policy

Organization > Auth Policies

Note

Auth Policy Labels は、[Organization] から [Auth Policy Labels] で設定・管理します
Auth Policy 設定時に、[Create Label] で設定することもできます



[Create Label] をクリックして、
Label を設定できます

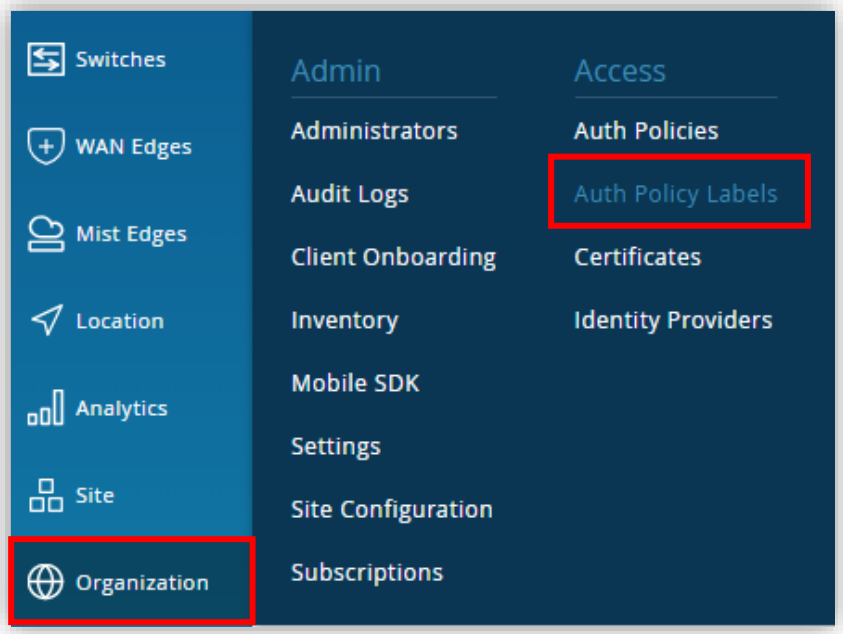
Auth Policy Labels

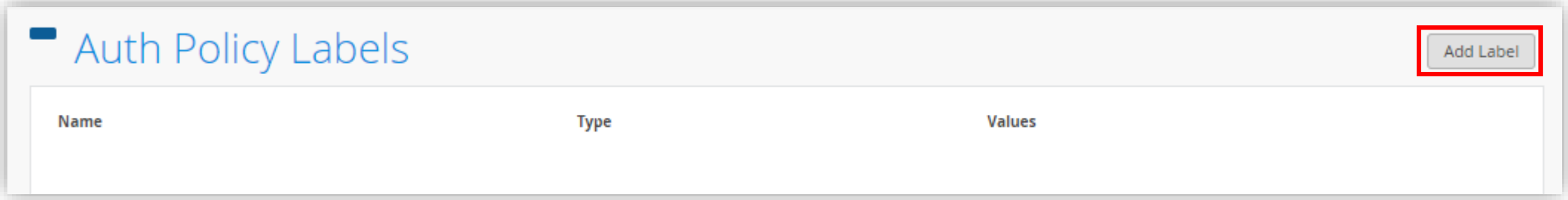
JUNIPER NETWORKS

Auth Policy Labels

Organization > Auth Policy Labels

1. [Organization] から [Auth Policy Labels] をクリックします
2. 画面右上の、[Add Label] をクリックします

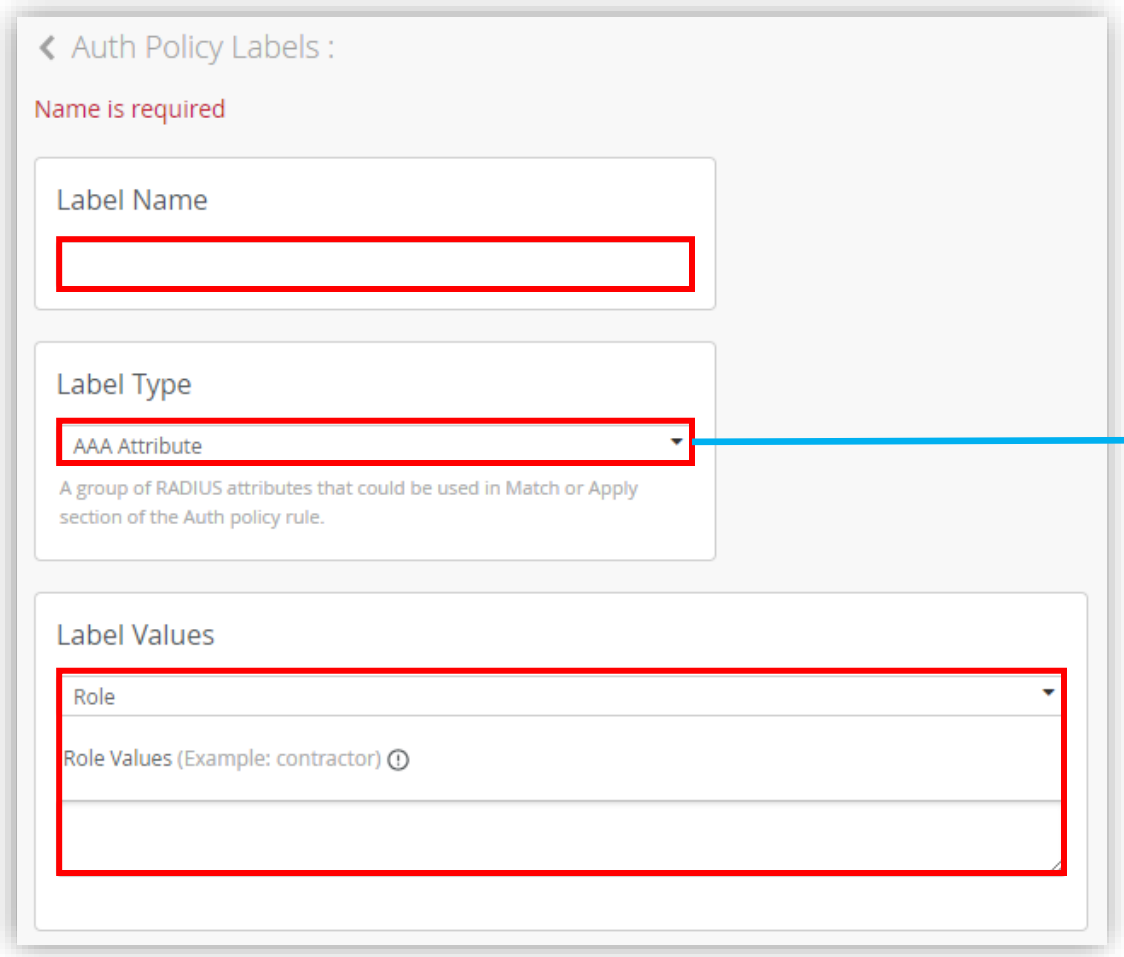




Auth Policy Labels

Organization > Auth Policy Labels

[Label Name]、[Label Type]、[Label Values] を設定します



- AAA Attribute
- Certificate Attribute
- Client List
- Directory Attribute
- SSID
- MDM Compliance
- Client Label

Label Type により、必要な Label Values の設定項目は異なります(詳細は次ページ以降)

Auth Policy Labels

Match Apply

AAA Attribute

Radius の AAA Attribute を参照して、ラベルを作成します
Auth Policy の **Match Criteria** および **Assigned Policies** で使用できます

Label Type	Label Values	
AAA Attribute	Role	***Role Values*** (Example: contractor)
	VLAN	***VLAN Values*** (Example: 750 or employee-vlan)
	Realm	***Realm Values*** (Example: @domain.com or domain)
	User Name	***Username Values*** (Example: steve or bob*)
	GBP Tag	***GBP Tag Values*** (Example: 100, allowed values 1-65535)
	Session Timeout	***Session Timeout Values*** (Example = 86400 for every day reauth, or 43200 for every 12 hours reauthentication)
	Custom Vendor Specific Attribute	***Attribute=Value*** (Example: PaloAlto-Admin-Role=superuser or Cisco-Av-pair=shell:priv-lvl=15.)
	Custom Standard Radius Attribute	***Attribute=Value*** (Example: Idle-Timeout=600 or Termination-Action=RADIUS-Request.)
	Dynamic Wired Port Configuration	***VLAN Name Values*** (Example: 1corp-vlan or 2mgmt-vlan Egress-VLAN-Name ※ 1* = tagged 、 2* = untagged)

Auth Policy Labels

Match | Apply

Certificate Attribute

証明書の Attribute を参照して、ラベルを作成します
Auth Policy の **Match Criteria** で使用できます

Label Type	Label Values	
Certificate Attribute	Common Name (CN)	***Common Name Values*** (Example, john or john,staff*)
	Subject	***Subject Values*** (Example: /C=US/ST=CA/O=Mist/OU=LAB/CN=john or /C=US/ST=CA/O=Mist*)
	Serial Number	***Serial Number Values*** (Example: 6a524ab782fb468c00c59f51cff00268d95533b8)
	Issuer	***Issuer Values*** (Example: /C=US/ST=CA/O=Mist/OU=LAB/CN=LAB-CA)
	Subject Alternative Name (SAN)	***Subject Alternative Name Values*** (Example: user@domain.com)

Auth Policy Labels

Match | Apply

Client List

クライアントの MAC アドレスをリストし、ラベルを作成します
複数設定可、ワイルドカード(*) で OUI(ベンダーコード) の指定ができます
Auth Policy の **Match Criteria** で使用できます

Label Type	Label Values
Client List	***Client MAC Address Values/Lists*** (Example: 1122AA33BB44 and/or 11-22-AA-33-BB-44 and/or 11-22-AA*)

Auth Policy Labels

Match | Apply

Directory Attribute

Directory Attribute の Group 名のラベルを作成します
Auth Policy の **Match Criteria** で使用できます
IdP のディレクトリ情報のグループ名を評価します

Label Type	Label Values	
Directory Attribute	Group	***Group Values*** (Example: Employee)

Auth Policy Labels

Match | Apply

SSID

SSID のラベルを作成します
Auth Policy の **Match Criteria** で使用できます
ユーザ・デバイス認証時の、Radius の Called-Station-Id の値に基づき評価します
コンマ区切りで複数設定できます

Label Type	Label Values
SSID	***SSID Values*** (Example: CORP-WiFi or CORP-WiFi,Vendor-WiFi)

Auth Policy Labels

Match | Apply

MDM Compliance

MDM の デバイスコンプライアンスステータスラベルを選択します(複数選択可)
Auth Policy の **Match Criteria** で使用できます
Authorization 時 MDM より受信したデバイスコンプライアンスステータスを評価します

Label Type	Label Values
MDM Compliance	Compliant
	Non Compliant
	Unknown

※ MDM(Microsoft Intune) と連携してデバイスコンプライアンスのステータスを評価できます
- アンチウイルスのソフト・パッチ有無
- ファイアウォールステータス etc..

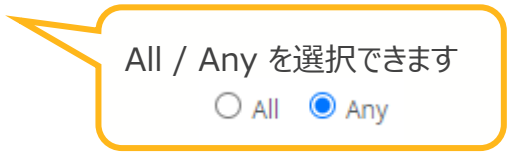
Auth Policy Labels

Match | Apply

Client Label

MAC アドレスに割り当てたラベル、およびラベルのリストを作成します
Auth Policy の **Match Criteria** で使用できます

Label Type	Label Values
Client Label	***Client Label*** (Example: building3, floor2, printer)



Use Case

- **MAB**
  MAC アドレスベースでの認証
- **EAP-TLS**
  証明書認証
- **EAP-TTLS**
  Entra ID (旧Azure AD)/OAuth
  ユーザ ID とパスワードによる認証

MAB

MAC アドレスベースでの認証

JUNIPER NETWORKS

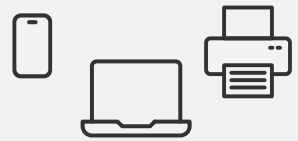
MAB (MACアドレス認証)設定手順

設定手順

STEP 01

MACアドレスの確認

- 端末の MAC アドレスを確認します



STEP 02

AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証

- AP の場合、SSID ごとの Radius 設定
- Switch の場合、Port Profile に 802.1X, MAC authentication を設定

STEP 03

Auth Policy Labels の作成

- Client List (MAC address) ラベルの作成
- VLAN ラベルの作成(Optional)

STEP 04

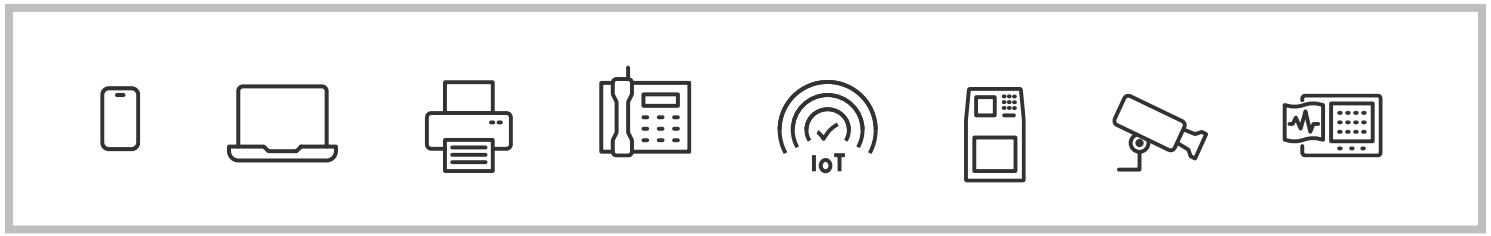
Auth Policy の設定

- STEP 03 で作成したラベルに適用するポリシーの作成

MAB (MACアドレス認証)

STEP 01 - MAC アドレスの確認

MAB 認証を行う端末の MAC アドレスを確認します



MAC アドレスを控えて、Auth Policy Label を作成します → **STEP 02**

現在、iOS 14 以降、Android 10 以降、Windows 10/11 では、デフォルトで MAC アドレスのランダム化が有効です
通常、MAC アドレス固定での運用は推奨されません

MAB は、 IEEE802.1x 認証をサポートしないサプリカント、プリンター、IP 電話、 IoT 端末(スマート家電・スマート工場)などに対するフォールバックとして提供されるのが一般的です
IEEE802.1x 認証と比較して、機密性(Confidentiality) は限定的です

MAB (MACアドレス認証)

STEP 02 - AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証

AP 設定

項目	値
Security	WPA2 > Enterprise(802.1X)
Authentication Servers	Mist Auth
VLAN	• Untagged • Tagged • Pool • Dynamic VLAN

AP 設定の詳細はこちらをご確認ください

SW 設定

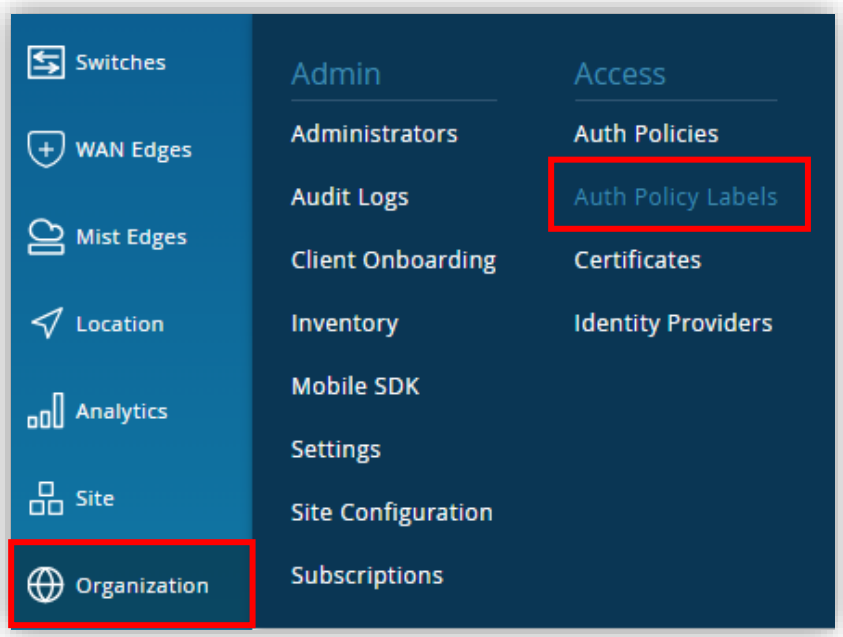
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: ***Profile Name*** ✅User dot1x authentication ✅Dynamic VLAN(Optional) Networks ✅Mac authentication
Port Configuration	Port ID: *Interface* Configuration Profile: ***Profile Name***

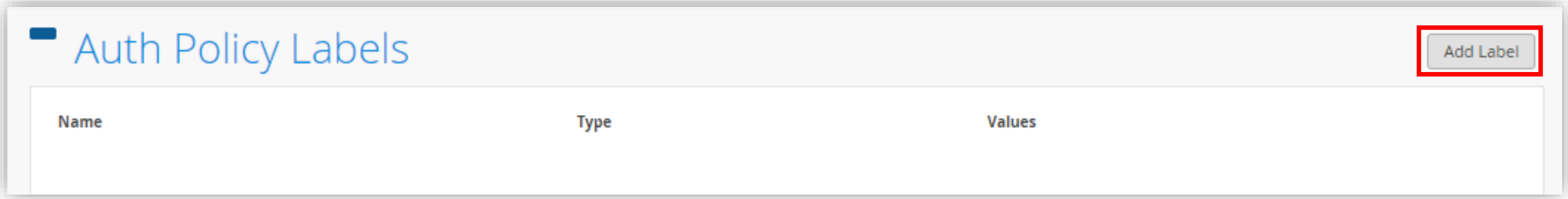
SW 設定の詳細はこちらをご確認ください

MAB（MACアドレス認証）

STEP 03 - Auth Policy Labels

1. [Organization] から [Auth Policy Labels] をクリックします
2. 画面右上の、[Add Label] をクリックします

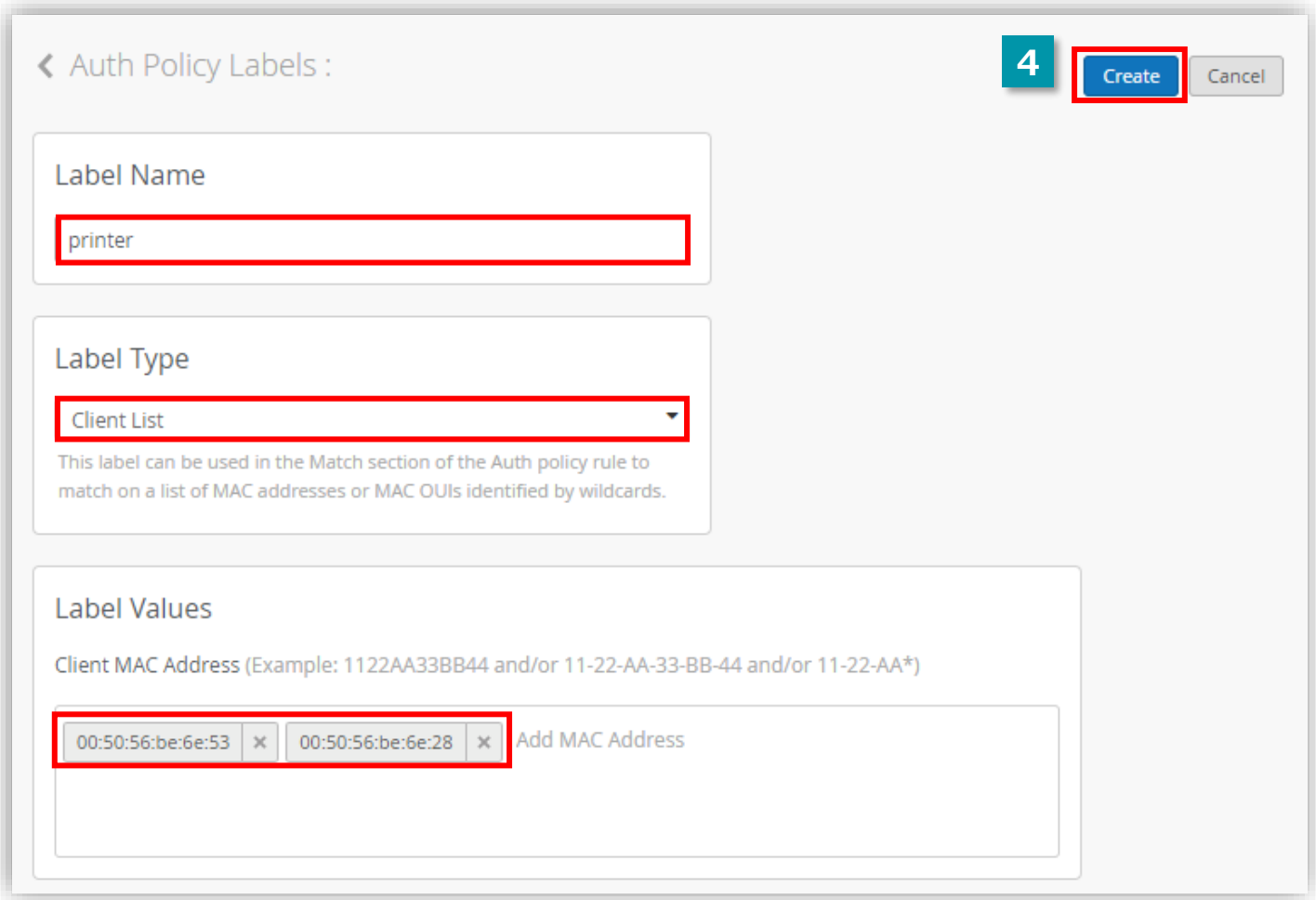




MAB（MACアドレス認証）

STEP 03 - Auth Policy Labels

3. Client List Label を作成します



1 [Label Name] を設定します

2 [Label Type] で [Client List] を選択します

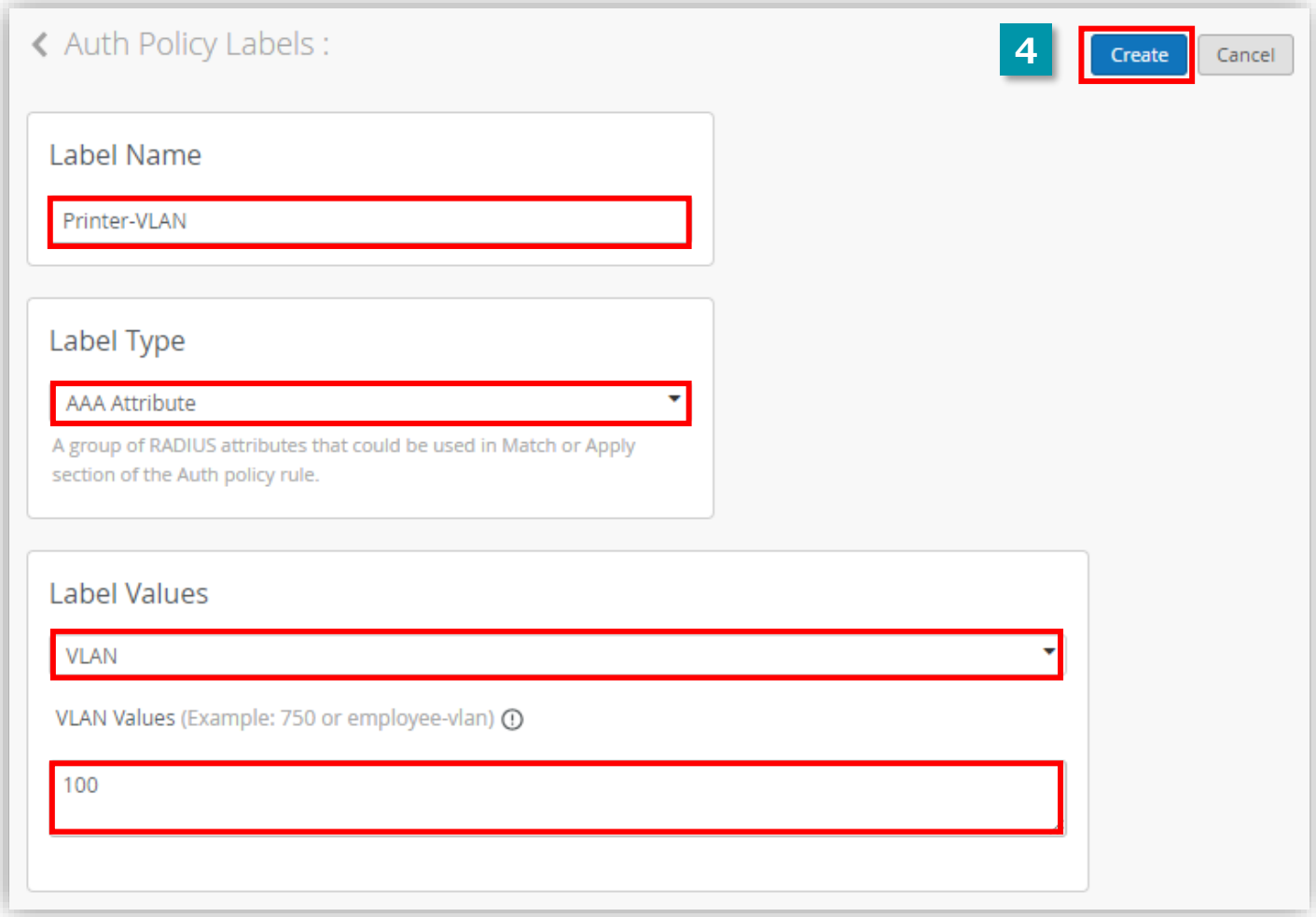
3 [Label Values] に MAC アドレスを設定します
- **複数設定できます**
- 末尾に「*」(ワイルドカード) を使用できます
- 入力時区切り文字は 「:」、「-」、「なし」 いずれも可

4 [Create] をクリックします

MAB（MACアドレス認証）

STEP 03 - Auth Policy Labels

4. 接続端末に割り当てる VLAN 用の Label を作成します(Optional)

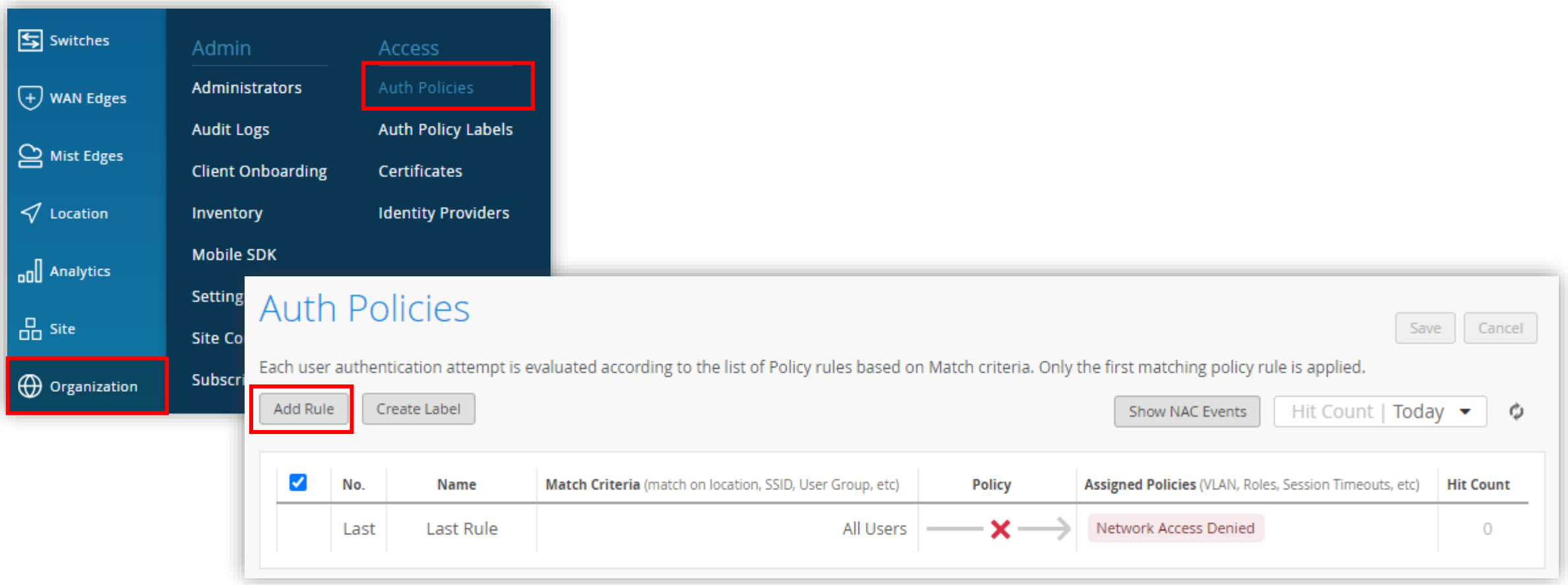


1. [Label Name] を設定します
2. [Label Type] で [AAA Attribute] を選択します
3. [Label Values] で [VLAN] を選択します
   [VLAN Values] に VLAN ID または、named VLAN を入力します
   ※ Tunnel-Private-Group-ID または、Airespace-Interface-Name をサポート
4. [Create] をクリックします

MAB（MACアドレス認証）

STEP 04 - Auth Policy

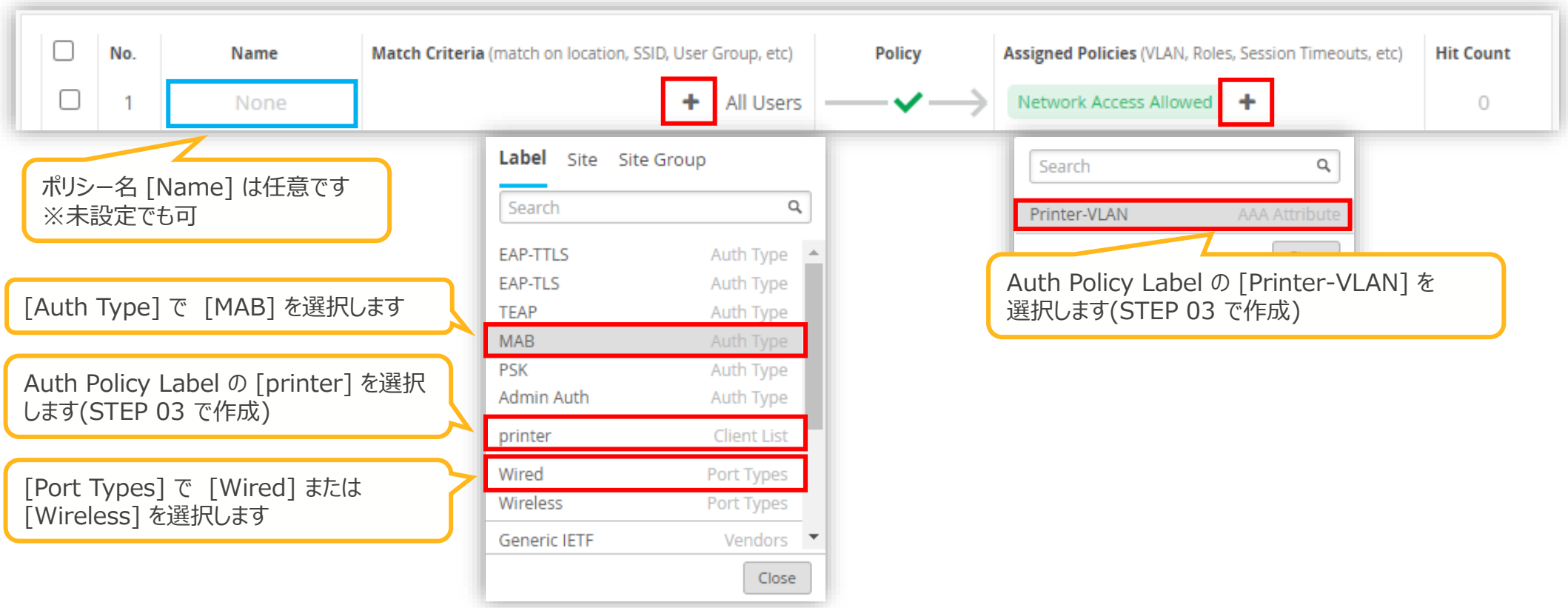
1. [Organization] から [Auth Policy] をクリックします
2. [Add Rule] をクリックします



MAB（MACアドレス認証）

STEP 04 - Auth Policy

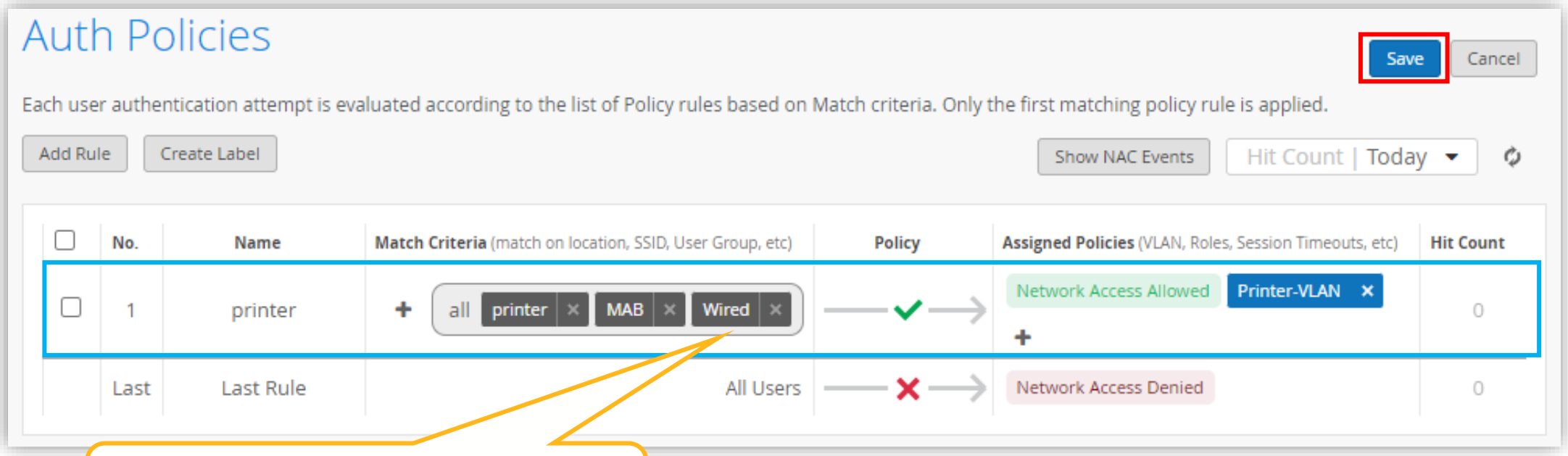
3. [Match Criteria] で [+] より、[Auth Type]、[Auth Policy Label]、[Port Types] をそれぞれ選択します
   [Assigned Policies] で [+] より、認証したクライアントに VLAN を割り当てます(Optional)



MAB（MACアドレス認証）

STEP 04 - Auth Policy

4. 作成した [Auth Policy] を確認し、[Save] をクリックします



ここでは、[Port Types] は [Wired] を選択しています
無線クライアントは、[Wireless] を選択します
[+] から設定を追加できます

Auth Policy は上から順に評価されます
最初にマッチしたポリシーのみ適用され、以降のポリシーは評価されません
どのポリシーにも該当しない場合、[Last Rule] により通信は許可されません(暗黙の Deny)

EAP-TLS

証明書認証

JUNIPER NETWORKS

EAP-TLS (証明書認証)設定手順

設定手順

STEP 01

証明書設定
- サーバ証明書の作成
- クライアント証明書の作成
- CA 証明書を Certificates に登録

クライアント設定 – PC/モバイル
- CA のルート証明書、クライアント証明書をインストール
- 接続プロファイル 無線/有線

STEP 02

AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証
- AP の場合、SSID ごとの Radius 設定
- Switch の場合、Port Profile に 802.1X を設定

STEP 03

Auth Policy Labels の作成
- Certificate Attribute Issuer ラベルの作成

STEP 04

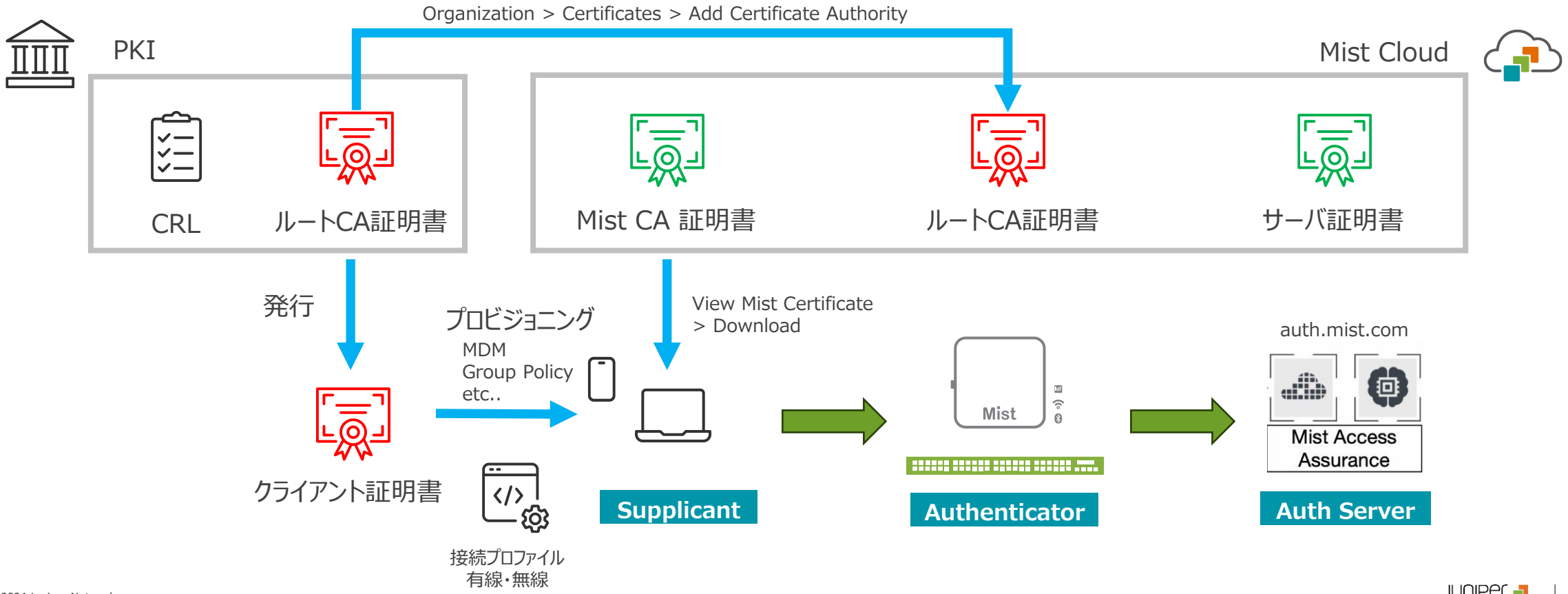
Auth Policy の設定
- STEP 03 で作成したラベルを適用したポリシーの作成

EAP-TLS (証明書認証)

STEP 01 - 証明書設定 / クライアント設定

ネットワーク環境にあわせて証明書の設定を行います

- **Mist はプライベート CA 局として動作し、サーバ証明書(auth.mist.com) を自動で発行します**
- **Mist ではクライアント証明書の発行・配布を行いません**



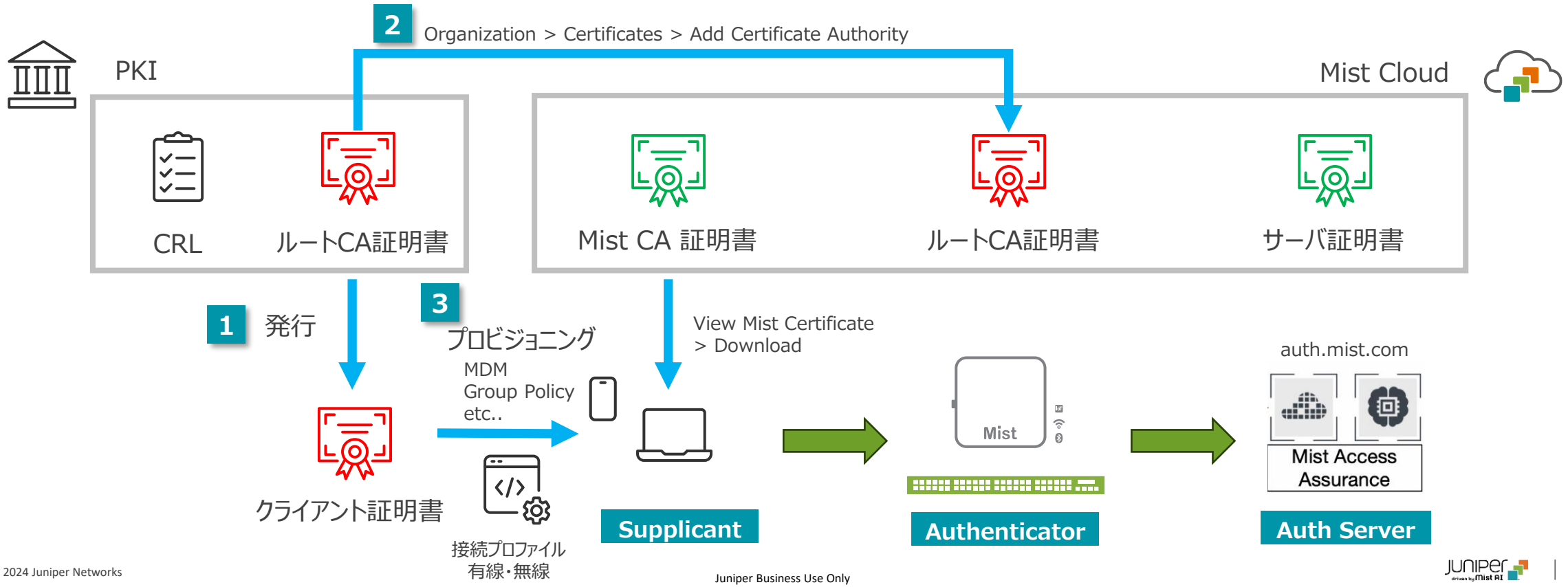
EAP-TLS (証明書認証)

STEP 01 - 証明書設定 / クライアント設定

例) デフォルトの Mist 証明書を利用、クライアント証明書外部発行

1. クライアント証明書を発行します
2. クライアント証明書を発行したルート CA 証明書を Mist にインポートします
3. Mist CA 証明書、クライアント証明書、802.1X 認証するための接続プロファイルをクライアントにインストールします

クライアントの設定は、MDM や Group Policy により構成するのが一般的です



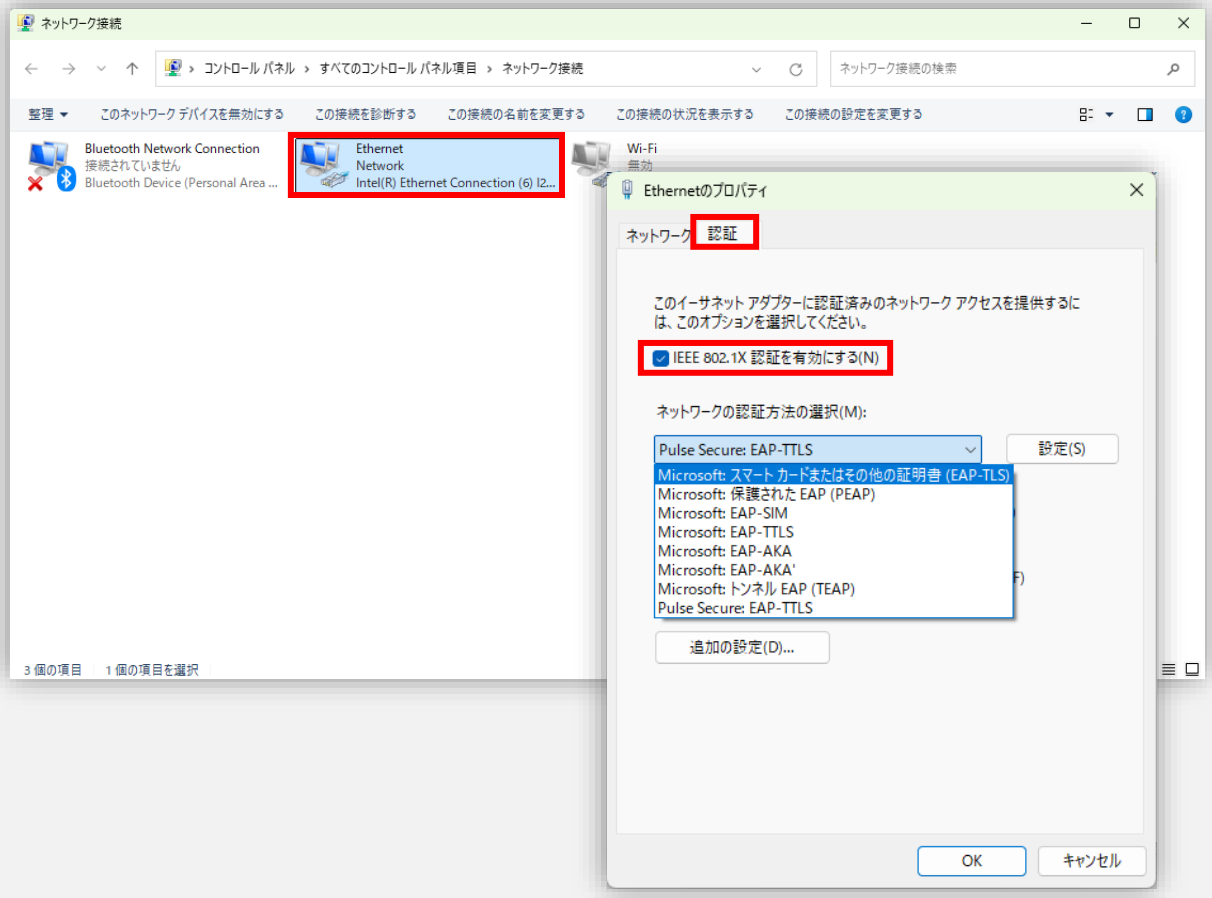
EAP-TLS (証明書認証)

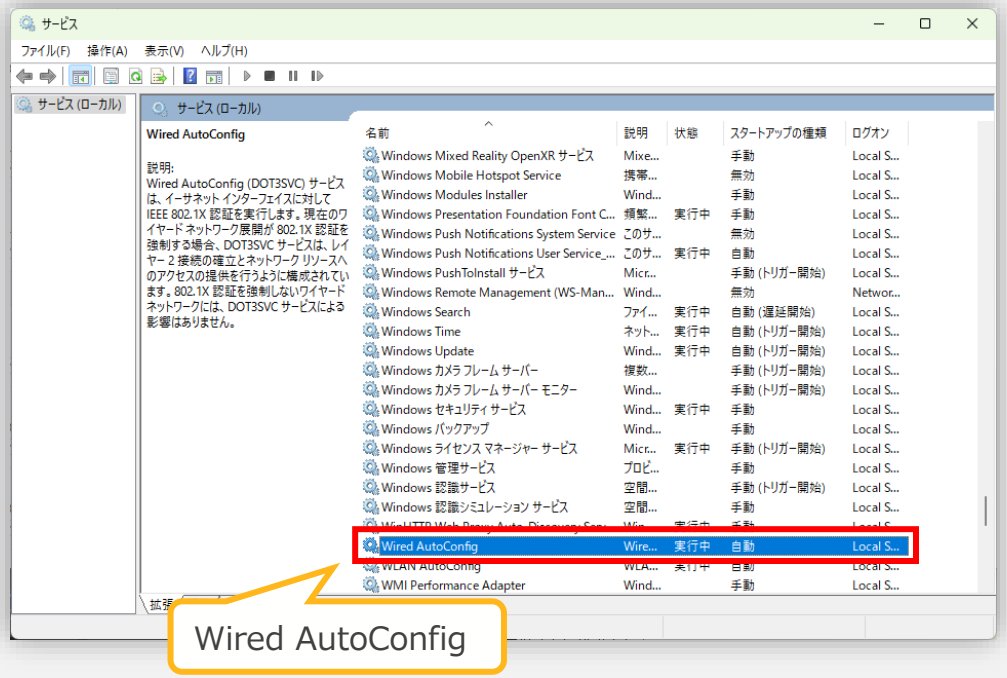
STEP 01 - 証明書設定 / クライアント設定

証明書の配布、接続プロファイルの設定詳細についてはシステム管理者にご相談ください

Note

802.1X 認証は、Ethernet のプロパティから認証タブで設定します
認証タブの表示には、Wireless/Wired AutoConfig サービスを起動する必要があります





EAP-TLS (証明書認証)

STEP 02 - AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証

Wireless: AP 設定

項目	値
Security	WPA2 > Enterprise(802.1X)
Authentication Servers	Mist Auth
VLAN	• Untagged • Tagged • Pool • Dynamic VLAN

AP 設定の詳細はこちらをご確認ください

Wired: SW 設定

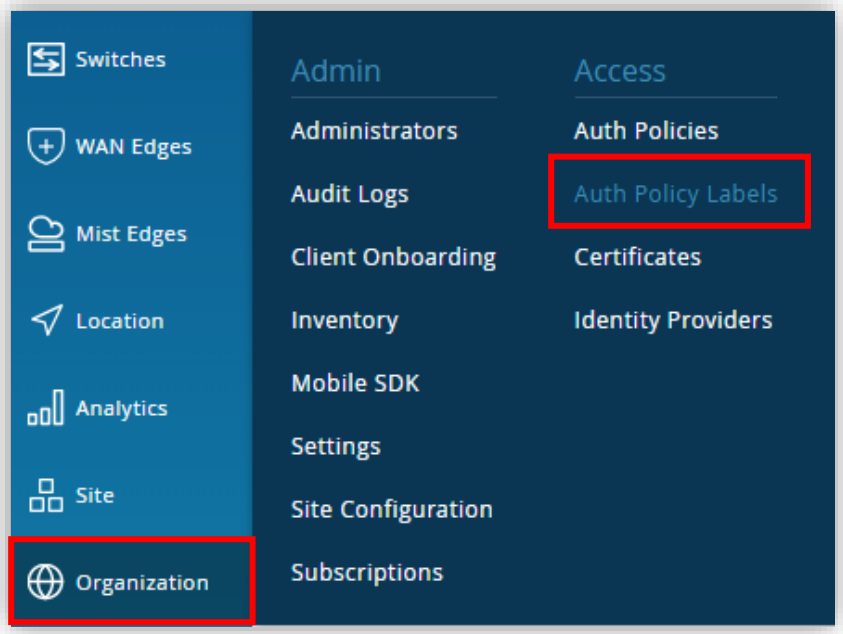
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: ***Profile Name*** ✅User dot1x authentication ✅Dynamic VLAN(Optional) Networks
Port Configuration	Port ID: *Interface* Configuration Profile: ***Profile Name***

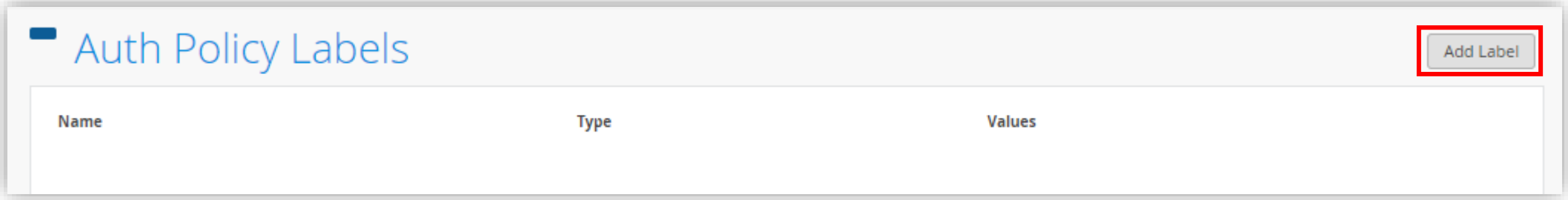
SW 設定の詳細はこちらをご確認ください

EAP-TLS (証明書認証)

STEP 03 - Auth Policy Labels

1. [Organization] から [Auth Policy Labels] をクリックします
2. 画面右上の、[Add Label] をクリックします



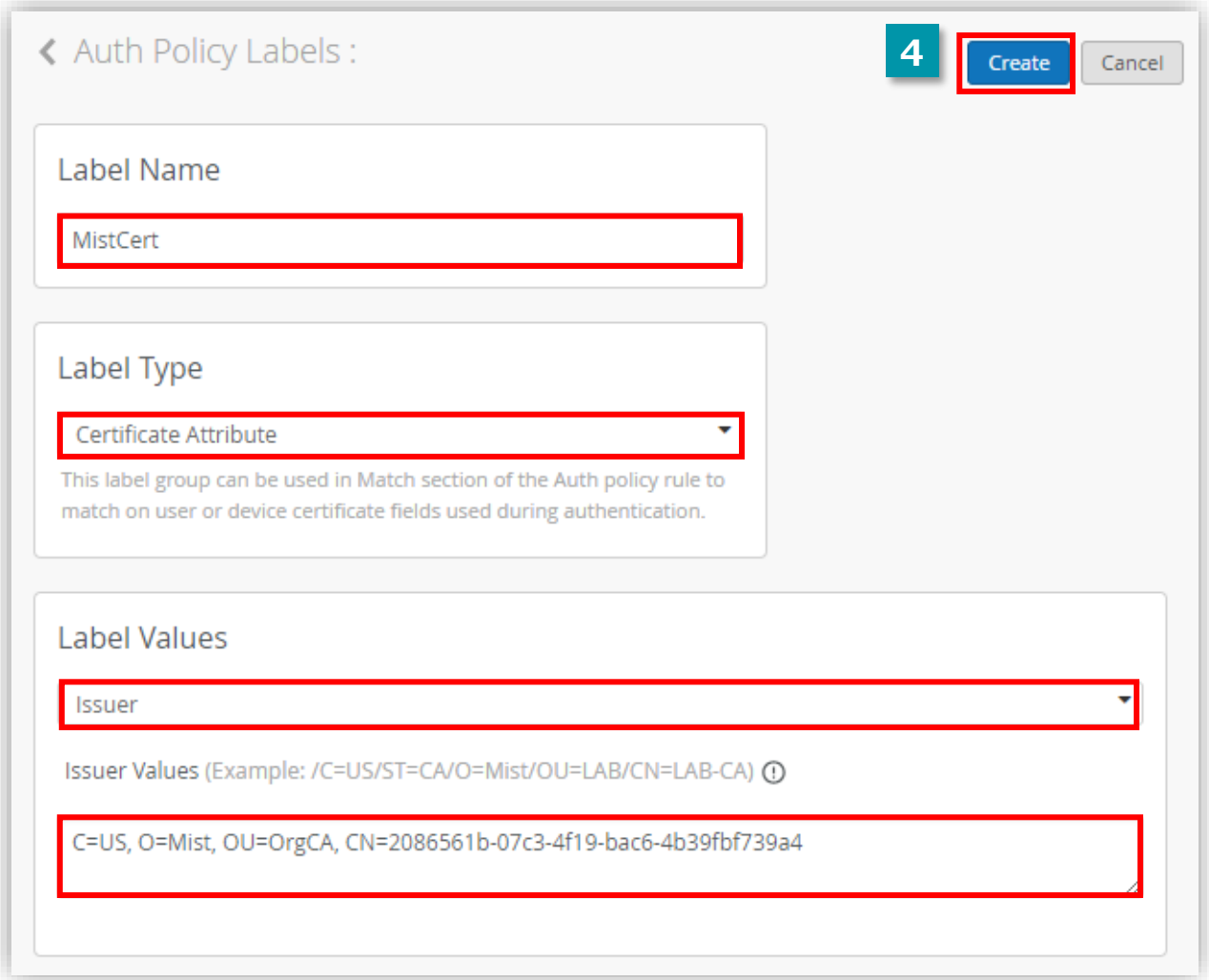


EAP-TLS (証明書認証)

STEP 03 - Auth Policy Labels

要件にあわせた Label を設定します
ここでは、一例として Certificate の Issuer を参照する Label を設定しています

3. Label を設定します



1. [Label Name] を設定します

2. [Label Type] で [Certificate Attribute] を選択します

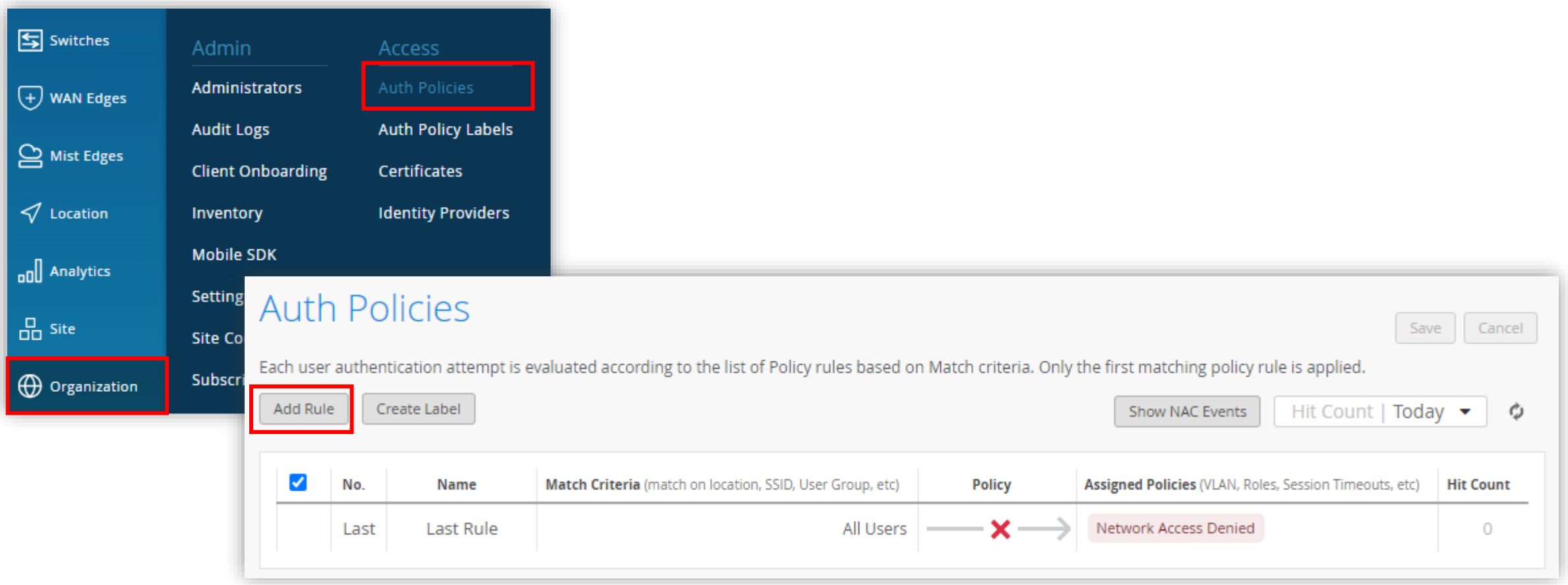
3. [Label Values] に [Issuer] を選択、[Issuer Values] に値を設定します
値は、デフォルトの Mist CA 証明書の Issuer を参照します
Organization > Certificate > View Mist Certificate > Issuer

4. [Create] をクリックします

EAP-TLS (証明書認証)

STEP 04 - Auth Policy

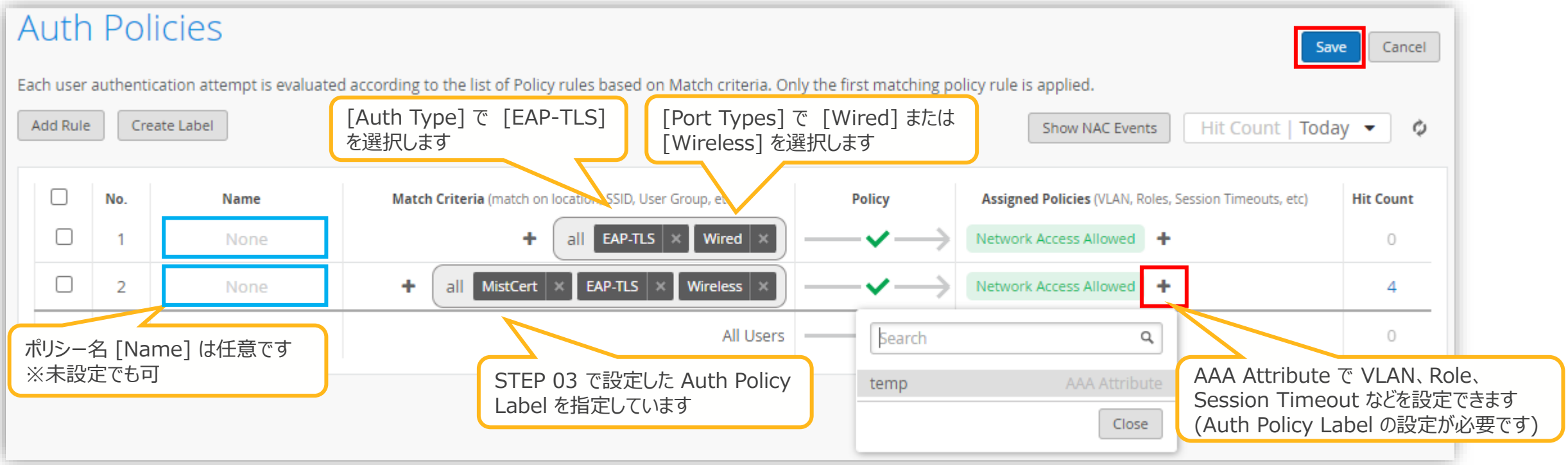
1. [Organization] から [Auth Policy] をクリックします
2. [Add Rule] をクリックします



EAP-TLS (証明書認証)

STEP 04 - Auth Policy

3. [Match Criteria] で [+] より、[Auth Type]、[Auth Policy Label]、[Port Types] をそれぞれ選択します
   [Assigned Policies] で [+] より、認証したクライアントに VLAN、Role、Session Timeout など設定できます (Optional)
   [Save] で設定を保存します



EAP-TTLS

Entra ID/OAuth

JUNIPER NETWORKS

EAP-TTLS Entra ID/OAuth 連携設定手順

設定手順

STEP 01

証明書設定
- サーバ証明書の作成
- CA 証明書を Certificates に登録

クライアント設定 – PC/モバイル
- CA のルート証明書をインストール
- 接続プロファイル 無線/有線

IdP 設定
- Entra ID: アプリの登録
- Mist: Add IDP

STEP 02

AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証
- AP の場合、SSID ごとの Radius 設定
- Switch の場合、Port Profile に 802.1X を設定

STEP 03

Auth Policy Labels の作成
- **Match:** Directory Attribute ラベルの作成 (Entra ID のディレクトリ情報を参照)
- **Assigned Policies:** AAA Attribute Role ラベルの作成 (ディレクトリ情報を Role としてユーザに付与)

STEP 04

Auth Policy の設定
- STEP 03 で作成したラベルを適用したポリシーの作成

WxLAN Policy 設定
- ラベル作成
- ポリシー作成

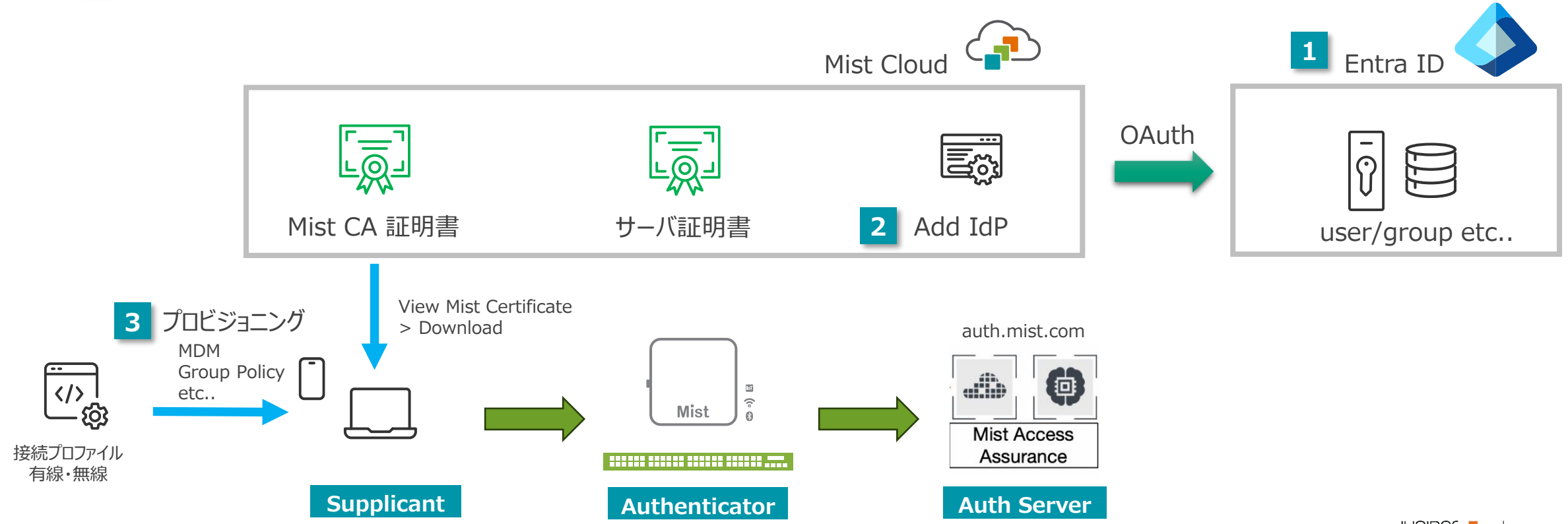
EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 01 - 証明書設定 / クライアント設定 / IdP 設定

例) EAP-TTLS Entra ID/OAuth 連携

1. Entra ID にアプリを登録します
2. Mist Cloud で Add IdP から Identity Providers を設定します
3. Mist CA 証明書、802.1X 認証するための接続プロファイルをクライアントにインストールします

Entra ID 連携では、内部認証プロトコルとして PAP のみサポートされます(EAP-TTLS の注意点参照)



EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 02 - AP 設定 / スイッチ設定：Mist Auth / 802.1X 認証

Wireless: AP 設定

項目	値
Security	WPA2 > Enterprise(802.1X)
Authentication Servers	Mist Auth
VLAN	• Untagged • Tagged • Pool • Dynamic VLAN

AP 設定の詳細はこちらをご確認ください

Wired: SW 設定

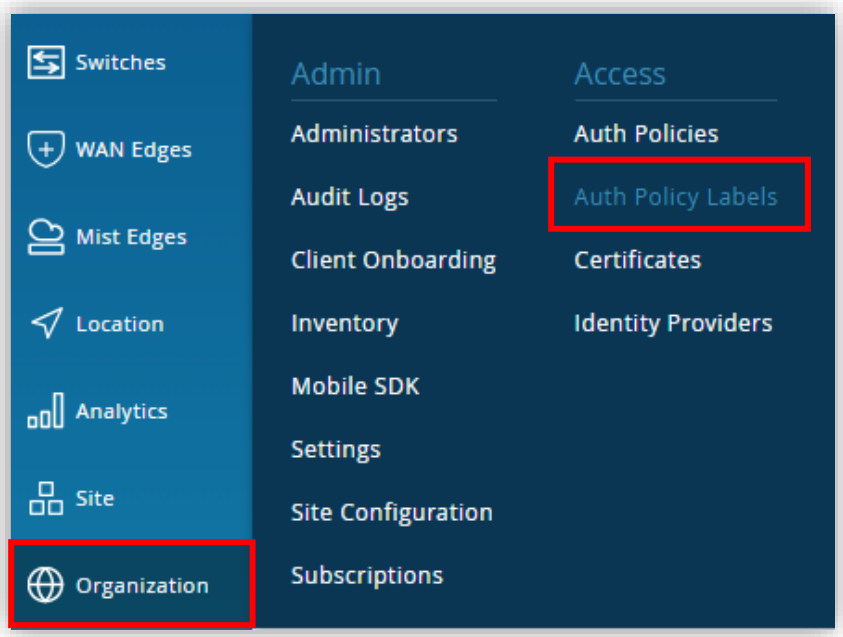
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: ***Profile Name*** ✅User dot1x authentication ✅Dynamic VLAN(Optional) Networks
Port Configuration	Port ID: *Interface* Configuration Profile: ***Profile Name***

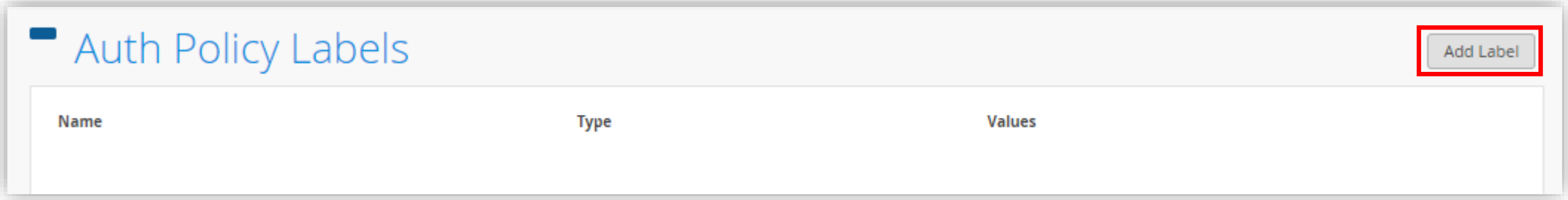
SW 設定の詳細はこちらをご確認ください

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 03 - Auth Policy Labels

1. [Organization] から [Auth Policy Labels] をクリックします
2. 画面右上の、[Add Label] をクリックします

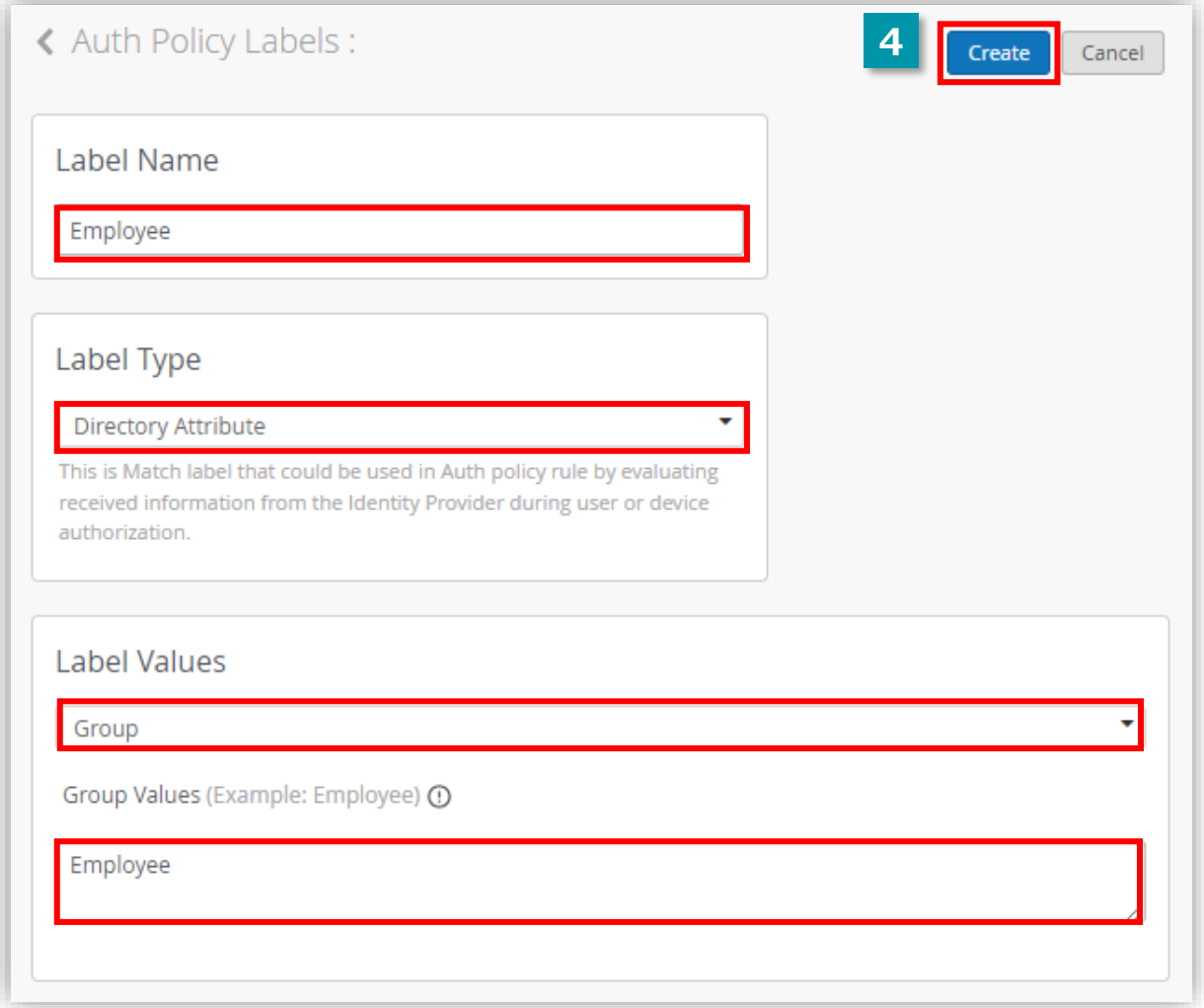




EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 03 - Auth Policy Labels

3. Directory Attribute Label を設定します



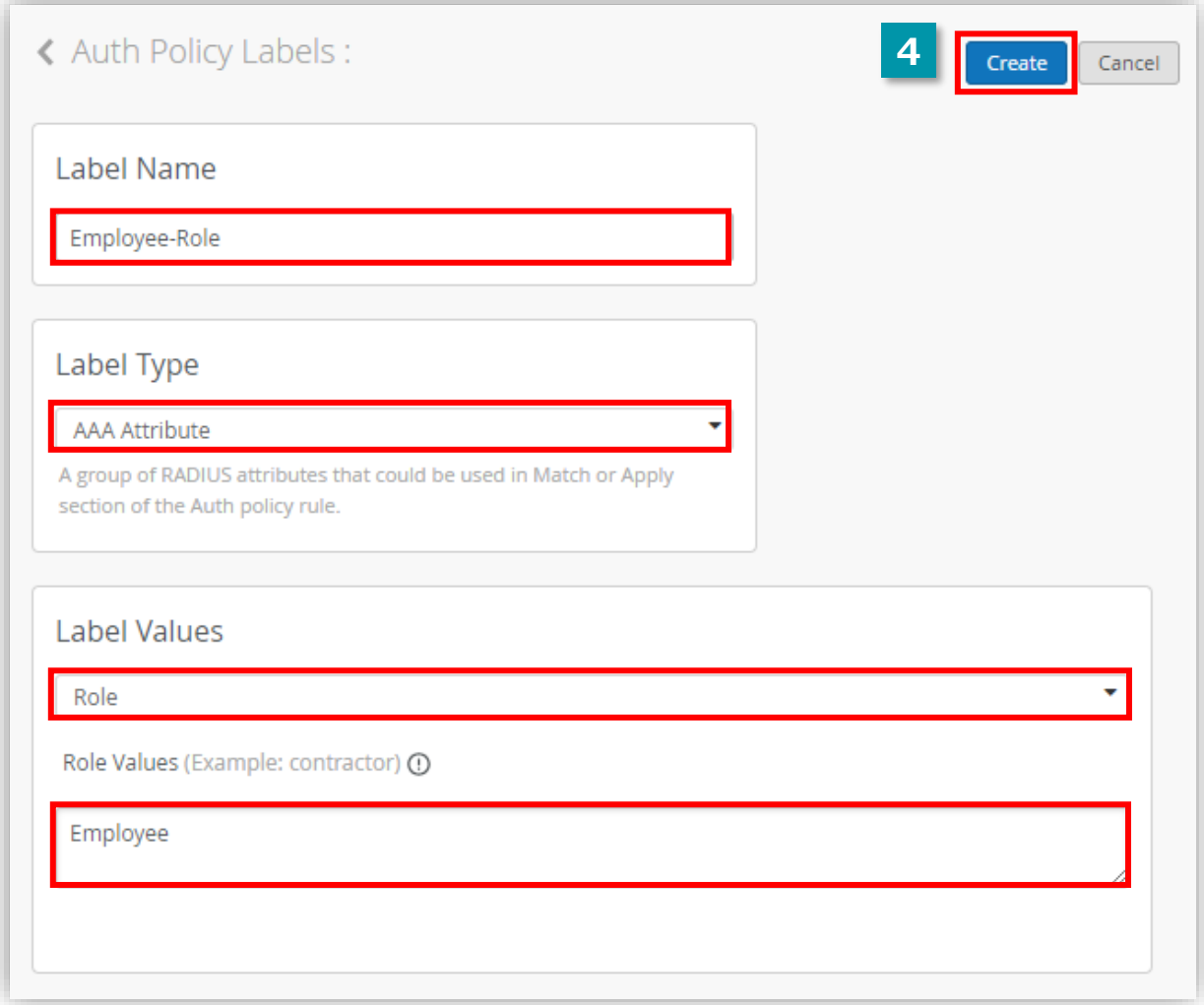
要件にあわせた Label を設定します
ここでは、一例として Entra ID の Directory 情報を参照しています

1. [Label Name] を設定します
2. [Label Type] で [Directory Attribute] を選択します
3. [Label Values] に [Group] を選択、[Group Values] に値を設定します
   Entra ID 連携し、Directory 情報を参照します
   ここでは、例として Employee としています
4. [Create] をクリックします

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 03 - Auth Policy Labels

4. AAA Attribute Label を設定します



参照した Directory 情報の Group: Employee を Role として設定します

1 [Label Name] を設定します

2 [Label Type] で [AAA Attribute] を選択します

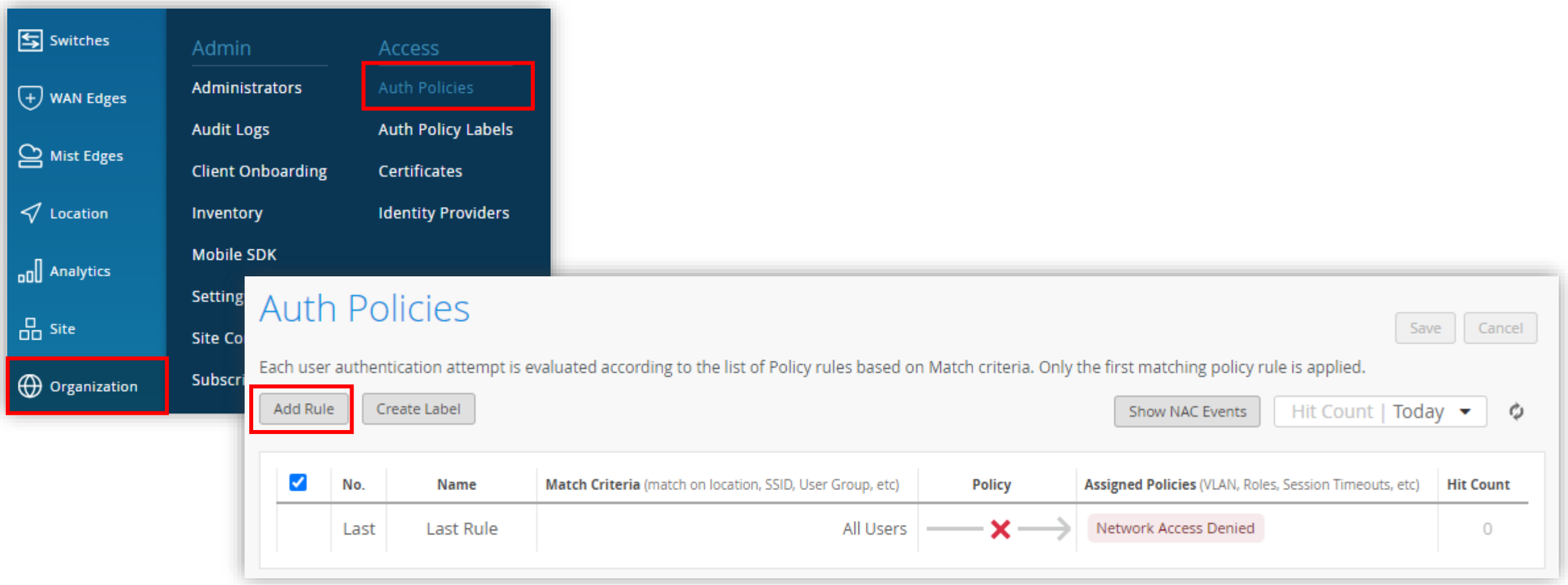
3 [Label Values] に [Role] を選択、[Role Values] に値を設定します
Entra ID 連携し、参照した Directory 情報 Employee を Role Values に設定します
(Role ベースでポリシー制御を行います)

4 [Create] をクリックします

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - Auth Policy

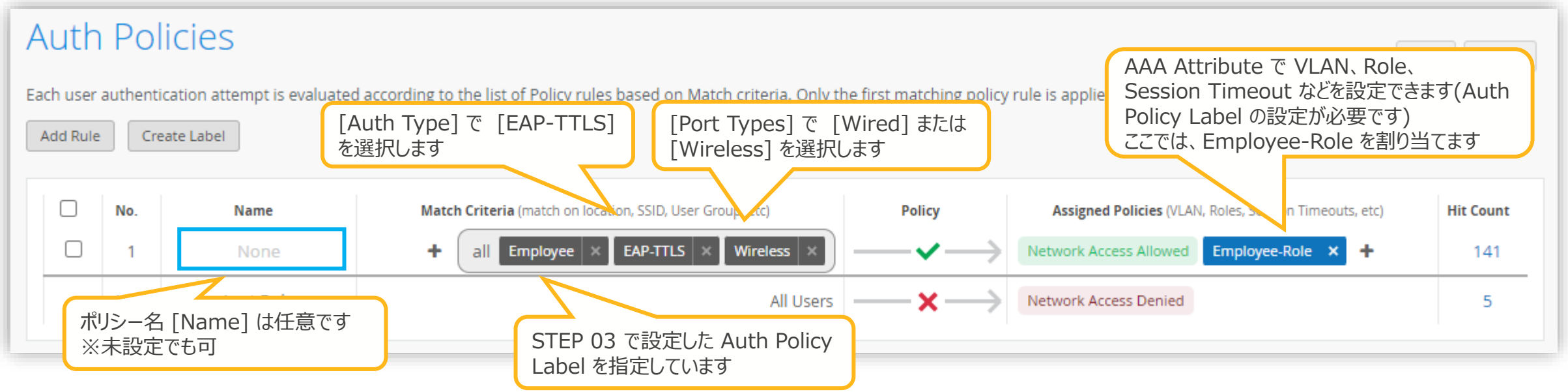
1. [Organization] から [Auth Policy] をクリックします
2. [Add Rule] をクリックします



EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - Auth Policy

3. [Match Criteria] で [+] より、[Auth Type]、[Auth Policy Label]、[Port Types] をそれぞれ選択します
   [Assigned Policies] で [+] より、認証したクライアントに VLAN、Role、Session Timeout など設定できます (Optional)
   [Save] で設定を保存します

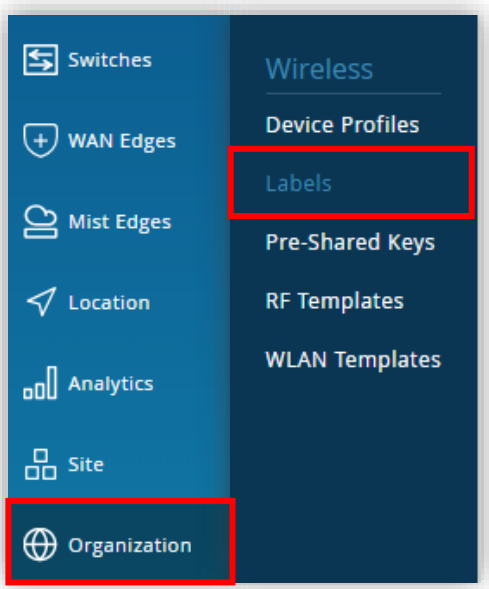


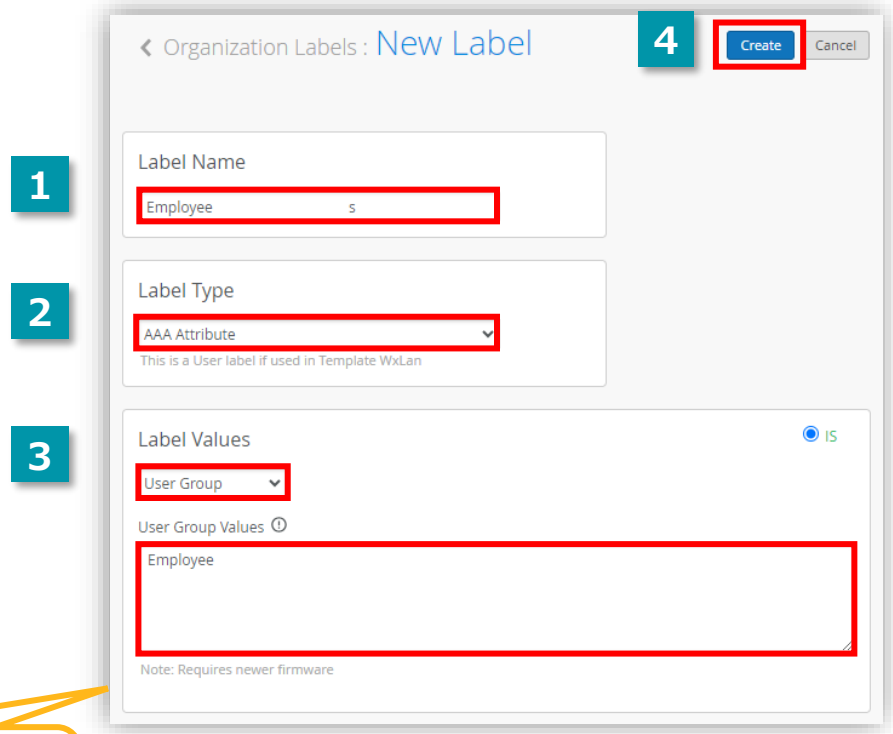
続いて、割り当てた Role に対してアクセス可能なリソースを設定するための WxLAN Policy を設定します

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - WxLAN Policy

1. [Organization] から [Labels] で、Label を作成します





WLAN Template の Policy には Organization レベルの Label を設定します

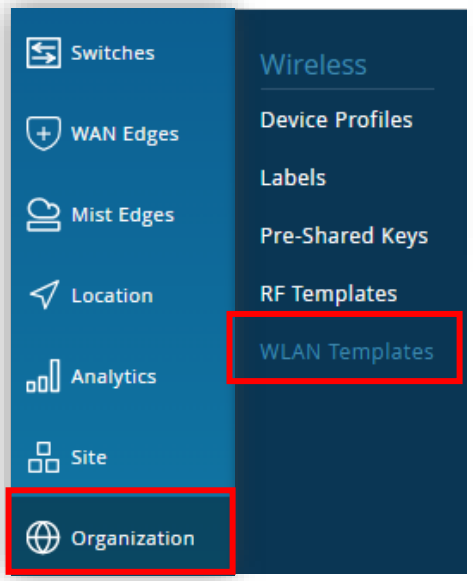
Auth Policy Labels とは別に、WxLAN Policy 用に Label を作成する必要があります

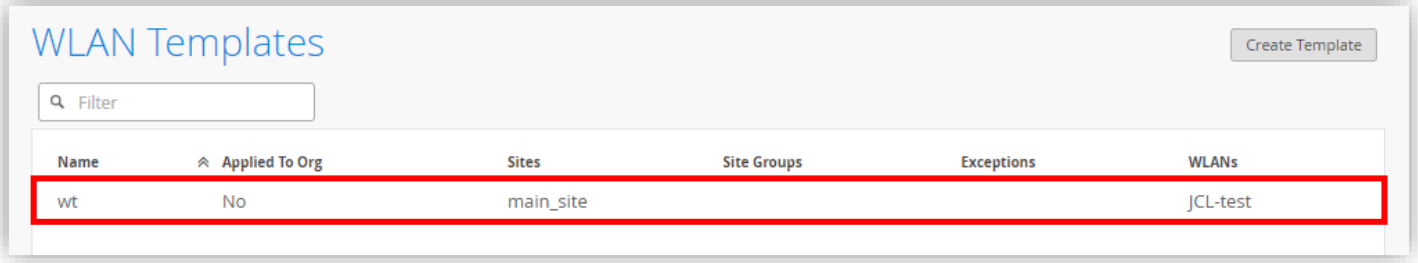
1. [Label Name] を設定します
2. [Label Type] で [AAA Attribute] を選択します
3. [Label Values] に [User Group] を選択、[User Group Values] に値を設定します
   Entra ID 連携し、参照した Directory 情報 Employee をUser Group Values に設定します
   (Role ベースでポリシー制御を行います)
4. [Create] をクリックします

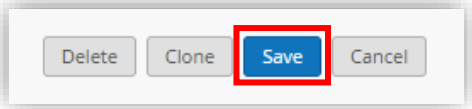
EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - WxLAN Policy

2. [Organization] から [WLAN Templates] で編集する WLAN Template を選択します
3. [Policy] の項目で、[User] に作成した Label(Role): Employee を設定、User に対する [Resource] を割り当て、[Save] で設定を保存します







Label(Role): Employee を設定します

設定した Role に対する Resource を割り当てます
ここでは、Facebook へのアクセスを制限、その他通信は許可しています

Wireless ユーザに対して、Role ベースの通信制御ができます

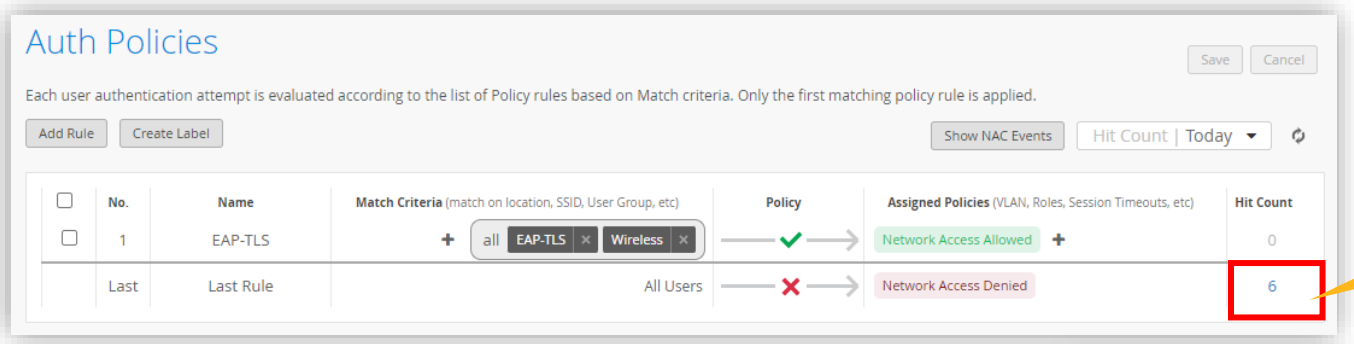
Troubleshoot Tips

JUNIPER NETWORKS

Troubleshoot Tips

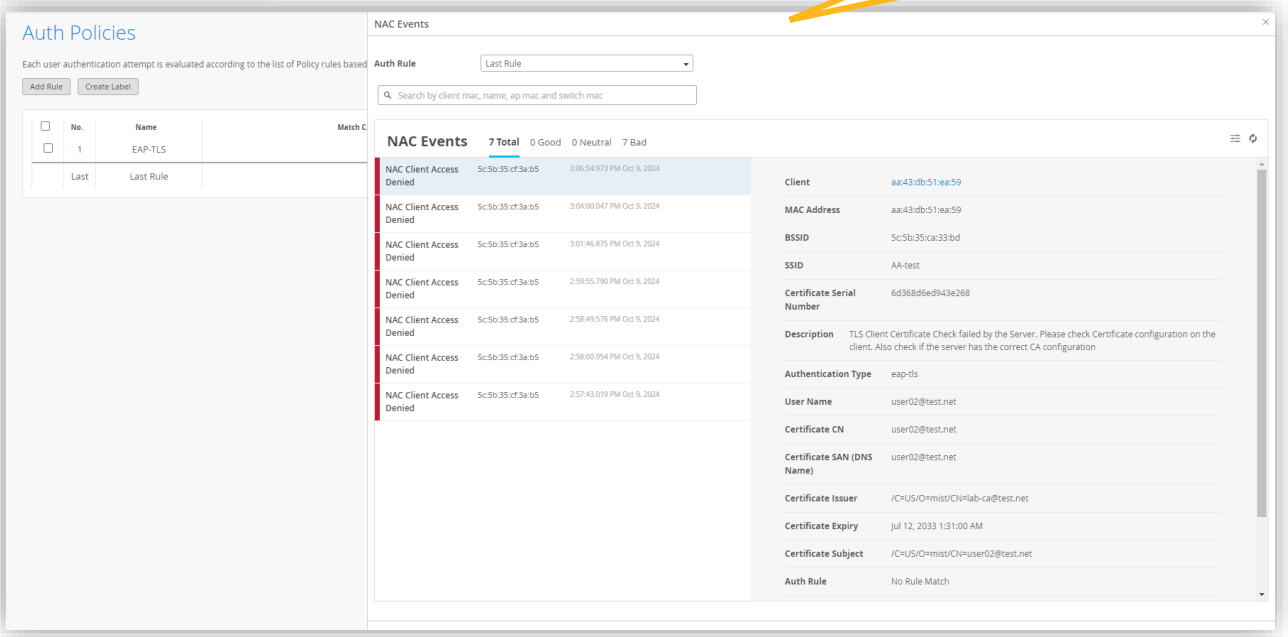
Auth Policy Hit Counts > NAC Events

Auth Policies の Hit Count から NAC Events を確認できます



Hit Count の数字部分をクリック

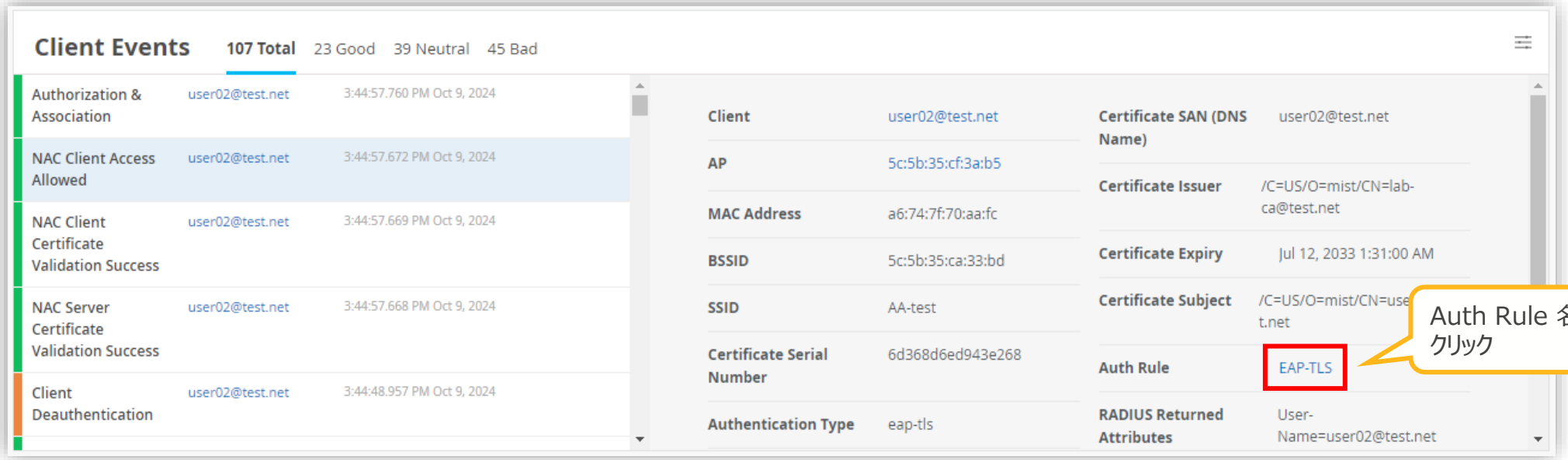
右端に NAC Events が表示されます

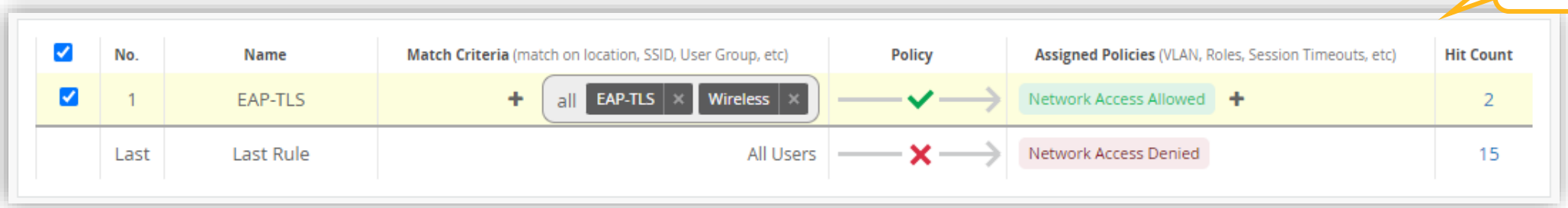


Troubleshoot Tips

Client Events > Auth Policy

Client Events から、Auth Rule 名をクリックすることで接続を処理した Auth Policy の設定に遷移できます

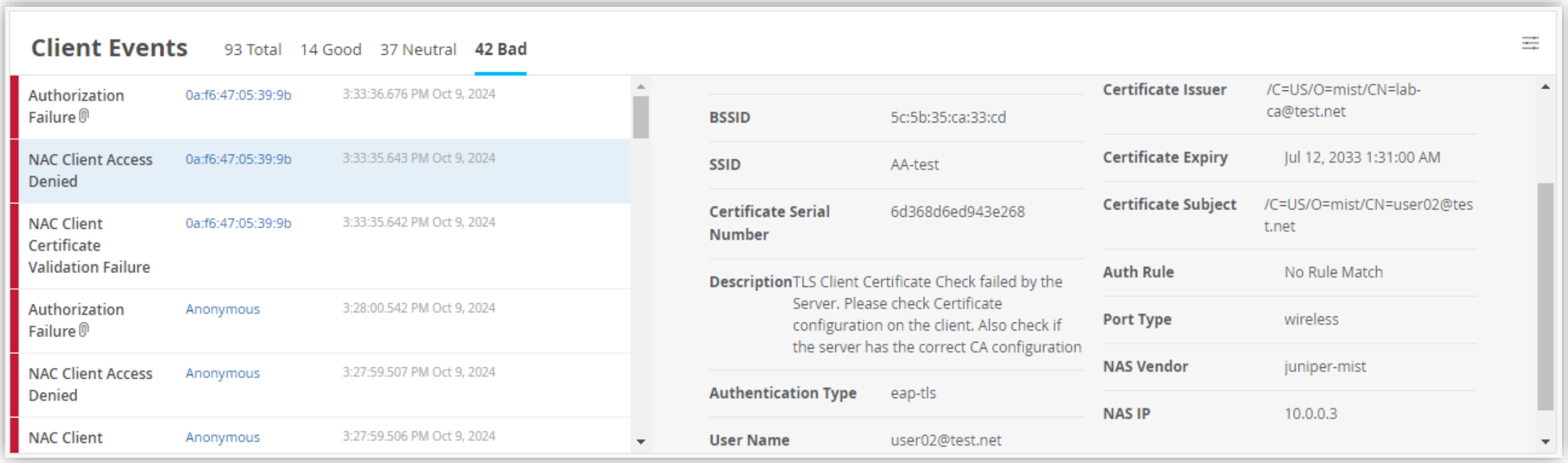




Troubleshoot Tips

EAP-TLS: Certificate Check failed

証明書認証において、正しく証明書が構成されていない場合、以下のようなログが表示されます

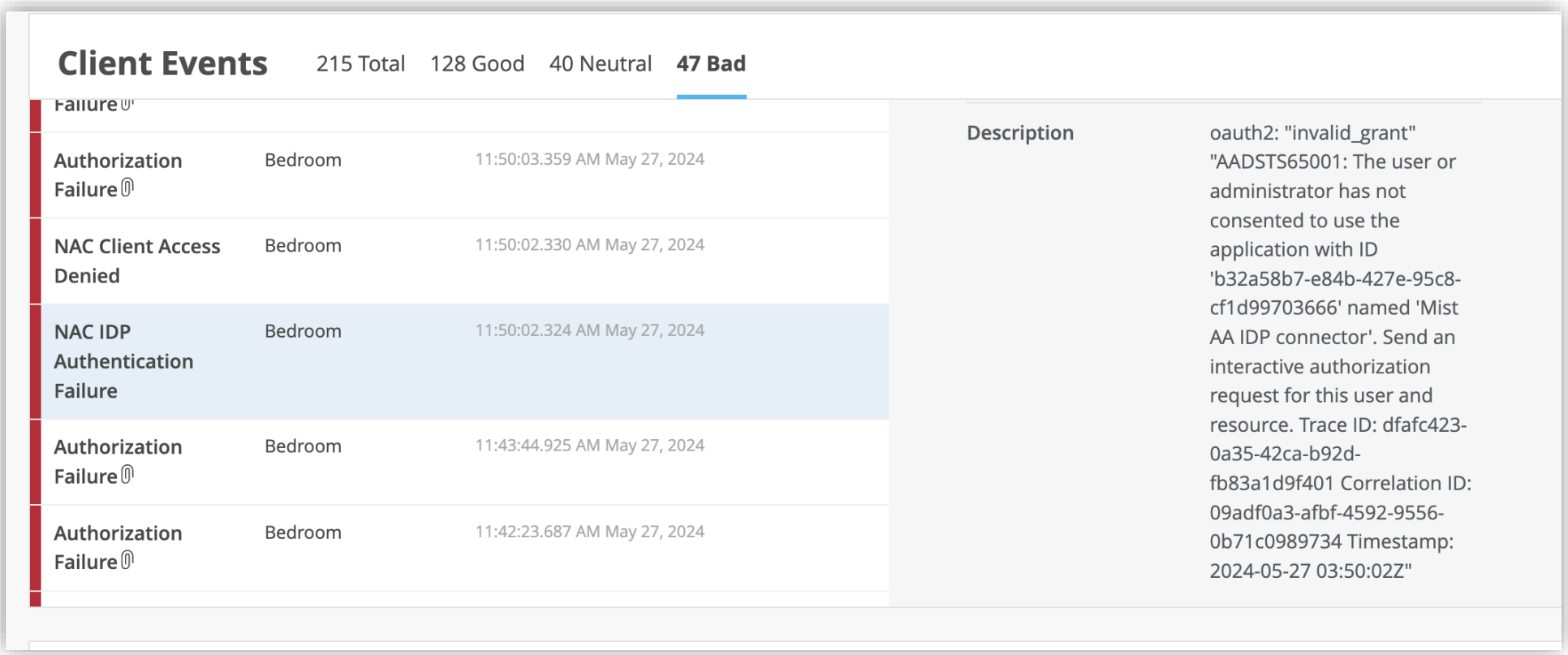


クライアントおよび Mist Cloud で証明書が正しく構成されていることを確認します

Troubleshoot Tips

EAP-TLS/EAP-TTLS: IdP connector error

Mist と Identity Provider で正しく設定がされていない場合や、アクセス権が付与されていない場合、以下のようなログが出力されます



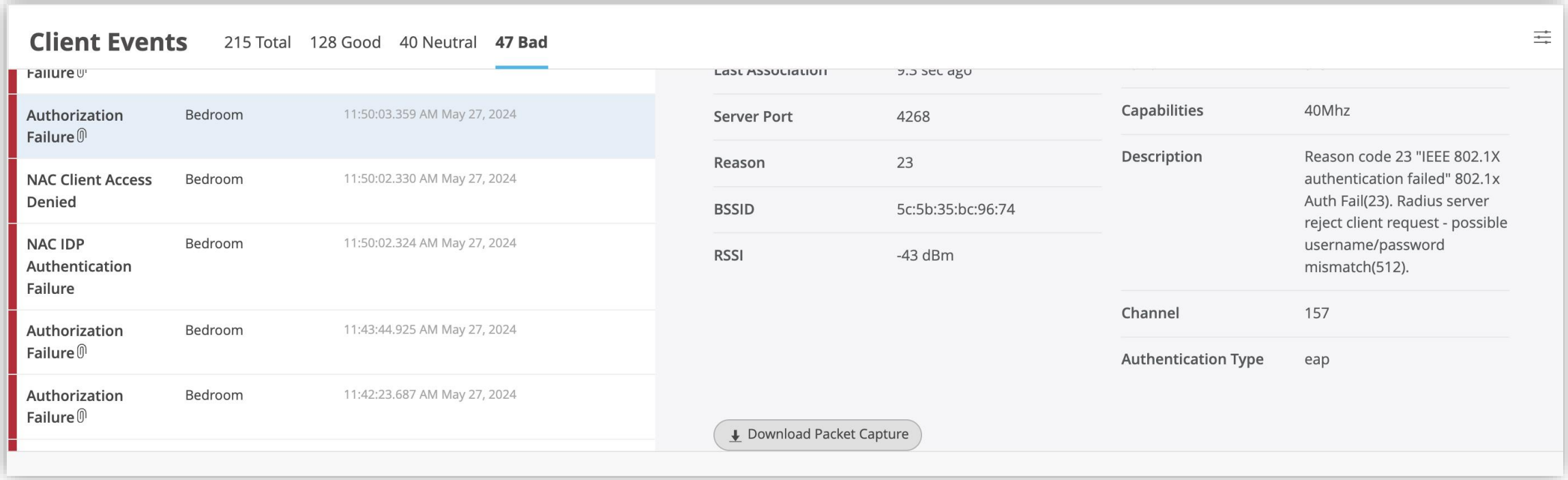
Mist および Entra ID 側で正しく設定され、権限が付与されていることを確認します

Troubleshoot Tips

Entra ID 連携では、内部認証プロトコルとして PAP のみサポートされます(EAP-TTLS の注意点参照)

EAP-TLS/EAP-TTLS: IdP Invalid Inner Authentication Protocol

クライアントが誤った認証情報(username/password) を入力した場合や、PAP 以外(MS-Chapv2 など)の内部認証プロトコルで認証を試みた場合、認証に失敗します
以下のようなログが表示されます



認証情報の確認および内部認証プロトコルとして PAP が使用されていることを確認します

Appendix

Webhook

JUNIPER NETWORKS

Webhook

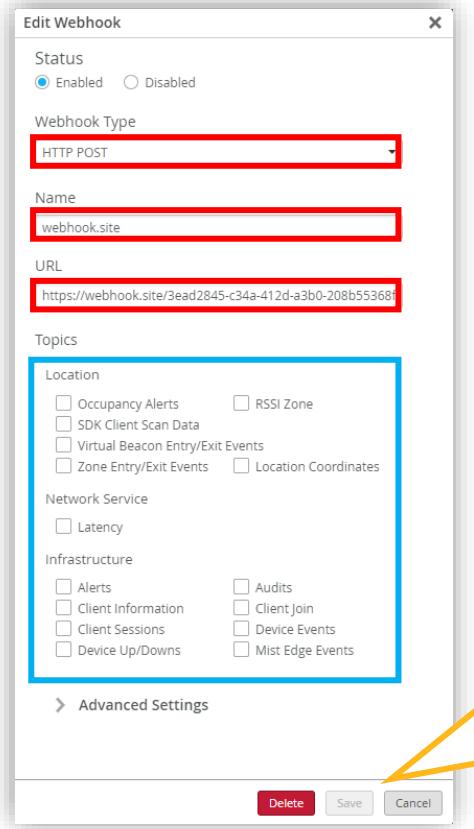
Webhook Configurations

この手順では、一旦 GUI 上で Webhook を設定し、
AA 関連の topics の追加を API で行っています

現時点では Access Assurance 関連の Webhook は API のみで設定可能です
"topics" の"nac-accounting", "nac-events“ の取得が可能です

1. Webhook(Site) の設定

- Organization > Site Configuration > {Site} > Add Webhook



[Webhook Type] を確認します

[Name] を設定します

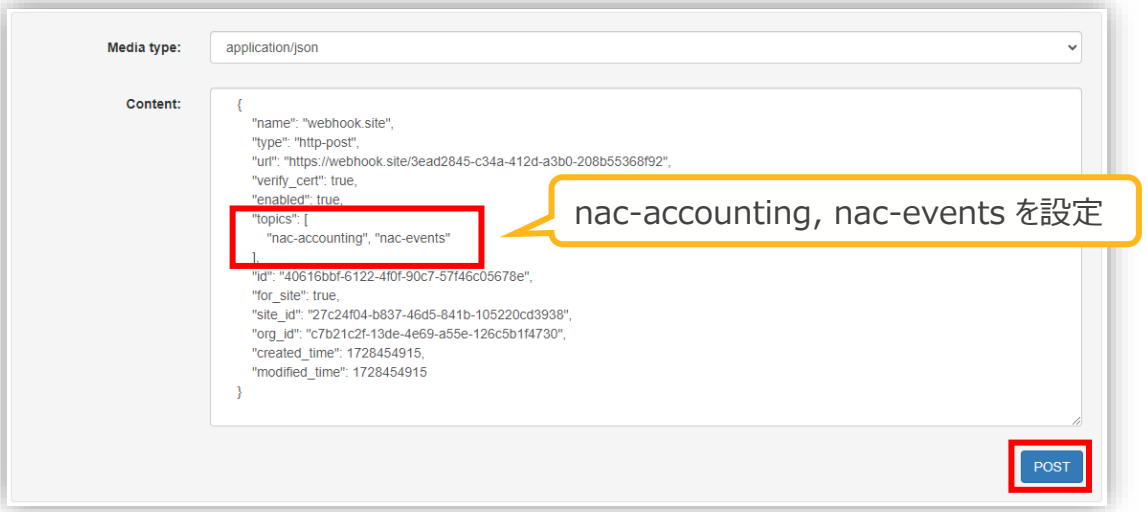
[URL] を設定します

Webhook で取得する [topics] に
チェックを入れます
**※現在 AA 関連の topics は
GUI で設定できません(右記参照)**

一つ以上の topics を有効化しないと
[Save] できません
AA 関連の topics を有効化したい
場合は一旦いずれかの topics を有
効にして [Save] してください

2. API での topics 追加

- Site ID を確認
  - Organization > Site Configuration > {Site} > Site ID
- https://api.mist.com/api/v1/sites/***{site_id}***/webhooks (Global 01)
  にアクセス、左記手順で作成した現在の Webhook の設定を確認します
- topics に、nac-accounting, nac-events を追加し [POST] します



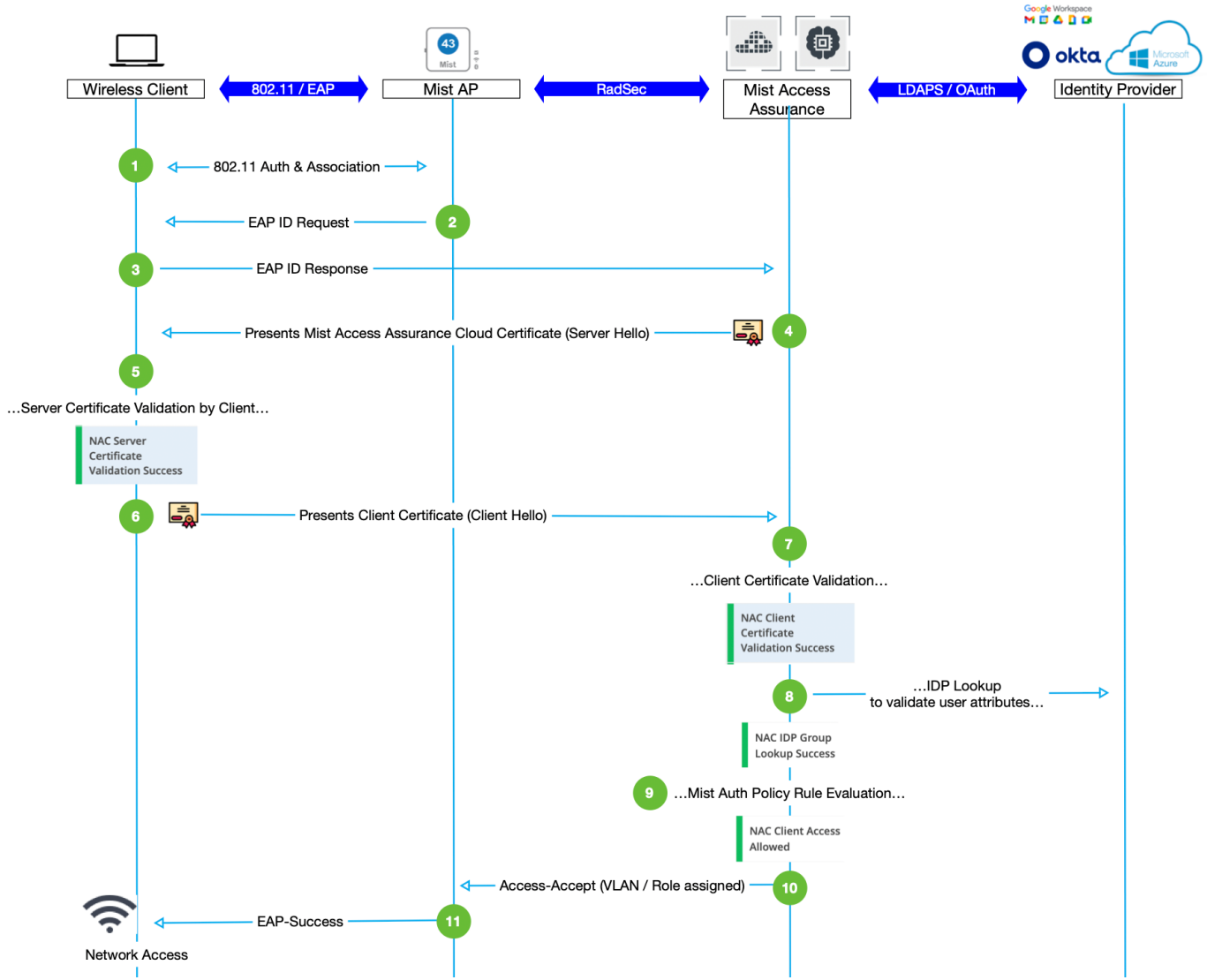
※ 設定の上書きではなく新規設定になるので、不要な設定は削除します

REFERENCE:
Configure Webhooks from the API
Webhooks(API Documentation) ※要サインイン

EAP 認証フロー

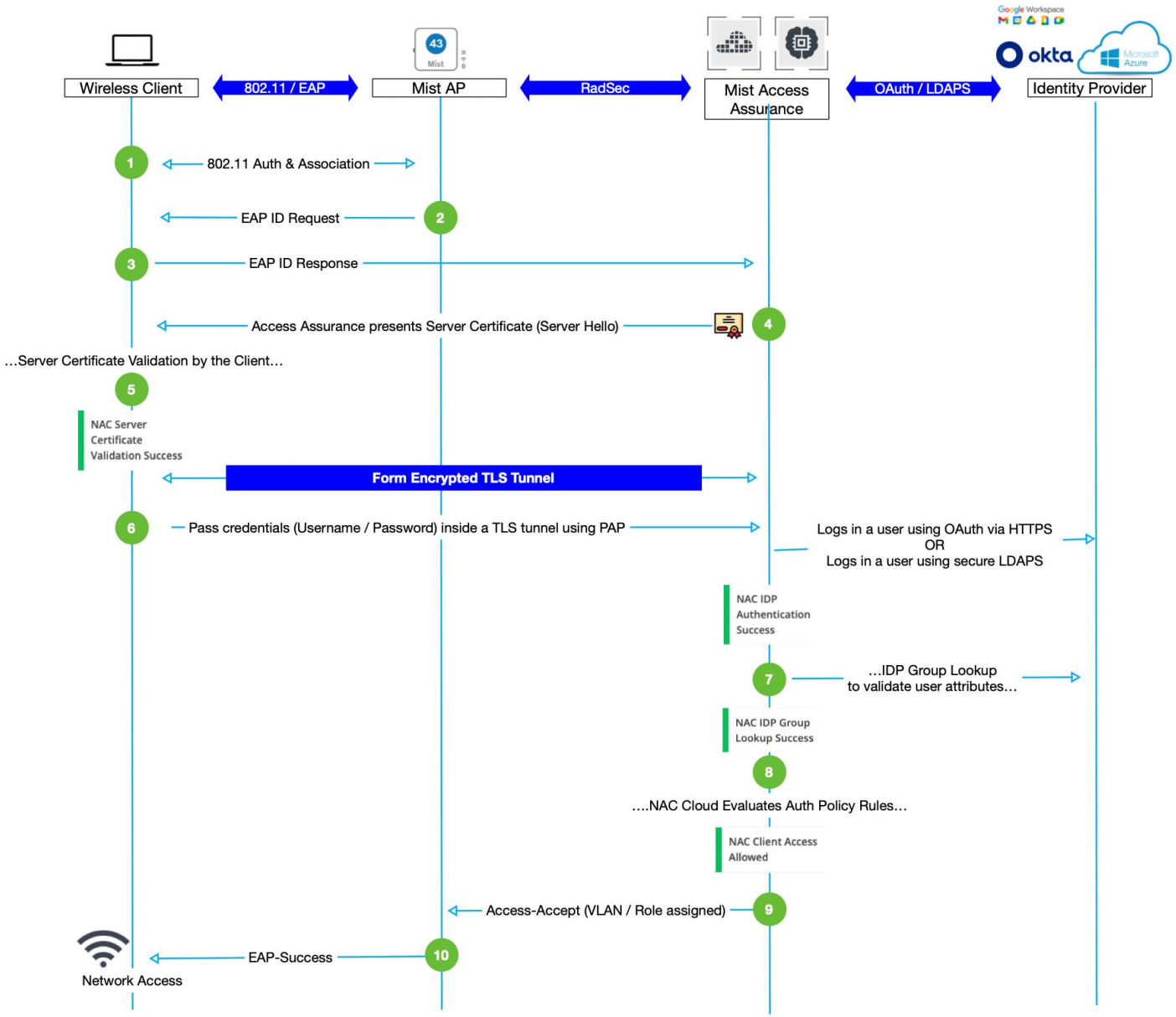
EAP-TLS 認証フロー

1. 認証装置 (AP など) がセッション要求を開始するか、サプリカント (ワイヤレス クライアント デバイス) が認証装置にセッション開始要求を送信します。
2. 認証装置はサプリカントに EAP 要求を送信し、サプリカントの ID を要求します。
3. サプリカントは認証装置を介して認証サーバー (Juniper Mist Access Assurance クラウド) に EAP 応答を送信します。
4. 認証サーバーは、証明書を含む「Server Hello」メッセージでクライアントデバイスに応答します。
5. サプリカントはサーバー証明書を検証します。つまり、サプリカントはサーバー証明書が信頼できる CA によって署名されているかどうかを確認します。
6. サプリカントは認証装置を介して「Client Hello」メッセージを送信し、クライアント証明書を Juniper Mist Access Assurance サービスに提示します。
7. Juniper Mist Access Assurance は、クライアント証明書が信頼できる CA によって署名されているかどうかを検証します。
8. Juniper Mist Access Assurance は、設定されたアイデンティティ プロバイダー (IdP) ソースを検索し、IdP に接続してユーザーの名前といくつかの基本属性を確認します。
9. Juniper Mist Access Assurance はポリシー検索を実行し、ロールと権限ベースのアクセスをクライアント デバイスに適用します。
10. Juniper Mist Access Assurance は、VLAN と割り当てられたロールに関する情報を認証装置に送信し、認証装置がサプリカントを適切なネットワークに割り当てることができるようにします。
11. 認証装置は EAP 成功メッセージを送信し、サプリカントにアクセスを提供します。



EAP-TTLS/PAP 認証フロー

1. 認証装置 (AP など) がセッション要求を開始するか、サプリカント (ワイヤレス クライアント デバイス) が認証装置にセッション開始要求を送信します。
2. 認証装置は、識別情報を要求する EAP 要求をサプリカントに送信します。
3. サプリカントは、EAP 応答を認証サーバー (例: Juniper Mist Access Assurance クラウド) に送信します。
4. 認証サーバーは、証明書を含む「Server Hello」メッセージでクライアント デバイスに応答します。サーバーは、認証装置を介してメッセージを送信します。
5. サプリカントは、サーバー証明書を検証します。つまり、サプリカントは、サーバー証明書が信頼できる CA によって署名されているかどうかを確認します。この検証により、暗号化された TLS トンネルが設定されます。
6. サプリカントは、ユーザー名やパスワードなどのアカウント資格情報を TLS トンネル経由でサーバーに送信します。サプリカントは、情報を Lightweight Directory Access Protocol over SSL (LDAPS) または OAuth (HTTPS) で暗号化します。
7. Juniper Mist Access Assurance は、設定された ID プロバイダ ソースに対して検索を実行し、ユーザー名といくつかの基本属性を検索します。
8. Juniper Mist Access Assurance はポリシー検索を実行し、ロールと権限ベースのアクセスをクライアント デバイスに適用します。
9. Juniper Mist Access Assurance は、VLAN と割り当てられたロールに関する情報を認証装置に送信し、認証装置がサプリカントを適切なネットワークに割り当てることができるようにします。
10. 認証装置は EAP 成功メッセージを送信し、サプリカントにアクセスを提供します。



THANK YOU

JUNIPER NETWORKS | Driven by Experience™