



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

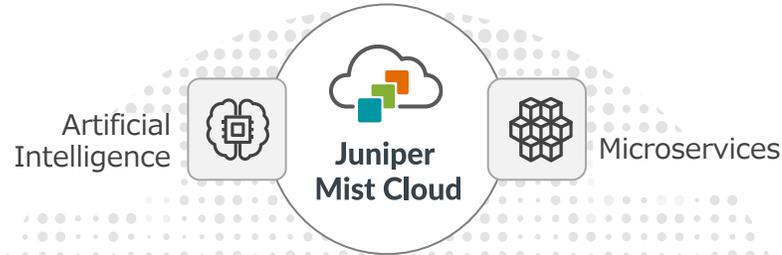
JUNIPER
NETWORKS

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



AI-Driven Cloud Services

仮想
ネットワーク
アシスタント

Marvis

- AIを活用した問題解決
- 会話型インターフェース



Marvis Actions

- プロアクティブな洞察と提案
- 包括的なネットワークの可視化



Premium Analytics



Wi-Fi Assurance



User Engagement



Asset Tracking



IoT Assurance



Access Assurance



Wired Assurance



WAN Assurance

Wireless Infrastructure



Mist Edge



AP12



AP24



AP33



AP34



AP43



AP45



AP63/64
(outdoor)



BT11 (BLE)

Wired Infrastructure



EX4600/4650 /9200



EX4300



EX4400 & -24X



QFX
5110/5120/10K



EX4100 &
EX4100-F



EX2300

EX3400

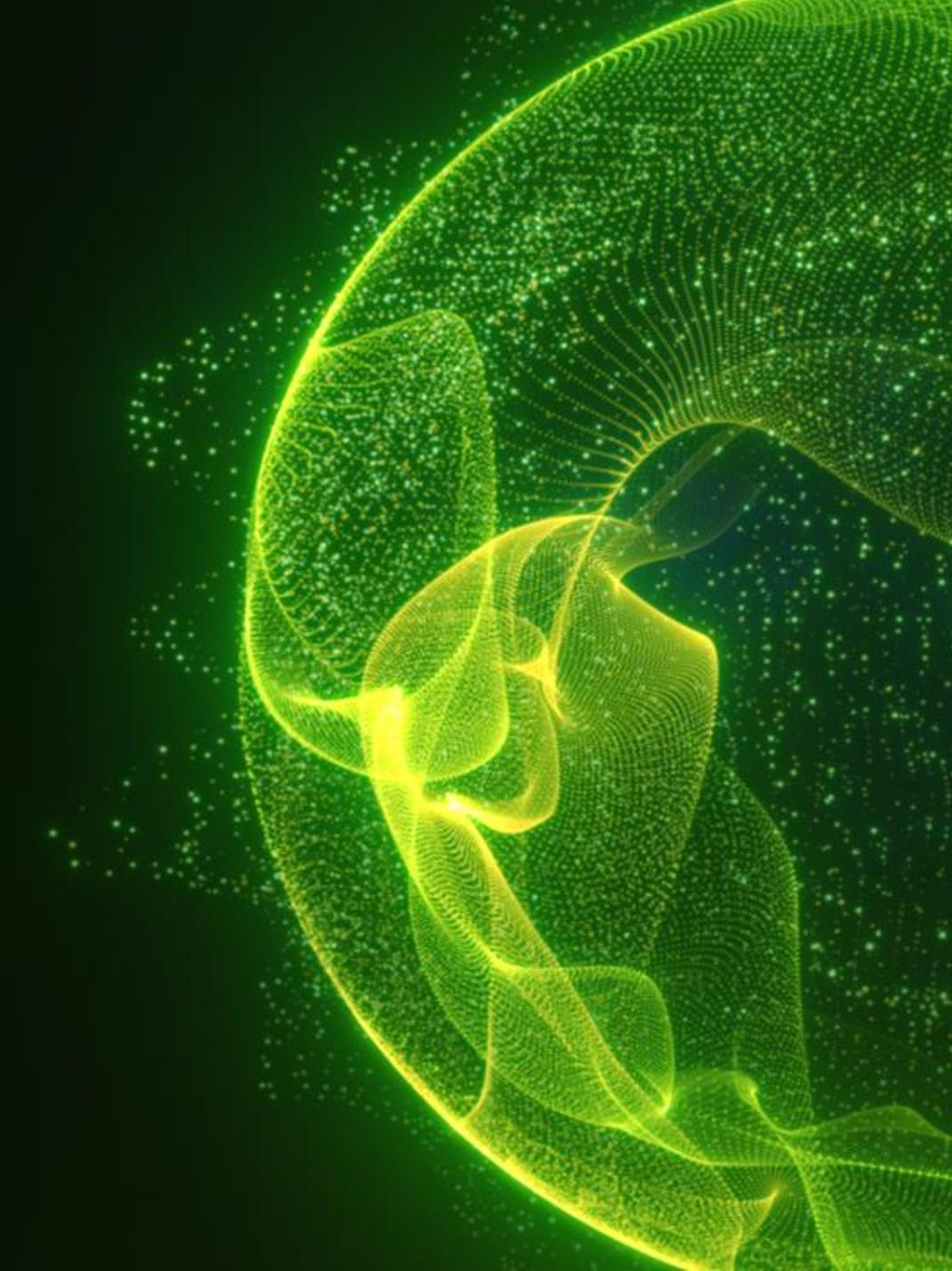
WAN Infrastructure



SRX



Session Smart
Routers



Access Assurance / IoT Assurance 購入ガイド



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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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



An abstract graphic on the left side of the slide, composed of numerous small, glowing green and yellow particles that form a complex, organic, and somewhat circular structure. The particles are arranged in a way that suggests a network or a dynamic system, with some areas appearing more dense and brighter than others. The overall effect is a sense of movement and energy, set against a dark background.

Access Assurance

NAC に求められる要素



認証・認可 (AAA)



クライアント プロファイリング



ポスチャ管理



ゼロトラスト ネットワークアクセス



クライアント オンボーディング

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

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

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

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

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・トラブルシューティング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

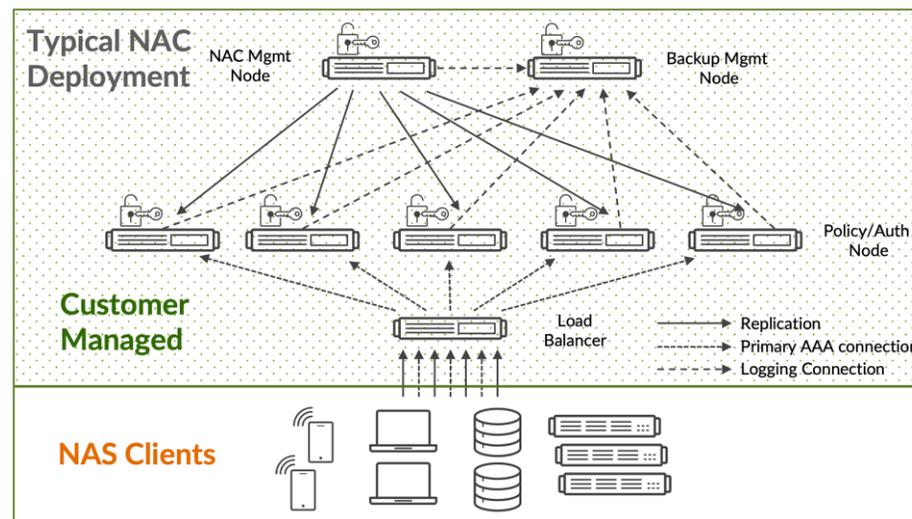
- ログが統合管理されておらず分散
- エンドツーエンドの不可視性
- 不十分なインサイト

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



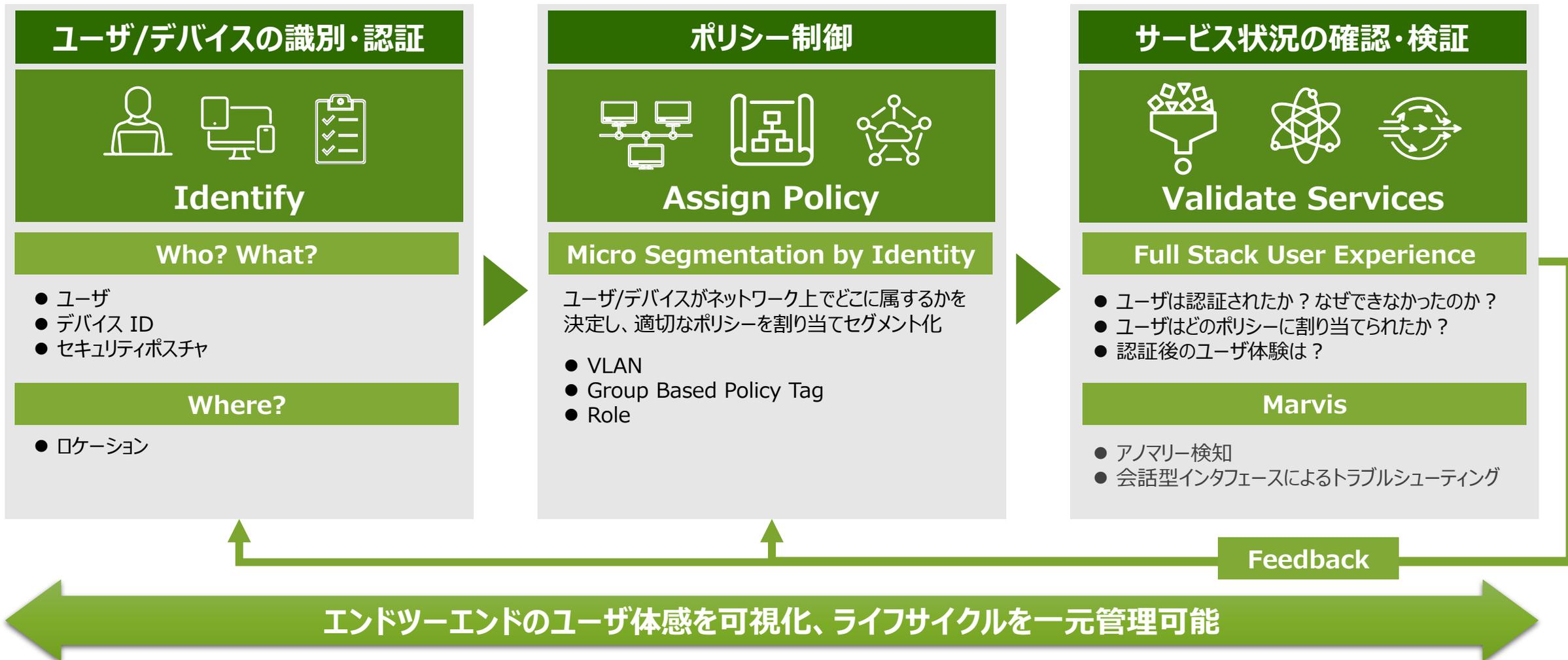
AI を活用し最適化された Day 0/1/2 のオペレーション



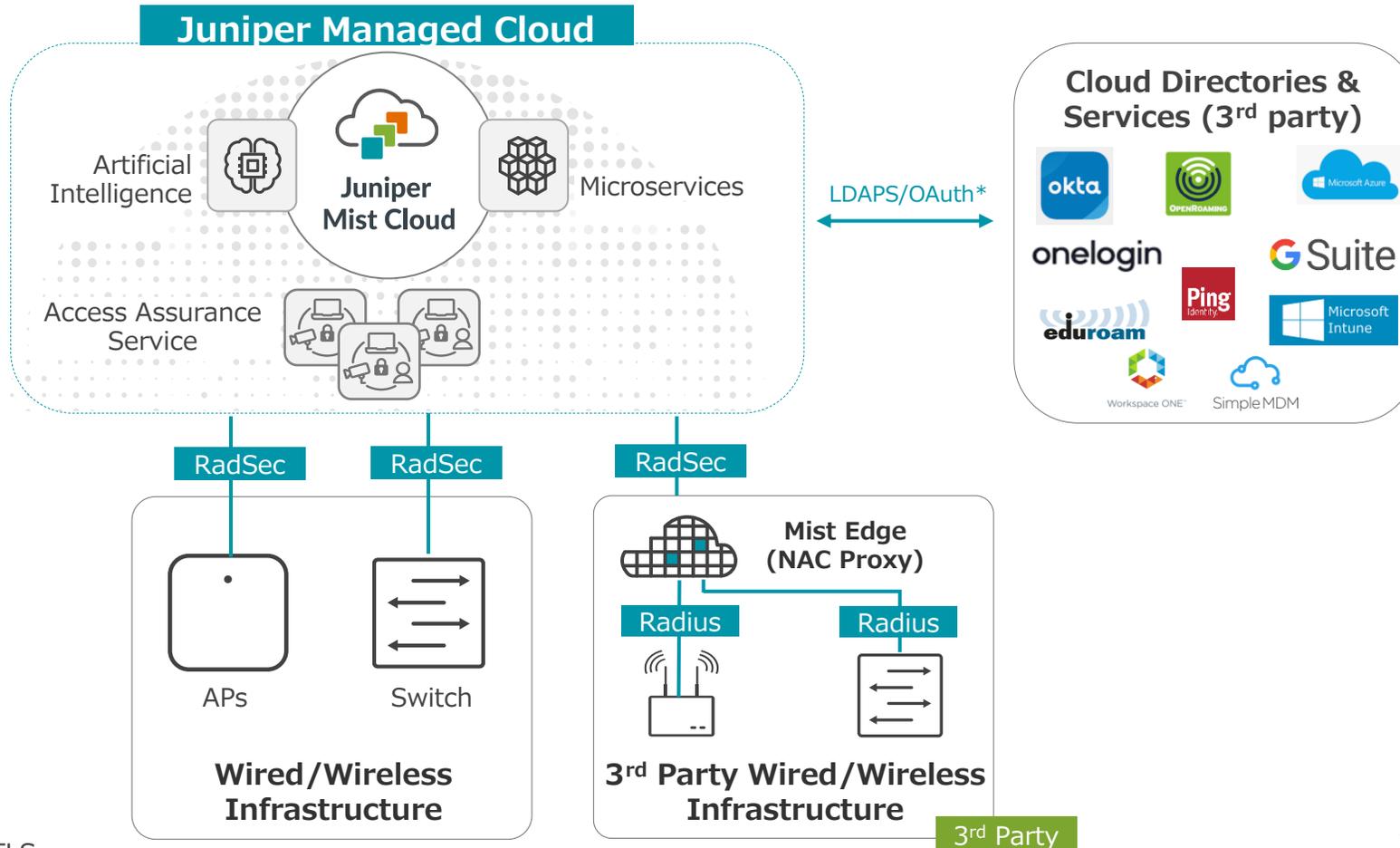
Mist Access Assurance

Mist NAC できること

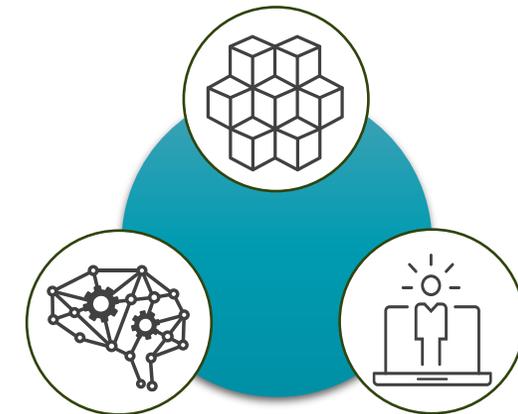
AIOps Powered by Mist



Mist Access Assurance



Micro-Services based Cloud NAC Offering



- ✓ EAP-TLS
- ✓ EPA-TTLS(PAP)
- ✓ MAB



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
を合わせてご確認ください



Mist AP & EX/QFX

Mist AP

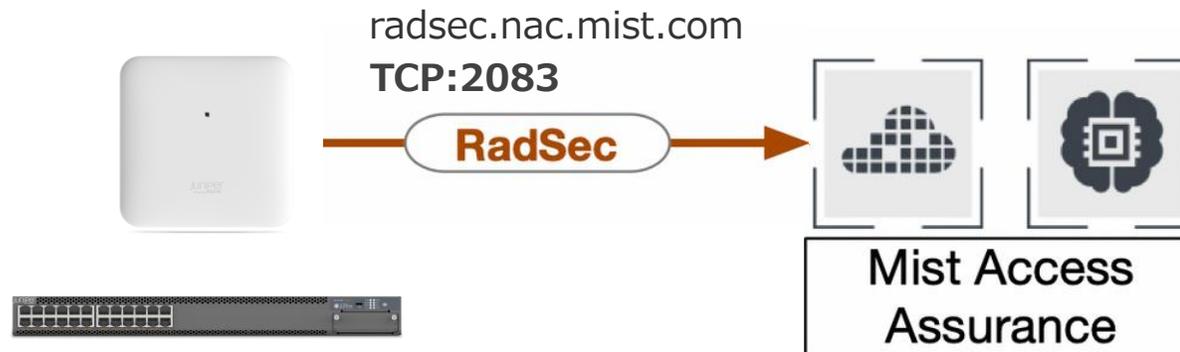
- 0.6.x 以降

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

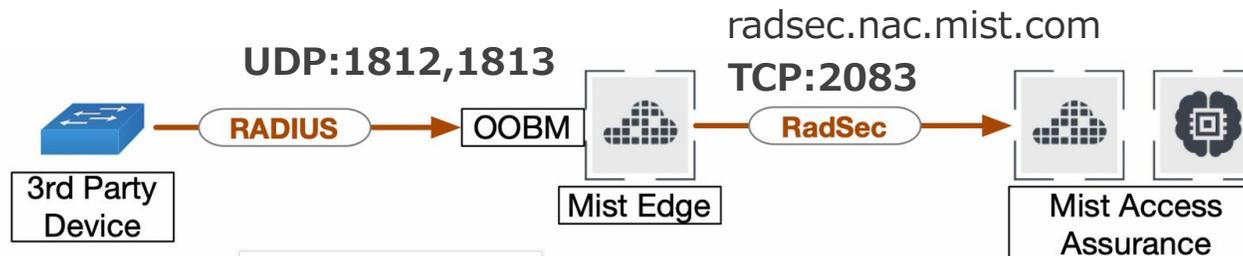
- radsec.nac.mist.com (TCP:2083)



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

The screenshot shows the 'Add Client' interface for Mist Edge Clusters. It includes a 'Radius Proxy' section with 'Enabled' selected and 'Mist NAC Proxy' as the type. Below is a table for 'RADIUS Clients' with columns for IP, Vendor, and Site. The table is currently empty with the text 'No clients defined'.

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

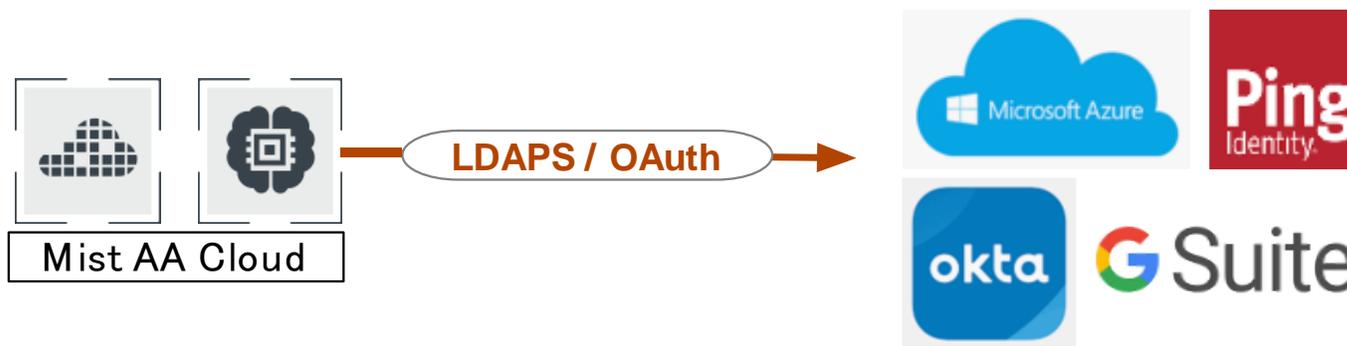
- ユーザ・アカウントのステータスとグループ・メンバーシップの検索 (EAP-TLS ではオプション)
- 証明書の代わりに認証情報を使用したユーザーログイン (EAP-TTLS のみサポート)

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

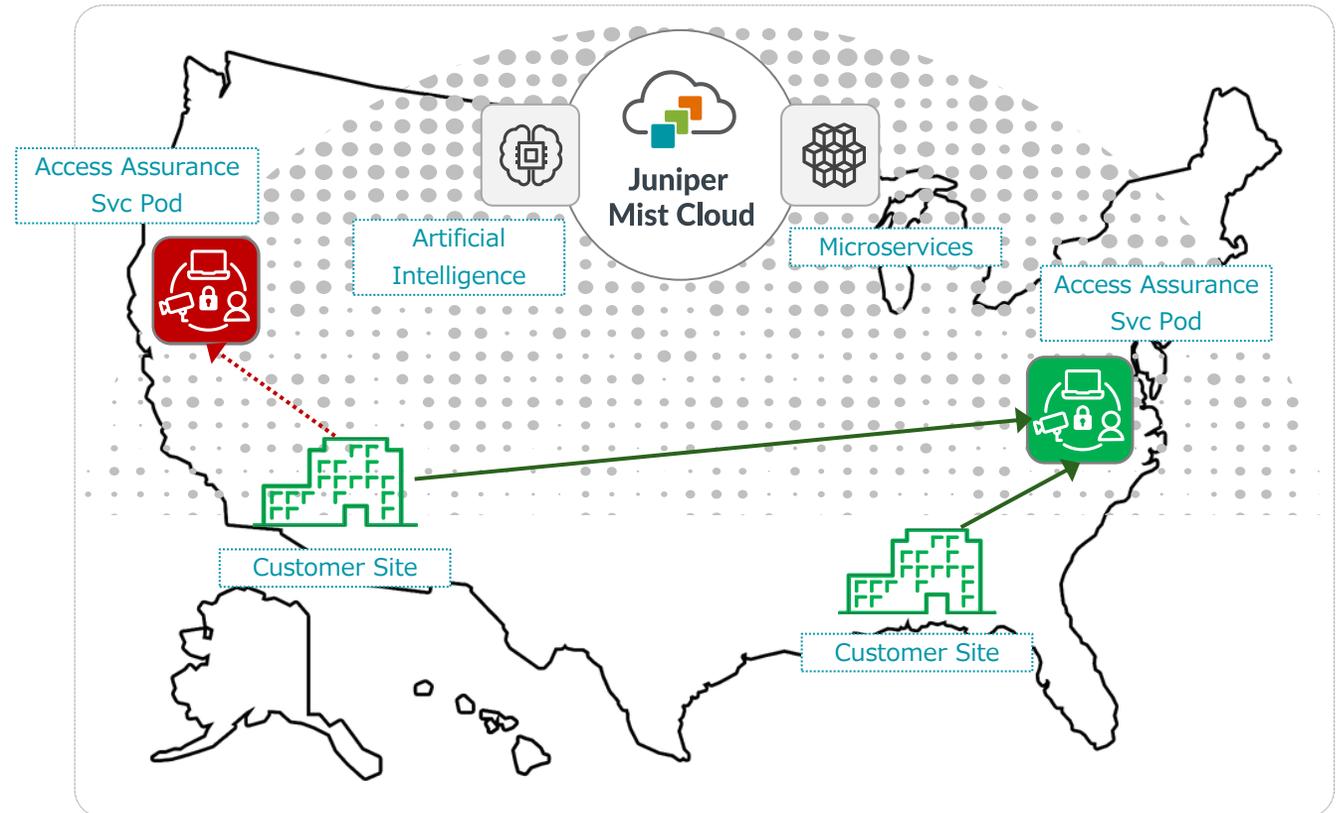
	Azure	Okta	Custom
LDAPS	○	○	○
OAuth	○	○	-



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ブ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

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

STEP 02

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

STEP 03

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

STEP 04

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

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

SSID

Security

WPA2 > Enterprise(802.1X)

Authentication Servers

Mist Auth

VLAN

- Untagged
- Tagged
- Pool
- Dynamic (VLAN Type)

Site Assign

WLANs(Site)

SSID

SSID

Security

WPA2 > Enterprise(802.1X)

Authentication Servers

Mist Auth

VLAN

- Untagged
- Tagged
- Pool
- Dynamic (VLAN Type)

Wireless - AP 設定

WLAN Templates: Create Template

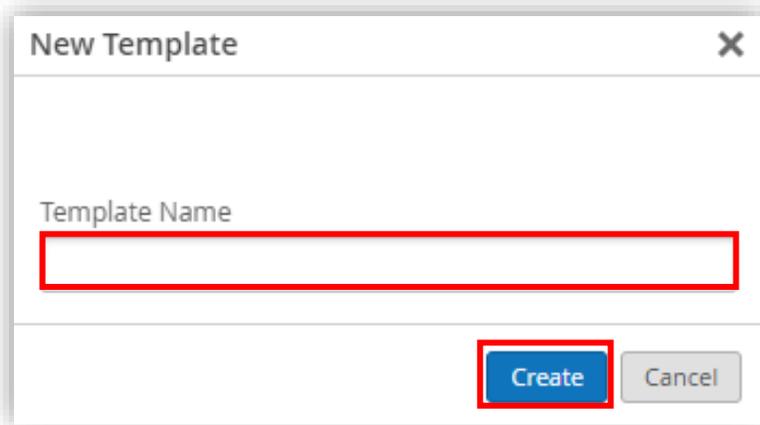
1. [Organization] から [WLAN Templates] をクリックします
2. [Create Template] をクリックします

The screenshot shows the Juniper Mist management console. On the left is a dark blue navigation sidebar with icons and labels for various sections: Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is divided into columns for Admin, Access, WAN, Wired, and Wireless. The 'Wireless' column contains 'WLAN Templates', which is highlighted with a red box. Below this, a modal window titled 'WLAN Templates' is open. It features a search filter, a table with columns for Name, Applied To Org, Sites, Site Groups, Exceptions, and WLANs, and a 'Create Template' button in the top right corner, also highlighted with a red box. The table content is empty, displaying the message 'This org has no templates'.

Wireless - AP 設定

WLAN Templates: Add WLAN

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

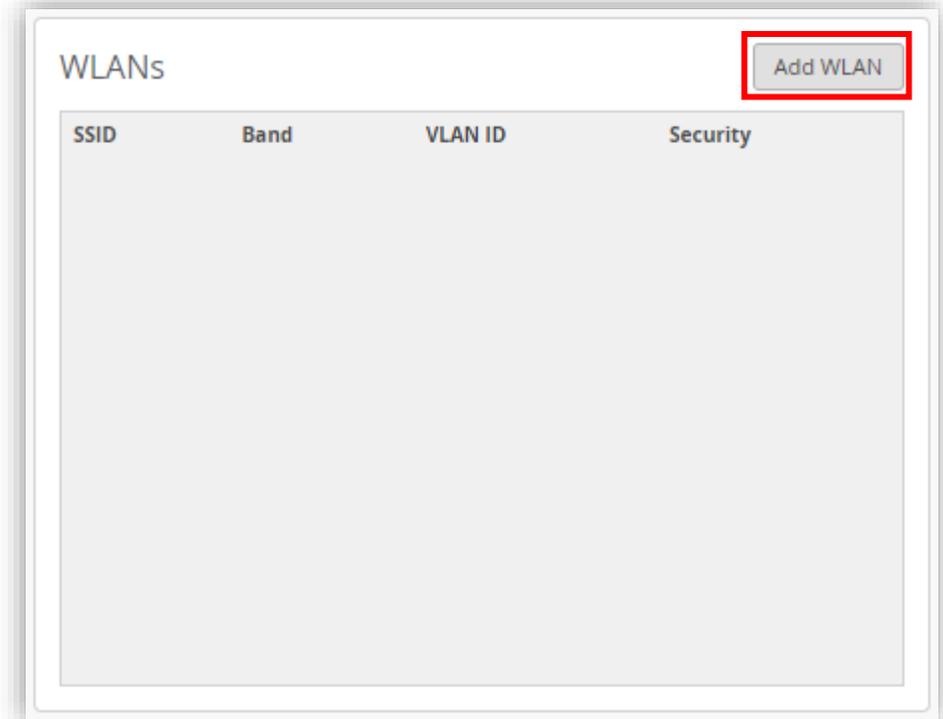


New Template

Template Name

Create Cancel

4. [Add WLAN] をクリックします



WLANs

Add WLAN

SSID	Band	VLAN ID	Security
------	------	---------	----------

Wireless - AP 設定

WLAN Templates: SSID / Security

5. [SSID] を設定します

SSID

WLAN-AA

WiFi SLE

Exclude this WLAN from WiFi SLEs (except AP Health SLE)

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

Security

Security Type

WPA3 WPA2 Legacy OWE Open Access

Enterprise (802.1X) Personal (PSK)

MAC address authentication by RADIUS lookup

Use EAPOL v1 (for legacy clients)

Enable EAP-Reauth

Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Fast Roaming

Default

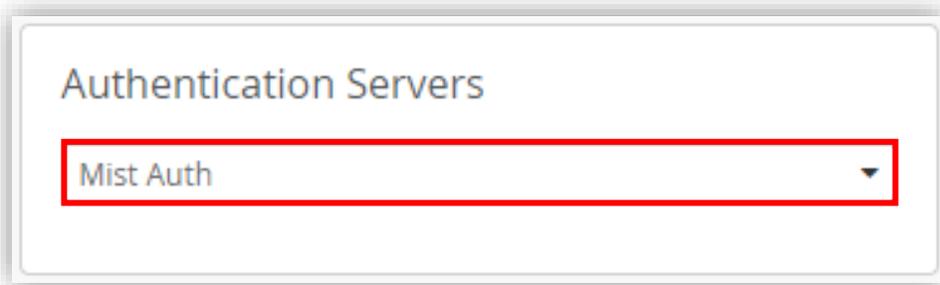
Opportunistic Key Caching (OKC)

.11r

Wireless - AP 設定

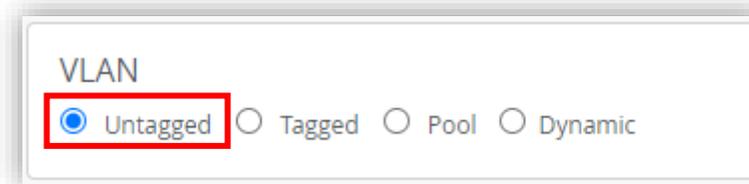
WLAN Templates: Authentication Servers / Untagged VLAN

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



A screenshot of a web interface showing a dropdown menu titled "Authentication Servers". The menu is open, and "Mist Auth" is selected and highlighted with a red rectangular border. A small downward arrow is visible on the right side of the dropdown box.

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



A screenshot of a web interface showing a configuration section titled "VLAN". Below the title are four radio button options: "Untagged", "Tagged", "Pool", and "Dynamic". The "Untagged" option is selected, indicated by a blue dot inside the radio button, and is highlighted with a red rectangular border.

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

VLAN

Untagged Tagged Pool Dynamic

VLAN ID ⓘ

100

(1 - 4094)

サイト変数も利用できます

8.(c) Pool VLAN

[Pool] を選択し、[VLAN ID(s)] リストを設定します

VLAN

Untagged Tagged Pool Dynamic

VLAN ID(s) ⓘ

{{POOL_VLAN}}

(1 - 4094)

サイト変数も利用できます
コンマ区切りで複数設定、
- でレンジ指定ができます
例) 201-210,4000

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

VLAN

Untagged Tagged Pool Dynamic

Static VLAN ID(s) ?

999
(1 - 4094)

VLAN Type **Named** ?

Dynamic VLAN ID(s)	Interface Name(s)
120	VLAN120
121	VLAN121
122	VLAN122
123	VLAN123

Add Rows

VLAN

Untagged Tagged Pool Dynamic

Static VLAN ID(s) ?

999
(1 - 4094)

VLAN Type **VLAN ID** ?

Dynamic VLAN ID(s)
120
121
122
123

Add Rows

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

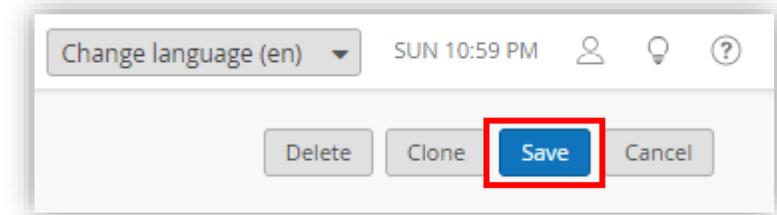
Wireless - AP 設定

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

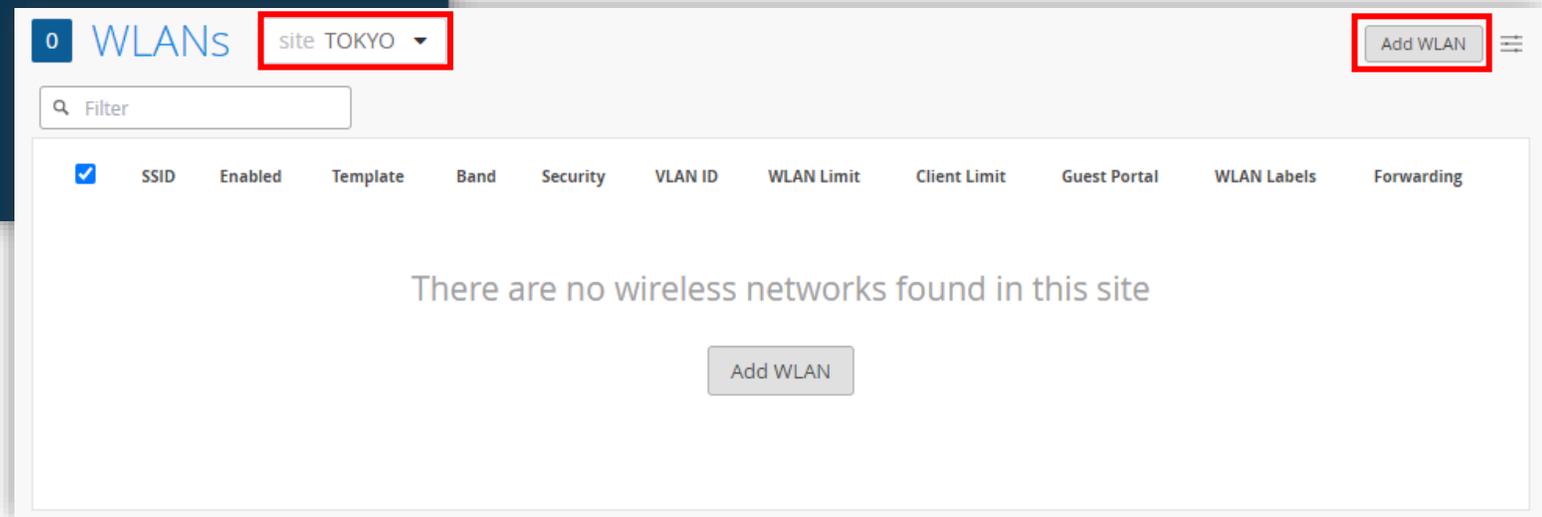
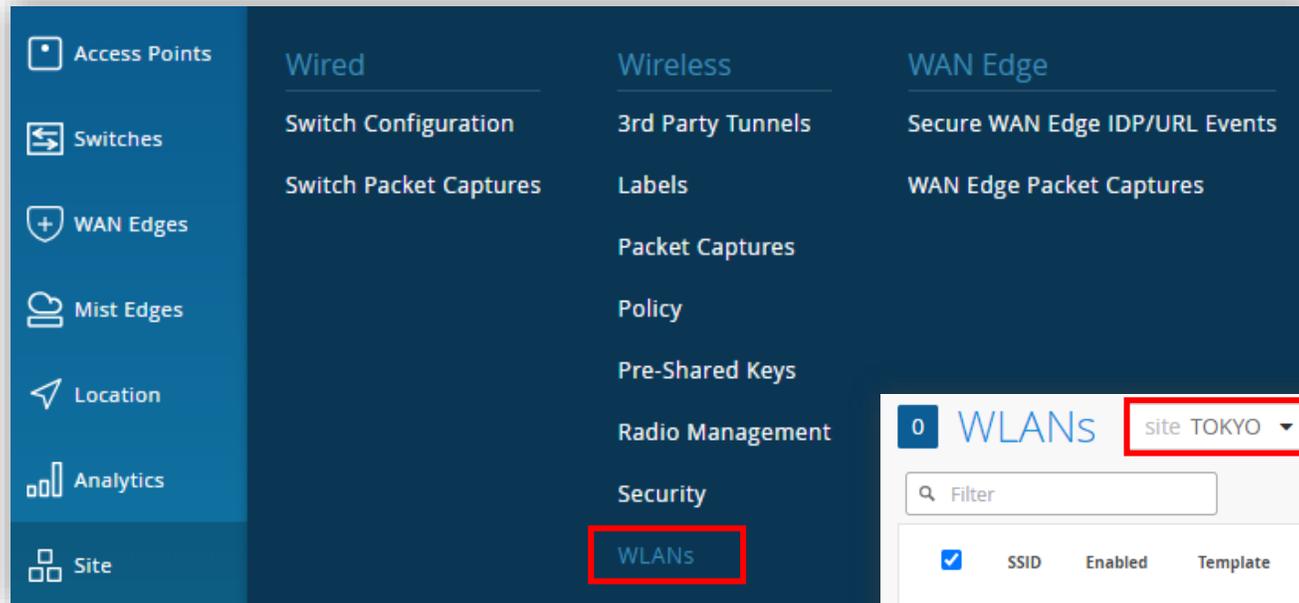


Wireless - AP 設定

WLANs: Add WLAN

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

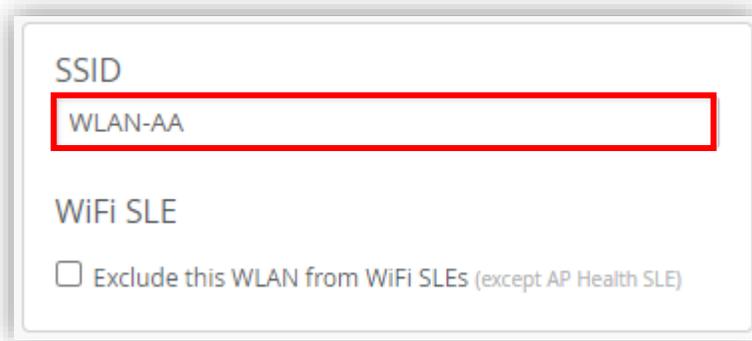
WLAN Template を使用しない場合、
Site > WLANs より設定します



Wireless - AP 設定

WLANs: SSID / Security

3. [SSID] を設定します



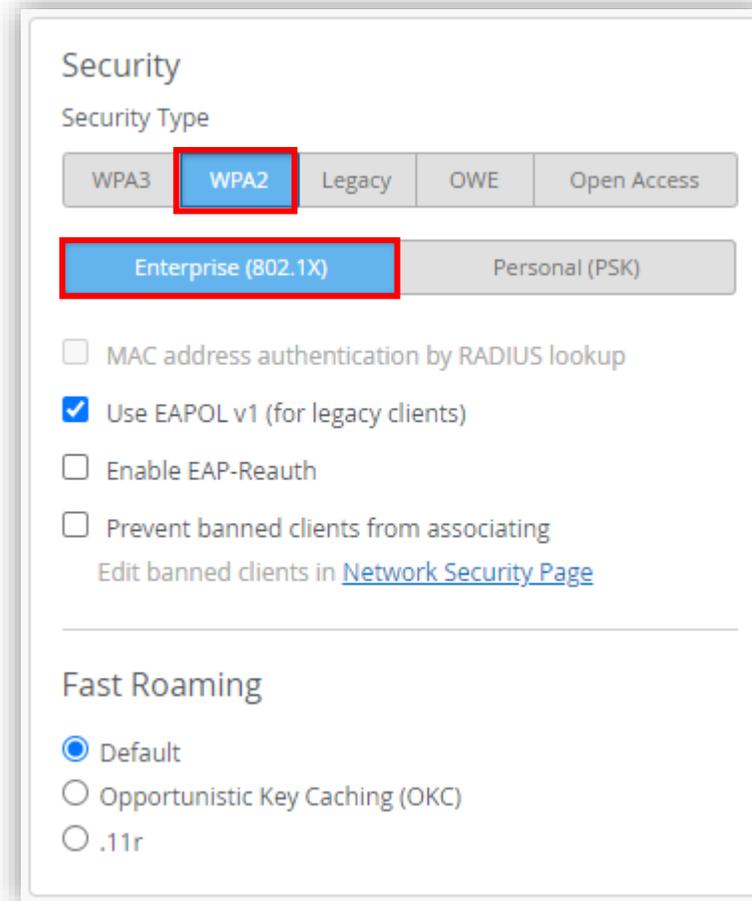
SSID

WLAN-AA

WiFi SLE

Exclude this WLAN from WiFi SLEs (except AP Health SLE)

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



Security

Security Type

WPA3 WPA2 Legacy OWE Open Access

Enterprise (802.1X) Personal (PSK)

MAC address authentication by RADIUS lookup

Use EAPOL v1 (for legacy clients)

Enable EAP-Reauth

Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Fast Roaming

Default

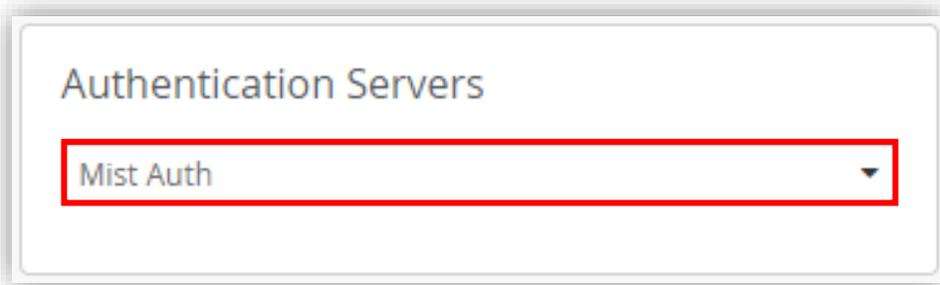
Opportunistic Key Caching (OKC)

.11r

Wireless - AP 設定

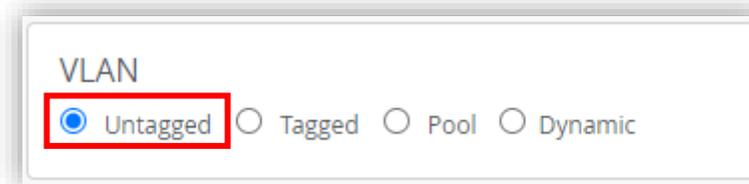
WLANs: Authentication Servers / Untagged VLAN

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



A screenshot of a web interface showing a dropdown menu titled "Authentication Servers". The menu is open, and "Mist Auth" is selected and highlighted with a red rectangular border. A small downward arrow is visible on the right side of the dropdown box.

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



A screenshot of a web interface showing the "VLAN" configuration options. The "Untagged" radio button is selected and highlighted with a red rectangular border. Other options include "Tagged", "Pool", and "Dynamic", each with an unselected radio button.

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

VLAN

Untagged Tagged Pool Dynamic

VLAN ID ⓘ

100

(1 - 4094)

サイト変数も利用できます

6.(c) Pool VLAN

[Pool] を選択し、[VLAN ID(s)] リストを設定します

VLAN

Untagged Tagged Pool Dynamic

VLAN ID(s) ⓘ

{{POOL_VLAN}}

(1 - 4094)

サイト変数も利用できます
コンマ区切りで複数設定、
- でレンジ指定ができます
例) 201-210,4000

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

VLAN

Untagged Tagged Pool Dynamic

Static VLAN ID(s) ?

999
(1 - 4094)

VLAN Type **Named** ?

Dynamic VLAN ID(s)	Interface Name(s)
120	VLAN120
121	VLAN121
122	VLAN122
123	VLAN123

Add Rows

VLAN

Untagged Tagged Pool Dynamic

Static VLAN ID(s) ?

999
(1 - 4094)

VLAN Type **VLAN ID** ?

Dynamic VLAN ID(s)
120
121
122
123

Add Rows

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



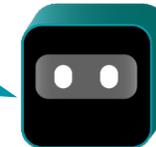


Wired - Switch 設定

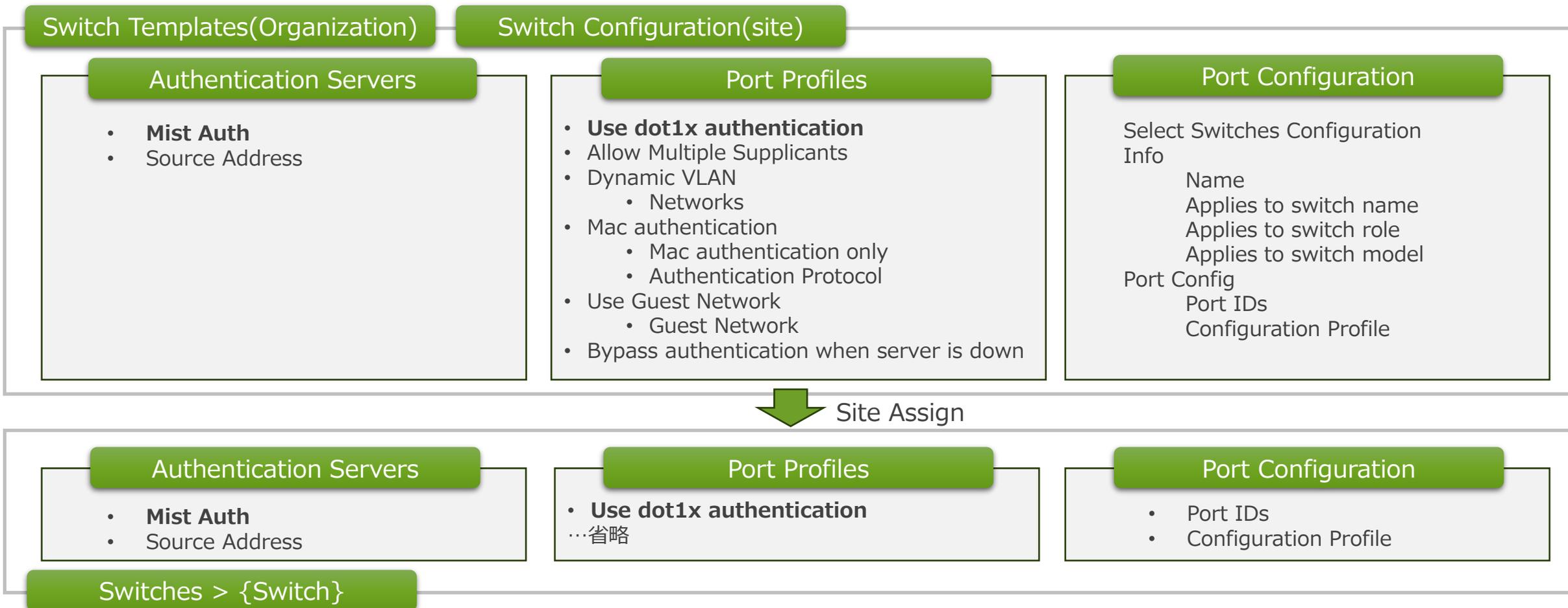
Wired - Switch 設定

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



Wired - Switch 設定

Switch Templates: Create Template

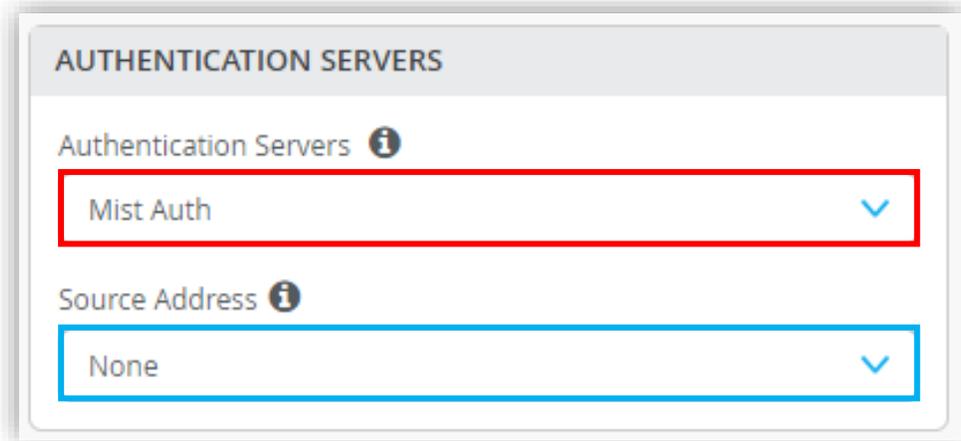
1. [Organization] から、[Switch Templates] をクリックします
2. [Create Template] をクリック、[Template Name] にテンプレート名を設定、[Create] をクリックします

The screenshot shows the Juniper Mist management console interface. On the left is a navigation sidebar with icons for Swatches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is divided into several tabs: Admin, Access, WAN, Wired, and Wireless. The 'Wired' tab is selected, and within it, the 'Switch Templates' option is highlighted with a red box. Below the navigation is a 'Switch Templates' panel showing '0 Templates' and a table with columns 'TEMPLATE', 'SITES', and 'SWITCHES'. A message states 'There are no Switch Templates in this org'. To the right of the table are two buttons: 'Import Template' and 'Create Template', with the latter highlighted by a red box. In the bottom right corner, a 'NEW TEMPLATE' dialog box is open, featuring a 'Template Name' input field containing the text 'st', which is also highlighted by a red box. At the bottom of the dialog are 'Create' and 'Cancel' buttons, with 'Create' highlighted by a red box.

Wired - Switch 設定

Switch Templates: Authentication Servers / Port Profiles

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



AUTHENTICATION SERVERS

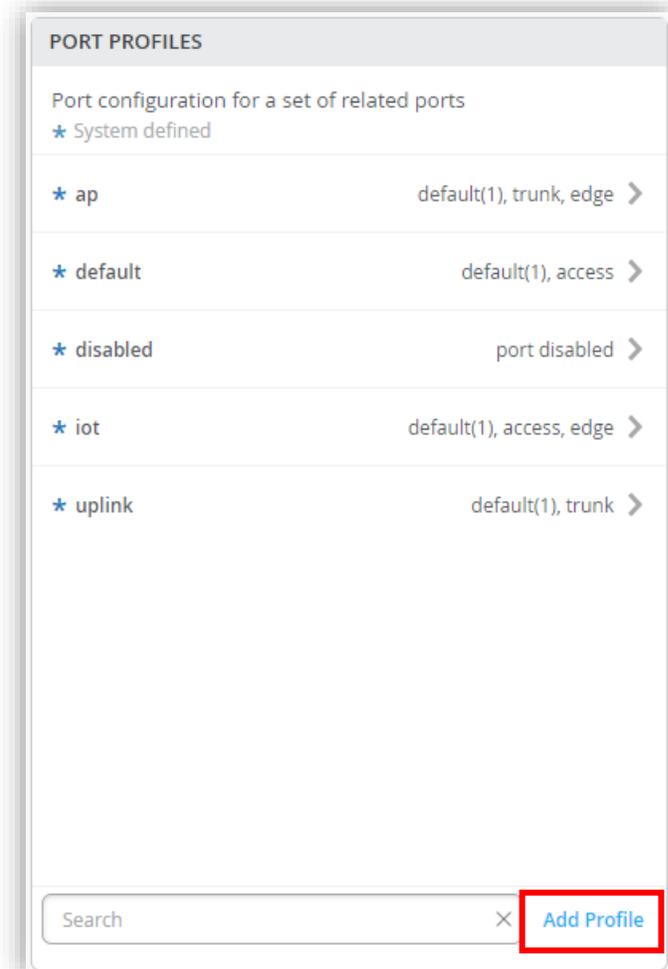
Authentication Servers ⓘ

Mist Auth ▼

Source Address ⓘ

None ▼

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



PORT PROFILES

Port configuration for a set of related ports

★ System defined

★ ap	default(1), trunk, edge >
★ default	default(1), access >
★ disabled	port disabled >
★ iot	default(1), access, edge >
★ uplink	default(1), trunk >

Search × **Add Profile**

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

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

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

Allow Multiple Supplicants

Dynamic VLAN ?

Networks

Mac authentication

Use Guest Network

Guest Network

default 1 ▾

Bypass authentication when server is down

[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ブ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

Allow Multiple Suplicants

Dynamic VLAN

Networks

+

Mac authentication

Mac authentication only

Authentication Protocol

None

Use Guest Network

Guest Network

default 1

Bypass authentication when server is down

[Use dot1x authentication] をチェックします

[Allow Multiple Suplicants] をチェックすると、同一ポートで複数サブ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)
サブ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

The screenshot shows the 'Select Switches Configuration' interface. On the left, there is a list of switch templates under the 'default' category, with 'all remaining switches' listed. On the right, the 'Add Rule' button is highlighted with a red box. Below it, the 'Info' tab is selected and highlighted with a red box. The configuration for the rule is as follows:

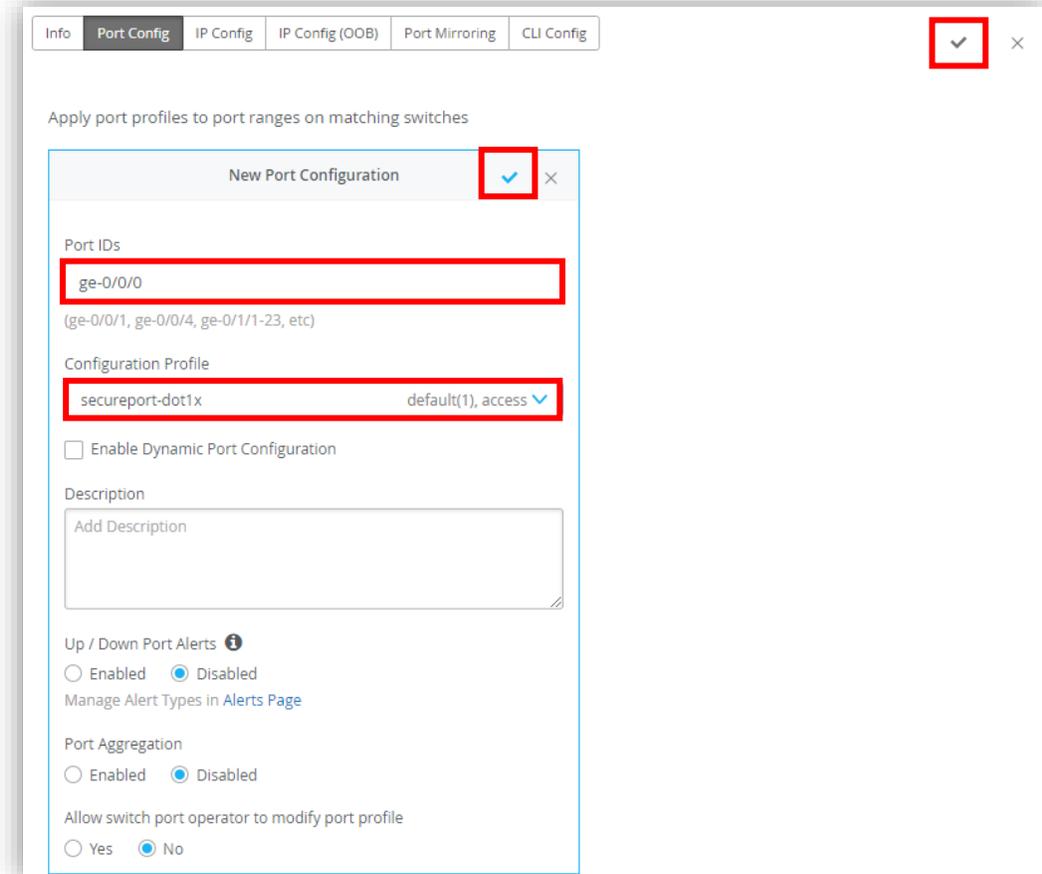
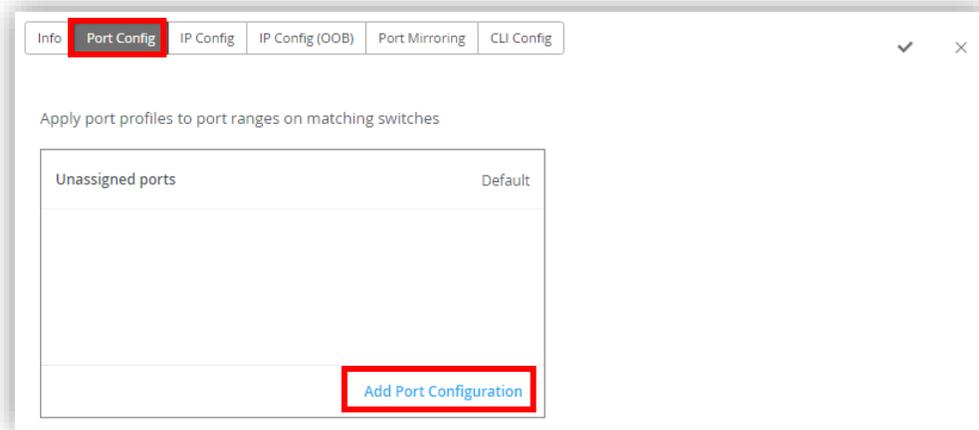
- Name:** port-config
- Applies to switch name:** (unchecked)
- Offset:** 0
- Applies to switch role:** (unchecked)
- Applies to switch model:** (checked)
- Role:** Select or create a role (dropdown menu showing EX4100-48P)
- Model:** EX4100-48P

Additional text below the model selection: letters, numbers, _ or -

Wired - Switch 設定

Switch Templates: Select Switches Configuration > Port Configuration

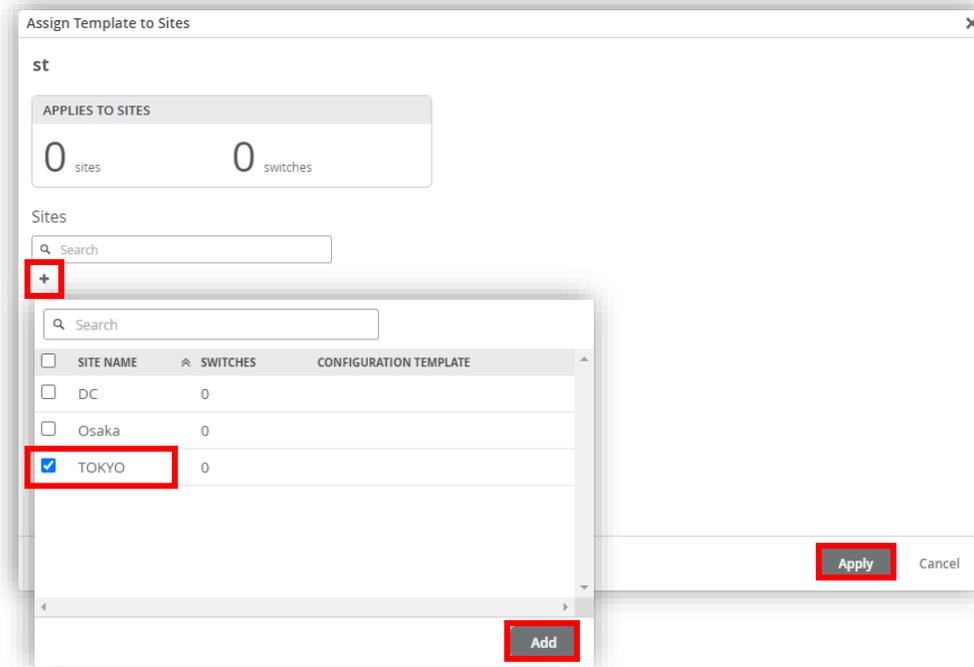
7. [Port Config] タブをクリック、[Add Port Configuration] をクリックします
[Port IDs] で適用するインタフェースを指定、[Configuration Profile] に作成したプロファイルを選択します
[✓] をクリックして、Port Configuration 設定を完了、[✓] で Rule 設定を完了します



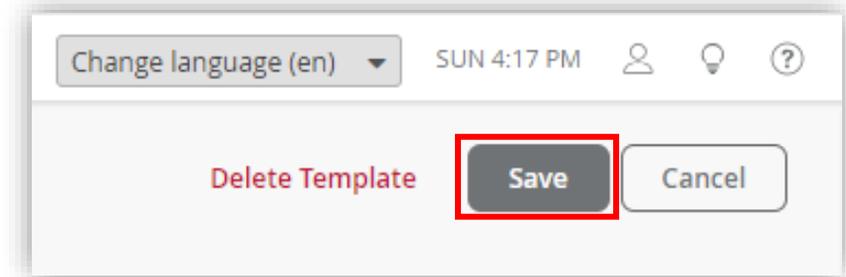
Wired - Switch 設定

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

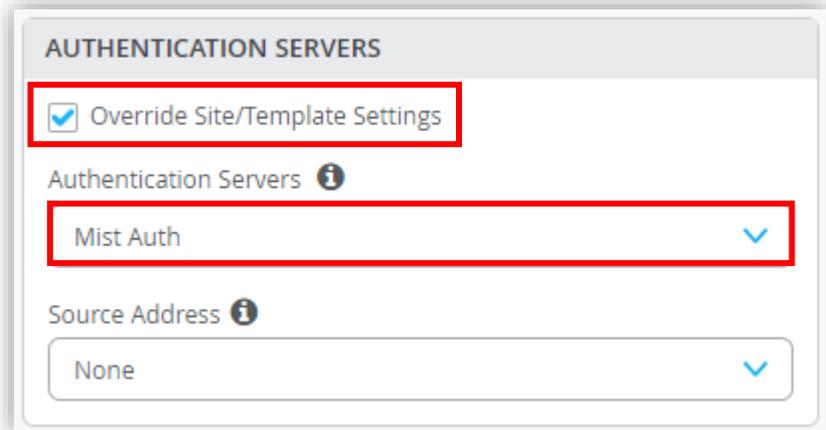
The screenshot displays the Juniper Mist management interface. The left sidebar contains navigation options: Monitor, Marvis™, Clients, Access Points, **Switches** (highlighted), WAN Edges, Mist Edges, and Location. The main header shows 'ORGANIZATION' and 'Switches' for the 'site main_site'. Summary statistics include 2 Cloud Connected Switches, 0 Discovered Switches, 3 Wired Clients, and 0 W Total Allocated AP Power. Below these are six green progress bars for 100% compliance in various areas: Switch-AP Affinity, PoE Compliance, VLANs, Version Compliance, Switch Uptime, and Config Success. A table below lists switch details:

	Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Insights
<input type="checkbox"/>	Connected	ex4300	100.123.105.1	EX4300-48T	1	2	2	Switch Insights
<input type="checkbox"/>	Connected	vEX	100.123.251.0	VEX9214	0	0	1	Switch Insights

Wired - Switch 設定

Per Switch Configuration

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



AUTHENTICATION SERVERS

Override Site/Template Settings

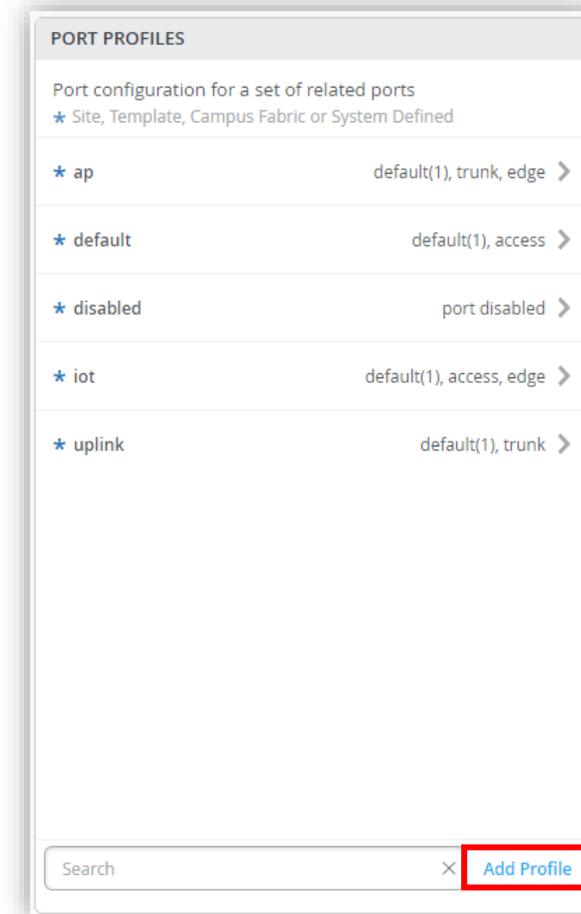
Authentication Servers ⓘ

Mist Auth ▼

Source Address ⓘ

None ▼

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



PORT PROFILES

Port configuration for a set of related ports
★ Site, Template, Campus Fabric or System Defined

* ap	default(1), trunk, edge >
* default	default(1), access >
* disabled	port disabled >
* iot	default(1), access, edge >
* uplink	default(1), trunk >

Search × **Add Profile**

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

New Port Profile

Name
secureport-dot1x

Port Enabled
 Enabled Disabled

Description
Add Description

Mode
 Trunk Access

Port Network (Untagged/Native VLAN)
default 1

VoIP Network
None

Use dot1x authentication

Allow Multiple Supplicants

Dynamic VLAN

Mac authentication

Use Guest Network

Bypass authentication when server is down

[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

New Port Profile

Name
secureport-dot1x

Port Enabled
 Enabled Disabled

Description
Add Description

Mode
 Trunk Access

Port Network (Untagged/Native VLAN)
default 1

VoIP Network
None

Use dot1x authentication

Allow Multiple Supplicants

Dynamic VLAN

Mac authentication

Mac authentication only

Authentication Protocol
None

Use Guest Network

Bypass authentication when server is down

[Name] にプロファイル名を設定します

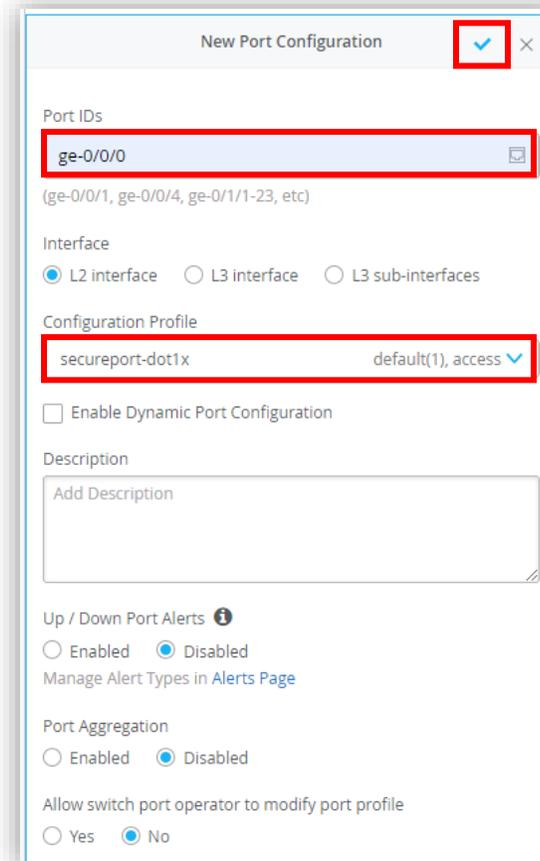
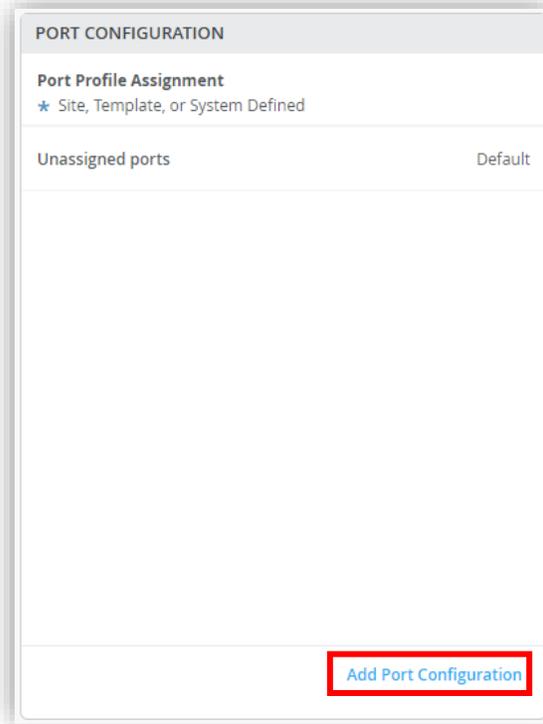
[Use dot1x authentication] をチェックします

[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



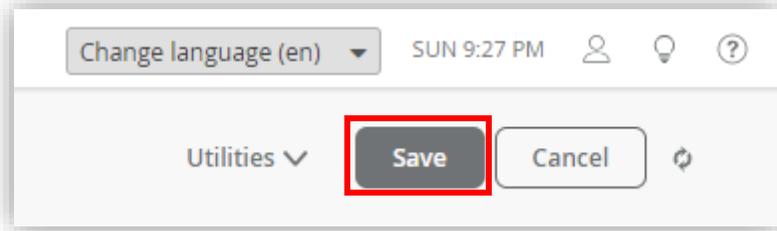
[Port IDs] で適用するインタフェースを指定します

[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



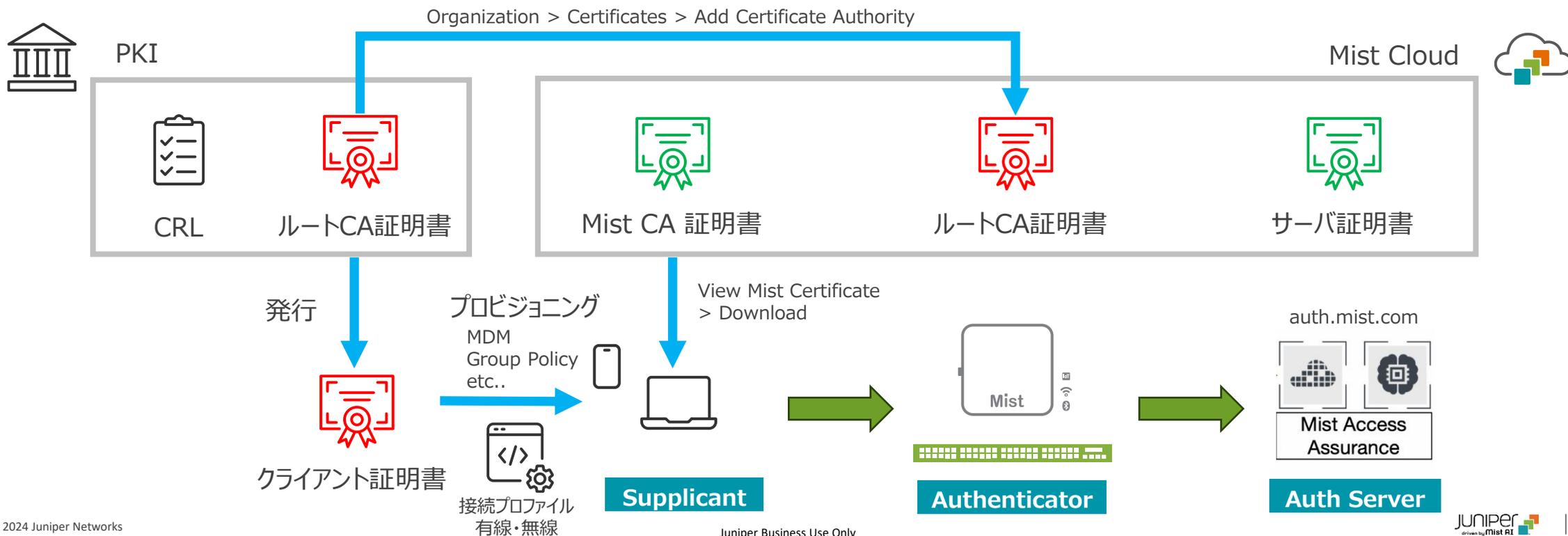


Certificate

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)

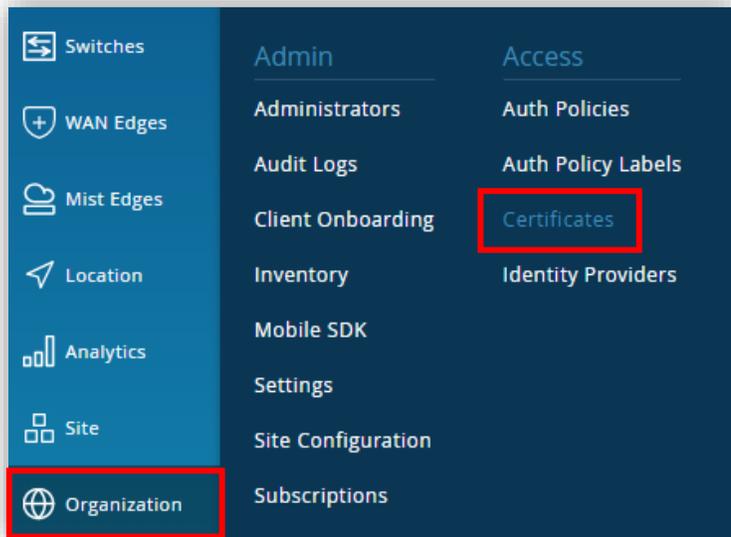
パブリック/プライベート PKI のいずれの場合も、サーバ/クライアント証明書を検証するため、正しく証明書チェーンを構成する必要があります



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

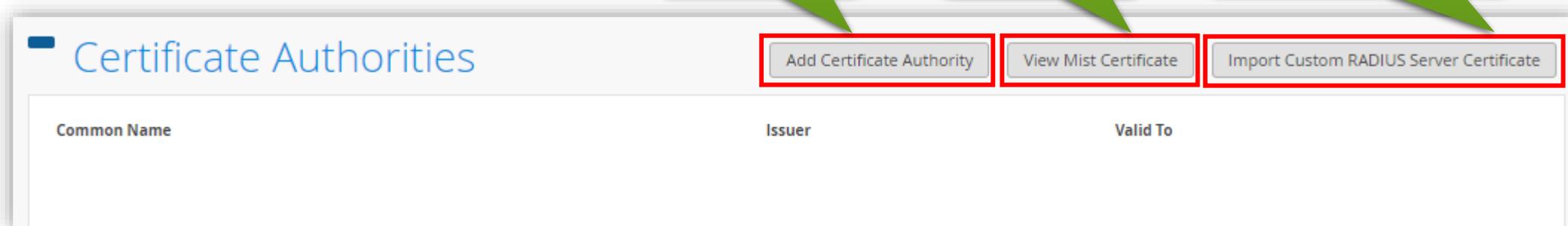
- **Import Custom RADIUS Certificate (Radius サーバ証明書のインポート)**

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

CA 証明書
の追加

Mist 証明書
の表示

Radius サーバ証明書
のインポート



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

The screenshot shows the 'Certificate Authorities' management page. At the top, there are three buttons: 'Add Certificate Authority', 'View Mist Certificate' (highlighted with a red box), and 'Import Custom RADIUS Server Certificate'. Below these is a table with columns for 'Common Name', 'Issuer', and 'Valid To'. A 'View Certificate' dialog box is open, displaying the following information:

View Certificate

Signed Certificate

```
-----BEGIN CERTIFICATE-----
MIIF0jCCA7qgAwIBAgIBATANBgkqhkiG9w0BAQsFAADBbMQswCQYDVQQGEWJlbnVz
EN
MAsGA1UECgwETWlzdDEOMAwGA1UECwwFT3JnQ0ExLTArBgNVBAMMJGMxZWJjMjlx
LWJjODItNGU5Zi1hNzg5LTZmMWUyYzhiZGkNDAAeFw0yMTA4MzAwNzEyNDZaFw0z
MTA4MjgwNzEyNDZaMFsxCzAJBgNVBAYTAiVMTM0wCwYDVQQKQkDARnN0M0M0wDAYD
VQQLDAVPCmdDQTEtMCA1UEAwkYzFYMmYjEtYmM4Mi00ZTImlLWE3ODktNmYx
ZTJjOGJkYmQ0MlICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICgKCAgEAXj2OymE1
G01Oaxl19lVtAPvErBX3NBIRNvvaAMdlPM3iYRnD9nhkhi8zT8VannO6mg+aOT
-----
```

Properties

Common Name	c1e	4	
Valid From	08/30/2021		
Valid To	08/28/2031		
Issuer	C=US, O=Mist, OU=OrgCA, CN=c1e		4
Serial Number	01		
CRL Distribution Points	http://api.mist.com/api/v1/orgs/c1ebc2		
Subject Alternative Name	c1eb		

At the bottom of the dialog box, there is a 'Download' button (highlighted with a red box) and a 'Close' button. A yellow callout box points to the 'Download' button with the text: "[Download] をクリックして、証明書を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

Import Custom RADIUS Server Certificate

Private Key

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-256-CBC,C2B449FC86C96D51A60B4617681FBD41  
  
1sRFDj1ZFyhFEwwQxHz9fMBSK7MrGxUI1tsAnM5Qnc3n3p5HZUHQxQ+G6cZja0jk  
yWgA6j+23litOB+7twD8Zdljrx3iAXotSZu4jpBn7cbh2vQ/aoFufQnDoGz3Nc2H  
eAf47yBMmmlYQwncPuZBEIMTS1zOZY/9hrN02iITzbuupifPrd+dWbYSCCaMxlyh
```

Private Key Password

.....

Signed Certificate

```
-----BEGIN CERTIFICATE-----  
MIIFIDCCA3CgAwIBAgIIvR5Pf9UdKUwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UE  
BhMCVVMxDTALBgNVBAoTBG1pc3QxGDAWBgNVBAMMD2xhYi1jYUB0ZXN0Lm5ldD Ae  
Fw0yNDASMTUwNDQzMDBaFw0zMzA3MTEwMjE1MjM0MDA4CzAJBgNVBAYTAiVTRAw  
DgYDVQQKEwdqdW5pcGvYyMR0wGwYDVQQDDBRyYWRpdXMtdGVzdEBOZXN0Lm5ldDCC  
AilwDQYJKoZIhvcNAQEBBQADggIPADCCAgogCggIBALVPG1hqqulwzYTEu2i0Wbj  
0o38Hrj6PC+h9PAHA1gP5d5f0oBMYnanAqCkJPkMsMfXr+fgWVHtgpKETV1MqK  
u66YhQVlQ05F5eQHx2/9beLk/delUDF5+XmKztkuMup5eBu46Rf5Q08axY09G
```

Properties	
Common Name	radius-test@test.net
Valid From	09/11/2024
Valid To	07/12/2033
Issuer	C=US, O=mist, CN=lab-ca@test.net
Serial Number	56b46c3dff5474a5
Extended Key Usage	TLS Web server authentication
Subject Alternative Name	radius-test@test.net

Valid To

---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)

1 Certificate Authorities

Add Certificate Authority View Mist Certificate View Custom RADIUS Server Certificate

Common Name Valid To

Update Custom RADIUS Server Certificate

Private Key

Private Key Password

Signed Certificate

Properties

Common Name	radius-test@test.net
Valid From	09/11/2024
Valid To	07/12/2033
Issuer	C=US, O=mist, CN=lab-ca@test.net
Serial Number	56b46c3dff5474a5
Extended Key Usage	TLS Web server authentication
Subject Alternative Name	radius-test@test.net

Delete Close

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

Identity Providers

Entra ID(Azure AD)/OAuth Overview

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



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



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

アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。
Mist AA IdP ✓

サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?
 この組織ディレクトリのみに含まれるアカウント (のみ - シングル テナント)
 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)
 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント) と個人用の Microsoft アカウント (Skype、Xbox など)
 個人用 Microsoft アカウントのみ

[選択に関する詳細...](#)

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。
プラットフォームの選択 ▼ 例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

[続行すると、Microsoft プラットフォーム ポリシーに同意したことになります](#)

登録

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

ホーム > [redacted] | アプリの登録 >

Mist AA IdP

検索

削除 エンドポイント プレビュー機能

- 概要
- クイック スタート
- 統合アシスタント
- 問題の診断と解決
- 管理
- サポート + トラブルシューティング

基本

表示名	Mist AA IdP	クライアントの資格情報	証明書またはシークレットの追加
アプリケーション (クライアント) ID	8064712b-05ea-486e-8ca[redacted]	リダイレクト URI	リダイレクト URI を追加する
オブジェクト ID	cd3fef53-a76b-4d4e-95c4-4ddbada4a5557	アプリケーション ID の URI	アプリケーション ID URI の追加
ディレクトリ (テナント) ID	d1db1fde-f083-4f59-b3db[redacted]	ローカル ディレクトリでのマネージド アプリケーション	Mist AA IdP
サポートされているアカウントの種類	所属する組織のみ		

概要 ドキュメント

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

The screenshot shows the Mist AA IdP management interface. On the left is a navigation menu with '証明書とシークレット' (Certificates and Secrets) highlighted. The main content area shows the 'クライアント シークレットの追加' (Add Client Secret) dialog box. The dialog has two input fields: '説明' (Description) with the value 'Mist AA IdP クライアントシークレット' and '有効期限' (Validity Period) with a dropdown menu set to '推奨: 180 日 (6 か月)'. A yellow callout box highlights the dropdown menu, showing a list of options: '推奨: 180 日 (6 か月)', '90 日 (3 か月)', '365 日 (12 か月)', '545 日 (18 か月)', '730 日 (24 か月)', and 'カスタム'. At the bottom of the dialog are '追加' (Add) and 'キャンセル' (Cancel) buttons.

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

ホーム > アプリの登録 > Mist AA IdP

Mist AA IdP | 証明書とシークレット

検索 フィードバックがある場合

- 概要
- クイック スタート
- 統合アシスタント
- 問題の診断と解決
- 管理
 - ブランド化とプロパティ
 - 認証
 - 証明書とシークレット**
 - トークン構成
 - API のアクセス許可
 - API の公開
 - アプリ ロール
 - 所有者
 - ロールと管理者
 - マニフェスト
- サポート + トラブルシューティング

お時間があれば、フィードバックをお寄せください。 →

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (1)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値 ①	シークレット ID
Mist AA IdP クライアントシークレット	2025/3/25	KP08Q~_AUjgWtCR0I1B5MdZihaYH...	fcb81fe9-757e-46f0-a9dd-0e6a5ee...

作成直後のみ値をコピーできます

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、[パブリッククライア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

The screenshot shows the 'Mist AA IdP | 認証' configuration page. The left sidebar contains a navigation menu with '認証' (Authentication) highlighted in red. The main content area is titled 'プラットフォーム構成' (Platform Configuration) and includes a search bar, a breadcrumb trail, and a list of navigation items. The '認証' section is expanded, showing 'サポートされているアカウントの種類' (Supported account types) with two radio button options: 'この組織ディレクトリのみに含まれるアカウント (上平 和也 のみ - シングル テナント)' (selected) and '任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)'. Below this is a warning message about account validity. The '詳細設定' (Advanced Settings) section is visible, with 'パブリック クライアント フローを許可する' (Allow public client flows) selected. The 'はい' (Yes) radio button is highlighted in red. At the bottom, the '保存' (Save) button is also highlighted in red.

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

ホーム > [組織名] | アプリの登録 > Mist AA IdP

Mist AA IdP | API のアクセス許可

検索

最新の情報に更新

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

よく使用される Microsoft API

Microsoft Graph
Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Microsoft Entra ID、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。

Azure Communication Services
Microsoft Teams で使用されるのと同じセキュリティで保護された CPaaS プラットフォームを使用した豊富なコミュニケーション エクスperiences

Azure Rights Management Services
検証済みのユーザーに、保護されたコンテンツの読み取りと書き込みを許可します

Azure Service Management
Azure portal で利用できる機能の大部分へのプログラムによるアクセス

Data Export Service for Microsoft Dynamics 365
Microsoft Dynamics CRM 組織から外部宛先にデータをエクスポートします

Dynamics 365 Business Central
Dynamics 365 Business Central のデータと機能へのプログラムによるアクセス

Dynamics CRM
CRM ビジネス ソフトウェアと ERP システムの機能にアクセスします

Intune
Intune データへのプログラムによるアクセス

Office 365 Management APIs
Office 365 と Microsoft Entra ID のアクティビティ ログからユーザー、管理者、システム、ポリシーのアクションとイベントに関する情報を取得します

OneNote
OneNote ノートブックでノート、リスト、画像、ファイルなどを作成して管理します

Power Automate
フロー テンプレートの埋め込みとフローの管理

Power BI Service
Power BI のデータセット、テーブル、行などのダッシュボード リソースへのプログラムによるアクセス

SharePoint
SharePoint データとリモートで対話します

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)

The screenshot shows the 'API Access Permissions' configuration page for a Microsoft Graph application. The main window is titled 'API アクセス許可の要求'. It displays a list of permissions under the heading 'アクセス許可を選択する'. A search bar at the top of the list contains 'User.Read.All'. The search results show 'User (1)' with a checked box next to 'User.Read.All (Read all users' full profiles)'. A red box highlights this row. Callouts in Japanese provide instructions: '委任済みの許可' (Delegated permissions) and 'アプリケーションの許可' (Application permissions) are shown in yellow boxes; '検索できます' (Searchable) is shown in a yellow box pointing to the search bar; '右表の値をそれぞれ許可します' (Grant each value from the table on the right) is shown in a yellow box pointing to the selected permission; and 'クリック' (Click) is shown in a yellow box pointing to the 'アクセス許可の追加' (Add permissions) button at the bottom.

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

管理者の同意の確認を与えます。

自分の代わりに付与済みのアクセス許可は影響を受け

"管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Device.Read.All	アプリケーション	Read all devices	はい	に付与されて...
Group.Read.All	アプリケーション	Read all groups	はい	に付与されて...
User.Read	委任済み	Sign in and read user profile	いいえ	...
User.Read.All	アプリケーション	Read all users' full profiles	はい	に付与されて...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (4)				
Device.Read.All	アプリケー...	Read all devices	はい	に付与されました
Group.Read.All	アプリケー...	Read all groups	はい	に付与されました
User.Read	委任済み	Sign in and read user profile	いいえ	に付与されました
User.Read.All	アプリケー...	Read all users' full profiles	はい	に付与されました

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)



ユーザー ...
Microsoft Entra ID

検索

新しいユーザー ▼ 削除 ↓ ユーザー情報をダウンロード 一括操作 更新

すべてのユーザー Azure Active Directory は Microsoft Entra ID になりました。

検索 フィルターを追加する

1人のユーザーが見つかりました

表示名 ↑	ユーザー プリンシパル名 ↓	ユーザーの種類
		メンバー

管理

- 削除済みのユーザー
- パスワードリセット
- ユーザー設定
- 一括操作の結果

トラブルシューティング + サポート

- 新しいサポートリクエスト

ホーム > ユーザー >
新しいユーザーの作成 ...
組織内に新しい内部ユーザーを作成する

基本 ● プロパティ 割り当て 確認と作成

組織内に新しいユーザーを作成します。このユーザーは alice@contoso.com などのユーザー名になります。詳細情報

ID

ユーザー プリンシパル名 * @ [domain] ▼

ドメインが一覧にありませんか? 詳細情報

メール ニックネーム *

ユーザー プリンシパル名から受け継ぐ

表示名 *

パスワード * パスワードの自動生成

有効なアカウント

レビューと作成 < 前へ 次: プロパティ >

Identity Providers

user/group

group を追加します

The screenshot shows the Microsoft Entra ID Groups management console. The left sidebar contains navigation options such as '概要 (プレビュー)', 'すべてのグループ', '削除したグループ', '問題の診断と解決', '設定', 'アクティビティ', and 'トラブルシューティング + サポート'. The main area displays a list of groups with columns for '名前', 'オブジェクト ID', 'グループの種類', and 'メンバーシップの種類'. Three groups are listed, all of type 'Microsoft 365' and '割り当て済み'.

<input type="checkbox"/>	名前 ↑	オブジェクト ID	グループの種類	メンバーシップの種類
<input type="checkbox"/>	[REDACTED]	d03502d3-76e[REDACTED]	Microsoft 365	割り当て済み
<input type="checkbox"/>	[REDACTED]	f9a2c0c6-7bf0[REDACTED]	Microsoft 365	割り当て済み
<input type="checkbox"/>	[REDACTED]	ec139509-e8c[REDACTED]	Microsoft 365	割り当て済み

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

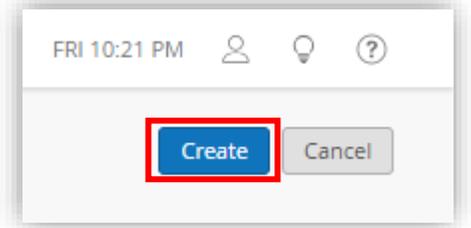
The screenshot displays the Juniper Mist management console interface. On the left is a dark blue navigation sidebar with icons and labels for various sections: Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is divided into several tabs: Admin, Access, WAN, Wired, and Wireless. Under the 'Access' tab, the 'Identity Providers' option is highlighted with a red box. A modal window titled 'Identity Providers' is open, showing a 'Static Configuration' section with an 'Add IDP' button highlighted in red. Below the button is a table with columns for 'Name', 'IDP Type', and 'Default IDP'. The table is currently empty, and the text 'There are no identity providers.' is displayed in the center.

Name	IDP Type	Default IDP
There are no identity providers.		

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
EntralID

Configuration

IDP type
 LDAPs OAuth Mist Edge Proxy

OAuth Type
Azure

OAuth Tenant ID ⓘ
b7aeraasd-7a68sdjf-asdgvgaadsfaer

Domain Names
.net

Default IDP ⓘ

OAuth Client Credential (CC) Client Id ⓘ
20wefas-df28-9kloaa4e

OAuth Client Credential (CC) Client Secret ⓘ
..... [Reveal](#)

OAuth Resource Owner Password Credential (ROPC) Client Id ⓘ
20wefas-df28-9kloaa4e

[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

The screenshot shows the Juniper network management interface. On the left, a navigation menu has 'Organization' highlighted with a red box. The main content area shows the 'Auth Policies' page, with 'Auth Policies' in the top navigation bar also highlighted with a red box. Below the navigation, there are buttons for 'Add Rule' (highlighted with a red box) and 'Create Label'. A table below shows a single policy rule with a red 'X' in the 'Policy' column, indicating a failure or error.

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

Save Cancel

Show NAC Events Hit Count | Today ↕

<input checked="" type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
	Last	Last Rule	All Users	— X —>	Network Access Denied	0

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

Match Criteria			Assigned Policies		
No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
1	None	All Users	Allow	Network Access Allowed	0

ポリシーは First Match です
上から順に評価されます

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

Auth Policy Label

- Port Types**
- Wireless
 - Wired

Label	Site	Site Group
Search		
EAP-TTLS		Auth Type
EAP-TLS		Auth Type
TEAP		Auth Type
MAB		Auth Type
PSK		Auth Type
Admin Auth		Auth Type
printer		Client List
Wired		Port Types
Wireless		Port Types
Generic IETF		Vendors

Label、Site/Site Group を指定します

- ✓ Allow
- ✗ Block

Vendors

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

Search	
SessionTimeOut	AAA Attribute
Role-contractor	AAA Attribute
Printer-VLAN	AAA Attribute

VLAN、Role、Session Timeout など

AAA Attribute (Auth Policy Label)

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

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

The screenshot displays the 'Auth Policies' configuration page. On the left, a table lists existing policy rules with columns for 'No.', 'Name', and 'Match Criteria'. The 'Create Label' button is highlighted with a red box. On the right, the 'Create Label' dialog box is open, also outlined in red. It contains the following fields:

- Name is required:** A red error message above the 'Label Name' input field.
- Label Name:** A text input field.
- Label Type:** A dropdown menu currently set to 'AAA Attribute'. Below it is a descriptive text: 'A group of RADIUS attributes that could be used in Match or Apply section of the Auth policy rule.'
- Label Values:** A dropdown menu currently set to 'Role'. Below it is a text input field with the placeholder text 'Role Values (Example: contractor)' and a help icon.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom right.

A yellow callout box points to the 'Create Label' button with the text: "[Create Label] をクリックして、Label を設定できます"

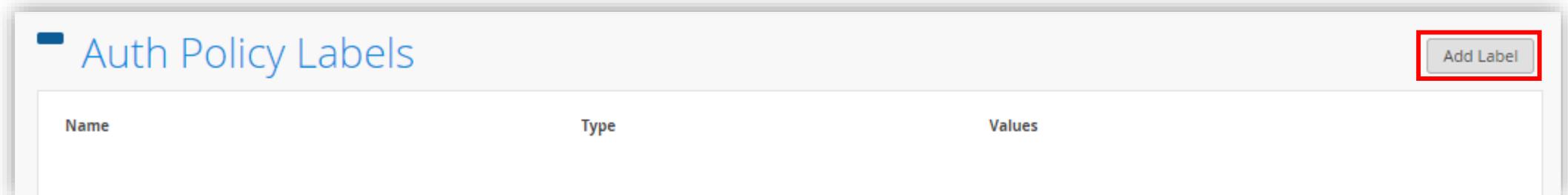
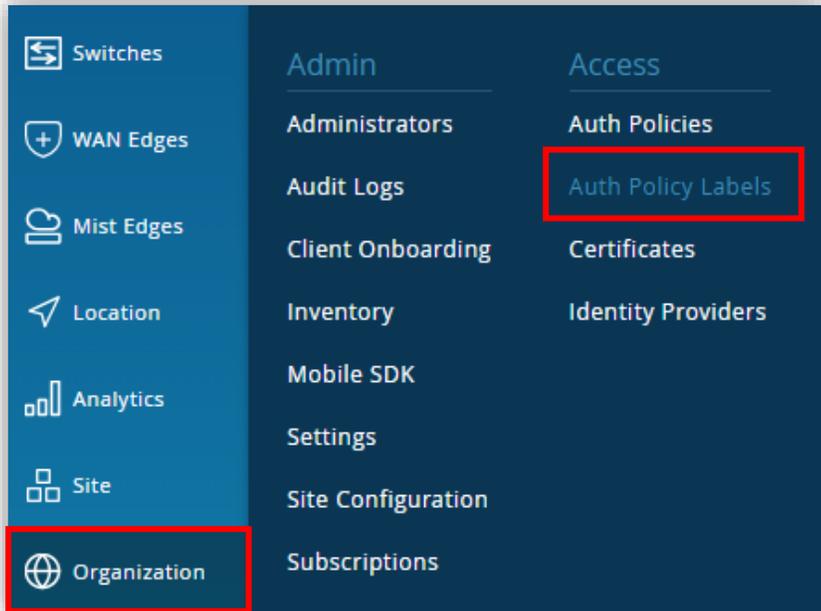


Auth Policy Labels

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

< Auth Policy Labels :

Name is required

Label Name

Label Type

AAA Attribute

A group of RADIUS attributes that could be used in Match or Apply section of the Auth policy rule.

Label Values

Role

Role Values (Example: contractor) ⓘ

- 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)

All / Any を選択できます

All Any



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

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

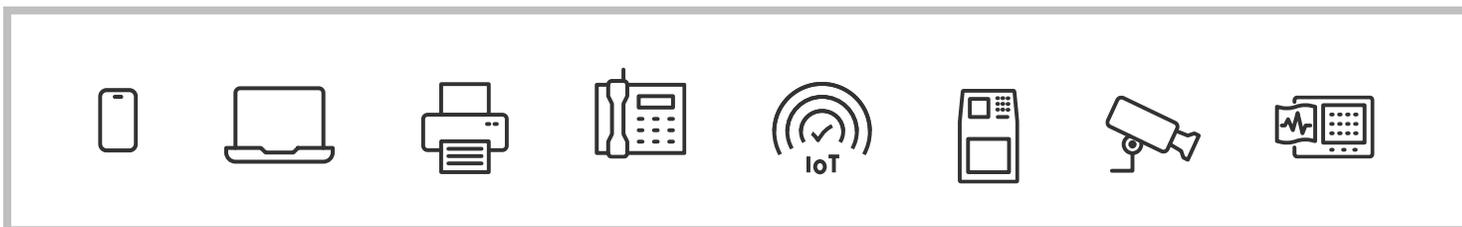
Auth Policy の設定

- 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ブリカント、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	<ul style="list-style-type: none">• 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

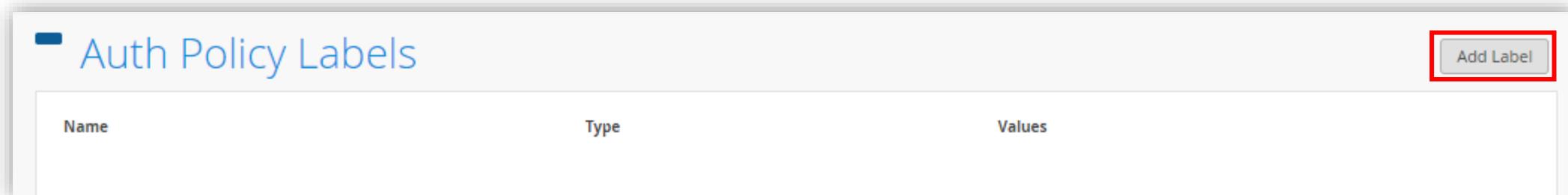
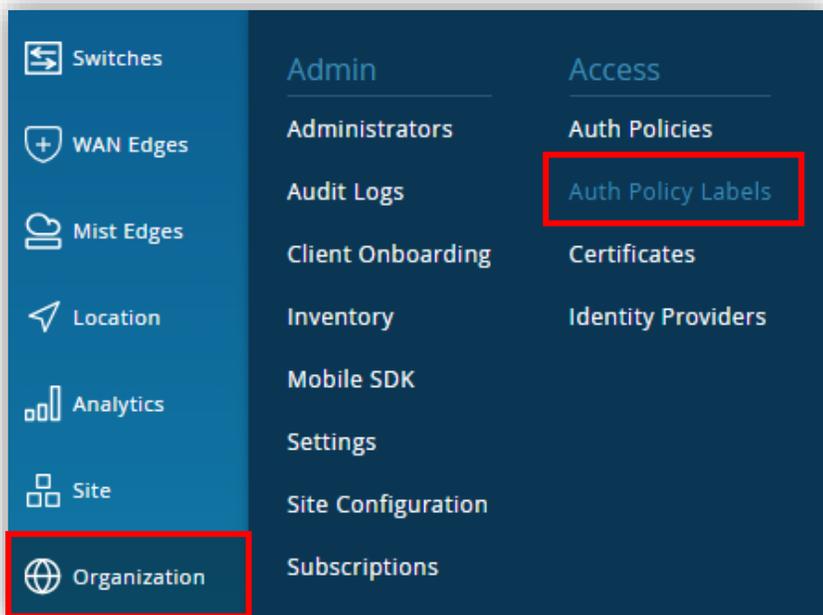
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: Profile Name <input checked="" type="checkbox"/> User dot1x authentication <input checked="" type="checkbox"/> Dynamic VLAN(Optional) Networks <input checked="" type="checkbox"/> Mac authentication
Port Configuration	Port ID: <i>Interface</i> Configuration 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

< Auth Policy Labels : 4 **Create** Cancel

1 Label Name
printer

2 Label Type
Client List
This label can be used in the Match section of the Auth policy rule to match on a list of MAC addresses or MAC OUIs identified by wildcards.

3 Label Values
Client MAC Address (Example: 1122AA33BB44 and/or 11-22-AA-33-BB-44 and/or 11-22-AA*)
00:50:56:be:6e:53 × 00:50:56:be:6e:28 × Add MAC Address

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)

< Auth Policy Labels : 4 Create Cancel

1 Label Name
Printer-VLAN

2 Label Type
AAA Attribute
A group of RADIUS attributes that could be used in Match or Apply section of the Auth policy rule.

3 Label Values
VLAN
VLAN Values (Example: 750 or employee-vlan) ⓘ
100

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

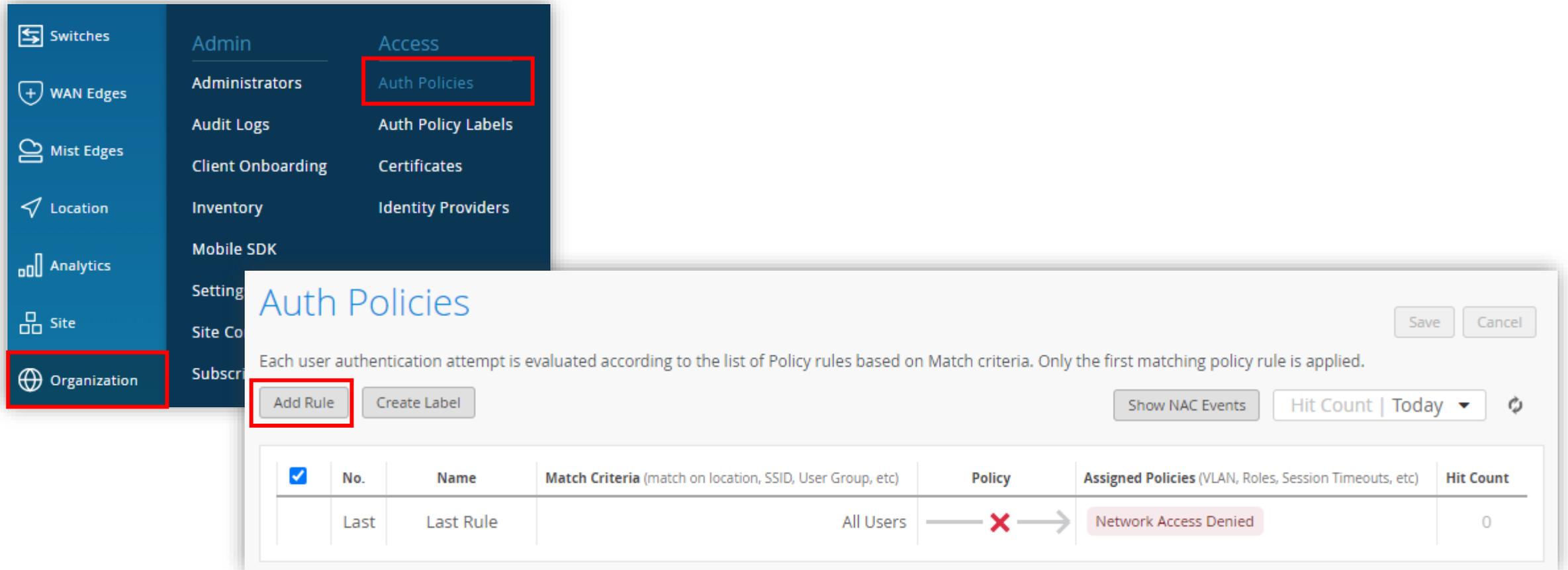
※ Tunnel-Private-Group-ID または、
Airespace-Interface-Name をサポート

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



The screenshot shows the Juniper Mist management interface. On the left, the 'Organization' menu item is highlighted with a red box. In the main navigation area, the 'Access' tab is selected, and the 'Auth Policies' link is highlighted with a red box. Below this, the 'Auth Policies' configuration page is displayed. The 'Add Rule' button is highlighted with a red box. The page includes a 'Save' and 'Cancel' button, a 'Show NAC Events' button, and a 'Hit Count | Today' dropdown menu. A table below shows the current policy rules.

<input checked="" type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
	Last	Last Rule	All Users	→ X →	Network Access Denied	0

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)

<input type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
<input type="checkbox"/>	1	None	+ All Users	✓	Network Access Allowed +	0

ポリシー名 [Name] は任意です
※未設定でも可

[Auth Type] で [MAB] を選択します

Auth Policy Label の [printer] を選択
します(STEP 03 で作成)

[Port Types] で [Wired] または
[Wireless] を選択します

Auth Policy Label の [Printer-VLAN] を
選択します(STEP 03 で作成)

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

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

Buttons: Add Rule, Create Label, Show NAC Events, Hit Count | Today

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
1	printer	+ all printer × MAB × Wired ×	✓	Network Access Allowed Printer-VLAN ×	0
Last	Last Rule	All Users	✗	Network Access Denied	0

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

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

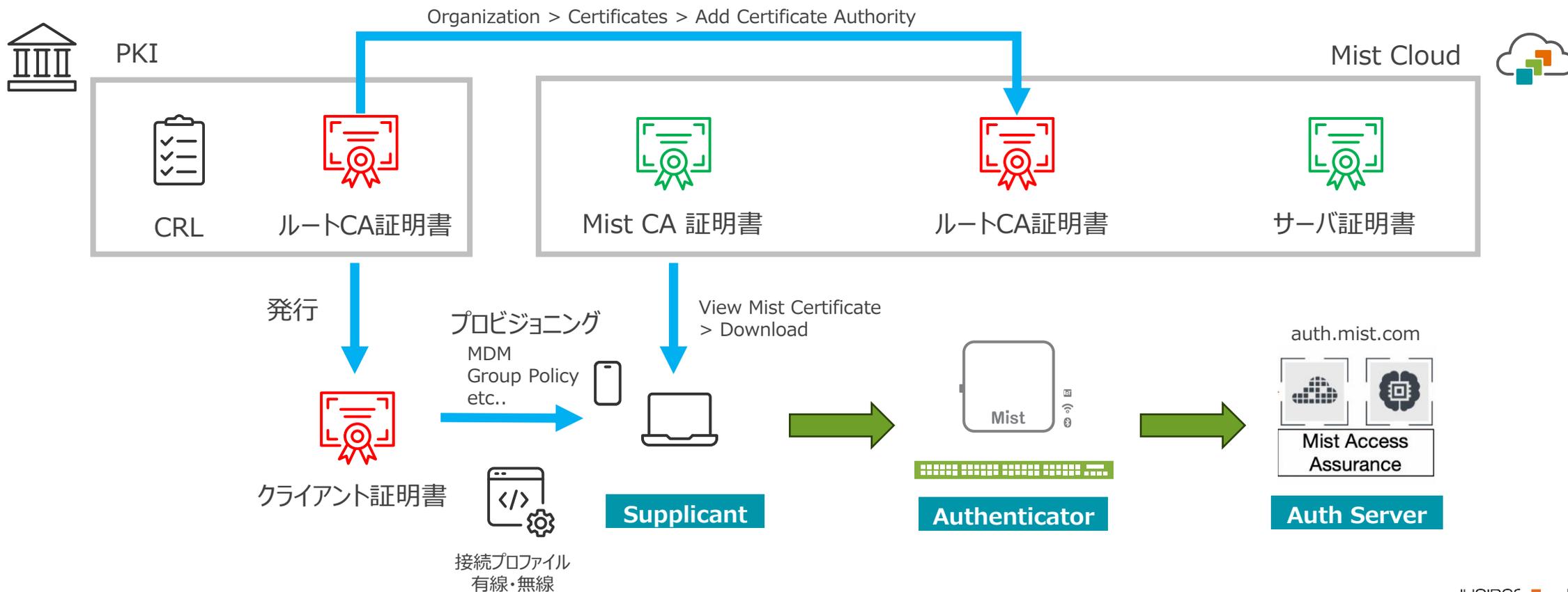
- STEP 03 で作成したラベルを適用したポリシーの作成

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



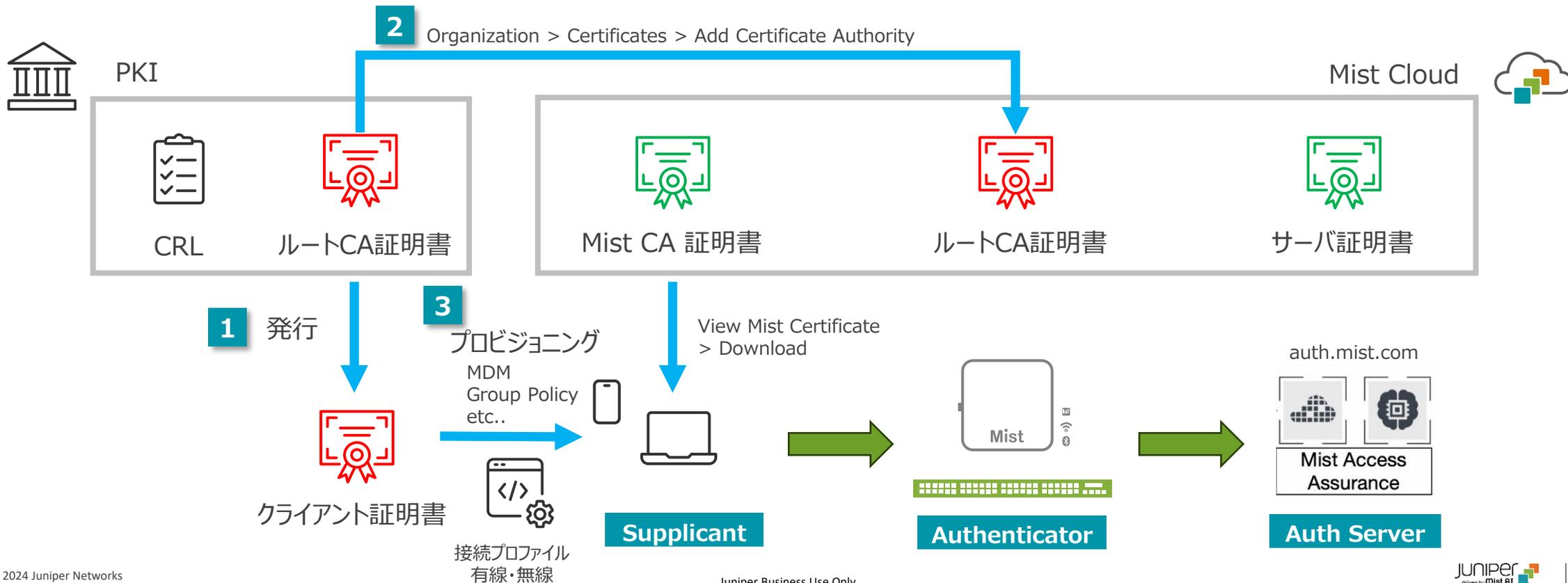
EAP-TLS (証明書認証)

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)

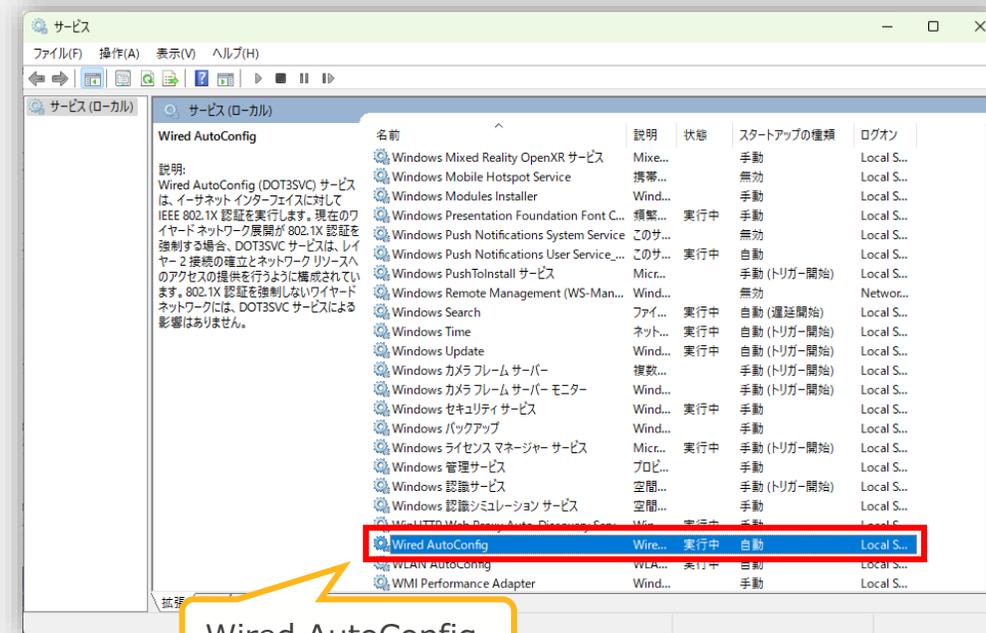
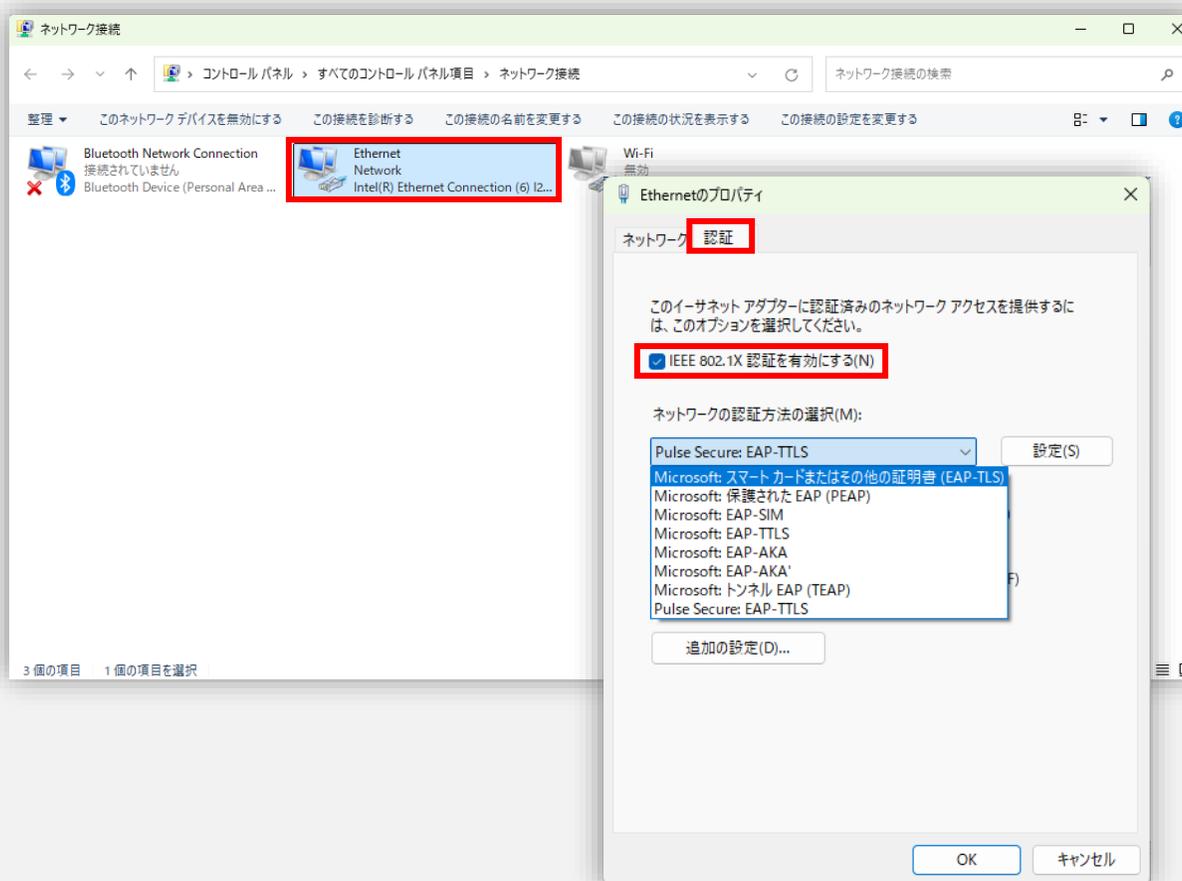
STEP 01 - 証明書設定 / クライアント設定

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



Wired AutoConfig

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	<ul style="list-style-type: none">• 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

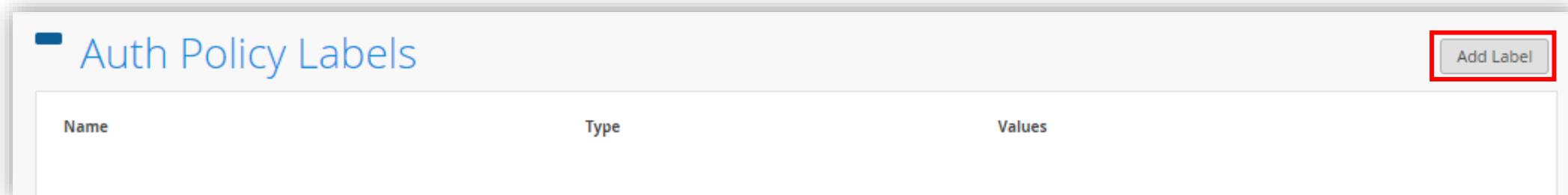
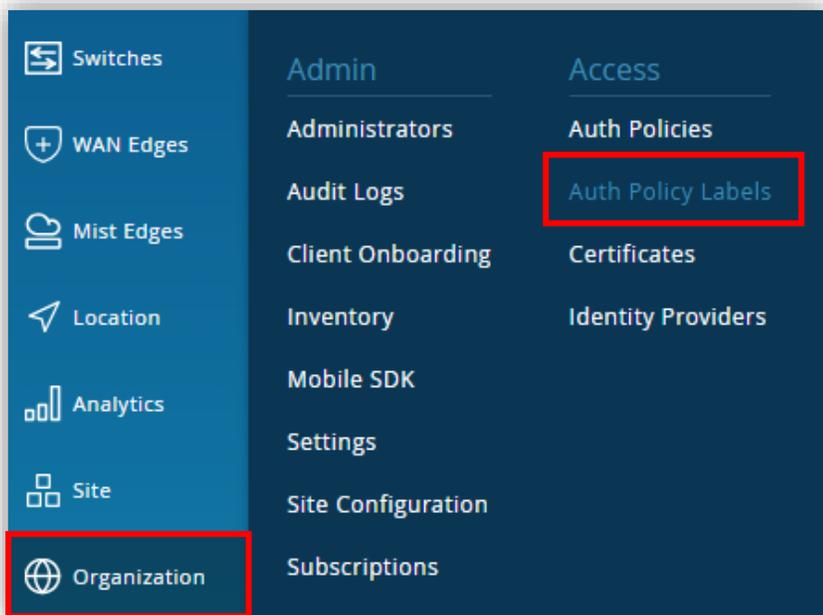
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: Profile Name <input checked="" type="checkbox"/> User dot1x authentication <input checked="" type="checkbox"/> Dynamic VLAN(Optional) Networks
Port Configuration	Port ID: <i>Interface</i> Configuration Profile: Profile Name

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

3. 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 Certificate の Issuer を
参照する Label を設定しています



< Auth Policy Labels : 4 Create Cancel

1 Label Name
MistCert

2 Label Type
Certificate Attribute
This label group can be used in Match section of the Auth policy rule to match on user or device certificate fields used during authentication.

3 Label Values
Issuer
Issuer Values (Example: /C=US/ST=CA/O=Mist/OU=LAB/CN=LAB-CA) ⓘ
C=US, O=Mist, OU=OrgCA, CN=2086561b-07c3-4f19-bac6-4b39fbf739a4

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

The screenshot shows the Juniper Mist management interface. On the left, the 'Organization' menu item is highlighted with a red box. In the main navigation area, the 'Access' tab is selected, and the 'Auth Policies' link is highlighted with a red box. Below this, the 'Auth Policies' configuration page is displayed. The 'Add Rule' button is highlighted with a red box. The page includes a 'Save' and 'Cancel' button, a 'Show NAC Events' button, and a 'Hit Count | Today' dropdown menu. A table below shows a single policy rule with a red 'X' indicating a failure.

<input checked="" type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
	Last	Last Rule	All Users	— X —>	Network Access Denied	0

EAP-TLS (証明書認証)

STEP 04 - Auth Policy

- [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

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

Save Cancel

Add Rule Create Label

[Auth Type] で [EAP-TLS] を選択します

[Port Types] で [Wired] または [Wireless] を選択します

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
1	None	+ all EAP-TLS × Wired ×	✓	Network Access Allowed +	0
2	None	+ all MistCert × EAP-TLS × Wireless ×	✓	Network Access Allowed +	4

ポリシー名 [Name] は任意です
※未設定でも可

STEP 03 で設定した Auth Policy Label を指定しています

AAA Attribute で VLAN、Role、Session Timeout などを設定できます
(Auth Policy Label の設定が必要です)

Search

temp AAA Attribute

Close



EAP-TTLS

Entra ID/OAuth

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

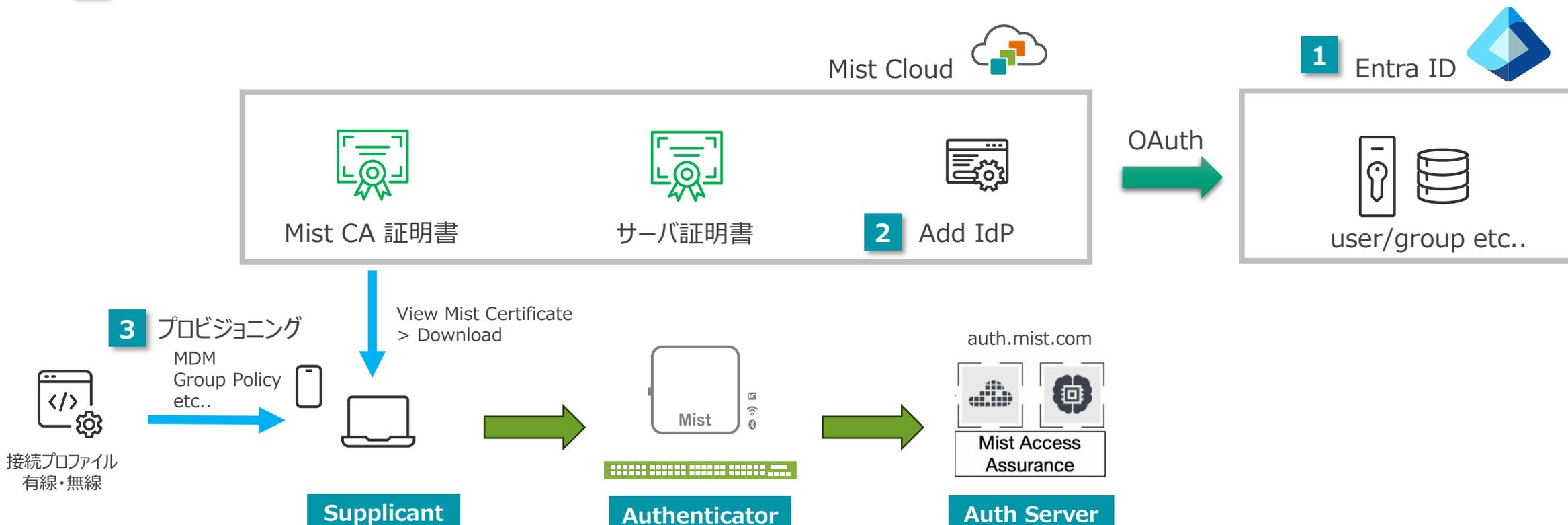
STEP 01 - 証明書設定 / クライアント設定 / IdP 設定

例) EAP-TTLS Entra ID/OAuth 連携

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](#))



- 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



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	<ul style="list-style-type: none">• 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

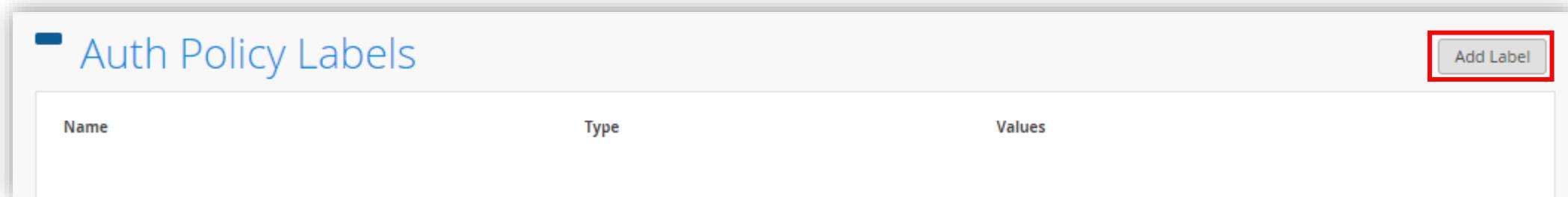
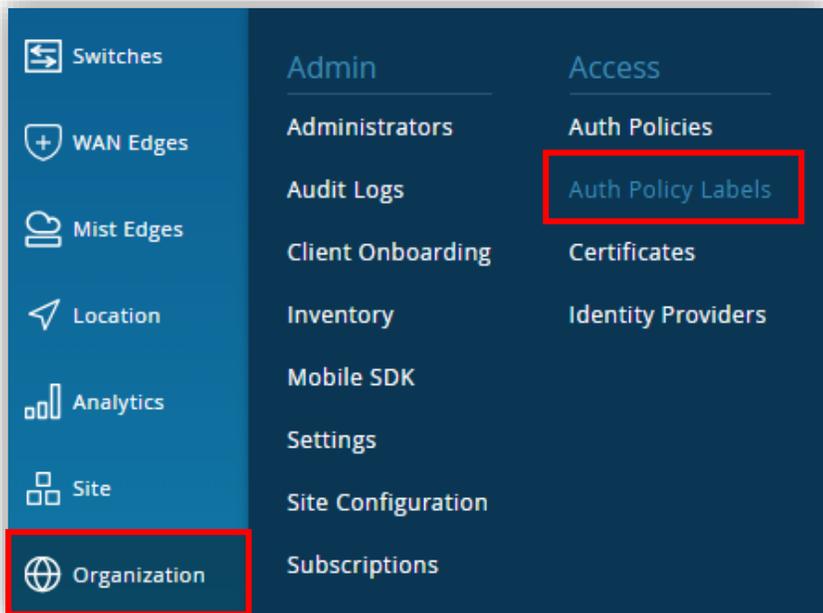
項目	値
Authentication Servers	Mist Auth
Port Profile	Name: Profile Name <input checked="" type="checkbox"/> User dot1x authentication <input checked="" type="checkbox"/> Dynamic VLAN(Optional) Networks
Port Configuration	Port ID: <i>Interface</i> Configuration Profile: Profile Name

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

Employee

2

Label Type

Directory Attribute

This is Match label that could be used in Auth policy rule by evaluating received information from the Identity Provider during user or device authorization.

3

Label Values

Group

Group Values (Example: Employee) ⓘ

Employee

4

Create

Cancel

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



4 **Create** Cancel

< Auth Policy Labels :

1 Label Name
Employee-Role

2 Label Type
AAA Attribute
A group of RADIUS attributes that could be used in Match or Apply section of the Auth policy rule.

3 Label Values
Role
Role Values (Example: contractor) ⓘ
Employee

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

The screenshot shows the Juniper Mist management console interface. On the left sidebar, the 'Organization' menu item is highlighted with a red box. The main content area shows the 'Auth Policies' page, with the 'Auth Policies' menu item also highlighted with a red box. Below the navigation, the 'Add Rule' button is highlighted with a red box. The page title is 'Auth Policies' and it includes a 'Save' and 'Cancel' button. Below the title, there is a descriptive text: 'Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.' Below this text, there are buttons for 'Add Rule', 'Create Label', 'Show NAC Events', and a 'Hit Count | Today' dropdown menu. At the bottom, there is a table with the following data:

<input checked="" type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
	Last	Last Rule	All Users	→ X →	Network Access Denied	0

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - Auth Policy

- [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

The screenshot shows the 'Auth Policies' configuration page. At the top, there are buttons for 'Add Rule' and 'Create Label'. Below is a table of policy rules. The first rule is selected, showing its configuration details. Callouts provide instructions for each field:

- [Auth Type] で [EAP-TTLS] を選択します**: Points to the 'EAP-TTLS' selection in the Match Criteria.
- [Port Types] で [Wired] または [Wireless] を選択します**: Points to the 'Wireless' selection in the Match Criteria.
- AAA Attribute で VLAN、Role、Session Timeout などを設定できます (Auth Policy Label の設定が必要です) ここでは、Employee-Role を割り当てます**: Points to the 'Employee-Role' selection in the Assigned Policies.
- ポリシー名 [Name] は任意です ※未設定でも可**: Points to the 'None' value in the Name field.
- STEP 03 で設定した Auth Policy Label を指定しています**: Points to the 'Employee' selection in the Match Criteria.

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
1	None	+ all Employee × EAP-TTLS × Wireless ×	✓ →	Network Access Allowed Employee-Role × +	141
		All Users	✗ →	Network Access Denied	5

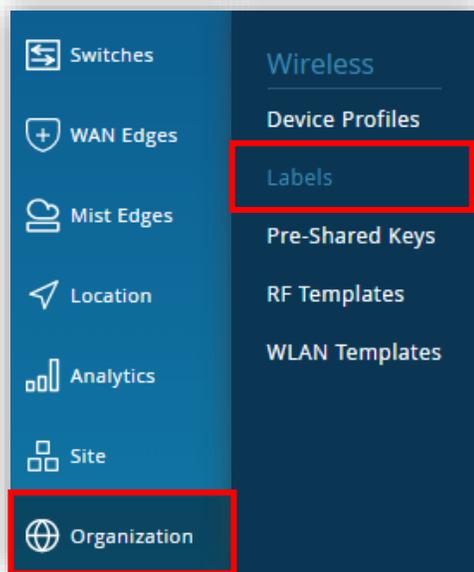
続いて、割り当てた Role に対してアクセス可能なリソースを設定するための WxLAN Policy を設定します



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



1

2

3

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)

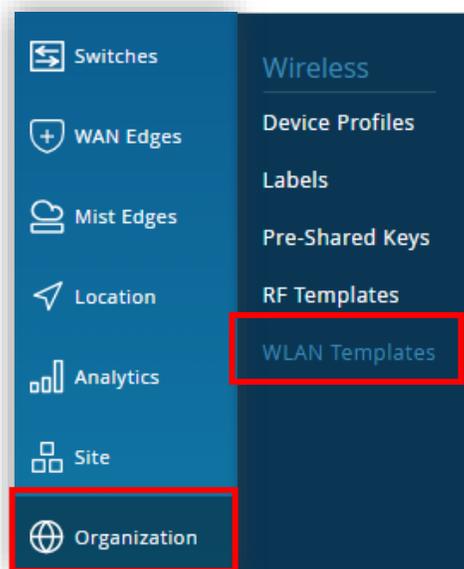
4 [Create] をクリックします

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

EAP-TTLS Entra ID/OAuth 連携設定手順

STEP 04 - WxLAN Policy

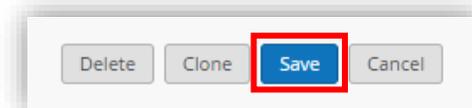
2. [Organization] から [WLAN Templates] で編集する WLAN Template を選択します
3. [Policy] の項目で、[User] に作成した Label(Role): Employee を設定、User に対する [Resource] を割り当て、[Save] で設定を保存します



WLAN Templates

Filter

Name	Applied To Org	Sites	Site Groups	Exceptions	WLANs
wt	No	main_site			JCL-test



Policy

Template Policies

Each user/resources session is evaluated against the first matching rule in the template WLAN.

Add Rule Edit Labels

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

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)
1	+ Employee x	→ ✓ →	Facebook x +

Wireless ユーザに対して、Role ベースの通信制御ができます





Troubleshoot Tips

Troubleshoot Tips

Auth Policy Hit Counts > NAC Events

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

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

Save Cancel

Add Rule Create Label Show NAC Events Hit Count | Today

No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
1	EAP-TLS	+ all EAP-TLS Wireless	→ ✓ →	Network Access Allowed +	0
Last	Last Rule	All Users	→ ✗ →	Network Access Denied	6

Hit Count の数字部分をクリック

右端に NAC Events が表示されます

Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

Add Rule Create Label

Auth Rule Last Rule

Search by client mac, name, ap mac and switch mac

NAC Events	7 Total	0 Good	0 Neutral	7 Bad
NAC Client Access Denied	Sc5b:35:cf:3a:b5	3:06:54:973 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	3:04:00:047 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	3:01:46:875 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	2:59:55:790 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	2:58:49:576 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	2:58:00:954 PM Oct 9, 2024		
NAC Client Access Denied	Sc5b:35:cf:3a:b5	2:57:43:019 PM Oct 9, 2024		

Client aa43:db:51:ea:59

MAC Address aa43:db:51:ea:59

BSSID Sc5b:35:ca:33:bd

SSID AA-test

Certificate Serial Number 6d368d6e9d943e268

Description TLS Client Certificate Check failed by the Server. Please check Certificate configuration on the client. Also check if the server has the correct CA configuration

Authentication Type eap-tls

User Name user02@test.net

Certificate CN user02@test.net

Certificate SAN (DNS Name) user02@test.net

Certificate Issuer /C=US/O=mist/CN=lab-ca@test.net

Certificate Expiry Jul 12, 2033 1:31:00 AM

Certificate Subject /C=US/O=mist/CN=user02@test.net

Auth Rule No Rule Match

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

Client Events 107 Total 23 Good 39 Neutral 45 Bad

Event Type	Client	Time
Authorization & Association	user02@test.net	3:44:57.760 PM Oct 9, 2024
NAC Client Access Allowed	user02@test.net	3:44:57.672 PM Oct 9, 2024
NAC Client Certificate Validation Success	user02@test.net	3:44:57.669 PM Oct 9, 2024
NAC Server Certificate Validation Success	user02@test.net	3:44:57.668 PM Oct 9, 2024
Client Deauthentication	user02@test.net	3:44:48.957 PM Oct 9, 2024

Client	user02@test.net	Certificate SAN (DNS Name)	user02@test.net
AP	5c:5b:35:cf:3a:b5	Certificate Issuer	/C=US/O=mist/CN=lab-ca@test.net
MAC Address	a6:74:7f:70:aa:fc	Certificate Expiry	Jul 12, 2033 1:31:00 AM
BSSID	5c:5b:35:ca:33:bd	Certificate Subject	/C=US/O=mist/CN=user02@test.net
SSID	AA-test	Auth Rule	EAP-TLS
Certificate Serial Number	6d368d6ed943e268	RADIUS Returned Attributes	User-Name=user02@test.net
Authentication Type	eap-tls		

Auth Rule 名をクリック

Auth Policy 設定に遷移

<input checked="" type="checkbox"/>	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)	Hit Count
<input checked="" type="checkbox"/>	1	EAP-TLS	+ all EAP-TLS × Wireless ×	→ ✓ →	Network Access Allowed +	2
	Last	Last Rule	All Users	→ ✗ →	Network Access Denied	15

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

The screenshot displays the 'Client Events' interface in Mist Cloud. It shows a list of events on the left and a detailed view of a selected event on the right.

Client Events Summary: 93 Total, 14 Good, 37 Neutral, 42 Bad

Event Type	Client MAC	Time
Authorization Failure	0a:f6:47:05:39:9b	3:33:36.676 PM Oct 9, 2024
NAC Client Access Denied	0a:f6:47:05:39:9b	3:33:35.643 PM Oct 9, 2024
NAC Client Certificate Validation Failure	0a:f6:47:05:39:9b	3:33:35.642 PM Oct 9, 2024
Authorization Failure	Anonymous	3:28:00.542 PM Oct 9, 2024
NAC Client Access Denied	Anonymous	3:27:59.507 PM Oct 9, 2024
NAC Client	Anonymous	3:27:59.506 PM Oct 9, 2024

Event Details:

BSSID	5c:5b:35:ca:33:cd	Certificate Issuer	/C=US/O=mist/CN=lab-ca@test.net
SSID	AA-test	Certificate Expiry	Jul 12, 2033 1:31:00 AM
Certificate Serial Number	6d368d6ed943e268	Certificate Subject	/C=US/O=mist/CN=user02@test.net
Description	TLS Client Certificate Check failed by the Server. Please check Certificate configuration on the client. Also check if the server has the correct CA configuration		
Authentication Type	eap-tls	Auth Rule	No Rule Match
User Name	user02@test.net	Port Type	wireless
		NAS Vendor	juniper-mist
		NAS IP	10.0.0.3

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

Client Events			215 Total	128 Good	40 Neutral	47 Bad
Failure						
Authorization Failure	Bedroom	11:50:03.359 AM May 27, 2024				Description oauth2: "invalid_grant" "AADSTS65001: The user or administrator has not consented to use the application with ID 'b32a58b7-e84b-427e-95c8-cf1d99703666' named 'Mist AA IDP connector'. Send an interactive authorization request for this user and resource. Trace ID: dfafc423-0a35-42ca-b92d-fb83a1d9f401 Correlation ID: 09adf0a3-afbf-4592-9556-0b71c0989734 Timestamp: 2024-05-27 03:50:02Z"
NAC Client Access Denied	Bedroom	11:50:02.330 AM May 27, 2024				
NAC IDP Authentication Failure	Bedroom	11:50:02.324 AM May 27, 2024				
Authorization Failure	Bedroom	11:43:44.925 AM May 27, 2024				
Authorization Failure	Bedroom	11:42:23.687 AM May 27, 2024				

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

Client Events

215 Total 128 Good 40 Neutral **47 Bad**

Event Type	Location	Time
Authorization Failure	Bedroom	11:50:03.359 AM May 27, 2024
NAC Client Access Denied	Bedroom	11:50:02.330 AM May 27, 2024
NAC IDP Authentication Failure	Bedroom	11:50:02.324 AM May 27, 2024
Authorization Failure	Bedroom	11:43:44.925 AM May 27, 2024
Authorization Failure	Bedroom	11:42:23.687 AM May 27, 2024

Last Association 9.5 sec ago

Server Port	4268	Capabilities	40Mhz
Reason	23	Description	Reason code 23 "IEEE 802.1X authentication failed" 802.1x Auth Fail(23). Radius server reject client request - possible username/password mismatch(512).
BSSID	5c:5b:35:bc:96:74	Channel	157
RSSI	-43 dBm	Authentication Type	eap

Download Packet Capture

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

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:

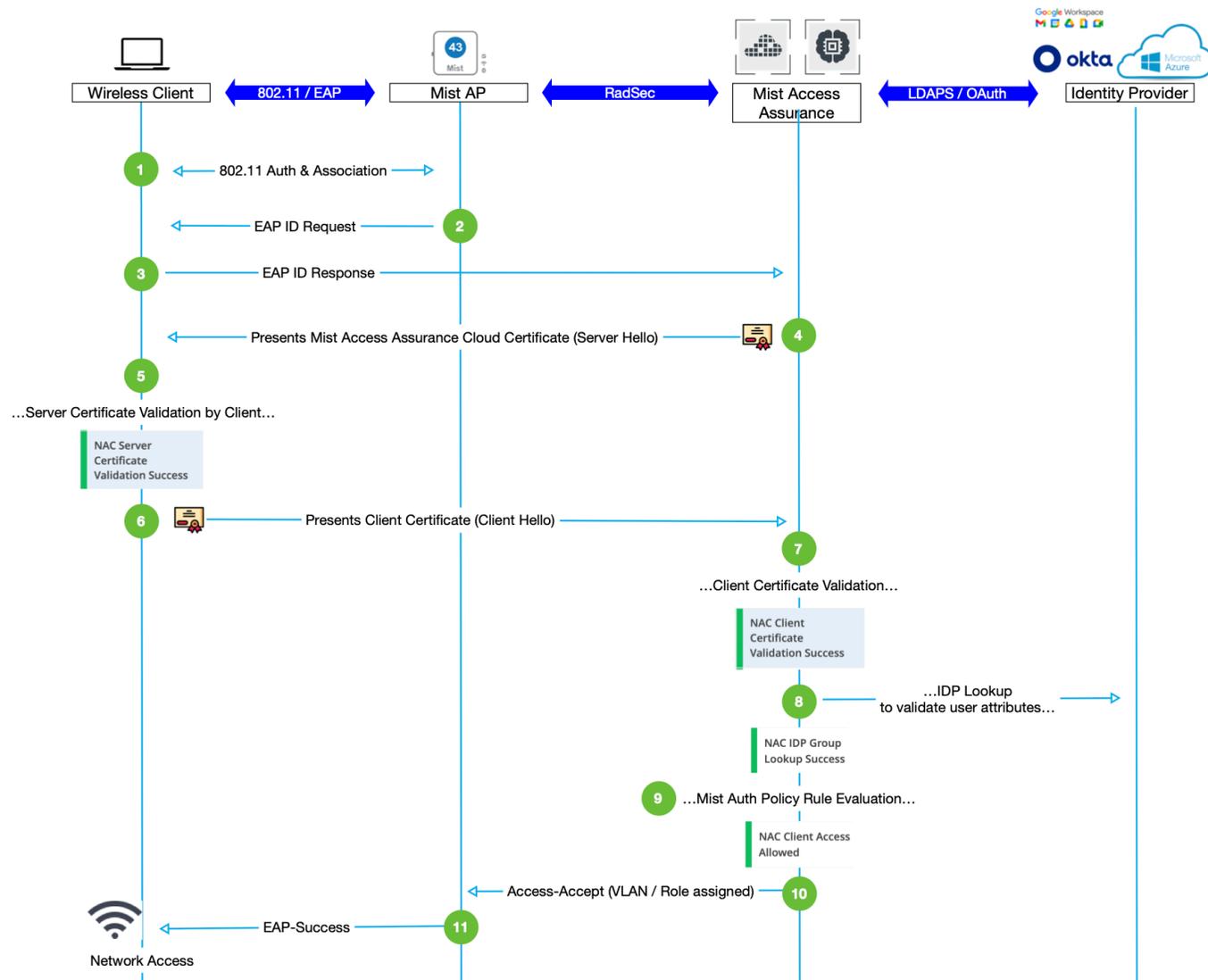
[Configure Webhooks from the API Webhooks\(API Documentation\)](#) ※要サインイン



EAP 認証フロー

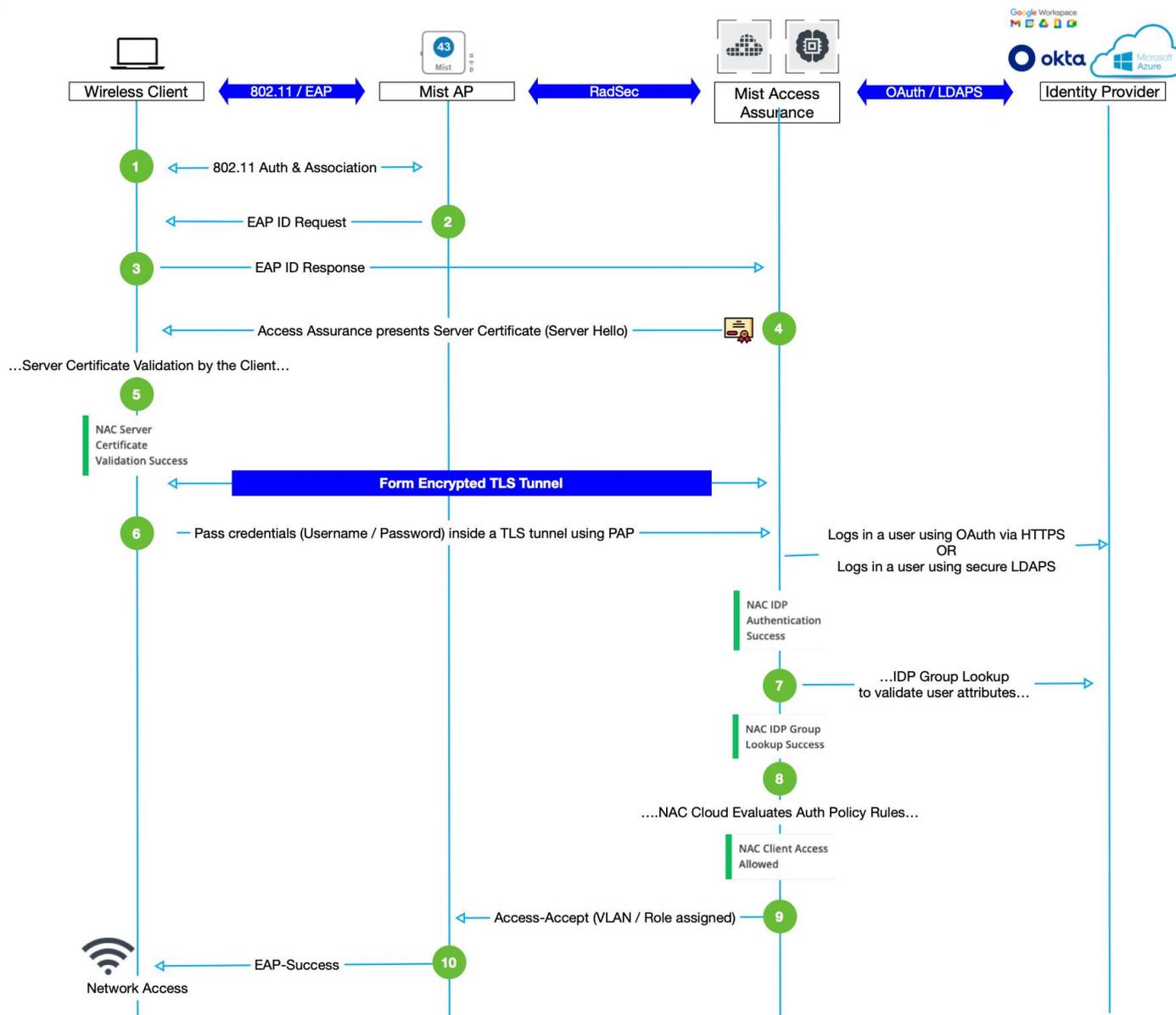
EAP-TLS 認証フロー

1. 認証装置 (AP など) がセッション要求を開始するか、サブリカント (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. 認証装置はサブリカントに EAP 要求を送信し、サブリカントの ID を要求します。
3. サブ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. サブリカントはサーバー証明書を検証します。つまり、サブ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. サブ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、認証装置がサブ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、サブ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、サブリカント (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 要求をサブリカントに送信します。
3. サブリカントは、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. サブリカントは、サーバー証明書を検証します。つまり、サブリカントは、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. サブリカントは、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。サブリカントは、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、認証装置がサブ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、サブリカントにアクセスを提供します。





THANK YOU

JUNIPER
NETWORKS®

Driven by
Experience™