Mist 設定マニュアル

- WLAN -

WPA3 の設定

ジュニパーネットワークス株式会社

2024年7月 Ver 1.0

JUNIPer driven by Mist AI

はじめに

- 本マニュアルは、『WPA3 の設定』について説明します
- 手順内容は 2024年7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ください
  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
  https://www.mist.com/documentation/
- 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

WPA3 の設定

WPA3 概要

WPA3 は、Wi-Fi Alliance® により発表された WPA2 の後継となるセキュリティ規格です

WPA3 では、管理フレームの暗号化(MFP)が必須となり、SAE による鍵交換や、Transition(移行) モードがサポートされます

動作モード

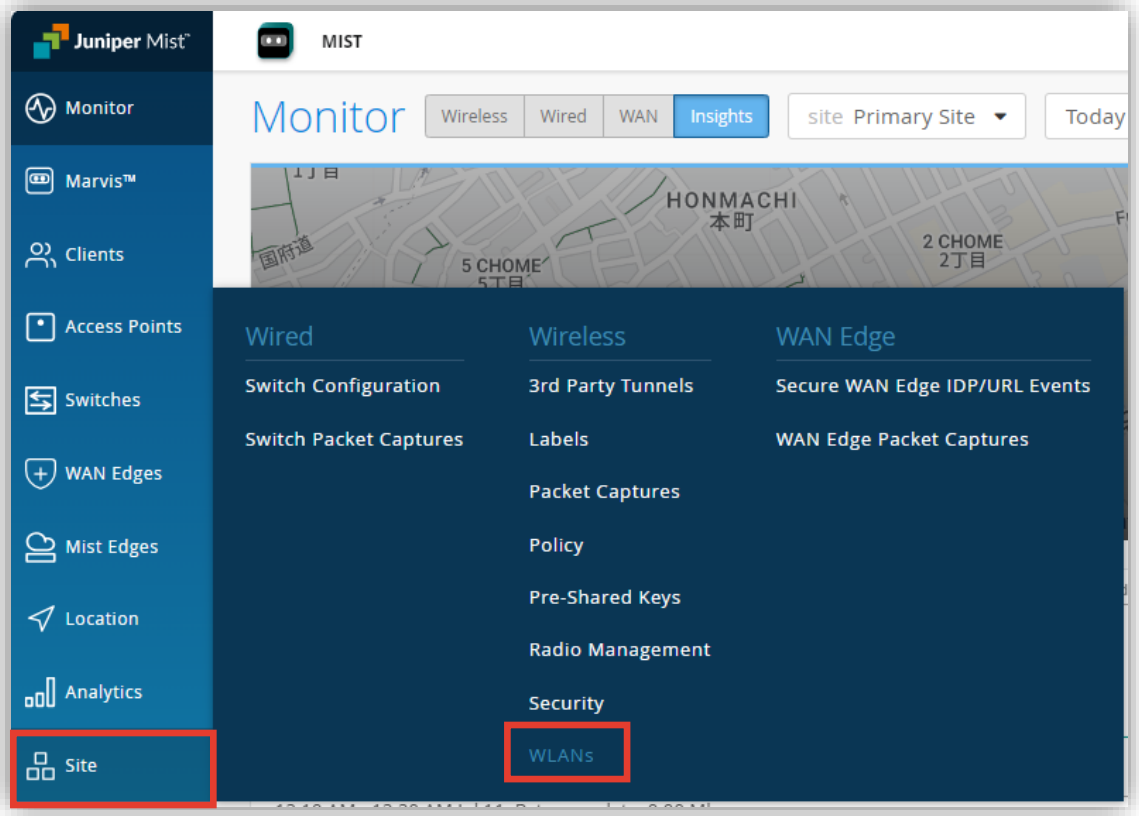
- WPA3 Personal(WPA3-SAE)
  - SAE(Simultaneous Authentication of Equals) による鍵交換
  - Transition モード有効時は、非対応端末は WPA2-PSK で接続 (MFP は任意)
- WPA3 Enterprise(WPA3-ENT/802.1x)
  - WPA2 Enterprise と互換性
  - Transition モード有効時は、非対応端末は WPA2 Enterprise で接続 (MFP は任意)
  - 192 bit モードの暗号オプションをサポート (WPA3 のみ、Fast Roaming 選択不可)
- OWE(Opportunistic Wireless Encryption)
  - パブリックネットワークで、認証なしで通信を暗号化し受動的な盗聴に対する保護を提供
  - Transition モード有効時は、非対応端末は OPEN(認証なし)で接続

WPA3-Personal(SAE)

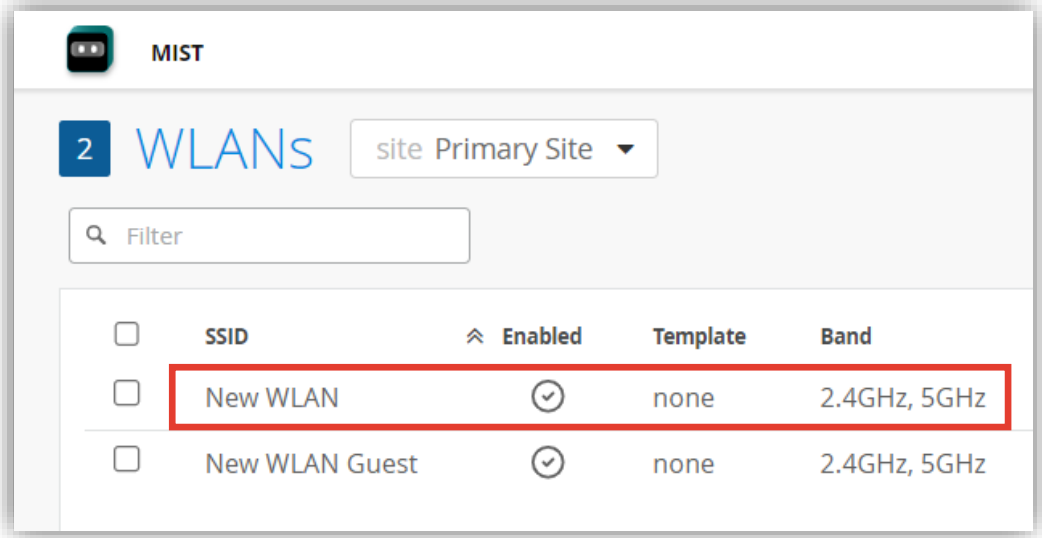
WPA3 の設定

WPA3-Personal(SAE)

1. [Site] から [WLANs] をクリックします



2. 編集する無線 LAN を選択します

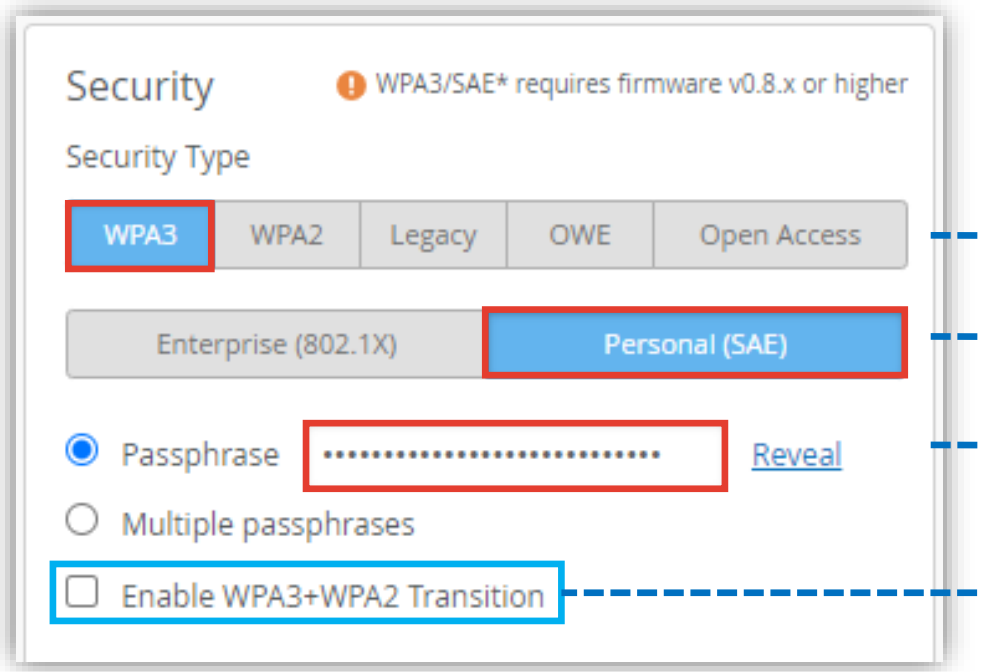


Organization > WLAN Template での設定も可能です

WPA3 の設定

WPA3-Personal(SAE)

3. [Security Type] で [WPA3] を選択、[Personal (SAE)] を選択し、[Passphrases] を設定します (0.8.x 以上)
   - WPA3 に対応していないクライアントに対して WPA2 での接続を許可する場合、 [Enable WPA3-WPA2 Transition] をチェックして、移行モードを有効にします(Optional)



[WPA3] を選択します

[Personal (SAE)] を選択します

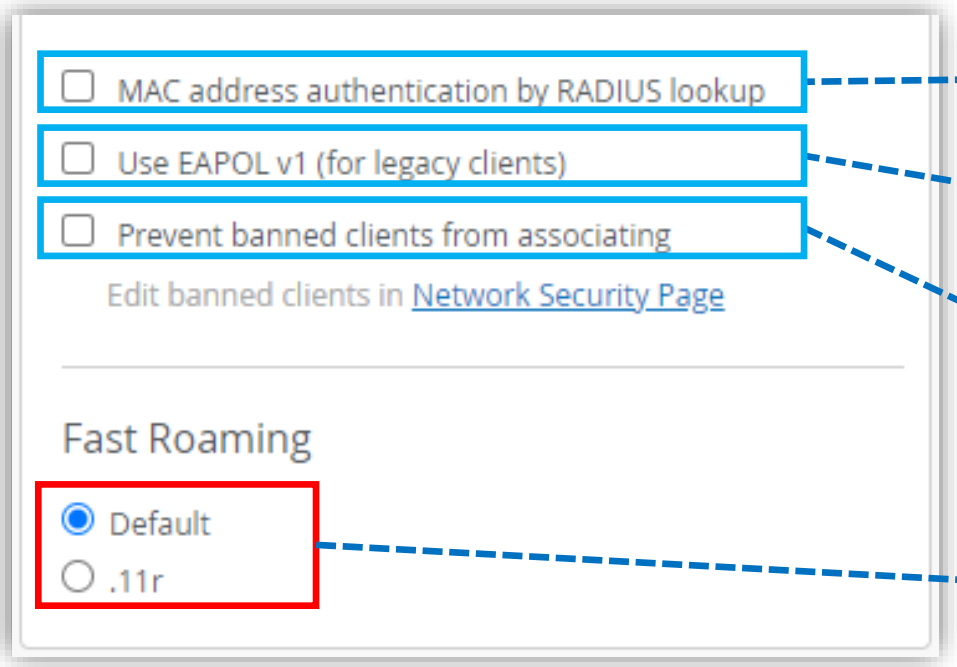
[Passphrase] を設定します

[Enable WPA3-WPA2 Transition] をチェックすると、移行モードが有効になります(Optional)

WPA3 の設定

WPA3-Personal(SAE)

4. その他オプション設定を確認します



[MAC address authentication by RADIUS lookup] をチェックすると、Radius サーバを参照し、MAC アドレス認証します

[Enable EAP-Reauth] をチェックすると、EAP 再認証が有効になります

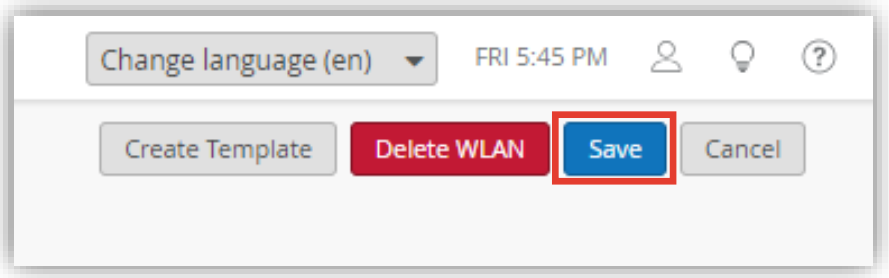
[Prevent banned clients from associating] をチェックすると、Banned Clients に指定したクライアントのアソシエーションが制限されます
(Site > Security > View Client Classification で設定)

Roaming オプションを選択します

WPA3 の設定

WPA3-Personal(SAE)

5. [Save] をクリックし変更内容を保存します

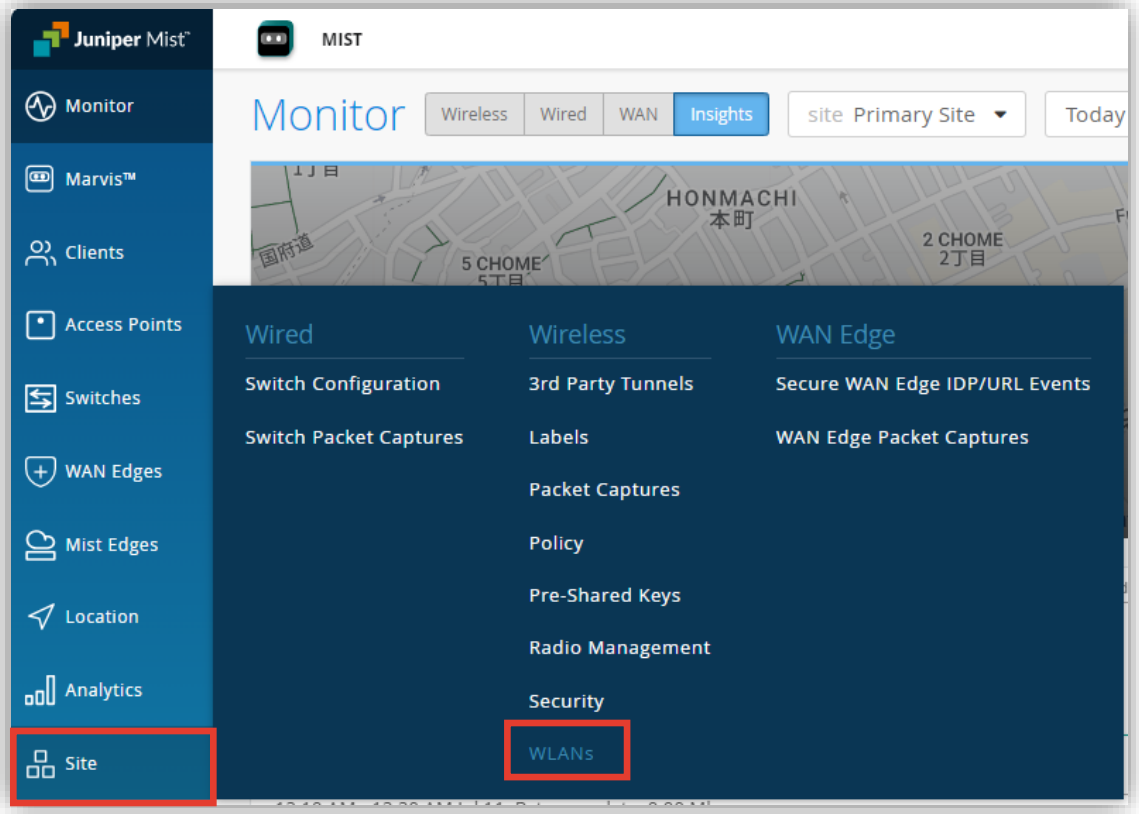


WPA3-Personal(SAE) マルチパスフレーズ

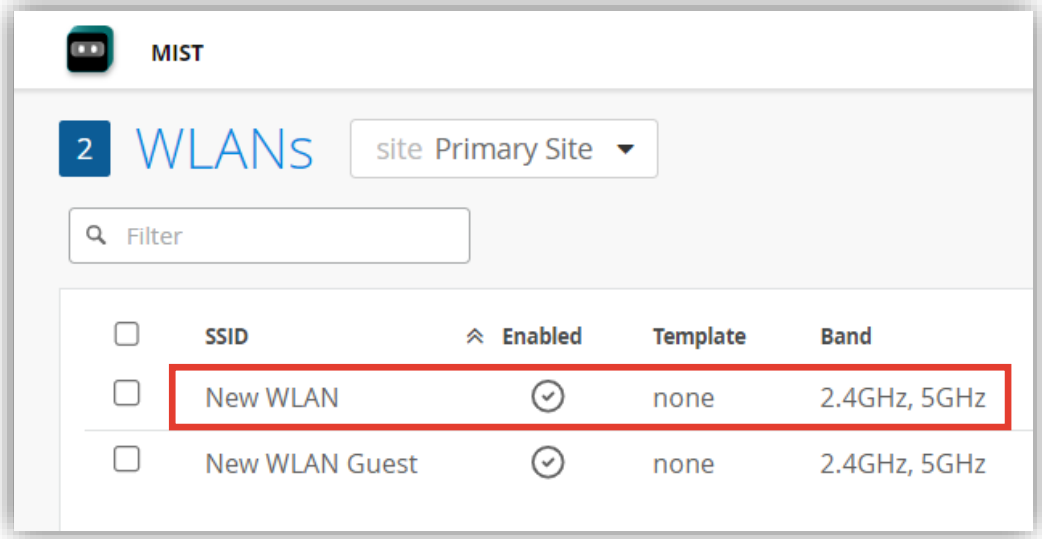
WPA3 の設定

WPA3-Personal(SAE) Multiple passphrase

1. [Site] から [WLANs] をクリックします



2. 編集する無線 LAN を選択します

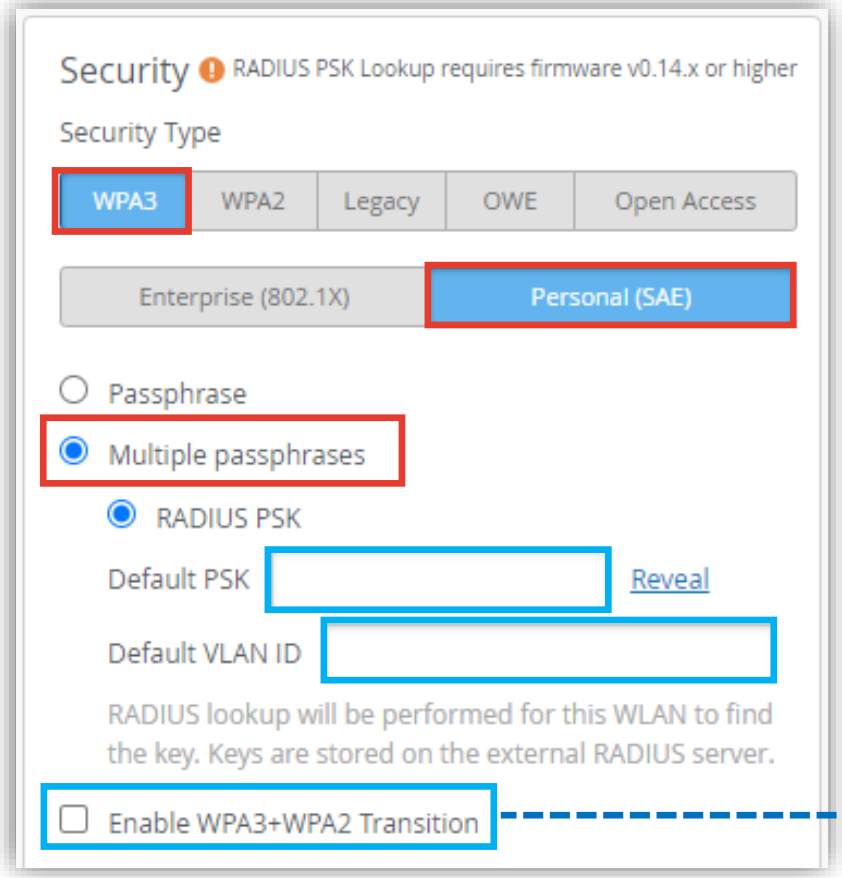


Organization > WLAN Template での設定も可能です

WPA3 の設定

WPA3-Personal(SAE) Multiple passphrase

3. [Security Type] で [WPA3] を選択、[Personal (SAE)] を選択し、[Multiple passphrases] を選択します
   - WPA3 に対応していないクライアントに対して WPA2 での接続を許可する場合、 [Enable WPA3-WPA2 Transition] をチェックして、移行モードを有効にします(Optional)



[WPA3] を選択します

[Personal (SAE)] を選択します

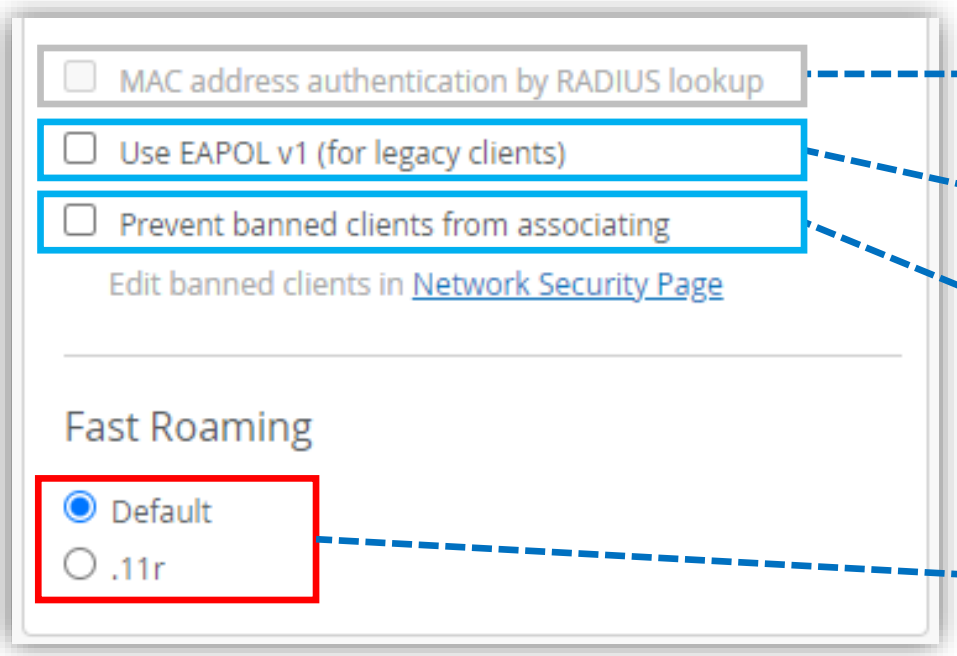
[Multiple passphrase] を設定します
- [Default PSK] を設定します(Optional)
- [Default VLAN ID] を設定します(Optional)

[Enable WPA3-WPA2 Transition] をチェックすると、移行モードが有効になります(Optional)

WPA3 の設定

WPA3-Personal(SAE) Multiple passphrase

4. その他オプション設定を確認します



Multi passphrase 選択時は、設定できません

[Use EAPOL v1(for legacy clients] をチェックすると、
eapol v1 を利用します

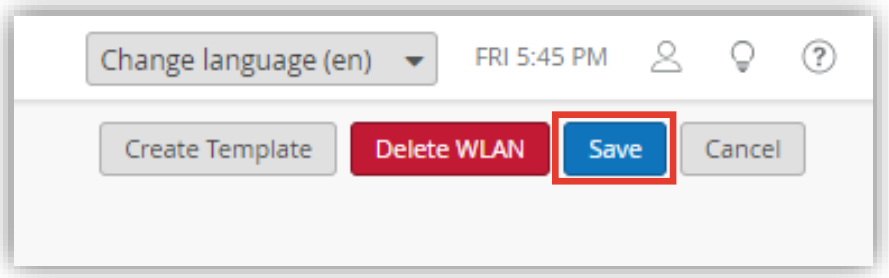
[Prevent banned clients from associating] をチェックすると、
Banned Clients に指定したクライアントのアソシエーションが制限されます
(Site > Security > View Client Classification で設定)

Roaming オプションを選択します

WPA3 の設定

WPA3-Personal(SAE) Multiple passphrase

5. [Save] をクリックし変更内容を保存します

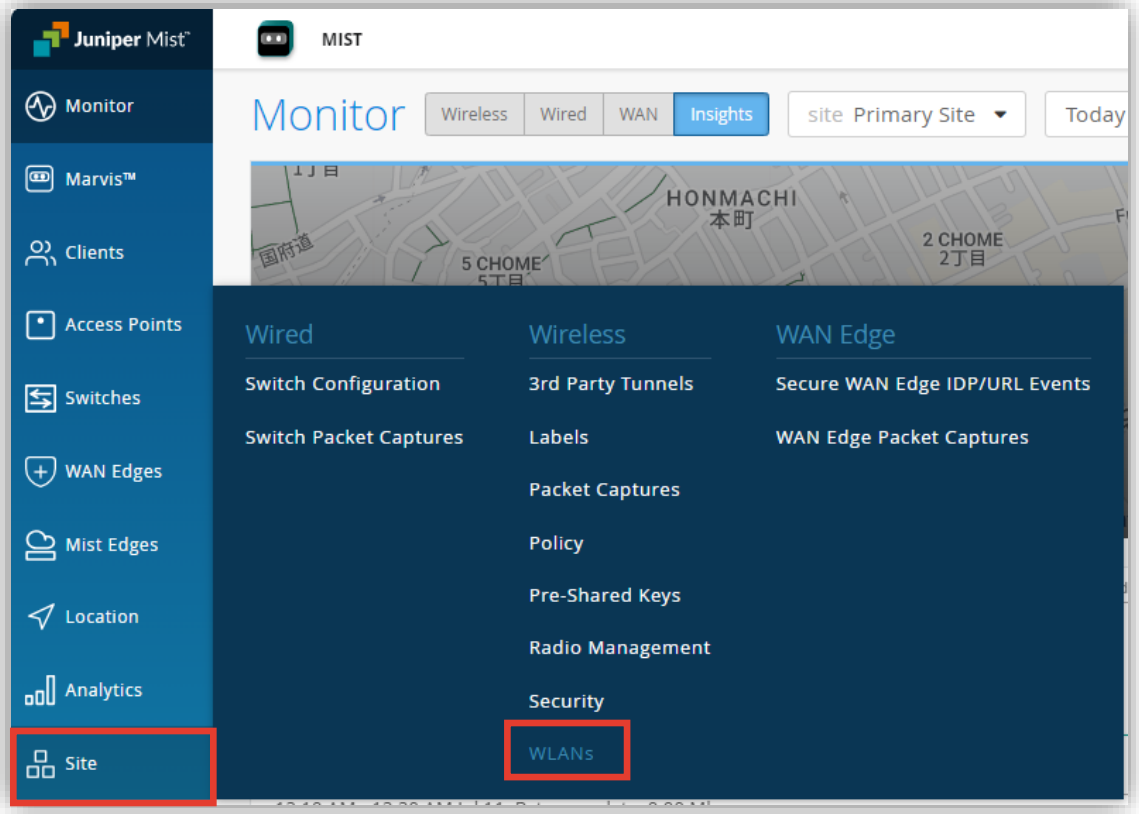


WPA3-Enterprise(802.1x)

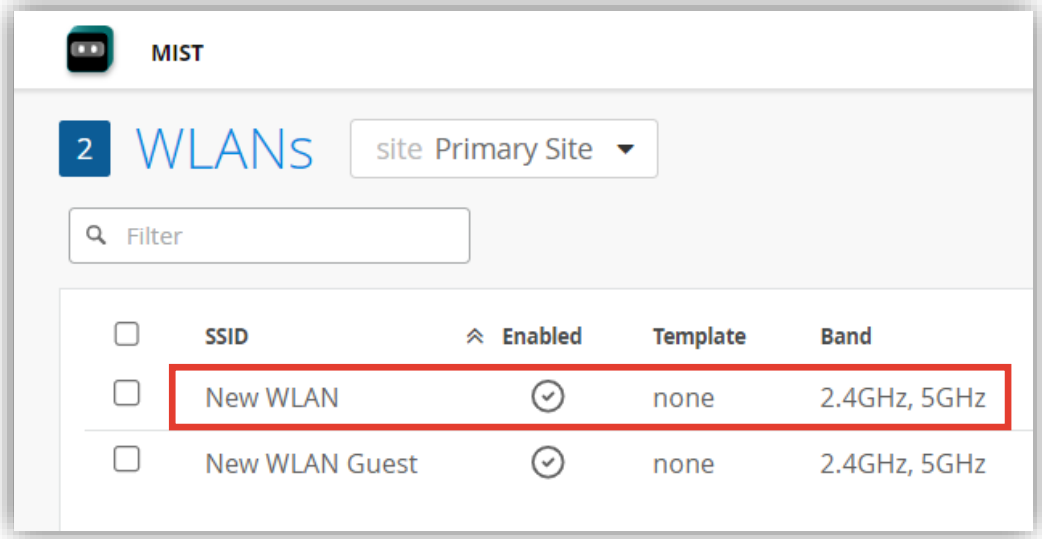
WPA3 の設定

WPA3-Enterpriese (802.1X)

1. [Site] から [WLANs] をクリックします



2. 編集する無線 LAN を選択します



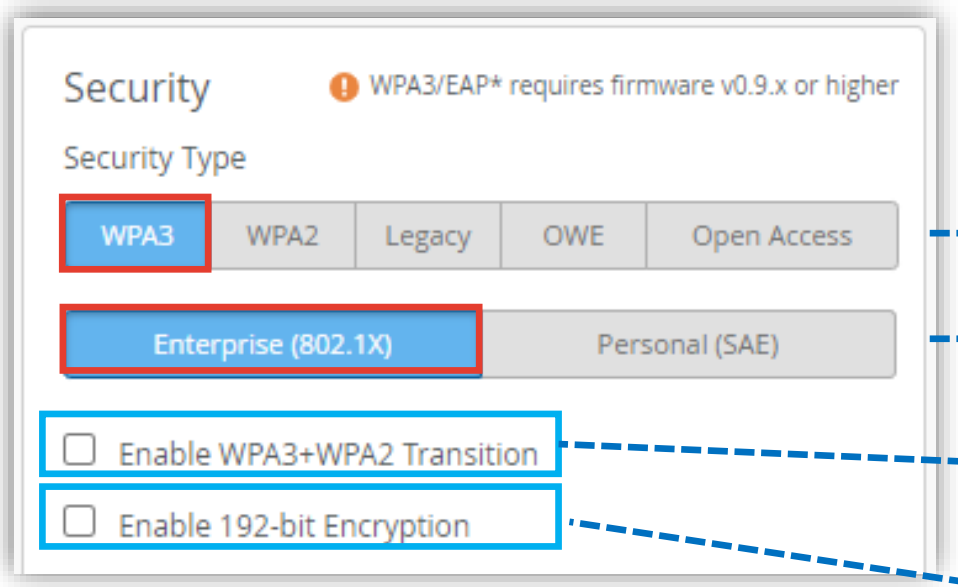
Organization > WLAN Template での設定も可能です

WPA3 の設定

WPA3-Enterpriese (802.1X)

3. [Security Type] で [WPA3] を選択、[Enterprise (802.1X)] を選択します (0.9.x 以上)
   - WPA3 に対応していないクライアントに対して WPA2 での接続を許可する場合、 [Enable WPA3-WPA2 Transition] をチェックして、移行モードを有効にします(Optional)
   - [Enable 192-bit Encryption] をチェックすると、192 bit モードの GCMP-256 暗号オプションを有効にします(Optional)

   ※ [Enable WPA3-WPA2 Transition] と [Enable 192-bit Encryption] は排他利用です



[WPA3] を選択します

[Enterprise (802.1X)] を選択します

[Enable WPA3-WPA2 Transition] をチェックすると、移行モードが有効になります(Optional)

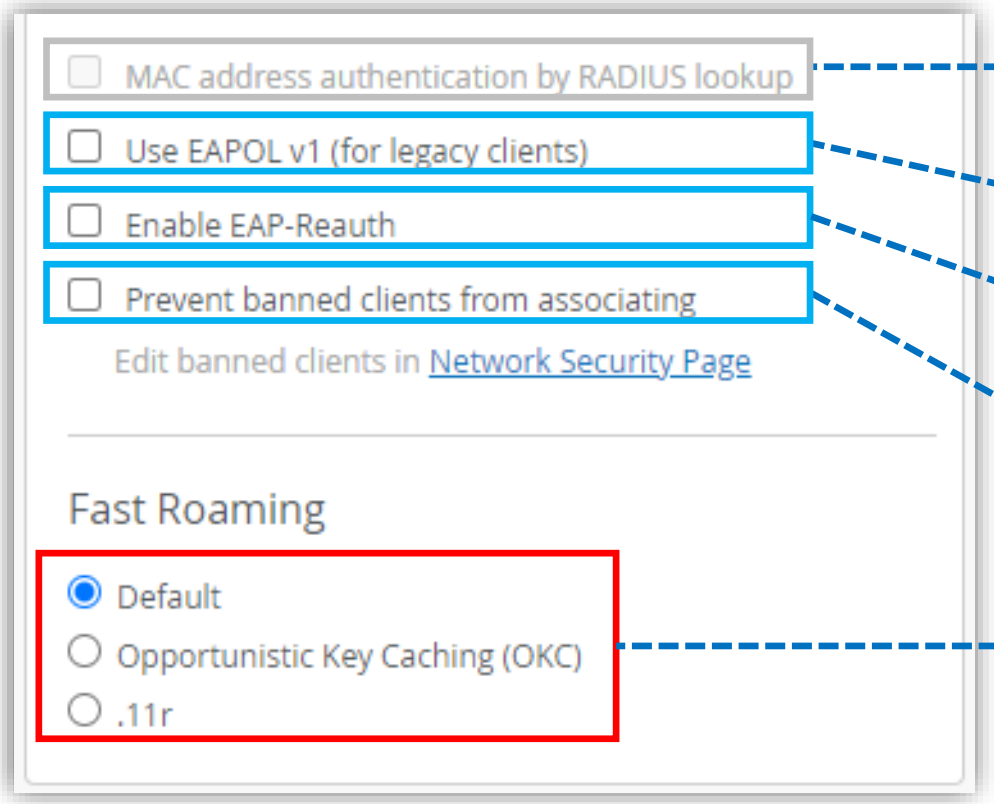
[Enable 192-bit Encryption] をチェックすると、192 bit モードの GCMP-256 暗号オプションを有効にします (0.14.x 以上)

排他利用

WPA3 の設定

WPA3-Enterpriese (802.1X)

4. その他オプション設定を確認します



Enterprise(802.1X) 選択時は、設定できません

[Use EAPOL v1(for legacy clients] をチェックすると、
eapol v1 を利用します

[Enable EAP-Reauth] をチェックすると、EAP 再認証を有効化します

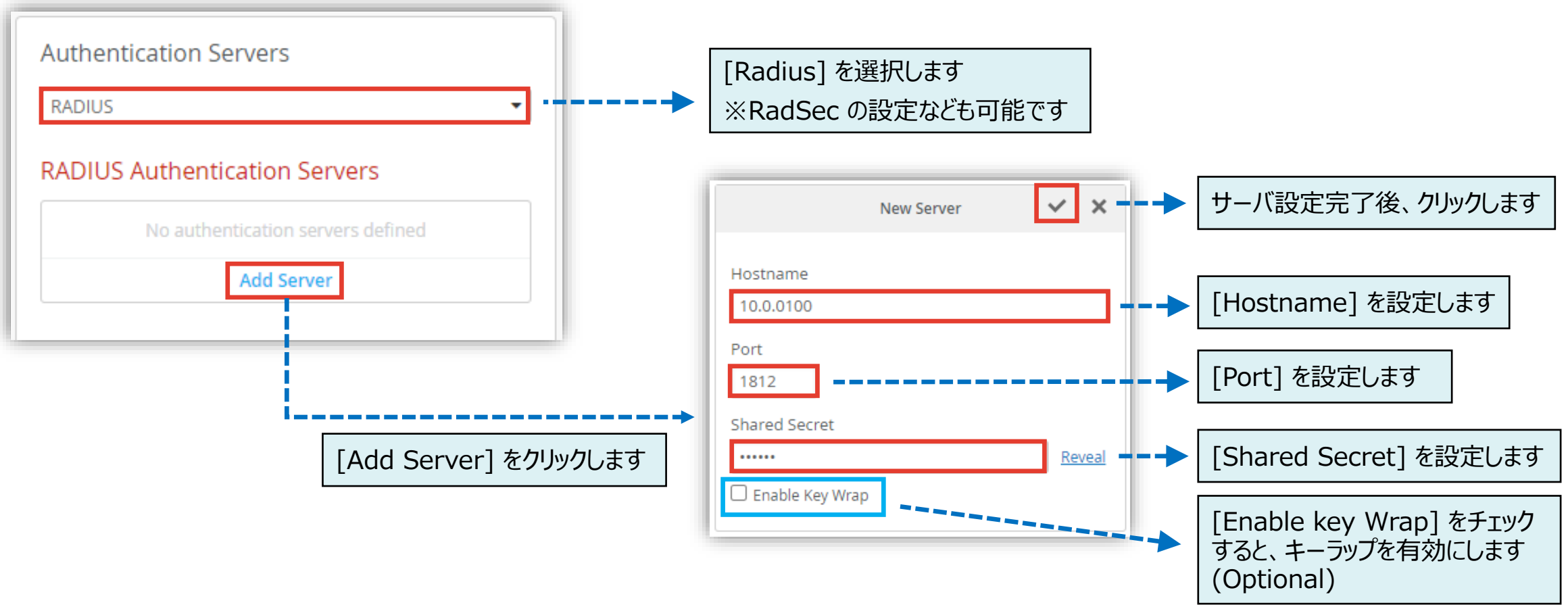
[Prevent banned clients from associating] をチェックすると、
Banned Clients に指定したクライアントのアソシエーションが制限されます
(Site > Security > View Client Classification で設定)

Roaming オプションを選択します
※ [Enable 192-bit Encryption] チェック時は、[Default] のみ

WPA3 の設定

WPA3-Enterpriese (802.1X)

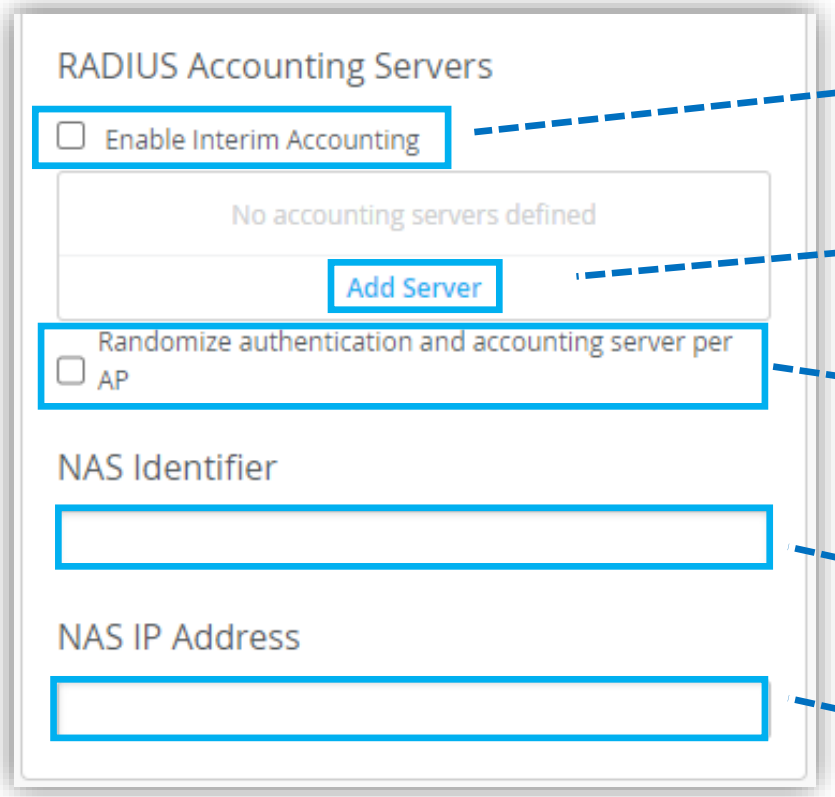
5. [Enterprise (802.1X)] を選択すると、[Authentication Servers] の項目が表示されます
   [Radius] を選択し、[Add Server] をクリックして、[Hostname]、[Port]、[Shared Secret] を設定します



WPA3 の設定

WPA3-Enterpriese (802.1X)

6. その他オプションを確認します



[Enable Interim Accounting] をクリックし、[Interim Accounting Interval] (60-600) を設定します(Optional)

[Add Server] をクリックし、[Radius Accounting Server] を設定します(Optional)

[Randomize authentication and accounting server per AP] をクリックすると、AP毎に Radius 認証/アカウンティングサーバがランダム化します(Optional)

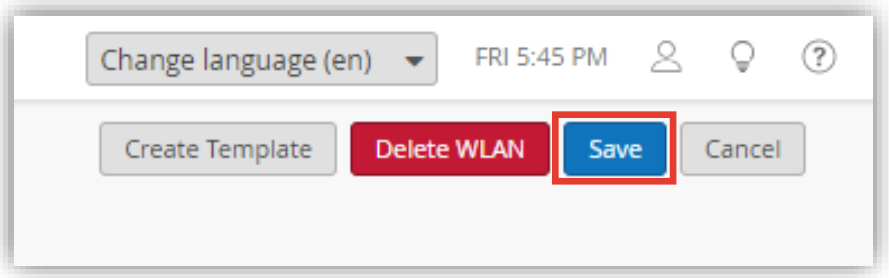
[NAS Identifier] を設定します(Optional)

[NAS IP Address] を設定します(Optional)

WPA3 の設定

WPA3-Enterpriese (802.1X)

7. [Save] をクリックし変更内容を保存します

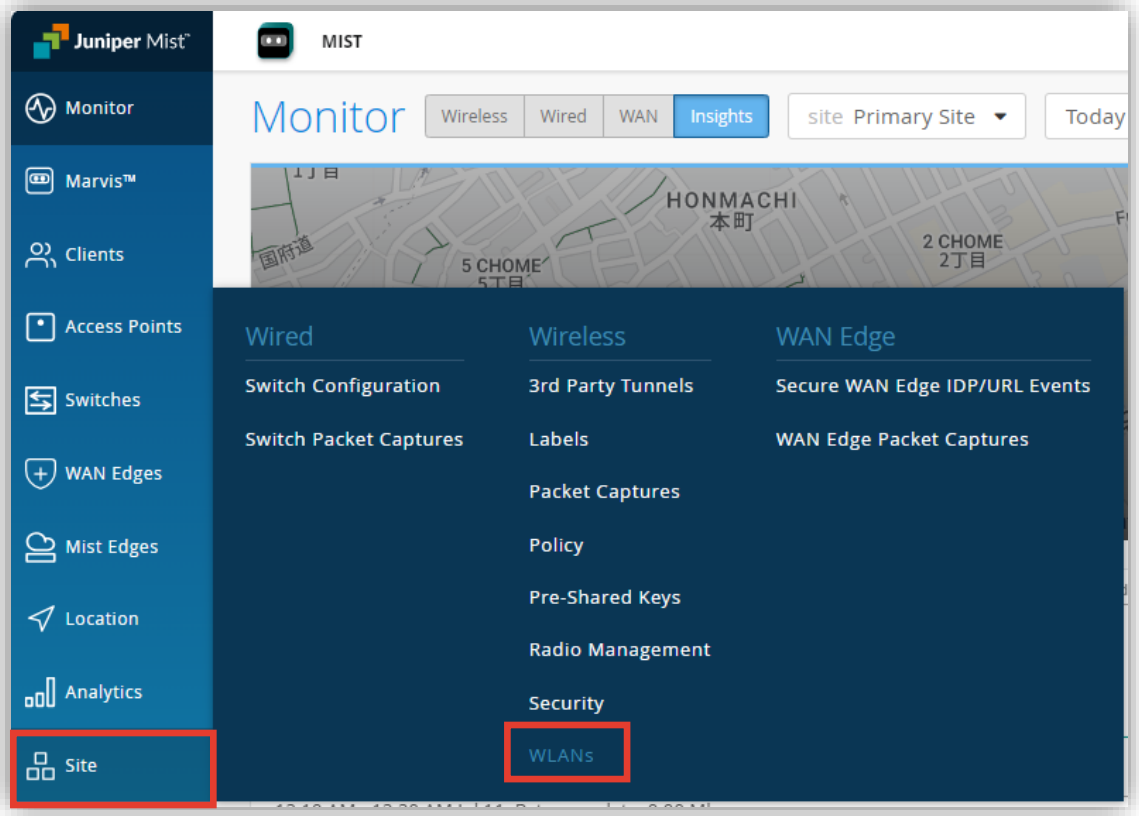


OWE(Opportunistic Wireless Encryption)

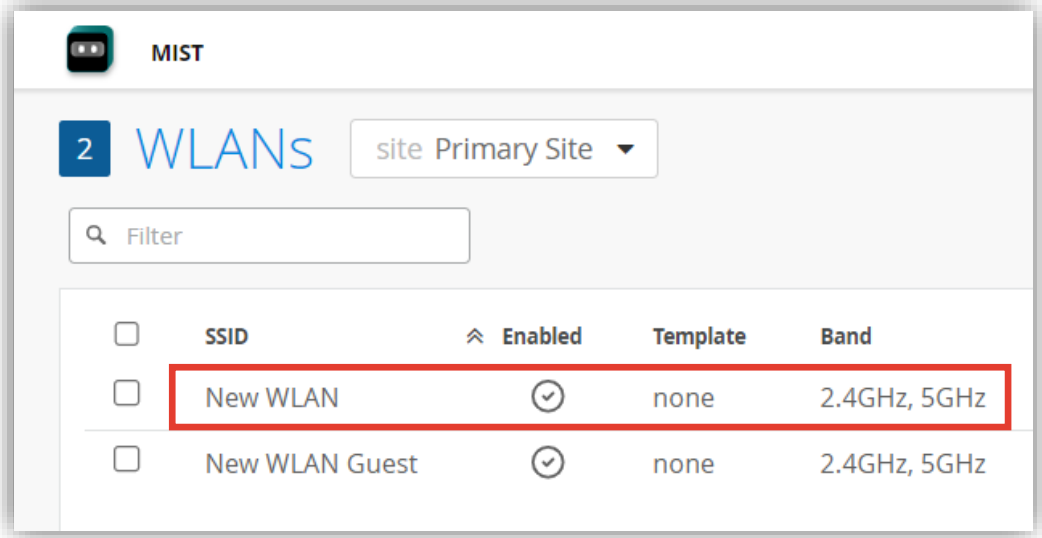
WPA3 の設定

OWE(Opportunistic Wireless Encryption)

1. [Site] から [WLANs] をクリックします



2. 編集する無線 LAN を選択します

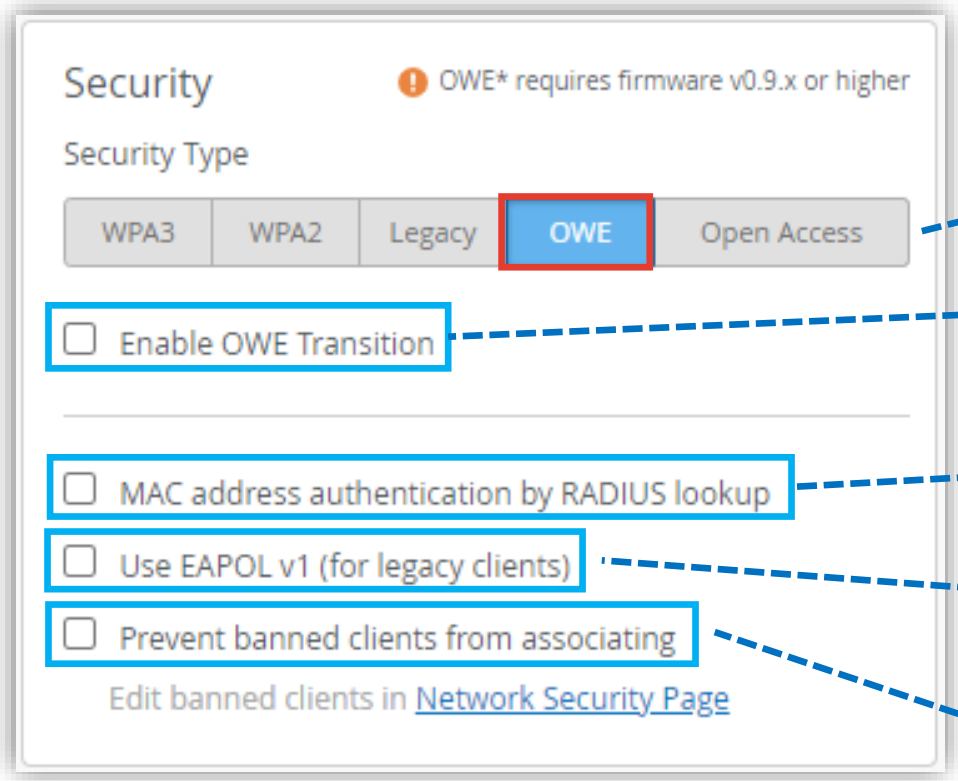


Organization > WLAN Template での設定も可能です

WPA3 の設定

OWE(Opportunistic Wireless Encryption)

3. [Security Type] で [OWE] を選択します(0.9.x 以上)
   [Enable OWE Transition] チェックして、移行モードを有効にします(Optional)
   ※ 移行モード選択時は、OWE での接続に対応していない端末は、OPEN(暗号化なし)での通信となります



[OWE] を選択します

[Enable OWE Transition] をチェックすると、
移行モードが有効になります(Optional)

[MAC address authentication by RADIUS lookup] をチェックすると、
Radius サーバを参照し、 MAC アドレス認証します

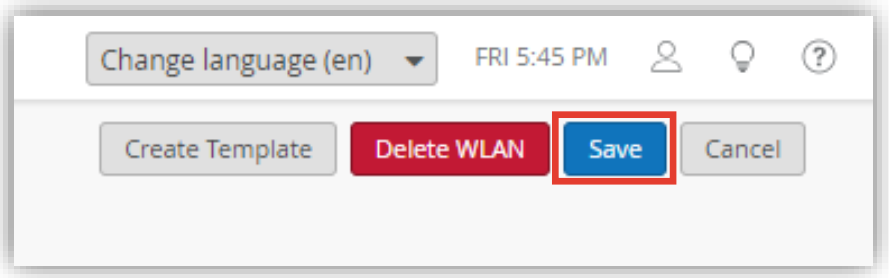
[Enable EAP-Reauth] をチェックすると、EAP 再認証が有効になります

[Prevent banned clients from associating] をチェックすると、
Banned Clients に指定したクライアントのアソシエーションが制限されます
(Site > Security > View Client Classification で設定)

WPA3 の設定

OWE(Opportunistic Wireless Encryption)

4. [Save] をクリックし変更内容を保存します



Appendix

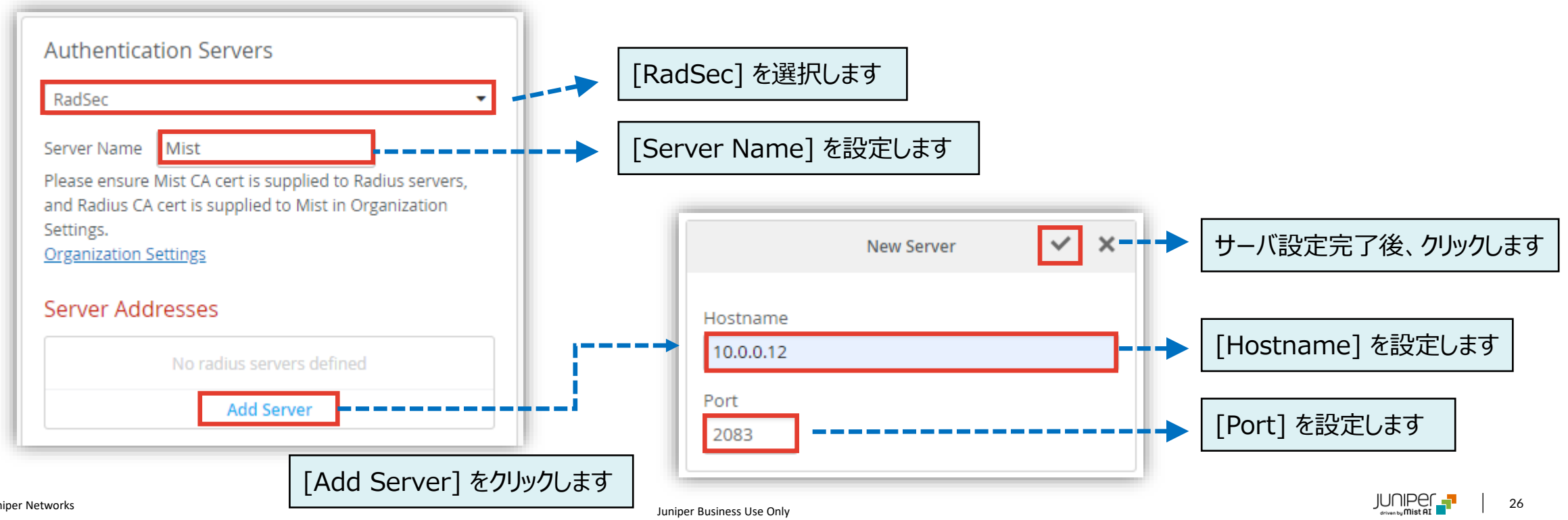
WPA3-Enterpise の設定オプション

WPA3-Enterpise の設定オプション

RadSec

RadSec は、RADIUS サーバーが TCP および TLS 経由でデータを転送してセキュリティを強化するプロトコルで、RADIUS パケットをパブリックネットワーク経由で転送すると同時に、トランスポート層を通じてエンドツーエンドのセキュリティを確保できます

1. [RadSec] を選択、[Server Name] を入力し、[Add Server] より、RadSec サーバを追加します
   [Hostname] と [Port] を設定します
   RadSec 設定時は、証明書の設定が必要になります(次ページ)

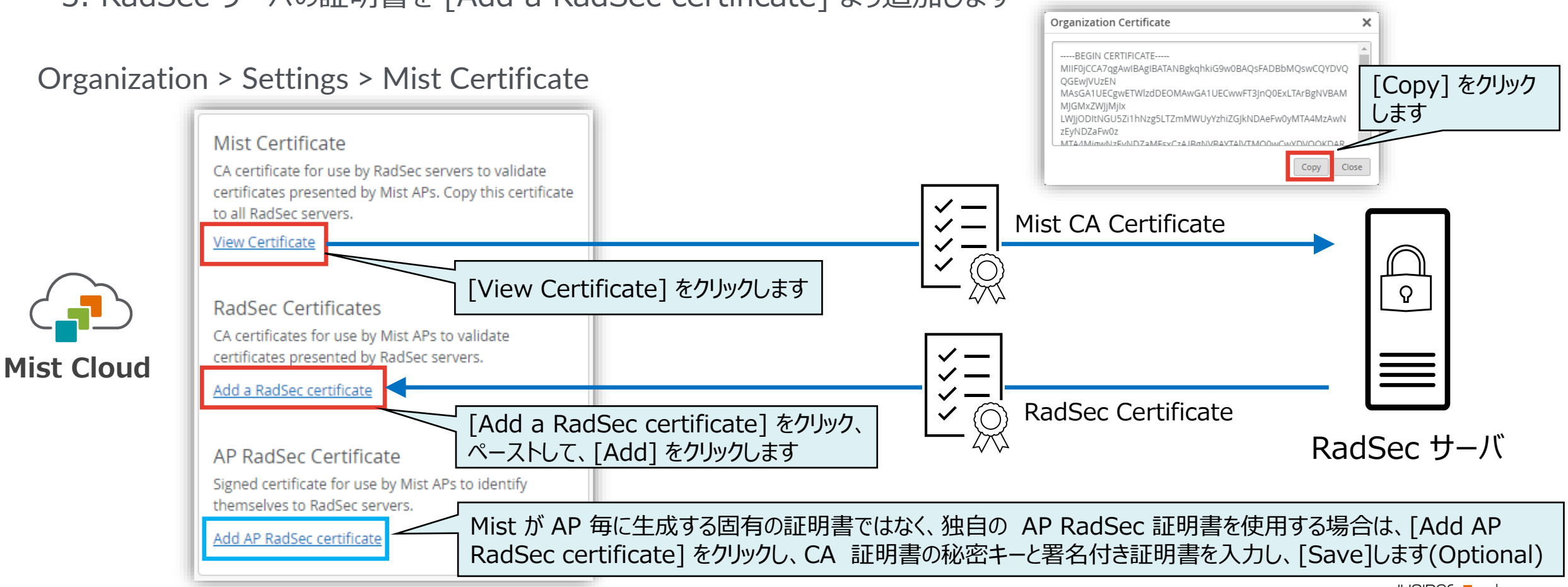


WPA3-Enterpise の設定オプション

RadSec

2. [Organization] > [Settings] > [Mist Certificate] より、[View Certificate] をクリック、証明書を [Copy] して RadSec サーバにインストールします
3. RadSec サーバの証明書を [Add a RadSec certificate] より追加します

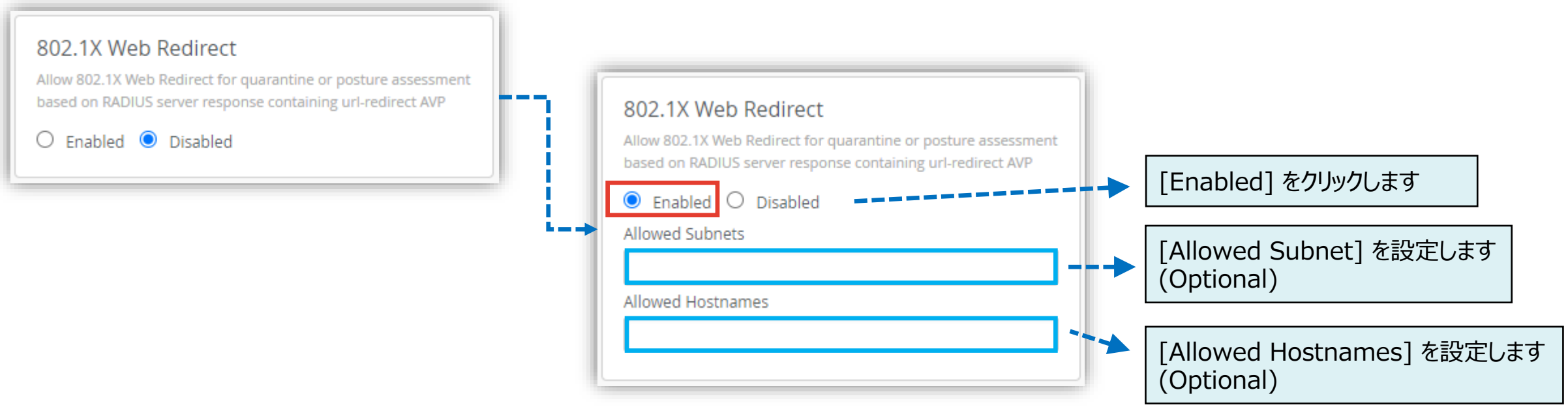
Organization > Settings > Mist Certificate



WPA3-Enterpise の設定オプション

802.1X Web Redirect

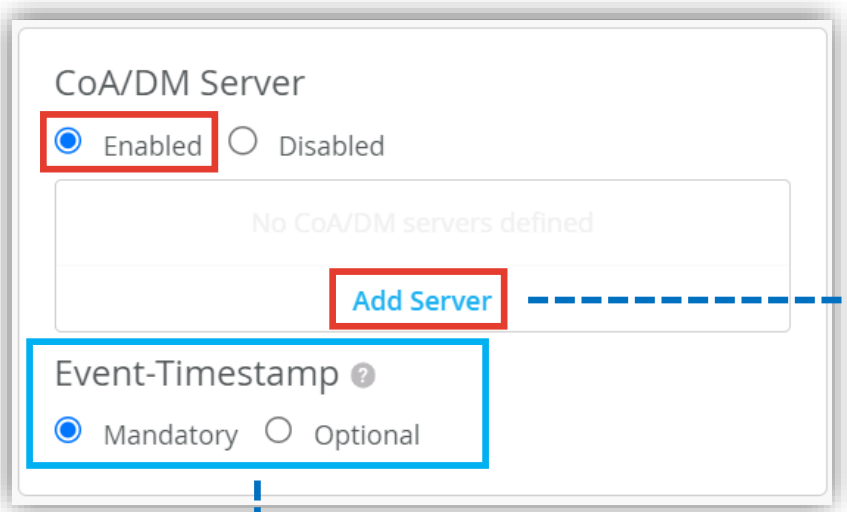
802.1X 認証が正常に完了した後、クライアントを特定の Web ページにリダイレクトすることができます
URL リダイレクト機能を使用して、エージェントがインストールされているクライアントのコンプライアンスチェックを実行します
RADIUS サーバは、URL-redirect を含む AVP(RADIUS 属性値ペア)を含む ACCESS-ACCEPT を送信し、クライアントを修復用の隔離ポータルに誘導します
この機能を有効にすると、クライアントは当初 DHCP/DNS、特定のサブネット、および 指定された リダイレクト URL に制限され、クライアントがリダイレクト URL で要求されたアクションを完了すると、完全に承認され、トラフィックの通過を開始できます

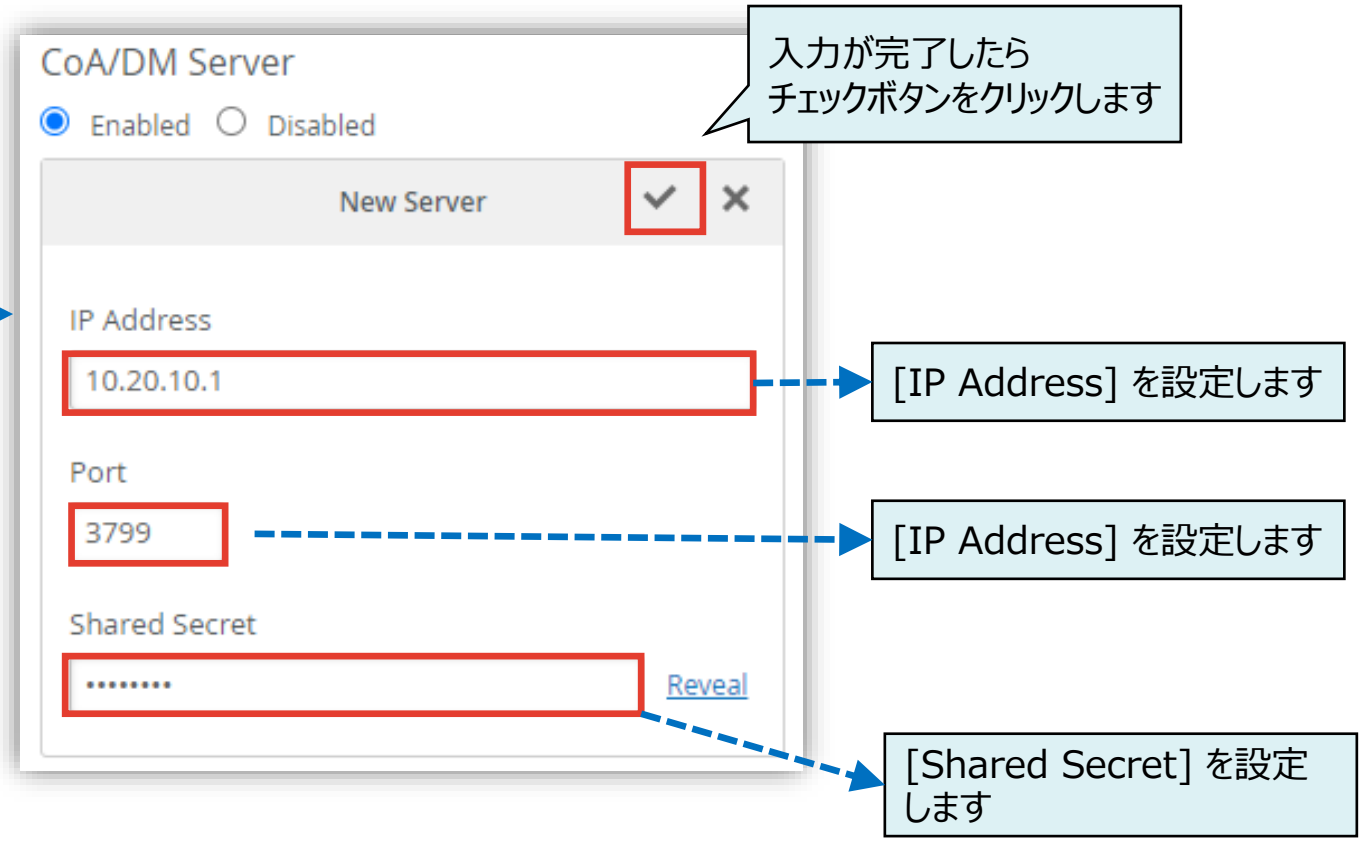


WPA3-Enterpise の設定オプション

CoA/DM サーバの設定

RFC 5176 で定義されている RADIUS の拡張 CoA を有効にする場合は、
[CoA/DM Server] の項目にて [Enabled] を選択し、[Add Server] からサーバの情報を入力します





- Event-Timestamp は RFC 5176 に定義された AVP (属性値ペア)です
- CoA に Event-Timestamp が含まれている場合は [Mandatory] を選択します
- [Mandatory] を選択した状態で、CoA に Event-Timestamp が含まれていない場合、CoA パケットが破棄されます

Thank you