

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

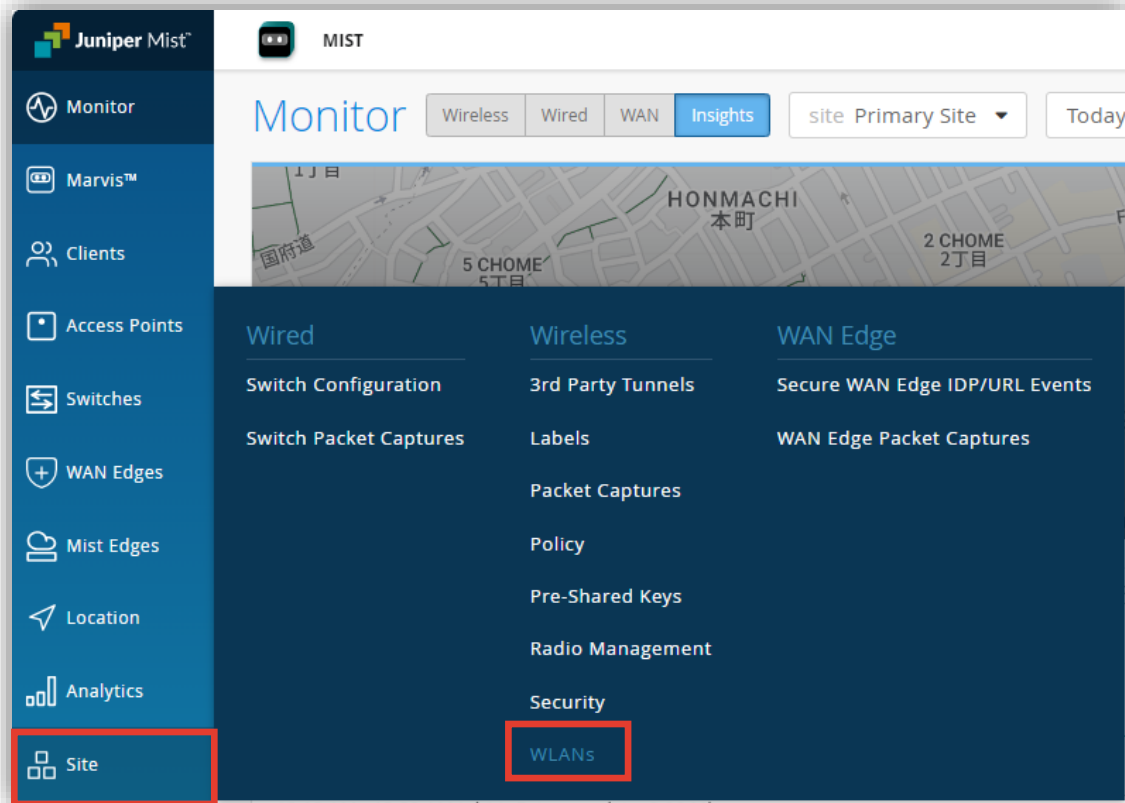
- WPA3 Personal(WPA3-SAE)
 - SAE(Simultaneous Authentication of Equals) による鍵交換
 - Transition モード有効時は、非対応端末は WPA2-PSK で接続 (MFP は任意)
- WPA3 Enterprise(WPA3-ENT/802.1x)
 - WPA2 Enterprise と互換性
 - Transition モード有効時は、非対応端末は WPA2 Enterprise で接続 (MFP は任意)
 - 192 bit モードの暗号オプションをサポート (WPA3 のみ、Fast Roaming 選択不可)
- 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)

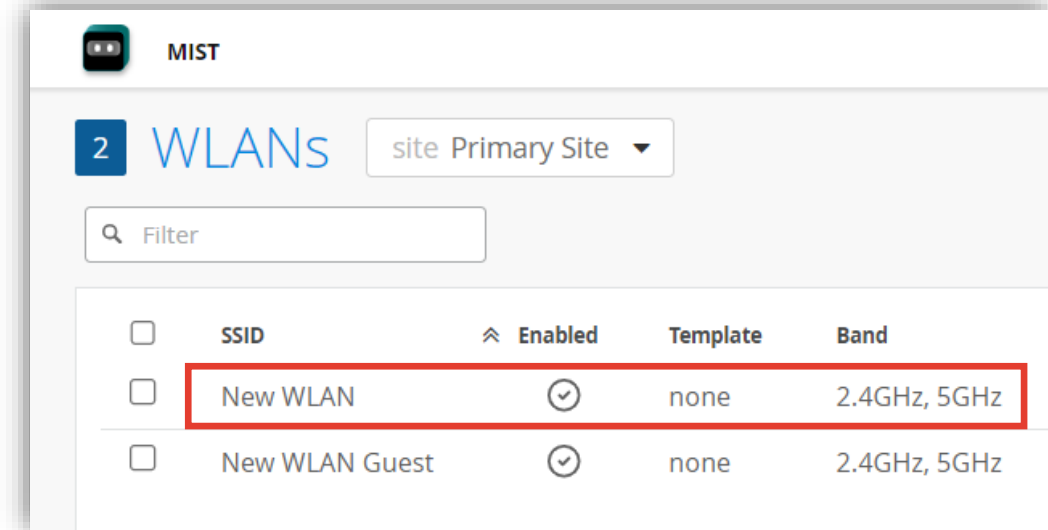
WPA3 の設定

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)

The screenshot shows the 'Security' configuration page. At the top, a warning icon and text state 'WPA3/SAE* requires firmware v0.8.x or higher'. Under 'Security Type', there are two rows of buttons. The first row contains 'WPA3', 'WPA2', 'Legacy', 'OWE', and 'Open Access'. The 'WPA3' button is highlighted with a red border. A dashed blue arrow points from this button to a callout box containing the text '[WPA3] を選択します'. The second row contains 'Enterprise (802.1X)' and 'Personal (SAE)'. The 'Personal (SAE)' button is highlighted with a red border. A dashed blue arrow points from this button to a callout box containing the text '[Personal (SAE)] を選択します'. Below the buttons, there are radio button options: 'Passphrase' (selected) and 'Multiple passphrases'. The 'Passphrase' option has a text input field with a red border containing a masked password and a 'Reveal' link. A dashed blue arrow points from this field to a callout box containing the text '[Passphrase] を設定します'. At the bottom, there is a checkbox labeled 'Enable WPA3+WPA2 Transition' which is currently unchecked. A dashed blue arrow points from this checkbox to a callout box containing the text '[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)'. The entire interface is enclosed in a light gray border.

WPA3 の設定

WPA3-Personal(SAE)

4. その他オプション設定を確認します

The screenshot shows the configuration page for WPA3-Personal(SAE). It features three unchecked checkboxes: 'MAC address authentication by RADIUS lookup', 'Use EAPOL v1 (for legacy clients)', and 'Prevent banned clients from associating'. Below these is a link 'Edit banned clients in Network Security Page'. The 'Fast Roaming' section has two radio buttons: 'Default' (selected) and '.11r'. Blue dashed arrows point from the first three checkboxes to explanatory text boxes on the right. A red box highlights the 'Default' radio button, with a blue dashed arrow pointing to a text box below.

[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

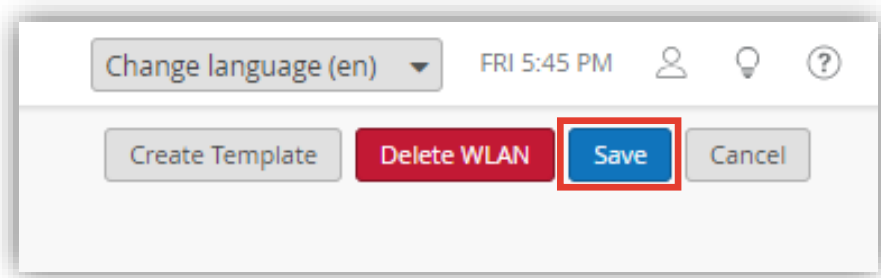
[Prevent banned clients from associating] をチェックすると、Banned Clients に指定したクライアントのアソシエーションが制限されます (Site > Security > View Client Classification で設定)

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

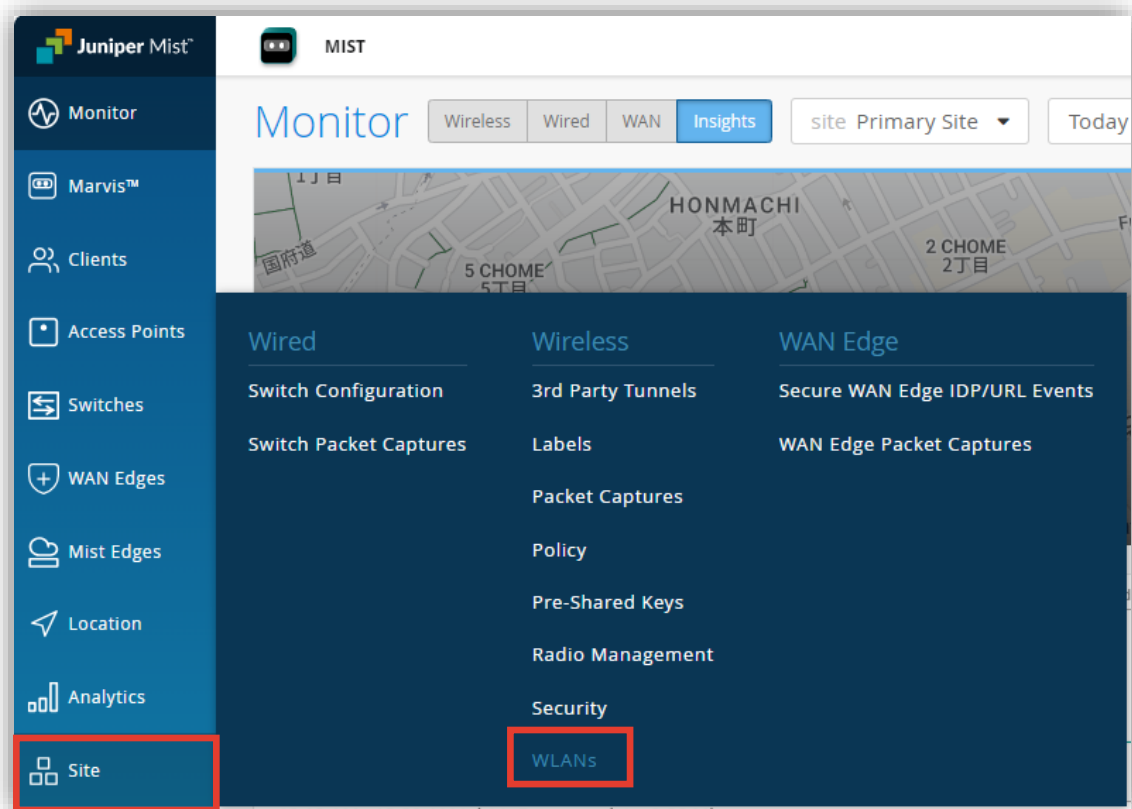


WPA3-Personal(SAE) マルチパスフレーズ

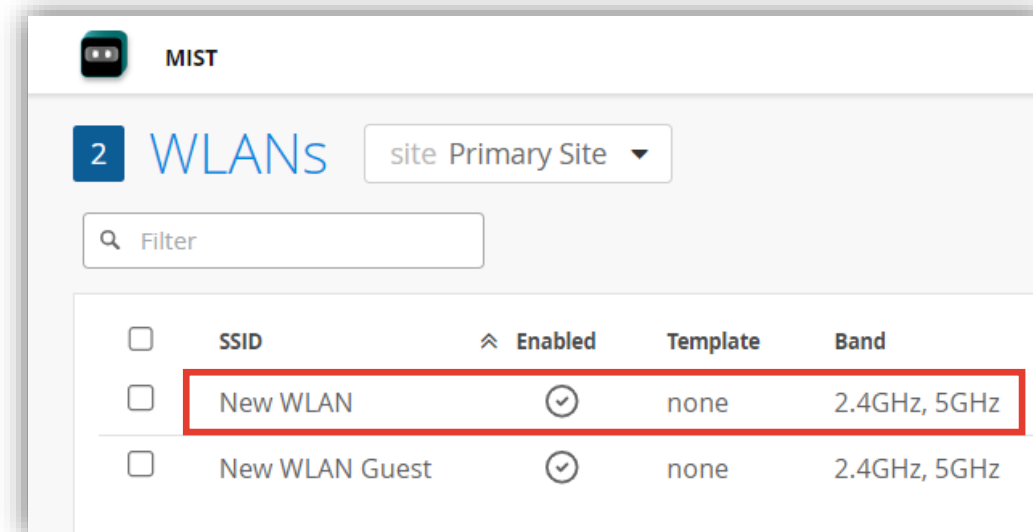
WPA3 の設定

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)

The screenshot shows the configuration page for WPA3. At the top, there is a warning: "Security RADIUS PSK Lookup requires firmware v0.14.x or higher". Under "Security Type", the "WPA3" button is highlighted with a red box. Below it, the "Personal (SAE)" button is also highlighted with a red box. In the "Passphrase" section, the "Multiple passphrases" radio button is selected and highlighted with a red box. Below this, there are input fields for "Default PSK" and "Default VLAN ID", both highlighted with blue boxes. At the bottom, the "Enable WPA3+WPA2 Transition" checkbox is highlighted with a blue box.

[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

The screenshot shows a configuration page for WPA3-Personal(SAE) Multiple passphrase. It features several checkboxes and a radio button group. Blue dashed arrows point from the checkboxes to explanatory text boxes on the right. A red box highlights the radio button group.

- MAC address authentication by RADIUS lookup
- Use EAPOL v1 (for legacy clients)
- Prevent banned clients from associating
[Edit banned clients in Network Security Page](#)

Fast Roaming

- Default
- .11r

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

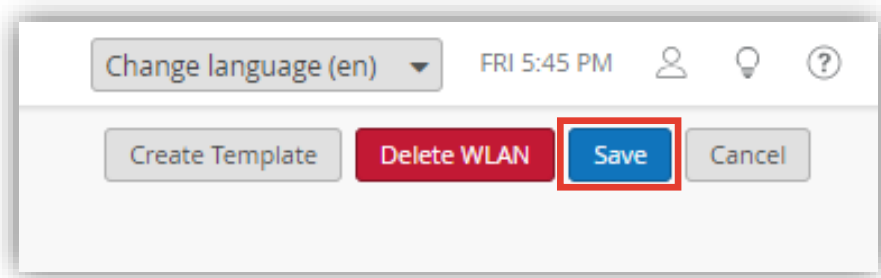
[Prevent banned clients from associating] をチェックすると、Banned Clients に指定したクライアントのアソシエーションが制限されます (Site > Security > View Client Classification で設定)

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

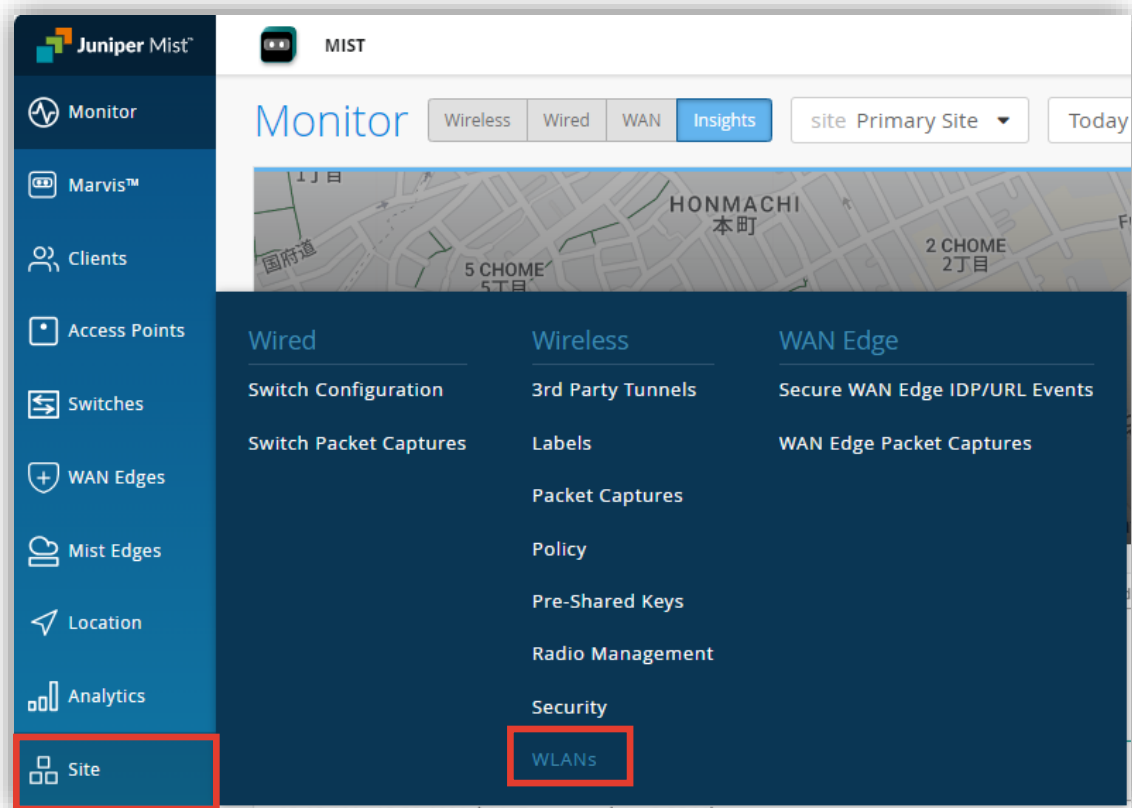


WPA3-Enterprise(802.1x)

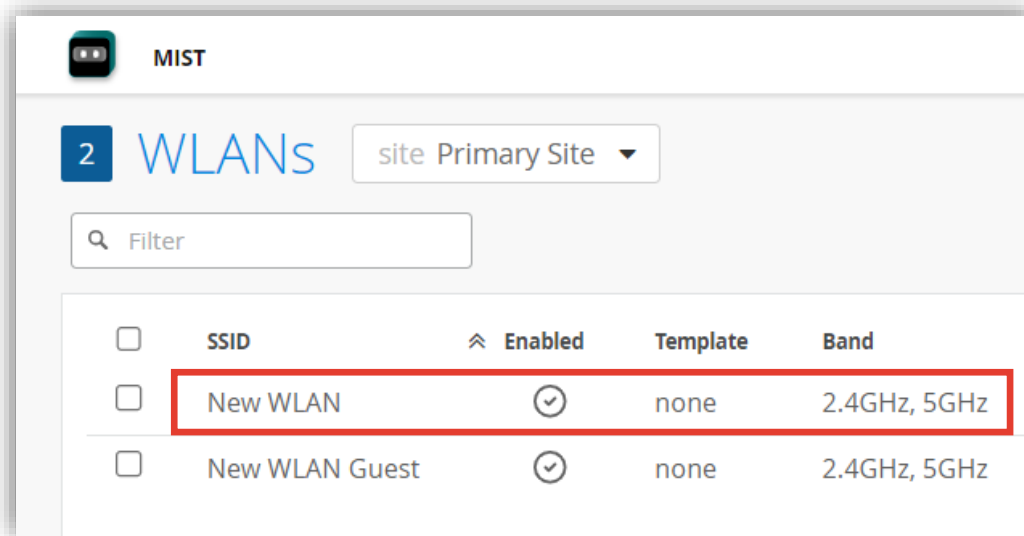
WPA3 の設定

WPA3-Enterprise (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-Enterprise (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

Security ! WPA3/EAP* requires firmware v0.9.x or higher

Security Type

WPA3 WPA2 Legacy OWE Open Access

Enterprise (802.1X) Personal (SAE)

Enable WPA3+WPA2 Transition

Enable 192-bit Encryption

[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-Enterprise (802.1X)

4. その他オプション設定を確認します

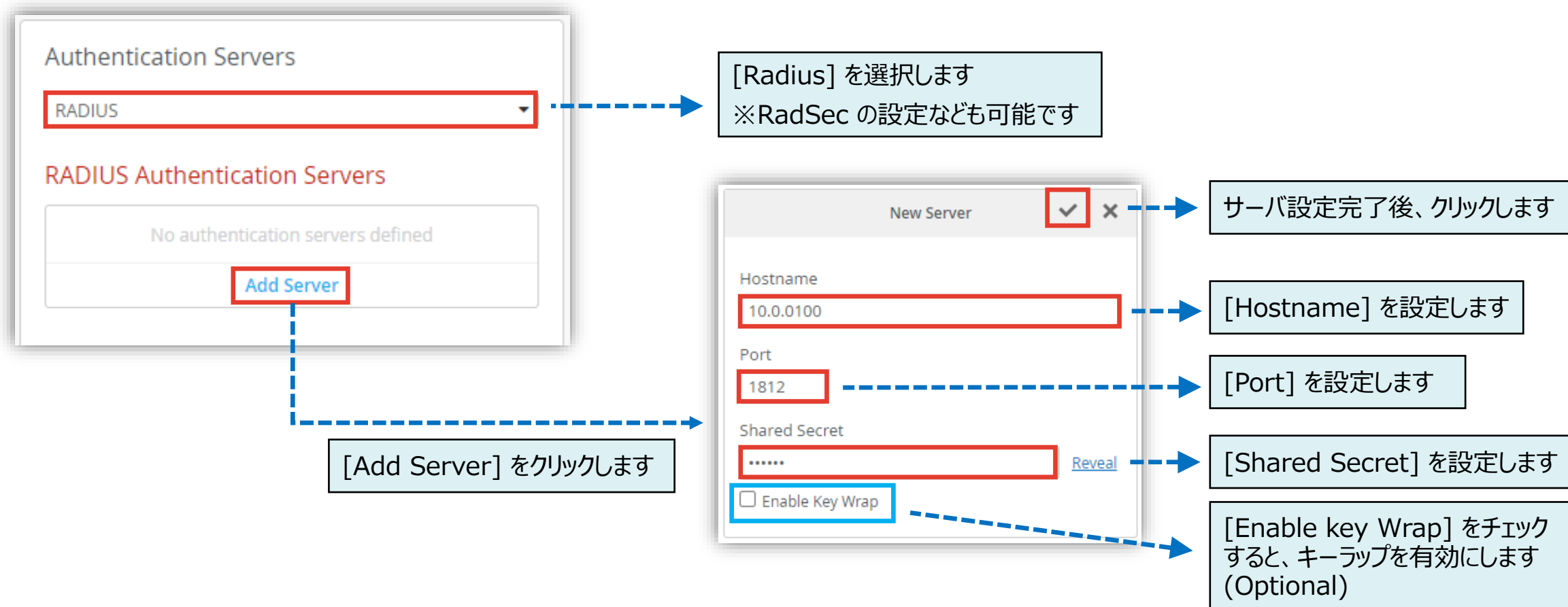
The screenshot shows the configuration page for WPA3-Enterprise (802.1X). The following options are highlighted with callouts:

- MAC address authentication by RADIUS lookup: Enterprise(802.1X) 選択時は、設定できません
- Use EAPOL v1 (for legacy clients): [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: [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: [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)
- Fast Roaming options: 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
 - Default
 - Opportunistic Key Caching (OKC)
 - .11r

WPA3 の設定

WPA3-Enterprise (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-Enterprise (802.1X)

6. その他オプションを確認します

RADIUS Accounting Servers

Enable Interim Accounting

No accounting servers defined

Add Server

Randomize authentication and accounting server per AP

NAS Identifier

NAS IP Address

[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)

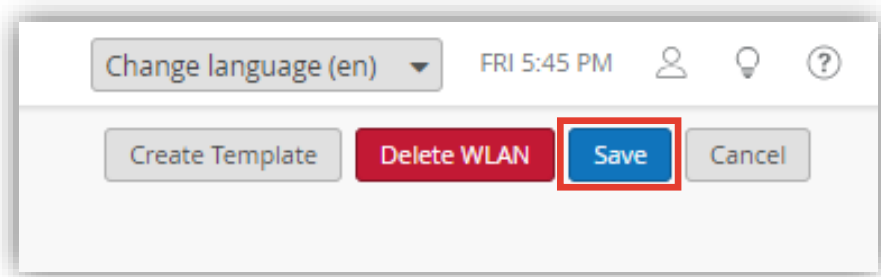
[NAS Identifier] を設定します(Optional)

[NAS IP Address] を設定します(Optional)

WPA3 の設定

WPA3-Enterprise (802.1X)

7. [Save] をクリックし変更内容を保存します

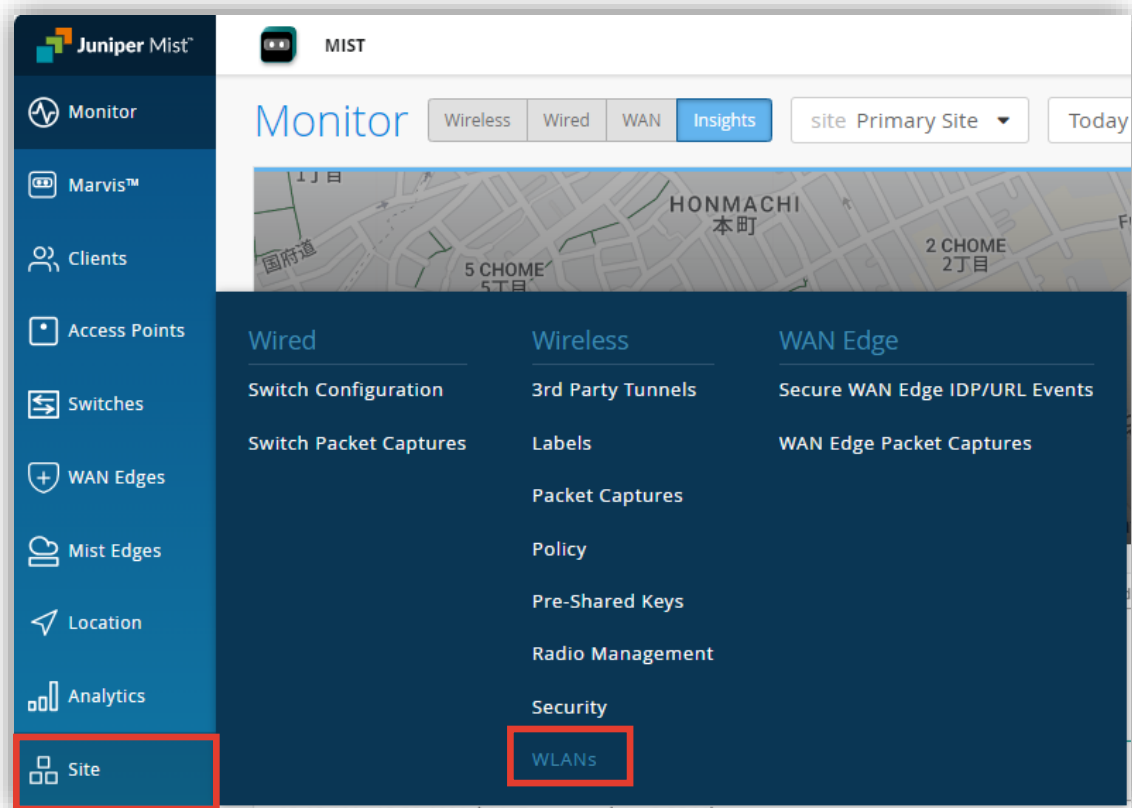


OWE(Oppportunistic Wireless Encryption)

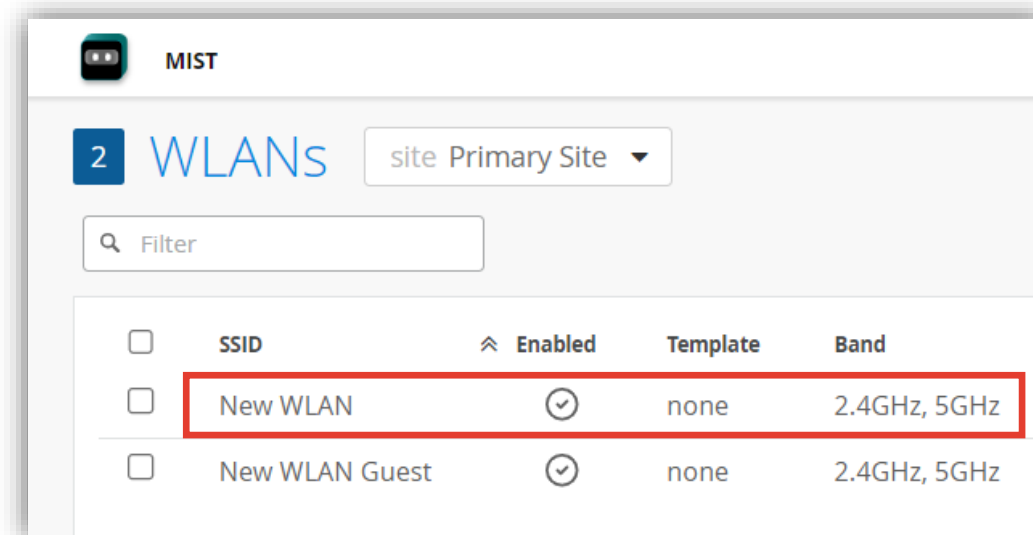
WPA3 の設定

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

Security ! OWE* requires firmware v0.9.x or higher

Security Type

WPA3 WPA2 Legacy **OWE** Open Access

Enable OWE Transition

MAC address authentication by RADIUS lookup

Use EAPOL v1 (for legacy clients)

Prevent banned clients from associating

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

[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

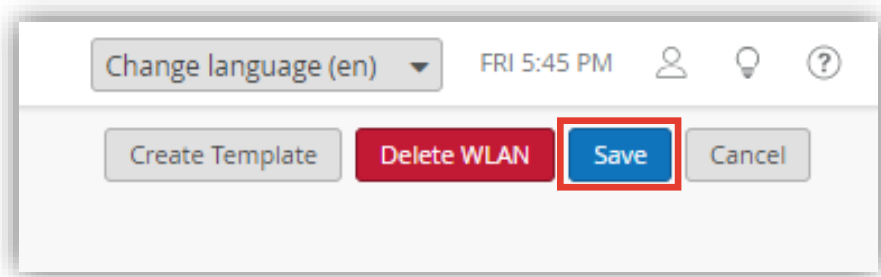
[Enable EAP-Reauth] をチェックすると、EAP 再認証が有効になります

[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-Enterprise の設定オプション

WPA3-Enterprise 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)

The image shows a two-step process for adding a RadSec server. The first step is in the 'Authentication Servers' configuration page. A dropdown menu is set to 'RadSec', and the 'Server Name' field contains 'Mist'. A red box highlights the 'Add Server' button. The second step is a 'New Server' dialog box where the 'Hostname' is set to '10.0.0.12' and the 'Port' is set to '2083'. A checkmark in a red box indicates the server is successfully added.

[RadSec] を選択します

[Server Name] を設定します

[Add Server] をクリックします

サーバ設定完了後、クリックします

[Hostname] を設定します

[Port] を設定します

WPA3-Enterprise 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



Mist Certificate
CA certificate for use by RadSec servers to validate certificates presented by Mist APs. Copy this certificate to all RadSec servers.

[View Certificate](#)

RadSec Certificates
CA certificates for use by Mist APs to validate certificates presented by RadSec servers.

[Add a RadSec certificate](#)

AP RadSec Certificate
Signed certificate for use by Mist APs to identify themselves to RadSec servers.

[Add AP RadSec certificate](#)

[View Certificate] をクリックします

[Add a RadSec certificate] をクリック、ペーストして、[Add] をクリックします

Mist が AP 毎に生成する固有の証明書ではなく、独自の AP RadSec 証明書を使用する場合は、[Add AP RadSec certificate] をクリックし、CA 証明書の秘密キーと署名付き証明書を入力し、[Save] します (Optional)

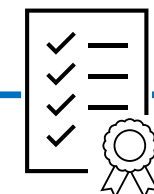
```
-----BEGIN CERTIFICATE-----
MIIF0jCCA7qgAwIBAgIBATANBgkqhkiG9w0BAQsFADBbMQswCQYDVQ
QGEwJlVUZEN
MA5GA1UECgwETWlzdDEOMAwGA1UECwwFT3JnQ0ExLTArBgNVBAM
MjJGMxZWJjMjIx
LWJjODItNGU5Zi1hNzg5LTZmMWUyYzhiZGJkNDAAeFw0yMTA4MzAwN
zEyNDZaFw0z
MTA4MjMwMjEzFw0zMDZaMFEyCzAIBRNVBAVTAiMjMOQWwCwYDVQ
QDAB
```

[Copy] Close

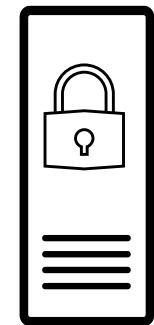
[Copy] をクリック します



Mist CA Certificate



RadSec Certificate

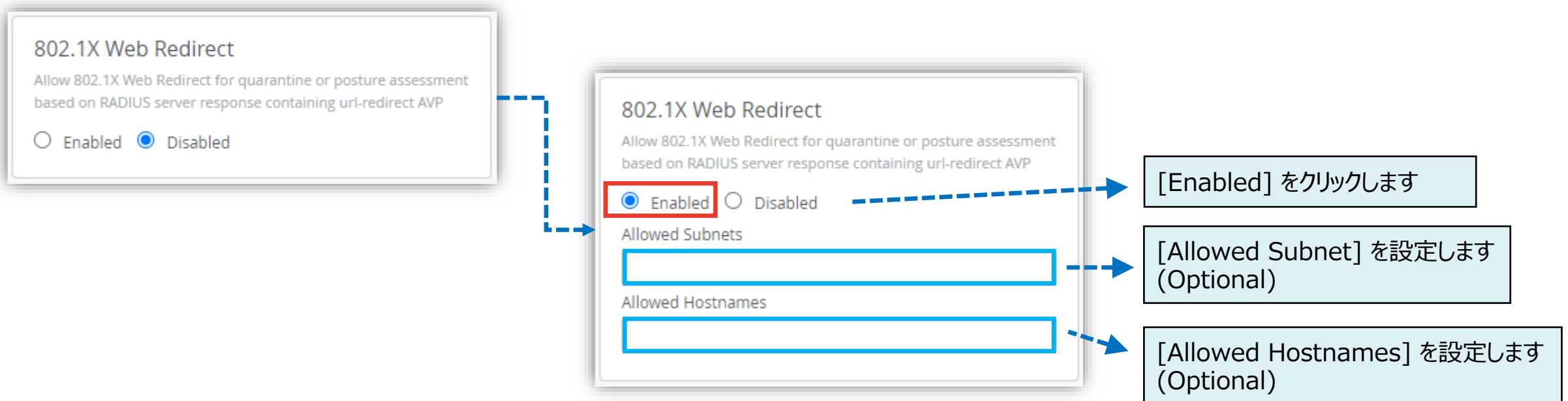


RadSec サーバ

WPA3-Enterprise 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-Enterprise 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

CoA/DM Server

Enabled Disabled

No CoA/DM servers defined

Add Server

Event-Timestamp ?

Mandatory Optional

CoA/DM Server

Enabled Disabled

New Server

IP Address

10.20.10.1

Port

3799

Shared Secret

..... [Reveal](#)

入力が完了したら
チェックボタンをクリックします

[IP Address] を設定します

[IP Address] を設定します

[Shared Secret] を設定
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

JUNIPER
driven by Mist AI 