

2023年6月8日リリース Mist 新機能のご紹介

ジュニパーネットワークス株式会社

JUNIPER 
driven by Mist AI

はじめに

- ❖ 本ドキュメントは以下のリリースノートを抄訳したものです

<https://www.mist.com/documentation/june-8th-2023-updates/>

- ❖ 本ドキュメントは2023年6月時点のMist cloudのGUIを使用しております
- ❖ 実際の画面と表示が異なる場合がございます
- ❖ 内容について不明な点、ご質問等がございましたら担当営業までお問い合わせください

本リリースで追加された機能一覧

Wired Assurance

- スイッチのGroup Based Policy機能
- スイッチのソフトウェアアップグレード手順の最適化

Simplified Operations

- ポートUp/Down通知
- Premium AnalyticsでのSSOサポート
- SiteレベルPSKのImport/Exportオプション
- MSPポータルの改良
- アセット位置情報トラッキング精度の向上
- ゲストアクセスのWPA3セキュリティモード
- デバイスプロファイルの検索フィルタ機能

WAN Assurance

- SSR/SRXのApp-IDデータベースインストール時のスケジュール機能

Wired Assurance

スイッチのGroup Based Policy機能

- キャンパスファブリックIP Closのデプロイ時にスイッチにGroup Based Policy（以下GBP）を設定、適用することができます
- GBPは実際のネットワークポロジに依存せず、より実用的なネットワークアクセスポリシーを作成することにより、ネットワークのマイクロセグメンテーションを可能とします
- GBPタグを用いたユーザやリソースをグループ化、ユーザのアクセス制御をすることにより、場所に依存しないエンドポイントのアクセス管理、一貫性のあるセキュリティポリシーの適用が可能となります
- Junos 22.4R1以降のバージョンを搭載した以下の機器で本機能を使用できます
 - EX4400、EX4100、EX4650、QFX5120-32C、QFX5120-48Y
- GBPは以下のいずれかの画面より設定可能です
 - スイッチコンフィグレーションテンプレート（Organization > Switch Templates）（左図）
 - スイッチダッシュボード（Switches > スイッチ名）

Switch Policy Labels BETA

GROUP BASED POLICY TAGS

NAME	TYPE	FROM	VALUE	GBP TAG
Employee	Dynamic	--	--	200
Contractor	Dynamic	--	--	300
Guest	Static	Network	vlan1033	1033
AWS-Server	Static	Subnets	54.10.0.0/16	400
Desktop1	Static	Subnets	10.99.99.99	99
Developers	Static	Network	vlan1088	1088
hackers?	Static	Subnets	10.99.99.99	99

Switch Policy BETA

SWITCH POLICY

NO.	NAME	USER/GROUP	RESOURCE
1	Desktops	Desktop2	Desktop3, Desktop1
2	Switch Policy 3	Employee	Guest, Contractor, All Resources, Desktop2
3	Switch Policy 2	Contractor	Developers, Employee, Guest, AWS-Server, All Resources
4	Switch Policy 4	Guest	Employee, Contractor, All Resources, Developers

スイッチのソフトウェアアップグレード手順の最適化

- 以下の機器のソフトウェアアップグレード時に発生するソフトウェアイメージダウンロード手順を最適化しました
 - Junos 20.4以降のバージョンで起動しているJuniper EX 2300、3400、4100、4300、4400
- この最適化により、ソフトウェアイメージをダウンロードする速度が向上します
- この変更を利用するために、以下のURLをファイアウォールの許可リストに追加ください
 - `cdn.juniper.net` (TCP 443)
- ファイアウォールで許可するポートの一覧については以下のページもご覧ください
 - [Ports to enable on your firewall – Mist](#)

Simplified Operations

ポートUp/Down通知

New Port Range

Invalid port ID range

Port Aggregation

Allow switch port operator to modify port profile

Yes No

Port IDs

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Configuration Profile

AP default(1), trunk, edge

Enable Dynamic Configuration

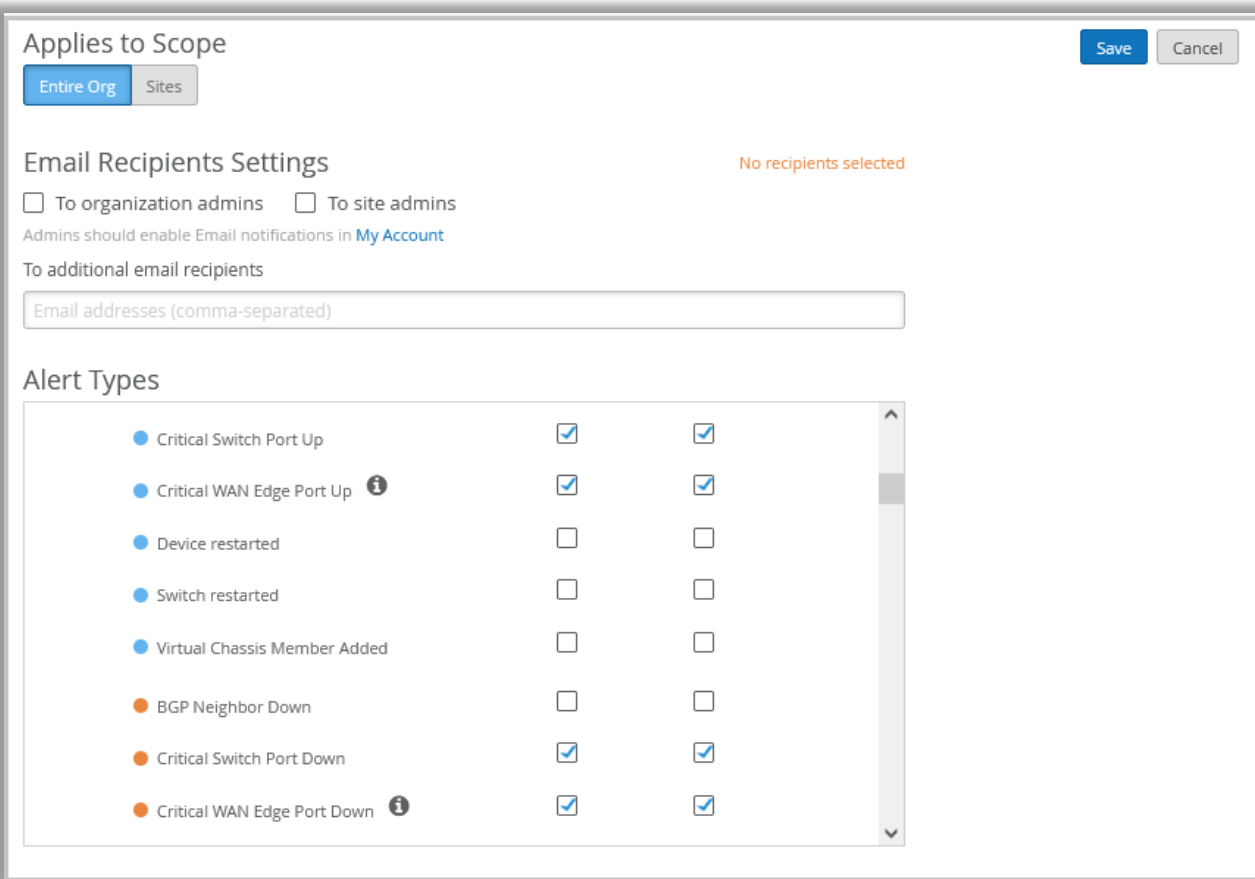
Enable "Up/Down Port" Alert Type ⓘ
Manage Alert Types in [Alerts Page](#)

Description

Add Description

- 指定したスイッチのポート、WANエッジのポートのインタフェース Up/Downイベントのアラート及びEメール通知を設定することができます
- 以下の手順にて設定が可能です
 1. ポートのアラートを設定します
 - WANエッジの場合：
WAN Templates (Organization > WAN Edge Templates) のLANまたはWAN設定セクションにて「Enable "Up/Down Port" Alert Type」のチェックボックスを選択ください
 - スイッチの場合：
Switch Templates (Organization > Switch Templates) のSelect Switches Configuration内のPort Configタブにて「Enable "Up/Down Port" Alert Type」のチェックボックスを選択ください (左図)

ポートUp/Down通知（続き）



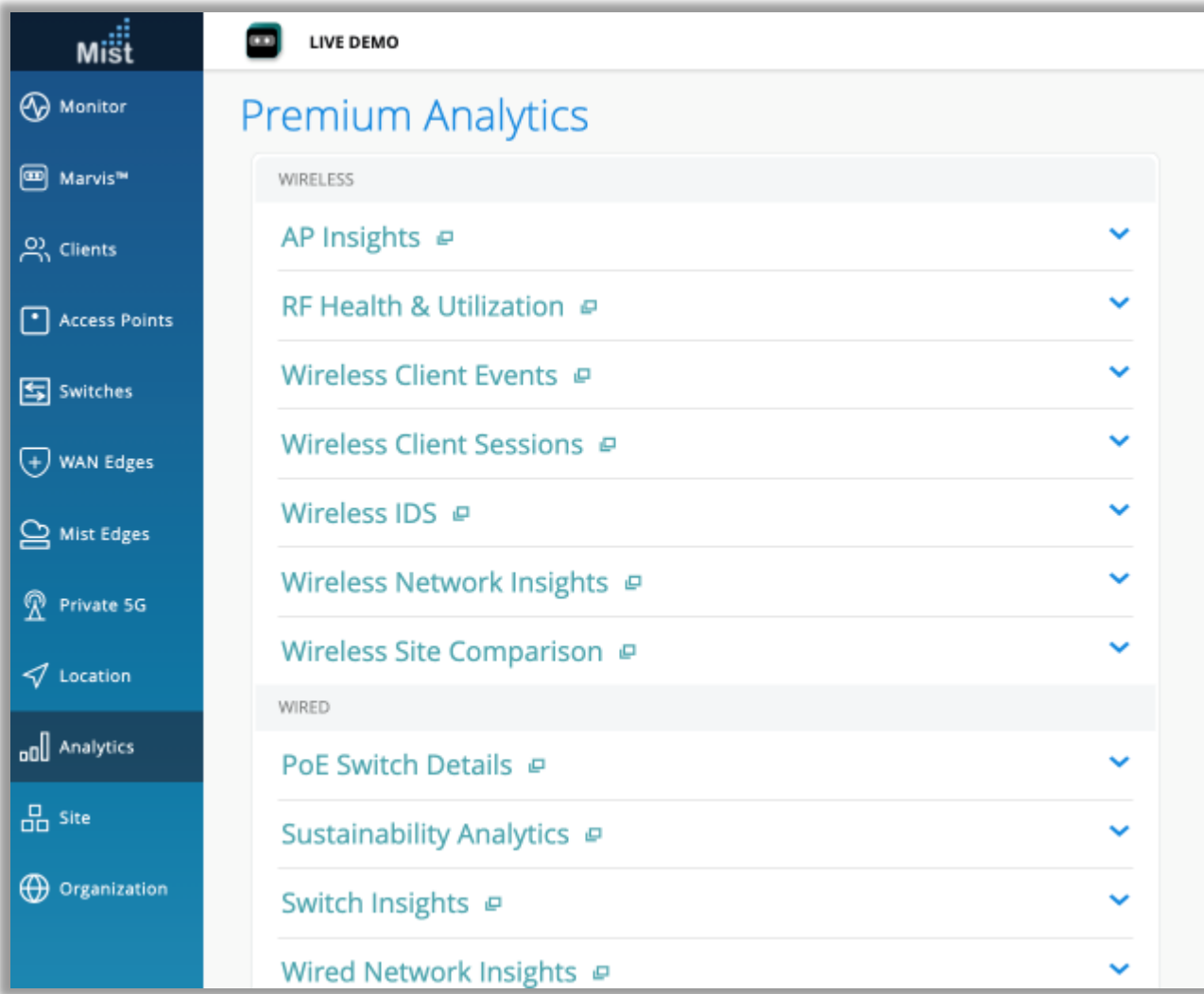
Alert Type	Critical	WAN Edge Port
Critical Switch Port Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critical WAN Edge Port Up ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device restarted	<input type="checkbox"/>	<input type="checkbox"/>
Switch restarted	<input type="checkbox"/>	<input type="checkbox"/>
Virtual Chassis Member Added	<input type="checkbox"/>	<input type="checkbox"/>
BGP Neighbor Down	<input type="checkbox"/>	<input type="checkbox"/>
Critical Switch Port Down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critical WAN Edge Port Down ⓘ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 設定（続き）

2. Monitor > Alerts > Alerts Configurationページにて、以下のチェックボックスを選択することにより、ポートのアラートを可能とします（左図）

- Critical WAN Edge Port Up
- Critical WAN Edge Port Down
- Critical Switch Port Up
- Critical Switch Port Down

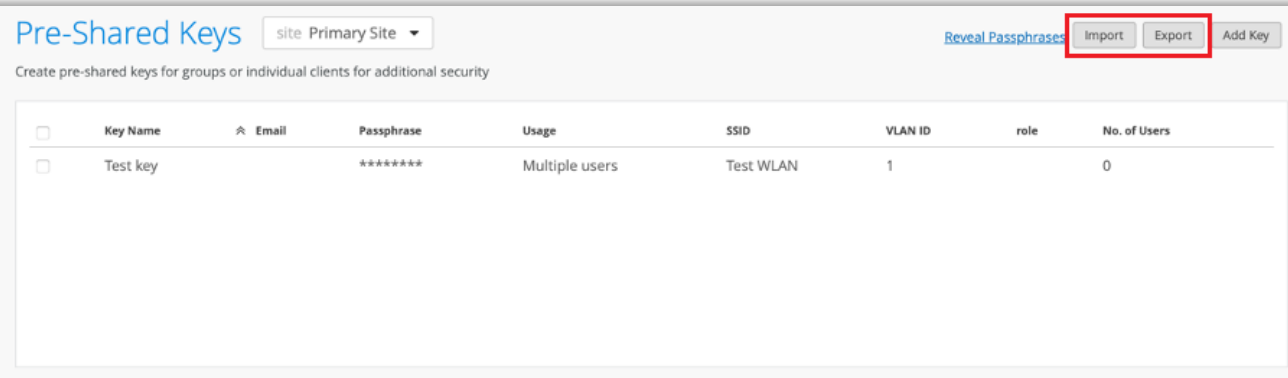
Premium AnalyticsでのSSOサポート



- Premium AnalyticsのSingle Sign-On（以下SSO）サポートにより、Mistポータルから直接Premium Analyticsのレポートダッシュボードへの遷移が可能となりました
- AnalyticsからPremium Analyticsへアクセス可能です（左図）
- 以下の役割（Role）の権限を持つユーザーがSSOが可能となります
 - Super User
 - Network Admin
 - Observer
 - Helpdesk
 - Reporting（Premium Analyticsや他のレポートへのアクセス制限有り）
- その他の役割を適用されたユーザーはこれまでと同様に以下のURLからアクセスし、レポートダッシュボードを閲覧可能です

premiumanalytics.mist.com

SiteレベルPSKのImport/Exportオプション



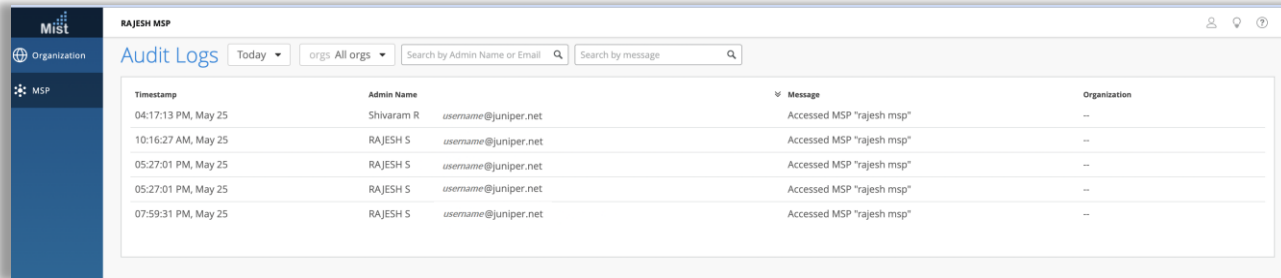
Pre-Shared Keys site: Primary Site [Reveal Passphrases](#) **Import** **Export** Add Key

Create pre-shared keys for groups or individual clients for additional security

<input type="checkbox"/>	Key Name	Email	Passphrase	Usage	SSID	VLAN ID	role	No. of Users
<input type="checkbox"/>	Test key		*****	Multiple users	Test WLAN	1		0

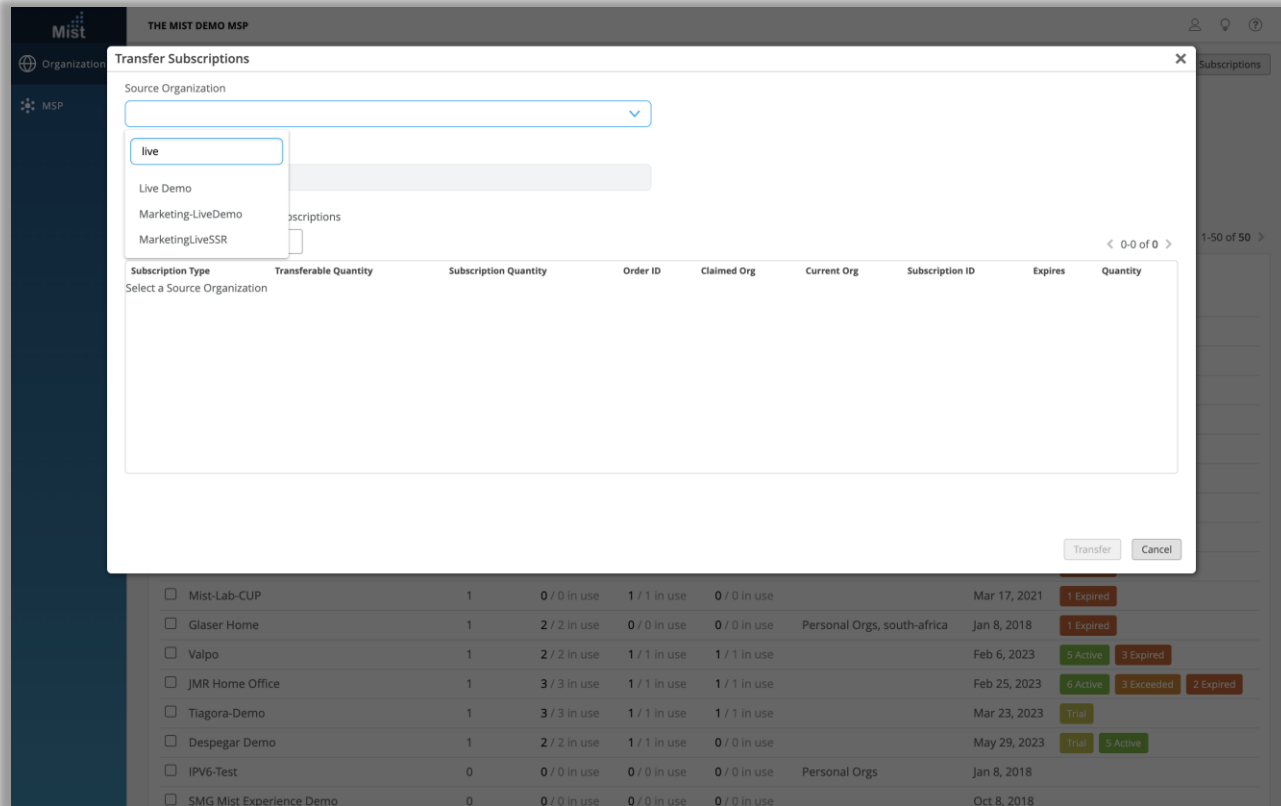
- Siteレベルのpre-shared key（以下PSK）の Import/Exportが可能となります
- Import/Exportには、Super UserまたはNetwork Adminの権限を持つユーザである必要があります
- SiteレベルのPSKを表示するには、Site > Pre-shared Keysを選択ください（左図）

MSPポータルでの改良



The screenshot shows the 'Audit Logs' page in the MSP portal. It features a search bar at the top and a table of logs. The table has columns for Timestamp, Admin Name, Message, and Organization. The logs show multiple instances of 'Accessed MSP' by 'RAJESH S' with the email 'username@juniper.net'.

Timestamp	Admin Name	Message	Organization
04:17:13 PM, May 25	Shivaram R username@juniper.net	Accessed MSP "rajesh msp"	--
10:16:27 AM, May 25	RAJESH S username@juniper.net	Accessed MSP "rajesh msp"	--
05:27:01 PM, May 25	RAJESH S username@juniper.net	Accessed MSP "rajesh msp"	--
05:27:01 PM, May 25	RAJESH S username@juniper.net	Accessed MSP "rajesh msp"	--
07:59:31 PM, May 25	RAJESH S username@juniper.net	Accessed MSP "rajesh msp"	--



The screenshot shows the 'Transfer Subscriptions' dialog box. It has a dropdown menu for 'Source Organization' with 'live' selected. Below the dialog is a table of subscriptions with columns for Subscription Type, Transferable Quantity, Subscription Quantity, Order ID, Claimed Org, Current Org, Subscription ID, Expires, and Quantity. The table lists various organizations and their subscription statuses.

Subscription Type	Transferable Quantity	Subscription Quantity	Order ID	Claimed Org	Current Org	Subscription ID	Expires	Quantity
Select a Source Organization								
Mist-Lab-CUP	1	0 / 0 in use	1 / 1 in use	0 / 0 in use			Mar 17, 2021	1 Expired
Glaser Home	1	2 / 2 in use	0 / 0 in use	0 / 0 in use	Personal Orgs, south-africa		Jan 8, 2018	1 Expired
Valpo	1	2 / 2 in use	1 / 1 in use	1 / 1 in use			Feb 6, 2023	5 Active 3 Expired
JMR Home Office	1	3 / 3 in use	1 / 1 in use	1 / 1 in use			Feb 25, 2023	6 Active 3 Exceeded 2 Expired
Tiagora-Demo	1	3 / 3 in use	1 / 1 in use	1 / 1 in use			Mar 23, 2023	Trial
Despegar Demo	1	2 / 2 in use	1 / 1 in use	0 / 0 in use			May 29, 2023	Trial 5 Active
IPV6-Test	0	0 / 0 in use	0 / 0 in use	0 / 0 in use	Personal Orgs		Jan 8, 2018	
SMG Mist Experience Demo	0	0 / 0 in use	0 / 0 in use	0 / 0 in use			Oct 8, 2018	

- MSP利用者はMSPポータルで実行されたアクティビティの監査ログを閲覧することができます（左上図）
 - MSP利用者は単一、または複数組織（Organization）の監査ログを期間を指定して閲覧することができます
 - アドミン名、アドミンEmailアドレス、ログメッセージをキーワードとして監査ログを検索することも可能です
 - 監査ログはMSP > Audit Logsで閲覧可能です
- サブスクリプション移行ページ（Transfer Subscriptions）で移行元、移行先組織（Organization）をフィルターする機能を追加したことにより、MSP利用者が簡単にサブスクリプションを移行できるようになりました（左下図）

アセット位置情報トラッキング精度の向上

- アセットが案内経路の数メートル以内に入った場合に、案内経路の方へ導くことができるようになりました
- Google道案内のようにアセットが目的地へ向かう経路を示すことができます

ゲストアクセスのWPA3セキュリティモード

The screenshot shows the Mist WLAN configuration page for a new WLAN. The 'Security' section is expanded, showing the following settings:

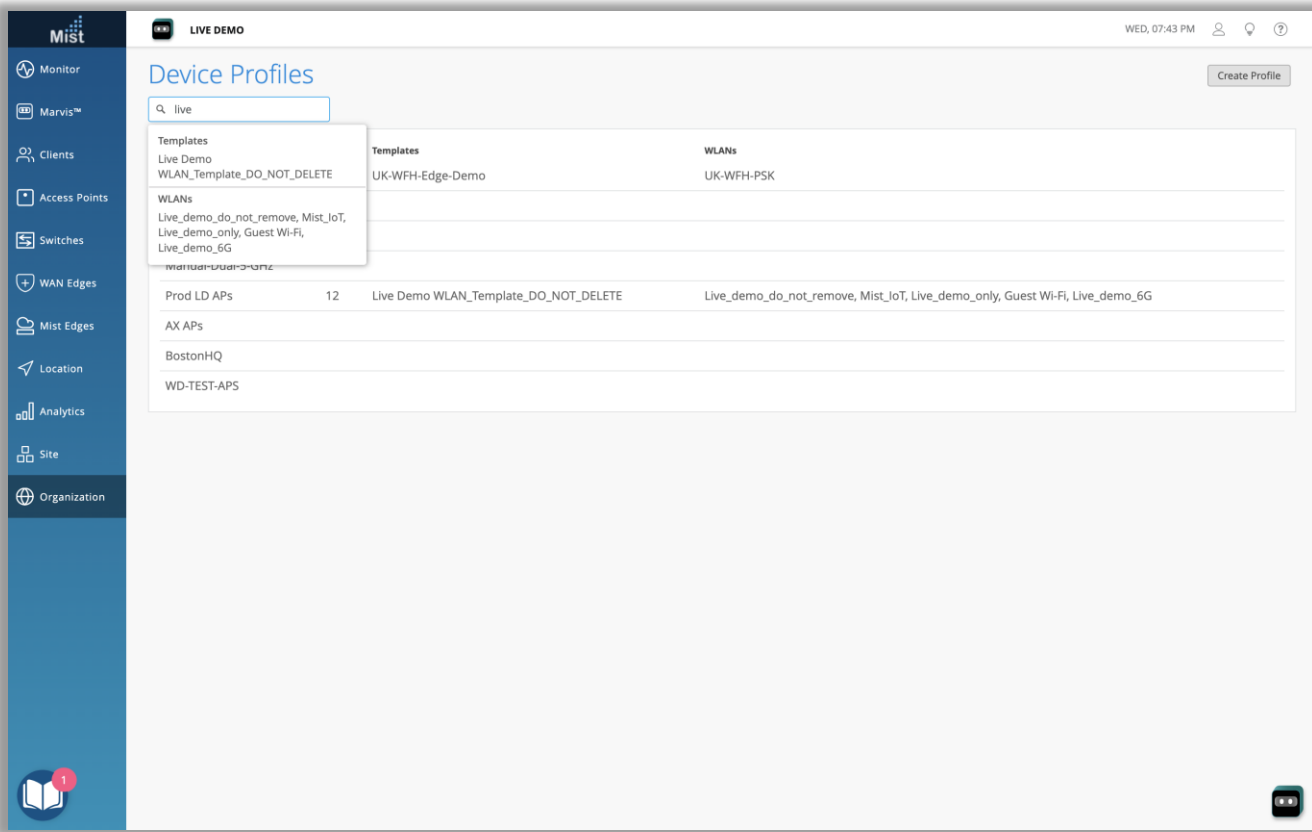
- Security Type: WPA3 (selected), OWE
- Enterprise (802.1X) / Personal (SAE) (selected)
- Passphrase: [Redacted]
- Enable WPA3+WPA2 Transition
- MAC address authentication by RADIUS lookup (highlighted with a red box)
- Use EAPOL v1 (for legacy clients)
- Prevent banned clients from associating

Other sections visible include:

- SSID: New WLAN
- WLAN Status: Enabled
- Radio Band: 2.4 GHz, 5 GHz, 6 GHz (all checked)
- Band Steering: Disabled
- Client Inactivity: 1800 seconds
- Geofence: Disabled
- Fast Roaming: Default
- VLAN: Untagged
- Guest Portal: No portal (go directly to internet)
- Apply to Access Points: All APs
- Isolation: Disabled
- Filtering (Wireless): Disabled
- DTIM Period: 2
- Custom Forwarding: Disabled
- SSID Scheduling: Disabled

- 以下のWLANセキュリティの設定時に、「Guest Access with Mac Authentication Bypass」をオプションとして選択できるようになりました（左図）
 - WPA3 Personal – WPA3+WPA2 Transition
 - OWE
 - OWE Transition

デバイスプロファイルの検索フィルタ機能



- デバイスプロファイルをキーワードを用いてフィルタすることができるようになりました（左図）

WAN Assurance

SSR/SRXのApp-IDデータベースインストール時のスケジュール機能

WAN Edge Advanced Security

IDP / App-ID Upgrade Schedule

Enable Auto Update

Time of Day required Day of Week

2:00 am ▼ Day: Sunday ▼

App Track license is required to manage and collect data for applications and service levels (SRX only)

My SRX devices have an App Track license

Log Source Interface (SRX Only)

- SSR/SRX WAN EdgeにSiteレベルのIDP/App-IDデータベースをインストールする時間をスケジュールできるようになりました（左図）
- Site IDP/App-IDデータベースをインストールする時間と曜日を設定できます
- 毎日実行（Daily）に設定も可能です
- スケジュールの初期値は日曜日の午前2時となっています

Thank you

JUNIPER 
driven by Mist AI 