

# Mist 設定マニュアル - Site Configuration - 不正 AP の検出

---

ジュニパーネットワークス株式会社  
2023年4月 Ver 1.1

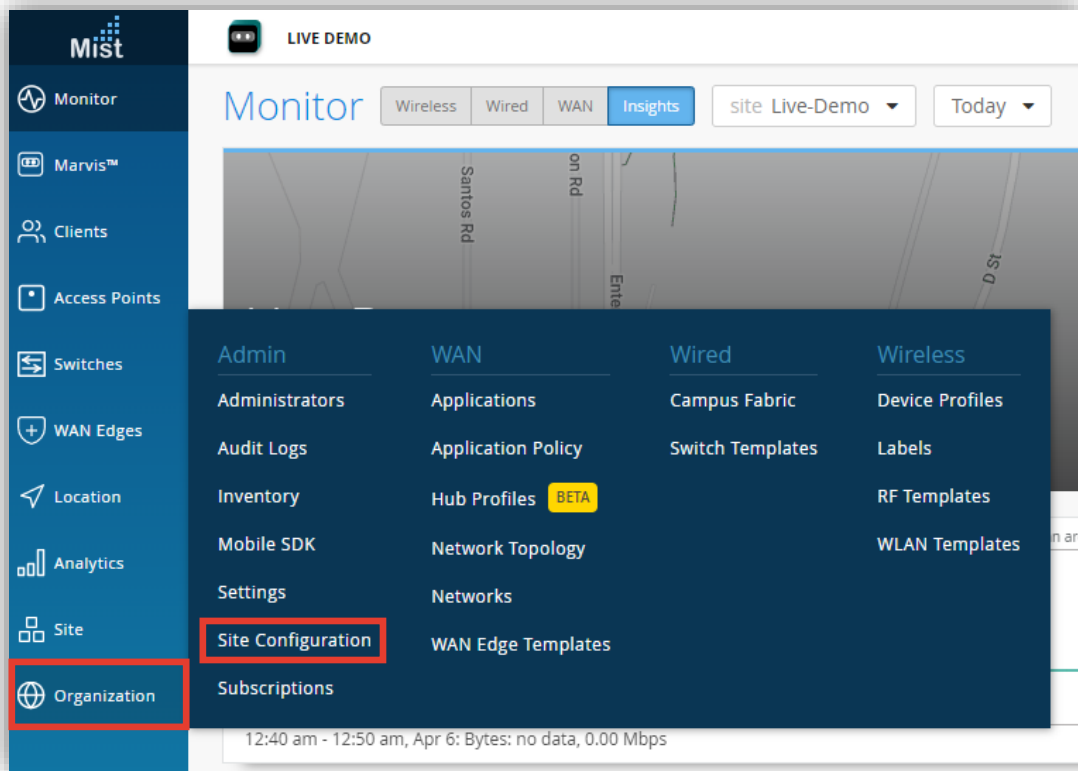
JUNIPER   
driven by Mist AI

# はじめに

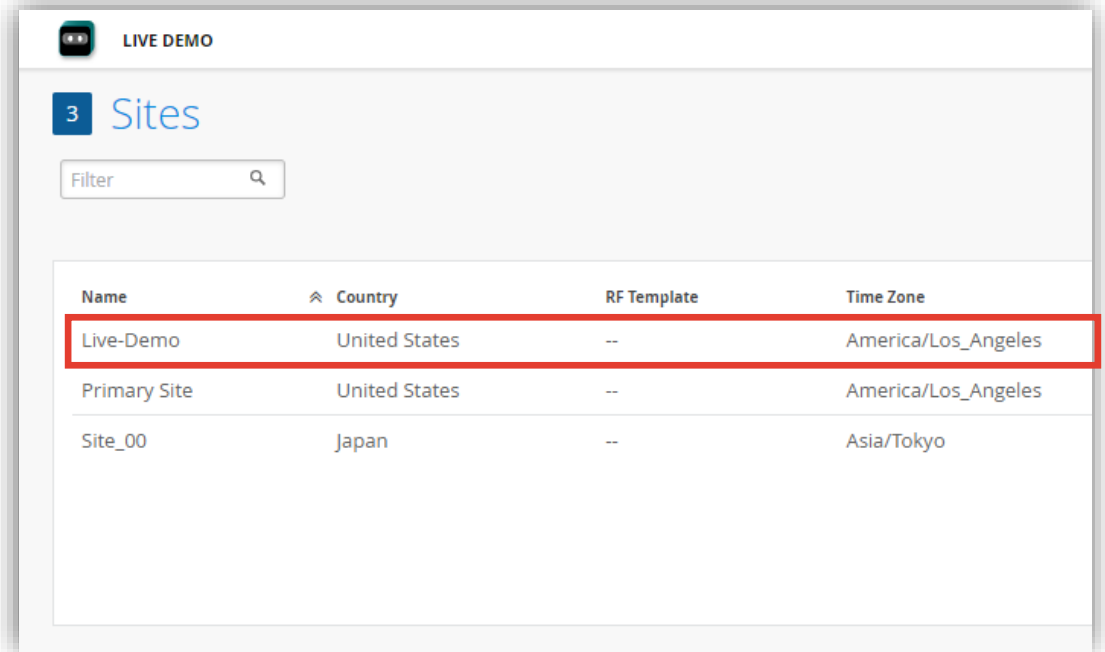
- ❖ 本マニュアルは、『不正 AP の検出』について説明します
- ❖ 手順内容は 2023年4月 時点の Mist Cloud にて確認を実施しております  
実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい  
<https://www.mist.com/documentation/category/product-updates/>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります  
各種設定内容の詳細は下記リンクよりご確認ください  
<https://www.mist.com/documentation/>
- ❖ 他にも多数の Mist 日本語マニュアルを「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>

# 不正 AP を検出する設定

1. [Organization] から [Site Configuration] を選択します



2. 対象となる Site を選択します



# 不正 AP を検出する設定

## 3. セキュリティの設定は「Security Configuration」で行います

Security Configuration

Detect Rogue and Neighbor APs

Neighbor RSSI Threshold

Neighbor Time Threshold  mins

Detect Honeypot APs

Approved SSIDs

Approved BSSIDs

Auto-Prevent Clients

Prevent association for clients having at least

auth failures within a time period of  seconds

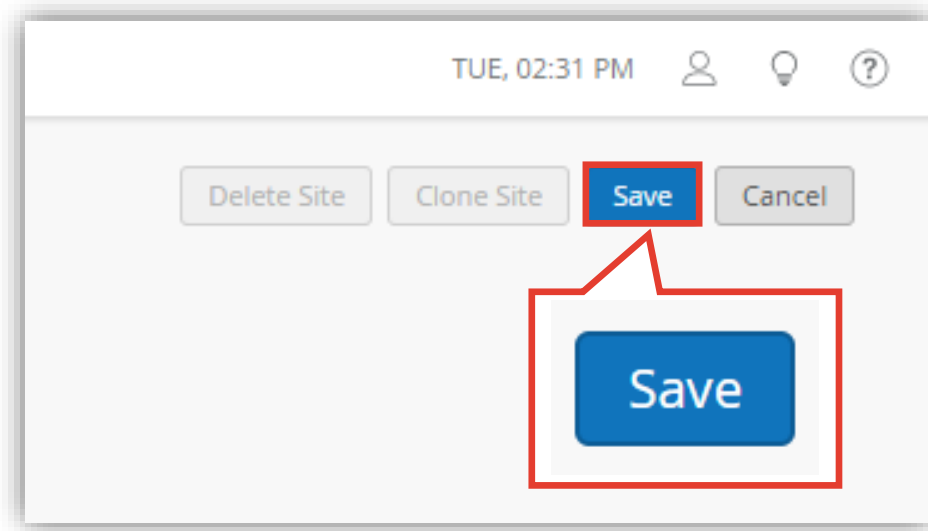
- ログ AP 及び ネイバー AP の検出はデフォルトで無効になっています  
この機能を有効とすることで未知の AP をネイバー AP として検出します  
また、Organizationに登録されていない、同じネットワークに接続されている AP をログ AP として検出します
- 検出するための基準として、無線電波の強さを表す RSSI の閾値を設定します  
RSSI 閾値は -40 dBm から -100 dBm の間に設定できます
- 一時的にしか表示されないネイバー AP によるフラッディングを防止するため、  
検出時間の閾値を設定します

- ハニーポット AP の検出はデフォルトで有効になっています  
この機能を有効とすることで攻撃者がログイン画面を偽装してパスワードを取得  
するといったネットワークに対する脅威を検出することができます
- 正当な AP が不正な AP と認識されないように、SSID と BSSID を入力します

- 認証失敗を繰り返すクライアントの接続を禁止します  
クライアントが行う接続要求において、認証失敗回数が設定値を上回った場合、  
サイトはそのクライアントに対し WLAN への再接続要求を自動的にブロックします
- デフォルトの値では、60 秒以内に 4 回の認証が失敗した場合、クライアントの  
再接続要求がブロックされます

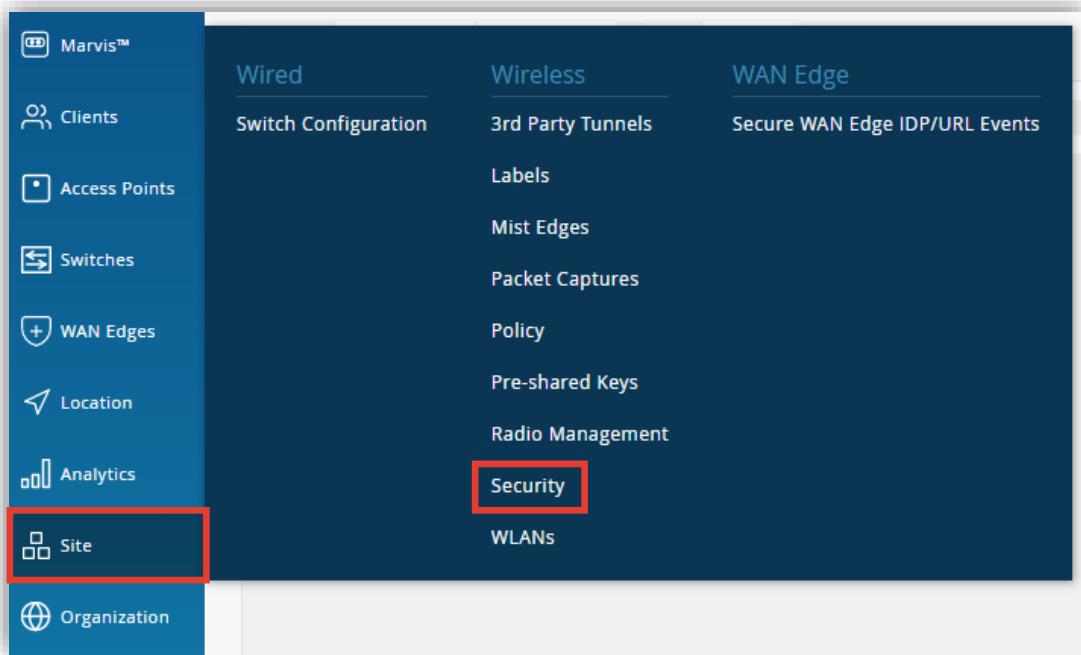
# 不正 AP を検出する設定

4. [Save] をクリックし変更内容を保存します

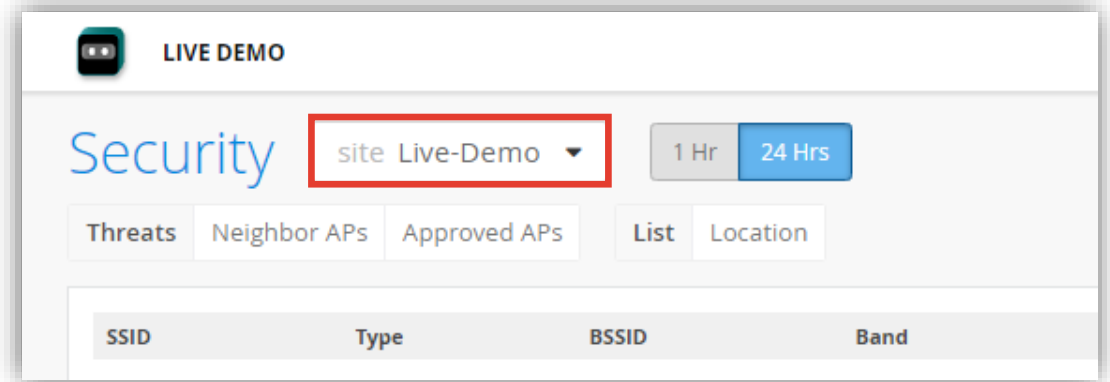


# 不正 AP の確認

1. 不正 AP を表示するには、[Site] から [Security] を選択します



2. 対象となる Site を選択します



# 不正 AP の確認

3. [Threats] の [List] タブではローグ AP、スプーフィング AP、ハニーポット AP をリスト表示で確認できます

Security site Live-Demo 1 Hr 24 Hrs Generate PCI Report View Client Classification

Threats Neighbor APs Approved APs **List** Location

List タブでは検出された不正な AP をリスト表示で確認することができます

| SSID                    | Type   | No. of | Seen By | Nearest AP    | Location                    | Action |
|-------------------------|--------|--------|---------|---------------|-----------------------------|--------|
| Guest Wi-Fi             | Spoofs | --     | 1 APs   | LD_Kitchen    | <a href="#">01 - Office</a> |        |
| Guest Wi-Fi             | Spoofs | --     | 1 APs   | LD_JSW        | <a href="#">01 - Office</a> |        |
| JS-LOCAL                | Rogue  | 0      | 1 APs   | LD_Kitchen-2  | <a href="#">01 - Office</a> | ⋮      |
| JS-LOCAL                | Rogue  | 1      | 1 APs   | LD_Kitchen-2  | <a href="#">01 - Office</a> | ⋮      |
| Live_demo_do_not_remove | Spoofs | --     | 1 APs   | LD_Kitchen    | <a href="#">01 - Office</a> |        |
| Live_demo_do_not_remove | Spoofs | --     | 1 APs   | LD_JSW        | <a href="#">01 - Office</a> |        |
| Live_demo_only          | Spoofs | --     | 1 APs   | LD_Kitchen    | <a href="#">01 - Office</a> |        |
| Live_demo_only          | Spoofs | --     | 1 APs   | LD_JSW        | <a href="#">01 - Office</a> |        |
| Mist_IoT                | Spoofs | --     | 1 APs   | LD_Kitchen    | <a href="#">01 - Office</a> |        |
| Mist_IoT                | Spoofs | --     | 1 APs   | LD_JSW        | <a href="#">01 - Office</a> |        |
| Rivendell-NAC           | Rogue  | 3      | 1 APs   | LD_RS_Support | <a href="#">01 - Office</a> | ⋮      |

# 不正 AP の確認

4. [Threats] の [Location] タブではローグ AP、スプーフィング AP、ハニーポット AP をフロアマップ上で確認できます

The screenshot displays the Juniper Security interface. At the top, there are navigation tabs: Threats (highlighted with a red box), Neighbor APs, Approved APs, List, and Location (highlighted with a blue box). A callout box points to the Location tab with the text: "Location タブではフロアマップ上の AP の位置を確認することができます". Below the tabs is a floorplan map showing various rooms and AP locations. A legend in the bottom left corner, also highlighted with a blue box, indicates: 8 Rogues (red square), 8 Spoofs (orange square), and 0 Honeypots (yellow square). On the right side, there is a "Floorplan" dropdown menu set to "01 - Office" and a "Threat APs" section with sub-tabs for Rogues, Spoofs, and Honeypots. The Rogues sub-tab is active, showing a list of APs with red bars next to their names.

| Threat APs |
|------------|
| 5c:        |
| JS-L       |
| d4:        |
| JS-L       |
| d4:        |
| Riv        |
| d4:        |
| Riv        |
| d4:        |
| Riv        |
| d4:        |
| Riv        |
| d4:        |
| Riv        |
| 40:        |
| SET        |
| ac:        |
| SYM        |



# 不正 AP の確認

5. [Neighbor APs] の [List] タブでは ネイバー AP をリスト表示で確認できます

The screenshot shows the Security dashboard for a site named 'Live-Demo'. The 'Neighbor APs' tab is selected, and the 'List' sub-tab is active. A callout box points to the 'List' sub-tab with the text: 'List タブでは検出されたネイバー AP をリスト表示で確認することができます'.

| SSID            | Seen By | Nearest AP    | Location                    |
|-----------------|---------|---------------|-----------------------------|
| !!!DNR          | 6 APs   | LD_Friday     | <a href="#">01 - Office</a> |
| !!!DNR          | 5 APs   | LD_Friday     | <a href="#">01 - Office</a> |
| !!-1            | 7 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-1            | 6 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-2            | 6 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-2            | 8 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-3            | 5 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-3            | 7 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !!-3            | 6 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |
| !@#\$%^pb_dot1x | 4 APs   | LD_Testbed_MD | <a href="#">01 - Office</a> |



# 不正 AP の確認

7. [Approved APs] では承認された AP を確認できます

| Name                          | No. of Clients | Mac Address |
|-------------------------------|----------------|-------------|
| LD_IDF_B_AP                   | 0              | 5c:         |
| LD_Marvis                     | 0              | d4:         |
| Connected_to_3rd_party_Switch | 0              | 5c:         |
| LD_JSW                        | 0              | d4:         |
| LD_RS_Support                 | 5              | 5c:         |
| LD_MCB_AP                     | 7              | ac:         |
| Simulated AP-1                | 0              | 5c:         |
| LD_Collin's AP                | 7              | d4:         |
| LD_Kitchen                    | 0              | d4:         |
| LD_Testbed_MD                 | 5              | 5c:         |

# Thank you

---

JUNIPER  
driven by Mist AI 