

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
2024年8月 Ver 1.2

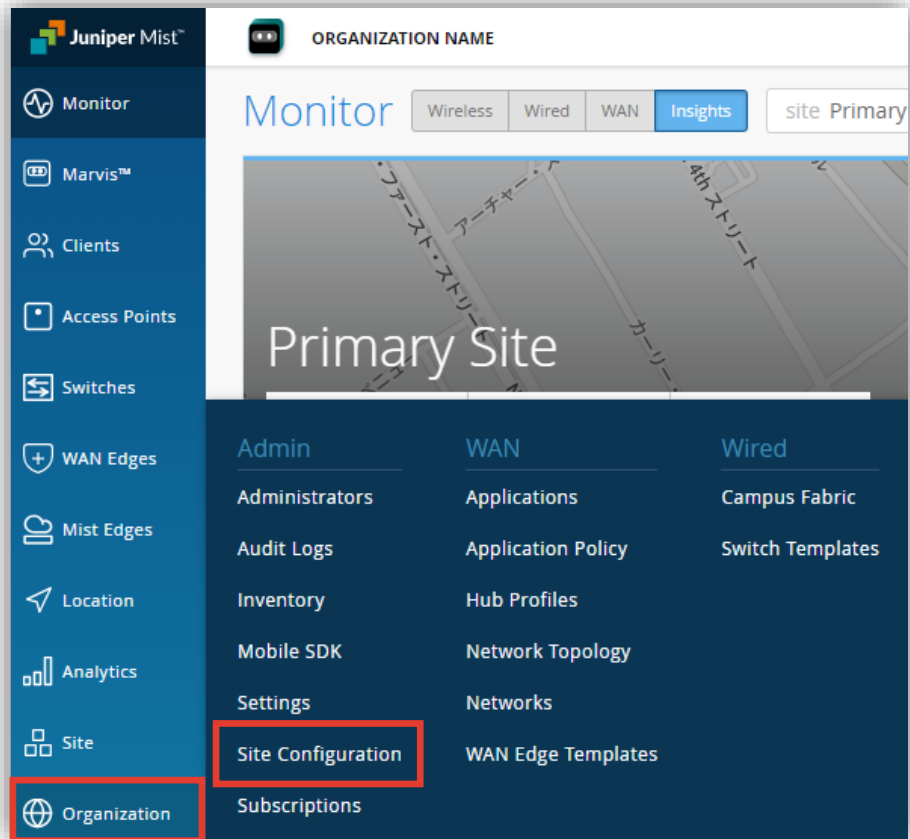


はじめに

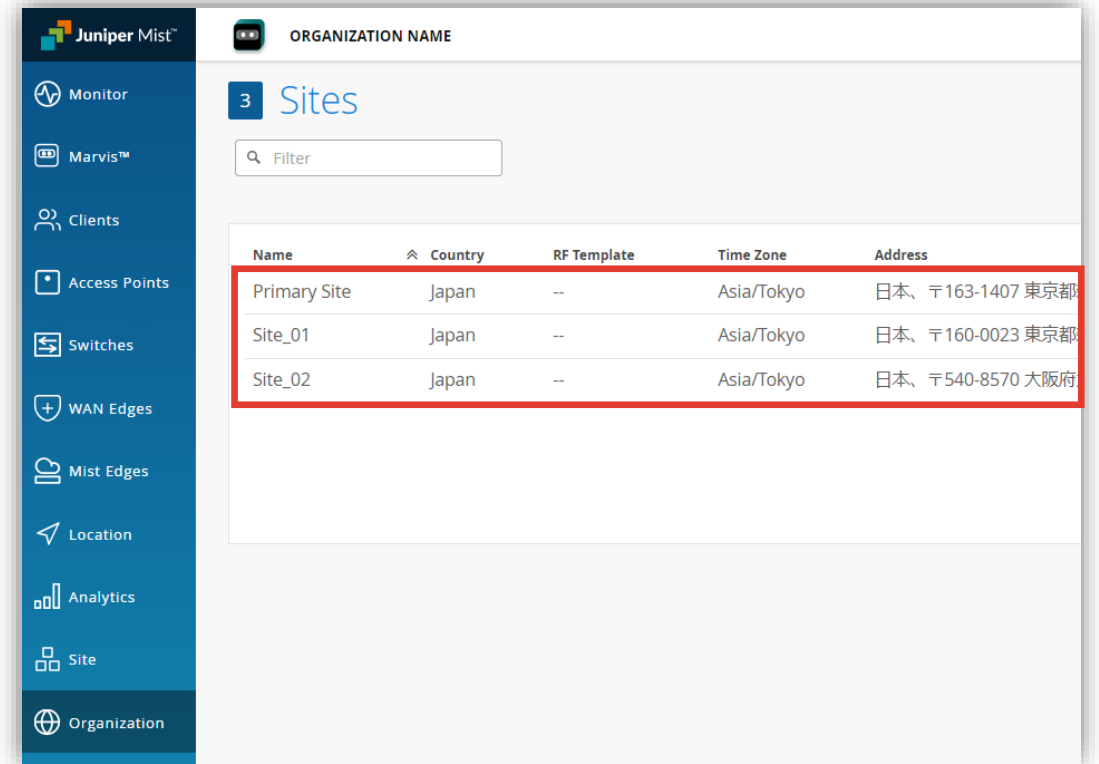
- ❖ 本マニュアルは、『不正 AP の検出』について説明します
- ❖ 手順内容は 2024年8月 時点の Mist Cloud にて確認を実施しております
実際の画面と表示が異なる場合は以下のアップデート情報をご確認ください
<https://www.mist.com/documentation/category/product-updates/>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります
各種設定内容の詳細は下記リンクよりご確認ください
<https://www.mist.com/documentation/>
- ❖ 他にも多数の Mist 日本語マニュアルを「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

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 client from associating for seconds when having at least auth failures within seconds

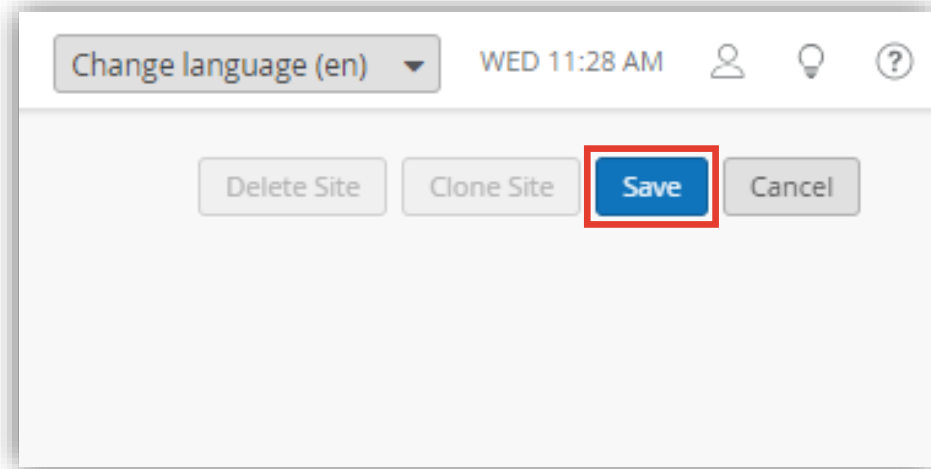
- ログ AP 及び ネイバー AP の検出はデフォルトで無効になっています
この機能を有効とすることで未知の AP をネイバー AP として検出します
また、Organizationに登録されていない、同じネットワークに接続されている AP をログ AP として検出します
- 検出するための基準として、無線電波の強さを表す RSSI の閾値を設定します
RSSI 閾値は -40 dBm から -100 dBm の間に設定できます
- 一時的にしか表示されないネイバー AP によるフラッディングを防止するため、検出時間の閾値を設定します

- 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

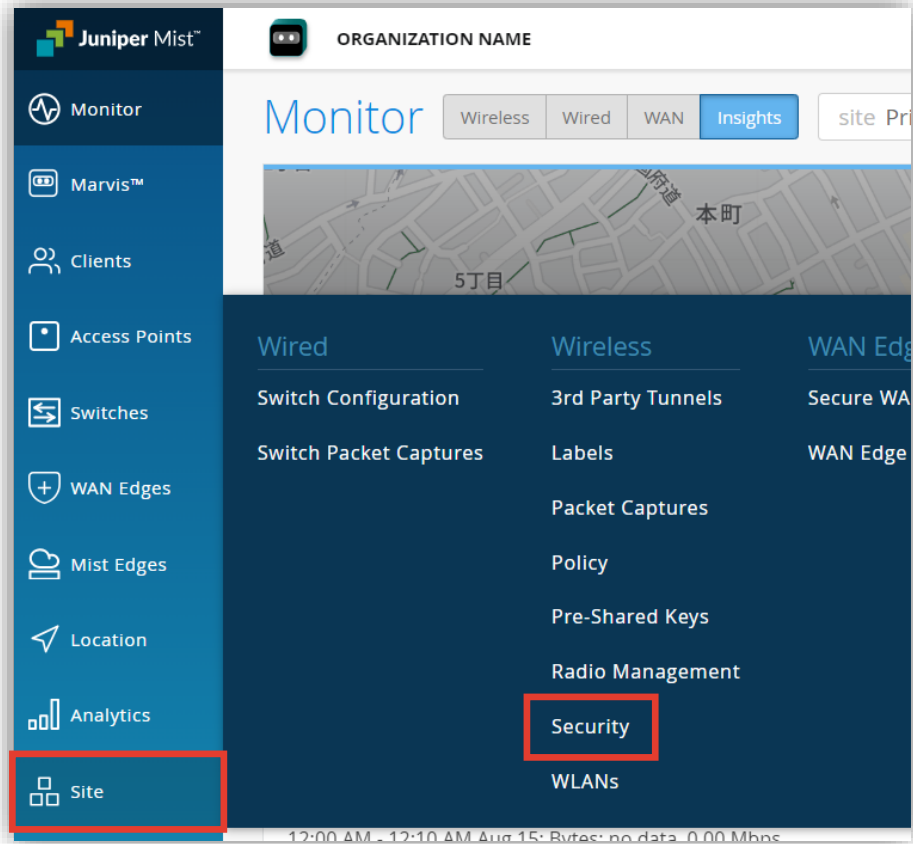
不正 AP を検出する設定

4. [Save] をクリックし変更内容を保存します

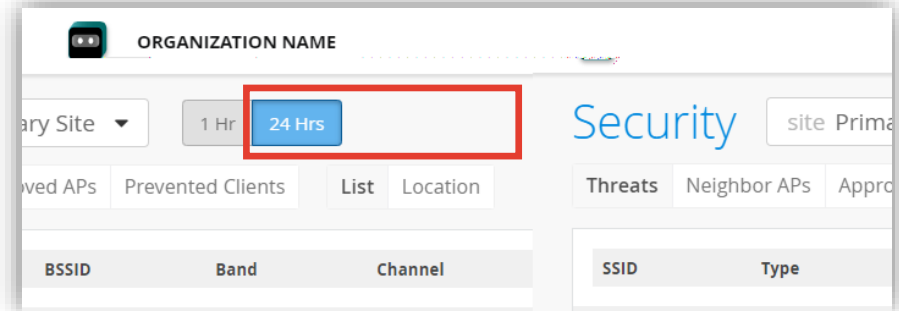


不正 AP の確認

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、ハニーポット AP をリスト表示で確認できます

Security

site Primary Site

1 Hr24 Hrs

Generate PCI ReportView Client Classification

ThreatsNeighbor APsApproved APsPrevented ClientsList

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 Clients	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location	Action
TEST	Rogue	0	00:00:00:00:00:00	5GHz	52	-61.0 dBm	1 AP	LD_APEng	01 - Office	⋮
rk@open	Rogue	1	ac:12:34:56:78:9a	5GHz	44	-73.0 dBm	1 AP	LD_RS_Support	01 - Office	⋮
Himanshu-desk	Rogue	2	d4:12:34:56:78:9a	5GHz	116	-52.0 dBm	1 AP	LD_APEng	01 - Office	⋮
Himanshu-desk	Rogue	0	d4:12:34:56:78:9a	2.4GHz	11	-44.0 dBm	1 AP	LD_APEng	01 - Office	⋮

不正 AP の確認

4. [Threats] の [Location] タブではローグ 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, the 'Security' header is visible, along with a 'site Primary Site' dropdown and time filters for '1 Hr' and '24 Hrs'. The 'Threats' tab is selected and highlighted with a red box. Below it, the 'Location' sub-tab is also highlighted with a red 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' (In the Location tab, you can confirm the location of APs on the floor map). The main area shows a floor map with several red squares indicating the locations of threat APs. A legend in the bottom left corner shows '4 Rogues' (red squares) and '0 Honeypots' (yellow squares). On the right side, there are buttons for 'Generate PCI Report' and 'View Client Classification'. Below these, the 'Floorplan' section shows '01 - Office' selected. The 'Threat APs' section has two tabs: 'Rogues' and 'Honeypots'. Under the 'Rogues' tab, a list of threat APs is shown, including MAC addresses and device names like 'Himanshu-desk'.

Security site Primary Site 1 Hr 24 Hrs

Threats Neighbor APs Approved APs Prevented Clients List Location

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

Floorplan 01 - Office

Threat APs Rogues Honeypots

00: TES
ac:
rk@
d4:
Him
d4:
Himanshu-desk

4 Rogues
0 Honeypots

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

Security

site Primary Site

1 Hr24 Hrs

ThreatsNeighbor APsApproved APsPrevented ClientsList

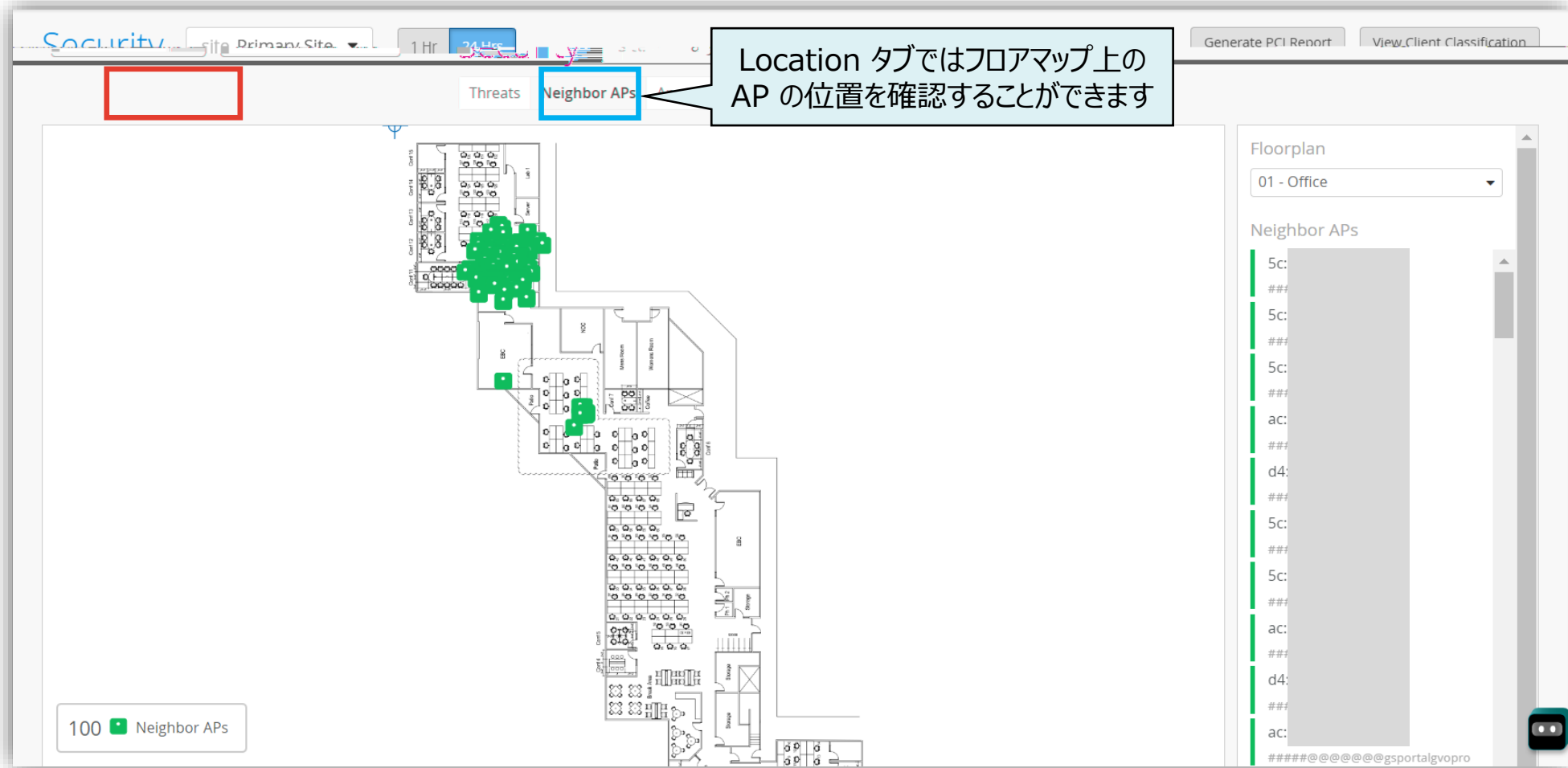
List タブでは検出されたネイバー AP をリスト表示で確認することができます

Generate PCI ReportView Client Classification

SSID	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location
###11r_FT-PSK	5c:	5GHz	36	-69.9 dBm	1 AP	LD_APEng	01 - Office
###11r_FT-PSK	5c:	5GHz	36	-64.8 dBm	1 AP	LD_APEng	01 - Office
####RPPSK_test	5c:	5GHz	36	-56.9 dBm	1 AP	LD_APEng	01 - Office
####RPPSK_test	ac:	5GHz	149	-73.9 dBm	1 AP	LD_APEng	01 - Office
####RPPSK_test	d4:	5GHz	149	-72.1 dBm	1 AP	LD_APEng	01 - Office
#####OKC_test	5c:	2.4GHz	11	-52.1 dBm	1 AP	LD_APEng	01 - Office
#####OKC_test	5c:	5GHz	36	-56.3 dBm	1 AP	LD_APEng	01 - Office
#####OKC_test	ac:	5GHz	149	-74.2 dBm	1 AP	LD_APEng	01 - Office
#####OKC_test	d4:	5GHz	149	-72.2 dBm	1 AP	LD_APEng	01 - Office
#####@.@.@.@gsportalgvoprod	ac:	5GHz	140	-56.9 dBm	1 AP	LD_APEng	01 - Office
#####@.@.@.@gsportalgvoprod	ac:	2.4GHz	1	-48.5 dBm	1 AP	LD_APEng	01 - Office

不正 AP の確認

6. [Neighbor APs] の [Location] タブでは ネイバー AP をフロアマップ上で確認できます



不正 AP の確認

7. [Approved APs] では承認された AP を確認できます

Security

site Primary Site

1 Hr24 Hrs

Generate PCI ReportView Client Classification

ThreatsNeighbor APsApproved APsPrevented Clients

Name	No. of Clients	MAC Address
LD_NewBobFriday	0	00:
LD_IDF_B_AP-3rd-Party-Switch	0	5c:
MCM_AP_33_Nishant	0	d4:
MC_AP-21	0	5c:
LD_Marvis	0	a8:
LD_Kitchen	0	00:
LD_Testbed_MD	0	5c:
LD_MCB_AP	0	ac:
LD_Conf2	0	a8:
LD_APEng	2	ac:

不正 AP の確認

8. [Prevented Clients] では禁止されたクライアントを確認できます

Security site Primary Site 1 Hr 24 Hrs Generate PCI Report View Client Classification

Threats Neighbor APs Approved APs **Prevented Clients**

Timestamp	Client	AP	WLAN	BSSID	Reason
09:16:54 am, Jun 25	d8:9c:67:5c:d7:b1	Mist: Engineering (F10)			Client is banned
09:17:38 am, Jun 25	d8:9c:67:5c:d7:b1	APHX- Near Abhi	Rivendell	5c: [redacted]	Repeated authorization failure
09:17:59 am, Jun 25	d8:9c:67:5c:d7:b1	Mist: Rosie			Client is banned
09:18:02 am, Jun 25	b8:27:eb:2a:00:15	Mist: KITT			Client is banned
09:18:28 am, Jun 25	d8:9c:67:5c:d7:b1	APHX- Near Abhi	Rivendell	5c: [redacted]	Repeated authorization failure
09:18:54 am, Jun 25	d8:9c:67:5c:d7:b1	Mist: Engineering (F10)			Client is banned
09:19:31 am, Jun 25	d8:9c:67:5c:d7:b1	APHX- Near Abhi	Rivendell	5c: [redacted]	Repeated authorization failure
09:20:21 am, Jun 25	d8:9c:67:5c:d7:b1	Mist: Board Room			Client is banned
09:20:22 am, Jun 25	d8:9c:67:5c:d7:b1	APHX- Near Abhi	Rivendell	5c: [redacted]	Repeated authorization failure
09:21:41 am, Jun 25	d8:9c:67:5c:d7:b1	Mist: Engineering (F10)			Client is banned
09:23:06 am, Jun 25	d8:9c:67:5c:d7:b1	APHX- Near Abhi	Rivendell	5c: [redacted]	Repeated authorization failure

参考情報

Prevented Clients の表示は Site Configuration にて Auto-Prevent Clients の有効化が必要です

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 client from associating for seconds when having at least auth failures within seconds

Thank you

