

Mist 運用マニュアル

Alert メッセージ 確認手順

ジュニパーネットワークス株式会社
2024年6月 Ver 1.1

JUNIPER 
driven by Mist AI

はじめに

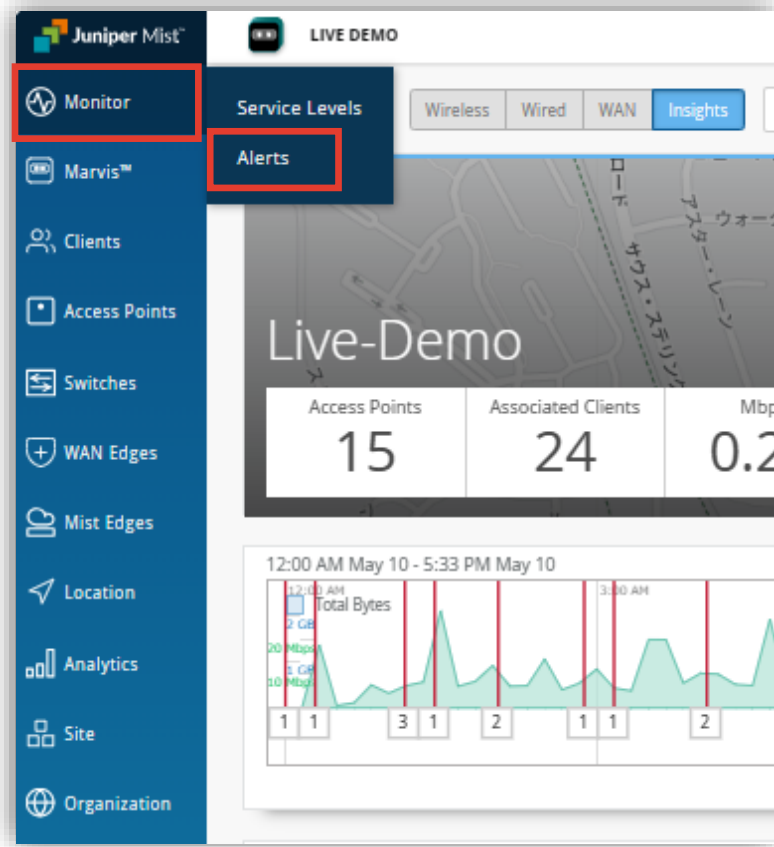
- ❖ 本マニュアルは、『Alert メッセージ 確認手順』について説明します
- ❖ 手順内容は 2024年6月 時点の Mist Cloud にて確認を実施しております
実際の画面と表示が異なる場合は以下のアップデート情報をご確認ください
<https://www.mist.com/documentation/category/product-updates/>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります
各種設定内容の詳細は下記リンクよりご確認ください
<https://www.mist.com/documentation/>
- ❖ 他にも多数の Mist 日本語マニュアルを「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

■ 運用ケース(例)

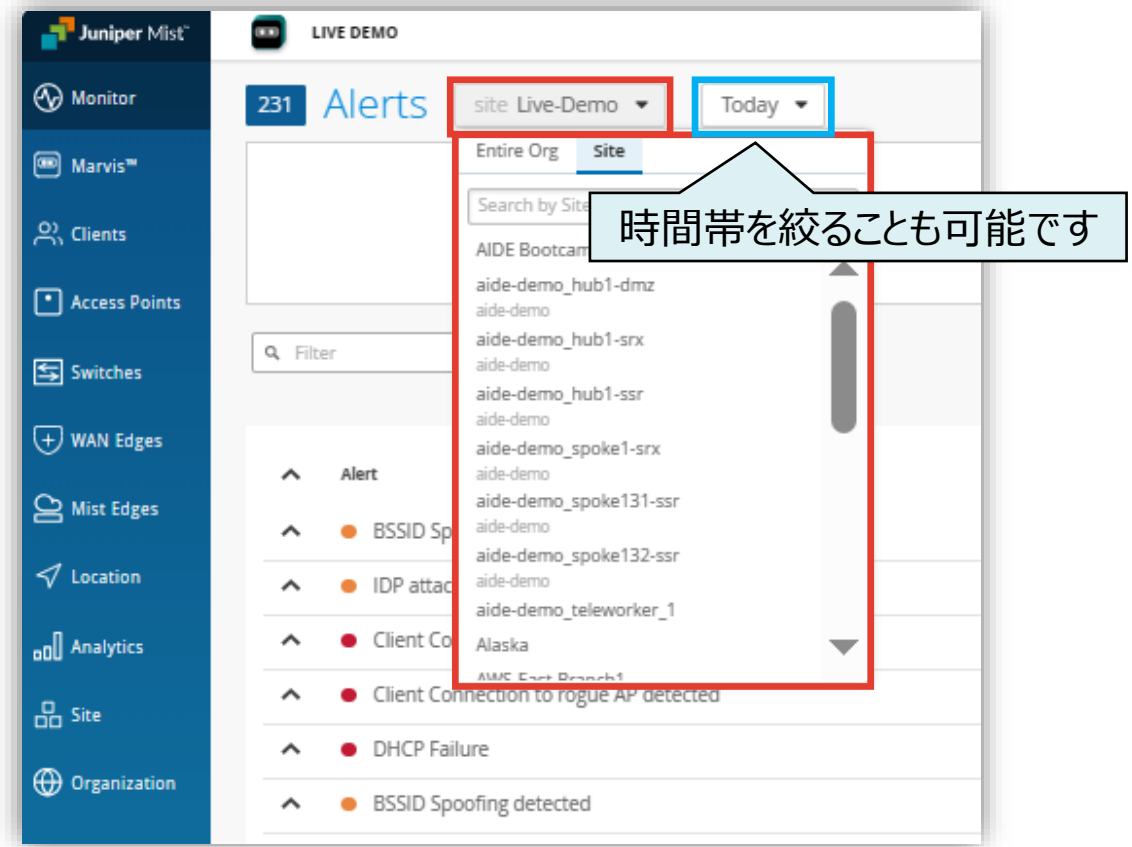
- Alert メッセージを確認したい時

Alert メッセージ 確認

1. [Monitor] から [Alerts] をクリックします



2. [site] から対象拠点 (Site Name)、もしくは Enter Org ですべてのサイトを選択します



Alert メッセージ 確認

3. 重要度 (Critical / Warning / Information) と件数を確認します

※それぞれの重要度の色分けは、Alert Configuration > Alerts Types の先頭の色に対応します

The screenshot shows the Alerts dashboard on the left and the Alert Types configuration page on the right. The Alerts dashboard displays the following data:

Category	Count
Total	232
Infrastructure	59
Marvis	0
Critical	121
Warning	108
Information	3

The Alert Types page shows a list of alert types with checkboxes for enabling them. The alert types are color-coded to match the alert counts:

- Red: Client Connection to rogue AP detected, Rogue AP detected
- Blue: Air Magnet Scan detected, EAP Handshake Flood detected
- Orange: Active Watched Station detected, Adhoc Network detected, Disassociation Attack detected, EAP Dictionary Attack detected

Dashed lines connect the alert counts to the corresponding alert types:

- Red dashed line connects 121 Critical to the red alert types.
- Blue dashed line connects 3 Information to the blue alert types.
- Orange dashed line connects 108 Warning to the orange alert types.

Alert メッセージ 確認

4. Alert メッセージを確認します

Alerts (site Live-Demo) Today

177 Total 47 Infrastructure 0 130 Security

93 Critical 82 Warning 2 Information

それぞれクリックすると、該当する重要度のメッセージに絞りこみできます

First Seen: Alert が初めて確認された日時
Last Seen: Alert が最後に確認された日時

詳細表示 Alert メッセージ 再発回数 関連ページリンク

Alert	Recurrence	First Seen	Last Seen	Details
Client Connection to rogue AP detected	1	May 13, 2024 4:29 PM	May 13, 2024 4:29 PM	Network Security
IDP attack detected	1	May 13, 2024 4:28 PM	May 13, 2024 4:28 PM	Network Security
DHCP Failure	1	May 13, 2024 4:25 PM	May 13, 2024 4:25 PM	Device Insights

IDP attack detected 1 May 13, 2024 4:28 PM May 13, 2024 4:28 PM Network Security

Attacks	SSL:OVERFLOW:KEY-ARG-NO-ENTROPY
Protocols	tcp
Attacker IPs	192.168.2.34
Applications	SSL
Ingress Ports	ge-0/0/3.2

Security (site Live-Demo) 1 Hr 24 Hrs

Threats	Neighbor APs	Approved APs	Clients	List	Location					
SSID	Type	No. of Clients	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location	Action
Live_demo_only	Spoofs	--	00:3e:73:63:cc:92	6GHz	5	-64.0 dBm	1 AP	LD_NewBobFriday	01 - Office	
Guest	Honeypot	--	a8:f7:d9:ed:89:42	2.4GHz	11	-40.0 dBm	1 AP	LD_NewBobFriday	01 - Office	
Guest	Honeypot	--	a8:f7:d9:ed:89:62	5GHz	100	-39.0 dBm	1 AP	LD_NewBobFriday	01 - Office	
	Rogue	0	5c:5b:35:31:5a:b1	2.4GHz	6	-50.0 dBm	1 AP	LD_APEng	01 - Office	
	Rogue	0	5c:5b:35:31:5a:c1	5GHz	124	-66.0 dBm	1 AP	LD_NewBobFriday	01 - Office	

Thank you

JUNIPER
driven by Mist AI 