

Mist 設定マニュアル - Policy -

WxLAN(アクセス制御ポリシー)の設定

ジュニパーネットワークス株式会社

2024年11月 Ver 1.1

JUNIPER 
driven by Mist AI

はじめに

- ❖ 本マニュアルは、『WxLAN(アクセス制御ポリシー)の設定』について説明します
- ❖ 手順内容は 2024年11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

WxLAN(アクセス制御ポリシー)の概要

WxLAN (アクセス制御ポリシー)で、ユーザの通信を制御することが可能です

- 送信元 (User) に対して宛先 (Resource) を指定して、Allow/Deny で通信の可否を制御
- Resource はシステム定義のアプリケーション (Deny 動作のみ) を選択可能、User とその他の Resource は Label の作成 (Site > Labels) が必要 (IP アドレスの直打ちは不可)
- デフォルトポリシー (Last) で、すべての通信を許可 (拒否も設定可)

No.	送信元 (User)	Policy	宛先 (Resource)	Usage (No. Sessions)
1	User (matching ALL labels) + Guest users	Application ✓	Application ×	0
2	+ Employee_SETraining	NOT (Twitter) ✓	Application ×	0
3	+ User 3 Mac	Application ✓	Social Network ×	0
4	+ Terminal 3	Application ✗	All Resources +	0
5	+ Guest-Open	Application ✓	Internet ×	0
Last	All Users	Application ✓	All Resources	

Callouts:

- Label (User) points to the User column.
- Label (Resource) points to the Resource column.
- アプリケーション → Deny (赤)動作のみ points to the red 'Social Network' resource.
- ユーザ定義の Resource → Allow (緑) or Deny (赤) points to the green 'Internet' resource.
- デフォルトポリシー points to the 'Last' row.

ポリシーの評価

ポリシーの適用ルールは以下の通りです

1. 上から順に評価
2. User に設定された**全てのラベルにマッチ**した場合にポリシーが実行
3. 一度ポリシーが適用されると以降のポリシーは評価されない (First Match)
4. ポリシーにマッチしない通信は、Last で全て許可または拒否される

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest users	✓	Internet × Intranet × +	0
2	+ Employee_SETraining	✓	Facebook × +	0
3	+ User 3 Mac	✓	Social Network × +	0
4	+ Terminal 3	✗	All Resources +	0
5	+ Guest-Open	✓	Internet × +	0
Last	All Users	✓ Allow	All Resources	

※ Last でどのポリシーにもマッチしない場合の動作を指定

Save Cancel

※ Save で設定を保存

ラベルの概要

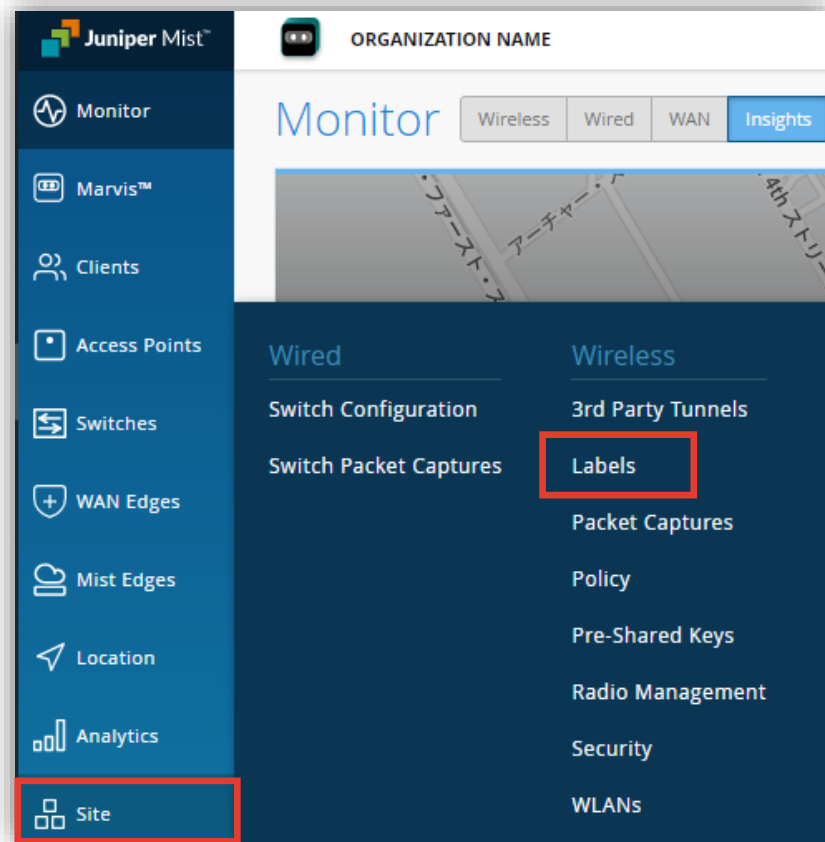
- ラベルには Label Name、Label Type、Label Values を設定します
- Policy への設定が可能な Label Type は 9 項目（右表）
- Label Type 毎に Policy の適用可能な箇所（User/Resource）が決まっています（右表）

Label Type	Label Values	Policy への設定
AAA Attribute	Radius Username（認証サーバに設定されたユーザー名）	User
WiFi Client	Wi-Fi クライアントの MAC アドレス	User
WLAN	作成済みの WLAN（SSID）一覧から選択	User
Access Point	登録済みの AP 一覧から選択	User
IP Address	IP アドレス、またはレンジ（CIDR 方式で入力）を指定	Resource
Hostname	URL で指定（例：xxx.org, xxx.com:8080）	Resource
Application	Mist で定義されているアプリケーション一覧から選択	Resource
Port	TCP/UDP のポート番号	Resource
IP/Protocol/Port	IP アドレス、Protocol、Port を指定	Resource

※ WiFi Client Name、BLE Asset、App Client、VLAN は Policy に適用不可

ラベルの作成

1. [Site] から [Labels] を選択します



2. [Add Label] をクリックします



ラベルの作成

3. 任意の [Label Name] を入力し、
[Label Type] を選択します

< Site Labels : New Label

Label Name
New Label

Label Type
AAA Attribute
AAA Attribute
App Client
Access Point
Application
BLE Asset
Hostname
IP Address
IP/Protocol/Port
Port
VLAN
WiFi Client
WiFi Client Name
WLAN

IS NOT

4. [Label Values] を入力します
例) [Label Type] に [IP Address] を選択した場合

Label Type
IP Address
This is a Resource label if used in WxLan

Label Values IS

List of IP (xxx.xxx.xxx.xxx),
or CIDR (xxx.xxx.xxx.xxx/xx)

Add IPs

IP アドレスを登録
• コンマ区切りで複数登録
• CIDR の指定可能

WxLAN(アクセス制御ポリシー)の設定

0. 設定するポリシーに必要なラベルを作成します
詳細は、「Mist 設定マニュアル ラベルの作成」を参照してください

ポリシー設定例

User	Resource	備考
WLANS	Youtube / Facebook	Youtube / Facebook へのアクセスをブロック
Guest	Private Address (RFC1918)	プライベートアドレスへの通信をブロック
All Users	All Resources	デフォルトポリシー(Last)で通信をブロック

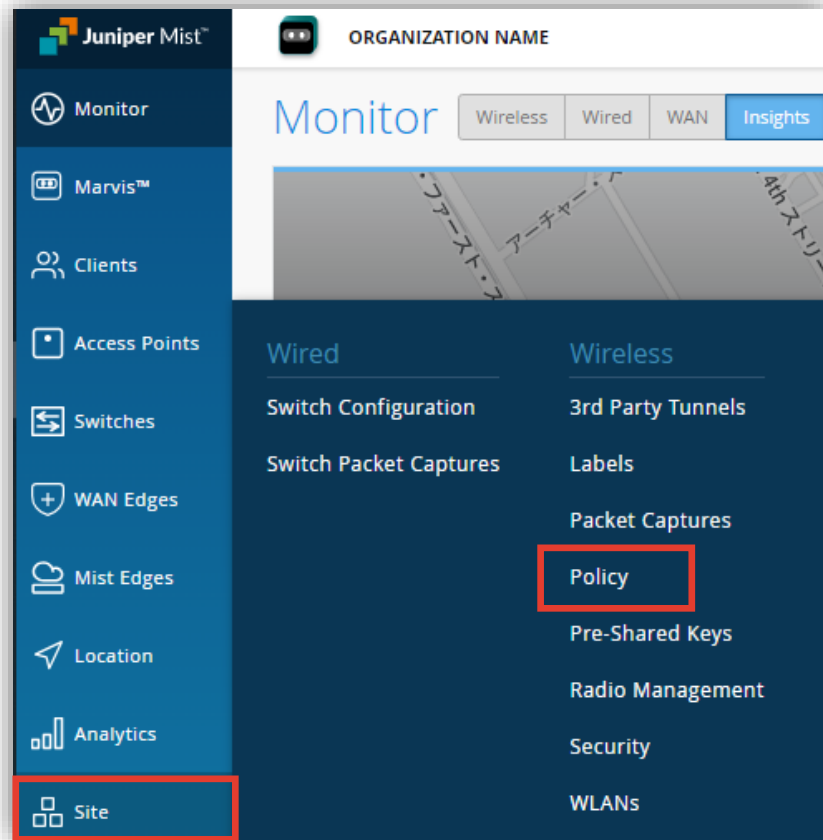
作成が必要なラベル

作成するラベル

Name	Type	Values
Private Address (RFC1918)	IP Address	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
WLANS	WLAN	WLAN_01,WLAN_02
Guest	WLAN	Guest

WxLAN(アクセス制御ポリシー)の設定

1. [Site] から [Policy] を選択します



2. [Add Rule] をクリックします



WxLAN(アクセス制御ポリシー)の設定

3. User のラベルを選択します
[+] から WLANs を選択

The screenshot shows the 'Policy' configuration page for 'Primary Site'. A table lists policy rules. The first rule is selected, and the 'User' column shows 'All Users'. A red box highlights a '+' icon in the 'User' column, with a callout box containing a larger '+' icon. A dropdown menu is open below the table, showing 'WLANs' selected and highlighted with a red box. Other options include 'Guest' and 'Edit Labels'.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	All Users	✓	All Resources	0

4. Resource のラベルを選択します
[+] から Youtube を選択

The screenshot shows the 'Policy' configuration page for 'Primary Site'. The table from the previous step is visible. A red box highlights a '+' icon in the 'Resource' column, with a callout box containing a larger '+' icon. A dropdown menu is open below the table, showing 'Youtube' selected and highlighted with a red box. Other options include 'Netflix', 'Pandora', 'Spotify', 'Twitch', 'Mixr', 'Vimeo', 'TeamViewer', 'Wikipedia', 'StackOverflow', and 'Github'.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	All Users	✓	All Resources	0

WxLAN(アクセス制御ポリシー)の設定

5. 同様に、Facebook を Resource に追加

The screenshot shows the 'Policy' configuration page for 'site Primary Site'. Under 'Site Policies', there is a table with one rule. The 'Resource' column for this rule currently contains 'Youtube'. A red box highlights a plus sign (+) next to 'Youtube', and a callout bubble with a plus sign points to it. A search dropdown menu is open, showing various resource categories. 'Facebook' is highlighted in red in the dropdown list.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ WLANs ×	✓	Youtube × +	0

Search dropdown items: Private Address(RFC1918) IP Address, All Emails Emails, Gmail Emails, Yahoo Mail Emails, Dropbox File Sharing, iCloud backup Online Backup, All Socials Social, Facebook Social, Flickr Social, Pinterest Social, Snapchat Social.

6. [Add Rule] でポリシーを追加します

The screenshot shows the 'Policy' configuration page for 'site Primary Site'. The 'Add Rule' button is highlighted with a red box. The table below shows two rules. The first rule has 'WLANs' in the User column and 'Facebook' and 'Youtube' in the Resource column. The second rule has 'All Users' in the User column and 'All Resources' in the Resource column.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ WLANs ×	✓	Facebook × Youtube × +	0
Last	All Users	✓	All Resources	

WxLAN(アクセス制御ポリシー)の設定

7. User のラベルを選択します
[+] から Guest を選択

Policy site Primary Site Save Cancel

Site Policies
Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	...
<input type="checkbox"/>	1	+ All Users	→ ✓ →	All Resources +	0	...
<input type="checkbox"/>	2	+ Search	→ ✓ →	Facebook × Youtube × +	0	...
	Last					

Guest WLAN

Edit Labels Close

8. Resource のラベルを選択します
[+] から Private Address (RFC1918) を選択

Policy site Primary Site Save Cancel

Site Policies
Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	...
<input type="checkbox"/>	1	+ Guest ×	→ ✓ →	All Resources +	0	...
<input type="checkbox"/>	2	+ WLANs ×	→ ✓ →	Search	0	...
	Last	All Users				

Private Address(RFC1918) IP Address

All Emails Emails
Gmail Emails
Yahoo Mail Emails
Dropbox File Sharing
iCloud backup Online Backup
All Socials Social
Facebook Social
Flickr Social
Pinterest Social
Snapchat Social

Edit Labels Close

WxLAN(アクセス制御ポリシー)の設定

9. Resource のポリシーを Deny に変更します

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	Private Address(RFC1918)	Private Address(RFC1918)	0
2	+ WLANs	Facebook Youtube	Facebook Youtube	0
Last	All Users	All Resources		

IP Address

172.16.0.0/12, 192.168.0.0/16

Allow Deny

クリックして Deny に変更

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	Private Address(RFC1918)	Private Address(RFC1918)	0
2	+ WLANs	Facebook Youtube	Facebook Youtube	0
Last	All Users	All Resources		

IP Address

172.16.0.0/12, 192.168.0.0/16

Allow Deny

クリックして Deny に変更

10. デフォルトポリシー (Last) を Block に変更します

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	Private Address(RFC1918)	Private Address(RFC1918)	0
2	+ WLANs	Facebook Youtube	Facebook Youtube	0
Last	All Users	All Resources		

Allow Deny

クリック

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	Private Address(RFC1918)	Private Address(RFC1918)	0
2	+ WLANs	Facebook Youtube	Facebook Youtube	0
Last	All Users	All Resources		

Allow Deny Block

Block を選択

WxLAN(アクセス制御ポリシー)の設定

11.[Save] で保存します

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest x	✓	Private Address(RFC1918) x +	0
2	+ WLANs x	✓	Facebook x Youtube x +	0
Last	All Users	✗	All Resources	

Save Cancel

追加したポリシーにマッチしない場合、通信をブロックする

ポリシー設定例(再掲)

User	Resource	備考
WLANs	Youtube / Facebook	Youtube / Facebook へのアクセスをブロック
Guest	Private Address (RFC1918)	プライベートアドレスへの通信をブロック
All Users	All Resources	デフォルトポリシー(Last)で通信をブロック

WxLAN(アクセス制御ポリシー)の設定の注意点!!



最初にマッチしたポリシーにより処理されます

下記のような場合、WLANs に対する No.2 のポリシーは評価されず、WLANs は Youtube へのアクセスが可能です

Policy site Primary Site Save Cancel

Site Policies
Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.
Add Rule Edit Labels

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	
<input type="checkbox"/>	1	+ WLANs x	→ ✓ →	Facebook x +	0	...
<input type="checkbox"/>	2	+ WLANs x	→ ✓ →	Youtube x +	0	...
	Last	All Users	→ ✗ →	All Resources		

First Match により No.2 は評価されない
→ WLANs は Youtube へアクセスできる

Facebook と Youtube 両方へのアクセスを制限する場合は、同一ポリシーの Resource に並べて設定します

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	
<input type="checkbox"/>	1	+ WLANs x	→ ✓ →	Facebook x Youtube x +	0	...
	Last	All Users	→ ✗ →	All Resources		

ポリシーの順番の入れ替え

ポリシーの順番入れ替え

1. ポリシーを選択
2. 順番を入れ替え (Move Up/Move Down、または ↑ ↓ で移動)
3. Save をクリックして設定を保存

Policy site Primary Site

3 Save Cancel

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

2 ↑ ↓ Enable Disable

<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	...
<input type="checkbox"/>	1	+ WLAN-2 ×	→ ✓ →	Youtube × +	0	...
<input checked="" type="checkbox"/>	2	+ All Users	→ ✓ →	local × +	0	...
<input type="checkbox"/>	3	+ All Users	→ ✓ →	Netflix × +	0	...
		All Users	→ ✓ →	All Resources		

1

ドラッグ&ドロップでも
入れ替え可能

※ (・・・)からも入替可能

Enable
Disable
Move Up
Move Down
Delete

ポリシーの有効化・無効化

※ポリシー選択、上部の Enable/Disable ボタンでも変更可能

ポリシーの有効化/無効化

1. Policy の右側の(⋮)をクリック
2. Enable/Disable を選択
3. Save をクリックして設定を保存

The screenshot shows the 'Policy' configuration page for 'site Primary Site'. It displays a table of Site Policies with columns for No., User, Policy, Resource, and Usage. The second policy (No. 2) is selected, and its context menu is open, showing 'Enable' and 'Disable' options. The 'Save' button is highlighted, indicating the final step of the process.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ WLAN-2	✓	Youtube	0
2	+ All Users	✓	local	0
3	+ All Users	✓	Netflix	0
Last	All Users	✓	All Resources	

無効化されたポリシーはグレースアウト

ポリシーの削除

ポリシーの削除

1. ポリシーを選択
2. ごみ箱アイコンをクリック
3. Save をクリックして設定を保存

Policy site Primary Site

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)	
1	+ WLAN-2 x	✓	Youtube x +	0	...
2	+ All Users	✓	local x +	0	...
3	+ All Users	✓	Netflix x +	0	
Last	All Users	✓	All Resources		

Enable Disable

Enable Disable Move Up Move Down Delete

※ (・・・)からも削除可能

Thank you

JUNIPER
driven by Mist AI 