

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
2021年7月 Ver 1.0

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 2021年7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>

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(「Network」>「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)

		送信元 (User)		宛先 (Resource)	Usage (No. Sessions)
<input type="checkbox"/>	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	
<input type="checkbox"/>	1	+ Guest users ×	→ ✓	Internet × Intranet × +	0
<input type="checkbox"/>	2	+ Employee_SETraining ×	→ ✓	Facebook × +	0
<input type="checkbox"/>	3	+ User 3 Mac ×	→ ✓	Social Network × +	0
<input type="checkbox"/>	4	+ Terminal 3 ×	→ ✗	All Resources +	0
<input type="checkbox"/>	5	+ Guest-Open ×	→ ✓	Canon\ MG5500\ series ×	0
<input type="checkbox"/>		+ Guest-Open ×	→ ✓	Internet × +	0
		Last	→ ✓	All Resources	

アプリケーション → Deny(赤)動作のみ

ユーザ定義の Resource → Allow(緑) or Deny(赤)

Label (User)

Label (Resource)

デフォルトポリシー

The screenshot shows a table of WxLAN policies. The 'User' column lists various users, some with custom labels like 'User 3 Mac' and 'Terminal 3'. The 'Resource' column lists system-defined resources like 'Internet', 'Intranet', 'Facebook', and 'Social Network' (all in red boxes, indicating Deny actions), and user-defined resources like 'Canon\ MG5500\ series' and 'Internet' (in green boxes, indicating Allow actions). A callout box points to the red boxes with the text 'アプリケーション → Deny(赤)動作のみ'. Another callout box points to the green boxes with the text 'ユーザ定義の Resource → Allow(緑) or Deny(赤)'. A third callout box points to the 'User' column with the text 'Label (User)'. A fourth callout box points to the 'Resource' column with the text 'Label (Resource)'. A fifth callout box points to the 'Last' policy row with the text 'デフォルトポリシー'. A legend on the right shows a red box with 'Deny' and a green box with 'Allow'.

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 Live Demo

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	+ Contractor × Guest users × Lab AP ×	→ ✓ →	Internet × Intranet × +	0 ...
2	+ Employee_SETraining ×	→ ✓ →	Facebook × +	0 ...
3	+ User 3 Mac ×	→ ✓ →	Social Network × +	0 ...
4	+ Terminal 3 ×	→ ✗ →	All Resources +	0 ...
5	+ Guest-Open ×	→ ✓ →	Canon\ MG5500\ series × Internet × +	0 ...
Last	All Users	→ ✓ →	All Resources	

Save

※ Save で設定を保存

✗ Block

✓ Allow

✗ Block

※ Last でどのポリシーにもマッチしない場合の動作を指定

Hostname ×

www.yahoo.co.jp

Allow Deny

yahoo × +

Deny ✗

Allow ✗

※ 定義した Resource のラベルは、Allow/Deny の選択が可能

ラベルの概要

- ラベルには Label Name, Label Type, Label Values を設定します
- WxLAN(アクセス制御ポリシー)への設定が可能な Label Type は 8 項目 (右表)
- Label Type 毎にポリシーの適用可能な箇所 (User/Resource) が決まっている (右表)

The screenshot shows the configuration interface for a label. It is divided into three main sections:

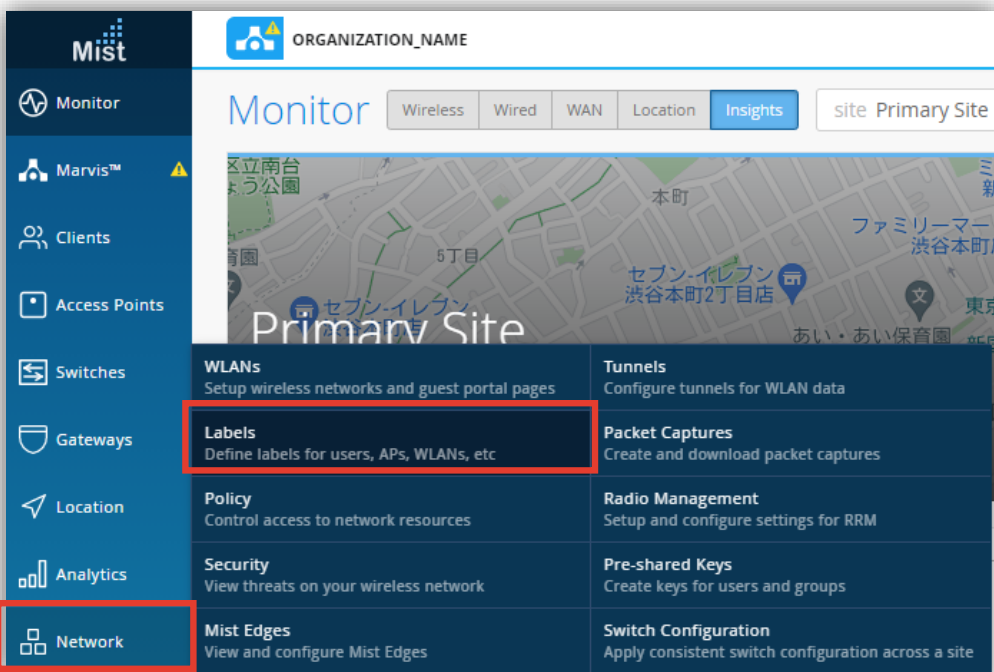
- ラベル名 (Label Name):** A text input field containing "New Label".
- ラベルタイプ (Label Type):** A dropdown menu currently set to "IP Address". Below the dropdown, it says "This is a Resource label if used in WxLan".
- ラベルに紐づけるオブジェクト (Label Values):** A text area with the placeholder "Add IPs". Above the text area, it says "List of IP (xxx.xxx.xxx.xxx), or CIDR (xxx.xxx.xxx.xxx/xx)".

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

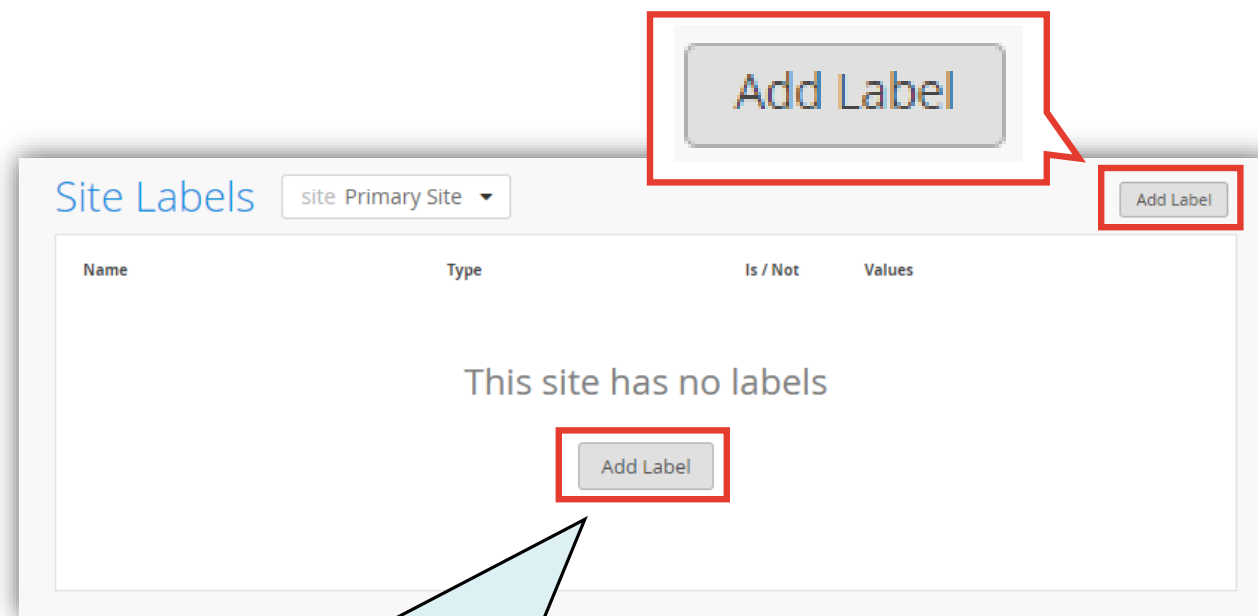
※ WiFi Client Name, BLE Asset, App Client は Policy に適用不可

ラベルの作成

1. [Network] から [Labels] を選択します



2. [Add Label] をクリックします



ラベルを一つも作成していない場合は
こちらをクリックしても可

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
- 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

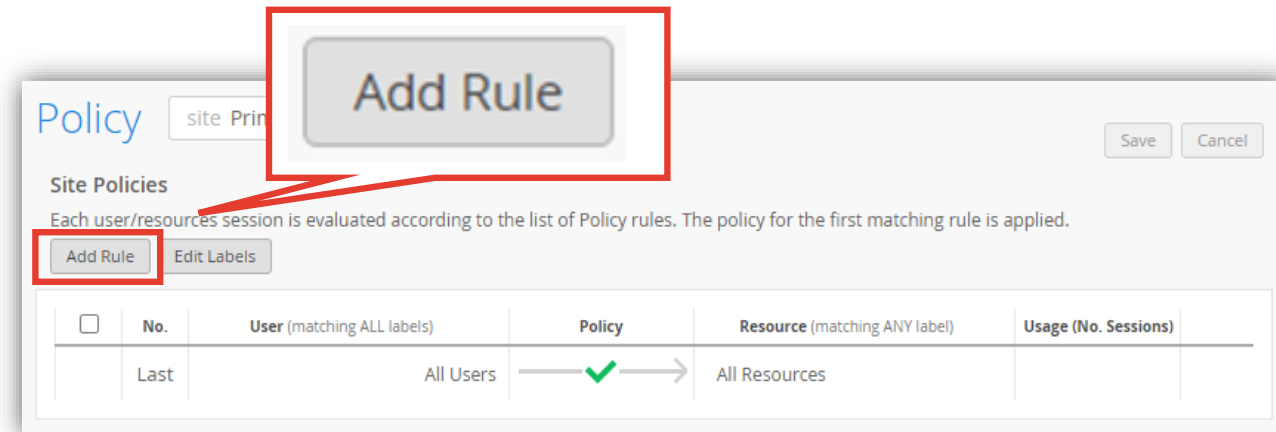
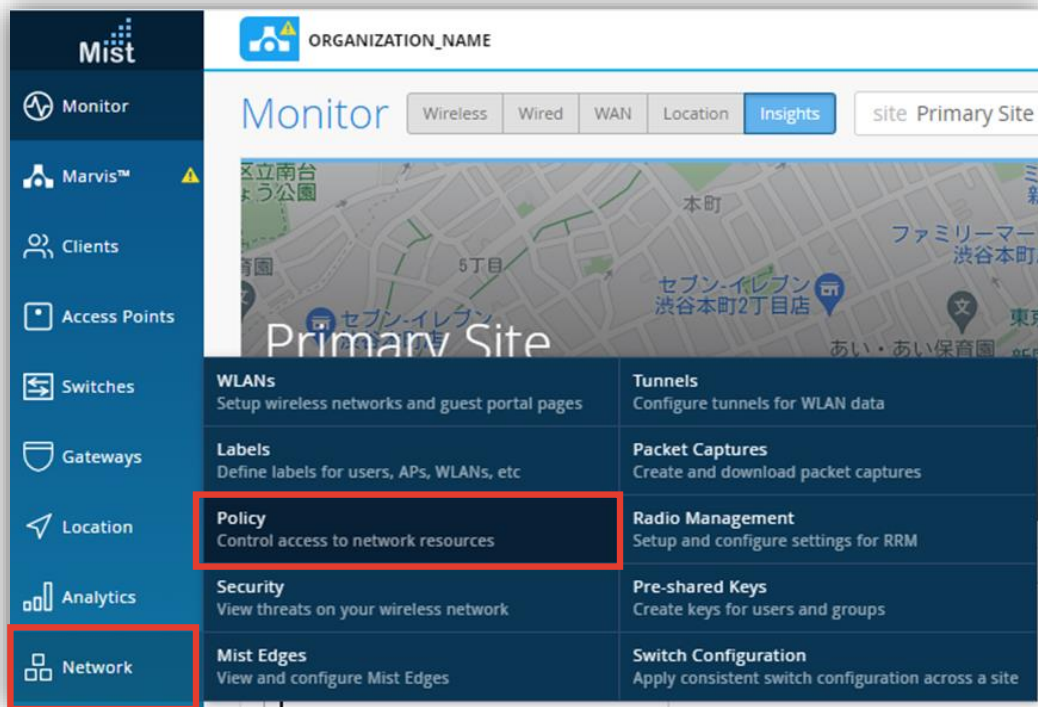
作成するラベル

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. [Network] 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 'site Primary Site'. A table lists policy rules. The first rule has 'All Users' as the user label. A red box highlights the '+' icon in the 'User' column, and a callout bubble points to it. A dropdown menu is open below the table, showing 'WLANs' selected and highlighted with a red box. Other options include 'Guest' and 'WLAN'. The 'Policy' column shows a green checkmark and arrow, and the 'Resource' column shows 'All Resources' with a '+' icon.

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 'site Primary Site'. A table lists policy rules. The first rule has 'All Resources' as the resource label. A red box highlights the '+' icon in the 'Resource' column, and a callout bubble points to it. A dropdown menu is open below the table, showing 'Youtube' selected and highlighted with a red box. Other options include 'Netflix', 'Pandora', 'Spotify', 'Twitch', 'Mixer', 'Vimeo', 'TeamViewer', 'Wikipedia', 'StackOverflow', and 'Github'. The 'Policy' column shows a green checkmark and arrow, and the 'User' column shows 'All Users'.

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'. A table lists existing rules. The first rule has 'WLANs' as the Resource. A red box highlights a '+' icon in the top right of the table, and another red box highlights a '+' icon at the end of the 'Resource' column for the first rule. A search dropdown is open, showing a list of resources with 'Facebook' highlighted in red.

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

Search results:

- 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' as the Resource, and the second rule has 'Facebook' and 'Youtube' as Resources.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ WLANs x	→ ✓ →	Facebook x Youtube x +	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

The screenshot shows the 'Policy' configuration page for 'Primary Site'. A red box highlights a '+' icon in the 'User' column of the first policy rule. A dropdown menu is open, showing 'Guest' selected. The table below shows the configuration for two policy rules.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ All Users	→ ✓ →	All Resources +	0
2	+ [Search] [WLANs] [Guest] [WLAN]	→ ✓ →	[Facebook] [Youtube] + [Resources]	0

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

The screenshot shows the 'Policy' configuration page for 'Primary Site'. A red box highlights a '+' icon in the 'Resource' column of the first policy rule. A dropdown menu is open, showing 'Private Address(RFC1918)' selected. The table below shows the configuration for two policy rules.

No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	→ ✓ →	All Resources +	0
2	+ [WLANs]	→ ✓ →	[Search] [Private Address(RFC1918)] [IP Address] [Youtube] +	0

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 dialog: 172.16.0.0/12, 192.168.0.0/16. Buttons: 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 dialog: 172.16.0.0/12, 192.168.0.0/16. Buttons: Allow, Deny.

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		

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.

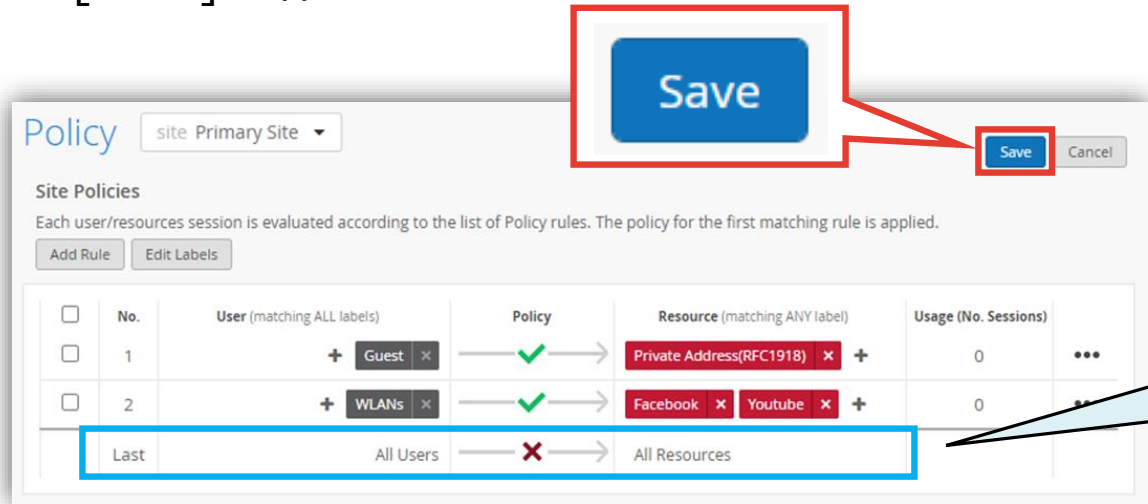
No.	User (matching ALL labels)	Policy	Resource (matching ANY label)	Usage (No. Sessions)
1	+ Guest	Private Address(RFC1918)	Private Address(RFC1918)	0
2	+ WLANs	Facebook Youtube	Facebook Youtube	0
Last	All Users	Block	All Resources	

Policy dropdown: Allow, Allow, 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



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

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

The screenshot shows the 'Policy' configuration page for 'site Primary Site'. It features a table of 'Site Policies' with columns for 'No.', 'User', 'Policy', 'Resource', and 'Usage'. The second policy is selected, and a context menu is open over it, showing options like 'Move Up', 'Move Down', and 'Delete'. Annotations 1, 2, and 3 highlight the selection checkbox, the reordering buttons, and the 'Save' button respectively.

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	

ドラッグ&ドロップでも
入れ替え可能

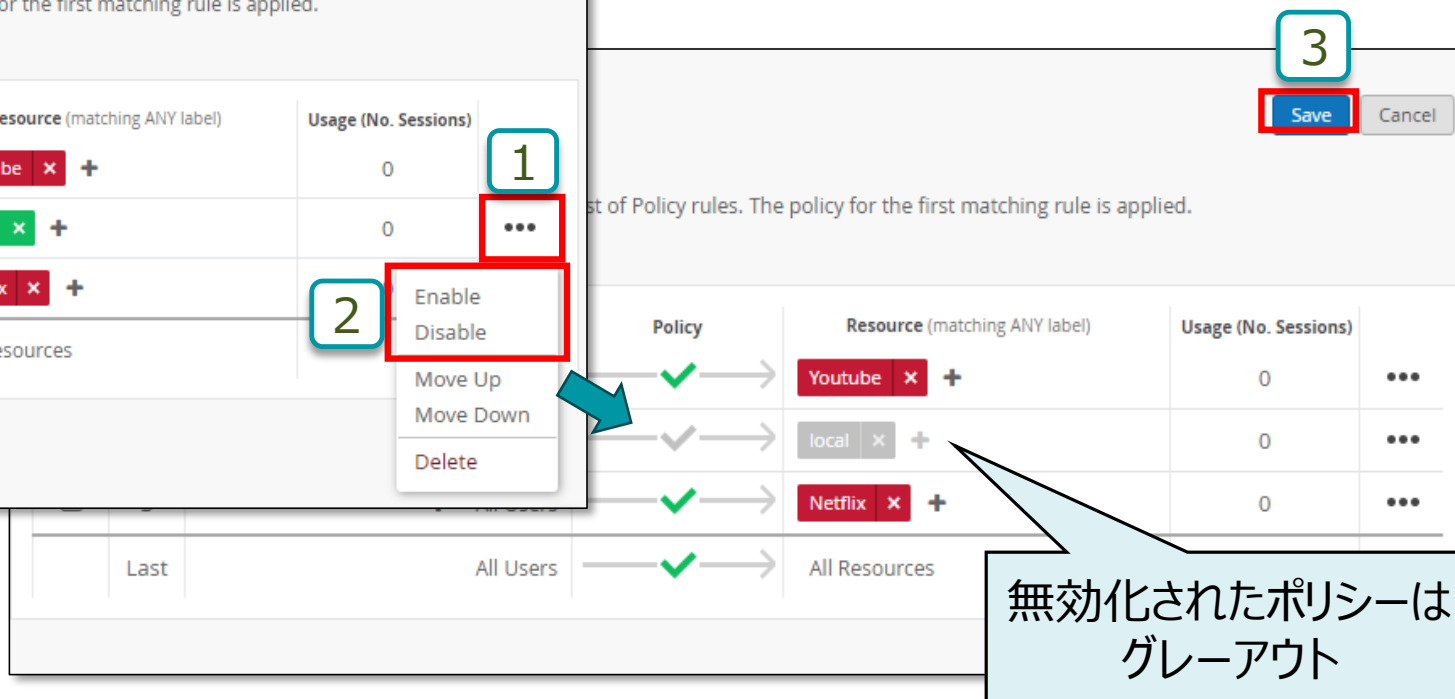
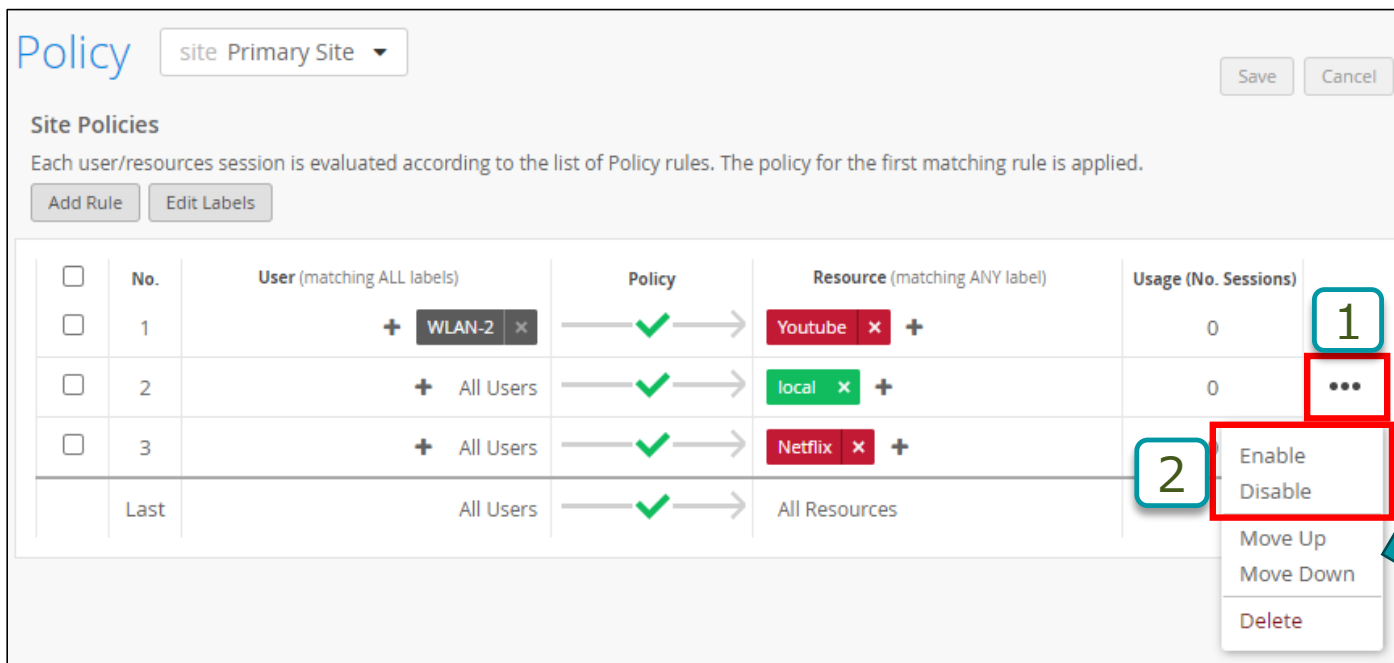
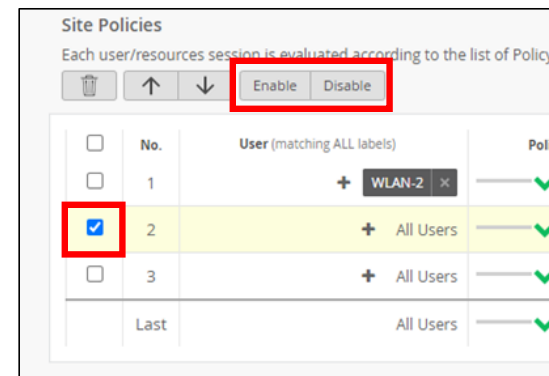
※ (···)からも入替可能。

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



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

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'. Policy 2 is selected. A red box highlights the trash icon in the toolbar (labeled '2'). Another red box highlights the 'Save' button (labeled '3'). A third red box highlights the 'Delete' option in the context menu for policy 2 (labeled '1').

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		

※ (⋮)からも削除可能。