

**Mist 設定マニュアル**  
**- Wired Assurance -**  
**PROTECTION OF ROUTING ENGINE 設定**

---

ジュニパーネットワークス株式会社  
2024年2月 Ver 1.0

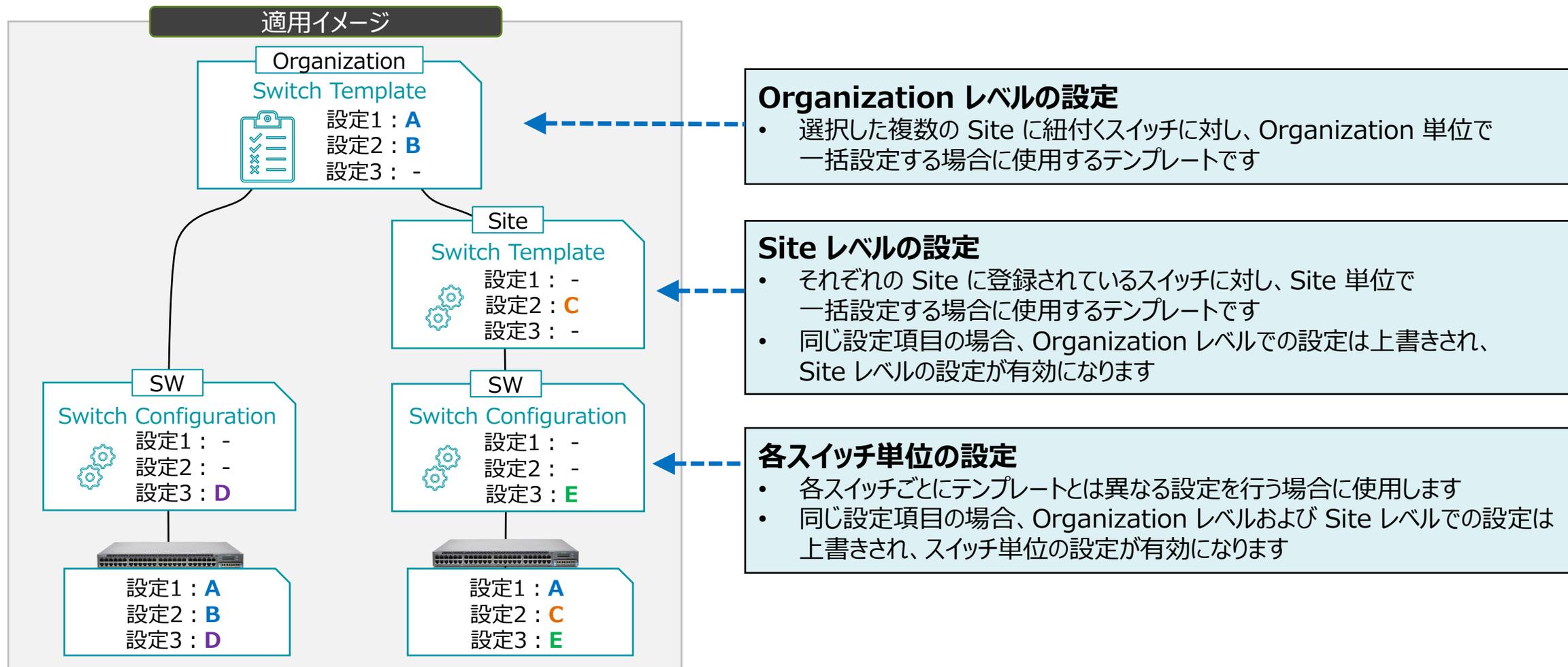


# はじめに

- ❖ 本マニュアルは、『Wired Assurance におけるスイッチへの PROTECTION OF ROUTING ENGINE の設定』について説明します
- ❖ 手順内容は 2024年2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>
- ❖ **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**

# テンプレートを使用した設定の概要

Mist の管理画面からスイッチに対し、テンプレートを使用した設定が可能です

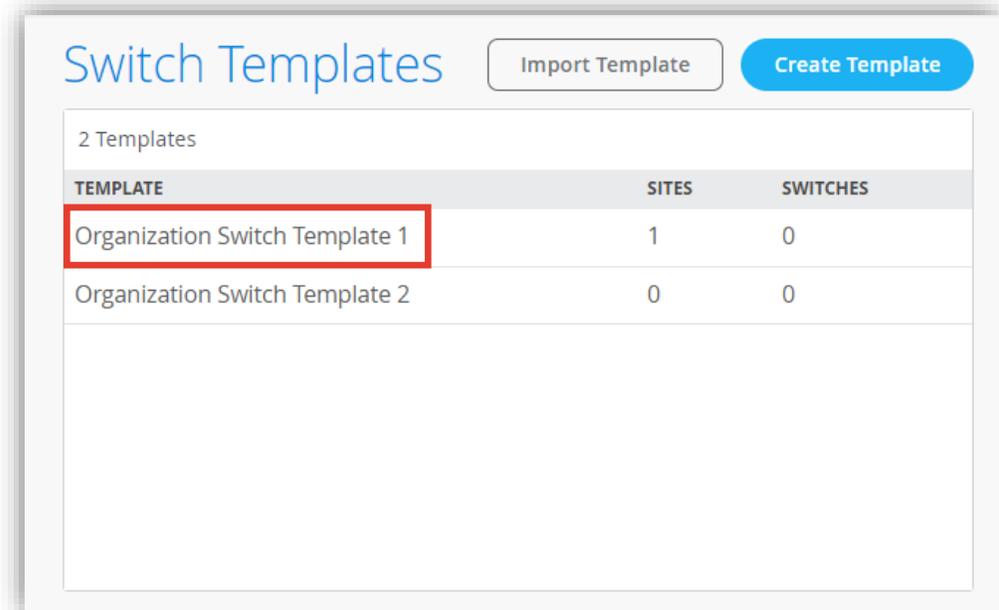
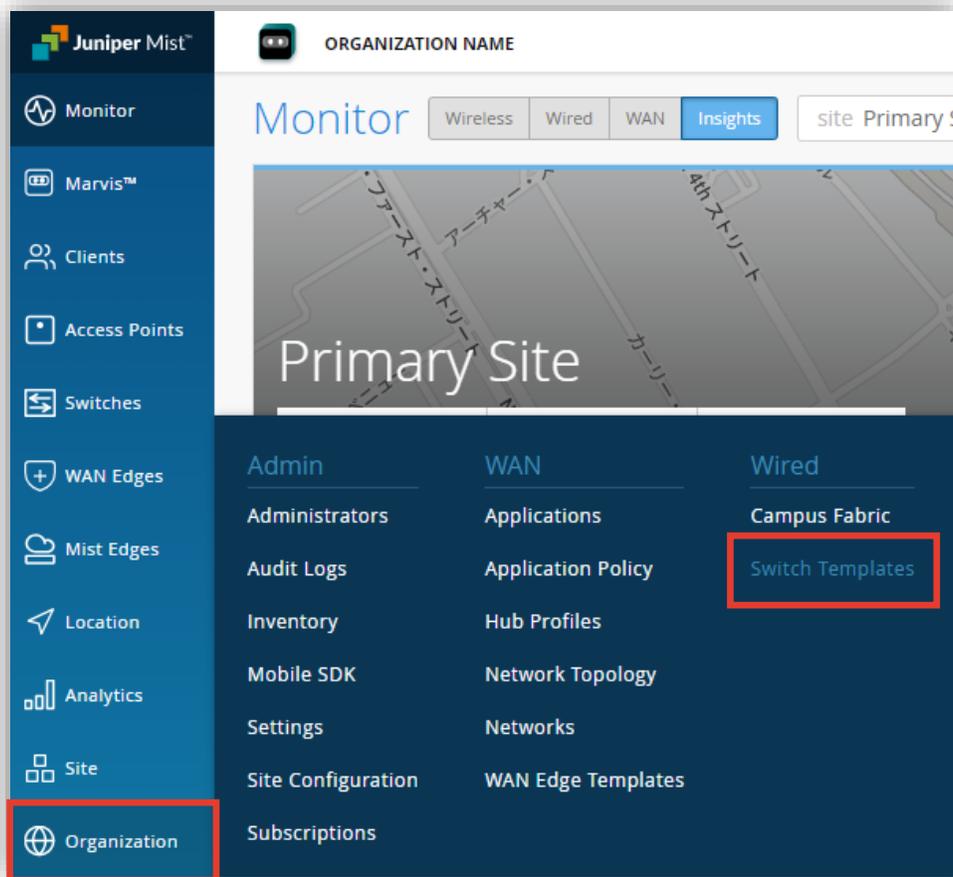


# Organization レベルの PROTECTION OF ROUTING ENGINE 設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

1. [Organization] から [Switch Templates] を  
選択します

2. 編集対象の [Switch Template] を選択します



# Organization レベルの PROTECTION OF ROUTING ENGINE 設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

3. [Management] 内の「PROTECTION OF ROUTING ENGINE」の項目にて設定を行います

Management

CONFIGURATION REVERT TIMER ⓘ

Configuration Revert Timer

10

ROOT PASSWORD

Root Password

Reveal

PROTECTION OF ROUTING ENGINE ⓘ

Protect Routing Engine

Enabled  Disabled

有効化により信頼できない送信元からルーティングエンジンを保護することができます

# Organization レベルの PROTECTION OF ROUTING ENGINE 設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

## 4. [Enabled] を選択し、設定を行います

The screenshot shows the configuration page for 'PROTECTION OF ROUTING ENGINE'. The 'Protect Routing Engine' section has the 'Enabled' radio button selected and highlighted with a red box. The 'Trusted Networks' field contains '192.168.1.0'. The 'Trusted Services' section has 'icmp' and 'ssh' checked. The 'Trusted IP/Protocol/Port' section has an 'Add IP/Protocol/Port' button. Three callout boxes with dashed blue arrows point to these elements: the 'Trusted Networks' field, the 'Trusted Services' section, and the 'Add IP/Protocol/Port' button.

**PROTECTION OF ROUTING ENGINE** ⓘ

Protect Routing Engine  
 Enabled  Disabled

Trusted Networks ⓘ  
192.168.1.0  
(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ  
 icmp  
 ssh

Trusted IP/Protocol/Port ⓘ [Add IP/Protocol/Port](#)

IP Address	Protocol	Port Range
------------	----------	------------

スイッチへのアクセスを許可するネットワークを設定します

スイッチが PING に応答できるようにする場合、icmp オプションを選択します  
スイッチに SSH 接続できるようにする場合、ssh オプションを選択します

スイッチへのアクセスを許可する IP /ポート/プロトコルを設定します

# Organization レベルの PROTECTION OF ROUTING ENGINE 設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

5. スイッチへのアクセスを許可する IP /ポート/プロトコルを [Add IP/Protocol/Port] をクリックし設定します
6. 設定内容を入力し、[Add] をクリックします

PROTECTION OF ROUTING ENGINE ⓘ

Protect Routing Engine

Enabled  Disabled

Trusted Networks ⓘ

192.168.1.0

(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ

icmp

ssh

Trusted IP/Protocol/Port ⓘ **Add IP/Protocol/Port**

IP Address	Protocol	Port Range
------------	----------	------------

Add Trusted IP/Protocol/Port

IP Address

100.100.100.1

(Comma-separated list of IP addresses or CIDRs)

Protocol

ICMP

Port Range

(Port range 1-65535. Single port or dash-separated range of ports)

Port Range を指定しない場合は Any となります

Trusted IP/Protocol/Port ⓘ	Add IP/Protocol/Port	
IP Address	Protocol	Port Range
100.100.100.1	ICMP	Any

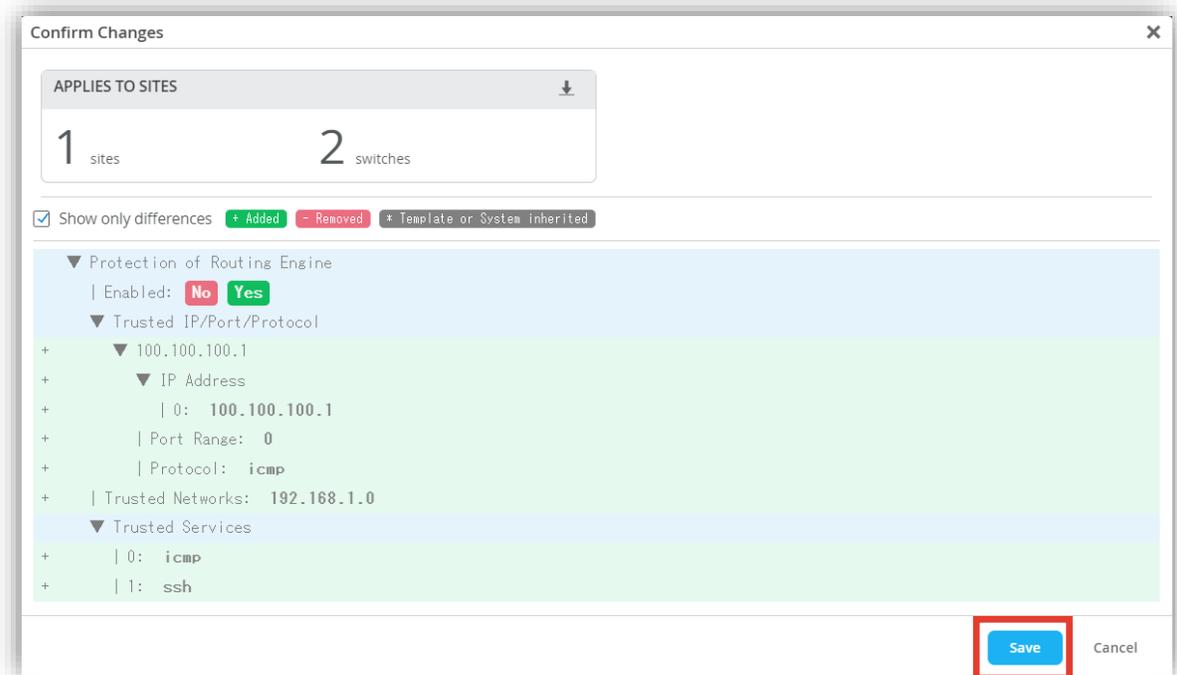
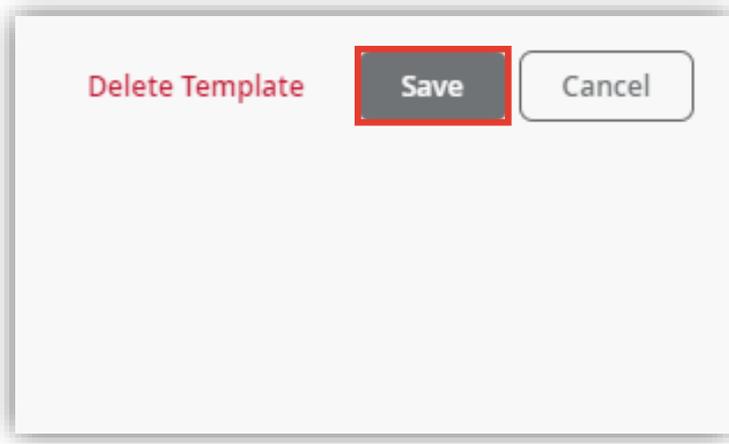
**Add** Cancel

# Organization レベルの PROTECTION OF ROUTING ENGINE 設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

7. [Save] をクリックし編集内容を保存します

8. 変更の差分が表示されるので、確認して再度 [Save] をクリックします

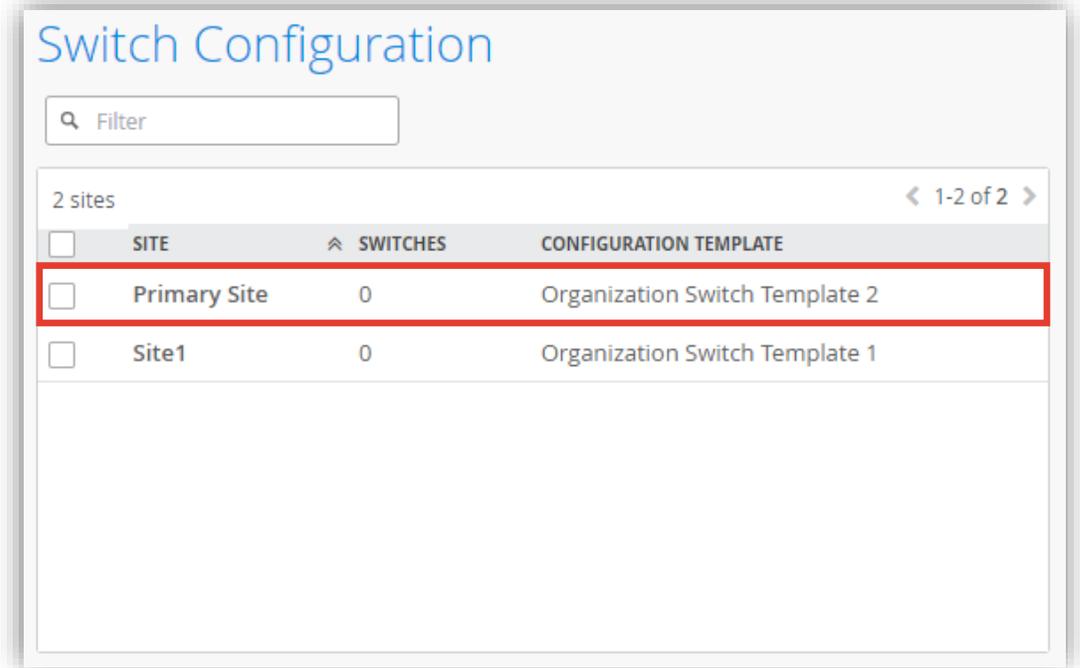
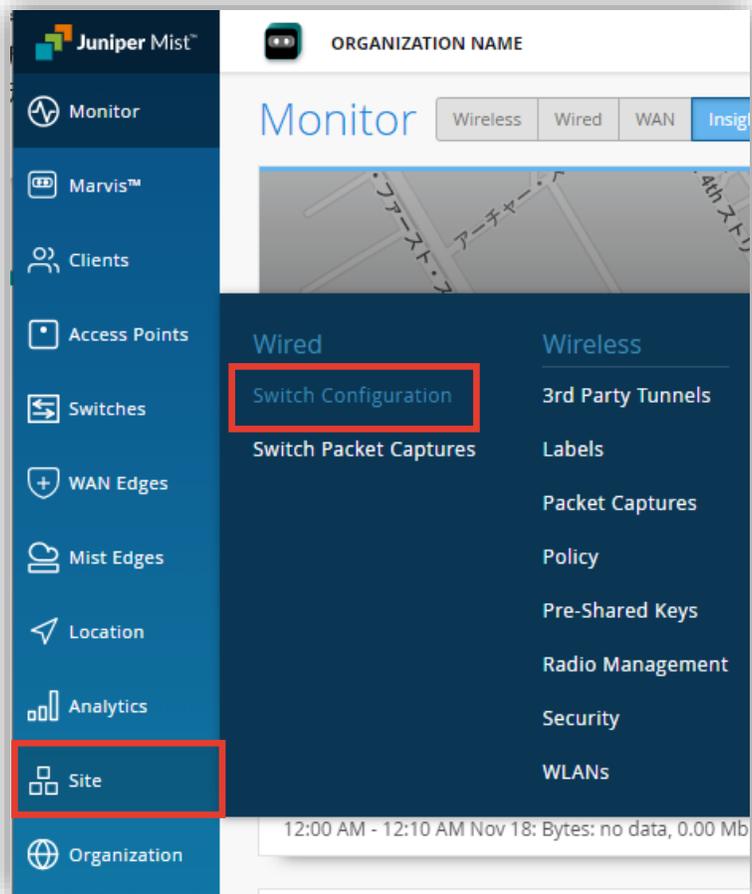


# Site レベルの PROTECTION OF ROUTING ENGINE 設定

Site ごとに設定を変更する場合

1. [Site] から [Switch Configuration] を  
選択します

2. 編集対象の [Site] を選択します



# Site レベルの PROTECTION OF ROUTING ENGINE 設定

Site ごとに設定を変更する場合

3. [Management] 内の「PROTECTION OF ROUTING ENGINE」の項目にて設定を行います
4. Site に Organization レベルのテンプレートを適用している場合、入力欄等がグレーアウトされています  
Organization レベルのテンプレートを上書きする場合は [Override Configuration Template] にチェックを入れます

The screenshot shows the Management interface for the PROTECTION OF ROUTING ENGINE configuration. The interface is divided into three main sections:

- CONFIGURATION REVERT TIMER**: Includes an unchecked checkbox for "Override Configuration Template" and a "Configuration Revert Timer" input field set to "10".
- ROOT PASSWORD**: Includes an unchecked checkbox for "Override Configuration Template" and a "Root Password" input field with a "Reveal" button.
- PROTECTION OF ROUTING ENGINE**: Includes a checked checkbox for "Override Configuration Template" (highlighted with a red box), and "Protect Routing Engine" radio buttons set to "Disabled".

# Site レベルの PROTECTION OF ROUTING ENGINE 設定

Site ごとに設定を変更する場合

## 5. [Enabled] を選択し、設定を行います

PROTECTION OF ROUTING ENGINE ⓘ

Override Configuration Template

Protect Routing Engine

Enabled  Disabled

Trusted Networks ⓘ

192.168.1.0

(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ

icmp

ssh

Trusted IP/Protocol/Port ⓘ [Add IP/Protocol/Port](#)

IP Address	Protocol	Port Range
------------	----------	------------

スイッチへのアクセスを許可するネットワークを設定します

スイッチが PING に応答できるようにする場合、icmp オプションを選択します  
スイッチに SSH 接続できるようにする場合、ssh オプションを選択します

スイッチへのアクセスを許可する IP /ポート/プロトコルを設定します

# Site レベルの PROTECTION OF ROUTING ENGINE 設定

Site ごとに設定を変更する場合

6. スイッチへのアクセスを許可する IP /ポート/プロトコルを [Add IP/Protocol/Port] をクリックし設定します

7. 設定内容を入力し、[Add] をクリックします

PROTECTION OF ROUTING ENGINE ⓘ

Override Configuration Template

Protect Routing Engine

Enabled  Disabled

Trusted Networks ⓘ

192.168.1.0

(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ

icmp

ssh

Trusted IP/Protocol/Port ⓘ **Add IP/Protocol/Port**

IP Address	Protocol	Port Range
------------	----------	------------

Add Trusted IP/Protocol/Port

IP Address

10.10.10.1

(Comma-separated list of IP addresses or CIDRs)

Protocol

ICMP

Port Range

(Port range 1-65535. Single port or dash-separated range of ports)

Port Range を指定しない場合は Any となります

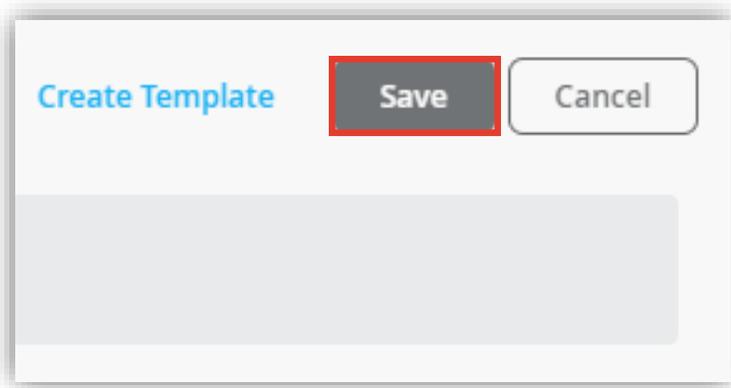
Trusted IP/Protocol/Port ⓘ	Add IP/Protocol/Port	
IP Address	Protocol	Port Range
10.10.10.1	ICMP	Any

**Add** Cancel

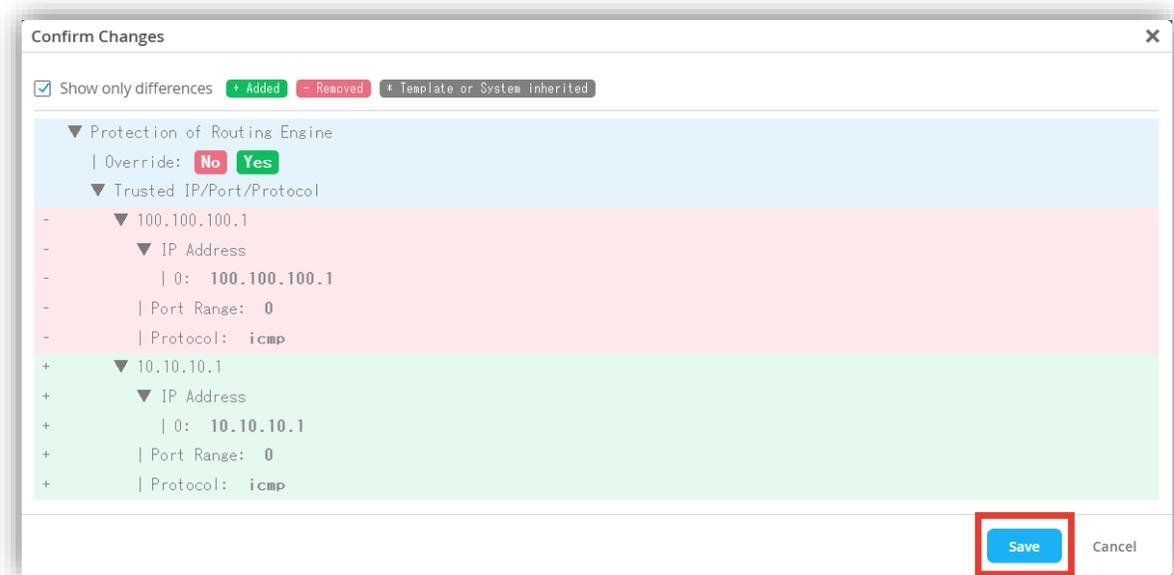
# Site レベルの PROTECTION OF ROUTING ENGINE 設定

Site ごとに設定を変更する場合

8. [Save] をクリックし編集内容を保存します



9. 変更の差分が表示されるので、確認して再度 [Save] をクリックします



# スイッチ単位の PROTECTION OF ROUTING ENGINE 設定

スイッチごとに設定を変更する場合

1. 各スイッチごとに設定を変更する場合は、[Switches] を選択し、一覧から変更対象となる [スイッチ] をクリックします

Juniper Mist™ LIVE DEMO MON 5:17 PM

16 Switches site Live-Demo List Topology Location 5:16:48 PM (updates every 3 minutes) Inventory

13 Cloud Connected Switches 3 Discovered Switches 48 Wired Clients 272 W Total Allocated AP Power

67% Switch-AP Affinity 93% PoE Compliance 100% VLANs 73% Version Compliance > 99% Switch Uptime 88% Config Success

Filter

<input type="checkbox"/>	Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Role
<input type="checkbox"/>	Connected	ld-cup-idf-d-desktop	192.168.2.91	EX2300-C-12P	1	0	4	--
<input type="checkbox"/>	Connected	ld-cup-idf-d	192.168.2.133	EX4100-48MP	0	0	--	--
<input type="checkbox"/>	Connected	ld-cup-idf-bb	10.100.0.212	EX4100-48MP	3	3	10	--
<input type="checkbox"/>	Connected	ld-cup-idf-a-core	10.100.1.47	EX4100-48MP	1	0	7	--
<input type="checkbox"/>	Connected	ld-cup-idf-c	10.100.0.121	EX4100-48MP	3	0	5	--
<input type="checkbox"/>	Connected	ld-cup-idf-d-desktop-22	10.100.0.114	EX4100-F-12P	0	0	2	--
<input type="checkbox"/>	Connected	ld-cup-idf-d-sw440000	192.168.2.95	EX4400-48T	0	0	1	--

# スイッチ単位の PROTECTION OF ROUTING ENGINE 設定

スイッチごとに設定を変更する場合

2. [Management] 内の「PROTECTION OF ROUTING ENGINE」の項目にて設定を行います
3. テンプレートを適用している場合は項目がグレーアウトされています  
設定を上書きする場合は [Override Site/Template Settings] にチェックを入れます

Management

CONFIGURATION REVERT TIMER ⓘ

Override Site/Template Settings

Configuration Revert Timer

10

ROOT PASSWORD

Override Site/Template Settings

Root Password

Reveal

PROTECTION OF ROUTING ENGINE ⓘ

Override Site/Template Settings

Protect Routing Engine

Enabled  Disabled

# スイッチ単位の PROTECTION OF ROUTING ENGINE 設定

スイッチごとに設定を変更する場合

## 4. [Enabled] を選択し、設定を行います

PROTECTION OF ROUTING ENGINE ⓘ

Override Site/Template Settings

Protect Routing Engine

Enabled  Disabled

Trusted Networks ⓘ

192.168.1.0

(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ

icmp

ssh

Trusted IP/Protocol/Port ⓘ [Add IP/Protocol/Port](#)

IP Address	Protocol	Port Range
------------	----------	------------

スイッチへのアクセスを許可するネットワークを設定します

スイッチが PING に応答できるようにする場合、icmp オプションを選択します  
スイッチに SSH 接続できるようにする場合、ssh オプションを選択します

スイッチへのアクセスを許可する IP /ポート/プロトコルを設定します

# スイッチ単位の PROTECTION OF ROUTING ENGINE 設定

スイッチごとに設定を変更する場合

5. スイッチへのアクセスを許可する IP /ポート/プロトコルを [Add IP/Protocol/Port] をクリックし設定します

6. 設定内容を入力し、[Add] をクリックします

PROTECTION OF ROUTING ENGINE ⓘ

Override Site/Template Settings

Protect Routing Engine

Enabled  Disabled

Trusted Networks ⓘ

192.168.1.0

(Comma-separated list of IP addresses or CIDRs)

Trusted Services ⓘ

icmp

ssh

Trusted IP/Protocol/Port ⓘ **Add IP/Protocol/Port**

IP Address	Protocol	Port Range
------------	----------	------------

Add Trusted IP/Protocol/Port

IP Address

1.1.1.1

(Comma-separated list of IP addresses or CIDRs)

Protocol

ICMP

Port Range

(Port range 1-65535. Single port or dash-separated range of ports)

Port Range を指定しない場合は Any となります

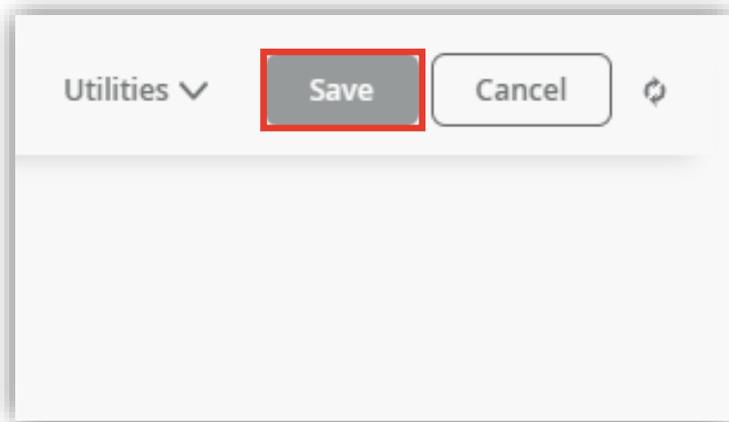
Trusted IP/Protocol/Port ⓘ	Add IP/Protocol/Port	
IP Address	Protocol	Port Range
1.1.1.1	ICMP	Any

**Add** Cancel

# スイッチ単位の PROTECTION OF ROUTING ENGINE 設定

スイッチごとに設定を変更する場合

7. [Save] をクリックし編集内容を保存します



8. 変更の差分が表示されるので、確認して再度 [Save] をクリックします



# Thank you

---

JUNIPER  
driven by Mist AI 