

# Mist 設定マニュアル

## - Wired Assurance -

# スイッチへの DHCP Snooping の設定

---

ジュニパーネットワークス株式会社  
2023年11月 Ver 1.0

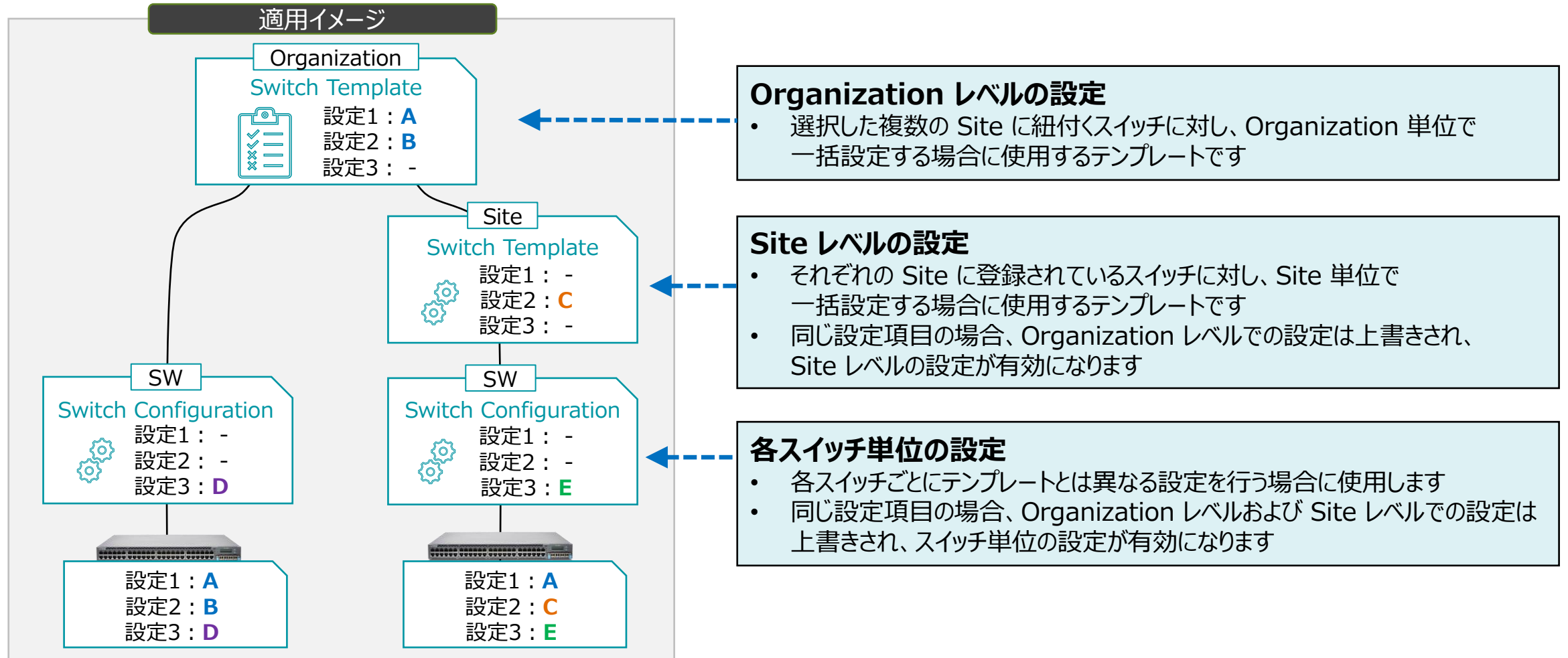
JUNIPER   
driven by Mist AI

# はじめに

- ❖ 本マニュアルは、『Wired Assurance におけるスイッチへの DHCP Snooping の設定』について説明します
- ❖ 手順内容は 2023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

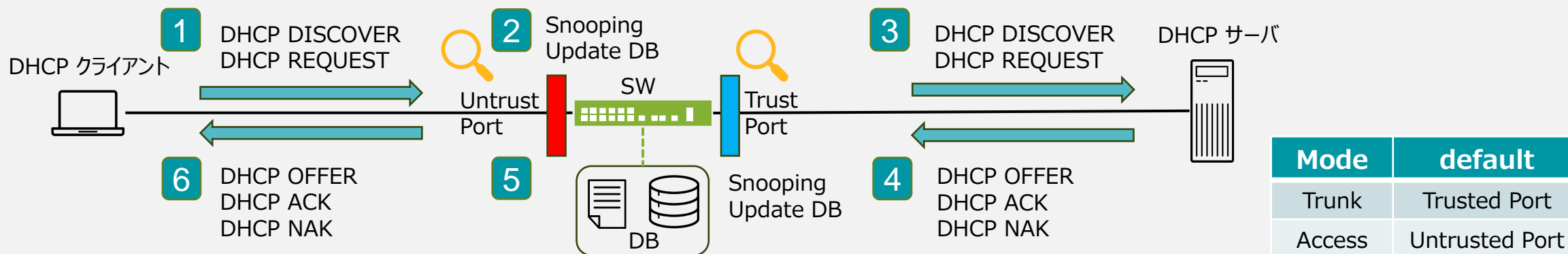


# ポートセキュリティ

## DHCP Snooping

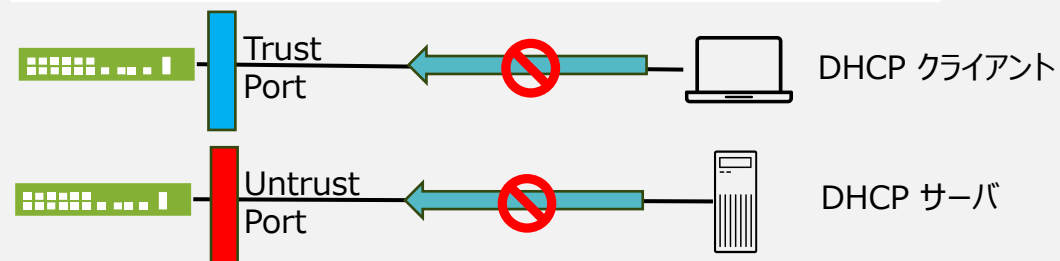
### DHCP Snooping

DHCP Snooping とは、スイッチ上で送受信される DHCP サーバと DHCP クライアント間の DHCP パケットを Snooping (のぞき見)して DB を構築することで、DHCP サーバ/クライアントのなりすまし等を防ぐポートセキュリティ機能の一つです



- 1 DHCP クライアントが DHCP DISCOVER/DHCP REQUEST を送信
- 2 スイッチは DHCP パケットを Snooping して、Snooping DB を更新
- 3 スイッチは DHCP DISCOVER/DHCP REQUEST をフォワーディング
- 4 DHCP サーバは DHCP OFFER/DHCP ACK/DHCP NAK を送信
- 5 スイッチは DHCP パケットを Snooping して、Snooping DB を更新
- 6 スイッチは DHCP OFFER/DHCP ACK/DHCP NAK をフォワーディング

Port Type	Description
Trusted Port	DHCP サーバからのトラフィックの受信を許可
Untrusted Port	DHCP クライアントからのトラフィックの受信を許可



# ポートセキュリティ

## ARP Inspection / IP Source Guard

### ARP Inspection

ARP Inspection は、DHCP snooping DB を利用して ARP スプーフィング攻撃をブロックします  
DAI(Dynamic ARP Inspection) は、Untrusted Port の ARP パケットを傍受して DHCP Snooping DB で ARP パケットの送信元 MAC アドレスが有効なエントリーと一致するか照合します

- データベース内の IP-MAC エントリーが ARP パケット内の情報に対応しない場合、ARP パケットを破棄します
- パケット内の IP アドレスが無効な場合、ARP パケットを破棄します

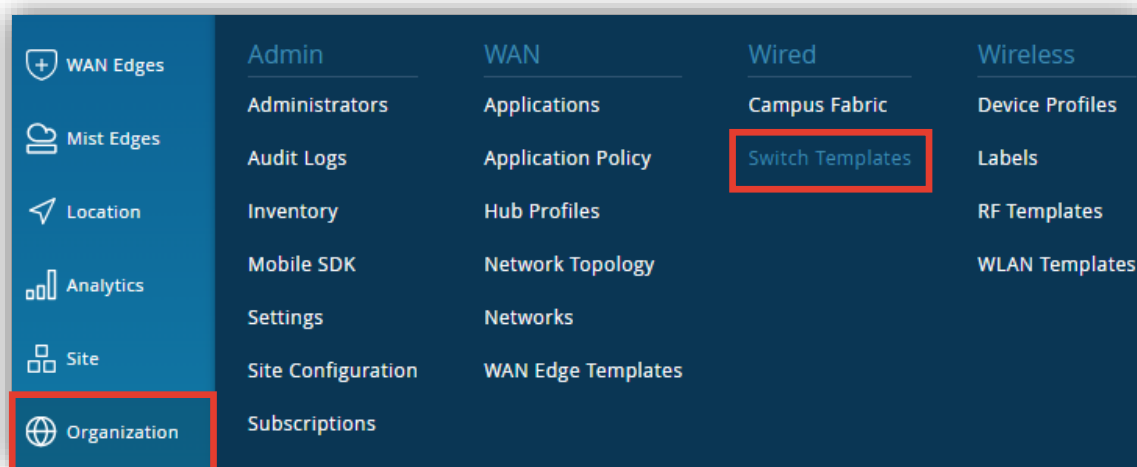
### IP Source Guard

IP Source Guard は、スイッチ上の Untrusted Port に接続されたホストから送信された各パケットを検査し、DHCP Snooping DB に格納されているエントリーと照合します  
パケットヘッダー(IP アドレス/MAC アドレス)が有効なエントリーと一致しない場合、スイッチはパケットを転送せず破棄します

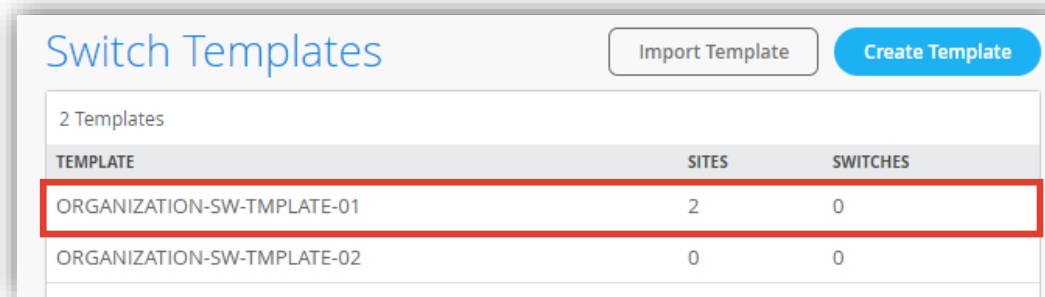
# Organization レベルの DHCP Snooping の設定

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 DHCP Snooping の設定

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. [All Switches Configuration] 内の「DHCP SNOOPING」の項目にて設定、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します

The screenshot displays the 'All Switches Configuration' page. The 'DHCP SNOOPING' section is highlighted with a red box. It contains the following settings:

- Enabled** (radio button selected)
- All Networks** (checkbox checked)
- ARP Inspection** (checkbox unchecked)
- IP Source Guard** (checkbox unchecked)

Below this section, there is another 'DHCP SNOOPING' section with the following settings:

- Enabled** (radio button unselected)
- Disabled** (radio button selected)

The interface also shows other configuration sections: 'AUTHENTICATION SERVERS' (with a dropdown menu set to 'Radius'), 'NTP' (with a text area for 'NTP Servers'), and 'DNS SETTINGS' (with text areas for 'DNS Servers' and 'DNS Suffix').

# Organization レベルの DHCP Snooping の設定

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] をクリックして、DHCP SNOOPING を有効化し、対象となるネットワークを指定します

5. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

DHCP SNOOPING

A network is required for DHCP snooping to be applied to the device

Enabled  Disabled

All Networks

Networks

ARP Inspection

IP Source Guard

All Networks ですべてのネットワークを対象にします

個別に選択する場合は、[+] から適宜選択します (DHCP Snooping を設定する Network を Shared Elements > Networks から選択)

DHCP SNOOPING

Enabled  Disabled

All Networks

Networks

corporate(10) x +

ARP Inspection

IP Source Guard

ARP Inspection を有効にします

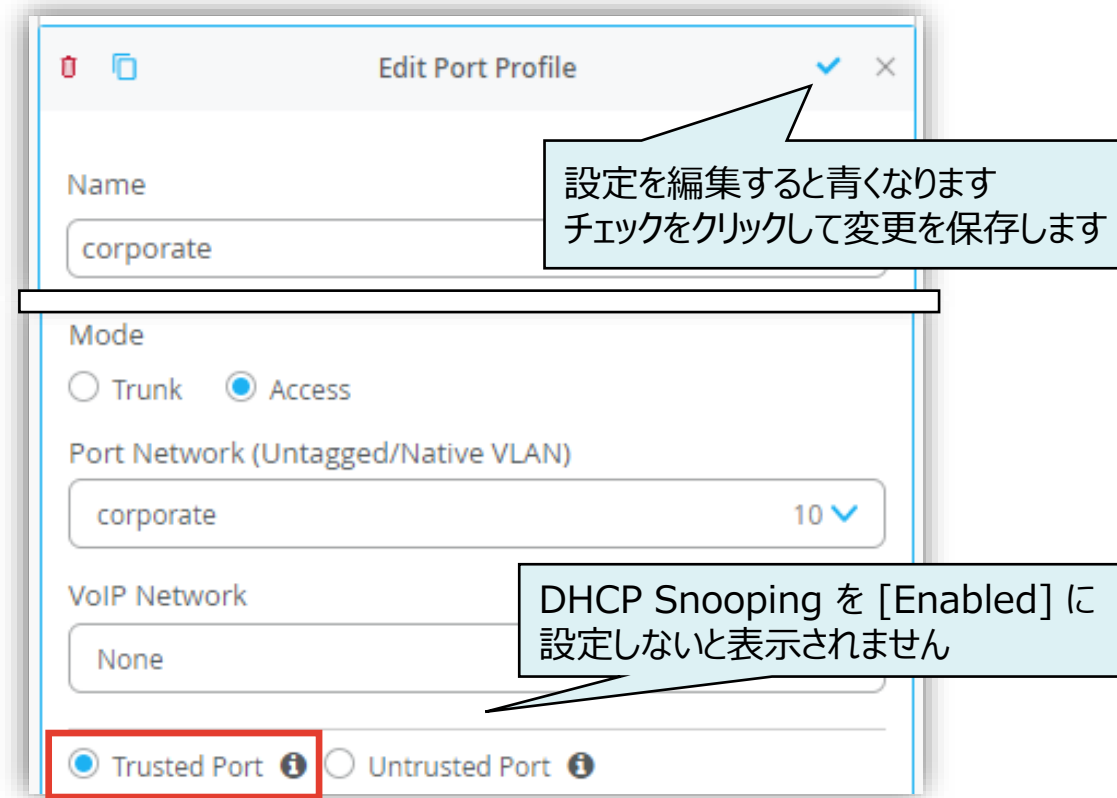
IP Source Guard を有効にします



# Organization レベルの DHCP Snooping の設定

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

6. 指定した Networks に対応する [Shared Elements] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します



## Note

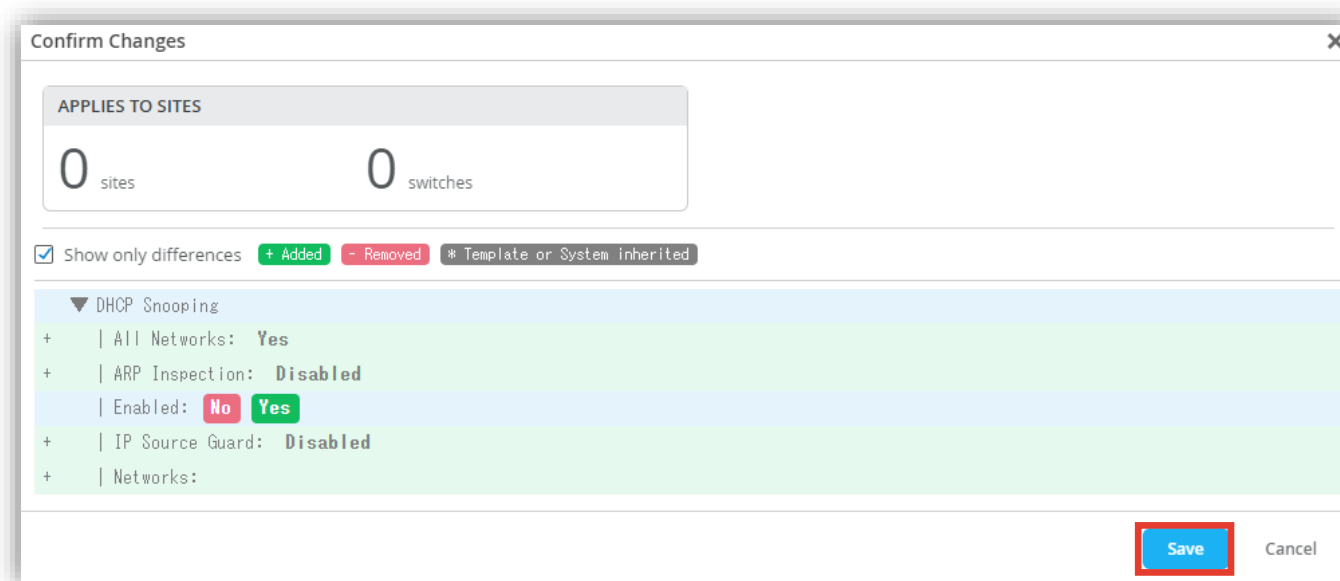
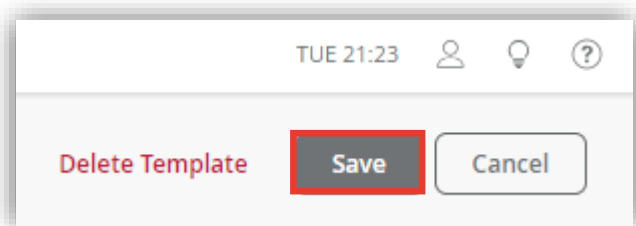
デフォルト設定のままで問題ない場合、この手順はスキップできます

Mode	default
Trunk	Trusted Port
Access	Untrusted Port

# Organization レベルの DHCP Snooping の設定

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

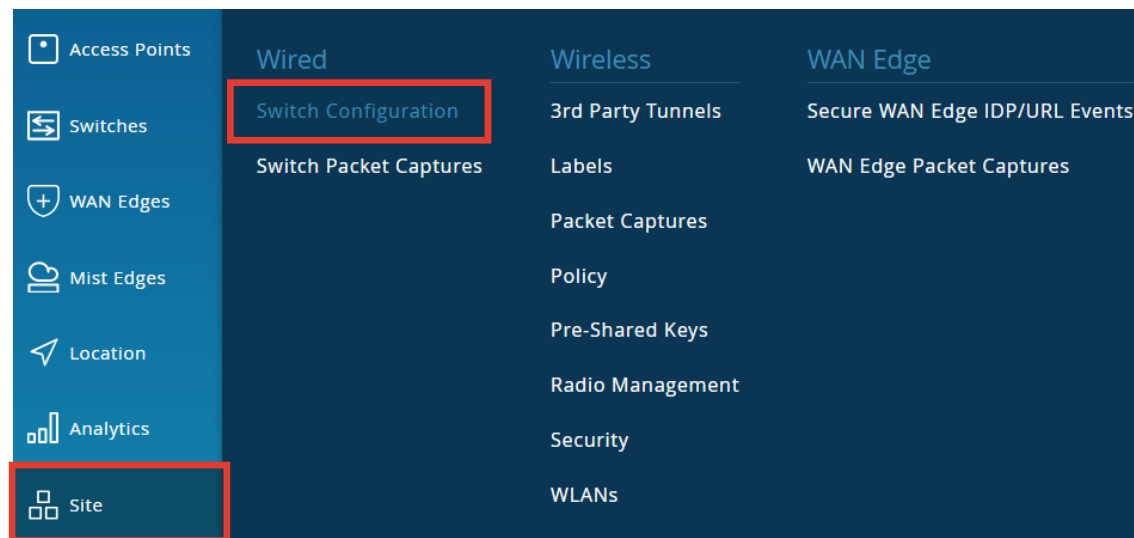
7. テンプレートの編集が終了したら、[Save] をクリックします  
変更の差分が表示されるので、確認して再度 [Save] をクリックします



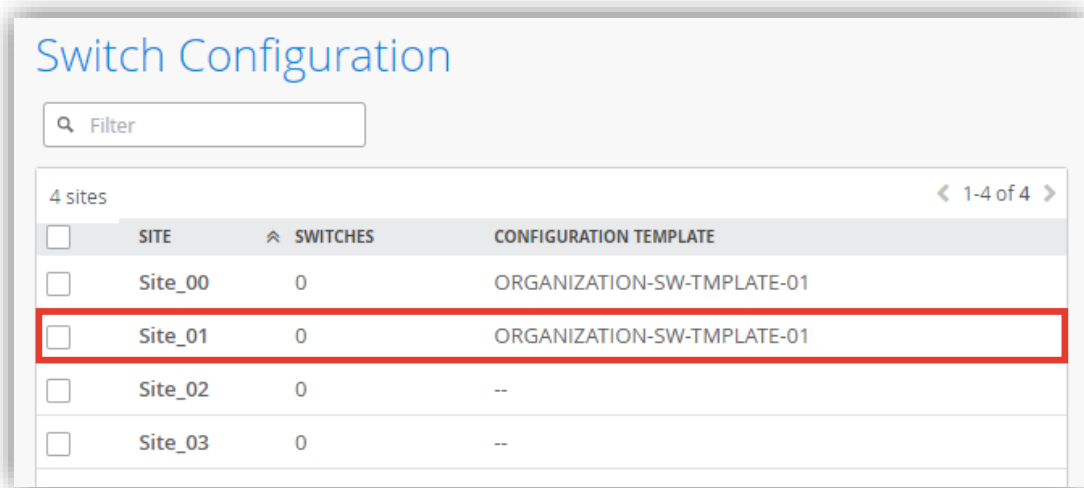
# Site レベルの DHCP Snooping の設定

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 DHCP Snooping の設定

Site ごとに設定を変更する場合

3. [All Switches Configuration] の「DHCP SNOOPING」で [Enabled] をクリックし設定を有効化、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します  
Organization レベルのテンプレート(Organization > Switch Template)を Site に適用している場合、[Override Configuration Template] にチェックを入れることで設定を上書きできます

The screenshot displays the Juniper configuration interface. The top section, titled "All Switches Configuration", shows the "DHCP SNOOPING" settings. The "Override Configuration Template" checkbox is checked and highlighted with a blue box. The "Enabled" radio button is selected and highlighted with a red box. Below it, the "All Networks" checkbox is also checked. Other options like "ARP Inspection" and "IP Source Guard" are unchecked. A callout box points to the "Override Configuration Template" checkbox with the text: "Organization レベルのテンプレートが適用されていると [Override Configuration Template] が表示されます 上書きする場合はチェックを入れます".

The bottom section shows the configuration for a specific Site. The "DHCP SNOOPING" settings are shown in a greyed-out state, indicating that the Organization-level template is applied. The "Override Configuration Template" checkbox is unchecked. The "Enabled" radio button is selected. The "All Networks" checkbox is checked. A callout box points to this section with the text: "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".

# Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

4. [Enabled] をクリックして、DHCP SNOOPING を有効化し、対象となるネットワークを指定します

5. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

DHCP SNOOPING

A network is required for DHCP snooping to be applied to the device

Override Configuration Template

Enabled  Disabled

All Networks

Networks

ARP Inspection

IP Source Guard

All Networks ですべてのネットワークを対象にします

個別に選択する場合は、[+] から適宜選択します (DHCP Snooping を設定する Network を Shared Elements > Networks から選択)

DHCP SNOOPING

Override Configuration Template

Enabled  Disabled

All Networks

Networks

corporate(10) × +

ARP Inspection

IP Source Guard

ARP Inspection を有効にします

IP Source Guard を有効にします

# Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

6. 指定した Networks に対応する [Shared Elements] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します

指定した Network に対応する Port Profile を選択します

## Note

デフォルト設定のままで問題ない場合、この手順はスキップできます

Mode	default
Trunk	Trusted Port
Access	Untrusted Port

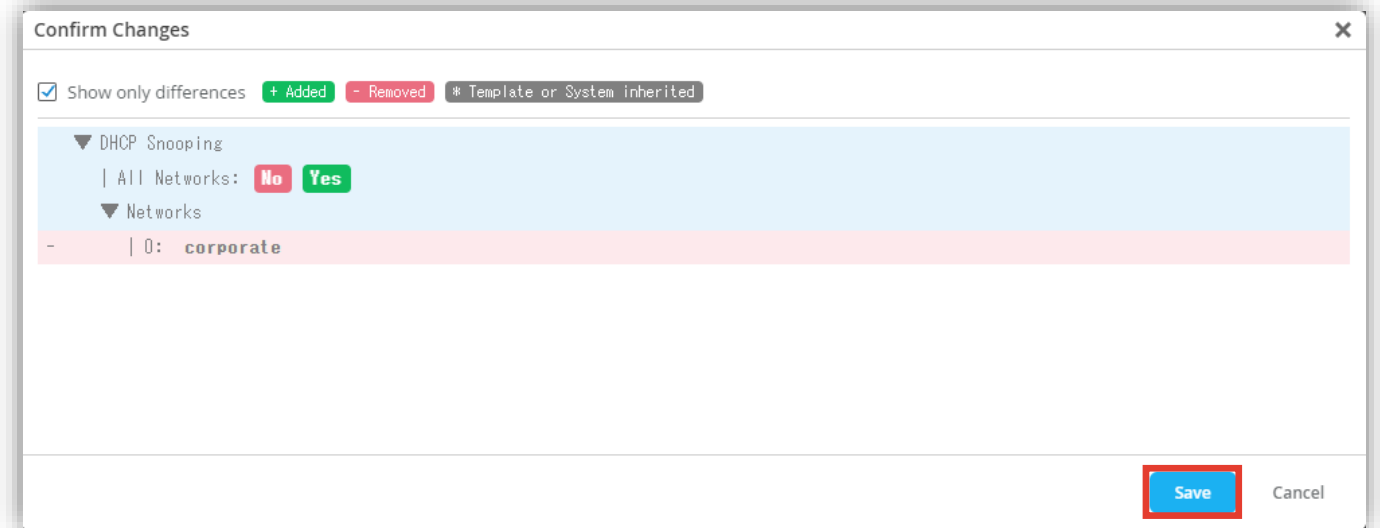
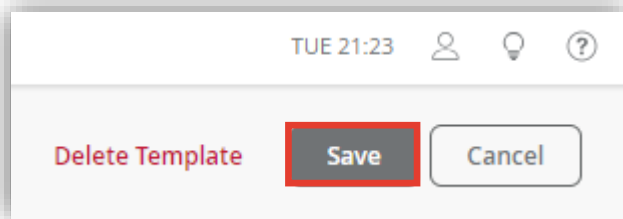
設定を編集すると青くなります  
チェックをクリックして変更を保存します

DHCP Snooping を [Enabled] に設定しないと表示されません

# Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

7. テンプレートの編集が終了したら、[Save] をクリックします  
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 DHCP Snooping の設定

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、[Switches] を選択し、一覧から [EX/QFXスイッチ] をクリックします

18 Switches site Live-Demo List Topology Location 22:00:12 (updates every 3 minutes) Inventory

16 Adopted Switches 2 Discovered Switches 0 Wired Clients 46 W Total Allocated AP Power

100% Switch-AP Affinity 93% PoE Compliance 100% VLANs 100% Version Compliance > 99% Switch Uptime 89% Config Success

Filter

<input type="checkbox"/>	Status	Name	IP Address	Model	Mist APs	Wireless Clients	Wired Clients	Insights
<input type="checkbox"/>	Connected	ld-cup-idf-c2	172.16.84.63	EX3400-48P	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	IPCLOS-DIST2	10.2.2.43	EX9214	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	IPCLOS-ACC2	10.2.2.47	EX9214	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	ld-cup-idf-d-desktop	192.168.2.11	EX2300-C-12P	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	ld-cup-idf-d	10.100.0.125	EX4100-48MP	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	ld-cup-idf-bb	10.100.0.212	EX4100-48MP	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	ld-cup-idf-a-core	10.100.1.47	EX4100-48MP	0	0	--	Switch Insights
<input type="checkbox"/>	Connected	ld-cup-idf-c	10.100.0.121	EX4100-48MP	0	0	--	Switch Insights
<input checked="" type="checkbox"/>	Connected	ld-cup-idf-d-VC	172.16.85.12	EX2300-48P EX2300-48P	0, 0	0	--	Switch Insights



# スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

2. [Services] の「DHCP SNOOPING」で [Enabled] をクリックし設定を有効化、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します  
Organization/Site レベルのテンプレート(Organization > Switch Template/Site > Switch Configuration)をスイッチに適用している場合、[Override Configuration Template] にチェックを入れることで設定を上書きできます



Organization/Site レベルのテンプレートが適用されていると [Override Configuration Template] が表示されます  
上書きする場合はチェックを入れます

スイッチに Organization/Site 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

# スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

3. [Enabled] をクリックして、DHCP SNOOPING を有効化し、対象となるネットワークを指定します

4. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

DHCP SNOOPING

A network is required for DHCP snooping to be applied to the device

Override Configuration Template

Enabled  Disabled

All Networks

Networks

ARP Inspection

IP Source Guard

All Networks ですべてのネットワークを対象にします

個別に選択する場合は、[+] から適宜選択します (DHCP Snooping を設定する Network を Shared Elements > Networks から選択)

DHCP SNOOPING

Override Configuration Template

Enabled  Disabled

All Networks

Networks

corporate(10) × +

ARP Inspection

IP Source Guard

ARP Inspection を有効にします

IP Source Guard を有効にします

# スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

5. 指定した Networks に対応する [Networks & Profiles] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します

指定した Network に対応する Port Profile を選択します

## Note

デフォルト設定のままで問題ない場合、この手順はスキップできます

Mode	default
Trunk	Trusted Port
Access	Untrusted Port

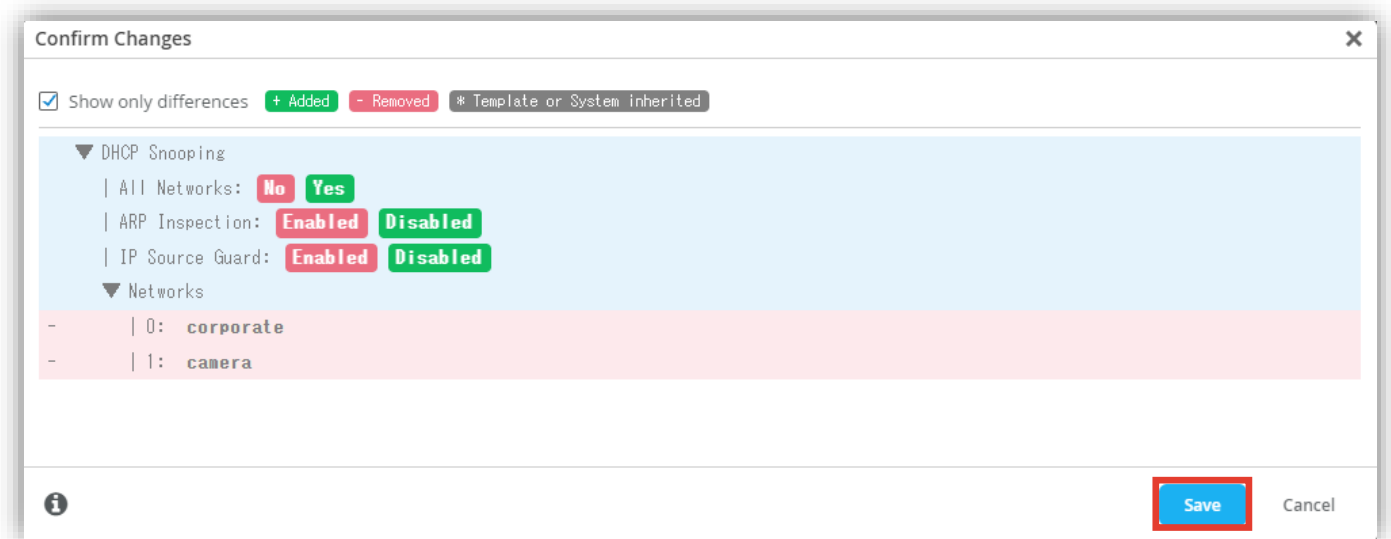
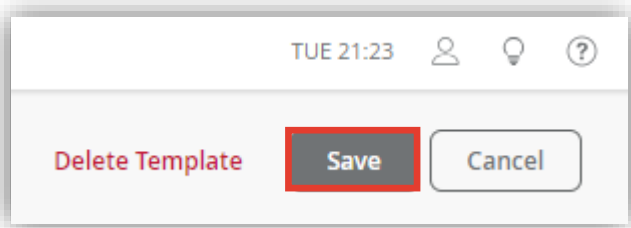
設定を編集すると青くなります  
チェックをクリックして変更を保存します

DHCP Snooping を [Enabled] に  
設定しないと表示されません

# スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

6. テンプレートの編集が終了したら、[Save] をクリックします  
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 