

[Home](#) » [JUNIPER NETWORKS](#) » **Juniper Networks Mist Access Assurance Wired Switch User Guide**

Juniper Networks logo



**Mist Access Assurance
Wired Switch
Version 1.0**

Contents [[hide](#)]

- [1 Mist Access Assurance Wired Switch](#)
- [2 Switch Templates: Port Profiles 802.1X](#)
- [3 Switch Templates: Port Profiles MAB](#)
- [4 Per Switch Configuration](#)
- [5 Port Profile/Client Info](#)
- [6 Documents / Resources](#)
 - [6.1 References](#)

Mist Access Assurance Wired Switch



- ❖ This manual explains “Wired Switch Configuration.”
- ❖ The procedures were verified using Mist Cloud as of September 2025.

If the screen display differs from the actual screen, please refer to the update information below.

<https://www.juniper.net/documentation/us/en/software/mist/product-updates/latest.html>

- ❖ Settings and parameters may vary depending on the deployment environment and configuration.

For details on various settings, please see the links below.

[Mist Documentation](#)

[Juniper Mist Access Assurance Guide](#)

- ❖ Many other Mist Japanese manuals are available on the “Solutions & Technical Information Site.”

<https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html>

- ❖ The contents of this document are current as of the time of writing and are subject to change without notice.

Furthermore, the configurations and features described in this document cannot be purchased as a condition of their provision.

- ❖ The company names, product names, and logos mentioned in this document are trademarks or registered trademarks of their respective companies.

History

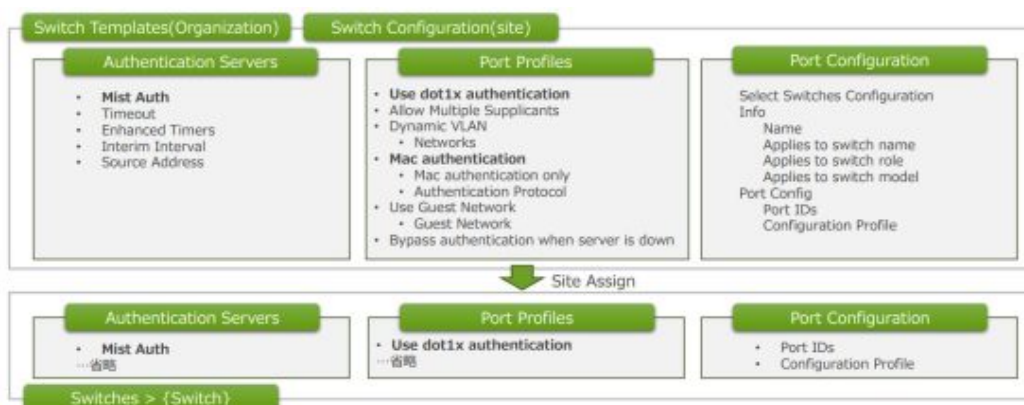
Version	Updated date	Overview
Ver 1.0	September 2025	First Edition

Wired – Switch



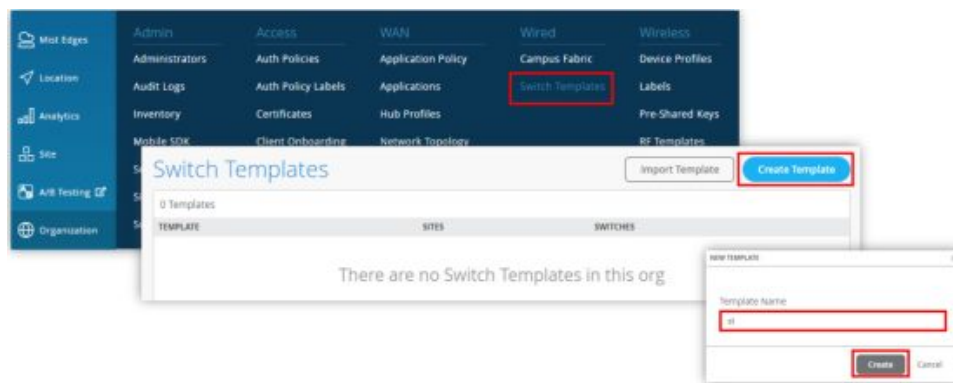
Switch Configuration

Set [Authentication Servers] to [Mist Auth], configure IEEE802.1X authentication-related settings in [Port Profiles], specify the port in [Port IDs] under [Port Configuration], and specify the profile you created in [Configuration Profile].

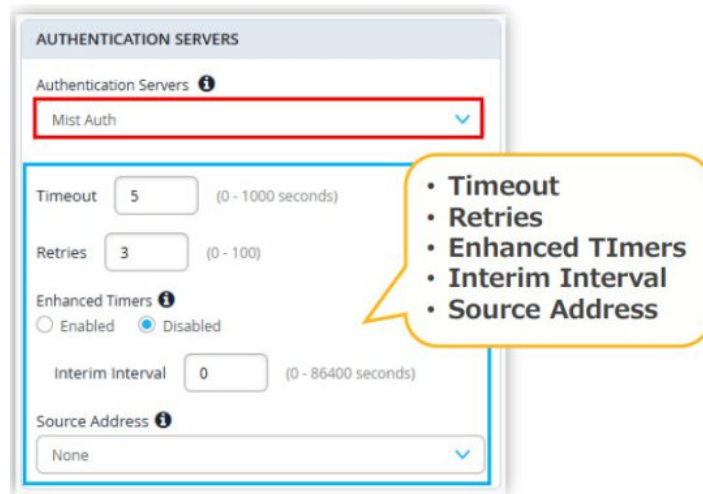


Switch Templates: Create Template

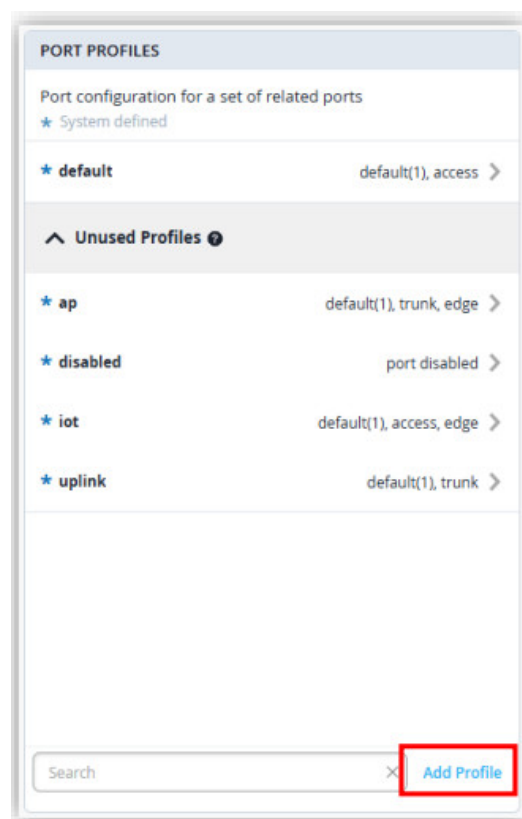
1. From [Organization], click [Switch Templates].
2. Click [Create Template], enter a name for the template in [Template Name], and click [Create].



3. Under [Authentication Servers], select [Mist Auth] and configure other options.

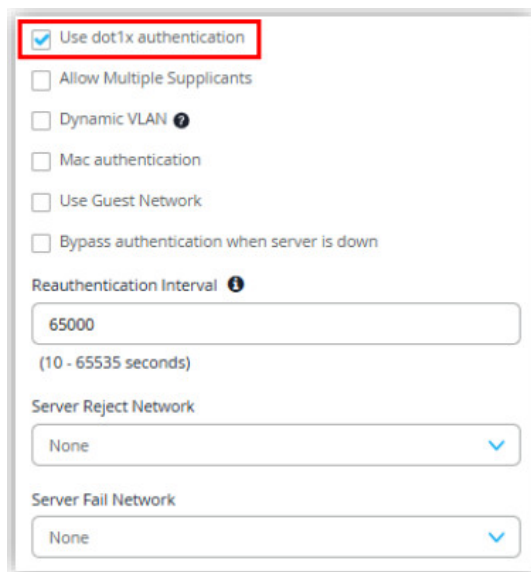


4. Under Port Profiles, click Add Profile



5. Set [Name], check [Use dot1x authentication], and set the required items.

5.(a) 802.1X Authentication: Check [Use dot1x authentication] (required).
Set other options.



☒ Use dot1x authentication

☐ Allow Multiple Supplicants

☐ Dynamic VLAN ⓘ

☐ Mac authentication

☐ Use Guest Network

☐ Bypass authentication when server is down

Reauthentication Interval ⓘ

65000

(10 - 65535 seconds)

Server Reject Network

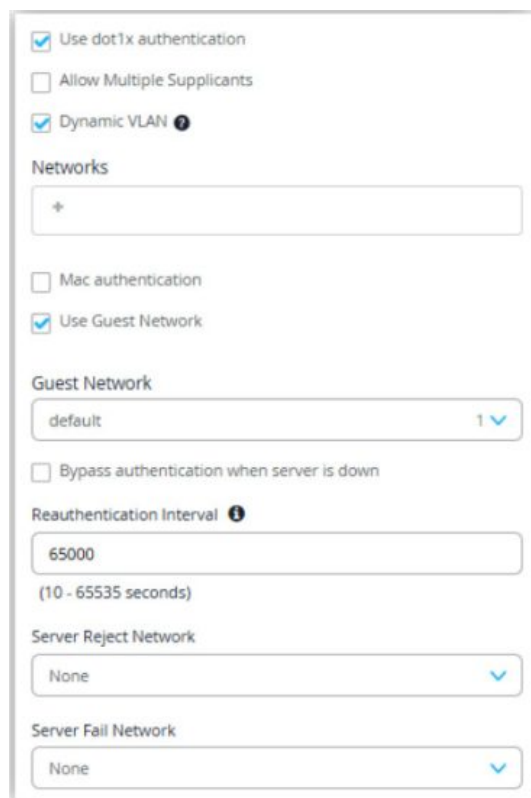
None

Server Fail Network

None

[Use dot1x authentication]

Switch Templates: Port Profiles 802.1X



☒ Use dot1x authentication

☐ Allow Multiple Supplicants

☒ Dynamic VLAN ⓘ

Networks

+

☐ Mac authentication

☒ Use Guest Network

Guest Network

default 1

☐ Bypass authentication when server is down

Reauthentication Interval ⓘ

65000

(10 - 65535 seconds)

Server Reject Network

None

Server Fail Network

None

Options	Descriptions
Allow Multiple Supplicants	Check this box to allow multiple supplicants on the same port.

Dynamic VLAN	Check [Dynamic VLAN] to dynamically assign VLANs. Click [+] to add a network. *Networks are configured separately.
Use Guest Network	Check [Use Guest Network] to authenticate to the guest network. Select a guest network from the drop-down list.
Bypass authentication when server is down	Check this box to allow clients to access the network without authentication if the server is down.
Reauthentication Interval	Set the reauthentication interval (10-65535 default: 65000).
Server Reject Network	To connect users to a specified VLAN (such as a guest network) if the authentication server rejects user authentication attempts, select [Server Reject] for [Network].
Server Fail Network	To connect users to a specified VLAN (such as a guest network) if the authentication server is unreachable or unresponsive, select [Server Fail] for [Network].

REF: [Switch Configuration Options](#) > Table 4: Port Profile Configuration Options

Switch Templates: Port Profiles MAB

5.(b) MAB Authentication: Check [Use dot1x authentication] and [Mac authentication] (required).

Set other options.

The image shows a network configuration window with the following settings:

- ☒ Use dot1x authentication
- ☐ Allow Multiple Supplicants
- ☐ Dynamic VLAN ?
- ☒ Mac authentication
- ☐ Mac authentication only
- Authentication Protocol: None (dropdown menu)
- ☐ Use Guest Network
- ☐ Bypass authentication when server is down
- Reauthentication Interval ⓘ: 65000 (input field)
(10 - 65535 seconds)
- Server Reject Network: None (dropdown menu)
- Server Fail Network: None (dropdown menu)

Check [Use dot1x authentication] Check [Mac authentication] If dot1x authentication is attempted and fails, a MAB connection attempt (fallback) will be performed.

Check [Mac authentication only] to immediately attempt a MAB connection without attempting dot1x authentication.

Select an [Authentication Protocol] (None/pap/eap-peap/eap-md5).

The supplicant will present credentials using the specified authentication protocol.

☒ Use dot1x authentication
☐ Allow Multiple Supplicants
☒ Dynamic VLAN ⓘ

Networks

☒ Mac authentication
☐ Mac authentication only

Authentication Protocol

☒ Use Guest Network

Guest Network
 1

☐ Bypass authentication when server is down

Reauthentication Interval ⓘ

 (10 - 65535 seconds)

Server Reject Network

Server Fail Network

Options	Descriptions
Allow Multiple Supplicants	Check this box to allow multiple supplicants on the same port.
Dynamic VLAN	To dynamically assign VLANs, check [Dynamic VLAN]. Click [+] to add a network. *Networks are configured separately.
Authentication Protocol	Select an Authentication Protocol (None/pap/eappeap/eap-md5). The supplicant will present its credentials using the specified authentication protocol.
Use Guest Network	Check [Use Guest Network] to authenticate to the Guest Network. Select [Guest Network] from the drop-down list.
Bypass authentication when server is down	If checked, clients can access the network without authentication if the server is down.

Reauthentication Interval	Set the re-authentication interval (10-65535 default:65000)
Server Reject Network	To connect users to a specified VLAN (such as a guest network) if the authentication server rejects their authentication attempt, select [Network] for [Server Reject].
Server Fail Network	To connect users to a specified VLAN (such as a guest network) if the authentication server is unreachable or does not respond, select "Network" for "Server Fail Network."

REF: [Switch Configuration Options](#) > Table 4: Port Profile Configuration Options

Switch Templates: Select Switches Configuration > Port Configuration

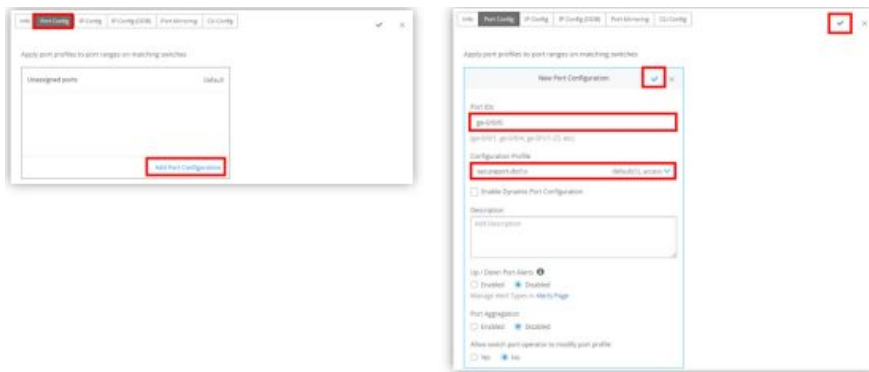
6. Click [Add Rule] under [Select Switches Configuration], set [Name] on the [Info] tab, and specify the target device by [Applies to name], [Applies to switch role], or [Applies to switch model].

The screenshot shows the 'Select Switches Configuration' dialog box. On the left, there's a list of switch groups: 'default' and 'all remaining switches'. On the right, the 'Info' tab is selected, showing configuration options. The 'Name' field is set to 'port-config'. Below it, there are checkboxes for 'Applies to switch name', 'Applies to switch role', and 'Applies to switch model'. The 'Applies to switch model' checkbox is checked, and a dropdown menu shows 'E54100-40P' as the selected model. An 'Add Rule' button is highlighted in the top right corner of the dialog.

7. Click the Port Config tab and click Add Port Configuration.

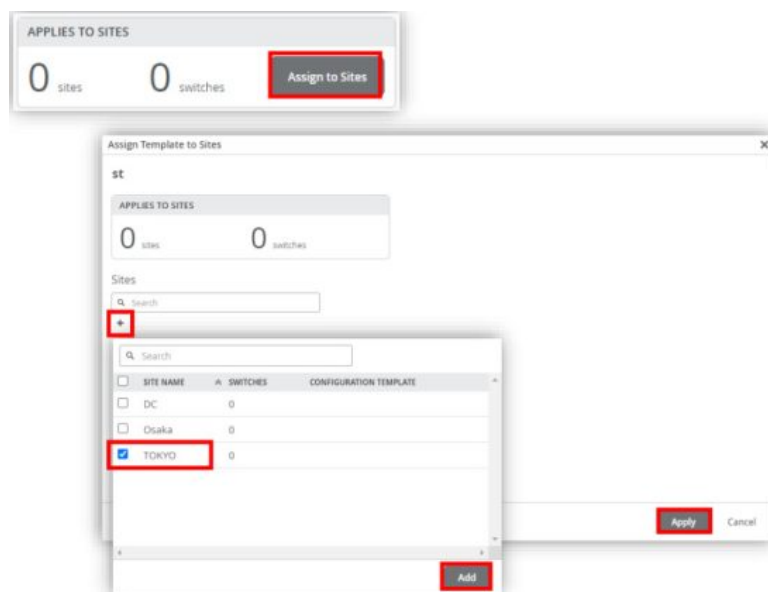
Specify the interface to which the configuration applies in Port IDs, and select the profile you created in Configuration Profile.

Click to complete the Port Configuration settings, and click to complete the Rule settings.

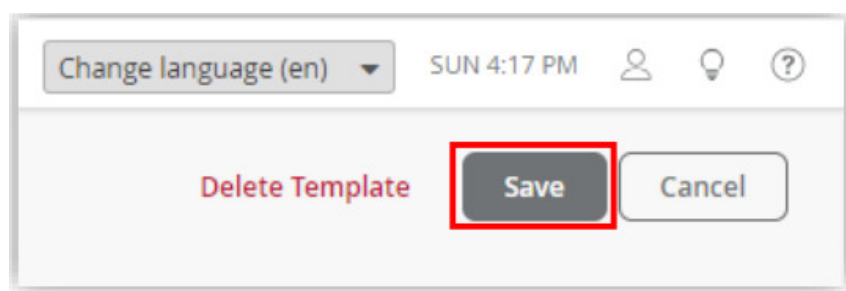


Switch Templates: Assign to Sites / Save

8. Under [Applies to Sites], click [Assign to Sites], Select the sites to which you want to apply the template from [+] (multiple selections are possible), Click [Add], and then click [Apply].

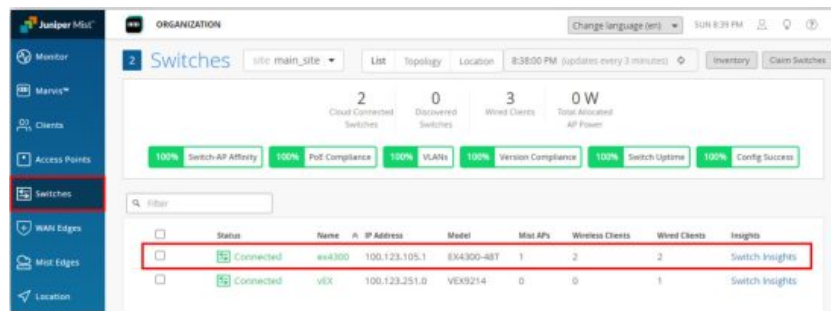


9. Complete the Switch Template settings in [Assign to Sites].

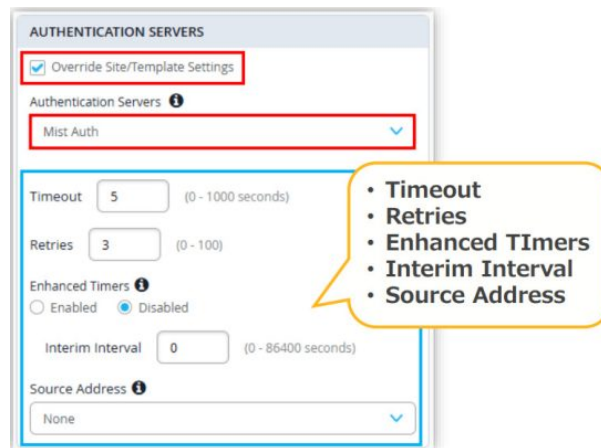


Per Switch Configuration

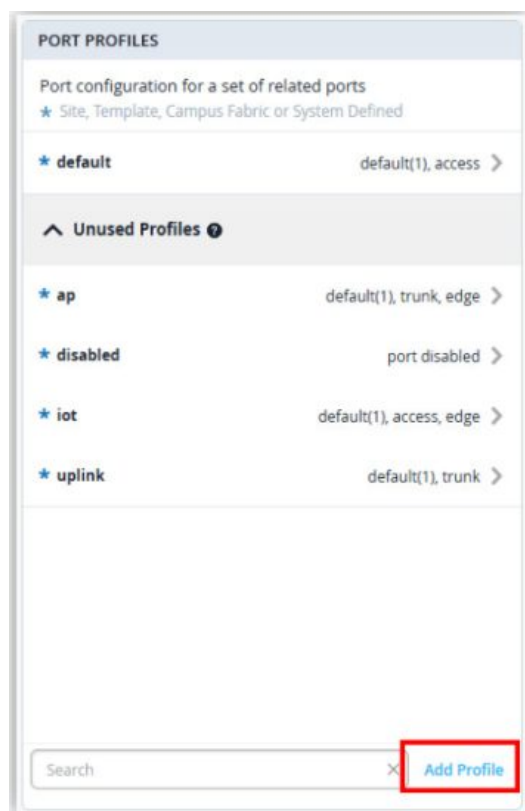
1. From [Switches], select the switch you want to configure.



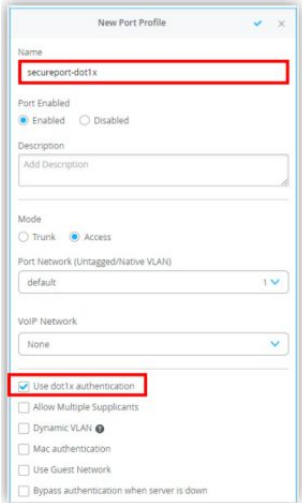
2. Select [Mist Auth] under [Authentication Servers] and configure other options.



3. Under Port Profiles, click Add Profile



4.(a) Port Profile: 802.1X Authentication



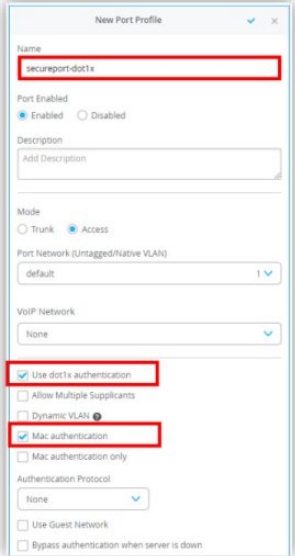
The 'New Port Profile' window shows the following configuration:

- Name:** secureport-dot1x (highlighted with a red box)
- Port Enabled:** Enabled (selected)
- Description:** Add Description
- Mode:** Access (selected)
- Port Network (Untagged/Native VLAN):** default
- VoIP Network:** None
- Authentication Options:**
 - ☒ Use dot1x authentication (highlighted with a red box)
 - ☐ Allow Multiple Supplicants
 - ☐ Dynamic VLAN
 - ☐ Mac authentication
 - ☐ Use Guest Network
 - ☐ Bypass authentication when server is down

[Name]

[Use dot1x authentication]

4.(b) Port Profile: MAB Authentication



The 'New Port Profile' window shows the following configuration:

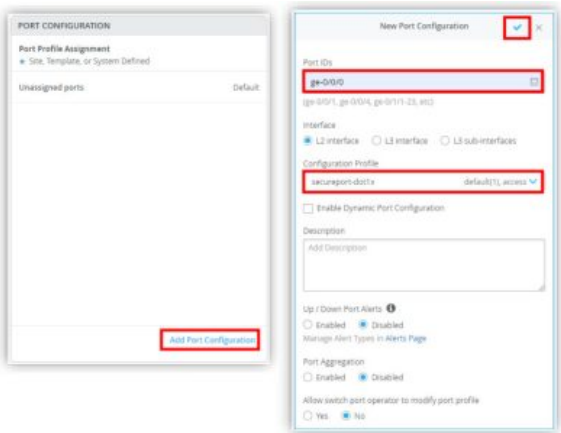
- Name:** secureport-dot1x (highlighted with a red box)
- Port Enabled:** Enabled (selected)
- Description:** Add Description
- Mode:** Access (selected)
- Port Network (Untagged/Native VLAN):** default
- VoIP Network:** None
- Authentication Options:**
 - ☒ Use dot1x authentication (highlighted with a red box)
 - ☐ Allow Multiple Supplicants
 - ☐ Dynamic VLAN
 - ☒ Mac authentication (highlighted with a red box)
 - ☐ Mac authentication only
- Authentication Protocol:** None
- ☐ Use Guest Network
- ☐ Bypass authentication when server is down

[Name]

[Use dot1x authentication]

[Mac authentication]

5. Under Port Configuration, click Add Port Configuration. Specify the interface to which the configuration applies under Port IDs, and select the profile you created under Configuration Profile. Click .



The 'PORT CONFIGURATION' window shows the 'Add Port Configuration' button highlighted with a red box.

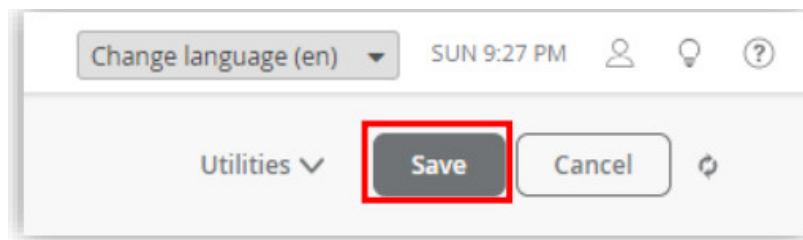
The 'New Port Configuration' window shows the following configuration:

- Port IDs:** ge-0/0/0 (highlighted with a red box)
- Interface:** L2 interface (selected)
- Configuration Profile:** secureport-dot1x (highlighted with a red box)
- Description:** Add Description
- Up / Down Port Alerts:** Enabled (selected)
- Port Aggregation:** Disabled (selected)
- Allow switch port operator to modify port profile:** No (selected)

[Port IDs]

[Configuration Profile]

6. Click [Save] to complete the settings.



You can configure these settings in any of the following locations:

- Organization > Switch Templates > {Template}
- Site > Switch Configuration > {Site}
- Switches > {Switch}

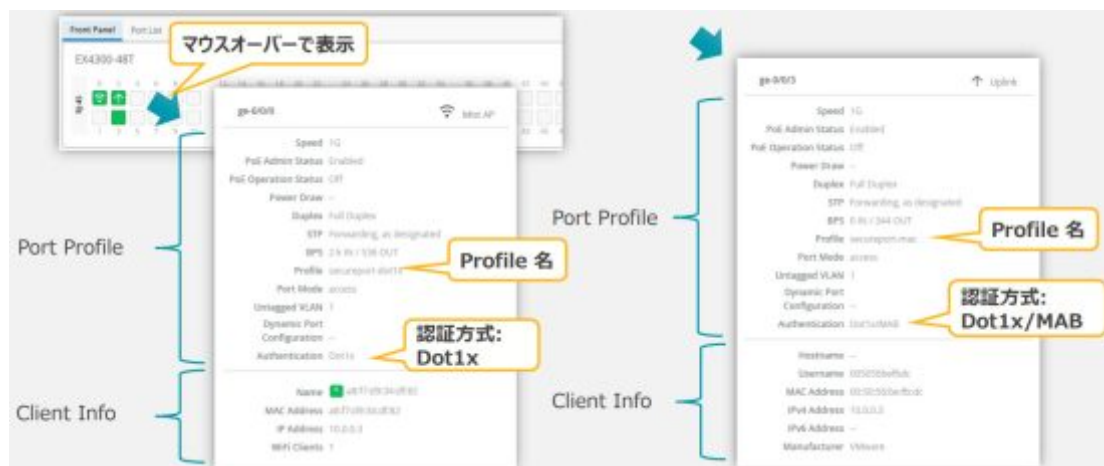
For manageability and scalability, configuring settings in Switch Templates is recommended.

You can also combine these settings by configuring the Network and Port Profile in the Switch Template and the Port Configuration on individual switches.

Port Profile/Client Info

Note

Select the switch in question from Switches and hover your mouse over the port to view information about it, including the authentication method.



THANK YOU



Juniper Networks logo

Documents / Resources

	Juniper Networks Mist Access Assurance Wired Switch [pdf] User Guide Mist Access Assurance Wired Switch, Assurance Wired Switch, Wired Switch
---	--

References

- [User Manual](#)

📁 JUNIPER
NETWORKS

💎 Assurance Wired Switch, JUNIPER NETWORKS, Mist Access Assurance Wired Switch, Wired Switch

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

[Manuals+](#) | [Upload](#) | [Deep Search](#) | [About Us](#) | [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#) | [LinkedIn](#) | [FaceBook](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.