WHITE

PAPER

Tech Talk | Port Security

Prevent attacks from UNTRUSTED users and devices.

MOXA®

Reliable Networks ▲ Sincere Service

ecs

Tech Talk | Port Security

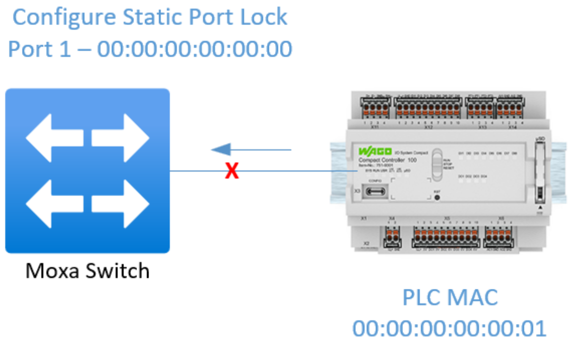
MOXA managed switches offer a Port Security feature that enhances security by managing access to Ethernet ports based on the MAC addresses of connected devices. This function allows the network administrators to associate only specific MAC addresses with each switch port or set a limit on the number of MAC addresses permitted per port. In some of the Moxa Managed switch manuals, this feature is referred to as Port Access Control, but the concepts are similar, focusing on regulating network access and enhancing security by managing which devices can connect to specific ports.

Use case Scenarios:

- Control rooms
- Machine building
- Automated Plant

Here are the details:

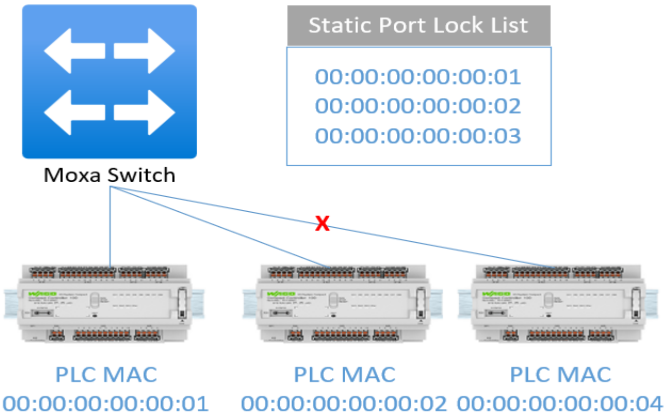
1. **Static Port Lock**: Allows users to configure specific MAC addresses that are allowed to access the port.



Pros:
- Simple & Straight-forward solution.
- Supported by most Moxa Managed switches

Cons:
- Manual Configuration
- Reconfiguration of the switch for the replacement.

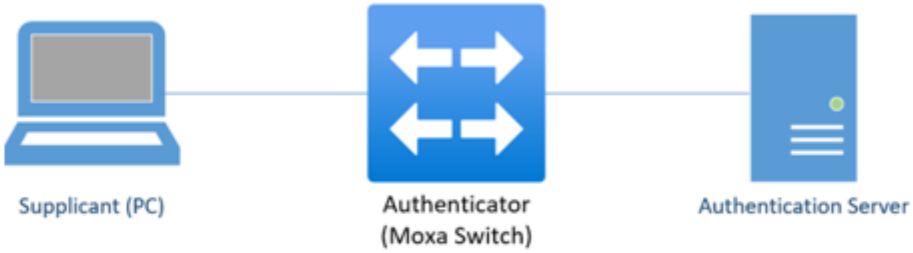
2. **MAC Address Sticky**: Allows users to configure the maximum number of MAC addresses (the Limit) that a port can "learn." Users can configure what action should be taken (under Violation Port Disable) when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned. The total number of allowed MAC addresses cannot exceed 1024.



Pros:
- Easy and quick deployment
- Basic alerting upon violation

Cons:
- Not flexible enough for mobile devices

3 **IEEE 802.1X:** This protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, in which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.



Three components are used to create an authentication mechanism based on 802.1X standards: *Client/Supplicant*, *Authentication Server*, and *Authenticator*.

Client/Supplicant: The PC that requests access to the LAN and switch serves and responds to the requests from the switch.

Authentication Server: The server that performs the actual authentication of the supplicant.

Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant. The Moxa switch acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange **EAPOL** (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server or implement the authentication server in the Moxa switch by using a Local User Database as the authentication look-up table. Then we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other. Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an EAPOL-Start frame to the authenticator. When the authenticator initiates the authentication process or when it receives an EAPOL Start frame, it sends an EAP Request/Identity frame to ask for the username of the supplicant.

Pros:
- Centralized network access control with Authentication server
- User identification

Cons:
- End devices need to support Supplicant functionality
- Usually not the case for OT devices

4. **MAC Authentication Bypass:** MAB is a fallback authentication method used when a device does not support 802.1X. It allows network access based on the MAC address of the device.

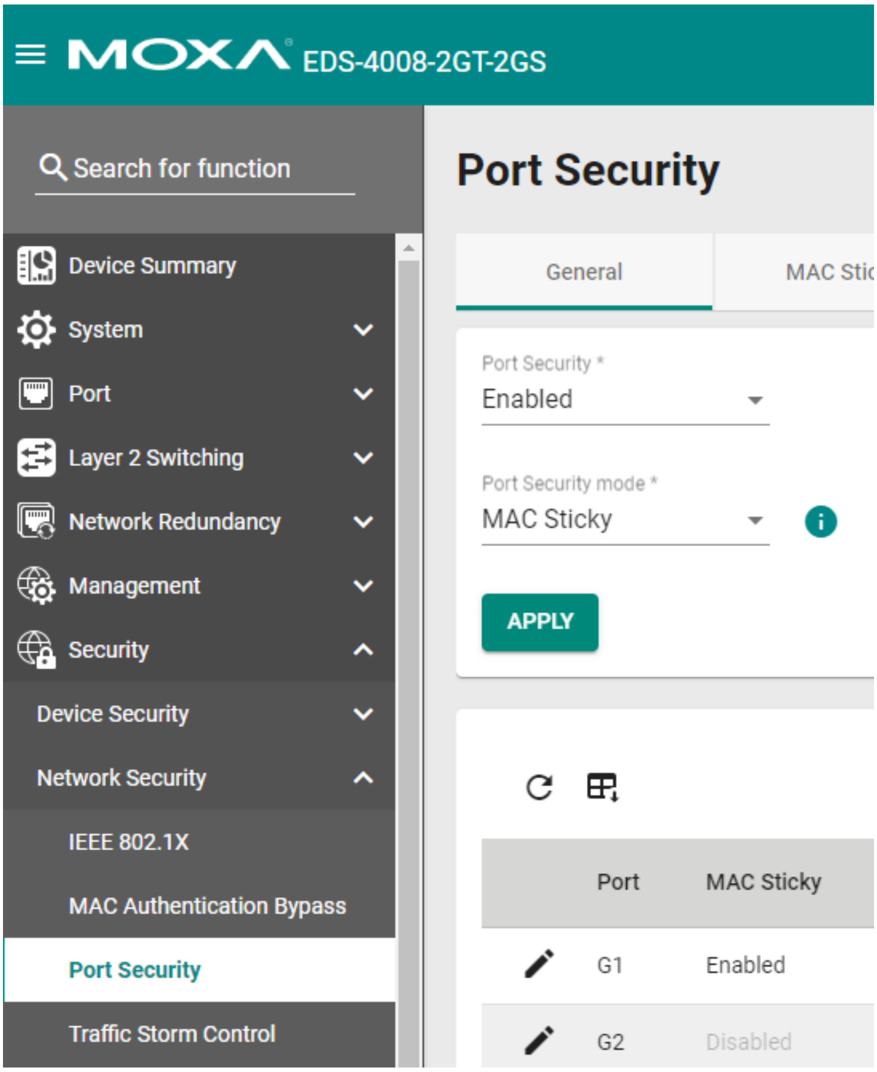
Pros: - Centralized network access control from Authentication server
Support any device

Cons: - Only MAC address-based authentication
- Same security level as with statis port local / MAC sticky.

How to Configure this feature in EDS-4008-2GT-2GS

A. Static Port Lock or Mac address sticky:-

1. Navigate the menu under **Security** > **Network Security** > **Port Security**



Port Security * Enabled

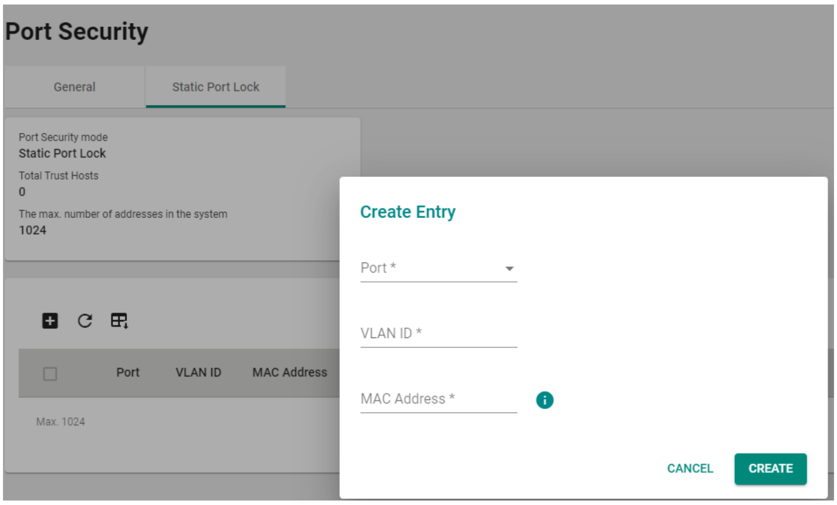
Port Security mode * MAC Sticky

	Port	MAC Sticky
✎	G1	Enabled
✎	G2	Disabled

2. Select the Enabled/Disabled, Static Port Lock / Mac sticky and apply.

You can only select one Port security mode.

3. If you want to enable the Static port lock
   - Click the pencil icon to select the port
   - Select enabled or disabled and apply
   - Select the Static Port lock tab and click the "+" icon to insert the port no, vlan id and mac address



Port Security

Port Security mode: Static Port Lock

Total Trust Hosts: 0

The max. number of addresses in the system: 1024

	Port	VLAN ID	MAC Address

Max. 1024

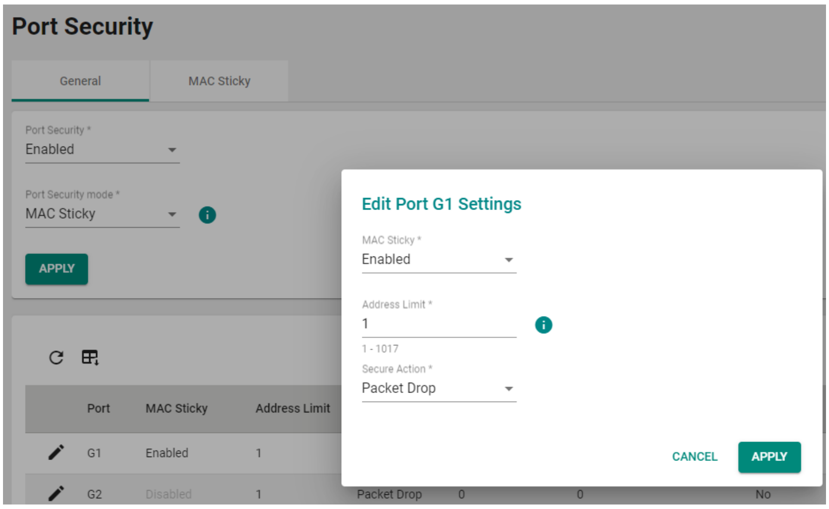
Create Entry

Port *

VLAN ID *

MAC Address *

4. If you want to enable the Mac Sticky
   - Click the pencil icon to select the port
   - Select enabled or disabled, mac add limit, secure action and apply



Port Security

Port Security *: Enabled

Port Security mode *: MAC Sticky

	Port	MAC Sticky	Address Limit				
	G1	Enabled	1				
	G2	Disabled	1	Packet Drop	0	0	No

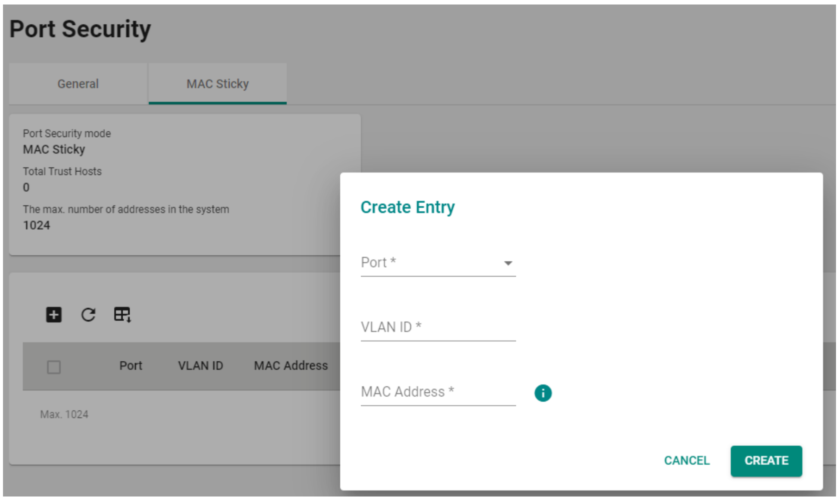
Edit Port G1 Settings

MAC Sticky *: Enabled

Address Limit *: 1 (1 - 1017)

Secure Action *: Packet Drop

   - If you want to insert the mac address manually, you can select the Mac Sticky tab and click the "+" icon to insert the port no, Vlan id and mac address



Port Security

Port Security mode
MAC Sticky

Total Trust Hosts
0

The max. number of addresses in the system
1024

Port	VLAN ID	MAC Address

Max. 1024

Create Entry

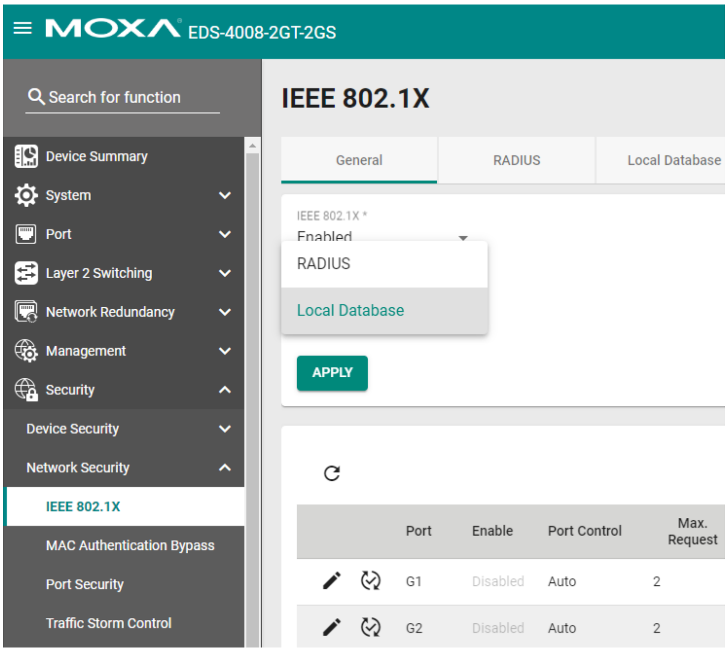
Port *

VLAN ID *

MAC Address *

B. IEEE 802.1X: -

1. Navigate the menu under **Security** > **Network Security** > **IEEE 802.1X**

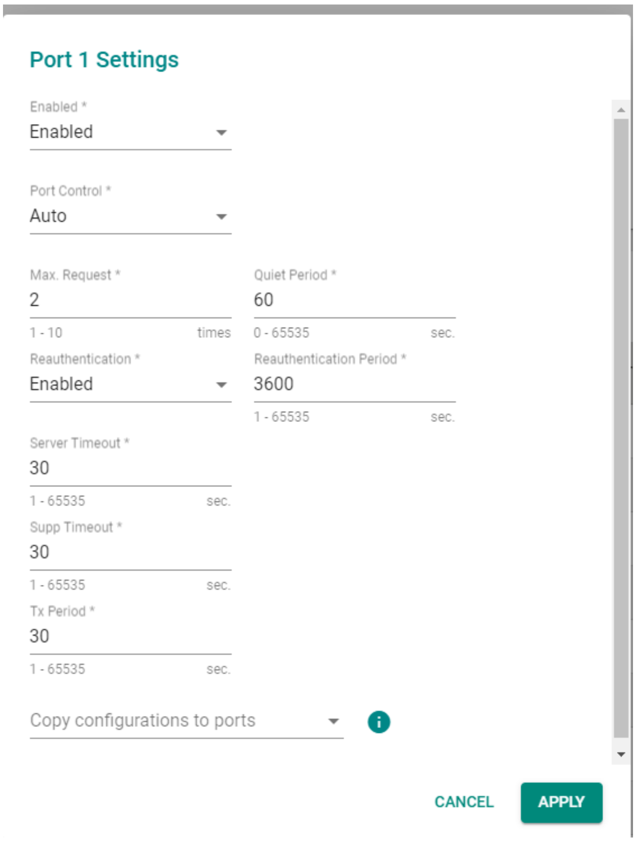


IEEE 802.1X

IEEE 802.1X *
Enabled

	Port	Enable	Port Control	Max. Request
	G1	Disabled	Auto	2
	G2	Disabled	Auto	2

2. Select the Enabled/Disabled, Radius / Local Database and apply.
3. Click the pencil icon to select the port
4. Select Enabled, other parameters and apply



Port 1 Settings

Enabled *
Enabled

Port Control *
Auto

Max. Request *
2
1 - 10 times

Quiet Period *
60
0 - 65535 sec.

Reauthentication *
Enabled

Reauthentication Period *
3600
1 - 65535 sec.

Server Timeout *
30
1 - 65535 sec.

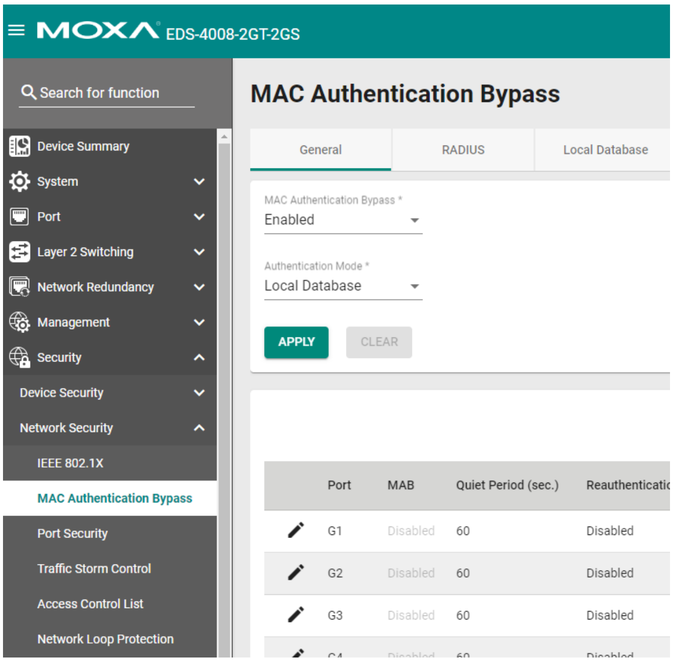
Supp Timeout *
30
1 - 65535 sec.

Tx Period *
30
1 - 65535 sec.

5. If you use Radius, you need to configure the server details under the Radius tab. Otherwise, you need to configure the username and password under the Local Database tab.

C. MAC Authentication Bypass or MAB

1. Navigate the menu under **Security** > **Network Security** > **MAC Authentication Bypass**



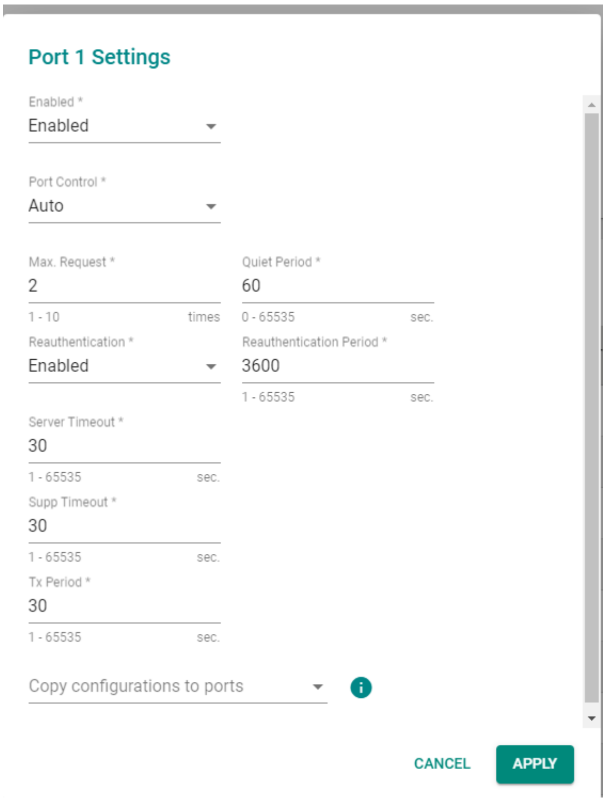
MAC Authentication Bypass

MAC Authentication Bypass *
Enabled

Authentication Mode *
Local Database

Port	MAB	Quiet Period (sec.)	Reauthenticatic
G1	Disabled	60	Disabled
G2	Disabled	60	Disabled
G3	Disabled	60	Disabled
G4	Disabled	60	Disabled

2. Select the Enabled/Disabled, Radius / Local Database and apply.
3. Click the pencil icon to select the port
4. Select Enabled, other parameters and apply



Port 1 Settings

Enabled *: Enabled

Port Control *: Auto

Max. Request *: 2 (1 - 10 times)

Quiet Period *: 60 (0 - 65535 sec.)

Reauthentication *: Enabled

Reauthentication Period *: 3600 (1 - 65535 sec.)

Server Timeout *: 30 (1 - 65535 sec.)

Supp Timeout *: 30 (1 - 65535 sec.)

Tx Period *: 30 (1 - 65535 sec.)

5. If you use Radius, you need to configure the server details under the Radius tab. Otherwise, you need to configure mac address under the Local Database tab.

Most Moxa switches support static port security and IEEE 802.1x, with some models offering all four modes. Additionally, the GUI may vary between different switch models. For more detailed information, please refer to the specific manual for each switch.

Please contact automation@ecsnz.com if you have any questions.

--- END ---