6AOSCG0001-29E
May 2016

Configuration Guide

Configuring Port Access Control in AOS

This configuration guide describes how to configure the ADTRAN Operating System (AOS) port access control suite of port protection methods. Configuration of the port access control suite can be accomplished using both the command line interface (CLI) and the web-based graphical user interface (GUI). This guide contains an overview of the port security, port protection, and port authentication features of the AOS port access control suite, as well as the steps necessary to enable and configure those features on your AOS product. Also included are configuration examples, how to verify the configuration, troubleshooting information, and additional resources for understanding the port access control features.

This guide consists of the following sections:

Overview of Port Access Control in AOS

Port access control is a combination of AOS features used to control and limit access to specific ports in order to provide network protection. Port access control is comprised of three features: port security, port protection, and port authentication. Port protection can be used in conjunction with either port security or port authentication, but port security and port authentication cannot be used together. Each of these features requires different configuration methods and provides different parts of port access security and network protection. Each of these features is described in the following sections.

Port Security

Port security is an AOS feature that relies on the medium access control (MAC) address of a device to determine whether or not the device is allowed to connect to the network. This feature controls which devices have access to the Layer 2 switch fabric based on the MAC address of the device. Port security operates by storing a table of allowed addresses and uses this table to determine access rights whenever a new physical connection is made to the port or whenever reauthentication of the device is scheduled.

In port security, when a user connects to the AOS device, the source MAC address of the first packet is inspected. If a match is found within the stored secure MAC address table, the port is allowed to pass traffic in a normal fashion. The number of MAC addresses stored in the secure MAC address table is specified by the user, and these addresses can be either static or dynamically learned MAC addresses. In addition, dynamically learned MAC addresses can be added to a forwarding table and the running configuration of the AOS unit as sticky MAC addresses. Sticky MAC addresses can be stored as static MAC addresses that persist through a reboot of the unit if the running configuration is saved.

Port security operates by storing the user-defined MAC addresses of specific devices in the secure MAC address table. When more MAC addresses than the user-specified number attempt to connect to the network, none of the traffic from these subsequent unknown sources is allowed to pass through the network and the associated MAC addresses are not added to the table. When traffic from unknown sources appears on the network, port security classifies this traffic as a security violation. In addition, security violations occur when traffic from an address that is configured as a secure MAC address appears on another interface within the same virtual local area network (VLAN). When security violations occur, port security can be configured to either shut down the interface on which the violation was detected, or restrict the traffic on that interface.

Typically, port security does not function on VLAN trunked ports. However, in AOS firmware release 17.09.01, support for port security was added to the VLAN trunk ports. VLAN-aware port security is used to provide security in networks with both voice and data traffic; for example, a network in which an IP phone is connected directly to a trunked port with a computer connected to the IP phone. In this scenario, port security provides a secure MAC address for the phone, as well as a secure MAC address for the PC, and splits the voice and data traffic into two secure VLANs.

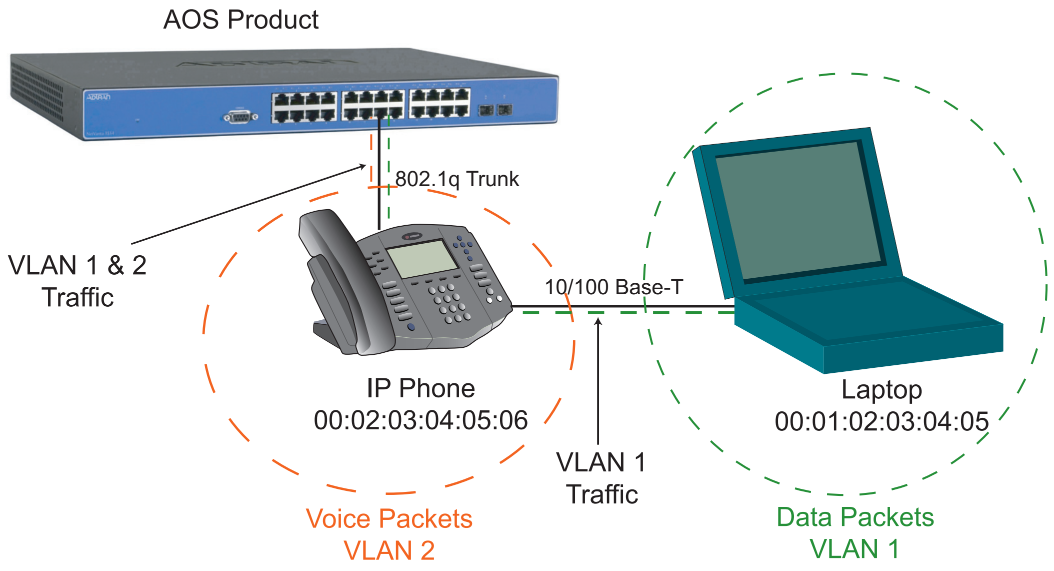


Figure 1. VLAN-Aware Port Security Network Diagram

Port Protection

Port protection is another method of port access control that effectively isolates ports from one another on the same broadcast domain. Port protection operates by placing ports in protected mode, which prevents intra-VLAN communication between the ports. This measure is sometimes necessary when ports communicating with each other on the same network pose a security risk, but it is still necessary for the ports to have access to the Internet and other resources. Port protection is achieved by configuring the port as a protected port.

Port Authentication

The third tier of port access control is port authentication, a security measure based on 802.1x authentication. In port authentication, port control can be based on authentication of a specific port, a specific MAC address of a device, or for IP phones and voice networks, voice based. Port authentication authorizes users based on a range of requirements; it can be based on a simple user name and password challenge or use the Extensible Authentication Protocol (EAP) over local area network (EAPOL).

Port authentication operates by determining which ports, MAC addresses, or virtual local area networks (VLANs) can access the network. Once an address or port is authenticated, traffic flows freely between the port and the network. The client requesting network access (known as the supplicant), provides a user name and password to the authenticating device (authenticator). It is the job of the authenticator to verify the supplicant’s credentials with an authentication server and either grant or deny access. Port authentication operates using methods similar to those used in authentication, authorization, and accounting (AAA), and often requires the use of an outside authenticator, usually a remote authentication dial-in user service (RADIUS) server.

However, it is possible for the AOS device to operate as either a supplicant or an authenticator. When the device is operating as an authenticator, it begins the authentication process by either receiving an EAPOL start frame from the supplicant or detecting a port (configured as an authenticator) that has been enabled. When either of these two conditions are met, the AOS device generates an EAP identity request. This request is sent to either an outside source (such as a RADIUS server) or to an internal authentication system (such as a local user list configured on the unit). Authorization is then sent back to the AOS device based either on the connecting device's port number or MAC address. When authentication is configured on a per-port basis, the entire port will either become authorized or unauthorized and multiple hosts have network access on the local area network (LAN) segment. When authentication is configured on a MAC address basis, each device must be authorized individually to access the network.

When the AOS device operates as a supplicant, unit interfaces request authentication from a peer authenticator and respond to EAP identity requests. The authentication process begins when an interface transmits an EAPOL start frame to the authenticator, or when the interface receives an EAP identity request from the authenticator. When the AOS device is operating as a supplicant, a user-specified user name and password is used for authentication. This information can optionally be encrypted using message-digest algorithm 5 (MD5). EAP methods supported by AOS are listed in *Port Authentication Limitations on page 5*.

Once the authorization process is complete, ports or specific devices (based on MAC addresses or voice VLANs) will either have access to the network, or they will be unauthorized. When ports are unauthorized, they can be configured to control the direction of traffic. This control can limit traffic to ingress only, or can limit both ingress and egress traffic if supported by the platform. If the Guest VLAN feature is enabled, devices that fail authentication can be given guest access with the privileges defined for the guest VLAN.

Hardware and Software Requirements and Limitations

The port security portion of the port access control suite has been available on most AOS products since AOS firmware release 8.0. However, VLAN-aware port security is only available on AOS products running AOS firmware 17.09.01 or later.

The port protection portion of the port access control suite has been available on most AOS products since AOS firmware release 10.01.00.

The port authentication portion of the port access control suite has been available on most AOS products since AOS firmware release 10.01.00.

The Guest VLAN portion of the port access control suite has been available on most AOS products since AOS firmware release R11.6.0.

Voice-based port authentication was introduced on AOS switch products in firmware release R11.13.0.

To determine whether your platform supports any of the port access control suite features, refer to the *AOS Product Feature Matrix* available online at https://supportforums.adtran.com.

Port Security Limitations

In non-VLAN aware port security, only static access ports can be secured. Ports configured as a trunk port, dynamic port, or cluster port will not support port security. In addition, ports that are configured as a destination port for a monitor session, a member of a port channel group, or are using the 802.1x protocol will not support port security. If a port is using 802.1x protocol, security measures are achieved by port authentication.

VLAN-aware port security allows interfaces that are VLAN trunked interfaces to support port security. Port channel interfaces will not support VLAN-aware port security.

In VLAN-aware port security, voice VLANs can learn new secure MAC addresses, as well as statically accept new secure MAC addresses. In addition, all traditional port security configurations are supported in VLAN-aware port security.

You cannot configure the same sticky or static MAC address on multiple ports in port security. Each host is locked to the port to which the address is assigned.

Port Protection Limitations

It is not possible to protect a port that is configured for trunking.

When a port is in access mode, a protected port will only communicate with an unprotected port.

Port Authentication Limitations

When using port authentication on a per-port basis, the entire port becomes either authorized or unauthorized. Only one supplicant needs to be authenticated for the port to operate as an authorized port. When using port authentication on a per-MAC address or voice VLAN basis, each device must be authorized in order to pass traffic.

As of AOS firmware release R10.8.0, AOS supports the following EAP authentication methods:

- EAP
- Protected EAP (PEAP)
- EAP-MD5
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Tunneled Transport Layer Security (EAP-TTLS)
- EAP-Generic Token Card (EAP-GTC)

Port authentication cannot be used with a port that is currently protected with port security.

Voice-based port authentication, typically used when an IP phone or other voice product is configured to authenticate using MAC authentication bypass (MAB), works in conjunction with a voice VLAN configured on the AOS device. A voice VLAN must be configured on the port for voice-based port authentication to function. In addition, the voice VLAN information used for voice-based port authentication is received on the IP phone (or other voice product) using Link Layer Discovery Protocol-Media Endpoint Discovery LLDP-MED. Dynamic Host Control Protocol (DHCP) is not required for VLAN discovery.

Configuring Port Security

Port security can be configured by adding the device's MAC address to the secure MAC address table using either the GUI or the CLI. To correctly configure port security, you will need to complete the following steps:

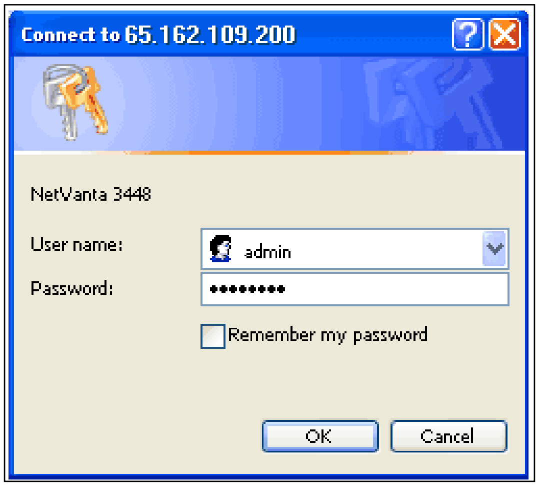
1. Enable port security on the interface.
2. Configure the general port security settings, including the timeout period for secure MAC address entries, the port expiration time, and the maximum number of allowed secure MAC addresses.
3. Enter the MAC address using one of the following methods: static entry, dynamic entry, or as a sticky address. Sticky MAC addresses are dynamically learned addresses that are added to the AOS unit's forwarding table and running configuration, and stored as static entries when the configuration is saved. If sticky MAC addresses are disabled, the MAC address entries become secure dynamic MAC addresses. At this time you will also specify if the address is associated with a VLAN to enable VLAN-aware port security.
4. Specify the action taken when a security violation is detected. (This can only be configured using the CLI. Refer to *Specifying the Action for Security Violations on page 16* for instructions).

Configuring Port Security Using the GUI

To begin configuring port security, you must first connect to the GUI. To connect to the GUI, follow these steps:

1. Open a new web page in your Internet browser.
2. Enter your AOS product's IP address in the Internet browser's address field in the form **http:**//<*ip address*>, for example:

   http://65.162.109.200
3. At the prompt, enter your user name and password and select **OK**.



Connect to 65.162.109.200

NetVanta 3448

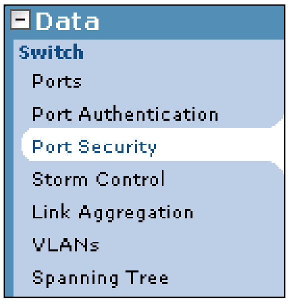
User name: admin

Password: ••••••••

□ Remember my password

*The default user name is **admin** and the default password is **password**.*

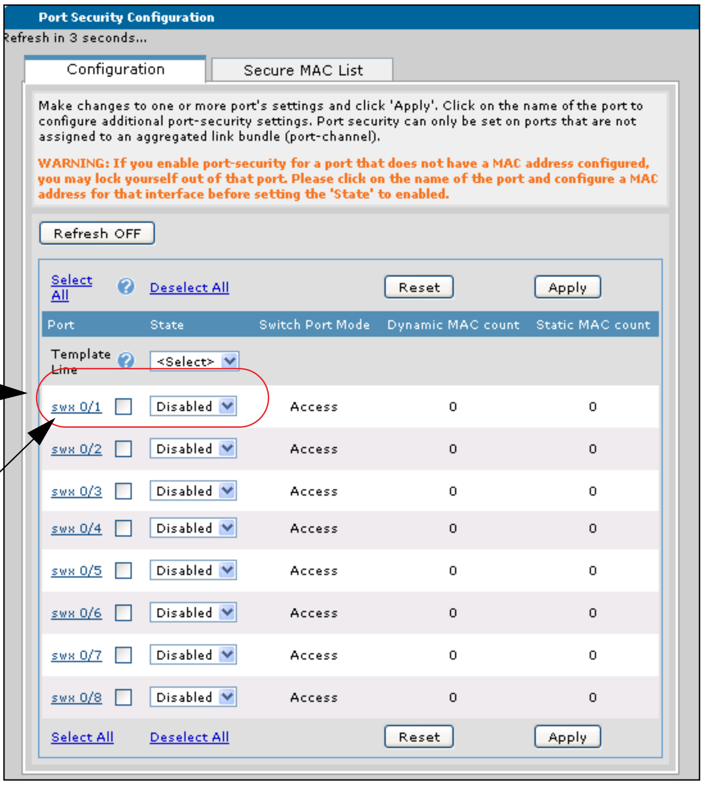
4. Navigate to **Data** > **Port Security**.



5. From the list on the left of the **Port Security Configuration** menu, enable port security on the interface using the check box next to the interface name and selecting **Enable** from the **State** drop-down list. Then select **Apply**.

> NOTE
>
> *You could lock yourself out of the port if you enable port security on an interface without a configured MAC address. If you need to add a MAC address to the port, select the interface from the list on the left of the **Port Security Configuration** menu and proceed to Step 6. Once you have configured the MAC address, return to this menu and enable port security.*

Once port security is enabled, select the interface hyperlink to change the default port security settings and add MAC addresses to the interface's port security settings.



Port Security Configuration

Refresh in 3 seconds...

Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port-security settings. Port security can only be set on ports that are not assigned to an aggregated link bundle (port-channel).

WARNING: If you enable port-security for a port that does not have a MAC address configured, you may lock yourself out of that port. Please click on the name of the port and configure a MAC address for that interface before setting the 'State' to enabled.

Port		State	Switch Port Mode	Dynamic MAC count	Static MAC count
Template Line		<Select>			
swx 0/1	☐	Disabled	Access	0	0
swx 0/2	☐	Disabled	Access	0	0
swx 0/3	☐	Disabled	Access	0	0
swx 0/4	☐	Disabled	Access	0	0
swx 0/5	☐	Disabled	Access	0	0
swx 0/6	☐	Disabled	Access	0	0
swx 0/7	☐	Disabled	Access	0	0
swx 0/8	☐	Disabled	Access	0	0

1. Select check box and select **Enable** from the **State** drop-down list.

2. Select the interface hyperlink to change the default port security settings.

> NOTE
>
> *In firmware releases prior to AOS 17.09.01, if a port is configured as a trunk, it will be light gray in appearance and cannot be selected for port security configuration. To access the port security settings for an interface used as a trunk, you must change the interface to access mode.*

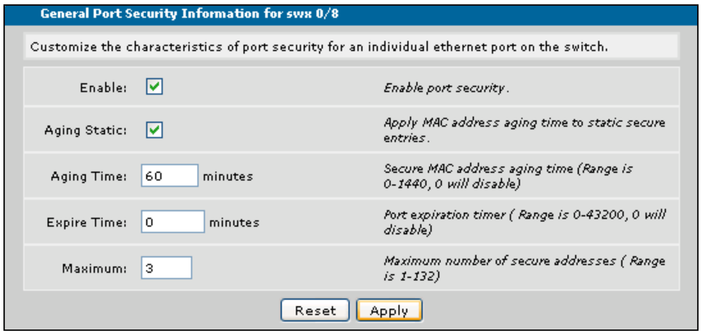
6. Configure the general settings for port security from the selected interface's **General Port Security Information** menu. From this menu, you can enable port security on the specific port by checking the box next to **Enable**.

   You can also specify that secure MAC address entries have the ability to time out by selecting the **Aging Static** check box and specifying the aging time (in minutes). By enabling aging, entries in the secure MAC address table are removed once the aging time assigned to each entry has expired. The address is relearned once another packet is received from the address as long as a security violation has not been detected, and the same MAC address has not been learned on another interface within the same VLAN. Aging timeout periods range from **0** to **1440** minutes. A timeout period of **0** disables the aging feature. By default, MAC address aging is disabled and the timeout period is set to **0**.

   You can also specify the port expiration time from this menu. Port expiration forces the port into a shutdown state after the specified period of time (regardless of inactivity). Port expiration times range from **0** to **43200** minutes. An expiration time of **0** disables the expiration feature. By default, port expiration is disabled and the expiration time is set to **0**.

   Lastly, from this menu you can specify the maximum number of allowed secure MAC addresses. By default, **1** secure MAC address is allowed. The valid range of allowed MAC addresses is **1** to **132**. This number should be adjusted to reflect the number of devices that will be connecting through the port. For example, if you are using port security with an IP phone and a PC, you will need to specify at least **2** secure MAC addresses are allowed to cover both the phone and the PC.

   In the example below, port security is enabled on switchport 0/8, and an aging time of **60** minutes is configured for secure MAC addresses. In addition, port expiration is disabled and a maximum of **3** MAC addresses are allowed.



General Port Security Information for swx 0/8

Customize the characteristics of port security for an individual ethernet port on the switch.

Enable:	☑	*Enable port security.*
Aging Static:	☑	*Apply MAC address aging time to static secure entries.*
Aging Time:	60 minutes	*Secure MAC address aging time (Range is 0-1440, 0 will disable)*
Expire Time:	0 minutes	*Port expiration timer (Range is 0-43200, 0 will disable)*
Maximum:	3	*Maximum number of secure addresses (Range is 1-132)*

   In addition, certain units support specifying the action taken when a security violation occurs and enabling sticky MAC addresses from this menu.

   Conditions that constitute security violations in port security include:

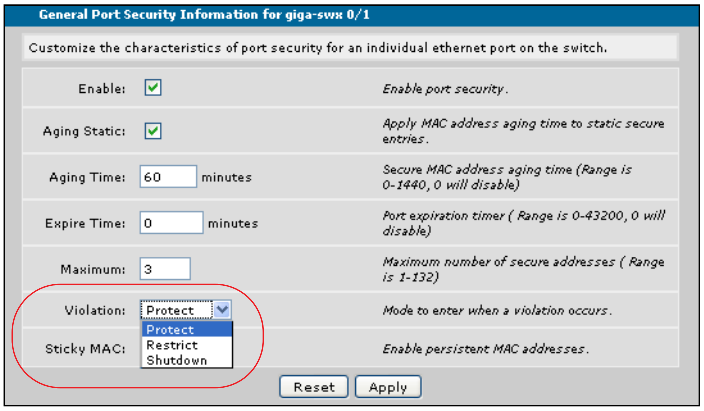
   - The system is attempting to learn a new address from an unknown source after the maximum number of secure addresses configured for that interface has been reached.
   - The system is attempting to learn a new address that is currently configured as a secure MAC address on another interface within the same VLAN.

   When either of these conditions is detected, it is determined to be a security violation. When a security violation occurs, you can specify what action you want to take. You can specify that the interface becomes protected, which means that the interface does not learn any new secure addresses (nor allow these new sources to pass traffic) until the number of currently active secure addresses drops below the maximum setting. You can also specify that access to the interface is restricted, which creates a log of the event in addition to protecting the port. You can also specify that the interface on which the violation has been detected is shut down and a log of the event is created.

> NOTE
>
> *Not all AOS platforms support violation actions. Consult the AOS Product Feature Matrix, available online at https://supportforums.adtran.com, to determine if your product supports port security violation actions.*

To specify an action once a security violation has been discovered, select **Protect**, **Restrict**, or **Shutdown** from the **Violation** drop-down list.

- The **Protect** parameter places the interface in a protected state, and does not forward packet frames above those from the allowed maximum of secure MAC addresses for the interface. When in a protected state, no notification of dropped packets is sent using syslog, event log, or Simple Network Management Protocol (SNMP) trap.
- The **Restrict** parameter restricts traffic across the interface, which also means that packet frames above those allowed by the maximum number of secure MAC addresses are dropped, but these packet losses are tracked by the security violation counter and notification of each event is sent using syslog, event log, or SNMP trap.
- The **Shutdown** parameter places the port in administrative shutdown, is tracked by the security violation counter, and is included in event notification through syslog, event log, or SNMP trap. When a port is placed in administrative shutdown, only the administrator can put the port back in service.

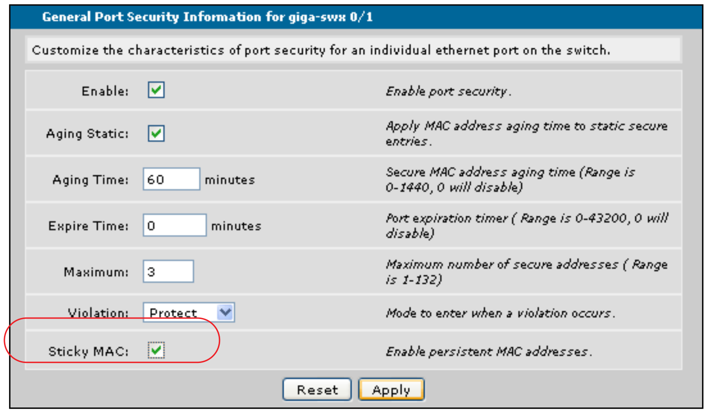


General Port Security Information for giga-swx 0/1

Customize the characteristics of port security for an individual ethernet port on the switch.

Enable:	☑	*Enable port security.*
Aging Static:	☑	*Apply MAC address aging time to static secure entries.*
Aging Time:	60 minutes	*Secure MAC address aging time (Range is 0-1440, 0 will disable)*
Expire Time:	0 minutes	*Port expiration timer (Range is 0-43200, 0 will disable)*
Maximum:	3	*Maximum number of secure addresses (Range is 1-132)*
Violation:	Protect	*Mode to enter when a violation occurs.*
Sticky MAC:		*Enable persistent MAC addresses.*

Next, enable sticky MAC addresses by using the **Sticky MAC** check box. A sticky MAC address is a secure MAC address that is learned in a dynamic manner and is added to the system as if it was configured statically. Sticky MAC addresses appear in the unit's configuration and persist after a reboot if the configuration is saved. If sticky MACs are enabled through the GUI, then all dynamic addresses become persistent.



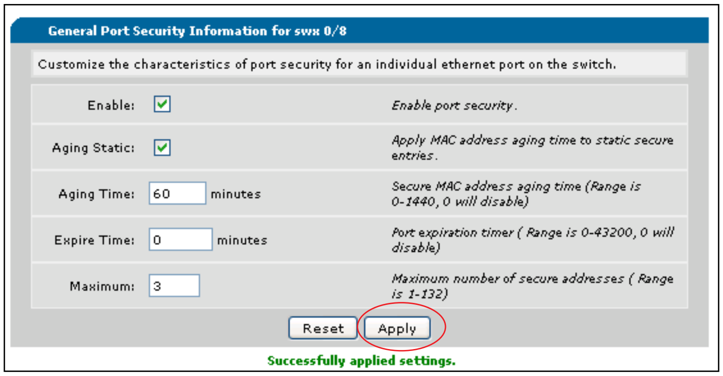
General Port Security Information for giga-swx 0/1

Customize the characteristics of port security for an individual ethernet port on the switch.

Enable:	☑	*Enable port security.*
Aging Static:	☑	*Apply MAC address aging time to static secure entries.*
Aging Time:	60 minutes	*Secure MAC address aging time (Range is 0-1440, 0 will disable)*
Expire Time:	0 minutes	*Port expiration timer (Range is 0-43200, 0 will disable)*
Maximum:	3	*Maximum number of secure addresses (Range is 1-132)*
Violation:	Protect	*Mode to enter when a violation occurs.*
Sticky MAC:	☑	*Enable persistent MAC addresses.*

*Not all units support security violation and sticky MAC address configuration through the GUI. If your unit does not show these features in the **General Port Security Information** menu, you must configure security violations and sticky MAC address parameters using the CLI. These steps are described in Entering MAC Addresses on page 15 and Specifying the Action for Security Violations on page 16.*

Once you have configured the general settings for port security, select **Apply** to apply the settings and receive configuration confirmation.



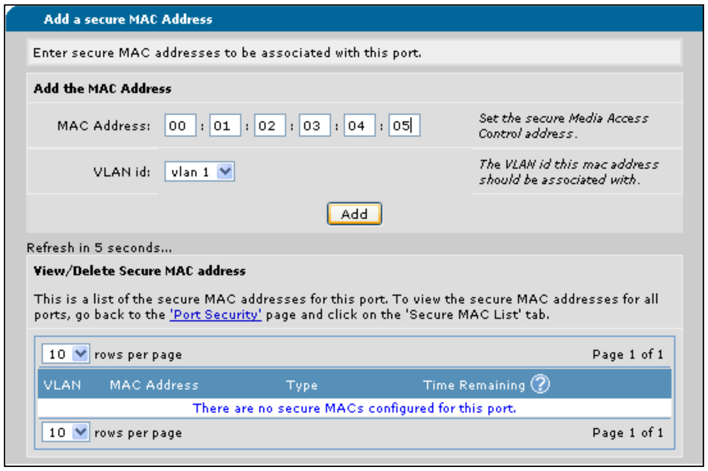
General Port Security Information for swx 0/8

Customize the characteristics of port security for an individual ethernet port on the switch.

Enable:	☑	*Enable port security.*
Aging Static:	☑	*Apply MAC address aging time to static secure entries.*
Aging Time:	60 minutes	*Secure MAC address aging time (Range is 0-1440, 0 will disable)*
Expire Time:	0 minutes	*Port expiration timer (Range is 0-43200, 0 will disable)*
Maximum:	3	*Maximum number of secure addresses (Range is 1-132)*

Successfully applied settings.

7. The next step in the port security configuration is to enter the MAC addresses you want associated with the port. Scroll down to the **Add a secure MAC Address** menu and enter the MAC address in the appropriate field. If you are adding port security to a VLAN trunk port, you can select the appropriate VLAN from the **VLAN id** drop-down list. When you have entered the correct MAC address and VLAN, select **Add**.



Add a secure MAC Address

Enter secure MAC addresses to be associated with this port.

Add the MAC Address

MAC Address: 00 : 01 : 02 : 03 : 04 : 05 — Set the secure Media Access Control address.

VLAN id: vlan 1 — The VLAN id this mac address should be associated with.

Refresh in 5 seconds...

View/Delete Secure MAC address

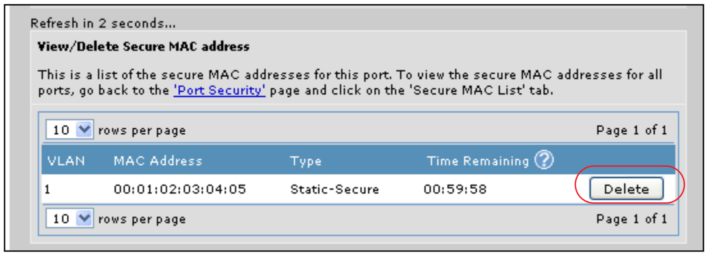
This is a list of the secure MAC addresses for this port. To view the secure MAC addresses for all ports, go back to the 'Port Security' page and click on the 'Secure MAC List' tab.

10 rows per page Page 1 of 1

VLAN	MAC Address	Type	Time Remaining
There are no secure MACs configured for this port.			

10 rows per page Page 1 of 1

Once you have selected **Add**, the MAC address appears in the list at the bottom of the **Add secure MAC Address** menu. You can repeat this process to add additional MAC addresses to the port. You can also delete any MAC addresses from the port by selecting **Delete** next to the MAC address in the list.



Refresh in 2 seconds...

View/Delete Secure MAC address

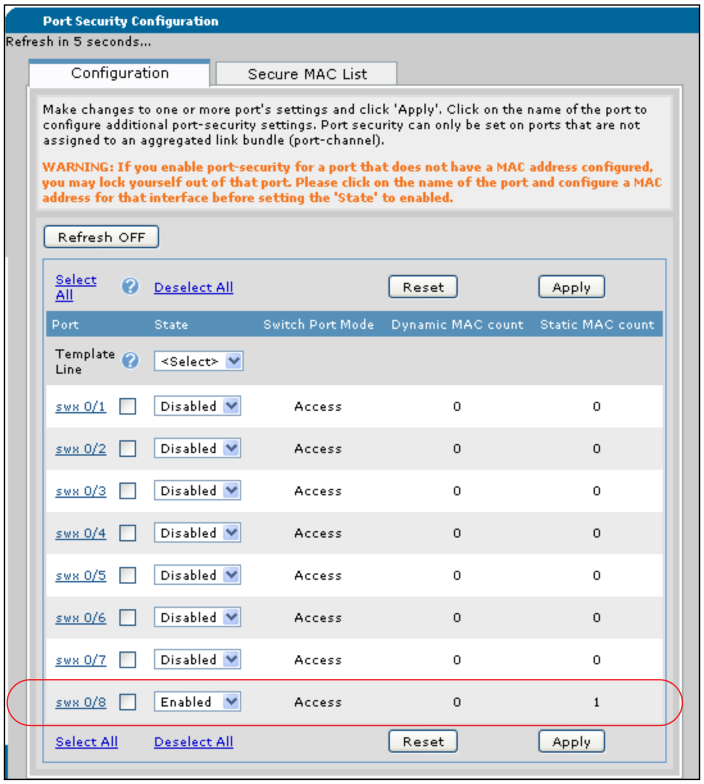
This is a list of the secure MAC addresses for this port. To view the secure MAC addresses for all ports, go back to the 'Port Security' page and click on the 'Secure MAC List' tab.

10 rows per page Page 1 of 1

VLAN	MAC Address	Type	Time Remaining	
1	00:01:02:03:04:05	Static-Secure	00:59:58	Delete

10 rows per page Page 1 of 1

8. To verify that port security is enabled on the specified port, navigate back to **Data** > **Port Security**. The configured port now appears in the list as **Enabled**.



Port Security Configuration

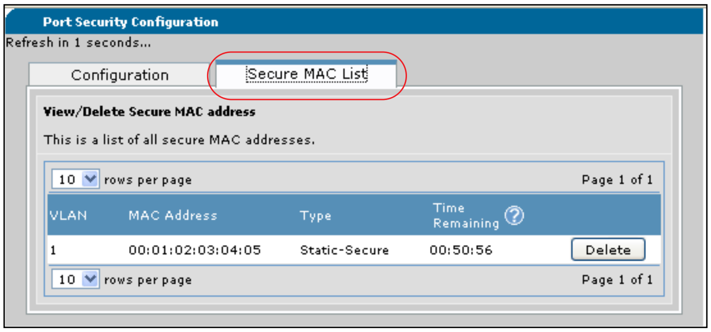
Refresh in 5 seconds...

Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port-security settings. Port security can only be set on ports that are not assigned to an aggregated link bundle (port-channel).

WARNING: If you enable port-security for a port that does not have a MAC address configured, you may lock yourself out of that port. Please click on the name of the port and configure a MAC address for that interface before setting the 'State' to enabled.

Port		State	Switch Port Mode	Dynamic MAC count	Static MAC count
Template Line		<Select>			
swx 0/1	□	Disabled	Access	0	0
swx 0/2	□	Disabled	Access	0	0
swx 0/3	□	Disabled	Access	0	0
swx 0/4	□	Disabled	Access	0	0
swx 0/5	□	Disabled	Access	0	0
swx 0/6	□	Disabled	Access	0	0
swx 0/7	□	Disabled	Access	0	0
swx 0/8	□	Enabled	Access	0	1

9. From this menu, you can also see a complete list of the secure MAC addresses configured for port security on the unit by selecting the **Secure MAC List** tab.



Port Security Configuration

Refresh in 1 seconds...

View/Delete Secure MAC address

This is a list of all secure MAC addresses.

10 rows per page Page 1 of 1

VLAN	MAC Address	Type	Time Remaining	
1	00:01:02:03:04:05	Static-Secure	00:50:56	Delete

10 rows per page Page 1 of 1

Port security has now been configured and enabled. Repeat these steps for additional port security configurations.

Dynamically learned secure MAC addresses do not have to be manually entered. The dynamic MAC addresses associated with the port will, however, be displayed on the ***Secure MAC List*** *tab in the main* ***Port Security Configuration*** *menu.*

Configuring Port Security Using the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 208.61.209.1.

> NOTE *If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter the Enable mode by entering **enable** at the prompt as follows:

   ```
   >enable
   ```

5. Enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

   ```
   #config terminal
   (config)#
   ```

After connecting to the CLI, the first step in configuring port security is to make sure the port is in static access mode. The port must be in static access mode for port security to be enabled. To set the port in static access mode, enter the **switchport mode access** command from the interface's configuration mode as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#switchport mode access
```

> NOTE *If you are using AOS firmware 17.09.01 or later, you do not need to specify that the port is in static access mode. You can begin configuring port security by enabling the feature on the interface.*

Next, enable port security on the interface using the **switchport port-security** command from the interface configuration mode. By default, port security is disabled and no MAC addresses are defined. Using the **no** form of this command disables port security. Enter the command as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#switchport port-security
```

General Port Security Settings

Next, specify the general port security settings for the port. These settings include specifying the timeout period for secure MAC address entries, the port expiration time, and the maximum number of allowed secure MAC addresses.

To specify the timeout period for secure MAC address entries, enter the **switchport port-security aging [static | time** <*value*> **| type absolute]** command from the interface's configuration mode. The aging parameter specifies that the entries in the secure MAC address table are removed once the aging time assigned to each type of entry has expired. The address is relearned once another packet is received after the expiration, providing a security violation has not been detected. The **static** parameter indicates that the MAC address aging time is applied to static secure MAC address entries. To specify that dynamic MAC addresses are aged, enter the **no** form of the **switchport port-security aging static** command. The **time** <*value*> parameter specifies the timeout period in minutes. The valid timeout range is **0** to **1440** minutes. When the timeout period is set to **0**, the aging feature is disabled. By default, the timeout period is set to **0**. The **type absolute** parameter indicates that the timeout occurs regardless of inactivity. Using the **no** version of this command disables the aging feature.

To specify that the aging time is set to **60** minutes, that **dynamic** MAC addresses are aged, and that the timeout occurs regardless of inactivity, enter the following commands:

```
(config-swx 0/8)#switchport port-security aging time 60
(config-swx 0/8)#no switchport port-security aging static
(config-swx 0/8)#switchport port-security aging type absolute
```

In addition to specifying the timeout period for secure MAC address entries, you can optionally specify an expiration time for the port itself. Specifying a port expiration time forces the interface into a shutdown state after the specified period of time. Port timeout periods are specified in minutes, with a valid range of **0** to **43200** minutes. When set to **0**, port expiration is disabled. By default, port expiration time is set to **0**. In addition, port expiration can be specified as an absolute timeout, which shuts down the port regardless of inactivity. To specify the port expiration time and type, enter the **switchport port-security expire [time** <*value*> **| type absolute]** command from the interface's configuration mode as follows:

```
(config-swx 0/8)#switchport port-security expire time 120
(config-swx 0/8)#switchport port-security type absolute
```

Using the **no** form of this command removes the port expiration from the port security configuration.

After configuring the aging time of MAC address entries and the expiration time for the port, the next step is to configure the maximum number of secure MAC addresses allowed in the secure MAC address table. This number is set using the **switchport port-security maximum** <*number*> command from the interface's configuration mode. The <*number*> parameter indicates how many addresses are allowed, and has a range of **1** to **132**. By default, **1** secure MAC address is allowed. Using the **no** form of this command returns the number to the default value. This number should be set to the number of devices you anticipate needing secure access to the network. To specify that **3** secure MAC addresses are stored in the secure MAC address table, and that no other addresses will gain secure access, enter the command as follows:

```
(config-swx 0/8)#switchport port-security maximum 3
```

Entering MAC Addresses

MAC addresses can be added to the secure MAC address table for port security in one of three ways: statically, dynamically, or as a sticky address.

Adding a static MAC address is completed by manually entering the address using the **switchport port-security mac-address** <*mac address*> command from the interface's configuration mode. Using the **no** form of this command removes the MAC address entry. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**). To specify a static MAC address as secure, enter the command as follows:

```
(config-swx 0/8)#switchport port-security mac-address 00:01:02:03:04:05
```

In addition, if the static MAC address is also part of a VLAN trunk that requires port security, you can specify the associated VLAN by entering the **switchport port-security mac-address** <*mac address*> **vlan** <*vlan id*> command from the interface's configuration mode. The <*vlan id*> parameter is the ID number of the VLAN you want to associate with the MAC address. The valid VLAN ID range is **1** to **4094**. To add a static MAC address with an associated VLAN, enter the command as follows:

```
(config-swx 0/8)#switchport port-security mac-address 00:01:02:03:04:05 vlan 100
```

> NOTE *VLANs can only be associated with secure MAC addresses in AOS products using AOS firmware release 17.09.01 or later.*

> NOTE *If no VLAN is specified, port security will automatically use the native VLAN.*

MAC addresses learned dynamically from an incoming packet can also be designated as a secure MAC addresses. These addresses do not have to be manually entered.

The third type of MAC address supported by port security is a sticky MAC address. A sticky MAC address is a secure MAC address that is learned in a dynamic manner and is added to the system as if it was configured statically. Sticky MAC addresses appear in the unit's configuration and persist after a reboot if the configuration is saved. To specify a sticky MAC address, enter the **switchport port-security mac-address sticky [**<*mac address*> **| sticky-volatile] [vlan** <*vlan id*>**]** command from the interface's configuration mode. You can optionally specify the MAC address using the <*mac address*> parameter. If you do not specify a MAC address with this command, then all dynamic addresses become persistent. If you do specify a MAC address, only the specified address is persistent. The **sticky-volatile** keywords specify that sticky address learning is enabled only for the immediate session. These learned addresses do not appear in the configuration and do not persist across a reboot. By default, sticky learning is disabled. To enable sticky learning and specify a MAC address, enter the command as follows:

```
(config-swx 0/8)#switchport port-security mac-address sticky 00:01:02:03:04:05
```

If you want to associate the MAC address with a VLAN, enter the **vlan** <*vlan id*> parameters at the end of the command. The VLAN ID is the ID number of the VLAN you want to associate with the MAC address. The valid VLAN ID range is **1** to **4094**. Enter the command as follows:

```
(config-swx 0/8)#switchport port-security mac-address sticky 00:01:02:03:04:05 vlan 100
```

Repeat these commands to add as many MAC addresses to the secure MAC address table as needed. You cannot add more addresses than specified as the maximum.

Specifying the Action for Security Violations

Conditions that constitute security violations in port security include:

- The system is attempting to learn a new address from an unknown source after the maximum number of secure addresses configured for that interface have been reached.
- The system is attempting to learn a new address that is currently configured as a secure MAC address on another interface within the same VLAN.

When either of these conditions is detected, it is determined to be a security violation. When a security violation occurs, you can specify what action you want to take. You can specify that the interface becomes protected, which means that the interface does not learn any new secure addresses (nor allow these new sources to pass traffic) until the number of currently active secure addresses drops below the maximum setting. You can also specify that access to the interface is restricted, which creates a log of the event in addition to protecting the port. You can also specify that the interface on which the violation has been detected is shut down and a log of the event is created.

> NOTE *Not all AOS platforms support violation actions. Consult the AOS Product Feature Matrix, available online at https://supportforums.adtran.com, to determine if your product supports port security violation actions.*

To specify an action once a security violation has been discovered, enter the **switchport port-security violation [protect | restrict | shutdown]** command from the interface's configuration mode. The **protect** parameter places the interface in a protected state, and does not forward packet frames above those from the allowed maximum of secure MAC addresses for the interface. When in a protected state, no notification of dropped packets is sent using syslog, event log, or SNMP trap. The **restrict** parameter restricts traffic across the interface, which also means that packet frames above those allowed by the maximum number of secure MAC addresses are dropped, but these packet losses are tracked by the security violation counter and notification of each event is sent using syslog, event log, or SNMP trap. The **shutdown** parameter places the port in administrative shutdown, is tracked by the security violation counter, and is included in event notification through syslog, event log, or SNMP trap. When a port is placed in administrative shutdown, only the administrator can put the port back in service by entering the **no shutdown** command from the interface's configuration mode.

Using the **no** form of the **switchport port-security violation** command removes the action from the port security configuration. By default, when a security violation is detected, the interface shuts down. To specify an action when a security violation is detected, enter the command as follows:

```
(config-swx 0/8)#switchport port-security violation shutdown
```

> NOTE *Once an interface is shut down because of a security violation, it can only be re-enabled by issuing the* ***no shutdown*** *command from the interface's configuration mode.*

Once the actions taken when a security violation is detected have been specified, the configuration of port security is complete. For port security configuration examples, refer to *Port Security Configuration Examples on page 34*.

Configuring Port Protection

Port protection operates by placing ports in protected mode, which prevents intra-VLAN communication between the protected ports. Any ports not configured as protected are considered unprotected, and can communicate with any other port.

Configuring port protection is basically specifying whether the port is protected or unprotected. Port protection can only be configured through the CLI. For directions to access the CLI, refer to *page 13*. By default, ports are in an unprotected state.

The port must be in static access mode for port protection to be enabled. To set the port in static access mode, enter the **switchport mode access** command from the interface’s configuration mode as follows:

```
(config-swx 0/8)#switchport mode access
```

NOTE *If you are using AOS firmware 17.09.01 or later, you do not need to specify that the port is in static access mode. You can begin configuring port security by enabling the feature on the interface.*

To place a port in a protected state after specifying the port is in access mode, enter the **switchport protected** command from the interface’s configuration mode as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#switchport protected
```

Using the **no** form of this command returns the port to an unprotected state.

Configuring Port Authentication

Port authentication is another way to control access to specified ports. Based on 802.1x authentication, port authentication provides the capability to restrict access to a port based on the port itself, the MAC address of a device attempting to use the port, or the VLAN of a device attempting to use the port. To correctly configure port authentication, you will need to complete the following steps:

1. Enable and configure AAA.
2. Specify that port authentication use a RADIUS server (configured by configuring AAA). Port authentication can also use a local user list rather than the RADIUS server, however, a RADIUS server is recommended.
3. Decide the type of authorization used by the port and/or enable 802.1x on the appropriate interface.
4. Decide if the 802.1x authorization will be port, MAC address, or voice based.

5. If the 802.1x authorization is port or voice based, optionally configure the following settings for the port: MAC authentication bypass. If the 802.1x authorization is port based, optionally configure the following settings for the port: multiple hosts and the direction of blocked traffic when the port is in an unauthorized state.
6. If a guest VLAN is to be used for devices that fail authentication, configure the guest VLAN and enable the Guest VLAN feature.

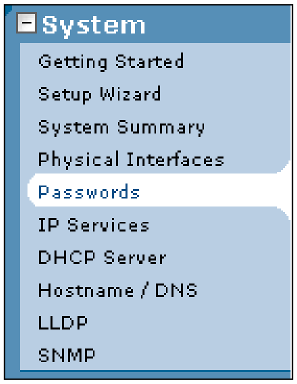
Configuring Port Authentication Using the GUI

To begin configuring port authentication, connect to the GUI (following the instructions outlined on *page 6*) and follow the steps outlined in the sections below.

Enabling AAA Services

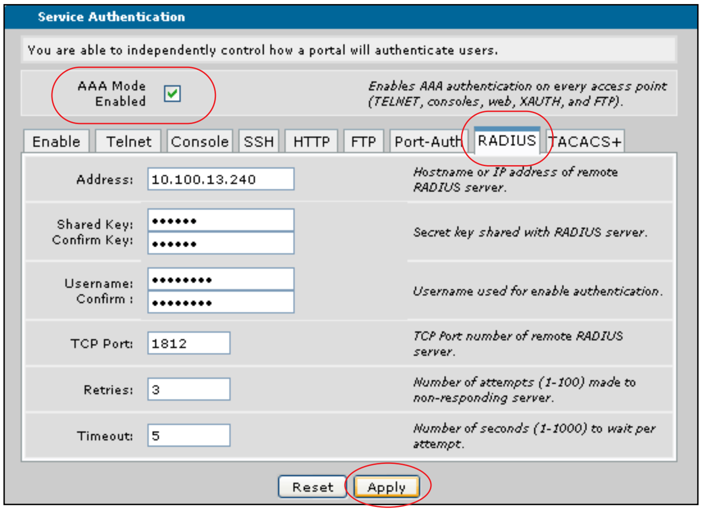
AAA must be enabled and configured for port authentication to be used. AAA is a complex suite of network security protocols and measures, and is not described in detail here. For more information about the complete configuration of AAA, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportforums.adtran.com. The following steps describe the necessary AAA configurations for use with port authentication.

1. Navigate to **System** > **Passwords** using the menu on the left of the GUI.



2. Scroll down to the **Service Authentication** menu and select the **AAA Mode Enabled** check box. Next, select the **RADIUS** tab and enter the RADIUS server configuration information. In the example below, the AOS unit is configured to send credentials to a RADIUS server at IP address **10.100.13.240**. Specify the key used by both the server and the AOS unit for authentication and the user name. Set the TCP port, which is set at **1812** by default, the number of allowed authentication attempts, which is set to **3** by

default, and the timeout period, which is set to **5** by default. When the necessary settings for your network have been entered, select **Apply**.



Service Authentication

You are able to independently control how a portal will authenticate users.

AAA Mode Enabled ☑ — *Enables AAA authentication on every access point (TELNET, consoles, web, XAUTH, and FTP).*

Address: 10.100.13.240 — *Hostname or IP address of remote RADIUS server.*

Shared Key: ••••••
Confirm Key: •••••• — *Secret key shared with RADIUS server.*

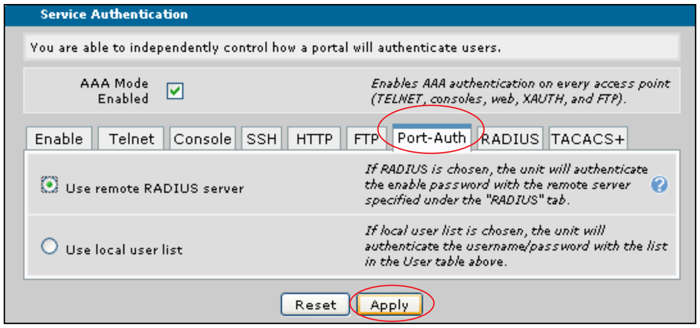
Username: ••••••••
Confirm : •••••••• — *Username used for enable authentication.*

TCP Port: 1812 — *TCP Port number of remote RADIUS server.*

Retries: 3 — *Number of attempts (1-100) made to non-responding server.*

Timeout: 5 — *Number of seconds (1-1000) to wait per attempt.*

3. Once the RADIUS settings have been applied, select the **Port-Auth** tab from the same **Service Authentication** menu. Select the **Use remote RADIUS server** radio button to specify that port authentication uses the RADIUS server for authentication, and select **Apply**.



Service Authentication

You are able to independently control how a portal will authenticate users.

AAA Mode Enabled ☑ — *Enables AAA authentication on every access point (TELNET, consoles, web, XAUTH, and FTP).*

● Use remote RADIUS server — *If RADIUS is chosen, the unit will authenticate the enable password with the remote server specified under the "RADIUS" tab.*

○ Use local user list — *If local user list is chosen, the unit will authenticate the username/password with the list in the User table above.*

You can optionally choose to use a local user list for port authentication rather than a RADIUS server. To specify that port authentication use the local user list, select **Use local user list** in the **Port-Auth** tab. The local user list is a user name and password system, defined in the **System** > **Passwords** menu at the top of the current GUI menu. You will need to specify user names and passwords in order to use the local user list as a port authentication method.

NOTE

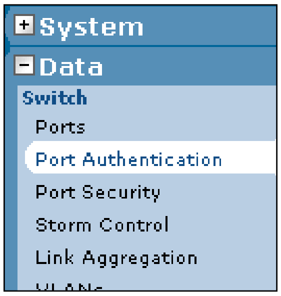
In certain cases, it is preferable to only define the RADIUS server, and not the local user list, to prevent users from accessing the network and its resources when the RADIUS server cannot be contacted. If this method is preferred, it is recommended to define multiple RADIUS servers in the event that the primary RADIUS server has a problem that cannot be readily corrected.

The necessary AAA portion of the port authentication configuration is now complete. The following sections describe the remaining port authentication configuration settings.

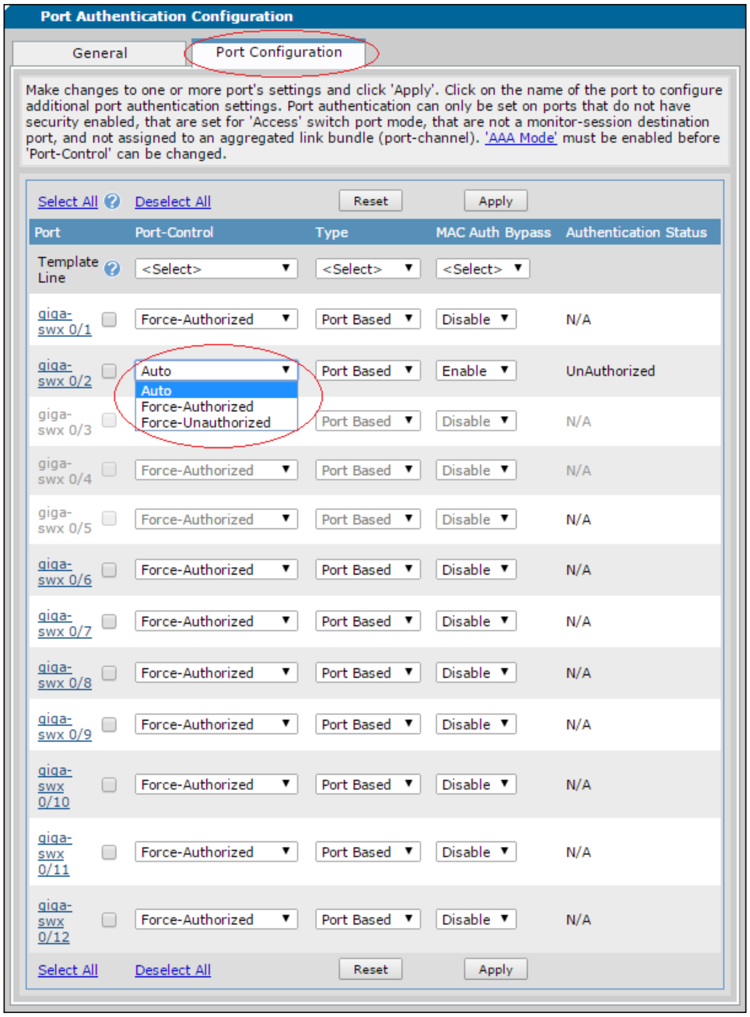
Configuring Port Authentication

After AAA is enabled and port authentication is set to use a RADIUS server for authentication, you can configure port authentication. To do so, follow these steps:

1. Navigate to **Data** > **Switch** > **Port Authentication** from the menu on the left of the GUI.



2. In the **Port Authentication Configuration** menu, select the **Port Configuration** tab.
3. Specify the **Port-Control** type from the drop-down list next to the interface you want to configure. Port control types include three options: **Auto**, **Force-Authorized**, and **Force-Unauthorized**.
   - **Auto** relies on 802.1x for authorization. This type of port control causes the port to enter an unauthorized state immediately after the port becomes active, and it allows a successful 802.1x authentication process to change its state to authorized.
   - **Force-Authorized** indicates that everyone attempting to access the port is allowed, without credentials. This type of port control forces the port into an authorized state when the port is in an active state. It is primarily used for connecting to other switches or devices that do not support 802.1x.
   - **Force-Unauthorized** indicates that no one receives access to the port. This type of port control forces the port into an unauthorized state when the port is in an active state. It is typically used when the port is never intended to be used, but a system administrator wants to keep the port active. By default, this condition will still transmit broadcast and multicast frames.



Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port	Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line	<Select>	<Select>	<Select>	
giga-swx 0/1 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/2 ☐	Auto	Port Based	Enable	UnAuthorized
giga-swx 0/3 ☐		Port Based	Disable	N/A
giga-swx 0/4 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/9 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/10 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/11 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/12 ☐	Force-Authorized	Port Based	Disable	N/A

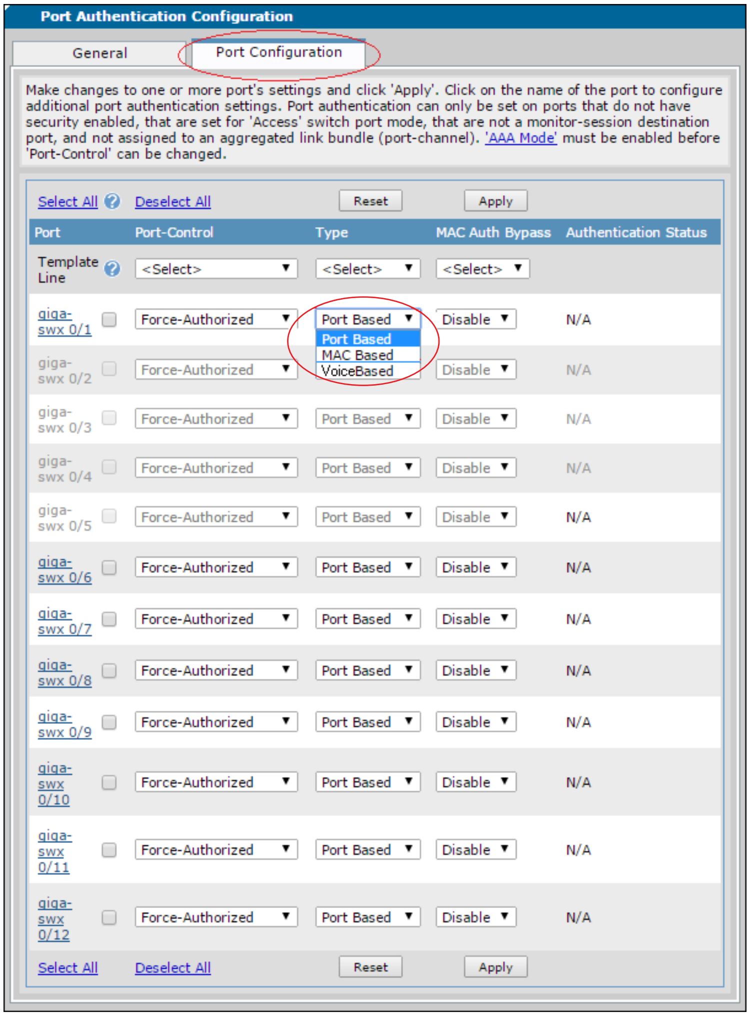
NOTE *If you find that the* ***Port-Control*** *options are not available, verify that AAA has been configured (as described in Enabling AAA Services on page 18) and make sure the port is not configured as a trunk.*

4. In the same menu, select the port authentication **Type** from the drop-down list next to the interface you are configuring. Type selections include **Port Based**, **MAC Based**, or **Voice Based**.

    - **Port Based** authentication specifies that the entire port is open to traffic when in an authorized state. This authentication method is compatible with every 802.1x client and authorizes the port to permit traffic flow after a single 802.1x client is authenticated. When using this type of port authentication, the port will immediately send an EAP identity request as soon as it becomes active. It will continue to send these requests periodically, even when it is active but in an unauthorized state. Once a device has been successfully authenticated, the port transitions to an authorized state and stops sending EAP identity requests. By default, this type of port authentication only allows the device that first authenticated to send traffic; however, this setting can be modified as described in *Optional Configuration for Port-Based Authentication on page 23*.
    - **MAC Based** authentication specifies that the port is open for the specific MAC address that is authorized. This authentication method requires that the 802.1x client supports EAP start messages

as is dictated by the IEEE 802.1x standard. When using this type of port authentication, the port enters an unauthorized state when it becomes active, but waits until it receives an EAP Start message from the client wanting to connect before it begins the authentication process. The port then sends the EAP Identity request to that specific client. Once the client has been successfully authenticated, the port transitions to an authorized state for only the authorized client’s MAC address.

- **Voice Based** authentication is used when two authenticated devices are expected on the port. One device will be the voice device and the other will be a data device. Typically the voice device is authenticated using MAC authentication bypass (MAB). The data device will be authenticated via MAB or EAP.



Port Authentication Configuration

Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port		Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line		<Select>	<Select>	<Select>	
giga-swx 0/1	□	Force-Authorized	Port Based Port Based MAC Based VoiceBased	Disable	N/A
giga-swx 0/2	□	Force-Authorized		Disable	N/A
giga-swx 0/3	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/4	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/9	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/10	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/11	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/12	□	Force-Authorized	Port Based	Disable	N/A

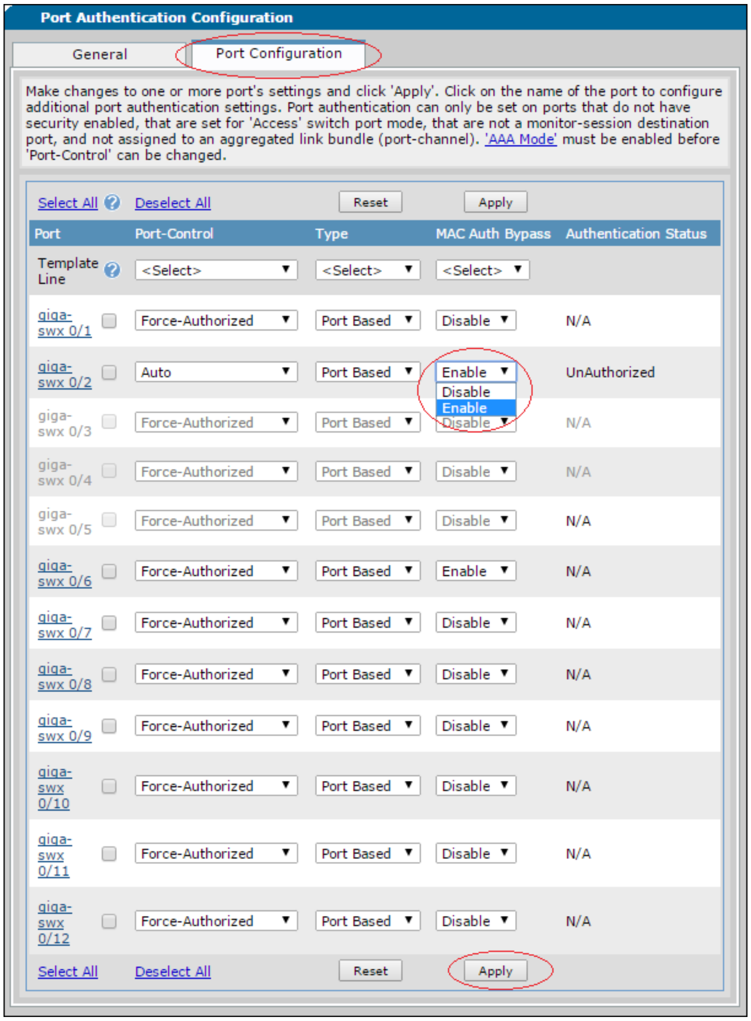
5. When you have specified the port control type and the authentication type, select **Apply** to apply the settings. If you have chosen **MAC Based** port authentication, you have completed the authentication configuration.

Optional Configuration for Port-Based Authentication

If you are using port-based authentication, you can optionally specify the following settings:

- MAC authentication bypass
- Direction of blocked traffic when the port is in an unauthorized state
- Multiple hosts can gain access when only a single device has been authorized

To configure MAC authentication bypass, select **Enable** from the **MAC Auth Bypass** drop-down list on the **Port Configuration** menu and then select **Apply**.



Port Authentication Configuration

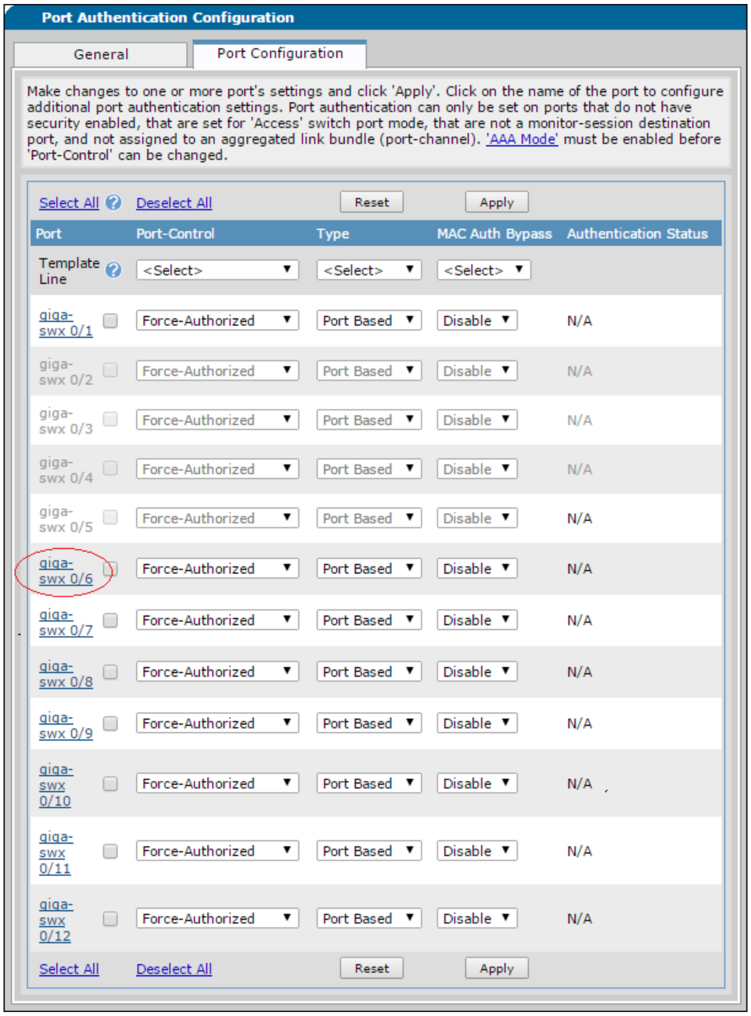
Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port		Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line		<Select> ▼	<Select> ▼	<Select> ▼	
giga-swx 0/1	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/2	☐	Auto ▼	Port Based ▼	Enable ▼ Disable Enable	UnAuthorized
giga-swx 0/3	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/4	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/5	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/6	☐	Force-Authorized ▼	Port Based ▼	Enable ▼	N/A
giga-swx 0/7	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/8	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/9	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/10	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/11	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A
giga-swx 0/12	☐	Force-Authorized ▼	Port Based ▼	Disable ▼	N/A

With MAC authentication bypass enabled, the port will authenticate with a RADIUS server using the source MAC address if 802.1x authentication times out. If a device connected to the port responds to 802.1x, MAC bypass will not be attempted.

To configure blocked traffic direction or to allow authorized port access to multiple hosts, follow these steps:

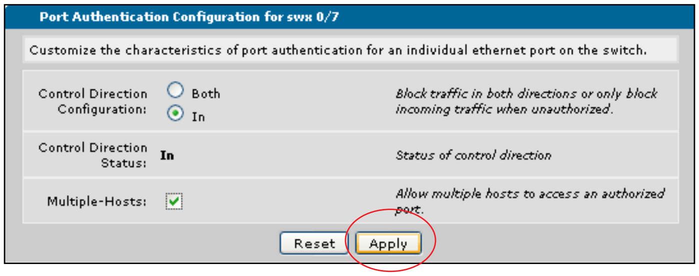
1. Select the interface from the list in the **Port Authentication Configuration** menu.



Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port	Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line	<Select>	<Select>	<Select>	
giga-swx 0/1 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/2 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/3 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/4 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/9 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/10 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/11 ☐	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/12 ☐	Force-Authorized	Port Based	Disable	N/A

2. When selected, you are directed to the **Port Authentication Configuration** menu for the specific interface. Here you can select whether the traffic on an unauthorized port is blocked in both directions, or only to incoming traffic, by selecting either the **Both** or **In** radio button (if applicable to your platform). In addition, you can specify that multiple hosts are allowed to access an authorized port by selecting the **Multiple-Hosts** check box. When you have made your selections, select **Apply**.

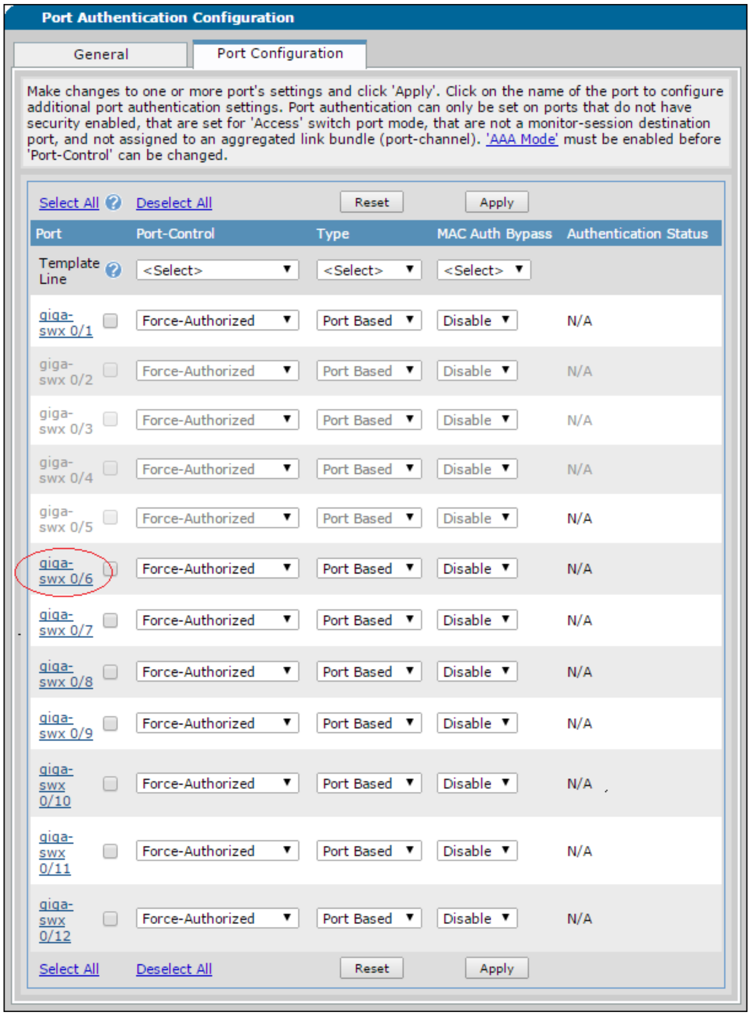


Customize the characteristics of port authentication for an individual ethernet port on the switch.

Control Direction Configuration:	○ Both ● In	*Block traffic in both directions or only block incoming traffic when unauthorized.*
Control Direction Status:	**In**	*Status of control direction*
Multiple-Hosts:	☑	*Allow multiple hosts to access an authorized port.*

Reauthentication

You can also immediately reauthorize a port, whether using port-based or MAC-based authentication, by selecting the interface from the list in the **Port Authentication Configuration** menu.



Port Authentication Configuration

General | Port Configuration

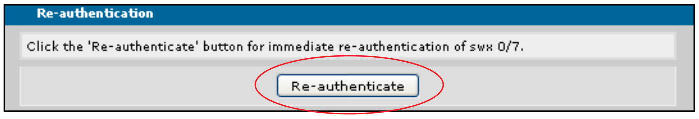
Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Select All | Deselect All | Reset | Apply

Port		Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line		<Select>	<Select>	<Select>	
giga-swx 0/1	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/2	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/3	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/4	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/9	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/10	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/11	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/12	□	Force-Authorized	Port Based	Disable	N/A

Select All | Deselect All | Reset | Apply

Once you have selected the interface, scroll down in the next menu to the **Re-authentication** menu. Select **Re-authenticate** to immediately reauthenticate the specific port.



Re-authentication

Click the 'Re-authenticate' button for immediate re-authentication of swx 0/7.

Re-authenticate

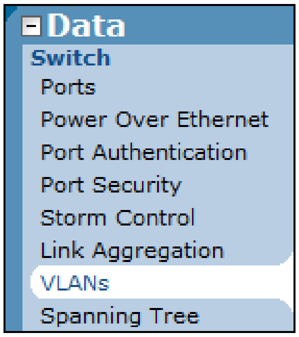
Optional Guest VLAN Configuration

Guest VLAN allows devices that fail 802.1x authentication to be assigned to a predefined guest VLAN. For example, if a printer is plugged into a port and there is no RADIUS server to authenticate the new device or if RADIUS is not responding, the printer will be assigned to the guest VLAN and have network access granted to that VLAN.

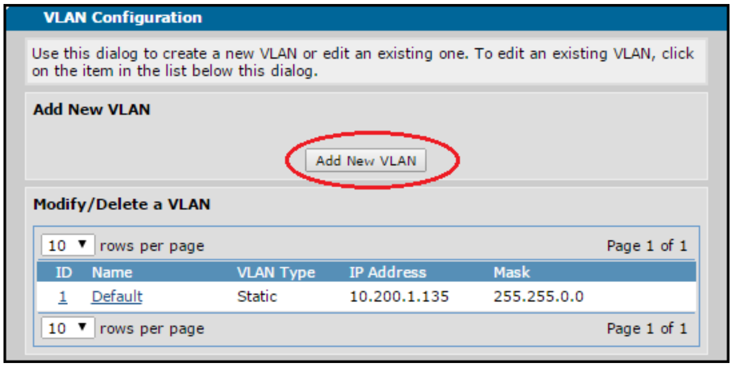
> NOTE *Remember to allow the guest VLAN to have connectivity to any other necessary VLANs.*

To create a guest VLAN, follow these steps:

1. Navigate to **Data** > **Switch** > **VLANs**.



2. From the **VLAN Configuration** menu, select **Add New VLAN**.



VLAN Configuration

Use this dialog to create a new VLAN or edit an existing one. To edit an existing VLAN, click on the item in the list below this dialog.

Add New VLAN

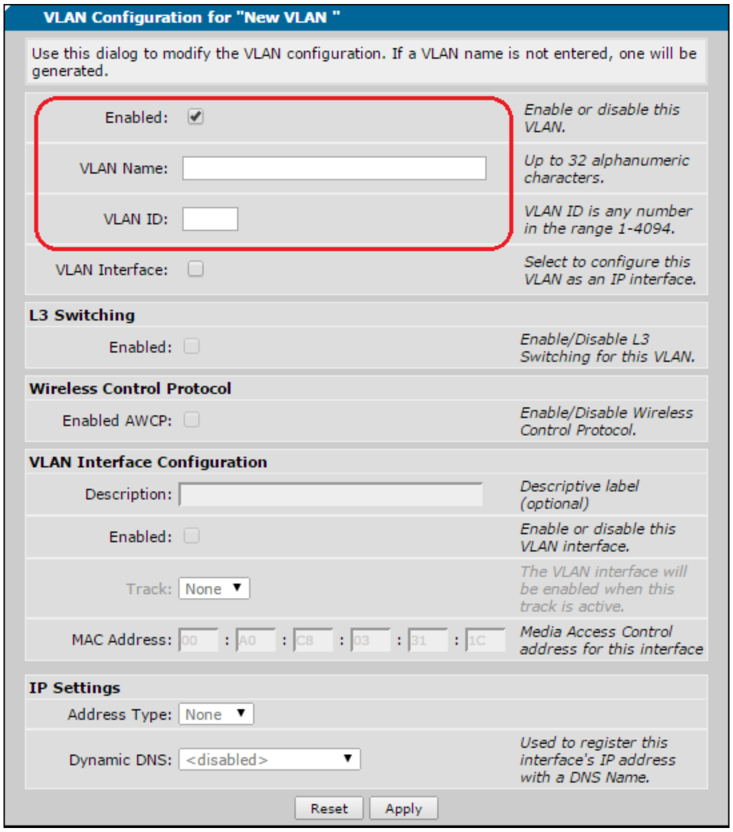
Modify/Delete a VLAN

10 ▼ rows per page Page 1 of 1

ID	Name	VLAN Type	IP Address	Mask
1	Default	Static	10.200.1.135	255.255.0.0

10 ▼ rows per page Page 1 of 1

3. Make sure the **Enabled** box is checked.



VLAN Configuration for "New VLAN "

Use this dialog to modify the VLAN configuration. If a VLAN name is not entered, one will be generated.

Enabled:	☑	*Enable or disable this VLAN.*
VLAN Name:		*Up to 32 alphanumeric characters.*
VLAN ID:		*VLAN ID is any number in the range 1-4094.*
VLAN Interface:	□	*Select to configure this VLAN as an IP interface.*
L3 Switching		
Enabled:	□	*Enable/Disable L3 Switching for this VLAN.*
Wireless Control Protocol		
Enabled AWCP:	□	*Enable/Disable Wireless Control Protocol.*
VLAN Interface Configuration		
Description:		*Descriptive label (optional)*
Enabled:	□	*Enable or disable this VLAN interface.*
Track:	None ▼	*The VLAN interface will be enabled when this track is active.*
MAC Address:	00 : A0 : C8 : 03 : 31 : 1C	*Media Access Control address for this interface*
IP Settings		
Address Type:	None ▼	
Dynamic DNS:	<disabled> ▼	*Used to register this interface's IP address with a DNS Name.*

Reset Apply

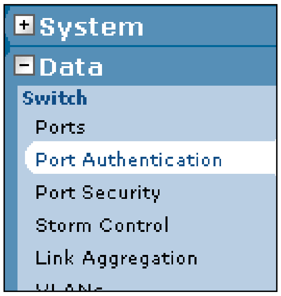
4. Enter the VLAN name and ID in the appropriate fields.

> NOTE
>
> *Both the VLAN name and ID must be unique throughout the network. The name is limited to 32 alphanumeric characters. The VLAN ID can be any number from **1** to **4094**.*

5. Select **Apply** to create the VLAN.

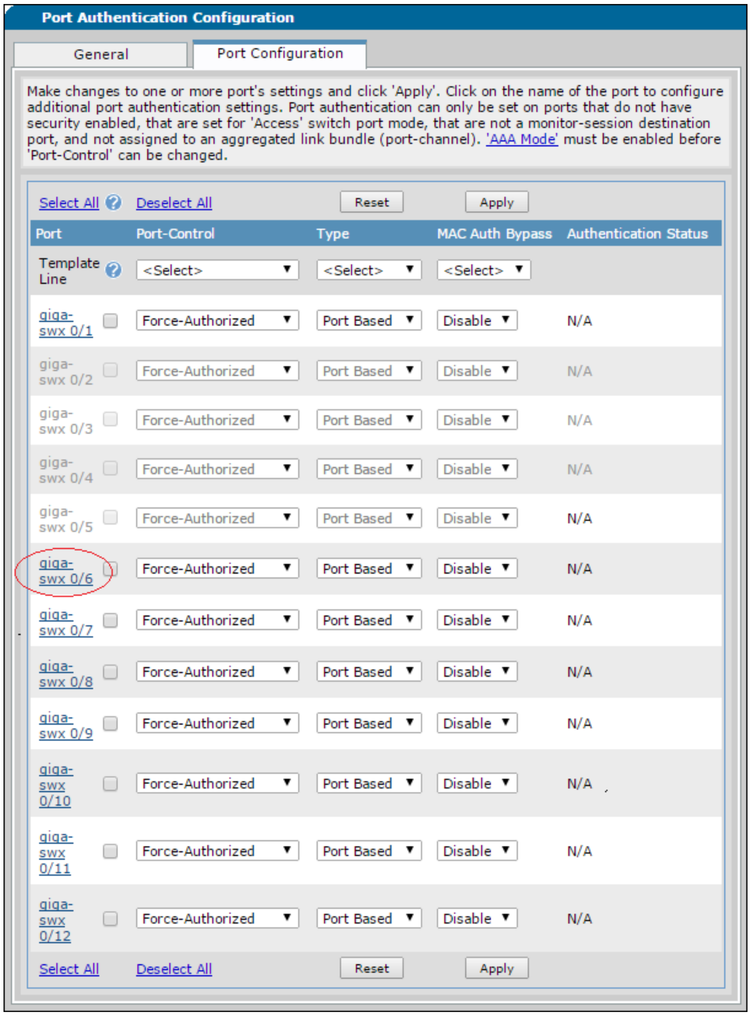
To enable the Guest VLAN feature, follow these steps:

1. Navigate to **Data** > **Switch** > **Port Authentication** from the menu on the left of the GUI.



2. In the **Port Authentication Configuration** menu, select the **Port Configuration** tab.

3. Select the interface from the list in the **Port Authentication Configuration** menu.

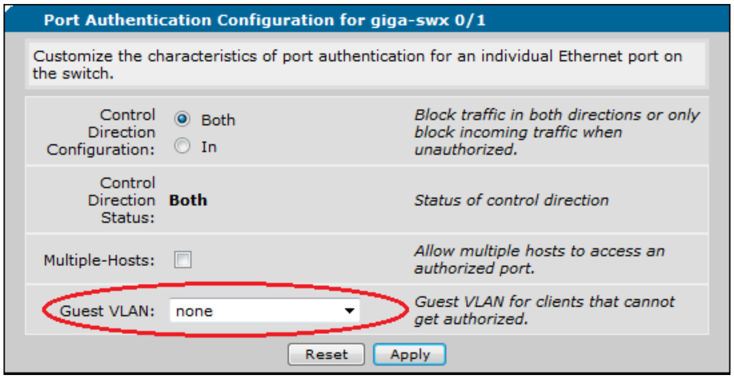


Port Authentication Configuration

Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port		Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line		<Select>	<Select>	<Select>	
giga-swx 0/1	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/2	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/3	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/4	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/9	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/10	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/11	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/12	□	Force-Authorized	Port Based	Disable	N/A

4. From the **Port Authentication Configuration** menu for the specific interface, select the VLAN to use from the **Guest VLAN** drop-down list.



Port Authentication Configuration for giga-swx 0/1

Customize the characteristics of port authentication for an individual Ethernet port on the switch.

Control Direction Configuration:	● Both ○ In	*Block traffic in both directions or only block incoming traffic when unauthorized.*
Control Direction Status:	**Both**	*Status of control direction*
Multiple-Hosts:	□	*Allow multiple hosts to access an authorized port.*
Guest VLAN:	none	*Guest VLAN for clients that cannot get authorized.*

5. Select **Apply**.

Configuring Port Authentication Using the CLI

Port authentication using the CLI is very similar to configuring the feature using the GUI. To configure port authentication using the CLI, you will need to configure AAA, specify that port authentication uses a RADIUS server (or local user list, if preferred), enable 802.1x on the appropriate ports, decide if 802.1x authentication is based on a port or MAC address, and then optionally (if using port-based authentication) specify in which direction traffic is blocked and if multiple hosts are allowed. These steps are covered in the following sections.

For directions to access the CLI, refer to *page 13*.

Enabling AAA Services

AAA must be enabled and configured for port authentication to be used. AAA is a complex suite of network security protocols and measures, and is not described in detail here. For more information about the complete configuration of AAA, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportforums.adtran.com. The following steps describe the necessary AAA configurations for use with port authentication.

1. Enable AAA using the **aaa on** command from the Global Configuration mode. Enter the command as follows:

   ```
   #configure terminal
   (config)#aaa on
   ```

2. Configure a RADIUS server for use with port authentication using the **radius-server host** <*ip address*> **key** <*key*> command from the Global Configuration mode. The <*ip address*> parameter refers to the IP address of the RADIUS server, and should be expressed in dotted decimal notation (for example, **10.10.10.1**). The <*key*> parameter is the preshared key that is used by the AOS product and the RADIUS server for authentication. Enter the command as follows:

   ```
   (config)#radius-server host 10.100.13.240 key adtran
   ```

3. Specify that AAA authentication uses port authentication (and vice versa) using the **aaa authentication port-auth default group radius [local | none]** command from the Global Configuration mode. This command specifies that AAA authentication relies on port authentication, and creates a default authentication list, which relies on the RADIUS server. The **local** and **none** parameters specify what authentication method is used if for some reason the RADIUS server is unavailable. The **local** parameter indicates that the local user list is used for authentication, and prevents a lock-out situation from occurring. If the **none** parameter is used, no additional authentication measures are taken if the RADIUS server is unavailable. Enter the command as follows:

   ```
   (config)#aaa authentication port-auth default group radius local
   ```

> NOTE *In certain cases, it is preferable to only define the RADIUS server, and not the local user list, to prevent users from accessing the network and its resources when the RADIUS server cannot be contacted. If this method is preferred, it is recommended to define multiple RADIUS servers in the event that the primary RADIUS server has a problem that cannot be readily corrected.*

> NOTE *If you are using a local user list for authentication, rather than a RADIUS server, you must enter the user names and passwords for the allowed users using the **username** <name> **password** <password> command from the Global Configuration mode. Enter the command for each user you want to add to the list.*

Configuring Port Authentication

After AAA has been enabled and configured, and the RADIUS server is set to use port authentication, you can begin to configure port authentication. To configure port authentication, follow these steps:

1. Specify the type of control port authorization will use on the interface using the **port-auth port-control [auto | force-authorized | force-unauthorized]** command. The **auto** parameter specifies that authorization relies on 802.1x for authorization. This type of port control causes the port to enter an unauthorized state immediately after the port becomes active, and it allows a successful 802.1x authentication process to change its state to authorized. The **force-authorized** parameter indicates that everyone attempting to access the port is allowed, without credentials. This type of port control forces the port into an authorized state when the port active. It is primarily used for connecting to other switches or devices that do not support 802.1x. The **force-unauthorized** parameter indicates that no one receives access to the port. This type of port control forces the port into an unauthorized state when the port is active. It is typically used when the port is never intended to be utilized but a system administrator wants to keep the port active for any reason. By default, this condition will still transmit broadcast and multicast frames. To specify the type of port control used in port authentication, enter the **port-auth port-control force-authorized**, **port-auth port-control force-unauthorized**, or **port-auth port-control auto** command from the interface's configuration mode. For example, to specify that the interface uses 802.1x authorization, enter the command as follows:

   ```
   (config)#interface switchport 0/8
   (config-swx 0/8)#port-auth port-control auto
   ```

   Using the **no** form of this command returns the port authentication port control to the default of **force-authorize**.

2. Next, you will specify whether port authentication is based on the port itself, on a MAC address of a device using the port, or on a voice VLAN of a device using the port. Port-based authentication specifies that the entire port is open to traffic when in an authorized state. This authentication method is compatible with every 802.1x client and authorizes the port to permit traffic flow after a single 802.1x client is authenticated. When using this type of port authentication, the port will immediately send an EAP identity request as soon as it becomes active. It will continue to send these requests periodically, even when it is active but in an unauthorized state. Once a device has been successfully authenticated, the port transitions to an authorized state and stops sending EAP identity requests. By default, this type of port authentication only allows the device that first authenticated to send traffic; however, this setting can be modified as described in Step 3 on *page 31*.

   MAC-based authentication specifies that the port is open for the specific MAC address that is authorized. This authentication method requires that the 802.1x client supports EAP start messages as is dictated by the IEEE 802.1x standard. When using this type of port authentication, the port enters an unauthorized state when it becomes active, but waits until it receives an EAP start message from the client wanting to connect before it begins the authentication process. The port then sends the EAP identity request to that specific client. Once the client is successfully authenticated, the port transitions to an authorized state for only the authorized client's MAC address.

Voice-based authentication is used when two authenticated devices are expected on the port. One device will be the voice device and the other will be a data device. Typically the voice device is authenticated using MAC authentication bypass (MAB). The data device will be authenticated via MAB or EAP**.**

To specify which type of authentication the interface uses, enter the **port-auth auth-mode [port-based | mac-based | voice-based]** command from the interface's configuration mode. For example, to specify that the interface uses port-based authentication, enter the command as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#port-auth auth-mode port-based
```

Using the **no** form of this command returns the port authentication mode to the default, which is port-based authentication.

3. If you selected port-based authentication, you can optionally specify that multiple hosts can use the port, even when only one device is authorized, using the **port-auth multiple-hosts** command from the interface's configuration mode. Enter the command as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#port-auth multiple-hosts
```

Using the **no** form of this command disables the multiple-host capability and only allows the authorized device to connect through the port.

4. If you selected port-based authentication, you can optionally specify the direction in which to block traffic when the port is unauthorized using the **port-auth control-direction [both | in]** command from the interface's configuration mode (if supported on your platform). The **both** parameter specifies that traffic is blocked in both directions when the port is unauthorized, and the **in** parameter specifies that only incoming traffic is blocked when the port is unauthorized. Enter the command as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#port-auth control-direction both
```

Using the **no** form of this command returns the blocked traffic direction to the default value of **both**.

5. If you selected port-based or voice-based authentication, you can optionally specify to allow MAC authentication bypass using the **port-auth auth-mode mac-auth-bypass** command from the interface's configuration mode (if supported by your platform). With MAC authentication bypass enabled, the port will authenticate with a RADIUS server using the source MAC address if 802.1x authentication times out. If a device connected to the port responds to 802.1x, MAC bypass will not be attempted. Enter the command as follows:

```
(config)#interface switchport 0/8
(config-swx 0/8)#port-auth auth-mode mac-auth-bypass
```

Using the **no** form of this command disables MAC authentication bypass.

Additional Global Port Authentication Settings

In addition to configuring port authentication on the interface, you can optionally configure certain port authentication parameters globally. These settings include the maximum number of identity requests, the authentication timeout period, and whether or not port authentication will automatically reauthenticate. These settings are all configured from the Global Configuration mode.

You can specify the maximum number of identity requests sent by port authentication before restarting the authentication process using the **port-auth max-req** <*number*> command. The <*number*> parameter specifies the maximum number of authentication requests, and by default is set to **2**. The valid range for requests is **1** to **10**. To specify the maximum number of identity requests, enter the command as follows:

```
(config)#port-auth max-req 3
```

You can specify port authentication timers using the **port-auth timeout quiet-period** <*value*>, **port-auth timeout re-authperiod** <*value*>, and **port-auth timeout tx-period** <*value*> commands. The **quiet-period** parameter specifies the amount of time the system waits before attempting another authentication after a failure has occurred. The valid range for this parameter is **1** to **65535** seconds, and by default is set to **60** seconds. The **re-authperiod** parameter specifies the amount of time between scheduled reauthentication attempts. Reauthentication attempt range is **1** to **4294967295** seconds, and by default is set to **3600** seconds. The **tx-period** parameter specifies the amount of time the authenticator waits between identity requests. The valid range for this parameter is **1** to **65535** seconds, and by default is set to **30** seconds. To globally configure the timers for port authentication, enter the commands as follows:

```
(config)#port-auth timeout quiet-period 120
(config)#port-auth timeout re-authperiod 4200
(config)#port-auth timeout tx-period 60
```

> NOTE *If the timeout periods are changed from their default values, the associated settings in the 802.1x supplicant might also need to be modified to match.*

You can also specify whether or not reauthentication is enabled for port authentication using the **port-auth re-authentication** command. By default, this command is disabled. To enable reauthentication, enter the command as follows:

```
(config)#port-auth re-authentication
```

Optional Guest VLAN Configuration

Guest VLAN allows devices that fail 802.1x authentication to be assigned to a predefined guest VLAN. For example, if a printer is plugged into a port and there is no RADIUS server to authenticate the new device or if RADIUS is not responding, the printer will be assigned to the guest VLAN and have network access granted to that VLAN.

> NOTE *Remember to allow the guest VLAN to have connectivity to any other necessary VLANs.*

> NOTE *Both the VLAN name and ID must be unique throughout the network. The name is limited to 32 alphanumeric characters. The VLAN ID can be any number from **1** to **4094**.*

To create a guest VLAN, use the **vlan** <*vlan id*> command from the Global Configuration mode. The <*vlan id*> parameter specifies the VLAN ID to assign to the VLAN. The following example creates VLAN **2** within the VLAN database:

```
(config)#vlan 2
(config-vlan 2)#
```

By default, the VLAN name is set to VLANxxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number. For example, the name VLAN 2 created in the example would default to VLAN0002. To assign a different name to the VLAN, use the **name** <*name*> command from the VLAN Configuration mode, where the <*name*> parameter specifies the name of the VLAN.The following example sets the name of VLAN 2 to **Guest**:

```
(config-vlan 2)#name Guest
```

To enable the guest VLAN on a port, use the **port-auth guest-vlan** <*vlan id*> command from the Switchport or Gigabit Switchport Interface Configuration mode. The <*vlan id*> specifies the ID number associated with the guest VLAN. The following example configures the Switchport interface 0/1 for guest VLAN **2**:

```
(config)#interface switchport 0/1
(config-swx 0/1)#port-auth guest-vlan 2
```

Configuration Examples

The following section describes different scenarios for configuring and applying the port access control features. The first set of examples applies to configuring port security, and includes a simple port security configuration, as well as two configurations for VLAN-aware port security. The second set of examples applies to configuring port protection, and the third set of examples applies to configuring port authentication. The last example shows a configuration using both port security and port authorization for situations in which the 802.1x protocol is not supported, but the port still needs to be secure. Each scenario is provided for example purposes only. Example configurations should be modified to fit your specific configuration needs.

Port Security Configuration Examples

The following configuration examples display the basic port security configurations, and include two VLAN-aware configurations.

Simple Port Security

The following example configures port security on Ethernet interface **0/23**, and specifies that port security is enabled, that the port is set to static access mode, and that the maximum number of allowed secure MAC addresses is set to **4**. In addition, the example specifies the following MAC address aging parameters: the aging time is set to **60** minutes, the aging type is **absolute**, and that static addresses are not aged. The action taken when a security violation occurs is to shut down the port, the port is set to expire in **120** minutes, MAC addresses are not saved to the running configuration, and the first MAC address allowed access is **00:00:01:00:00:01**.

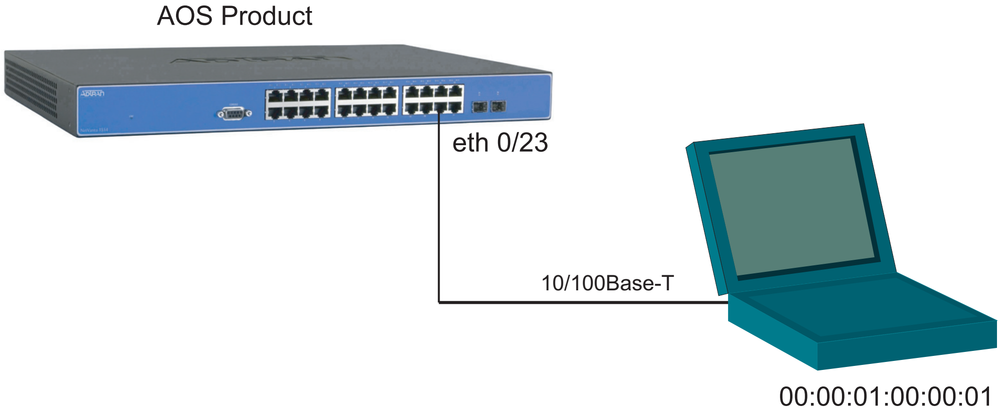
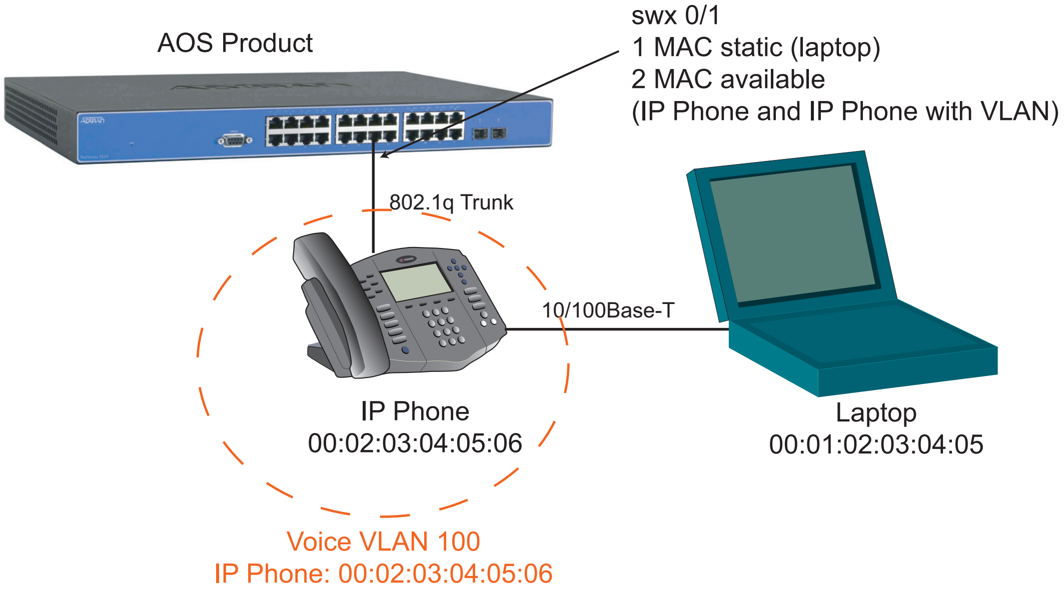


Figure 2. Simple Port Security Illustration

```
interface ethernet 0/23
    switchport port-security
    switchport port-security aging time 60
    switchport port-security aging type absolute
    no switchport port-security aging static
    switchport port-security maximum 4
    switchport port-security violation shutdown
    no switchport port-security mac-address sticky
    switchport port-security expire time 120
    switchport port-security expire type absolute
    switchport port-security mac-address 00:00:01:00:00:01
    switchport mode access
!
```

VLAN-Aware Port Security

In the following examples, port security is configured for a typical voice and data network using VLAN-aware port security (available in AOS firmware 17.09.01 or later). In this network, a PC is connected to an IP phone, which is in turn connected to an AOS switching product. The phone goes through a two-stage bootup process. In this configuration, the first MAC address learned by the port is the address of the native VLAN. After traffic is generated, the MAC address is associated with the configured VLAN. In this scenario, the voice VLAN is VLAN **100**, and the maximum number of dynamically learned MAC addresses is **3**.



NOTE *If no VLAN is specified, port security will automatically use the native VLAN.*

Figure 3. VLAN-Aware Port Security Illustration

In the first example, the switchport interface **0/1** is configured with a static laptop MAC address of **00:01:02:03:04:05**, and the interface is configured to learn two additional MAC addresses:

```
interface switchport 0/1
    spanning-tree edgeport
    no shutdown
    switchport port-security
    switchport port-security maximum 3
    switchport port-security mac-address 00:01:02:03:04:05
    switchport voice vlan 100
    switchport mode trunk
!
```

In the second example, the static computer MAC address is set to **00:01:02:03:04:05**, and two additional MAC addresses for the IP phone are specified. The IP phone's MAC address is **00:02:03:04:05:06**, and the next address entered is the phone's MAC address associated with the voice VLAN (**00:02:03:04:05:06 vlan 100**):

```
interface switchport 0/1
    spanning-tree edgeport
    no shutdown
    switchport port-security
    switchport port-security maximum 3
    switchport port-security mac-address 00:01:02:03:04:05
    switchport voice vlan 100
    switchport port-security mac-address 00:02:03:04:05:06
    switchport port-security mac-address 00:02:03:04:05:06 vlan 100
    switchport mode trunk
!
```

Port Protection Configuration Examples

In the following example, two ports are configured with port protection and one is configured without port protection. In this scenario, the protected ports can communicate with the unprotected port, but not with another protected port. All of the ports are in the default VLAN (VLAN 1). For example, if two servers (switchport interfaces **0/1** and **0/2**) have port protection enabled, but they cannot communicate with each other, they can both connect to the Internet by communicating with a router connected to a port that does not have port protection enabled (switchport interface **0/24**).

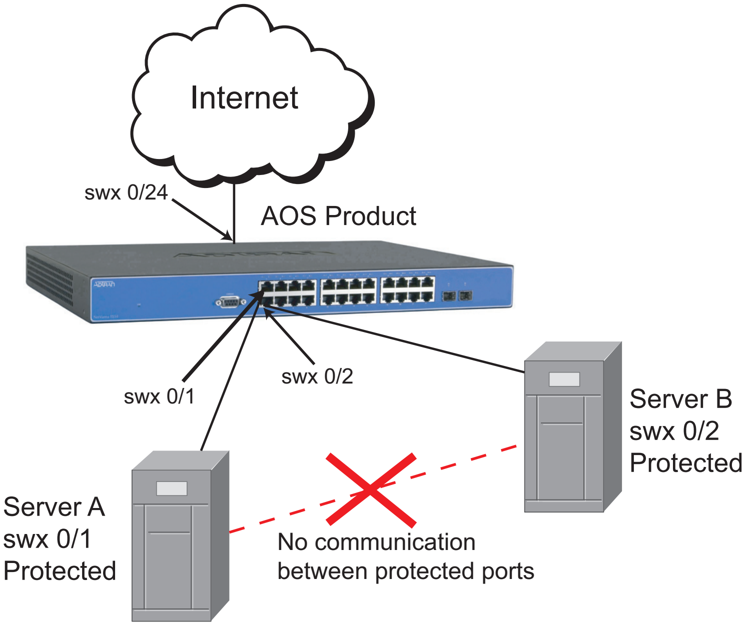


Figure 4. Port Protection Illustration

```
interface switchport 0/1
    switchport protected
    switchport mode access
!
interface switchport 0/2
    switchport protected
    switchport mode access
!
interface switchport 0/24
    switchport mode access
!
```

Port Authentication Configuration Examples

In the following example, the switchport interface **0/8** is configured with port authentication. This configuration includes the basic AAA and RADIUS server configuration, associating port authentication with the RADIUS server, and configuring port authentication on the switchport interface. The port authentication configuration specifies that multiple hosts are allowed on an authorized port, which receives its authentication based on the port. The port is configured to use 802.1x authentication (**auto** setting), and traffic is blocked in both directions when the port is unauthorized.

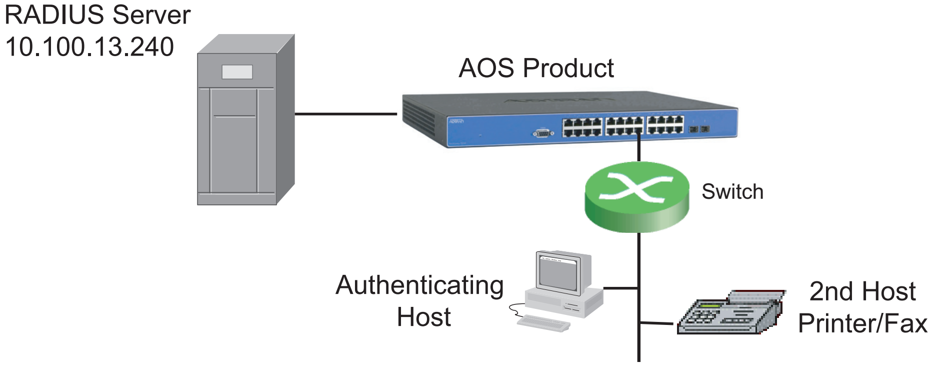


Figure 5. Port Authentication Illustration

```
aaa on
!
radius-server host 10.100.13.240 key adtran
!
aaa authentication port-auth default group radius local
!
interface switchport 0/8
    port-auth port-control auto
    port-auth control-direction both
    port-auth auth-mode port-based
    port-auth multiple-hosts
    switchport mode access
!
```

In the following example, an IP phone is used to connect a client computer to a NetVanta 1550 switch. The client computers traffic passes through the IP phone and uses 802.1x authentication with the switch to gain access to the network. It is placed on either a data VLAN or guest VLAN depending on the outcome of the authentication. The phone authenticates with the switch via MAB. *Figure 6* describes this network configuration, and the sample configuration below includes the relevant port authentication configuration.

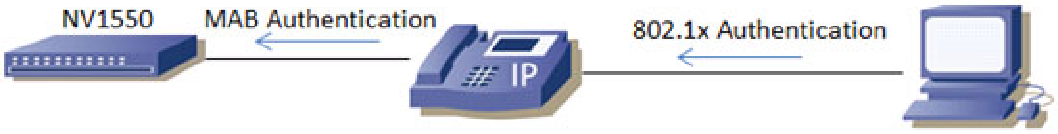


Figure 6. Voice Based Port Authentication Network Topology

```
!
interface gigabit-switchport 0/23
  no shutdown
  switchport voice vlan 10
  port-auth port-control auto
  port-auth auth-mode voice-based mac-auth-bypass
  port-auth guest-vlan 20
!
```

Command Summaries

The following tables summarize the configuration commands necessary for each of the port access control features: port security, port protection, and port authentication.

Table 1. Port Security Configuration Commands

Prompt	Command	Description
(config-interface <*interface*>)#	**[no] switchport port-security**	Enables port security on the interface. By default, port security is disabled. Using the **no** form of the command disables port security.
(config-interface <*interface*>)#	**[no] switchport mode access**	Places the port in static access mode. The port must be in static access mode for port security to function. Note that if you are using AOS firmware 17.09.01 or later, you do not need to specify that the port is in static access mode. You can begin configuring port security by enabling the feature on the interface.
(config-interface <*interface*>)#	**[no] switchport port-security aging [static | time** <*value*> **| type absolute]**	Specifies the aging time for stored secure MAC addresses. The **static** parameter applies the aging time to static MAC addresses. The **time** <*value*> parameter specifies the aging time in minutes. Range is **0** to **1440** minutes. A time value of **0** disables aging. The **type absolute** parameter specifies that the timeout occurs regardless of outside conditions. By default, the aging time is set to **0**, **static** is disabled, and aging type is set to **absolute**.
(config-interface <*interface*>)#	**[no] switchport port-security expire [time** <*value*> **| type absolute]**	Specifies the port expiration time and type. The **time** <*value*> parameter specifies the expiration time in minutes. Range is **0** to **43200** minutes. A time value of **0** disables port expiration. The **type absolute** parameter specifies that the timeout occurs regardless of outside conditions. By default, the expiration time is set to **0**.

Table 1. Port Security Configuration Commands ***(Continued)***

Prompt	Command	Description
(config-interface <*interface*>)#	**[no] switchport port-security maximum** <*number*>	Specifies the maximum number of secure MAC addresses allowed to access the port. Valid range is **1** to **132**. By default, **1** secure MAC address is allowed.
(config-interface <*interface*>)#	**[no] switchport port-security mac-address** <*mac address*> **[vlan** <*vlan id*>**]**	Manually enters a secure MAC address. Enter MAC addresses in the following format: xx:xx:xx:xx:xx:xx. The **vlan** <*vlan id*> parameter associates the specified VLAN with the secure MAC address. This option is available only in units running AOS firmware 17.09.01 or later. The valid VLAN ID range is **1** to **4094**. By default, no MAC addresses are given access to the port.
(config-interface <*interface*>)#	**[no] switchport port-security mac-address sticky [**<*mac address*> **| sticky-volatile] [vlan** <*vlan id*>**]**	Specifies that dynamically learned MAC addresses are saved to the running configuration, and if the configuration is saved, they are kept across a unit reboot. Entering a MAC address specifies that only that MAC address is saved. The **sticky-volatile** parameter specifies that addresses are kept only for the current session. The **vlan** <*vlan id*> parameter associates the specified VLAN with the secure MAC address. This option is available only in units running AOS firmware 17.09.01 or later. The valid VLAN ID range is **1** to **4094**. By default, sticky MAC addresses are disabled.

Table 1. Port Security Configuration Commands *(Continued)*

Prompt	Command	Description
(config-interface <*interface*>)#	**[no] switchport port-security violation [protect | restrict | shutdown]**	Specifies the action taken when a security violation is detected. The **protect** parameter places the interface in a protected state, the **restrict** parameter restricts traffic flow, and **shutdown** shuts down the interface. By default, the interface shuts down when a security violation is detected.
(config-interface <*interface*>)#	**no shutdown**	Returns the interface to an active state after it has been shut down due to a security violation.

Table 2. Port Protection Configuration Commands

Prompt	Command	Description
(config-interface <*interface*>)#	**[no] switchport protected**	Specifies that the interface port is in protected mode. Using the **no** form of this command places the interface port in unprotected mode. By default, ports are unprotected.
(config-interface <*interface*>)#	**[no] switchport mode access**	Places the port in static access mode. The port must be in static access mode for port protection to function.

Table 3. Port Authentication Configuration Commands

Prompt	Command	Description
(config)#	**[no] aaa on**	Enables AAA services for use with port authentication. By default, AAA services are disabled.

Table 3. Port Authentication Configuration Commands ***(Continued)***

Prompt	Command	Description
(config)#	**[no] radius-server host** *<ip address>* **key** *<key>*	Configures a RADIUS server for use with port authentication. IP addresses should be expressed in dotted decimal notation, for example: **10.10.10.1**. The **key** parameter is the preshared key used by the AOS product and the RADIUS server for authentication. By default, no RADIUS server is configured.
(config)#	**[no] aaa authentication port-auth default group radius [local | none]**	Specifies that AAA services use port authentication, and links the port authentication feature to the RADIUS server. Using the **local** parameter specifies that if the RADIUS server is unavailable, a local user list is used to authenticate access to the port. Using the **none** parameter specifies that if the RADIUS server is unavailable, the port is inaccessible. By default, AAA services do not use port authentication for authentication.
(config-interface *<interface>*)#	**[no] port-auth port-control [auto | force-authorized | force-unauthorized]**	Specifies the type of port control for port authentication. The **auto** parameter specifies that the port relies on 802.1x authentication. The **force-authorized** parameter places the port into an authorized state when the port is active. The **force-unauthorized** parameter places the port into an unauthorized state when the port is active. By default, port control is set to **force-authorize**.

Table 3. Port Authentication Configuration Commands *(Continued)*

Prompt	Command	Description
(config-interface <*interface*>)#	**[no] port-auth auth-mode [mac-based | port-based | voice-based]**	Specifies the authentication method for port authentication. The **mac-based** parameter specifies that the port is only open to a specific MAC address when in an authorized state. The **port-based** parameter specifies that authentication occurs based on the port, and it specifies that the entire port is open to traffic when in an authorized state. The **voice-based** parameter specifies that authentication occurs on the port for the voice VLAN. By default, **port-based** authentication is used.
(config-interface <*interface*>)#	**[no] port-auth multiple-hosts**	Specifies that when a port is in **port-based** authentication mode, multiple devices can access the port even when only one device is authorized. By default, only one authorized device can use the port.
(config-interface <*interface*>)#	**[no] port-auth control-direction [both | in]**	Specifies that when a port is in **port-based** authentication mode, and the port is in an unauthorized state, traffic flow direction can be controlled. The **both** parameter indicates that both directions of traffic flow are suspended. The **in** parameter indicates that only incoming traffic is suspended. By default, both directions of traffic are suspended.
(config-interface <*interface*>)#	**[no] port-auth auth-mode port-based mac-auth-bypass**	Specifies that if 802.1x authentication times out, the port will authenticate with a RADIUS server using the source MAC address. If the device connected to the port responds to 802.1x, MAC bypass will not be attempted.

Table 3. Port Authentication Configuration Commands *(Continued)*

Prompt	Command	Description
(config)#	**port-auth max-req** *<number>*	Specifies the maximum number of identity requests transmitted before restarting the authentication process. The valid range is **1** to **10**. By default, the maximum number of request is set to **2**.
(config)#	**port-auth timeout quiet-period** *<value>*	Specifies the amount of time the system will wait before attempting another authentication once a failure has occurred. The valid range is **1** to **65535** seconds, and by default is set to **60** seconds.
(config)#	**port-auth timeout re-authperiod** *<value>*	Specifies the amount of time between scheduled reauthentication attempts. The valid range is **1** to **4294967295** seconds. By default, the reauthentication period is set to **3600** seconds.
(config)#	**port-auth tx-period** *<value>*	Specifies the amount of time the authenticator waits between identity requests. The valid range is **1** to **65335** seconds. By default, the wait time is set to **30** seconds.
(config)#	**[no] port-auth re-authentication**	Enables reauthentication for port authentication. By default, this command is disabled.
(config-interface)#	**[no] port-auth guest-vlan** *<vlan id>*	Configures guest VLAN for an interface. By default, this command is disabled.

Troubleshooting

There are two methods for troubleshooting port access control features. Troubleshooting can be done from either the GUI or the CLI. Both methods reveal feature statistics and information specific to the configuration of port security, port protection, and port authentication. Both methods are described in the following sections.

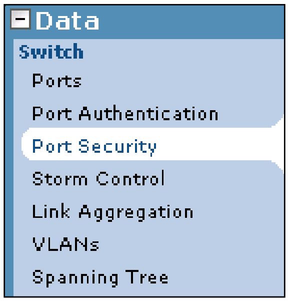
Viewing Port Access Control Statistics Using the GUI

Certain statistics for port security and port authentication are available on the GUI. The GUI provides summary statistics that aid in monitoring the activity of the port access control features.

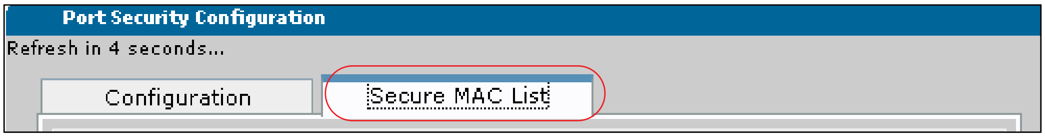
Viewing Port Security Statistics

To view port security statistics using the GUI, follow these steps:

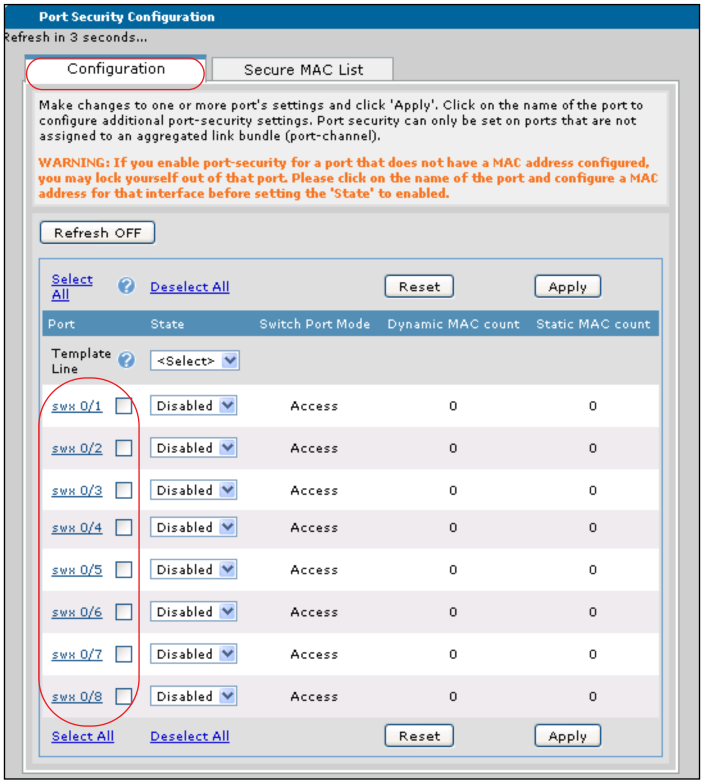
1. Navigate to **Data** > **Port Security**.



2. To view all of the secure MAC addresses associated with port security, select the **Secure MAC List** tab in the **Port Security Configuration** menu. The MAC list contains the VLAN associations, MAC address, MAC address type (static or dynamic), and the remaining time before the entry expires for all secure MAC addresses.



3. To view the secure MAC list for a single interface, select the interface from the list in the **Configuration** tab of the **Port Security Configuration** menu.

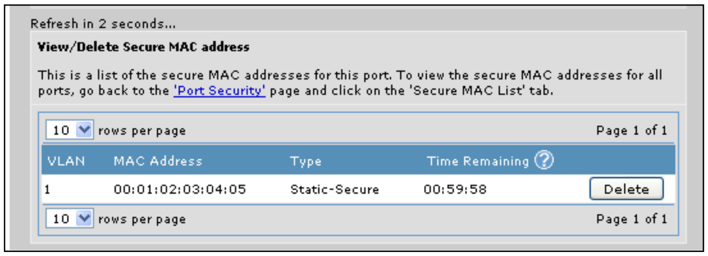


Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port-security settings. Port security can only be set on ports that are not assigned to an aggregated link bundle (port-channel).

WARNING: If you enable port-security for a port that does not have a MAC address configured, you may lock yourself out of that port. Please click on the name of the port and configure a MAC address for that interface before setting the 'State' to enabled.

Port		State	Switch Port Mode	Dynamic MAC count	Static MAC count
Template Line		<Select>			
swx 0/1	☐	Disabled	Access	0	0
swx 0/2	☐	Disabled	Access	0	0
swx 0/3	☐	Disabled	Access	0	0
swx 0/4	☐	Disabled	Access	0	0
swx 0/5	☐	Disabled	Access	0	0
swx 0/6	☐	Disabled	Access	0	0
swx 0/7	☐	Disabled	Access	0	0
swx 0/8	☐	Disabled	Access	0	0

4. The secure MAC list for the interface is displayed at the bottom of the **Add a Secure MAC Address** menu. This list contains the same information as the **Secure MAC List**, however, the information is for a single interface only.



View/Delete Secure MAC address

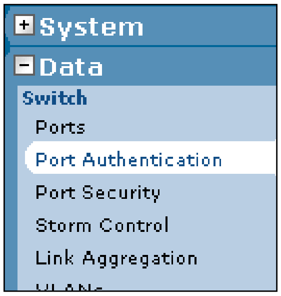
This is a list of the secure MAC addresses for this port. To view the secure MAC addresses for all ports, go back to the 'Port Security' page and click on the 'Secure MAC List' tab.

VLAN	MAC Address	Type	Time Remaining	
1	00:01:02:03:04:05	Static-Secure	00:59:58	Delete

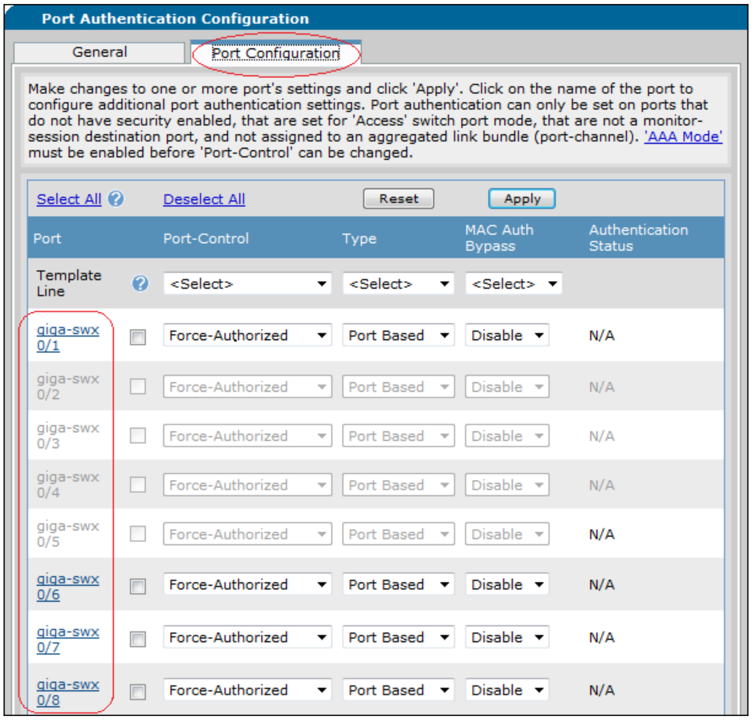
Viewing Port Authentication Statistics

To view port authentication statistics using the GUI, follow these steps:

1. Navigate to **Data** > **Port Authentication**.



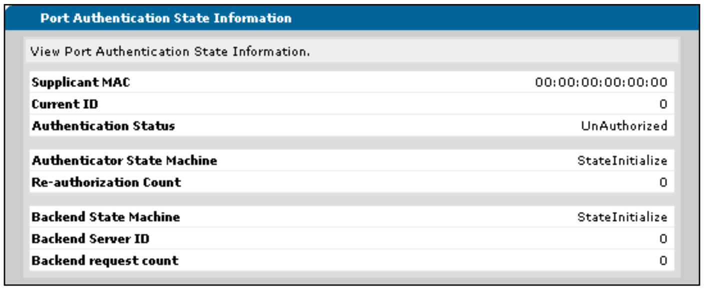
2. Select the **Port Configuration** tab in the **Port Authentication Configuration** menu and select the interface you want to view from the list.



Make changes to one or more port's settings and click 'Apply'. Click on the name of the port to configure additional port authentication settings. Port authentication can only be set on ports that do not have security enabled, that are set for 'Access' switch port mode, that are not a monitor-session destination port, and not assigned to an aggregated link bundle (port-channel). 'AAA Mode' must be enabled before 'Port-Control' can be changed.

Port		Port-Control	Type	MAC Auth Bypass	Authentication Status
Template Line		<Select>	<Select>	<Select>	
giga-swx 0/1	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/2	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/3	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/4	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/5	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/6	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/7	□	Force-Authorized	Port Based	Disable	N/A
giga-swx 0/8	□	Force-Authorized	Port Based	Disable	N/A

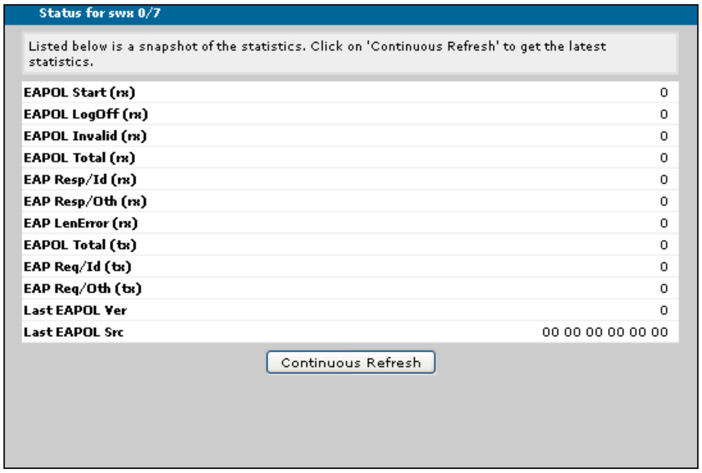
3. The next menu contains a **Port Authentication State Information** section that displays port authentication information. This menu includes the supplicant MAC address, the current ID of the port, the authentication status of the port, and other pertinent information.



View Port Authentication State Information.

Supplicant MAC	00:00:00:00:00:00
Current ID	0
Authentication Status	UnAuthorized
Authenticator State Machine	StateInitialize
Re-authorization Count	0
Backend State Machine	StateInitialize
Backend Server ID	0
Backend request count	0

This menu also includes a **Status** section for the interface, which includes EAP and EAPOL information for the port.



Status for swx 0/7

Listed below is a snapshot of the statistics. Click on 'Continuous Refresh' to get the latest statistics.

EAPOL Start (rx)	0
EAPOL LogOff (rx)	0
EAPOL Invalid (rx)	0
EAPOL Total (rx)	0
EAP Resp/Id (rx)	0
EAP Resp/Oth (rx)	0
EAP LenError (rx)	0
EAPOL Total (tx)	0
EAP Req/Id (tx)	0
EAP Req/Oth (tx)	0
Last EAPOL Ver	0
Last EAPOL Src	00 00 00 00 00 00

Viewing Port Access Control Statistics Using the CLI

Port security, port protection, and port authentication statistics can also be viewed using the CLI. These statistics are displayed using various **show** commands and are outlined in the following table.

Table 4. Port Access Control Show Commands

Prompt	Command	Description
#	**show port-security**	Displays port security configuration information for all interfaces with port security configured.
#	**show port-security address**	Displays the secure MAC addresses for all interfaces with port security configured.
#	**show port-security interface** *<interface>* **[address]**	Displays the port security configuration information for the specified interface. The **address** parameter displays the secure MAC addresses for the specified interface.
#	**show port-security port-expiration [detailed]**	Displays the port security port expiration information. The optional **detailed** parameter includes more detailed information in the output.
#	**show running-config interface** *<interface>* **[verbose]**	Displays configuration information for the specified interface. This output includes whether the port is in a protected or unprotected state. The optional **verbose** parameter displays the complete interface configuration, including hidden default commands.
#	**show port-auth [detailed]**	Displays port authentication information for all interfaces with port authentication configured. The optional **detailed** parameter includes more detailed information in the output.

Table 4. Port Access Control Show Commands *(Continued)*

Prompt	Command	Description
#	**show port-auth [detailed] interface** *<interface>*	Displays port authentication information for the specified interface. The optional **detailed** parameter includes more detailed information in the output.
#	**show port-auth statistics [interface** *<interface>***]**	Displays port authentication statistics for all interfaces with port authentication configured or only the specified interface.
#	**show port-auth summary [interface** *<interface>***]**	Displays port authentication configuration summaries for all interfaces with port authentication configured or only the specified interface.
#	**show port-auth supplicant [interface** *<interface>* **| summary]**	Displays supplicant information for all interfaces with port authentication configured, or only the specified interface. The **summary** keyword specifies that a summary of the information is displayed.

The following is sample output from a few of the port access control **show** commands. All **show** commands are entered from the Enable mode prompt, and if an interface is specified, it is specified in the format *<interface type [slot/port | slot/port.subinterface id]>*. For example, to specify an Ethernet interface, use **eth 0/1**.

To display the secure MAC addresses for a single interface, enter the **show port-security interface** *<interface>* **address** command as follows:

```
>enable
#show port-security interface eth 0/1 address
VLAN   Mac Address         Type of Entry      Interface    Remaining Time
------------------------------------------------------------------------------------------------------------------------
1      00:a0:c8:0a:c6:4a   Dynamic-Secure     eth 0/1      --
1      00:a0:c8:0a:c6:4b   Dynamic-Secure     eth 0/1      --
------------------------------------------------------------------------------------------------------------------------
Dynamic Address Count: 2
Static Address Count: 0
Sticky Address Count: 0
Total Address Count: 2
```

To display the port security configuration for a single interface, enter the **show port-security interface** *<interface>* command as follows:

```
>enable
#show port-security interface eth 0/23
Port Security: Enabled
Violation Action: Shutdown
Maximum Secure MAC addresses: 4
Dynamic Secure MAC addresses: 2
```

```
Static Secure MAC addresses: 1
Sticky secure MAC addresses: 0
Aging Time: 0 mins
Aging Type: Absolute
Expire Time: 0 mins
Expire Type: Absolute
Static Address Aging: Disabled
Sticky Address Learning: Disabled
Security Violation Count: 0
```

To display the configured port authentication information for the AOS unit, enter the **show port-auth** command as follows:

```
>enable
#show port-auth
Global Port-Authentication Parameters:
   re-authentication enabled: False
   reauth-period: 3600
   quiet-period: 60
   tx-period: 30
   supp-timeout: 30
   server-timeout: 30
   reauth-max: 2
Port-Authentication Port Summary:
  Interface    Status      Type          Mode   Authorized
 -------------------------------------------------------------------------------------
  eth 0/1      disabled    port-based    n/a    n/a
  eth 0/2      disabled    port-based    n/a    n/a
  eth 0/3      disabled    port-based    n/a    n/a
  eth 0/4      disabled    port-based    n/a    n/a
  eth 0/5      disabled    port-based    n/a    n/a
  eth 0/6      disabled    port-based    n/a    n/a
  eth 0/7      disabled    port-based    n/a    n/a
  eth 0/8      disabled    port-based    n/a    n/a
  eth 0/9      disabled    port-based    n/a    n/a
  eth 0/10     disabled    port-based    n/a    n/a
  eth 0/11     disabled    port-based    n/a    n/a
  eth 0/12     disabled    port-based    n/a    n/a
  eth 0/13     disabled    port-based    n/a    n/a
  eth 0/14     disabled    port-based    n/a    n/a
  eth 0/15     disabled    port-based    n/a    n/a
  eth 0/16     disabled    port-based    n/a    n/a
  eth 0/17     disabled    port-based    n/a    n/a
  eth 0/18     disabled    port-based    n/a    n/a
  eth 0/19     disabled    port-based    n/a    n/a
  eth 0/20     disabled    port-based    n/a    n/a
  eth 0/21     disabled    port-based    n/a    n/a
Port Authentication Port Details:
  Port-Authentication is disabled on eth 0/1
```

Port-Authentication is disabled on eth 0/2

You can also see the port authentication information for a specific interface by entering the **show port-auth statistics interface** <*interface*> command. For example:

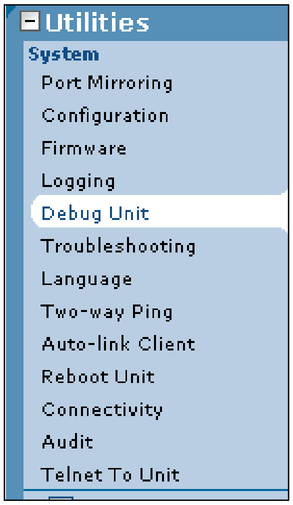
>enable
#show port-auth statistics interface giga-swx 0/1

```
giga-swx 0/1:
  Rx: EAPOL       EAPOL     EAPOL      EAPOL    EAP        EAP         EAP
      Start       LogOff    Invalid    Total    Resp/Id    Resp/Oth    LenError
      0           0         0          0        0          0           0

      Last        Last
      EAPOLVer    EAPOLSrc
      0           00:00:00:00:00:00

  Tx: EAPOL       EAP       EAP
      Total       Req/Id    Req/oth
      2           0         0
```

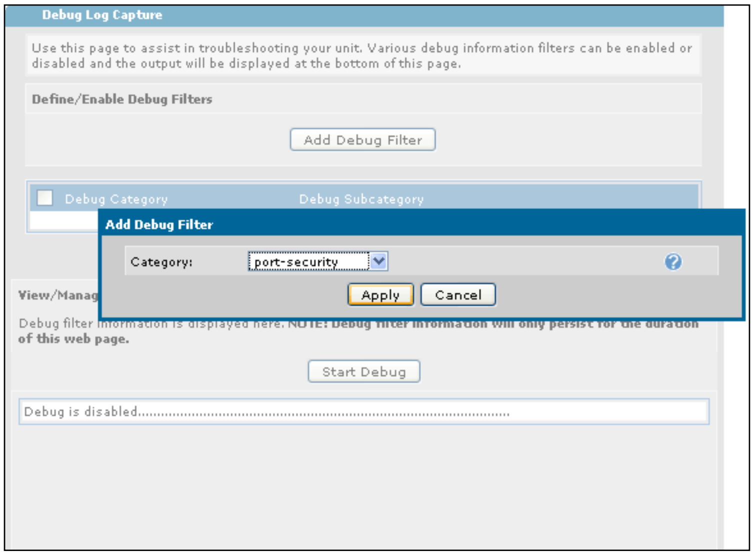
Troubleshooting Using the GUI

To activate debug messages for port security or port authentication using the GUI, follow these steps:

1. Navigate to **Utilities** > **System** > **Debug Unit**.



2. Select the **Add Debug Filter** button and choose the desired item to debug from the following **Category** drop-down list. Select **Apply** when the correct item is chosen. The item you choose will appear in the **Debug Category** tab in the middle of the menu.



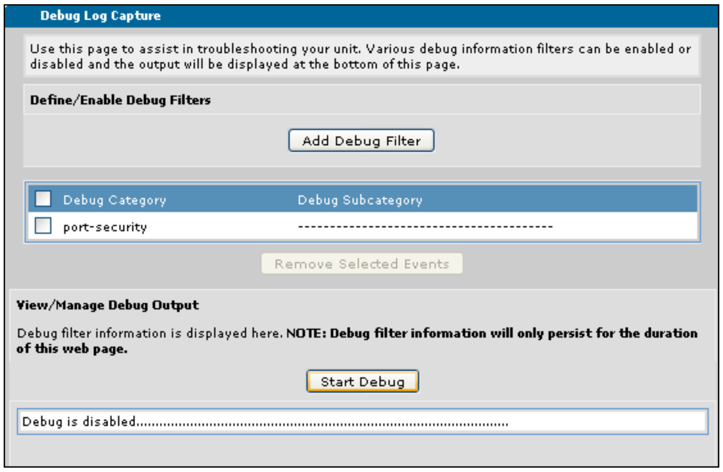
Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

Category: port-security

Debug filter information is displayed here. NOTE: Debug filter information will only persist for the duration of this web page.

Debug is disabled...

3. Select **Start Debug** and begin receiving debug information for the item you selected.



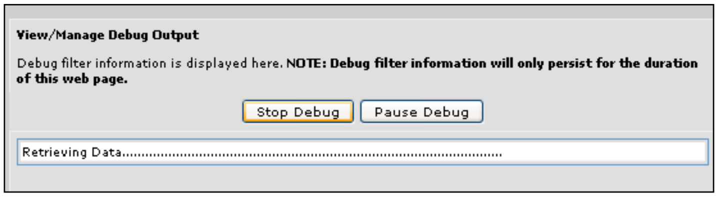
Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

□ Debug Category	Debug Subcategory
□ port-security	--

Debug filter information is displayed here. **NOTE: Debug filter information will only persist for the duration of this web page.**

Debug is disabled...

4. To turn off debug capabilities, select **Stop Debug** from the **View/Manage Debug Output** menu.



Debug filter information is displayed here. **NOTE: Debug filter information will only persist for the duration of this web page.**

Retrieving Data...

Troubleshooting Using the CLI

After configuring port security or port authentication, several **debug** commands can be issued from the Enable mode in the CLI to assist in troubleshooting. The **debug** commands send messages when certain types of activity are detected in the configuration, and they work hand-in-hand with the **show** commands to verify proper configuration and performance. Both the port security and port authentication **debug** commands are detailed in the following table.

Table 5. Port Security and Port Authentication Debug Command Summary

Prompt	Command	Description
#	**debug port-security**	Enables debug event messages for all port security configurations.
#	**debug port-auth**	Enables debug event messages for all port authentication configurations.
#	**debug port-auth auth-sm**	Enables debug event messages associated with the Auth PAE-state machine.
#	**debug port-auth bkend-sm**	Enables debug event messages associated with the backend-state machine.
#	**debug port-auth general**	Displays configuration changes to the port authentication system.
#	**debug port-auth packet [both | tx | rx]**	Displays packet exchange information. The **both** parameter displays information about both received and transmitted packets. The **tx** parameter displays only transmitted packet information, and the **rx** parameter displays only received packet information.
#	**debug port-auth reauth-sm**	Enables debug event messages associated with the reauthentication-state machine.
#	**debug port-auth supp-sm**	Enables debug event messages associated with the supplicant-state machine.
#	**debug port-auth voice**	Enables debug event messages associated with voice-based port authentication.

By enabling **debug** commands, debug messages are sent to alert you whenever specified actions take place. These messages can be beneficial when you are troubleshooting your configuration. You can also enter the **no** version of any of the above commands to disable debug reporting, or you can enter **undebug all** from the Enable mode prompt to disable all debug reporting.

NOTE *Using **debug** commands can be very processor intensive, and should be used with caution.*

Sample Debug Output

The following is a sample of debug output from the **debug port-auth** command. Each **debug** command is entered from the Enable mode prompt. The following output shows a successful user authentication attempt.

```
#debug port-auth
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.PACKET RX Rcvd EAP Resp for sess 11 on int swx 0/11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in RESPONSE state
2007.09.11 11:55:30 PORT_AUTH.GENERAL Init auth with server for sess 11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Sent EAP Resp/Id to AuthServer for sess 11
on int swx 0/11
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.GENERAL Rcvd response from server for sess 11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in SUCCESS state
2007.09.11 11:55:30 PORT_AUTH.PACKET TX Sent EAP Success for sess 11 on int swx
0/11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in IDLE state
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.AUTHSM Int swx 0/11 sess 11 in AUTHENTICATED state
; sess is authorized
```

Clearing Port Security Statistics Using the CLI

In addition to **show** and **debug** commands, the CLI also provides a method of clearing the counters associated with port security using the **clear** commands. These commands are described in the following table.

Table 6. Port Security Clear Command Summary

Prompt	Command	Description
#	**clear port-security dynamic [address** *<mac address>* **| interface** *<interface>***]**	Clears the dynamic MAC addresses for a specific MAC address or for a specific interface. Interfaces are specified in the format *<interface type [slot/port | slot/port.subinterface id]>*. For example, to specify an Ethernet interface, use **eth 0/1**. MAC addresses are specified in the following format: xx:xx:xx:xx:xx:xx.

Table 6. Port Security Clear Command Summary *(Continued)*

Prompt	Command	Description
#	**clear port-security sticky [address** *<mac address>* **| interface** *<interface>***]**	Clears the sticky secure MAC addresses for a specific MAC address or for a specific interface. Interfaces are specified in the format *<interface type [slot/port | slot/port.subinterface id]>*. For example, to specify an Ethernet interface, use **eth 0/1**. MAC addresses are specified in the following format: xx:xx:xx:xx:xx:xx.
#	**clear port-security violation-count** *<interface>*	Clears the security violation count associated with a particular interface. Interfaces are specified in the format *<interface type [slot/port | slot/port.subinterface id]>*. For example, to specify an Ethernet interface, use **eth 0/1**.

To use a clear command, enter the command from the Enable mode prompt as follows:

```
#clear port-security sticky address 00:01:02:03:04:05
```

Additional Resources

The following table outlines additional documentation that might be helpful to you in configuring various parts of the port control access suite. These documents are all available online at https://supportforums.adtran.com.

Table 7. Additional Documentation

Document Title
Configuring RADIUS Authentication for Port Authentication and Dynamic VLAN Assignment
Configuring 802.1X in AOS
Configuring AAA in AOS