Creating MAC Access Control Lists Using the Web-Based GUI and AOS CLI

Quick Configuration Guide

61700412E1-42.1B



Media access control (MAC) access control lists (ACLs) allow tighter security in wireless networks by blocking unwanted computer or device connections. The MAC ACL is a common filtering option, based on source MAC addresses, that only allows specified devices to access the network. MAC ACLs are applicable to ADTRAN Operating System (AOS) products that support wireless traffic. A MAC ACL can be created by entering the MAC address for each computer or device that you want to allow access through either the command line interface (CLI) or Web-based graphical user interface (GUI). The CLI provides direct interaction with your unit through a text-based user interface, and the GUI provides direct interaction with your unit through a Web-based user interface.



MAC ACLs are used as packet selectors by the wireless features. By themselves, the MAC ACLs do nothing. AOS provides only standard MAC ACLs that match based on the source of the packet.

Creating a MAC ACL Using the GUI

The GUI is an online configuration tool that allows you to easily configure and view system settings, as well as the status of your AOS product.



If restrictions in your network prevent you from accessing the GUI, proceed to **Creating a** *MAC ACL Using the CLI* on page 7.

To create a MAC ACL using the GUI, follow these steps:

- 1. Open a new page in your Web browser.
- 2. Type your unit's IP address in the browser's address field in the following form:

http://<ip address>



The IP address may also be entered in **https:**// if your unit has **ip http secure-server** enabled.

3. At the prompt, enter your user name and password and select **OK**.



4. Navigate to **Data > Wireless > MAC Access List** on the left of the GUI menu as seen below:

🗉 Data 📃	
Switch	MAC Access Control Lists
Ports	
Port Authentication	Use the 'Add' button to create a MAC ACL, Existing ACL(s) can be deleted using the 'Delete MAC ACL' button. To add more MAC addresses to a particular ACL, click the appropriate link below.
Port Security	
Storm Control	WARNING: Deleting or modifying an existing MAC ACL(s) could affect network traffic.
Link Aggregation	Add
VLANs	
Spanning Tree	MAC ACL Name
MAC Forwarding	There are no MAC access lists configured.
Class Of Service	Delete MAC ACI
Stacking	
Router / Bridge	
Detault Gateway	
Routing	
ID Interfaces	
Loophack Interfaces	
GRE Tuppels	
OoS Wizard	
QoS Mans	
Bridaina	
UDP Relay	
Demand Routing	
VRRP	
Firewall	
Firewall Wizard	
Firewall / ACLs	
Security Zones	
Wireless	
AC/AP	
Radios / VAPs	
Clients	1
MAC Access List	
AP Firmware	

5. Select Add to add a MAC ACL.

6. Enter the MAC ACL Name and the source MAC Address in the appropriate fields.

Please enter information requested to create a new MAC ACL. 'Delete ACL Entry' button. To add more MAC addresses to a p below. WARNING: Deleting or modifying an existing ACL(s) could affe	Each ACL entries can be deleted using the articular ACL, click the appropriate link MAC ct network traffic.
MAC ACL Name:	The name to uniquely identify Nan this ACL.
MAC Address: : : : : : : : : : : : : : : : : : :	Set the source Media Access Control address to permit.
Apply	
MAC ACL Name ACL Type M	MAC Address MAC
There are no MAC access list	configured. Addr
Delete ACL Entry	



All MAC ACLs are case sensitive. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx (for example, 00:A0:C8:00:00:01).

7. Select Apply to create the MAC ACL.

Add MAC Access Control Lists	
Please enter information requested to create a new MAC ACL. Each AC 'Delete ACL Entry' button. To add more MAC addresses to a particular below.	L entries can be deleted using the ACL, click the appropriate link
WARNING: Deleting or modifying an existing ACL(s) could affect netwo	rk traffic.
MAC ACL Name: allowadtrn	The name to uniquely identify this ACL.
MAC Address: 00 : A0 : c8 : 00 : 00 : 01	Set the source Media Access Control address to permit.
Apply	
MAC ACL Name ACL Type MAC Add	ress
There are no MAC access list configure	ed.
Delete ACL Entry	

8. The new MAC ACL will appear on the bottom portion of the menu.

	Add MAC Access Control Lists			
	Please enter information reques 'Delete ACL Entry' button. To a below.	ted to create a new MA dd more MAC addresse	C ACL. Each ACL s to a particular A	entries can be deleted using the CL, click the appropriate link
	WARNING: Deleting or modifyin	g an existing ACL(s) c	ould affect network	<traffic.< td=""></traffic.<>
	MAC ACL Name:			The name to uniquely identify this ACL.
	MAC Address::			Set the source Media Access Control address to permit.
		Арр	y .	
New	MAC ACL Name	ACL Type	MAC Addr	ess
MAC	allowadtrn	Permit	00:A0:C8:	:00:00:01
ACL		Delete AC	L Entry	

9. To add additional source MAC addresses to the MAC ACL, select the MAC ACL name from the bottom of the menu (allowadtrn). The MAC ACL name appears in the MAC ACL Name field (allowadtrn) and you enter the additional MAC address you want to give access to your network in the MAC Address field and select Apply. You can add as many new addresses to the MAC ACL as you need by repeating these steps.

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below. WARNING: Deleting or modifying an existing ACL(s) could affect network traffic. MAC ACL Name: allowadtrn The name to uniquely identify this ACL. MAC Address: 00 ; A0 ; C8 ; 00 ; 00 ; 02 Set the source Media Access Control address to permit.	
WARNING: Deleting or modifying an existing ACL(s) could affect network traffic. MAC ACL Name: allowadtrn The name to uniquely identify this ACL. MAC Address: 00 : A0 : C8 : 00 : 00 : 02 Set the source Media Access Control address to permit.	
MAC ACL Name: allowadtrn The name to uniquely identify this ACL. MAC Address: 00 : A0 : C8 : 00 : 00 : 02 Set the source Media Access Control address to permit.	
MAC Address: 00 : A0 : C8 : 00 : 00 : 02 Set the source Media Access Control address to permit.	
Apply	
MAC ACL Name ACL Type MAC Address	Second
allowadtrn Permit 00:A0:C8:00:00:01	address fo
Delete ACL Entry	allowadtr

10. Configuration of the MAC ACL is complete. You can make additional changes to each MAC ACL by selecting its hyperlink.

11. To delete an address from a MAC ACL (in this case, the MAC ACL **allowadtrn**), check the box next to the MAC address you want to delete and select the **Delete ACL Entry** button on the bottom of the menu. This step only deletes an address from the MAC ACL, not the entire ACL.

Add M	IAC Access Control Lists			
Please 'Delete below.	enter information reques ACL Entry' button. To ac	ted to create a new M Id more MAC address	AC ACL. Each AC ses to a particular /	L entries can be deleted using the ACL, click the appropriate link
WARNI	NG: Deleting or modifyin	g an existing ACL(s)	could affect networ	′k traffic.
MA	AC ACL Name:			The name to uniquely identify this ACL.
	MAC Address:;		:	Set the source Media Access Control address to permit.
		Ар	ply	
	MAC ACL Name	ACL Type	MAC Addi	ress
	<u>allowadtrn</u>	Permit	00:A0:C8	3:00:00:01
	allowadtrn	Permit	00:A0:C8	3:00:00:02
		Delete A	CL Entry	

Note Deleting MAC ACL entries will only delete the selected MAC address entries in the ACL, not the MAC ACL itself.

12. To delete an entire MAC ACL, return to the main MAC ACL menu by selecting **MAC Access** List from the menu on the left.

Wireless
AC/AP
Radios / VAPs
Clients
MAC Access List
AP Firmware

13. Check the box next to the MAC ACL you want to delete (allowadtrn), and select Delete MAC ACL.

MAC Access (Control Lists
Use the 'Add' b button. To add	outton to create a MAC ACL. Existing ACL(s) can be deleted using the 'Delete MAC ACL' more MAC addresses to a particular ACL, click the appropriate link below.
WARNING: De	leting or modifying an existing MAC ACL(s) could affect network traffic.
	Add
V	MAC ACL Name
	allowadtrn
	Delete MAC ACL

14. Once the MAC ACL is configured, it must be applied to the radio. To apply the ACL to the radio, navigate to **Wireless** > **APs/Radios/VAPs** and select the access point (AP) ID from the list.

Wireless Settings			
Access Points	Radios	Virtual Acces	s Points
Add an Access Point Use the button below to a	add a new Access Point.	lew AP	
Modify/Delete Access Po Select a link below to vie	ints w or modify an AP or sel	ect a box to rem	nove an AP.
Access Point ID	MAC Address	Location	Control Status
dot11ap 2	00 A0 C8 00 00 00		N/A
	Remove S	elected ADs	

15. After selecting the appropriate AP ID, select the MAC ACL you want to apply to the radio from the drop-down menu.

Access Point Config	uration	
Access Point Interface:	2	Access Point number range is 1-24 .
Name:	AP2	Alphanumeric string to be used as a unique name for the Access Point.
Location:		Alphanumeric string for the location of this Access Point. (optional)
MAC Address:	00 : A0 : C8 : 00 : 00 : 00	MAC address of the Access Point's ethernet interface.
Speed/Duplex:	AUTO	Specifies the speed and duplex of the Access Point's ethernet interface.
Country/Region:	United States 💌	Specifies the country in which the Access Point is being operated.
MAC Access List:	None	Associate this AP to a specific MAC Access List. To create MAC Access Lists go to the <u>'MAC ACL'</u> page.

- 16. After selecting the MAC ACL, apply it to the radio using the **Apply** button at the bottom of the menu. The ACL is now applied to the radio.
- 17. You can save your configuration (recommended) and exit the GUI using the **Save** and **Logout** links (at the upper right of your current menu).

Creating a MAC ACL Using the CLI

As a text-based user interface, the AOS CLI prompts you to input commands line by line when you interface with your AOS product. To create a MAC ACL through the CLI, follow these steps:

- 1. Boot up the unit.
- 2. Telnet to the unit:

telnet <ip address>

For example, **telnet 208.61.209.1**

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



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. Enable your unit by entering **enable** at the > prompt as follows:

>enable

- 5. Enter your Enable mode password at the prompt.
- 6. Enter the Global Configuration mode by entering the following command at the **#** prompt:

#configure terminal

7. From the Global Configuration mode prompt, enter the **mac access-list standard** command followed by the MAC ACL name. In the following example, a MAC ACL name **Allowadtrn** will be created.

(config)#**mac access-list standard Allowadtrn** (config-std-mac-acl)#

 You have now entered the Standard MAC Access List Configuration mode. Here you can enter the MAC addresses to be included in the MAC ACL that will allow other devices to connect to your network. To give access to a specific MAC address, enter the permit command followed by the MAC address. Enter addresses in the following format: xx:xx:xx:xx:xx:xx. For example:

(config-std-mac-acl)# **permit 00:A0:C8:00:00:01** (config-std-mac-acl)#

Enter each address to add to the specified MAC ACL. Address entries can be removed from the list by using the **no** parameter in the following manner:

(config-std-mac-acl)#no permit 00:A0:C8:00:00:01

To exit the Standard MAC Access List Configuration mode, enter the **exit** keyword at the prompt. For example:

(config-std-mac-acl)#**exit** (config)#

From the Global Configuration mode, entire MAC ACLs can be deleted by using the **no** parameter of the **mac access-list standard** command followed by the MAC ACL name. For example:

(config)#no mac access-list standard Allowadtrn

9. The MAC ACL has been created, and you should save the configuration. Multiple MAC ACLs can be created by using the same process, either through the GUI or CLI.

10. After creating and saving the MAC ACL, it must be applied to the radio. To apply the ACL, use the **association access-list** *<name>* command from the radio interface configuration mode (reached by using the **interface dot11ap** command). For example:

(config)#interface dot11ap 1 ap-type nv150 (config)#association access-list Allowadtrn

11. Save your configuration using the **do write memory** command from the Global Configuration mode prompt as follows:

(config)#do write memory

Troubleshooting Note

If unwanted clients or devices have connected to the wireless access point (AP) radio before the MAC ACL has been applied, the AP radio must be rebooted for the applied MAC ACL to filter out the unwanted client. To reboot the AP, follow the steps outlined in the following sections.

Rebooting the AP Using the GUI

To reboot the AP radio using the GUI, follow these steps:

1. Navigate to **Data > Wireless > AP Firmware** in the menu on the left.

🗖 Data	Apply Access Point Firmware
Switch	Select the Firmware and Access Boint to upgrade. Verify the upgrade with the Upload Status
Ports	Select die Fininware and Access Point to apgrade. Veniy die apgrade with the Optoad Status.
Port Authentication	Firmware Image to send to
Port Security	the Access Point.
Storm Control	Specify Access Point to
Link Aggregation	Access Point: 1 receive the image.
VLANs	
Spanning Tree	Upload Status:Ready for Upload
MAC Forwarding	
Class Of Service	Cancel Apply
Stacking	
Router / Bridge	
Default Gateway	Access Point Firmware Upgrade
Routing	Browse or enter the firmware file to upload to the Access Controller. Then, apply the firmware above to
Route table	the Access Point.
IP Interfaces	Firmware images have a img
Loopback Interfaces	Upload Firmware: Browse extension.
GRE Tunnels	
QoS Wizard	Cancel Upload
Qos maps Bridaina	
UDP Relav	Delete Firmware
Demand Routing	Te sudante velo de su francesa una esta de delses alder unationet esta sub-
VRRP	system. Select firmware file to delete from your Access Controller and click 'Delete.'
Firewall	
Firewall Wizard	Delete Firmware: Select the firmware image to delete
Firewall / ACLs	mage to beece.
Security Zones	Cancel Delete
Wireless	
AC / AP Discovery	D-bash Assess D-bah
APs / Radios / VAPs	Redoot Access Point
Clients	Select the Access Point to reboot.
MAC Access List	
AP Firmware	Access Point: 1 💙 Specify Access Point to reboot.
YPN	
VPN Wizard	Reboot Factory Default and Reboot

2. Select the Access Point number to reboot from the drop-down menu.

Bridging	
UDP Relay	Delete Firmware
Demand Routing	In order to upload new firmware, you may need to delete older versions to make room on the file
VRRP	system. Select firmware file to delete from your Access Controller and click 'Delete.'
Firewall	
Firewall Wizard	Delete Firmware: Select the firmware image to delete.
Firewall / ACLs	
Security Zones	Cancel Delete
Wireless	
AC / AP Discovery	Pahaat Arcare Daint
APs / Radios / VAPs	Rebout Access Polit
Clients	Select the Access Point to reboot.
MAC Access List	
AP Firmware	Access Point: 1 🔮 Specify Access Point to reboot.
VPN	
VPN Wizard	2 pot Factory Default and Reboot
VPN Peers	4
Certificates	
Network Monitor	
Wizard	
Probes / Tracks	
Probe Responder	
URL Filtering	
URL Filters	
l op Websites	

3. Select the **Reboot** button. The unit will take approximately 60 seconds to reboot, so traffic will be disrupted during this period.

AC / AP Discovery	
APs / Radios / VAPs	Reboot Access Point
Clients	Select the Access Point to reboot.
MAC Access List	
AP Firmware	Access Point: 🚺 😪 Specify Access Point to reboot.
VPN	
VPN Wizard	Reboot Factory Default and Reboot
VPN Peers	
Certificates	
Network Monitor	

Rebooting the AP Using the CLI

To reboot the AP using the CLI, use the following steps:

1. To reboot the unit while saving the current configuration, enter the following command from the enable prompt:

#reload dot11 interface dot11ap <number>

The <number> parameter is used to specify the AP to reboot.