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.

> **NOTE**
> *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.

> **NOTE**
> *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>

> **NOTE**
> *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:
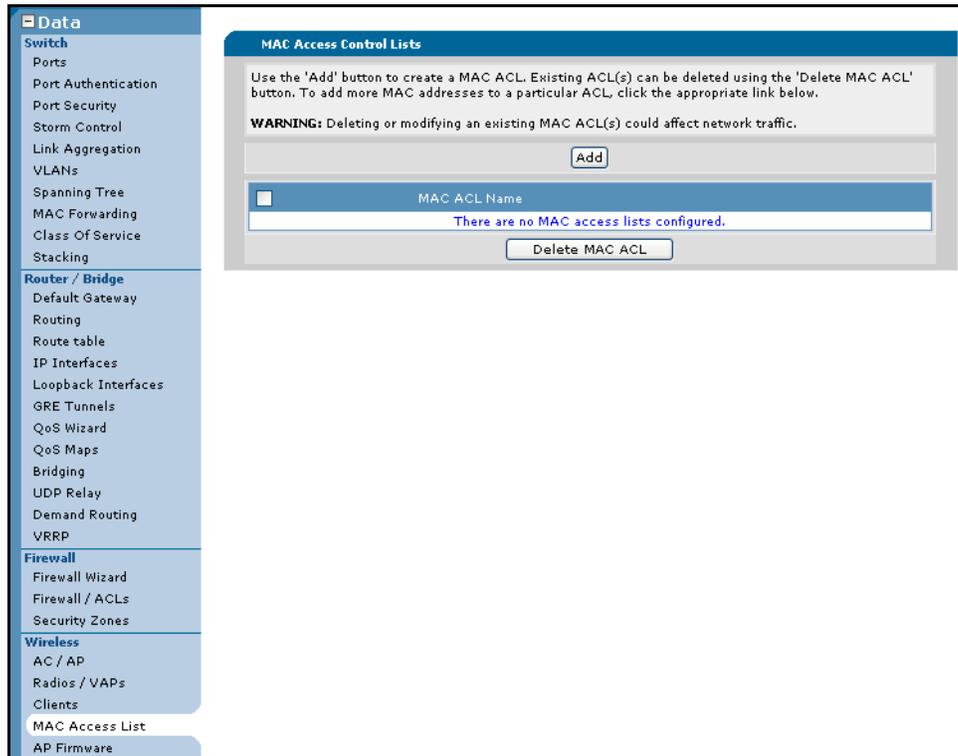
5. Select **Add** to add a MAC ACL.

Copyright © 2009 ADTRAN, Inc.

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

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

7. Select **Apply** to create the MAC ACL.

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

New
MAC
ACL

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.

Second
MAC
address for
allowadtrn
MAC ACL.

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.

> *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.
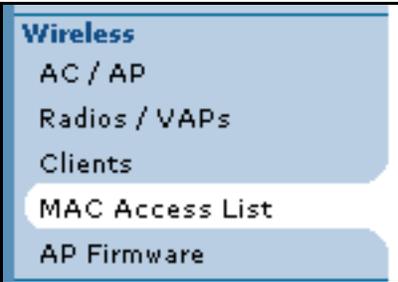
13. Check the box next to the MAC ACL you want to delete (**allowadtrn**), and select **Delete MAC ACL**.
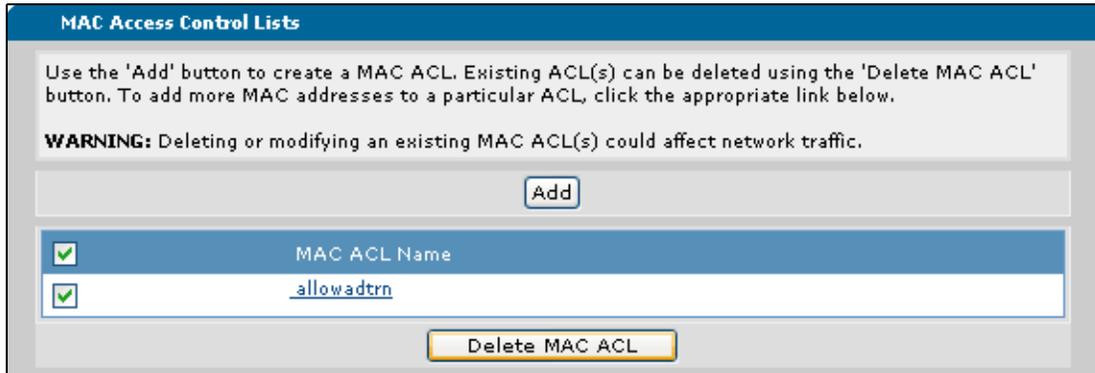
14. Once the MAC ACL is configured, it must be applied to the radio. To apply the ACL to the radio, navigate to **Wireless** > **APs/Radios/VAPs** and select the access point (AP) ID from the list.
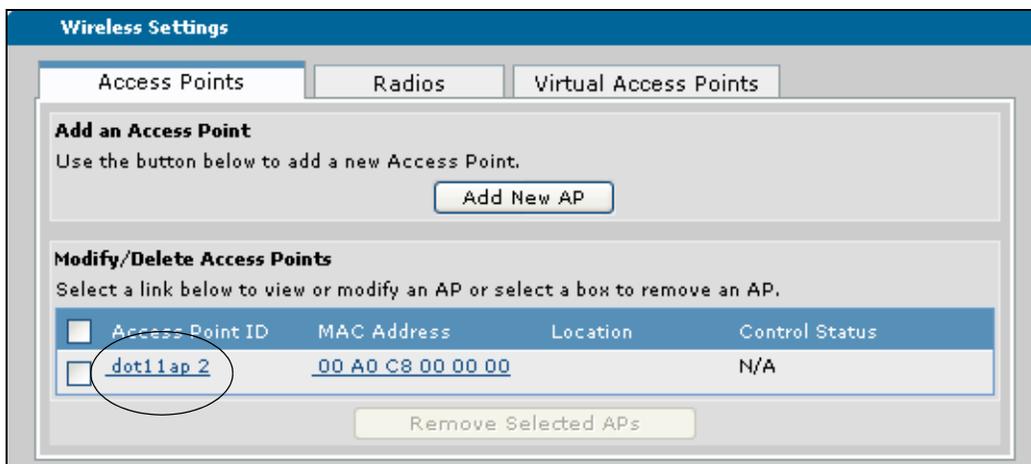
15. After selecting the appropriate AP ID, select the MAC ACL you want to apply to the radio from the drop-down menu.

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)#

8. 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.

---

2. Select the **Access Point** number to reboot from the drop-down menu.
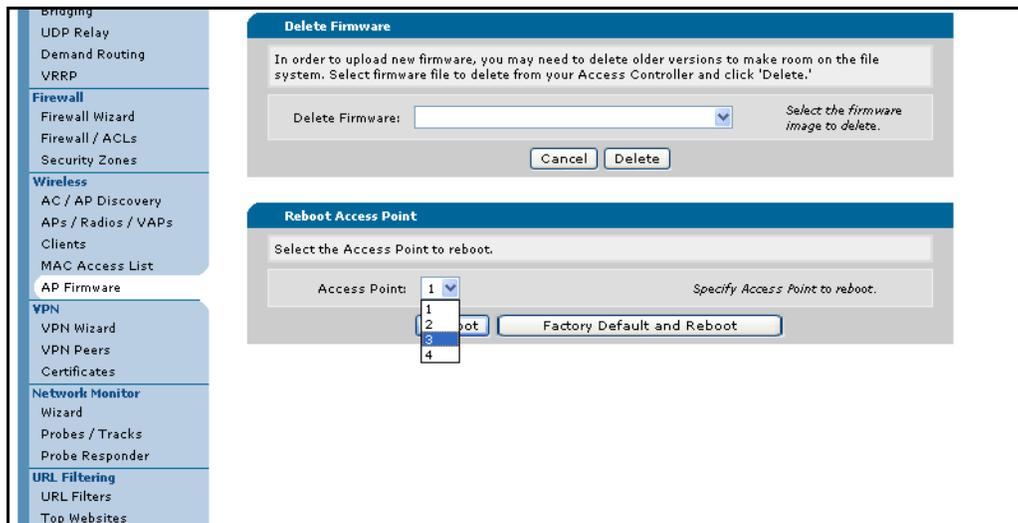
3. Select the **Reboot** button. The unit will take approximately 60 seconds to reboot, so traffic will be disrupted during this period.
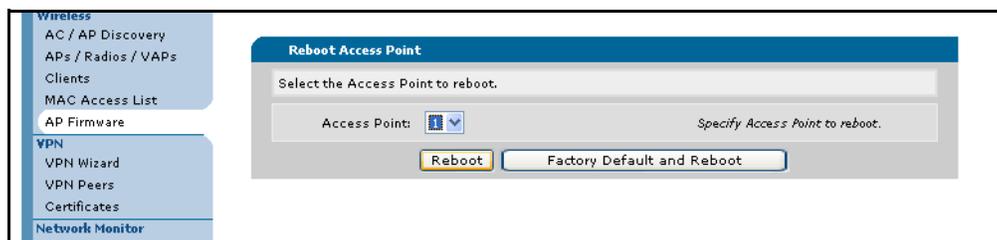
Rebooting the AP Using the CLI

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.