Configure IPv6 Access Control List (ACL) on the WAP125

Objective

Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Access Control Lists (ACLs) are a set of rules applied to packets received by the Wireless Access Point (WAP). Each rule is used to determine whether access to the network should be permitted or denied. The ACLs can be configured to inspect fields of a frame like the source or destination IP address, the Virtual Local Area Network (VLAN) Identifier (ID), or the Class of Service (CoS). When a frame enters the WAP device port, it inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

Configuring ACLs is commonly used to authorize access to network resources. In a corporate setting, the ones granted access to the resources to select devices in the network are typically managers, or the ones authorized to access the resources. This makes the resource server more efficient, and makes the network more secure.

This article aims to show you how to configure an IPv6 ACL on a WAP125 access point.

Note: In this example, all traffic from select host with the IP address 2001:DB8::22:F673:FF3B:AC99/10 will be allowed to access the network. All other traffic from other hosts will be denied.

Applicable Devices

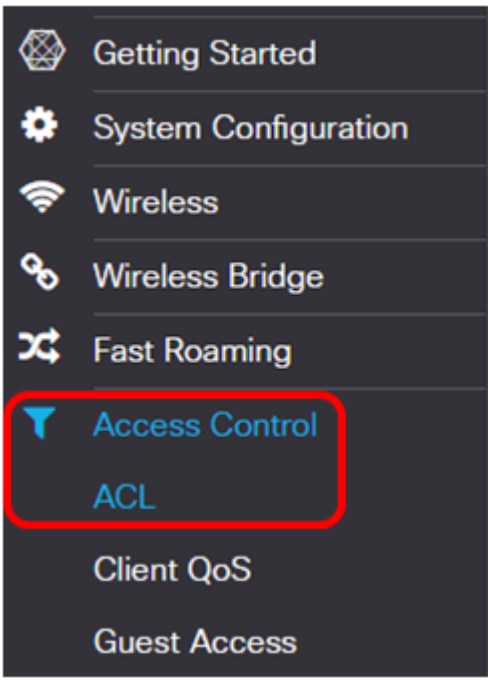
- WAP125

Software Version

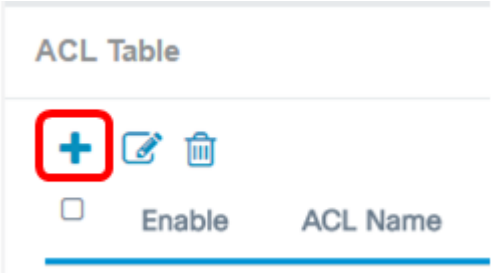
- 1.0.0.3

Configure an IPv6 ACL

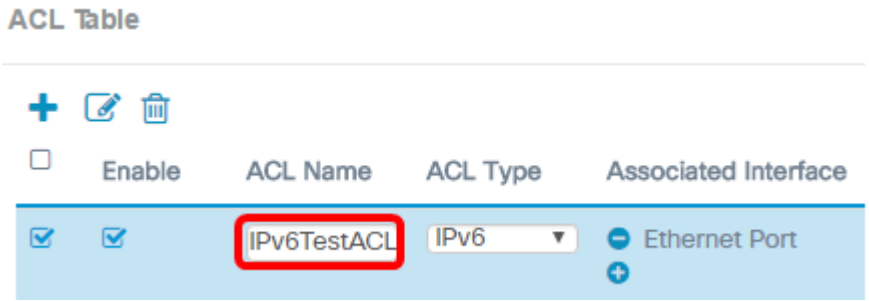
Step 1. Log in to the web-based utility of the WAP125 and choose **Access Control > ACL**.



Step 2. Click the button to add an ACL.

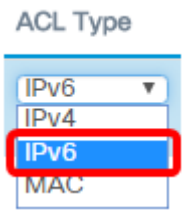


Step 3. Enter a name for the ACL in the *ACL Name* field.



Note: In this example, IPv6TestACL is entered.

Step 4. Choose IPv6 from the ACL Type drop-down list.

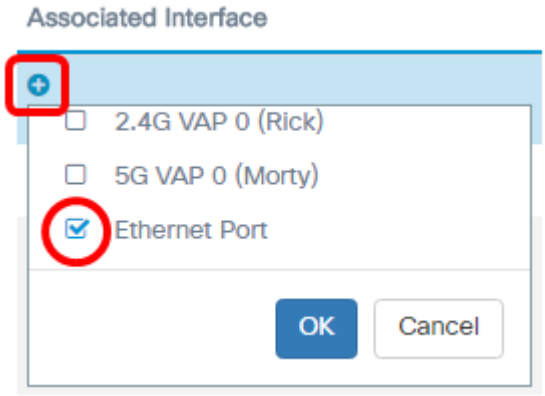


Step 5. Click the button and choose an interface from the Associated Interface drop-down list. The options are:

- 2.4G VAP 0 (SSID Name) — This option will apply the MAC ACL to the 2.4 GHz Virtual

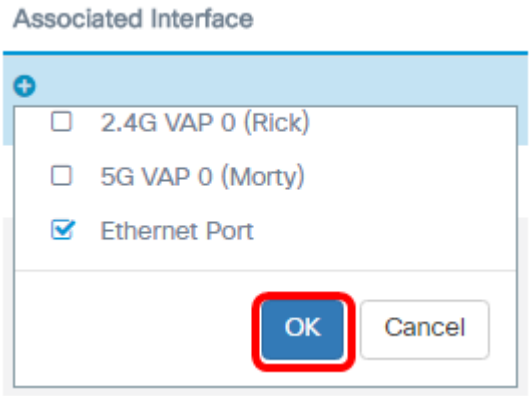
Access Point (VAP). The SSID Name section may change depending on the SSID name configured on the WAP.

- 5G VAP 0 (SSID Name) — This option will apply the MAC ACL to the 5 GHz VAP.
- Ethernet Port — This option will apply the MAC ACL to the Ethernet interface of the WAP.

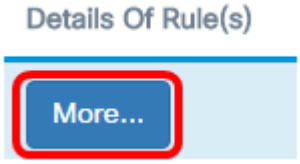


Note: Multiple interfaces can be associated to an ACL. However, it cannot be associated to another ACL when it has already been associated to an ACL. In this example, Ethernet Port is being associated to IPv6TestACL. Uncheck the box to disassociate the interface from the ACL.

Step 6. Click **OK**.



Step 7. Click the **More…** button to configure the parameters of the ACL.

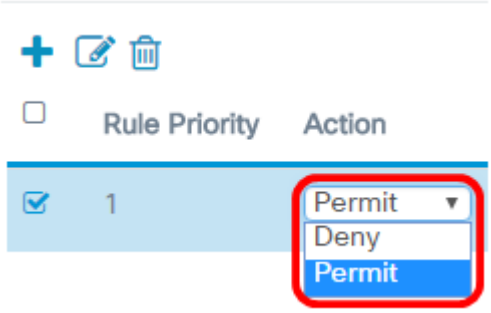


Step 8. Click the + button to add a new rule.

Step 9. Choose an action from the Action drop-down list. The options are:

- Permit — This option will allow packets that match the ACL criteria to connect to the network.

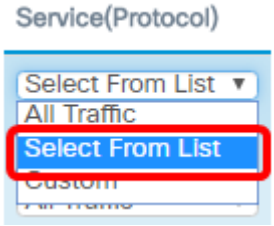
- Deny — This option will prevent packets that match the ACL criteria from connecting to the network.



Note: In this example, Permit is chosen.

Step 10. Choose a service or protocol to be filtered from the Service (Protocol) drop-down list. The options are:

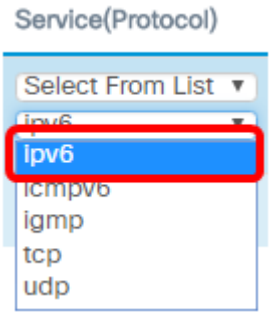
- All Traffic — This option will treat all packets as a match to the ACL filter.
- Select From List — This option will allow you to choose ipv6, icmpv6, igmp, tcp, or udp as filters for the ACL. If this option is chosen, proceed to Step 11.
- Custom — This option will allow you to enter a custom protocol identifier as a filter for the packets. The value is a four-digit hexadecimal number. The range is 0 to 255.



Note: In this example, Select From List is chosen.

Step 11. Choose a protocol from the Service(Protocol) drop-down list. The options are:

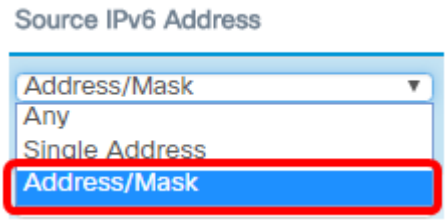
- ipv6 — This option will let the access point filter the hosts accessing the network using their IPv6 address as the filter.
- icmpv6 — This option will let the access point filter Internet Control Message Protocol version 6 (ICMPv6) packets entering the network through the access point.
- igmp — This option will let the access point filter Internet Group Management Protocol (IGMP) packets entering the network through the access point.
- tcp — This option will let the access point filter Transmission Control Protocol (TCP) packets entering the network through the access point.
- udp — This option will let the access point filter User Datagram Protocol (UDP) packets entering the network through the access point.



Note: In this example, ipv6 is chosen.

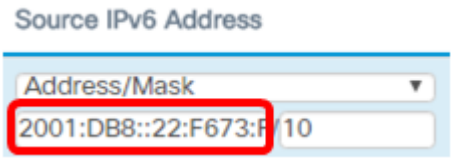
Step 12. Define the Source IPv6 Address from the Source IPv6 Address drop-down list. The options are:

- Any — This option will let the WAP apply the filter to packets from any IP address.
- Single Address — This option will let the WAP apply the filter to packets from a specified IP address.
- Address/Mask — This option will let the WAP apply the filter to packets to an IP address and the mask of the IP.



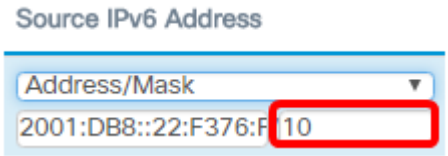
Note: In this example, Address/Mask is chosen.

Step 13. Enter the source IPv6 address in the *Source IPv6 Address* field.



Note: In this example, 2001:DB8::22:F673:FF3B:AC20 is entered.

Step 14. Enter the IPv6 mask in the *mask* field.



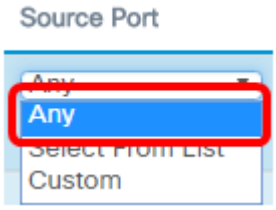
Note: In this example, 10 is entered.

Step 15. Choose a source port for the condition. The options are:

- Any — This option will allow all packets from the source port that meets the criteria.
- Select From List — This option allows you to choose ftp, ftp data, http, smtp, snmp, telnet, tftp, and www.
- Custom — This option will allow you to enter an IANA port number to match the source

port identified in the datagram header. The port range is from 0 to 65535 and includes the following:

- 0 to 1023 — Well known ports
- 1024 — 49151 — Registered ports.
- 49152 — 65535 — Dynamic and/or private ports



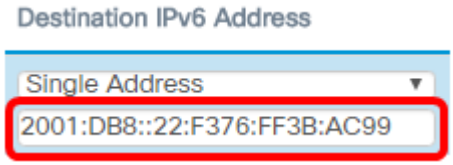
Note: In this example, Any is chosen.

Step 16. Choose a destination address from the Destination IPv6 Address drop-down list. The options are:

- Any — This option treats any IP address as a match to the ACL statement.
- Single Address — This option lets you enter a specific IP address for the ACL condition.
- Address/Mask — This option lets you enter an IP address range.

Note: In this example, Single Address is chosen.

Step 17. Enter the destination IPv6 address in the *Destination IPv6 Address* field.

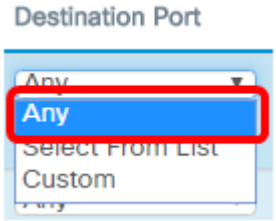


Note: In this example, 2001:DB8::22:F376:FF3B:AC99 is entered.

Step 18. Choose a destination port from the Destination Port drop-down list. The options are:

- Any — This option treats all of the destination ports of the packets as a match to the statement in the ACL.
- Select From List — This option lets you choose a keyword associated with the destination port to match. The options are: ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www. These keywords translate to their corresponding port numbers.
- Custom — This option will allow you to enter an IANA port number to match the source port identified in the datagram header. The port range is from 0 to 65535 and includes the following:
- 0 to 1023 — Well known ports
- 1024 — 49151 — Registered ports.

- 49152 — 65535 — Dynamic and/ or private ports



Note: In this example, Any is chosen.

Step 19. Choose an IPv6 flow label from the Flow Label drop-down list. This specifies a 20-bit number unique to an IPv6 packet. The options are:

- Any — This option specifies any 20-bit number.
- DSCP Value — This option matches the packets based on their custom DSCP value. When choosing this option, enter a value from 0 to 63 in the DSCP Value field.

Note: In this example, Any is chosen.

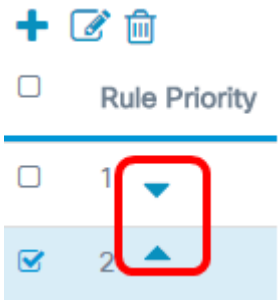
Step 20. Choose a Differentiated Services Code Point (DSCP) setting from the DSCP drop-down list. The options are:

- Any — This option treats any type of service as a match.
- Select From List — This option allows you to choose a DSCP filter from the DSCP list. The choices will depend on the DSCP configuration.
- Custom — This option lets you enter a custom DSCP value from 0 to 63.

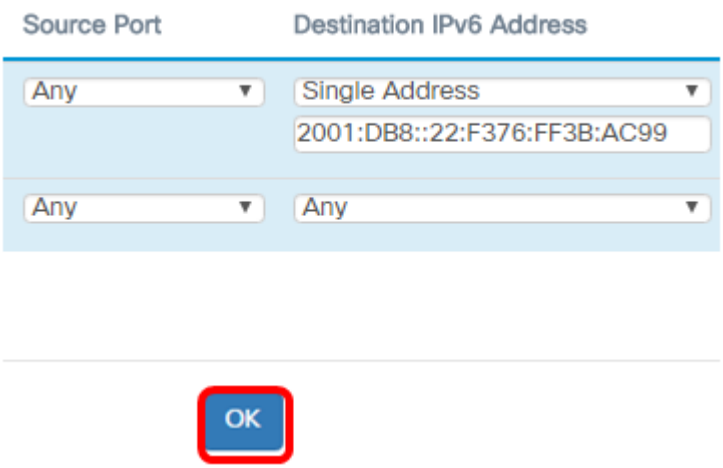
Note: In this example, Any is chosen.

Step 21. (Optional) Repeat Step 8 to Step 20 until the ACL is complete.

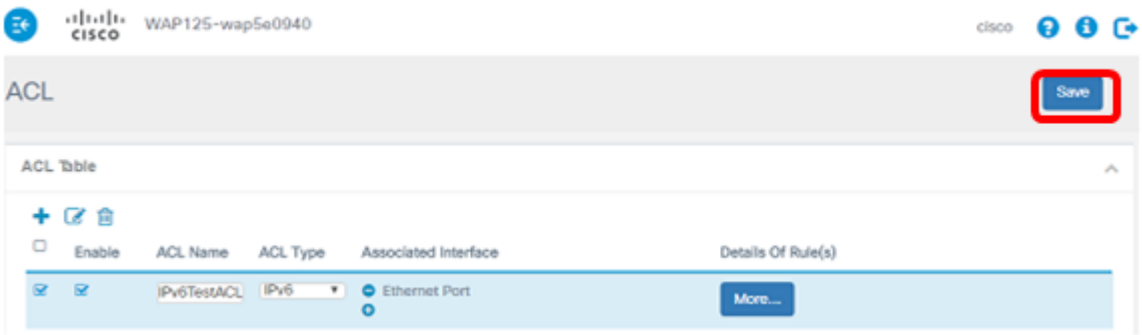
Step 22. (Optional) Change the order of the conditions on the ACL by clicking the up and down buttons until they are in the correct order.



Step 23. Click **OK**.



Step 24. Click **Save**.



You should now have completed the IPv6 ACL on the WAP125 access point.