Access Control

This chapter describes how to configure the ACL and the quality of service (QoS) feature on the WAP device. It contains the following topics:

ACL

Access Control Lists (ACLs) are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.

The WAP device supports up to 50 IPv4, IPv6, and MAC ACLs and up to 10 rules in each ACL. Each ACL supports multiple interfaces.

IPv4 and IPv6 ACLs

Each ACL is a set of rules applied to traffic received by the WAP device. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one or more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet. The IP ACLs classify traffic for Layers 3 and 4.

Note There is an implicit deny at the end of every rule created. To avoid denying all, we strongly recommend that you add a permit rule to the ACL to allow traffic.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect fields of a frame such as the source or destination MAC address, the VLAN ID, or the class of service. When a frame enters the WAP device port, the WAP device 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.

Workflow to Configure ACLs

Use the ACL Rule(s) to configure the ACLs, and then apply the rules to a specified interface.

To configure the ACLs follow these steps:

Step 1 Select **Access Control > ACL**.

Step 2 In the ACL Table, click ✚ to add a new row and create an ACL.

Step 3 Enter a name for the ACL.

Step 4 Select the ACL type from the drop down list (**IPv4, IPv6** or **MAC**).

Step 5 Click ✚, select the associated interfaces to apply the ACL, and click **OK**. If you want to change the associated interfaces, you can click ━ to delete the selected interfaces, and click ✚ to choose the new associated interfaces.

Step 6 Click **More** to view the ACL's parameters.

Step 7 Next, to configure the rules for the ACL. For IPv4 ACLs, see Configure IPv4 ACLs, on page 2. For IPv6 ACLs, see Configure IPv6 ACLs, on page 4. For MAC ACLs, see Configure MAC ACLs, on page 7.

Step 8 Click **Apply** to save all changes.

Configure IPv4 ACLs

To configure an IPv4 ACL:

Step 1 Select **Access Control > ACL**.

Step 2 Click ✚ to add an ACL.

Step 3 In the **ACL Name** field, enter the name of the ACL. The name is limited to 31 alphanumeric and special characters without any space.

Step 4 Choose **IPv4** as the **ACL Type** from the ACL Type list. The IPv4 ACL's control access to the network resources are based on the Layer 3 and Layer 4 criteria.

Step 5 Click ✚ and select the associated interfaces to apply the ACL. Click **OK**. If you want to change the associated interfaces, you can click ━ to delete the selected interface, and click ✚ to choose new associated interfaces.

Step 6 Click **More...** to view the configuration parameters. Click ✚ to add a rule and configure the following:

Note If no rules are added, the WAP denies all the traffic by default.

- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in order of priority. A smaller number means a higher priority. The priority of the new rule will be the lowest of all explicit rules. Note that there is always an implicit rule denying all traffic with lowest priority.
- **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.

  When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.

- **Service (Protocol)** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field. You can choose one of these options:
  - **All Traffic** — Allows all traffic that meets the rule criteria
  - **Select From List** — Choose one of these protocols: **IP, ICMP, IGMP, TCP**, or **UDP**.
  - **Custom** — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed in the Select From List.
- **Source IPv4 Address** — Requires the packet's source IP address to match the address defined in the appropriate fields.
  - **Any**— Allows for any IP address.
  - **Single Address** — Enter the IP address to apply this criteria.
  - **Address/Mask** — Enter the source IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

    A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.
- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header
  - **All Traffic**— Allows all traffic that meets the rule criteria.
  - **Select From List** — Choose the keyword associated with the source port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well known ports
    - 1024 to 49151 — Registered ports
    - 49152 to 65535 — Dynamic and/or private port
- **Destination IPv4 Address** — Requires a packet's destination IP address to match the address defined in the appropriate fields.
  - **Any** — Enter any IP address.
  - **Single Address** — Enter an IP address to apply this criteria.
  - **Address/ Mask** — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

    A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **Any** — Any port that meets the rule criteria.
  - **Select From List** — Choose the keyword associated with the destination port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Enter the IANA port number to match to the destination port identified in the datagram header. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well known ports
    - 1024 to 49151 — Registered ports
    - 49152 to 65535 — Dynamic and/or private port

- **Type Of Service** — Matches the packets based on specific service type.
  - **Any** — Any type of service.
  - **Select From List** — Matches the packets based on their DSCP Assured Forwarding (AS), Class of Service (CS), or Expedited Forwarding (EF) values.
  - **DSCP** — Matches the packets based on a custom DSCP value. If selected, enter an value from 0 to 63 in this field.
  - **Precedence** — Matches the packets based on their IP precedence value. If selected, enter an IP Precedence value from 0 to 7.
  - **ToS/Mask** — Enter an IP ToS Mask value to identify the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field in a packet.

    The IP ToS Mask value is a two-digit hexadecimal number from 00 to FF, representing an inverted (that is, wild card) mask. The zero-valued bits in the IP ToS Mask denote the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field of a packet. For example, to check for an IP ToS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use an IP ToS Bits value of 0 and an IP ToS Mask of 00.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**

To delete or modify a rule, select the rule in the **Details Of Rule(s)** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Configure IPv6 ACLs

To configure an IPv6 ACL:

Step 1 Select **Access Control > ACL**.

Step 2 Click ✚ to add an ACL.

Step 3 In the **ACL Name** field, enter the name of the ACL.

Step 4 Choose **IPv6** as the ACL type from the **ACL Type** list. The IPv4 ACL's control access to the network resources are based on the Layer 3 and Layer 4 criteria.

Step 5 Click ✚ and select the associated interfaces to apply the ACL. Next, click **OK**. If you want to change the associated interfaces, you can click ━ to delete the selected interface then click ✚ to choose new associated interfaces.

Step 6 Click **More...** to view the configuration parameters. Click ✚ to add a rule and configure the following:

Note If no rules are added, the WAP denies all traffic by default.

- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in order of priority. A smaller number means a higher priority. The priority of the new rule will be the lowest of all explicit rules. You can click the up or down button to change its priority. Note that there is always an implicit rule denying all traffic with lowest priority.
- **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.

  When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- **Service (Protocol)** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field. You can choose one of these options:
  - **All Traffic** — Allows all traffic that meets the rule criteria.
  - **Select From List** — Choose one of these protocols: **IPv6, ICMPv6, IGMP, TCP**, or **UDP**.
  - **Custom** — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed in the Select From List.
- **Source IPv6 Address** — Requires the packet's source IP address to match the address defined in the appropriate fields.
  - **Any**— Allows for any IP address.
  - **Single Address** — Enter the IP address to apply this criteria.
  - **Address/Mask** — Enter the source IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

    A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.
- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
  - **Any**— Allows for any source port.
  - **Select From List** — Choose the keyword associated with the source port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.

- **Custom** — Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:
  - 0 to 1023 — Well known ports
  - 1024 to 49151 — Registered ports
  - 49152 to 65535 — Dynamic and/or private port

- **Destination IPv6 Address** — Requires a packet's destination IP address to match the address defined in the appropriate fields.
  - **Any** — Enter any IP address.
  - **Single Address** — Enter an IP address to apply this criteria.
  - **Address/ Mask** — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

    A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **Any** — Any port that meets the rule criteria.
  - **Select From List** — Choose the keyword associated with the destination port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Enter the IANA port number to match to the destination port identified in the datagram header. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well known ports
    - 1024 to 49151 — Registered ports
    - 49152 to 65535 — Dynamic and/or private port

- **Flow Label** — Specifies a 20-bit number that is unique to an IPv6 packet.
  - **Any** — Any 20- bit number.
  - **DSCP** — Matches the number based on a custom DSCP value.

- **DSCP**— Matches the packets based on their IP DSCP value.
  - **Any** — Allows for any DSCP value.
  - **Select From List** — Select a DSCP value from the drop down list.
  - **Custom** — Enter a custom DSCP value, from 0 to 63.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**.

To delete or modify a rule, select the rule in the **Details Of Rule(s)** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Configure MAC ACLs

To configure a MAC ACL:

Step 1 Select **Access Control > ACL**.

Step 2 Click ✚ to add a MAC ACL.

Step 3 In the **ACL Name** field, enter the name to identify the ACL.

Step 4 Choose **MAC** as the type of ACL from the list. MAC ACLs control access based on Layer 2 criteria.

Step 5 Click ✚ and select the associated interfaces to apply the ACL and click **OK**. If you want to change the associated interfaces, you can click ━ to delete the selected interface and then click ✚ to choose new associated interfaces.

Step 6 Then, click **More...** to view the configuration parameters. Click ✚ to add a rule and configure the following parameters:

- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in the order of their priorities. Smaller number means higher priority. The priority of the new rule will be the lowest of all explicit rules and you can click the up or down button to change its priority. Note that there is always an implicit rule denying all traffic with lowest priority.
- **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.

  When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- **Service (ETH Type)** — Choose to compare the match criteria against the value in the header of an Ethernet frame. You can select an ETH Type from the drop down list.
  - Any — Allows for any protocol.
  - **Select From List** — Choose one of these protocol types: **AppleTalk, ARP, IPv4, IPv6, IPX, NetBIOS** or **PPPoE**.
  - **Custom** — Enter a custom protocol identifier to which the packets are matched. The value is a four-digit hexadecimal number in the range of 0600 to FFFF.
- **Source MAC Address** — Requires the packet's source MAC address to match the address defined in the appropriate fields.
  - **Any** — Allows for any source MAC address.
  - **Single Address** — Enter the source MAC address to compare against an Ethernet frame.
  - **Address/ Mask** — Enter the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

For each bit position in the MAC mask, a 0 indicates that the corresponding address bit is significant and a 1 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of 00:00:00:00:ff:ff is used. A MAC mask of 00:00:00:00:00:00 checks all address bits and is used to match a single MAC address.

- **Destination MAC Address** — Requires the packet's destination MAC address to match the address defined in the appropriate fields.
  - **Any** — Allows for any destination MAC address.
  - **Single Address** — Enter the destination MAC address to compare against an Ethernet frame.
  - **Address/Mask** — Enter the destination MAC address mask to specify which bits in the destination MAC to compare against an Ethernet frame
- **VLAN ID** — The VLAN ID to compare against an Ethernet frame.
  - **Any** — Allows for any VLAN ID.
  - **Custom** — Enter the specific VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag. The port range is 1 to 4094.
- **Class Of Service** — Specifies the class of service 802.1p user priority value.
  - **Any** — Allows for any class of service.
  - **Custom** — Enter an 802.1p user priority to compare against an Ethernet frame. The valid range is from 0 to 7.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**. To delete or modify a rule, select the rule in the **Details Of Rule(s)** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Client QoS

Client Quality Of Service (QoS) is used to control the wireless clients connected to the network, and manages the bandwidth that is used. Client QoS can control the traffic such as the HTTP traffic or traffic from a specific subnet by the use of Access Control Lists (ACLs). An ACL is a collection of permit and deny conditions, called rules, that provide security and block unauthorized users and allow authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.

Traffic Classes

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams. It is also given a certain QoS treatment in accordance with defined per-hop behaviors.

The standard IP-based networks are designed to provide best-effort data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications,

such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, on applications with strict timing requirements, such as voice or multimedia, any degradation of service has undesirable effects.

A DiffServ configuration begins with defining class maps, which classify traffic according to their IP protocol and other criteria. Each class map can then be associated with a policy map, which defines how to handle the traffic class. Classes that include time-sensitive traffic can be assigned to the policy maps.

Configuring IPv4 Traffic Classes

To add and configure an IPv4 class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click ✚ to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the **Traffic Class Name** text box, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 In the **Class Type**, choose **IPv4** from the list. The IPv4 traffic classes applies only to IPv4 traffic on the WAP device.

Step 5 Configure the following:

- **Source Address** — Requires a packet's source IPv4 address to match the IPv4 address defined in the appropriate fields.
  - **Any** — Any IPv4 address to be used as the source address.
  - **Single Address** — Enter a single IPv4 address to apply this criteria.
  - **Address/ Mask**— Enter the source IPv4 address mask. The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP address to use for matching against packet content.

    A DiffServ mask of 255.255.255.255 indicates that all bits are important, and mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a mask of 255.255.255.0.
- **Destination Address** — Requires a packet's destination IPv4 address to match the IPv4 address defined in the appropriate fields.
  - **Any** — Any IPv4 address to be used as the destination address.
  - **Single Address** — Enter the IPv4 address to apply this criteria.
  - **Address/Mask** — Enter the destination IP address mask.

Step 6 Click **More...**, and configure the following parameters:

- **Protocol** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
  - **All Traffic** — Allows all traffic from any protocol.

- **Select From List** — Matches the selected protocol: **IP, ICMP, IGMP, TCP** or **UDP**.
- **Custom** — Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.

Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
  - **Any** — Any port is allowed as the source port.
  - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well-Known ports
    - 1024 to 49151 — Registered ports
    - 49152 to 65535 — Dynamic and/or private ports

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **Any** — Any port is allowed as the destination port.
  - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well-known ports
    - 1024 to 49151 — Registered ports
    - 49152 to 65535 — Dynamic and/or private ports

- **Service Type** — Specifies the type of service to use in matching the packets to the class criteria.
  - **Any** — Allows for any type of service as a match criterion.
  - **IP DSCP Select from List** — Choose a DSCP value to use as a match criterion.
  - **IP DSCP Match to Value** — Enter a custom DSCP value from 0 to 63.
  - **IP Precedence** — Matches the packet's IP precedence value to the IP precedence value defined in this field. The IP precedence range is from 0 to 7.
  - **IP ToS Bits** — Uses the packet's type of service (ToS) bits in the IP header as the match criteria. The IP ToS bit value ranges between (00 to FF). The high-order three bits represent the IP precedence value. The high-order six bits represent the IP DSCP value.
  - **IP ToS Mask** — Enter an IP ToS Mask value to identify the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field in a packet.

The IP ToS Mask value is a two-digit hexadecimal number from 00 to FF. The nonzero-valued bits in the IP ToS Mask denote the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field of a packet.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, select the **Traffic Class Name** from the list and click **Delete** or **Edit**. The class map cannot be deleted if it is already attached to a policy.

Step 8 Click **Apply**.

Configuring IPv6 Traffic Classes

To add and configure an IPv6 class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click ✚ to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the **Traffic Class Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 Choose **IPv6** as the type of Traffic Classes from the list. The IPv6 traffic classes applies only to IPv6 traffic on the WAP device.

Step 5 Configure the following:

- **Source Address** — Requires a packet's source IPv6 address to match the IPv6 address defined in the appropriate fields.
  - **Any** — Any IPv6 address to be used as the source address.
  - **Single Address** — Enter the IPv6 address to apply this criteria.
  - **Address/ Mask**— Enter the prefix length of the source IPv6 address.
- **Destination Address** — Requires a packet's destination IPv4 address to match the IPv4 address defined in the appropriate fields.
  - **Any** — Any IPv6 address to be used as the destination address.
  - **Single Address** — Enter the IPv6 address to apply this criteria.
  - **Address/Mask** — Enter the destination IPv6 address and Enter the prefix length of the destination IPv6 address.

Step 6 Click **More...**, and configure the following parameters:

- **Protocol** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
  - **All Traffic** — Allows all traffic from any protocol.

- **Select From List** — Matches the selected protocol: **IPv6, ICMPv6, TCP** or **UDP**.
- **Custom** — Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.

- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.

  Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

  - **Any** — Any port is allowed as the source port.
  - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, ftp** or **www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well-Known Ports
    - 1024 to 49151 — Registered Ports
    - 49152 to 65535 — Dynamic and/or Private Port

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - Any — Any port is allowed as the destination port.
  - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
  - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
    - 0 to 1023 — Well-Known Ports
    - 1024 to 49151 — Registered Ports
    - 49152 to 65535 — Dynamic and/or Private Port

- **IPv6 Flow Label** — The Flow Label is used by a node to label packets in a flow.
  - **Any** — Any 20-bit number that is unique to an IPv6 packet.
  - **User Defined** — Enter a 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers (range 0 to FFFFF).

- **Service Type** — Specifies the type of service to use in matching the packets to the class criteria.
  - **Any** — Allows for any type of service as a match criterion.
  - **IP DSCP Select from List** — Choose a DSCP value to use as a match criterion.
  - **IP DSCP Match to Value** — Enter a custom DSCP value from 0 to 63

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, select the **Traffic Class Name** from the list and click **Delete** or **Edit**. The class map cannot be deleted if it is already attached to a policy.

Step 8 Click **Apply**.

Configuring MAC Traffic Classes

To add and configure a MAC class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click ✚ to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the **Traffic Class Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 Choose **MAC** as the type of class map from the **Class Type** list. The MAC class map applies to Layer 2 criteria.

Step 5 **Source Address** — Includes a source MAC address in the match condition for the rule.

- **Any** — Any MAC address to be used as the source address.
- **Single Address** — Enter the source MAC address to compare against an Ethernet frame.
- **Address/Mask** — Enter the source MAC address mask specifying which bits in the destination MAC address to compare against an Ethernet frame.

  For each bit position in the MAC mask, a 1 indicates that the corresponding address bit is significant and a 0 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of ff:ff:ff:ff:00:00 is used. A MAC mask of ff:ff:ff:ff:ff:ff checks all address bits and is used to match a single MAC address.

Step 6 **Destination Address** — Includes a destination MAC address in the match condition for the rule.

- **Any** — Any MAC address to be used as the destination address.
- **Single Address** — Enter the destination MAC address to compare against an Ethernet frame.
- **Address/Mask** — Enter the destination MAC address mask specifying which bits in the destination MAC address to compare against an Ethernet frame.

Step 7 Click **More...**, and configure the following parameters:

- **Protocol** — Compares the match criteria against the value in the header of an Ethernet frame. Choose an EtherType keyword or enter an EtherType value to specify the match criteria:
  - **All Traffic** — Allows all traffic from any protocol.
  - **Select From List** — Matches the Ethertype in the datagram header with the selected protocol types: **AppleTalk, ARP, IPv4, IPv6, IPX, NetBIOS** or **PPPoE**.
  - **Custom** — Matches the Ethertype in the datagram header with a custom protocol identifier that is specified. The value can be a four-digit hexadecimal number in the range of 0600 to FFFF.

Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

- **Class Of Service** — Specifies the class of service 802.1p user priority value.
  - **Any** — Allows for any class of service.
  - **User Defined** — Enter an 802.1p user priority to compare against an Ethernet frame. The valid range is from 0 to 7.
- **VLAN ID** — The VLAN ID to compare against an Ethernet frame.
  - **Any** — Allows for any VLAN ID.
  - **User Defined** — Enter the specific VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag. The port range is 1 to 4094.

Step 8 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, choose the class map from the list and click **Delete** or **Edit**. The class map cannot be deleted if it is already attached to a policy.

Step 9 Click **Apply**.

QoS Policy

Packets are classified and processed based on the defined criteria. The classification criteria is defined by a class on the **Traffic Classes** page. The processing is defined by a policy attributes on the **QoS Policy** page. Policy attributes may be defined on a per-class instance basis and determine how traffic that matches the class criteria is handled.

The WAP device can hold up to 50 policies and up to 10 classes in each policy.

To add and configure a policy map:

Step 1 Select **Client QoS > QoS Policy**.

Step 2 Click ✚ to add a QoS Policy. In the **QoS Policy Name** field, enter the name for the QoS policy. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 3 You can select an associated traffic class that was created previously.

Step 4 Configure these parameters for the policy map:

- **Committed Rate (Kbps)** — The committed rate, in Kbps, to which traffic must conform. The range is from 1 to 1000000 Kbps.
- **Committed Burst (Bytes)** — The committed burst size, in bytes, to which traffic must conform. The range is from 1 to 204800000 bytes.
- **Action** — Select from one of the following options:
  - **Send** — Specifies that all packets for the associated traffic stream are to be forwarded if the traffic class criteria is met.

- **Drop** — Specifies that all packets for the associated traffic stream are to be dropped if the traffic class criteria is met.

- **Remark Traffic** — Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.
  - **Remark COS** — Network traffic can be partitioned into multiple priority levels or Classes of Service. CoS values range from 0 to 7 with 0 as the lowest priority and 7 as the highest priority.
  - **Remark DSCP** — Specifies a particular per-hop behavior (PHB) that is applied to a packet, based on the QoS provided. Select a value from the drop-down list.
  - **Remark IP Precedence** — Marks all packets for the associated traffic stream with the specified IP precedence value. The IP precedence value is an integer from 0 to 7

Step 5 Click ✚ . You can add another class map. The class map count for this specific policy has the maximum limit of 10.

Step 6 Click **Apply**.

Note To delete or modify a QoS policy, select the QoS policy from the list and click **Delete** or **Edit**.

QoS Association

The QoS Association page provides additional control over certain QoS aspects of the wireless and Ethernet interface.

In addition to controlling the general traffic categories, the QoS allows you to configure the per-client conditioning of the various microflows through the QoS Policy Name. The QoS Policy Name is a useful tool for establishing general microflow definition and treatment characteristics that can be applied to each wireless client, both inbound and outbound, when it is authenticated on the network.

To configure the QoS Association parameters:

Step 1 Select **Client QoS** > **QoS Association**.

Step 2 Click ✚ to add a QoS association.

Step 3 From the **QoS Policy Name** drop down list, choose a QoS Policy name.

Step 4 Configure the following:

- **Rate Limit (From AP to Client)** — The maximum allowed transmission rate from the WAP device to the client in bits per second (bps). The valid range is from 0 to 1733Mbps.
- **Rate Limit (From Client to AP)** — The maximum allowed transmission rate from the client to the WAP device in bits per second (bps). The valid range is from 0 to 1733Mbps.

Step 5 Click **Apply**.

Note An interface can be bound with either a QoS policy or an ACL, but not both.

Guest Access

You can create up to two CP instances on the WAP device. The CP instance is a defined set of instance parameters. The instance can be associated with one or more VAPs.

When you use a wireless client connect to VAP, and access any URL, the web will redirect the URL to **Web Portal Locale** page, which you have configured in the **Access Control/Guest Access** page.

Web Portal Locale Table defines the show style of the authentication web page while the **Guest Group Table** decides the users' username and password.

To configure Guest Access Instance:

Step 1 Edit **Web Portal Locale Table** to design the display of the authentication web page. Click the **Preview** tab to view the display.

Step 2 Edit the **Guest Group Table**, click the value link on **Total Guest Users** number to add a user and click **Apply**.

Step 3 Configure the **Guest Access Instance Table**, select **Guest Group** and **Web Portal Locale** which you configured by using the above steps.

Step 4 Go to **Wireless** > **Networks** to associate the VAP Guest Access and configure the **Guest Access Instance**.

Guest Access Instance Table

Step 1 Select **Guest Access** > **Guest Access Instance Table**.

Step 2 Specify a name for the CP instance in the **Guest Access Instance** field. The name can contain up to 32 alphanumeric characters.

Step 3 Configure the following parameters:

- **Protocol** — Choose either HTTP or HTTPS as the protocol for the CP instance to use during the verification process.
  - **HTTP** — Does not use encryption during verification.
  - **HTTPS** — Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
- **Authentication Method** — Choose the authentication method for CP to use to verify the clients. The options are:
  - **Local Database** — The WAP device uses a local database to authenticate the users. Configure the following if using the **Local Database** setting.
    - **Guest Group**—Enter a name for the guest group.
    - **Idle Timeout (min.)**—Enter the time in minutes for idle timeout.
    - **Maximum Bandwidth Up (Mbps)**— Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth used to send data into the network. The range is from 0 to 1733Mbps. The default value is 0.

- **Maximum Bandwidth Down (Mbps)**— Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth used to receive data from the network. The range is from 0 to 1733Mbps. The default value is 0.
- **Total Guest Users**— Total number of guest users.

- **Radius Authentication** — The WAP device uses a database on a remote RADIUS server to authenticate the users. Configure the following if using the **Radius Authentication** setting.
  - **RADIUS IP Network** — Select the Radius IP network from the drop down list (**IPv4 or IPv6**).
  - **Global RADIUS**— Check **Enable** to enable global RADIUS. If you want the CP feature to use a different set of RADIUS servers, uncheck the box and configure the servers in the fields on this page.
  - **RADIUS Accounting** — Check **Enable** to track and measure the resources that a particular user has consumed, such as the system time and the amount of data transmitted and received.

    If you enable RADIUS accounting, it is enabled for the primary RADIUS server, all backup servers, and all configured servers.
  - **Server IP Address-1 or Server IPv6 Address-1**— Enter the IPv4 or IPv6 address for the primary RADIUS server for this VAP. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10). The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

    When the first wireless client tries to authenticate with a VAP, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and the authentication requests are sent to the specified address.

    Server IP Address-2 or Server IPv6 Address-2 —Enter up to three IPv4 or IPv6 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.
  - **Key-1**— Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter is shown as asterisks.

    Key-2—Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address-1 uses Key-1, Server IP Address-2 uses Key-2, and so on.

- **No Authentication** — The users do not need to be authenticated by a database.
- **3rd Party Credentials** — The WAP device uses the credentials on the social media to authenticate the users. Configure the following if using **3rd Party Credentials** authentication setting.
  - **Accepted credentials** — Select **Facebook** or **Google** or both of them to be the credentials authentication.
  - **Walled Garden** — The relevant default configuration will be set automatically while **Accepted credentials** are selected.

Note Cisco integrates data protection, privacy, and security requirements into product design and development methodologies from ideation through launch. For more information, see *https://www.cisco.com/c/en/us/about/trust-center/gdpr.html*.

- **Active Directory Service** — The WAP device uses a database on a remote ADS server to authenticate the users. Configure the following if using the **Active Directory Service** authentication setting.

- **Active Directory Servers** — Add new ADS server by clicking the ✚ icon. You can add upto 3 servers. Use **arrow** to move and prioritize the servers. Choose **trash can** to delete the configuration. Use the **Test** to check if the ADS server is valid.

- **External Capture Portal** — The WAP device uses an external site to customize and authenticate users on the captive portal page. For this purpose, it uses Purple WiFi: *https://purple.ai/* to access on an external site.

  In the Purple WiFi page, create a purple account and register. Specify the venue and location when requested. Add the hardware details based on the MAC address of the WAP. This generates a User Guide with all the required information for configuring the External Capture Portal (EXCAP) interface on the WAP.

  Note Make sure that your Purple WiFi account is configured right before on-boarding the Cisco AP. This ensures an appropriate functioning of the Purple WiFi redirection service.

  Configure the following if using an external captive portal setting.

  - **Splash Page URL** — Enter the URL (including *https://*) for the portal page which is obtained after successful registration into the Purple WiFi. The range is 0 to 256 characters. The EXCAP hosts the initial login page called the splash page on the cloud or on an external web server which may be outside the AP network. For example: *https://region3.purpleportal.net/access/* if your region is ASIA-PACIFIC in Purple Wi-Fi.

  - **Walled Garden** — Specify a list of domains that users can access before passing through the Web portal page. Items in the list should be separated by a comma, and domains can include wildcards in the form of an asterisk (*). The length of each domain cannot be greater than 100. Ensure that the total length of the Walled Garden must be less than 4096. The following options should be set if you want to use them on Purple Wi-Fi's EXCAP solution:

Purple WiFi (MUST)	purpleportal.net, cloudfront.net, venuewifi.com, openweathermap.org, stripe.com
Facebook (Optional)	facebook.com, fbcdn.net, akamaihd.net, facebook.net
Twitter (Optional)	twitter.com, twimg.com
LinkedIn (Optional)	linkedin.com, licdn.net, licdn.com
Instagram (Optional)	instagram.com
Vkontakte (Optional)	vk.com, vk.me

  - **RADIUS Server IP Address-1** — Enter the IPv4 address for the primary RADIUS server for this VAP. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx.

    When the first wireless client tries to authenticate with a VAP, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and the authentication requests are sent to the specified address.

  - **RADIUS Server IP Address-2** — Enter the IPv4 backup RADIUS server addresses. If the authentication fails with the primary server, the configured backup server is tried.

- **Key-1** — Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. For example, the secret can be 6n8!5ETGb^nd if you use Purple Wi-Fi. The text that you enter is shown as asterisks.
- **Key-2** — Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address-1 uses Key-1, Server IP Address-2 uses Key-2.

  For the Purple WiFi, the Server IP Address-1 and Address-2 varies for different regions. The table below specifies the same:

Regions	Address-1	Address-2
AMERICAS	34.94.146.135	34.94.183.201
EUROPE	35.230.139.41	35.246.18.82
ASIA-PACIFIC	35.244.93.31	35.244.98.247
The value for Key-1 and Key-2 is 6n8!5ETGb^nd		

- **RADIUS Accounting** — Check Enable to track and measure the resources that a particular user has consumed, such as the system time and the amount of data transmitted and received.

  If you enable RADIUS accounting, it is enabled for the primary RADIUS server and the backup server.

- **Guest Group** — If the **Authentication Method** is set to **Local Database** or **Radius Authenticated**, select a **Guest Group** that was created previously . All users who belong to the group are permitted to access the network through this portal.
- **Redirect URL** — To enable the URL Redirect, enter the URL (including http://). The range is from 0 to 256 characters.
- **Session Timeout (min.)** — Enter the time remaining, in minutes, for the CP session to be valid. After the time reaches zero, the client is de-authenticated. The range is from 0 to 1440 minutes. The default value is 0. The session timeout got from the Radius Server will over ride the user configured timeout in the event of a session timeout.
- **Web Portal Locale** — Select a web portal locale that was created previously from the drop-down list.

Step 4 Click **Apply** . Your changes are saved to the Startup Configuration.

Note **Redirect URL** and **Web Portal Locale** are not of use in EXCAP mode.

Please refer to Hardware manual in Purple Wi-Fi for more detailed settings of EXCAP

Guest Group Table

On the device, each local user is assigned to a user group and the group is assigned to a CP instance. The group facilitates managing the assignment of users to CP instances.

The user group named Default is built-in and cannot be deleted.

To configure a local user:

Step 1 Select **Guest Access > Guest Group Table**.

Step 2 In the Guest Groups Settings area, configure the following parameters:

- **Guest Group Name** — Specify the name for the new guest group. The default Guest Group Name is **Default**

Step 3 Configure these parameters:

- **Idle Timeout** — Enter the period of time that a user remains in the CP authenticated client list after the client disassociates from the WAP device. If the time specified in this field expires before the client attempts to re-authenticate, the client entry is removed from the authenticated client list. The range is from 0 to 1440 minutes. The default value is 60. The timeout value configured here has precedence over the value configured for the CP instance, unless the user value is set to 0. When it is set to 0, the timeout value configured for the CP instance is used.
- **Maximum Bandwidth Up** — Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth used to send data into the network. The range is from 0 to 1733 Mbps. The default is 0.
- **Maximum Bandwidth Down** — Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth used to receive data from the network. The range is from 0 to 1733 Mbps. The default is 0.
- **Total Guest Users** — Displays the number of total guest users. Click the value link on the **Total Guest Users** to display the **Guest User Account** page.

Step 4 Click **Apply**.

Guest User Account

To configure a guest user account:

Step 1 Select **Guest Access > Guest Group Table** .

Step 2 Click the number link on the **Total Guest Users** field to display the **Guest User Account Table** in the **Guest User Account** page.

Step 3 Click ✚ to add a user.

Step 4 **Guest User Name** — Enter the name for the new guest user. The name can contain up to 32 alphanumeric characters.

Step 5 **Guest User Password** — Enter the password. The password can contain 8 to 64 alphanumeric and special characters.

Step 6 Click **Apply**.

Note You can click **Back** button link to view the **Guest Access** page.

To delete or modify a guest user, you need to select it and then click **Delete** or **Edit**.

Web Portal Customization

After the CP instance is associated with a VAP, create a locale and map it to the CP instance. When the user accesses a VAP that is associated with a CP instance, the authentication page will appear.

Use the Web Portal Customization page to create unique pages for different locales on your network, and to customize the text and images on the pages.

Step 1 Select **Guest Access** > **Web Portal Locale Table**.

Step 2 In this table, click ✚ to access the **Web Portal Customization** page. To modify the locale, check the row and click **Edit** or click **Delete** to delete.

You can create up to three different authentication pages with different locales on your network.

Step 3 In the **Web Portal Customization** page, configure the following parameters:

- **Web Portal Locale Name** — Enter a web locale name to assign to the page. The name can be from 1 to 32 alphanumeric characters.

Step 4 The **Guest Access Instance Name** cannot be edited. The editable fields are populated with default values. Configure the following parameters:

- **Guest Access Instance Name** — Displays the name of the guest access instance.
- **Background Image** — Click **Browse** to choose the image. You can click **Upload** to upload the images for CP instances. The filesize must be 64K or less.
- **Logo Image** — Click **Browse** to choose the logo image. You can click **Upload** to upload the logo images. The filesize must be 64K or less.
- **Foreground Color** — Enter the HTML code for the foreground color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Background Color** — Enter the HTML code for the background color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Separator Color** — Enter the HTML code for the color of the thick horizontal line that separates the page header from the page body, in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Account Image** — Click **Browse** to choose the image. You can click **Upload** to upload the account images. The filesize must be 64K or lesser per alert message.
- **Fonts**—Select a font from the drop down list. This font will be used when displaying all text.
- **Account Prompting** — Enter a user name. The range is from 1 to 32 characters.
- **Username Prompting** — The label for the user name text box. The range is from 1 to 32 characters.
- **Password Prompting** — The label for the user password text box. The range is from 1 to 64 characters.
- **Button Prompting** — The label on the button that users click to submit their user name and password for authentication. The range is from 2 to 32 characters. The default is Connect.
- **Browser Head Prompting** — The text that appears in the browser title bar. The range is from 1 to 128 characters. The default is Captive Portal.

- **Portal Title Prompting** — The text that appears in the page header, to the right of the logo. The range is from 1 to 128 characters. The default is Welcome to the Wireless Network.
- **Account Tips Prompting** — The text that appears in the page body below the user name and password text boxes. The range is from 1 to 256 characters. The default is To start using this service, enter your credentials and click the connect button.
- **Acceptance Policy** — The text that appears in the Acceptance Use Policy box. The range is from 1 to 4096 characters. The default is Acceptance Use Policy.
- **Acceptance Prompting** — The text that instructs users to select the check box to acknowledge reading and accepting the Acceptance Use Policy. The range is from 1 to 128 characters.
- **No Acceptance Warning** — The text that appears in a pop-up window when a user submits login credentials without selecting the Acceptance Use Policy check box. The range is from 1 to 128 characters.
- **Work In Progress Prompting**—The text that appears during the authentication process. The range is from 1 to 128 characters.
- **Invalid Credentials Prompting** — The text that appears when a user fails the authentication. The range is from 1 to 128 characters.
- **Connect Success Prompting** — The text that appears when the client has authenticated to the VAP. The range is from 1 to 128 characters.
- **Welcome Prompting** — The text that appears when the client has connected to the network. The range is from 1 to 256 characters.
- **Restore** — Deletes the current locale.

Step 5 Click **Apply**. Your changes are saved to the Startup Configuration.

Step 6 Click **Preview** to view the updated page.

Clicking **Preview** will show the text and the images that have already been saved to the Startup Configuration. If you make a change, click **Apply** before clicking **Preview** to see your changes.