Security Tab

The Security tab on the menu bar enables you to configure and set security policies on your Cisco WLC. Use the Selector area to access specific security parameters. Making this selection from the menu bar opens the RADIUS Authentication Servers page.

You can access the following pages from the security tab:

- General (AAA)
- RADIUS Authentication Servers
- RADIUS Accounting Servers
- RADIUS Fallback Parameters
- RADIUS DNS Parameters
- TACACS+ Authentication Servers
- TACACS+ Accounting Servers
- TACACS+ Authorization Servers
- TACACS DNS Parameters
- LDAP Servers
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Policies
- AP Policies
- Password Policies
- General (Local EAP)
- Local EAP Profiles
- EAP-FAST Method Parameters
- Authentication Priority
- Priority Order of Management Users
- Local Significant Certificates
- Self Significant Certificates
- Access Control Lists

General (AAA)

Choose **SECURITY > AAA > General** to navigate to the General page.

This page enables you to specify the maximum number of local network users that can exist on the local user database:

- Maximum Local Database entries—Enables you to enter a value for the maximum number of local network users that can be added to the local user database the next time that the Cisco WLC reboots. The currently configured value appears in parentheses to the right of the field. The valid range is from 512 to 2048, and the default setting is 2048.
- Number of entries, already used—Displays the number of entries currently in the database.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** to navigate to the RADIUS Authentication Servers page.

This page displays RADIUS server information for your configured RADIUS server and enables you to edit the Call Station ID Type:

- Auth Called Station ID Type— The Call Station ID Type is applicable only for non-802.1X authentication. The different Call Station ID types are as follows:
  - IP address
  - System MAC address
  - AP MAC address:SSID
  - AP MAC Address
  - AP Name
  - AP Name: SSID
  - AP Group
  - Flex Group
  - AP Location
  - VLAN ID
  - AP Eth MAC Address
  - AP Eth MAC Address:SSID
  - AP Label MAC Address
  - AP Label MAC Address:SSID
- Use AES KeyWrap—RADIUS-to-Cisco WLC key transport using AES KeyWrap protection. The AES KeyWrap is required for FIPS customers. All defined RADIUS must have AES KeyWrap keys defined.
- MAC Delimiter—Delimiter that you can use when you specify the MAC address. The available options are as follows:
  - Colon
  - Hyphen
  - Single Hyphen
  - No Delimiter
- Network User—Network user authentication check box. If this option is enabled, this entry is considered as the network user RADIUS authenticating server entry. If you did not set the RADIUS server entry on the WLAN configuration (**WLANs > Edit > Security > AAA Servers**), you must enable this option for network users.
- Management—Management authentication check box. If this option is enabled, this entry is considered as the management RADIUS authenticating server entry. If you enable this option, authentication requests go to the RADIUS server.
- Server Index—RADIUS server index. The Cisco WLC tries Index 1 first, and then Index 2 and so on, in an ascending order. This value should be 1 if your network is using only one authentication server.
- Server Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—Communication port number for the interface protocols. The default is 1812.
- IPSec—Read-only field. Displays the IPsec mechanism. If this option is enabled, the IP Security Parameters fields are also displayed.

- Admin Status—Whether the RADIUS authentication server is enabled or disabled.

Click the server index number to open the Updating RADIUS Authentication Servers page.

To delete an existing RADIUS authentication server, click the blue arrow adjacent the desired access point and choose your cursor over the blue drop-down arrow and choose **Remove**.

To send ping packets to the RADIUS server to verify that you have a working connection between the Cisco WLC and the RADIUS server, click the blue arrow adjacent the desired server and choose **Ping**.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **New** to add a new RADIUS authentication server (For more information, see Adding RADIUS Authentication Servers).

Adding RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** and then click **New** to navigate to the RADIUS Authentication Servers > New page.

This page enables you to add a new RADIUS server:

- Server Index (Priority)—Index of the RADIUS server. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set the server index to 1 if your network is using only one authentication server.

Note You can have a maximum of 17 RADIUS authenticating server entries for a single WLAN.

- Server IP Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.
- Key Wrap—Check box that you can select to enable the following AES KeyWrap keys:
  - Key Wrap Format—ASCII or hexadecimal.

Note FIPS customers must enter keys using hexadecimal notation.

  - Key Encryption Key (KEK)—128-bit (16-byte) AES KeyWrap Key Encryption Key.
  - Message Authentication Code Key (MACK)—160-bit (20-byte) AES KeyWrap Message Authentication Code Key.
- Port Number—Communication port number for the interface protocols.

Note Do not assign the port number that is used by another application. Use the default (1812) or any other port unused by any other application.

- Server Status—RADIUS authentication server that you enable or disable.
- Support for RFC 3576—Support for RFC 3576 that you can enable or disable. RFC 3576 is an extension to the RADIUS protocol, which allows dynamic changes to a user session including support for disconnecting users and changing authorizations applicable to a user session (support

for Disconnect and Change-of-Authorization [CoA] messages). Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.

- Server Timeout—Time in seconds after which the RADIUS authentication request times out and a retransmission is taken up by the Cisco WLC. You can specify a value between 2 to 30 seconds.
- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user. If you did not set the RADIUS server entry on the WLAN configuration (**WLANs > Edit > Security > AAA Servers**), you must enable this option for network users.
- Management—Management authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user. If you enable this option, authentication requests go to the RADIUS server.
- IPsec—Check box that allows you to enable or disable the IP Security mechanism. If you enable this option, the IP Security Parameters fields are displayed.

Note The IPsec option is displayed only if a crypto card is installed on the Cisco WLC.

Note IPsec does not support IPv6. Use this only if you have used IPv4 for Server IP Address.

- IPsec Authentication: Set the IP security authentication protocol to be used. Options are as follows:
  - HMAC-SHA1
  - HMAC-MD5

    Message Authentication Codes (MACs) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions. HMAC can be used with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA-1 are two constructs of the HMAC using the MD5 hash function and the SHA-1#hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.
- IPsec Encryption—IP security encryption mechanism to be used. Options are as follows:
  - DES —Data Encryption Standard that uses a private data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
  - Triple DES—Data Encryption Standard that applies three keys in succession.
  - AES CBS—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses 128 bit data path in Cipher Clock Chaining (CBC) mode.
- IKE Phase 1: Internet Key Exchange protocol (IKE). Options are as follows:
  - Aggressive
  - Main

    IKE Phase-1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.
- Lifetime (seconds): Set the timeout interval for the session expiry. The default is 28800 seconds.
- IKE Diffie Hellman Group: Set the IKE Diffie Hellman Group. The options are as follows:

  - Group 1 (768 bits)
  - Group 2 (1024 bits)
  - Group 5 (1536 bits)

    Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

    Although all the three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 keys might occur slightly faster because of their smaller prime number size.
  - Group 14 (2048 bits)

    Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

    Although all the four groups provide security from conventional attacks, Group 14 is considered most secure because of its larger key size. However, computations involving Group 1, Group 2, and Group 5 keys might occur slightly faster because of their smaller prime number size. The default value is Group 1.

- Auth Method—IPsec authentication method that can be PSK or Certificate.Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Updating RADIUS Authentication Servers

Choose **SECURITY > AAA > RADIUS > Authentication** and click on a link in the Server Index column to update RADIUS authentication servers.

This page enables you to change the RADIUS Authentication parameters on an existing RADIUS server. See Adding RADIUS Authentication Servers.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** to navigate to the RADIUS Accounting Servers page.

This page displays RADIUS information for your existing RADIUS server.

- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user. The default is unselected.
- Server Index—The RADIUS server index. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set the server index to 1 if your network is using only one accounting server.

Note You can configure a maximum of 17 RADIUS accounting server entries for a single WLAN.

- Server Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—Controller port number for the interface protocols.
- IPsec—Read-only field. Displays the status of the IPsec mechanism. If this option is enabled, the IP Security Parameters fields are also be displayed.
- Admin Status—Whether the RADIUS accounting server is enabled or disabled.

Click the server index number to update the RADIUS accounting servers (see Editing RADIUS Accounting Servers).

Click the blue arrow adjacent the desired server and choose **Remove** to delete an existing RADIUS accounting server.

Click the blue arrow adjacent the desired server and choose **Ping** to send ping packets to the RADIUS server to verify that you have a working connection between the Cisco WLC and the RADIUS server.

Click **New** to add a new RADIUS accounting server (For more information, see Adding RADIUS Accounting Servers).

Adding RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** and then click **New** to navigate to the RADIUS Accounting Servers > New page.

This page enables you to add a new RADIUS server:

- Server Index (Priority)—Index of the RADIUS server. The Cisco WLC tries Index 1 first, and then Index 2 through 17, in an ascending order. Set to 1 if your network is using only one accounting server.
- Server IP Address (IPv4/IPv6)—IP address of the RADIUS server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.
- Port Number—Port number for the interface protocols.

Note Do not assign the port number to one that is used by another application. Use the default (1813) or any other port unused by any other application.

- Server Status—RADIUS accounting server that you enable or disable.
- Server Timeout—Time in seconds after which the RADIUS authentication request times out and a retransmission is taken up by the Cisco WLC. You can specify a value between 2 to 30 seconds.
- Network User—Network user authentication that you can enable or disable. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
- IPSec—Check box that you can select to enable or disable the IP Security mechanism. If you enable this option, the IP Security Parameters fields are displayed.

Note IPSec does not support IPv6. Use this only if you have used IPv4 for Server IP Address.

- IPSec Authentication: Set the IP security authentication protocol to be used. Options are as follows:

  - HMAC-SHA1
  - MAC-MD5
  - None

    Message Authentication Codes (MACs) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions. HMAC can be used with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA-1 are two constructs of the HMAC using the MD5 hash function and the SHA-1#hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

- IPsec Encryption—IP security encryption mechanism. Options are as follows:
  - DES—Data Encryption Standard that uses a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
  - Triple DES—Data Encryption Standard that applies three keys in succession.
  - AES 128 CBC—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses 128-bit data path in Cipher Clock Chaining (CBC) mode.
- IKE Authentication: (Display Only Field).
- IKE (Internet Key Exchange protocol) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.
- IKE Phase 1: Set the Internet Key Exchange protocol (IKE). Options are as follows:
  - Aggressive
  - Main

    IKE Phase-1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection establishment, at the cost of transmitting the identities of the security gateways in the clear.
- Lifetime (seconds): Timeout interval for the session expiry. The default is 28800 seconds.
- IKE Diffie Hellman Group—Options are as follows:
  - Group 1 (768 bits)
  - Group 2 (1024 bits)
  - Group 5 (1536 bits)
  - Group 14 (2048 bits)

    Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.

    Although all the four groups provide security from conventional attacks, Group 14 is considered most secure because of its larger key size. However, computations involving Group 1, Group 2, and Group 5 keys might occur slightly faster because of their smaller prime number size.
- Auth Method—IPsec authentication method that can be PSK or Certificate.
- Shared Secret Format—Format of the shared secret that you set to either ASCII of Hex.
- Shared Secret/Confirm Shared Secret—RADIUS server login Shared Secret.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing RADIUS Accounting Servers

Choose **SECURITY > AAA > RADIUS > Accounting** and then click **Edit** to navigate to the RADIUS Accounting Servers > Edit page.

This page enables you to change the RADIUS accounting parameters on an existing RADIUS server. for more information about the parameters, see Adding RADIUS Accounting Servers:

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RADIUS Fallback Parameters

Choose **SECURITY > AAA > RADIUS > Fallback** to navigate to the RADIUS > Fallback Parameters page.

If the primary RADIUS server (for example, Index 1) is unavailable, the Cisco WLC switches to the next RADIUS server (for example, Index 2). By default, when the RADIUS server configured as Index 1 becomes available again, the current RADIUS server remains the primary server.

You can configure the RADIUS server fallback behavior to specify which RADIUS server is the primary server. This table describes the RADIUS fallback parameters.

Table 6-1 RADIUS Fallback Parameters

Parameter	Description
Fallback Mode	Specify the RADIUS server fallback mode: • Active—Specifies that the Cisco WLC will revert to a server with a lower server index from the backup servers by sending RADIUS probe messages to determine whether a server that has been marked as inactive is back online. The Cisco WLC ignores all inactive servers for all active RADIUS requests. • Passive—Specifies that the Cisco WLC will revert to a server with a lower server index from the backup servers without using probe messages. The Cisco WLC ignores all inactive servers for a period of time and then retries later when a RADIUS message needs to be sent. • Off—(Default) Disable server fallback.
Username	Enter the name to be sent in the inactive server probes, up to 16 alphanumeric characters. The default value is cisco-probe.
Interval in sec	Enter the probe interval (when using Active mode) or inactive time (when using Passive mode) in seconds. Valid values are from 180 to 3600; the default value is 300.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RADIUS DNS Parameters

Choose **SECURITY > AAA > RADIUS > DNS** to navigate to the RADIUS DNS Parameters page.

This page allows Cisco WLC to retrieve the RADIUS IP information from a DNS server. The DNS server is queried at regular intervals for updates. The Cisco WLC also runs the query if you manually change the DNS server list, or if one of the servers timeouts. As the DNS list overrides the static list, all manual AAA configurations on the WLAN will stop functioning as soon as the global server list gets populated from the DNS server. DNS AAA is also valid for FlexConnect AP clients using central authentication.

Note RADIUS DNS is not supported for FlexConnect AP groups and FlexConnect clients with local switching.

Note DNS does not support IPv6.

This table describes the DNS parameters.

Table 6-2 DNS Parameters

Parameter	Description
DNS Query	Check box to enable the Cisco WLC to retrieve the RADIUS IP information from a DNS server. The default is disabled. **Note** When you enable the DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.
Port Number	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port. **Note** The accounting port is derived from the authentication port.
Secret Format	Format of the shared secret that you set to either ASCII or Hex.
Secret/Confirm Secret	RADIUS server login secret. **Note** All the DNS servers should use the same secret.
DNS Timeout	Maximum time, in seconds, that the Cisco WLC waits before timing out the request and resending it. The range is from 1 to 180 days.
URL	Fully qualified domain name (FQDN) of the RADIUS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
Server IP Address	DNS server IP address. **Note** IPv6 is not supported for DNS.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** to navigate to the TACACS+ Authentication Servers page.

This page displays a summary of the existing TACACS+ authentication servers.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.
- Admin Status—TACACS+ server status.

You can perform the following actions:

- To edit an existing TACACS+ authentication server, click the index number for that server.
- To remove an existing TACACS+ authentication server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ authentication server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ Authentication server.

Adding TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** and then click **New** to navigate to the TACACS+ Authentication Servers > New page.

This page enables you to configure a TACACS+ authentication server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS+ server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.

- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing TACACS+ Authentication Servers

Choose **SECURITY > AAA > TACACS+ > Authentication** and then click a Server Index number to navigate to the TACACS+ Authentication Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ authentication server.

- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** to navigate to the TACACS+ Accounting Servers page.

This page displays a summary of the existing Terminal Access Controller Access Control System Plus (TACACS+) Accounting servers.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.
- Admin Status—TACACS+ server status.

To edit an existing TACACS+ accounting server, click the index number for that server.

- To remove an existing TACACS+ accounting server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ accounting server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ accounting server.

Adding TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** and then click **New** to navigate to the TACACS+ Accounting Servers > New page.

This page enables you to configure a TACACS+ accounting server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—Enter the TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing TACACS+ Accounting Servers

Choose **SECURITY > AAA > TACACS+ > Accounting** and then click a Server Index number to navigate to the TACACS+ Accounting Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ accounting server.

- Shared Secret Format—Shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server that you enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** to navigate to the TACACS+ Authorization Servers page.

This page displays a summary of the existing TACACS+ authorization servers:

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the Cisco WLC automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

This page displays the following information about the configured TACACS servers:

- Server Index—Index of the TACACS+ server.
- Server Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TACACS+ server TCP port number.
- Admin Status—TACACS+ server status.

You can perform the following actions:

- To edit an existing TACACS+ Authorization server, click the index number for that server.
- To remove an existing TACACS+ Authorization server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the TACACS+ Authorization server, click the blue arrow adjacent the desired server and choose **Ping**.
- Click **New** to add a new TACACS+ Authorization server.

Adding TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** and then click **New** to navigate to the TACACS+ Authorization Servers > New page.

This page enables you to configure a TACACS+ authorization server:

Note You must configure TACACS+ on both your Cisco Secure Access Control Server (ACS) and your Cisco WLC. For information on configuring the ACS, refer to the *Cisco Wireless Controller Configuration Guide* or the *Cisco Secure ACS Configuration Guide*.

- Server Index (Priority)—Index of the TACACS server. Choose a number to specify the priority order of this server in relation to any other configured TACACS+ servers. You can configure up to three servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the TACACS+ server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Port Number—TACACS+ server TCP port number. The valid range is 1 to 65535; the default value is 49.

Note Do not assign a port number that is used by another application. Use the default (49) or any other port unused by any other application.

- Server Status—Enable or disable this TACACS+ server.
- Server Timeout—Enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing TACACS+ Authorization Servers

Choose **SECURITY > AAA > TACACS+ > Authorization** and then click a Server Index number to navigate to the TACACS+ Authorization Servers > Edit page.

This page enables you to change the settings for an existing TACACS+ authorization server:

- Shared Secret Format—Format of the shared secret that you set to either ASCII or Hex.
- Shared Secret/Confirm Shared Secret—TACACS+ server login Shared Secret.
- Server Status—TACACS+ server status that you can enable or disable.
- Server Timeout—Number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

TACACS DNS Parameters

Choose **SECURITY > AAA > TACACS > DNS** to navigate to the TACACS DNS Parameters page.

This page allows Cisco WLC to retrieve the TACACS IP information from a DNS server. The DNS server is queried at regular intervals for updates. The Cisco WLC also runs the query if you manually change the DNS server list, or if one of the servers timeouts. As the DNS list overrides the static list, all manual AAA configurations on the WLAN will stop functioning as soon as the global server list gets populated from the DNS server. DNS AAA is also valid for FlexConnect AP clients using central authentication.

Note TACACS DNS is not supported for FlexConnect AP groups and FlexConnect clients with local switching.

Note DNS does not support IPv6.

This table describes the TACACS DNS parameters.

Table 6-3 TACACS DNS Parameters

Parameter	Description
DNS Query	Check box to enable the Cisco WLC to retrieve the TACACS IP information from a DNS server. The default is disabled. **Note** When you enable the DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.
Port Number	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port. **Note** The accounting port is derived from the authentication port.
Secret Format	Format of the shared secret that you set to either ASCII or Hex.
Secret/Confirm Secret	TACACS server login secret. **Note** All the DNS servers should use the same secret.
DNS Timeout	Maximum time, in seconds, that the Cisco WLC waits before timing out the request and resending it. The range is from 1 to 180 days.
URL	Fully qualified domain name (FQDN) of the TACACS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
Server IP Address	DNS server IP address. **Note** IPv6 is not supported for DNS.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

LDAP Servers

Choose **SECURITY > AAA > LDAP** to navigate to the LDAP Servers page.

This page displays a summary of the existing Lightweight Directory Access Protocol (LDAP) servers:

- Server Index—Index of the LDAP server.
- Server Address (IPv4/IPv6)—IP address of the LDAP server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port—TCP port number of the LDAP server.
- Server State—Current status of the server.
- Bind—Local authentication bind method for the LDAP server.

You can perform the following actions:

- To edit an existing LDAP server, click the index number for that server.
- To remove an existing LDAP server, click the blue arrow adjacent the desired server and choose **Remove**.
- To ping the LDAP server, click the blue arrow adjacent the desired server and choose **Ping**.

Click **New** to add a new LDAP server.

Adding LDAP Servers

Choose **SECURITY > AAA > LDAP** and then click **New** to navigate to the LDAP Servers > New page.

This page enables you to configure a Lightweight Directory Access Protocol (LDAP) server as a back-end database, which is similar to a RADIUS or local user database. An LDAP back-end database allows the Cisco WLC to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its back-end database to retrieve user credentials.

Note The LDAP back-end database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC.

LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password. For example, Microsoft Active Directory is not supported because it does not return a clear-text password.

If the LDAP server cannot be configured to return a clear-text password, LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are not supported.

- Server Index (Priority)—Index of the LDAP server. Choose a number to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to 17 servers. If the Cisco WLC cannot reach the first server, it tries the second one in the list and so on.
- Server IP Address (IPv4/IPv6)—IP address of the LDAP server. From Release 8.0, the controller supports both, IPv4 and IPv6.
- Port Number—LDAP server TCP port number. The valid range is 1 to 65535; the default value is 389.
- Simple Bind—Local authentication bind method for the LDAP server that you can specify: either Anonymous or Authenticated. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access.

- Bind Username—(for Authenticated bind method) Username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

Note If the username starts with "cn=" (in lowercase letters), the Cisco WLC assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.

- Bind Password—(for Authenticated bind method) Password to be used for local authentication to the LDAP server.
- Confirm Bind Password—(for Authenticated bind method) Password to be used for local authentication to the LDAP server.
- User Base DN—Distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, ou=next organizational unit, and o=corporation.com. If the tree that contains users is the base DN, type **o=***corporation***.com** or **dc=***corporation***,dc=com**.
- User Attribute—Name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.
- User Object Type—Value of the LDAP objectType attribute that identifies the record as a user.
- Server Timeout—Number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
- Enable Server Status—LDAP server that you can enable or disable.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing LDAP Servers

Choose **SECURITY > AAA > LDAP** and then click a Server Index number to navigate to the LDAP Servers > Edit page.

This page enables you to change the settings for an existing Lightweight Directory Access Protocol (LDAP) server:

- Enable Server Status—LDAP server that you can enable or disable.
- Simple Bind—Local authentication bind method for the LDAP server that you can specify: either Anonymous or Authenticated. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access.
- Bind Username—Username to be used for local authentication to the LDAP server.
- Bind Password—Password to be used for local authentication to the LDAP server.
- Confirm Bind Password—Password to be used for local authentication to the LDAP server.
- User Base DN—Distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, ou=next organizational unit, and o=corporation.com. If the tree that contains users is the base DN, type **o=***corporation***.com** or **dc=***corporation***,dc=com**.
- User Attribute—Name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.

- User Object Type—Value of the LDAP objectType attribute that identifies the record as a user.
- Server Timeout—Number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Local Net Users

Choose **SECURITY > AAA > Local Net Users** to navigate to the Local Net Users page.

This page displays a summary of the existing local network clients who are allowed to access a specific Cisco WLAN Solution WLAN sorted by the username. You must enable Layer 3 Web Authentication located on the Adding Local Net Users page must be enabled.

This table describes the local net user parameters.

Table 6-4 Local Net User Parameters

Parameter	Description
User Name	Username of the local net user.
WLAN Profile	WLAN profile of the local net user.
Guest User	Whether the user is a guest user.
Role	Role of the local net user.
Description	Short description about the configured local net user.

Client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

- Click the username to edit a local network user definition on the Editing Local Net Users page.
- Click the blue arrow adjacent the desired client and choose **Remove** to remove an existing local network client.

Click **New** to add a new local network client (Adding Local Net Users).

Adding Local Net Users

Choose **SECURITY > AAA > Local Net Users** and then click **New** to navigate to the Local Net Users > New page.

This page enables you to add a local network user. You must enable Layer 3 Web Authentication located on Editing WLANs page.

- User Name—Username of the local network user.
- Password—Password of the local network user.
- Confirm Password—Password for the local network user.
- Guest User—Guest User check box that you can select to limit the amount of time that the user has access to the local network. The default setting is unselected.

- Lifetime—If you selected the Guest User check box, enter the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2592000 seconds, and the default setting is 86400 seconds.
- Guest User Role—If you created a QoS role for guest users (QoS Roles for Guest Users), select the Guest User Role check box and select a Role from the drop-down list.
- WLAN Profile—Select WLAN profile that the user is allowed to access. If you choose **Any WLAN**, which is the default setting, the user can access any of the configured WLANs.
- Description—User description that you can enter.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing Local Net Users

Choose **SECURITY > AAA > Local Net Users** and then click the username to navigate to the Local Net Users > Edit page.

This page enables you to edit a local network user definition. You must enable Layer 3 Web Authentication located on Editing WLANs page.

- User Name—Read-only field that displays the username of the local network user.
- Password—Password that you can specify.
- Confirm Password—Password that you can specify.
- Lifetime (seconds)—Lifetime of the user in seconds.
- Guest User Role—Guest User parameter that you can confirm or change if you want to limit the amount of time that the user has access to the local network. The default setting is unselected. If you selected the Guest User check box, confirm or change the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2592000 seconds, and the default setting is 86400 seconds.
- Guest User Role—If you created a QoS role for guest users (QoS Roles for Guest Users), confirm or change the Guest User Role check box and select a Role from the drop-down list.
- WLAN Profile—WLAN profile that you can select from the drop-down list.
- Description—User description that you can enter.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

MAC Filtering

Choose **SECURITY > AAA > MAC Filtering** to navigate to the MAC Filtering page.

This page displays the RADIUS Compatibility Mode, MAC delimiters for MAC Filtering, and the client MAC addresses that you entered into the Cisco WLC's local database.

You can configure each client MAC address to access network services through a specific Cisco WLAN and interface, or you can configure the WLAN as “Any WLAN” and the interface as “None” so that the client is not limited to that single WLAN or interface.

When MAC filtering is configured on the WLAN, the Cisco WLC checks the local database for the client MAC address. If the client MAC address is not found locally, then the Cisco WLC queries a RADIUS server following the RADIUS Compatibility mode, if one is configured.

- Radius Compatibility Mode—Select the required RADIUS Compatibility Mode for MAC filtering:
  - Cisco ACS—In the RADIUS access-request packet, the username and password are the client MAC address.
  - Free RADIUS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the shared secret between the Cisco WLC and that RADIUS server.

Note The shared secret is the phrase that you entered when configuring the RADIUS server on the Cisco WLC.

Note Cisco ACS supports the free RADIUS compatibility mode.

  - Other—In the RADIUS access-request packet, the username is the client MAC address, but the password is not sent in the RADIUS access-request packet.
- Choose the required MAC delimiters for MAC filtering. The MAC delimiters can be a colon (xx:xx:xx:xx:xx:xx), hyphen (xx-xx-xx-xx-xx-xx), single hyphen (xxxxxx-xxxxxx), or none (xxxxxxxxxxxx), as required by the RADIUS server.

This page lists the current local MAC filters:

- MAC Address—Client MAC address.
- Profile Name—Profile name to which the client has access.
- Interface—Interface name as defined in the Interfaces page.
- IP Address—IP address.
- Description—Description of the local MAC filter.

You can perform the following actions:

- Click the MAC address to change a current local MAC filter definition on the Editing MAC Filters page.
- Click the blue arrow adjacent the desired filter and choose **Remove** to remove a current local MAC filter.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **New** to add a new client by the MAC address (Adding MAC Filters).

Adding MAC Filters

Choose **SECURITY > AAA > MAC Filtering** and then click **New** to navigate to the MAC Filtering > New page.

This page enables you to add a client by the MAC address:

- MAC Address—Client MAC address that you can specify.
- Profile Name—Profile name to which the client has access.

- Description—Client description that you can specify.
- IP Address—IP address of the client.
- Interface Name—Associated interface name, as defined in the Interfaces page.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing MAC Filters

Choose **SECURITY > AAA > MAC Filtering** and then click a MAC address to navigate to the MAC Filtering > Edit page.

This page enables you to change a MAC filter definition for an existing client MAC address.

- MAC Address—Read-only field that displays the client MAC address.
- Profile Name—Profile name to which the client has access from the drop-down list.
- IP Address—Client IP address that you can specify.
- Interface Name—Associated Interface Name, as defined in the Interfaces page.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Disabled Clients

Choose **SECURITY > AAA > Disabled Clients** to navigate to the Disabled Clients page.

This page presents a summary of the clients who are prevented (manually barred by the MAC address) from accessing to network services.

This page displays the following information:

- Search by MAC Address—MAC address that you can specify to search for a disabled client. Click **Search** to search for a disabled client.
- MAC Address—Disabled client MAC address.
- Description—Description of the disabled client.

You can perform the following actions:

- Click the MAC address to open the Disabled Client > Edit page.
- Click the blue arrow adjacent the desired client and choose **Remove** to enable a client that was formerly disabled.

Click **New** to manually disable a client (see Adding Disabled Clients for more information).

Adding Disabled Clients

Choose **SECURITY > AAA > Disabled Client** and then click **New** or **MONITOR > Clients** then click **Disable** to navigate to the Disabled Client > New page.

This page enables you to disable a client by its MAC address.

- MAC Address—Disabled client MAC address.

- Description— Client description of the client you want to disable.

Note When you enter a client MAC address to be disabled, the operating system checks that the MAC address is not one of the known Local Net clients (Local Net Users), Authorized clients (MAC Filtering), or Local Management users (Local Management Users) MAC addresses. If the entered MAC address is on one of these three lists, the operating system does not allow the MAC address to be manually disabled.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing Disabled Clients

Choose **SECURITY > AAA > Disabled Clients** and then click **Edit** to navigate to the Disabled Client > Edit page.

This page enables you to change the client description, based on the client MAC address that prevents a client from accessing the network.

- MAC Address—Disabled client MAC address.
- Description—Description of the disabled client.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

User Policies

Choose **SECURITY > AAA > User Login Policies** to navigate to the User Policies page.

This page enables you to specify the maximum number of concurrent logins for a single username, 0 (unlimited) through eight.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

AP Policies

Choose **SECURITY > AAA > AP Policies** to navigate to the AP Policies page.

This page enables you to set policies that help in the authorization of access points. Access points are authorized against AAA and/or a certificate.

This table describes the policy configuration parameters.

Table 6-5 Policy Configuration Parameters

Parameter	Description
Accept Self Signed Certificate (SSC)	Check box that you can select if you want the access point to accept self-signed certificates (SSCs).
Accept Manufactured Installed Certificate (MIC)	Check box that you can select if you want the access point to accept manufactured installed certificates (MICs).
Accept Local Significant Certificate (LSC)	Check box that you can select if you want the access point to accept local significant certificate (LSC).
Authorize MIC APs against auth-list or AAA	Check box that you can select if you want the access points to be authorized against AAA.
Authorize LSC APs against auth-list	Check box that you can select if you want the access points to be authorized against a local significant certificate.

Note Before you can accept an LSC, you must enable LSC on the Cisco WLC. See the Local Significant Certificates page for information on enabling LSC on the Cisco WLC.

To delete an access point from the authorization list, click the blue arrow adjacent the desired access point and choose **Remove**.

Search by MAC

You can search the AP Authorization List by MAC address.

Enter the MAC address as six two-digit hexadecimal numbers separated by colons (for example, 01:23:45:67:89:AB) and click **Search**. The AP Authorization Details page is displayed.

Adding an AP to Authorization List

To add an access point to the authorization list of a Cisco 4100 Series Wireless LAN Controller, follow these steps:

Step 1 Click **Add** to display the Add AP to Authorization List area.

Step 2 In the MAC Address text box, enter the MAC address of the AP.

Step 3 From the Certificate Type drop-down list, choose **MIC**.

Step 4 Click **Add**.

To add an AP to the authorization list of a Cisco 2000 Series Wireless LAN Controller or Cisco 4400 Series Wireless LAN Controller, follow these steps:

Step 1 Click **Add** to display the Add AP to Authorization List area.

Step 2 In the MAC Address field, enter the MAC address of the AP.

Step 3 From the Certificate Type drop-down list, choose **MIC**, **SSC**, or **LSC**.

Step 4 In the SHA1 Key Hash **text box,** enter the SHA1 key hash in hexadecimal format**.**

Note **The SHA1 Key Hash option is displayed only if you have chosen** SSC **as the certificate type in the previous step.**

Step 5 Click **Add AP to AuthList**.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Password Policies

Choose **SECURITY > AAA > Password Policies** to navigate to the Password Policies page.

This page enables you to enforce strong password checks on newly created passwords for additional management users of Cisco WLC and access point. The following are the requirements enforced on the new password:

- When the Cisco WLC is upgraded from old version, all the old passwords are maintained as it is, even though the passwords are weak. After the system upgrade, if strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
- Depending on the settings done in the Password Policy page, the local management and access point user configuration is affected.

This table describes the password policy parameters.

Table 6-6 Password Policy Parameters

Parameter	Description
Password Policies —Local Management User and AP	
Password must contain characters from at least three different classes	Check box that you can select if you want your password to contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
No character can be repeated more than three times consecutively	Check box that you enable if you do not want any character in the new password to be repeated more than three times consecutively.
Password cannot be default words such as cisco, admin	Check box that you can select if you do not want the password to contain words such as Cisco, ocsic, admin, nimda, or any variant obtained by changing the capitalization of letters or by substituting 1, |, or ! or substituting 0 for o, or substituting $ for s.

Table 6-6 Password Policy Parameters

Parameter	Description
Password cannot contain username or reverse of username	Check box that you can enable if you do not want the password to contain a username or the reverse letters of a username.
Password position check	Check box that you can enable to verify a four-character change from the old password.
Password case digit check	Check box that you can enable to verify if all four combinations (lower, upper, digits) or special characters are there in the password.
Strong password minimum length	Minimum length of the password.
Strong password minimum upper case characters	Minimum number of upper-case characters that are required in the password.
Strong password minimum lower case characters	Minimum number of lower-case characters that are required in the password.
Strong password minimum digits	Minimum number of digits that are required in the password.
Strong password minimum special characters	Minimum number of special characters that are required in the password.
Management User	
Management User Lockout Enable	Check box that you can select to lock out a management user when the number of successive failed attempts exceeds the Management User Lockout Attempts. When disabled, this option unlocks the management user who was locked out.
Management User Lockout Attempts	Number of successive incorrect password attempts after which the management user is locked.
Management User Lockout Time	Amount of time, in seconds, after lockout attempts when the management user is locked.
Management User Password Lifetime	Number of days before the management user requires a change of password due to the age of the password.
SNMPv3 User	
SNMP User Lockout Enable	Check box that you can select to lock out an SNMP user when the number of successive failed attempts exceeds the SNMP User Lockout Attempts. When disabled, this option unlocks the SNMP user who is locked out.
SNMP User Lockout Attempts	Number of successive incorrect password attempts after which an SNMP user is locked.
SNMP User Lockout Time	Amount of time, in seconds, after lockout attempts when an SNMP user is locked.
SNMP User Password Lifetime	Number of days before an SNMP user requires a change of password due to the age of the password.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

General (Local EAP)

Choose **SECURITY > Local EAP > General** to navigate to the General page. This page enables you to specify timeout values for local EAP.

This table describes the local EAP parameters.

Table 6-7 Local EAP Parameters

Parameter	Description
Local Auth Active Timeout (in secs)	Amount of time (in seconds) that the Cisco WLC attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.
Identity Request Timeout (in secs)	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 1 second.
Identity request Max Retries	Maximum number of times that the Cisco WLC attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.
Dynamic WEP Key Index	Key index used for dynamic wired equivalent privacy (WEP). The default setting is 0.
Request Timeout (in secs)	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 1 second.
Request Max Retries	Maximum number of times that the Cisco WLC attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.
Max-Login Ignore Identity Response	Number of devices that you can be connected to the Cisco WLC with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same Cisco WLC. The default value is enabled.
EAPOL-Key Timeout	Amount of time (in seconds) in which the Cisco WLC attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.
EAPOL-Key Max Retries	Maximum number of times that the Cisco WLC attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Local EAP Profiles

Choose **SECURITY > Local EAP > Profiles** to navigate to the Local EAP Profiles page.

Note Local EAP Profiles is not supported on AP602 OEAP.

This page lists any local EAP profiles that you have configured and specifies their EAP types. You can create up to 24 local EAP profiles. To remove an existing profile, click the blue arrow adjacent the desired profile and choose **Remove**.

This page displays the following information:

- Profile Name—Profile name.
- LEAP—Check box indicating if Local EAP is enabled. The default is disabled.
- EAP-FAST—Check box indicating if EAP-FAST is enabled. The default is disabled.
- EAP-TLS—Check box indicating if EAP-TLS is enabled. The default is disabled.
- PEAP—Check box indicating if PEAP is enabled. The default is disabled.

Click **New** to create a new local EAP profile.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Adding Local EAP Profiles

Choose **SECURITY > Local EAP > Profiles** and then click **New** to navigate to the Local EAP Profiles > New page.

This page enables you to create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients. This page allows you to modify the following settings:

- Profile Name—Name (up to 63 alphanumeric characters; do not include spaces) for your new profile.

After you create a profile, you can edit the parameters from the Editing Local EAP Profiles page.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing Local EAP Profiles

Choose **SECURITY > Local EAP > Profiles** and then click on the profile name to navigate to the Local EAP Profiles > Edit page.

This page enables you to edit a local EAP profile used for authentication:

- LEAP.
- EAP-FAST.

- EAP-TLS.
- PEAP—EAP type used for local authentication. Both PEAPv0/EAP-MSCHAPv2 and PEAPv1/EAP-GTC are enabled on the Cisco WLC.
- Local Certificate Required—Setting if you use EAP-FAST and want the device certificate on the Cisco WLC to be used for authentication. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.
- Client Certificate Required—Setting if you use EAP-FAST and want the wireless clients to send their device certificates to the Cisco WLC in order to authenticate or if you chose EAP-TLS and the client is using a certificate that is generated by a CA. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected. The default is disabled.
- Certificate Issuer—Certificates that will be sent to the client, either from Cisco or from another Vendor. The default setting is Cisco.
- Check Against CA Certificates—Setting that you use if you want the incoming certificate from the client to be validated against the CA certificates on the Cisco WLC. The default is enabled.
- Verify Certificate CN Identity—Setting that you use if you want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the Cisco WLC. You must enable this setting when you use an LDAP server as backup database. The default is disabled.
- Check Certificate Date Validity—Setting that you use if you want the Cisco WLC to verify that the incoming device certificate is still valid and has not expired. The default is enabled.

Note Certificate date validity is checked against the current UTC (GMT) time that is configured on the Cisco WLC. The time zone offset will be ignored.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

EAP-FAST Method Parameters

Choose **SECURITY > Local EAP > EAP-FAST Parameters** to navigate to the EAP-FAST Method Parameters page.

This page enables you to configure the following EAP-FAST settings if you configured an EAP-FAST profile from the Adding Local EAP Profiles page:

- Server Key (in hex)—Key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Key that you reenter (in hexadecimal characters).
- Time to Live for the PAC—Number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.
- Authority ID (in hex)—Authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
- Authority ID Information—Authority identifier of the local EAP-FAST server in text format.
- Anonymous Provision—Setting if you want to enable anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned. Disable this feature when you use EAP-FAST with certificates. The default is enabled.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Authentication Priority

Choose **SECURITY > Local EAP > Authentication Priority** to navigate to the Priority Order > Local-Auth page.

This page enables you to specify the order in which user credentials are retrieved from the back-end database servers.

Highlight the desired database from the left User Credentials box.

Use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right User Credentials box.

Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP back-end database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP back-end database.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Priority Order of Management Users

Choose **Security > Priority Order > Management User** to navigate to the Priority Order > Management User page.

This page enables you to specify the order of authentication when multiple databases are configured:

- Authentication Priority—Choose either **Radius** or **TACACS+** to specify which server has priority over the other when the Cisco WLC attempts to authenticate.

  By default, the local database is always queried first. If the username is not found, the Cisco WLC switches to the TACACS+ server if configured for TACACS+ or to the RADIUS server if configured for RADIUS. The default setting is local and then RADIUS.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Local Significant Certificates

Choose **SECURITY > Certificate > LSC** to navigate to the Local Significant Certificates page.

This page enables you to enable local significant certificates (LSCs) on the Cisco WLC.

Prior to release Cisco WLC 7.0, MAPs supported only the Manufactured Installed Certificate (MIC) for authentication and association with the Cisco WLC. Starting with this release, you can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, validity periods, restrictions, and usages on the

generated certificates. After these customer-generated or locally significant certificates (LSCs) are present on the APs and Cisco WLCs, the devices start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the Cisco WLC 5.2 release and later releases and extended the support for mesh APs as well from the Cisco WLC 7.0 release.

The LSC is installed on access points and Cisco WLCs. You need to provision the LSC first on the Cisco WLC, which should be configured to communicate with a CA server.

Note Only external dedicated CA servers are supported in this release.

The access point gets a signed X.509 certificate by sending a certRequest to the Cisco WLC. The Cisco WLC acts as a CA proxy and receives the certRequest signed by the CA for the access point.

Note Access points that are configured in bridged mode are not supported.

General Tab

This table describes the LSC parameters.

Table 6-8 General Tab Parameters

Parameter	Description
Certificate Type	Certificates that are added to the Cisco WLC's CA certificate database. To add the CA certificate or device certificate into the Cisco WLC's CA certificate database, click the blue arrow adjacent the desired certificate type and choose **Add**. To remove a certificate, click the blue arrow adjacent the desired certificate type and choose **Remove**.
Enable LSC on Controller	Check box to enable LSC on the Cisco WLC. The default is disabled.

Table 6-8 General Tab Parameters

Parameter	Description
CA Server URL	URL of the CA server in the following format: **http://***url***:***port***/***path* The *url* can be either a domain name or an IP address.
Params	Parameters for the device certificate. The keysize is a value from 384 to 2048 (in bits); the default value is 2048. The following parameters are available: • Country Code—Enter the country code. The country code is a three byte string. • State—Enter the state. This value can be up to 64 bytes. • City—Enter the city. The value can be up to 64 bytes. • Organization—Enter the organization. The value can be up to 64 bytes. • Department—Enter the department. The value can be up to 64 bytes. • Email—Enter a valid e-mail address. • Key Size—Enter the key size. The range includes 360 to 2048 bits. The default is 2048.

AP Provisioning Tab

This table describes the AP provisioning tab parameters.

Table 6-9 AP Provisioning Tab Parameters

Parameter	Description
Enable	Parameter that enables you to provision the LSC on the access point. Click **Update** to enable an LSC on the access point. The default is disabled.
Number of attempts to LSC	Number of times that the access point attempts to join the Cisco WLC using an LSC before the access point reverts to the default certificate (MIC or SSC). The valid range is 0 to 255, and the default value is 3. If you set the number of retries to a nonzero value and the access point fails to join the Cisco WLC using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the Cisco WLC using an LSC, the access point does not attempt to join the Cisco WLC using the default certificate. **Note** If you are configuring an LSC for the first time, we recommend that you configure a nonzero value.

Table 6-9 AP Provisioning Tab Parameters

Parameter	Description
AP Ethernet MAC Addresses	Ethernet MAC address of the access point.
MAC Address	Access point MAC addresses.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Self Significant Certificates

Choose **SECURITY > Certificate > SSC** to navigate to the Self Signed Certificates page.

This page enables you to view the Self Signed Certificate of the virtual Cisco WLC and enable hash validation of the SSC certificate by the access points.

Virtual Cisco WLCs use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical Cisco WLCs.

You can select the **Enable SSC Hash Validation** check box to allow an AP to validate the SSC certificate of the virtual Cisco WLC. When an AP validates the SSC certificate, it checks if the hash key of the virtual Cisco WLC matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the Cisco WLC and restarts the discovery process.

By default, hash validation is enabled. Therefore, an AP must have the virtual Cisco WLC hash key in its flash before associating with the virtual Cisco WLC. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the run state.

To configure the hash key of the virtual Cisco WLC, choose **CONTROLLER > Mobility Management > Mobility Groups**, click **New** and enter the IP address, MAC address, mobility group name, and hash key of the virtual Cisco WLC.

APs can associate with a physical Cisco WLC, download the hash keys and then associate with a virtual Cisco WLC. If the AP is associated to a physical Cisco WLC, if hash validation is disabled, it joins any virtual Cisco WLC without hash validation.

Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** to navigate to the Access Control Lists page.

This page enables you to view current access control lists (ACLs) that are similar to standard firewall access control lists.

Note You can define up to 64 ACLs with up to 64 rules (filters) per ACL.

- Enable Counters—Check box that you can select to see if packets are hitting any of the ACLs that are configured on your Cisco WLC. The default is unselected.

Note ACL counters are available only on the following Cisco WLCs: Cisco 5500 Series Controller, Cisco 4400 Series Controller, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

- Name—ACL name to open the Editing Access Control Lists page.
- Type—IPv4 or IPv6 ACL.

To remove an existing ACL, click the blue arrow adjacent the desired ACL and choose **Remove**.

To clear the counters for an ACL, click the blue arrow adjacent the desired ACL and choose **Clear Counters**.

Guidelines

- Pre-auth ACL must have the following two rules for proper operation:
  - One allowing traffic to the DNS server.
  - One allowing traffic from the DNS server.
- Beginning in Cisco WLC Release 7.4 and later, DNS traffic is handled based on deny rules defined in the WLAN Pre-Auth ACL.
  - If no Pre-Auth ACL is configured and applied, then all DNS packets are allowed to pass to any server.
  - If Pre-Auth ACL is configured, but no matching deny rule is configured, then allow all DNS packets to pass to any server.
  - If Pre-Auth ACL is configured with a rule to allow DNS traffic to a given server and a rule configured to drop all traffic based on protocol/IP address, then allow DNS to one server only and block all other DNS traffic.

Click **New** to add a new ACL (see the Adding Access Control Lists topic).

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Adding Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** and then click **New** to navigate to the Access Control Lists > New page.

- Access Control List Name— ACL name that you can specify.
- Access Control List Type—ACL type as either IPv4 or IPv6.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing Access Control Lists

Choose **SECURITY > Access Control Lists > Access Control Lists** and then click on the ACL name to navigate to the Access Control Lists > Edit page.

This page enables you to view and/or change an ACL definition, which is similar to standard firewall ACLs.

Note You can define up to 64 ACLs with up to 64 rules (filters) per ACL.

To remove a rule, click the blue arrow adjacent the desired ACL and choose **Remove**.

This table describes the current rule parameters.

Table 6-10 Current Rule Parameters

Parameter	Description
Access List Name	Name of the ACL.
Deny Counters	Number of times that packets have matched the explicit deny ACL rule. **Note** You must enable ACL counters on the Access Control Lists page to enable the Deny Counters.
Sequence	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6. **Note** Click the sequence number to modify the rule (See the Editing Access Control Lists Rules topic).
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.

Table 6-10 Current Rule Parameters

Parameter	Description
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client), or Outbound (to client).
Number of Hits	Number of times that packets have matched an ACL rule. **Note** This field appears only if you enabled ACL counters on the Access Control Lists page.

When the ACL contains one or more ACL rule, click the sequence number to modify the rule on the Editing Access Control Lists Rules page.

Click **Add New Rule** to add a new rule to an existing ACL.

Editing Access Control Lists Rules

Choose **SECURITY > Access Control Lists > Access Control Lists,** click the ACL name. Click the sequence number of the rule that you want to change to navigate to the Access Control Lists > Rules > Edit page.

This page enables you to change an ACL rule definition.

Note The operating system enables you to define up to 64 ACLs with up to 64 rules (filters) per ACL.

This table describes the rule parameters.

Table 6-11 Rule Edit Parameters

Parameter	Description
Sequence	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns Sequence 6 to 7 and sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv6 addresses, the prefix length is also displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)

Table 6-11 Rule Edit Parameters

Parameter	Description
Source Port/Destination Port	Source/Destination Ports for this ACL: • Any • HTTP • HTTPS • Telnet • RADIUS • DHCP Server • DHCP Client • DNS • L2TP • PPTF Control • SMTP • SNMP • LDAP • Kerberos • NetBIOS NS • NetBIOS DS • NetBIOS SS • MS Dir Server • Other • Port Range
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Direction	Any, Inbound (from client), or Outbound (to client).
Action **Note** The default filter is to deny all access unless a rule explicitly permits it.	Deny or Permit.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Adding Access Control Lists Rules

Choose **SECURITY > Access Control Lists > Access Control Lists,** click the ACL name of an existing ACL, and then click **Add New Rule** to navigate to the Access Control Lists > Rules > New page.

This table describes the new rule parameters.

Table 6-12 New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA's Website)
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.

Table 6-12 New Rule Parameters

Parameter	Description
Direction	Any, Inbound (from client), or Outbound (to client).
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

CPU Access Control Lists

Choose **SECURITY > Access Control Lists > CPU Access Control Lists** to navigate to the CPU Access Control Lists page.

This page enables you to configure and apply an Access Control List (ACL) to the Cisco WLC CPU to control traffic to the CPU.

This table describes the CPU ACL parameters.

Table 6-13 CPU ACL Parameters

Parameter	Description	Default
Enable CPU ACL	Designated ACL that you can enable to control the IPv4 traffic to the Cisco WLC CPU.	Unselected (disabled)
ACL Name	Previously configured ACL. To configure an ACL, see Adding Access Control Lists. If you choose **none** while the CPU ACL feature is enabled, an error message appears.	none
Enable CPU IPv6 ACL	Designated ACL that you can enable to control the IPv6 traffic to the Cisco WLC CPU.	Unselected (disabled)
IPv6 ACL Name	Previously configured ACL. To configure an ACL, see Adding Access Control Lists. If you choose **none** while the CPU ACL feature is enabled, an error message appears.	none

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

FlexConnect ACLs

With FlexConnect ACLs, you can control access at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. Using the Cisco WLC, you can create FlexConnect ACLs and then configure the FlexConnect ACL with the WLAN using WLAN-ACL mapping. These are then pushed to the AP.

Choose **SECURITY > Access Control Lists > FlexConnect ACLs** to navigate to the FlexConnect ACLs page.

This page enables you to list the ACLs configured for FlexConnect access points. To remove a FlexConnect ACL, click the blue arrow adjacent the desired ACL and choose **Remove**.

Click **New** to add a new FlexConnect ACL.

Adding FlexConnect ACLs

Choose **SECURITY > Access Control Lists > FlexConnect ACLs** and click **New**. The FlexConnect ACL > New page enables you to create an ACL. Enter the FlexConnect ACL name in the Access Control List Name text box.

Click **Apply** to create the new FlexConnect ACL with the configured name.

Editing Access Control List

Choose **SECURITY > FlexConnect ACLs** and click the ACL name of an existing ACL to open the Access Control List > Edit page.

This table describes the FlexConnect ACL parameters.

Table 6-14 FlexConnect Access Control List Parameters

Parameter	Description
General	
Access List Name	Name of the FlexConnect ACL.
Seq	Up to 64 rules can be defined for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and sequence 5 to 6.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.
Source IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination IP/Mask	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.

Table 6-14 FlexConnect Access Control List Parameters

Parameter	Description
Protocol	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)
Source Port	Any or IP address and netmask.
Dest Port	Any or IP address and netmask.
DSCP	Any or Specific (from 0 to 63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service (QoS) across the Internet.

Click **Add a New Rule** to add a new rule to an existing ACL .

Adding FlexConnect ACL Rules

Choose **SECURITY > Access Control List > FlexConnect ACLs** to navigate to the FlexConnect Access Control Lists page. Click an ACL name to open the **Access Control List > Edit** page and click **Add New Rule** button to create a new ACL Rule.

This table describes the FlexConnect ACL new rule parameters.

Table 6-15 FlexConnect ACL New Rule Parameters

Parameter	Description
Sequence	Operator that can define up to 64 rules for each ACL. The rules for each ACL are listed in a contiguous sequence from 1 to 64. If rules 1 through 4 are already defined and you add rule 29, it is be added as rule 5. **Note** If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 6 to 7 and Sequence 5 to 6.
Source	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Destination	Any or IPv4 or IPv6 address and netmask. For IPv4 addresses, the netmask is displayed and for IPv6 addresses, the prefix length is displayed.
Protocol **Note** When you select some of these protocols, one or more additional data entry fields open up. Enter the port number in a single data entry field, or enter the source and destination port when there are two data entry fields.	Protocol to use for this ACL: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol (For IPv4 ACL) • ICMPv6-Internet Control Message Protocol (For IPv6 ACL) • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • OSPF—Open Shortest Path First • Other—Any other IANA protocol (Go to IANA Website)

Table 6-15 FlexConnect ACL New Rule Parameters

Parameter	Description
DSCP	Any or Specific (from 0–63) Differentiated Services Code Point (DSCP). A packet header code that can be used to define quality of service across the Internet.
Action	Deny or Permit. **Note** The default filter is to deny all access unless a rule explicitly permits it.

Rogue Policy

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > General** to navigate to the Rogue Policies page.

This page enables you to select global parameters for rogue access point detection.

Note The Cisco 5500 Series Wireless Controllers support up to 2000 rogues (including acknowledged rogues); the Cisco 4400 Series Wireless Controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues, and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each Cisco WLC limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

Rogue Location Discovery Protocol

The Cisco WLC continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the Cisco WLC discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

You can configure the Cisco WLC to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The later option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure the Cisco WLC to use RLDP on all access points, the Cisco WLC always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS) on a monitor mode access point.

Rogue Policies

This table describes the rogue policy parameters.

Table 6-16 Rogue Policy Parameters

Parameter	Description
Rogue Detection Security Level	Rogue detection security level that you can select: • Low—Basic rogue detection for small-scale deployments. Auto containment is not supported for this security level. • High—Basic rogue detection and auto containment for medium-scale or less critical deployments. RLDP is disabled for this security level. • Critical—Basic rogue detection, auto containment, and RLDP for highly critical deployments. • Custom—You can configure the rogue policy parameters. Each security level has preset configurations for each rogue detection security level.
Rogue Location Discovery Protocol	RLDP options that you can specify: • Disable—Disables RLDP. This is the default value. If the rogue detection security level is Low, RLDP is disabled. • Monitor Mode APs—Enables RLDP only on monitor mode access points. If the rogue detection security level is High, the RLDP mode is set to Monitor Mode APs mode. • All APs—Enables RLDP on all the access points (monitor mode and data). If the rogue detection security level is Critical, the RLDP mode is All APs. **Note** If you configure the Cisco WLC to use RLDP on all the access points, the Cisco WLC always chooses the monitor access point for the RLDP operation if a monitor access point and a local (data) access point are both nearby.
Expiration Timeout for Rogue AP and rogue Client Entries	Number of seconds after which the rogue access point will be taken off the list. The range is from 240 to 3600 and the default value is 1200. The expiration timeout for rogue AP and client entries for each rogue detection security levels are as follows: • Low—240 • High—1200 • Critical—10
Validate rogue clients against AAA	Validation that you can enable using the AAA server or local database to validate if rogue clients are valid clients. The default is disabled. If DNS query is enabled (**SECURITY > AAA > RADIUS > DNS**), the validation occurs using the RADIUS list from the DNS server.
Validate rogue clients against MSE	Validation that you can enable using MSE to validate if rogue clients are valid clients. The default is disabled. You cannot validate rogue clients against MSE and AAA at the same time.

Table 6-16 Rogue Policy Parameters

Parameter	Description
Detect and report Ad-Hoc Networks	Ad-hoc rogue detection and reporting that you can enable or disable. The default value is enabled.
Rogue Detection Report Interval (10 to 300 Sec)	Time interval, in seconds, at which the APs should send the rogue detection report to the Cisco WLC. The default value is 10. The rogue detection report interval for each rogue detection security levels are as follows: • Low—60 • High—30 • Critical—10 **Note** This feature is applicable to APs that are in monitor mode only.
Rogue Detection Minimum RSSI (–70 dBm to –128 dBm)	Minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. The default value is –128 dBm. The rogue detection minimum RSSI for each rogue detection security levels are as follows: • Low— –80 dBm • High— –128 dBm • Critical— –128 dBm **Note** This feature is applicable to all the AP modes.
Rogue Detection Transient Interval	Time interval, in seconds, at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the Cisco WLC. The APs filter the transient rogues that are active for a very short period and are then silent. The range is from 120 to 1800. The rogue detection transient interval for each rogue detection security level is as follows: • Low—120 • High—300 • Critical—600 **Note** This feature applies to APs that are in monitor mode only.
Rogue Client Threshold	Threshold rogue client count after which a trap is sent from the Cisco WLC. Enter 0 to disable the feature. The range is from 1 to 256. The default is disabled. The rogue client threshold for each rogue detection security levels is 0.
Rogue Containment Automatic Rate Selection	Check box that you can select to enable automatic rate selection for rogue containment.

This table describes the details of rogue containment automatic rate selection.

RSSI (dBm)	802.11b/g Tx Rate (Mbps)	802.11a Tx Rate (Mbps)
–74	1	6
–70	2	12
–55	5.5	12
< –40	5.5	18

Auto Contain

If you want the Cisco WLC to automatically contain certain rogue devices, check the following check boxes. Otherwise, leave the check boxes unselected, which is the default value.

Caution When you enable any of these parameters, the following warning appears:

"Using this feature may have legal consequences. Do you want to continue?"

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

This table describes the auto contain parameters.

Table 6-17 Auto Contain Parameters

Parameter	Description
Auto Containment Level	Drop-down list from which you can choose the rogue auto containment level from 1 to 4. You can choose up to four APs for auto containment when a rogue is moved to a contained state through any of the auto containment policies. You can also choose Auto for automatic selection of the number of APs used for auto containment. The Cisco WLC chooses the required number of APs based on the RSSI for effective containment. The RSSI value associated with each containment level is as follows: • 1—0 to –55 dBm • 2— –75 to –55 dBm • 3— –85 to –75 dBm • 4—Less than –85 dBm
Auto Containment only for Monitor mode APs	Check box that you can select to enable the monitor mode APs for auto containment. The default is disabled.

Table 6-17 Auto Contain Parameters

Parameter	Description
Auto Containment on FlexConnect Standalone	Check box that you can select to enable auto containment on FlexConnect APs in the standalone mode. The default is disabled. When the FlexConnect APs are in the standalone mode, you can enable only the Using our SSID or AdHoc Rogue AP auto containment policies. The containment stops after the standalone AP connects back to the Cisco WLC.
Rogue on Wire	Check box that you enable to automatically contain the rogues that are detected on the wired network. The default is disabled.
Using our SSID	Check box that you enable to automatically contain those rogues that are advertising your network's SSID. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled.
Valid client on Rogue AP	Check box that you enable to automatically contain a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled.
AdHoc Rogue AP	Check box that you enable to automatically contain ad-hoc networks detected by the Cisco WLC. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a network is detected. The default is disabled.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** to navigate to the Rogue Rules page.

This page enables you to add new rogue rules and to change the priority of the rogue rules.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

This table describes the rogue rules parameters.

Table 6-18 Rogue Rules Parameters

Parameter	Description
Rule Name	Name of the rogue rule. You can configure a maximum of 64 rogue rules.
Type	Whether the rule is Friendly, Malicious, or Custom.
Status	Status of the rule: enabled or disabled.

Table 6-18 Rogue Rules Parameters

Parameter	Description
Notify	Type of notification upon rule match that is one of the following: • All—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure. • Global—Notifies only a trap receiver such as Cisco Prime Infrastructure. • Local—Notifies only the Cisco WLC. • None—No notifications are sent.
State	State of the rogue access point after a rule match. It can be one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. The Cisco WLC forwards an immediate alert to the system administrator for further action. • Contain—The Cisco WLC contains the offending device so that its signals no longer interfere with authorized clients. • Internal—The unknown access point is inside the network and poses no threat to WLAN security. The Cisco WLC trusts this rogue access point. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. The Cisco WLC acknowledges the presence of this rogue access point. For example, the access points that belongs to a neighboring coffee shop are external rogue access points. • Delete—The rogue access point is deleted from the database when the rogue rule is applied to the rogue access point.
Match Operation	Click the **Match All** radio button to enable the rogue rule only when a detected rogue access point meets all the conditions of the rule. Click the **Match Any** radio button to enable the rule when any of the conditions are met.

Table 6-18 Rogue Rules Parameters

Parameter	Description
Enable Rule	Check box that you can select to enable a rogue rule.
Condition	Drop-down list from which you can choose one or more of the following rogue rule conditions: • SSID—Requires that a rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User-Configured SSID text box, and click **Add SSID**. You can configure up to 25 SSIDs per rogue rule. • RSSI—Requires that a rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, the access point is classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI text box. The range is from –95 to –50 dBm (inclusive), and the default value is 0 dBm. • Duration—Requires that a rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds. • Client Count—Requires that a minimum number of clients be associated to a rogue access point. For example, if the number of clients associated to a rogue access point is greater than or equal to the configured value, the access point is classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients text box. The range is from 1 to 10 (inclusive), and the default value is 0. • No Encrytion—Requires that a rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. • Managed SSID—Requires that a rogue access point's managed SSID (the SSID configured for the WLAN) be known to the Cisco WLC. No further configuration is required for this option. • Substring SSID—Requires that a rogue access point have a substring of a user-configured SSID. If you choose this option, enter the substring of the SSID in the User-Configured SSID text box. For example, if you have an SSID as ABCDE, you can specify the substring as ABCD or ABC. You can classify multiple SSIDs with matching patterns. You can configure up to 25 SSID substrings per rogue rule.

- Click **Add Rule** to add a new rogue rule:
  a. Enter a rule name. The rule name cannot contain any spaces.
  b. Choose the rule type (**Friendly** or **Malicious**) to classify rogue access points that match this rule as friendly or malicious.
  c. Click **Add**.
- Click the rule name to open the Editing Rogue Rules page.

Click **Add Rule** to add a new rogue rule.

Click **Change Priority** to change the order in which rogue classification rules are applied.

Editing Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** and click the rule name to navigate to the Rogue Rule > Edit page.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

This page enables you to edit the rogue rule settings.

This table describes the rogue rule parameters.

Table 6-19 Rogue Rule Parameters

Parameter	Description
Rule Name	Name of the rogue rule.
Type	Whether the rule is Friendly, Malicious, or Custom.
Notify	Type of notification upon rule match that is one of the following: • All—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure. • Global—Notifies only a trap receiver such as Cisco Prime Infrastructure. • Local—Notifies only the Cisco WLC. • None—No notifications are sent.

Table 6-19 Rogue Rule Parameters

Parameter	Description
State	State of the rogue access point after a rule match. It can be one of the following: • Alert—The unknown access point is not in the neighbor list or in the user-configured friendly MAC list. The Cisco WLC forwards an immediate alert to the system administrator for further action. • Contain—The Cisco WLC contains the offending device so that its signals no longer interfere with authorized clients. • Internal—The unknown access point is inside the network and poses no threat to WLAN security. The Cisco WLC trusts this rogue access point. For example, the access points in your lab network is an internal rogue access point. • External—The unknown access point is outside the network and poses no threat to WLAN security. The Cisco WLC acknowledges the presence of this rogue access point. For example, the access points that belongs to a neighboring coffee shop are external rogue access points. • Delete—The rogue access point is deleted from the database when the rogue rule is applied to the rogue access point.
Match Operation	Rule that you choose: • Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. • Match Any—(Default) If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.
Enable Rule	Rule that you enable or disable. The default is disabled.
Severity Score	Custom classification severity score. The range is from 1 to 100. This field appears only when you choose Custom rule type.
Classification Name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.This field appears only when you choose Custom rule type.

Conditions

To add conditions to the rogue rule, select the condition from the drop-down list and click **Add Condition**.

This table describes the rogue rules condition parameters.

Table 6-20 Rogue Rules Condition Parameters

Parameter	Description
Time Duration (0 to 3600)	Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration field. The range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
Minimum RSSI (-95 to -50)	Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI field. The range is from –95 to –50 dBm (inclusive), and the default value is 0 dBm.
Minimum number of Rogue client (1-10)	Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients field. The range is from 1 to 10 (inclusive), and the default value is 0.
No Encryption	Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. **Note** Prime Infrastructure refers to this option as "Open Authentication."
Managed SSID[1]	Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the Cisco WLC. No further configuration is required for this option.
User configured SSID[1]	Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID field, and click **Add SSID**. You can add multiple SSIDs. To remove an SSID, select the SSID and click **Remove**.

1. The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

To remove a condition, click the blue arrow adjacent the desired condition and choose the **Remove** link.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Priority of Rogue Rules

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Rogue Rules** and click **Change Priority** to navigate to the Rogue Rules > Priority page.

This page enables you to change the order in which rogue classification rules are applied.

Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

Continue to move the rules up or down until the rules are in the desired order.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Friendly Rogues

Choose **SECURITY > Wireless Protection Policies > Rogue Policies > Friendly Rogue** to navigate to the Friendly Rogue page.

This page enables you to classify any rogue access points as friendly and add them to the friendly MAC address list.

To classify a rogue rule, follow these steps:

Step 1 In the MAC Address text box, enter the MAC address of the friendly rogue access point.

Step 2 Click **Apply** to commit your changes.

Step 3 Click **Save Configuration** to save your changes.

This access point is added to the Cisco WLC's list of friendly access points and appears on the **Friendly Rogue APs** page.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Standard Signatures

Choose **SECURITY > Wireless Protection Policies > Standard Signatures** to access the Standard Signatures page.

This page enables you to view standard signature information:

- Enable Check for All Standard and Custom Signatures—Check box to enable if you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled. The default is enabled. When the signatures are enabled, the access points joined to the Cisco WLC perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the Cisco WLC.

  If you unselect this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

- Precedence—Precedence Order Number.

- Name—Name of the signature.
- Frame Type—Type of frame, such as Management or Data.
- Action—Type of action to take, such as report.
- State—Whether the state is enabled or disabled.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”

Click the precedence order number to view more detailed information. See the Standard Signature Details topic.

Standard Signature Details

Choose **SECURITY > Wireless Protection Policies > Standard Signatures** to navigate to the Standard Signatures page. Click the precedence order number to access the Standard Signature > Detail page. This page enables you to view detailed signature information:

- Precedence—Precedence order number.
- Name—Name of the signature, such as Bcast deauth.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”
- Frame Type—Management or Data.
- Action—None or Report.
- Measurement Interval (sec)—Number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.
- Tracking—Tracking method used by the access points to perform signature analysis and report the results to the Cisco WLC. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.
- Signature Frequency—Number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.
- Signature MAC Frequency—Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.
- Quiet Time (secs)—Length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.
- State—Whether this signature to detect security attacks is enabled or disabled. The default value is enabled (or checked).

Patterns

- Offset—Offset, in bytes, from the start of the packet header or body based on the value of the preceding <offsetStart> where the pattern match operation is to be performed.

- Pattern—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.
- Mask—Mask is a hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.

Custom Signatures

Choose **SECURITY > Wireless Protection Policies > Custom Signatures** to access the Custom Signatures page.

- Enable Check for All Standard and Custom Signatures—Check box to enable or disable signatures (both standard and custom) whose individual states are set to Enabled to remain enabled. The default is enabled. When the signatures are enabled, the access points joined to the Cisco WLC perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the Cisco WLC.

  If you unselect this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.
- Precedence—Precedence Order Number.
- Name—Name of the custom signature.
- Frame Type—Frame type, such as Management, or data.
- Action—Type of action to take, such as report.
- State—Whether the state is enabled or disabled.
- Description—Text description of the signature.

Custom Signature Details

Choose **SECURITY > Wireless Protection Policies > Custom Signatures,** and then click **Detail** to access this page. This page enables you to view detailed signature information:

- Precedence—Precedence Order Number.
- Name—Name of the signature, such as Bcast deauth.
- Description—Text description of the signature, such as “Broadcast Deauthentication Frame.”
- Frame Type—Management or Data.
- Action—None or Report.
- Measurement Interval (sec)—Interval in seconds.
- Signature Frequency—Packet match frequency in packets/interval.
- Signature MAC Frequency—Packet match frequency in packets/interval.
- Quiet Time (secs)—Interval in seconds.
- State—Whether the state is enabled or disabled.

Signature Patterns

- Offset—Offset, in bytes, from the start of the packet header or body based on the value of the preceding <offsetStart> where the pattern match operation is to be performed.

- Pattern—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.
- Mask—Hexadecimal string that starts with '0x'. It must have an even number of ASCII characters. For example, 0xaabbcc is OK, but 0xaab is not.

Signature Events Summary

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary** to access the Signature Events Summary page.

This table describes the signature events summary parameters.

Table 6-21 Signature Events Summary Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
# Events	Number of attack event occurrences for that particular signature.

Click the signature type to view more detailed information. See the Signature Events Summary Details topic.

Signature Events Summary Details

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary**, and click the signature type to access the Signature Events Summary Details page.

This table describes the signature events summary parameters.

Table 6-22 Signature Events Summary Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
Source MAC Address	MAC address of the attacking client radio.
Track Method	Tracking method AP used to track the signature attacks per signature, source MAC, or both.
Frequency	Packet match frequency in packets/interval (50 per signature and 30 Per MAC tracking method).
# APs	Number of radio interfaces/APs on the channel that detected the attack.
Last Heard	Latest time stamp at which the radio interface/AP detected the attack.

Click **Detail** to view more detailed information. See the Signature Event Track Details topic.

Signature Event Track Details

Choose **SECURITY > Wireless Protection Policies > Signature Events Summary** and then click the Signature Type to access the Signature Event Track Details page.

This table describes the signature event detail parameters.

Table 6-23 Signature Event Detail Parameters

Parameter	Description
Signature Type	Management or data.
Precedence	Precedence order number.
Signature Name	Name of the standard or custom signature.
Source MAC Address	MAC address of the attacking client radio.
Track Method	Tracking method AP used to track the signature attacks per signature, source MAC, or both.
Frequency	Packet match frequency in packets/interval (50 per signature and 30 per MAC tracking method).
# APs	Number of radio interfaces/APs on the channel that detected the attack.
AP MAC Address	Radio MAC address of the AP that detected the attack.
AP Name	Hostname of the AP.
Radio Type	802.11a or 802.11g.
Channel	Radio channel number.
Last Reported by this AP	Time stamp at which the AP reported the attack earlier.

Client Exclusion Policies

Choose **SECURITY > Wireless Protection Policies > Client Exclusion Policies** to access the Client Exclusion Policies page.

This page enables you to configure the Cisco WLC to exclude clients under certain conditions:

- Excessive 802.11 Association Failures—Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11 Authentication Failures—Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11X Authentication Failures—Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—Clients are excluded if the IP address is already assigned to another device.
- Excessive Web Authentication Failures—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

AP Authentication

Choose **SECURITY > Wireless Protection Policies > AP Authentication** to access the AP Authentication Policy page.

This page enables you to set access point authentication policies:

When you enable the AP authentication feature, the access points sending RRM neighbor packets with different RF network names are reported as rogues.

When you enable Infrastructure Management Frame Protection (MFP), it is enabled globally for the Cisco WLC. You can enable or disable Infrastructure MFP validation for a particular access point (All APs Details) or protection for a particular WLAN (Editing WLANs) if MFP is enabled globally for the Cisco WLC.

- Protection Type—None, AP Authentication, or Management Frame Protection. Management Frame Protection is the default if AP Authentication was not previously configured and is the preferred method for authenticating access points.

Note This setting does not affect Client MFP, which is configured per WLAN.

- Alarm Trigger Threshold—AP Authentication sets the number of hits to be ignored from a foreign access point before an alarm is raised. The valid range is from 1 to 255; the default value is 255.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Management Frame Protection Settings

Choose **SECURITY > Wireless Protection Policies > Management Frame Protection** to navigate to the Management Frame Protection page.

General Parameters

Click **General** from the left navigation pane to access the Management Frame Protection Settings > General page.

This table describes the MFP general parameters.

Table 6-24 General Parameters

Parameter	Description
Management Frame Protection	Disabled/Enabled (globally). **Note** This MFP status represents the status of the Cisco MFP and not the status of 802.11w, introduced in Release 7.4
Controller Time Source Valid	True (time is set externally [for example, NTP]). False (time is set locally).

WLAN Parameters

Click **WLAN** from the left navigation pane to access the Management Frame Protection Settings > WLANs page.

This table describes the WLAN parameters.

Table 6-25 WLAN Parameters

Parameter	Description
WLAN-ID	Unique identifier.
WLAN Name	Unique identifier.
WLAN Status	Enabled/Disabled.
Infrastructure Protection	Enabled/Disabled. Shows if MFP infrastructure protection is enabled for individual WLANs.

Web Login Page

Choose **SECURITY > Web Auth > Web Login** to navigate to the Web Login page.

This page enables you to customize the content and appearance of the Login page for guest users and all others. It allows you to personalize the login page with a company logo, graphics, colors, type styles, a welcome message, any terms and conditions, and so on.

The login page is shown the first time that you access the WLAN if Web Authentication is turned on (under WLAN Security Policies). Cisco provides a default web login page that can be modified with any text-based HTML editor. However, the User Name and Password fields should not be changed, and the Submit method should be retained. After you create the customized web login page, you must make it into a tar file that contains the page code and any images desired, and then upload to the Cisco WLC through the TFTP server as a Webauth Bundle (see the Download File to Controller page).

Note For Cisco 5500 Series Wireless Controllers, and Cisco WLC network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under **Security Policies > Web Policy** on the Editing WLANs page.

This table describes the web login page parameters.

Table 6-26 Web Login Page Parameters

Parameter	Description
Web Authentication Type	Internal (Default); Customize (Downloaded); External (Redirect to external server). Enable this last option and enter the URL if you want to use a customized login page configured on your web server for web authentication, instead of the default web authentication page provided by the Cisco WLC. The maximum length is 254 characters. **Note** Your web server should be on a different network from the Cisco WLC service port network. If you are using a custom web-auth bundle that is served by the internal Cisco WLC web server, the page should not contain more than 5 elements (including HTML, CSS, and Images) because the internal Cisco WLC web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time (For example Firefox 4) if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection. If you have a complex custom web authentication module, we recommend that you use an external web-auth config on the Cisco WLC, where the full login page is hosted at an external web server. For more information, see the External Web Authentication topic.
Redirect URL after login	URL that you want the user to be redirected after a login. For example, you may enter your company's URL here and the users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page was served.
Headline	Login page headline. For example, "Welcome to Cisco Wireless Network." The maximum length is 127 characters.
Message	Login page message. For example, "Please enter your user name and password" or "This page will not be available from 1:00 Hrs to 2:00 today due to maintenance." The maximum length is 2047 characters.
External Web Server	IP address of the external web server if used.
Preview button	Ability to view either the default page, the customized web login page you created, or the landing page on the external server if that Web Auth option is chosen.
Apply button	Button that you click after previewing your web login page selection. If you have selected a customized (downloaded) page, you will be prompted to ensure that you have downloaded a customized web authentication bundle to the system (Cisco WLC) before applying the setting. If not, this selection fails.

Commands

- Preview—Views either the default page, the customized web login page you created, or the landing page on the external server if that Web Auth option is chosen.

- Apply—Selects a Customized (Downloaded) page, and displays a message asking you to make sure that you have downloaded a customized web authentication bundle to the system (Cisco WLC) before applying the setting. If you do not save, this selection fails.

External Web Authentication

The following steps describe how external web authentication works.

Step 1 When you open a web browser with a URL, it is verified for authentication. If it is not authenticated, the Cisco WLC forwards the request to the Cisco WLC web server to collect authentication details.

Step 2 The Cisco WLC web server then redirects you to the external web server URL that leads you to a login page. At this point, you are also allowed to access the Walled Garden sites (Walled Garden sites are a group of websites that users can browse before they are authenticated on to your wireless network).

Note If you are using an external web server with a Cisco 5500 Series Controller or a Cisco WLC network module, you must configure a preauthentication ACL on the WLAN for the external web server. This ACL should then be set as a WLAN preauthentication ACL under the Web Policy.

Step 3 The login request is sent back to the action URL of the Cisco WLC web server. The Cisco WLC web server submits the username and password for authentication.

Step 4 The Cisco WLC application initiates the RADIUS server request and authenticates you.

Step 5 If successful, the Cisco WLC web connects the client and the Cisco WLC web server forwards you to the configured redirect URL or to the initially requested URL.

Step 6 If user authentication fails, the Cisco WLC web server redirects you to the URL of the user login page.

Cisco Support for External Web Authentication

The Cisco support for external web authentication is as follows:

- External Web Authentication login URL—The Cisco WLC allows you to configure the login URL by using a flag to turn on the External Web Authentication mode. If this flag is configured, you are redirected to the customized login page instead of Cisco's default Web Authentication page.
- CLI commands for External Web Authentication—The following commands are available for configuring external web authentication:

```
custom-web ext-webauth-url <url>
custom-web ext-webauth-mode enable
```

- Provide AP MAC address—The Cisco WLC web server appends the MAC address of the AP with which you are associated with the external webauth URL.
- Provide the connect back URL—The external webauth URL is appended with the Cisco WLC web server URL that can be used by you to connect back and forward the user credentials.

Template for Customer Login Page

You can use the login page template provided by Cisco to develop your own login screen. The template contains the following:

- Hidden attribute names that enable the Cisco WLC to authenticate the user.
- A JavaScript function that extracts the AP MAC address and the redirected URL from the query string.
- A function that sets your web auth page's action URL.

Based on the AP MAC address, you can change your login page using scripts or display a message to the user.

The HTML code for the customer login page template is as follows:

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
      var link = document.location.href;
      var searchString = "redirect=";
      var equalIndex = link.indexOf(searchString);
      var redirectUrl = "";
      if(equalIndex >= 0) {
            equalIndex += searchString.length;
            redirectUrl = "http://";
            redirectUrl += link.substring(equalIndex);
      }
      if(redirectUrl.length > 255)
      redirectUrl = redirectUrl.substring(0,255);
      document.forms[0].redirect_url.value = redirectUrl;

      document.forms[0].buttonClicked.value = 4;
      document.forms[0].submit();
}

function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
      //alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The controller URL is " + args.switch_url);
      document.forms[0].action = args.switch_url;
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
```

```
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password"
name="password" SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

Web Authentication Certificate

Choose **SECURITY > Web Auth > Certificate** to navigate to the Web Authentication Certificate page.

This page enables you to view the current web authentication certificate type, download an SSL certificate, or regenerate a new locally generated web auth certificate.

Note The operating system automatically generates a fully functional web authentication certificate as it is loaded onto your Cisco WLC, which means that you do not have to do anything to use certificates with Layer 3 web authentication.

However, if you would like to use a new operating system-generated web authentication certificate, click **Regenerate Certificate**. The operating system generates a new web auth certificate and displays a "Successfully generated Web Authentication Certificate" message. Reboot the Cisco WLC to register the new certificate.

If you prefer to use an externally generated web authentication certificate, verify that the Cisco WLC can ping the TFTP server, check the **Download SSL Certificate** check box, and fill in the following parameters:

- Server IP address.
- Maximum Retries—Maximum number of times each download can be attempted.

- Timeout—Amount of time allowed for each download.
- Certificate File Path—Usually "/" so the TFTP software can use its default directory.
- Certificate File Name—Web authentication certificate filename in encrypted .PEM (Privacy Enhanced Mail) format.
- Certificate Password.

Note The TFTP server cannot run on the same computer as the Cisco WCS, because the Cisco WCS and the TFTP server use the same communication port.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

When you have filled in the required information, click **Apply** and the operating system collects the new certificate from the TFTP server. Reboot the Cisco WLC to register the new certificate.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Regenerate Certificate** to direct the operating system to internally generate a new Web Authentication certificate.

TrustSec SXP

You can use the SGT Exchange Protocol (SXP) to propagate the security group tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. The SXP sends SGT information to the CTS-enabled switches so that appropriate role-based access control lists (RBACLs) can be activated depending on the role information represented by the SGT. By default, the Cisco WLC is always in the Speaker mode. To implement the SXP on a network, only the egress distribution switch needs to be CTS-enabled, and all the other switches can be non-CTS-capable switches.

The SXP runs between any access layer and distribution switch or between two distribution switches. The SXP uses TCP as the transport layer. CTS authentication is performed for any host (client) joining the network on the access layer switch similar to an access switch with CTS-enabled hardware. The access layer switch is not CTS hardware enabled. Therefore, data traffic is not encrypted or cryptographically authenticated when it passes through the access layer switch. Also, the hardware cannot insert the SGT into the packet. The SXP is used to pass the IP address of the authenticated device, that is a wireless client, and the corresponding SGT up to the distribution switch. If the distribution switch is CTS hardware enabled, the switch inserts the SGT into the packet on behalf of the access layer switch. If the distribution switch is not CTS hardware enabled, the SXP on the distribution switch passes the IP-SGT mapping to all the distribution switches that have CTS hardware. On the egress side, the enforcement of the RBACL occurs at the egress L3 interface on the distribution switch.

SXP Configuration

Choose **SECURITY > TrustSec SXP** to navigate to the SXP Configuration page.

This table describes the TrustSec SXP parameters.

Table 6-27 TrustSec SXP Parameters

Parameter	Description
Total SXP Connections	Total number of SXP connections configured.
SXP State	Status of SXP connections as either disabled or enabled.
SXP Mode	SXP mode of the Cisco WLC. The Cisco WLC is always set to the Speaker mode in SXP connections.
Default Password	Password for MD5 authentication of SXP messages We recommend that the password contain a minimum of 6 characters.
Default Source IP	IP address of the management interface. The default source IP address for all SXP connections is the management IP address of the Cisco WLC. The source IP address cannot be configured.
Retry Period	The SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000. The SXP retry period determines how often the Cisco TrustSec software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco TrustSec software makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This page also displays the following SXP Connection information:

- **Peer IP Address**—The IP address of the peer, that is the IP address of the next hop switch to which the Cisco WLC is connected.
- **Source IP Address**—The IP address of the source, that is the management IP address of the Cisco WLC.
- **Connection Status**—Status of the SXP connection.

Click **New** to create a new SXP connection.

Local Policies

Choose **SECURITY > Local Policies** to navigate to the Policy List page.

This page enables you to configure the device-based policies on the Cisco WLC. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. Click the name of the policy to navigate to the Edit page and update the parameters. For more information, see Configuring Policies.

Click **New** to add a new policy.

Configuring Policies

Choose **SECURITY > Local Policies** and click the name of the policy to navigate to the Edit page. You can define parameters under Match Criteria and specify the policy action for the client. Policies applied on AP groups have more priority than those applied on WLANs.

Note Policies are not applied on WLANs and AP groups if AAA Override is configured on the Cisco WLC.

To apply the configured policies on a WLAN, choose **WLAN**, click the WLAN ID to navigate to the Edit page, and click the **Policy-Mapping** tab. You can configure up to 16 policies on a WLAN.

To apply the configured policies on an AP group, choose **WLAN > Advanced > AP Groups** , click the AP Group name to navigate to the Edit page, and click the **WLAN** tab. You can configure up to 16 policies on an AP group.

This table describes the policy parameters.

Table 6-28 Policy Parameters

Parameter	Description
Policy Name	Name of the policy.
Policy ID	Unique identifier of the policy
Match Criteria	
Match Role String	User type or user group of the user, for example, student, employee, and so on.
Match EAP Type	EAP authentication method used by the client. The available methods are as follows: • LEAP • EAP-FAST • EAP-TLS • PEAP
Device Type	Drop-down list from which you can choose a type of device. Click **Add** to add the device to the policy device list.
Device List	Devices configured for the policy.
Action	
IPv4 ACL	Drop-down list from which you can choose an IPv4 ACL for the policy.
VLAN ID	VLAN associated with the policy.

Table 6-28 Policy Parameters

Parameter	Description
QoS Policy	Drop-down list from which you can choose the QoS policy that can be one of the following: • Platinum (Voice)—Assures a high QoS for Voice over Wireless. • Gold (Video)—Supports high-quality video applications. • Silver (Best Effort)—Supports the normal bandwidth for clients. • Bronze (Background)—Provides the lowest bandwidth for guest services.
Session Timeout	Maximum amount of time, in seconds, before a client is forced to reauthenticate. The default value is 0.
Sleeping Client Timeout	Maximum amount of time, in hours, after the idle timeout before a guest client is forced to reauthenticate. The default value is 12. The range is from 1 to 720.
Flexconnect ACL	Drop down list from which you can choose the Fexconnect ACL for the policy.
AVC Profile	Drop down box lists all the configured AVC profiles on the controller for selection.
Active Hours	
Day	Day of the week on which the policy is active.
Start Time	Start time of the policy.
End Time	End time of the policy.

Cisco Intrusion Detection System

Cisco WLCs are equipped with sensors to detect intrusion attempts by unauthorized clients. These intruders are added to a shun list, which is forwarded to all Cisco mobility groups. A Renew flag is used to indicate that the Cisco WLC receiving the shun list should remove all entries from the sending Cisco WLC before processing the received list.

In a scenario where the primary Cisco WLC that has a connection to a Cisco Intrusion Detection System sensor is rebooted and some entries on this Cisco Intrusion Detection System sensor have expired, the first query after a reboot should renew and synchronize the newly acquired shun list from this Cisco Intrusion Detection System sensor in the mobility group.

The querying Cisco WLC compares the newly acquired shun list with its local list every time. If a new entry is found, it should be included in the next mmCidsUpdate. If an entry is removed in the new list, it sends this entry in the next mmCidsUpdate with Remaining Minutes set to zero. If the Remaining Minutes are set to zero, the receiving Cisco WLC removes this entry from the shun list.

Cisco Intrusion Detection System Sensors List

Choose **SECURITY > Advanced > CIDS > Sensors** to navigate to the Cisco Intrusion Detection System Sensors List page.

This table describes the Cisco Intrusion Detection System Sensors List parameters.

Table 6-29 Cisco Intrusion Detection System Sensors List Parameters

Parameter	Description
Index	Typically 1.
Server Address	URL of the CIDS sensor server.
Port	Typically 443.
State	State that is either enabled or disabled
Query Interval	To be specified in seconds.

Adding Cisco Intrusion Detection System Sensors

Choose **SECURITY > Advanced > CIDS > Sensors > New** to navigate to the Cisco Intrusion Detection System Sensor Add page.

This table describes the Cisco Intrusion Detection System Sensor Add parameters.

Table 6-30 Cisco Intrusion Detection System Sensor Add Parameters

Parameter	Description
Index	Index value from the drop-down list.
Server Address	URL of the Cisco Intrusion Detection System sensor server.
Port	SNMP port number. The default is 443.
Username	Name that the Cisco WLC uses to authenticate to the IDS sensor. **Note** This username must be configured on the IDS sensor and have at least a read-only privilege.
Password	Password that the Cisco WLC uses to authenticate to the IDS sensor.
Confirm Password	Password that you reenter so that the Cisco WLC can authenticate to the IDS sensor.
Query Interval	Interval in seconds.
State	State that allows you to enable to register the Cisco WLC with this IDS sensor. The default is disabled.
Fingerprint (SHA1 hash)	40 hexadecimal characters.

Editing Cisco Intrusion Detection System Sensors

Choose **SECURITY > Advanced > CIDS > Sensors** and then click the index number to navigate to the Cisco Intrusion Detection System Sensor Edit page.

This table describes the Cisco Intrusion Detection System Sensor Edit parameters.

Table 6-31 Cisco Intrusion Detection System Sensor Edit Parameters

Parameter	Description
Index	Configured index number.
Server Address	URL of the CIDS sensor server.
Port	SNMP port number. The default is 443.
Username	Name that the Cisco WLC uses to authenticate to the IDS sensor.
Password	Password that the Cisco WLC uses to authenticate to the IDS sensor.
State	Check box that enables you to enable or disable the state. The default is disabled.
Query Interval	Interval in seconds.
Fingerprint (SHA1 hash)	40 hexadecimal characters.
Last Query (count)	Unknown (0) when disabled.

Cisco Intrusion Detection System Shun List

Choose **SECURITY > Advanced > CIDS > Sensors > Shunned Clients** to navigate to the Cisco Intrusion Detection System Shun List page.

This table describes the CIDS shun list parameters.

Table 6-32 CIDS Shun List Parameters

Parameter	Description
IP Address	URL of the Cisco WLC Shun List sensor.
Last MAC Address	MAC address of the Shun List sensor.
Expire	Time remaining until expiration of the current list.
Sensor IP/Index	Cisco WLC sensor IP and index number.

Re-sync—Purges and resets the list.

CA Certification

Choose **SECURITY > Advanced > Vendor Certs > CA Certificate** to navigate to the CA Certification page.

This page contains the current CA certificate information. If you choose to add an operator-generated or purchased CA Certificate, paste the new CA certificate ASCII text into the certificate box and click **Apply**.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Delete Certificate** to delete the current CA Certification. You are prompted to confirm if you select this option.

ID Certificate

Choose **SECURITY > Advanced > Vendor Certs > ID Certificate** to navigate to this page.

This page summarizes existing network ID certificates by the ID certificate name and valid period. An ID certificate can be used by web server operators to ensure secure server operation.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

Click **New** to add a new ID certificate.

Adding ID Certificates

Choose **SECURITY > Advanced > Vendor Certs > ID Certificate** and then click **New** to navigate to the New ID Certificate page.

Caution Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

This page enables you to add new ID certificates, in addition to the factory-supplied ID certificate. For each new ID certificate, add the following:

- Certificate Name—Certificate name that you can specify.
- Certificate Password—Certificate password (private key).
- Certificate—New ID certificate ASCII text into the Certificate box.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.