

WLAN Security

- Layer 2 Security, on page 1
- Layer 3 Security, on page 21
- EAP and AAA Servers, on page 50
- Advanced WLAN Security, on page 71

Layer 2 Security

This section contains the following subsections:

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X

Note

- Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.
- WLAN WEP is not supported in Cisco Aironet 1810w Access Points.

- WPA+WPA2

Note

- Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- Static WEP (not supported on Wave 2 APs)

MAC Filtering of WLANs

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.

MAC Filtering with Centrally Authenticated WLANs

After the initial 802.11 authentication exchange between the AP and the clients, the AP sends the client association request in CAPWAP to the controller. If the controller is using a local MAC filter list, it will immediately send a successful or failed association response. If external RADIUS is used, the controller sends an Access-Request to the AAA server, and based on the response from RADIUS, sends its association response to the client.

Note Wireless clients may time out their wait for association response within as little as 300 ms. Therefore, if you use an external RADIUS server with MAC filtering, ensure that the server responds within this timeframe.

Restrictions for MAC Filtering

- MAC filtering cannot be configured for Guest LANs.
- Interface mapping and profile precedence—MAC filtering for the WLAN set to any WLAN/Interface requires a mandatory profile name, followed by the interface name for the traffic to work properly.

Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

- Enable MAC filtering by entering the **config wlan mac-filtering enable** *wlan_id* command.
- Verify that you have MAC filtering enabled for the WLAN by entering the **show wlan** command.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

When a client tries to associate to a WLAN for the first time, the client gets authenticated with its MAC address from AAA server. If the authentication is successful, the client gets an IP address from DHCP server, and then the client is connected to the WLAN.

When the client roams or sends association request to the same AP or different AP and is still connected to WLAN, the client is not authenticated again to AAA server.

If the client is not connected to WLAN, then the client has to get authenticated from the AAA server.

Local MAC Filters

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Prerequisites for Configuring Local MAC Filters

You must have AAA enabled on the WLAN to override the interface name.

Configuring Local MAC Filters (CLI)

- Create a MAC filter entry on the controller by entering the **config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] command.

  The following parameters are optional:

  - *mac_addr*—MAC address of the client.
  - *wlan_id*—WLAN id on which the client is associating.
  - *interface_name*—The name of the interface. This interface name is used to override the interface configured to the WLAN.
  - *description*—A brief description of the interface in double quotes (for example, “Interface1”).
  - *IP_addr*—The IP address which is used for a passive client with the MAC address specified by the mac addr value above.

- Assign an IP address to an existing MAC filter entry, if one was not assigned in the **config macfilter add** command by entering the **config macfilter ip-address** *mac_addr IP_addr* command.
- Verify that MAC addresses are assigned to the WLAN by entering the **show macfilter** command.

Note For ISE NAC WLANs, the MAC authentication request is always sent to the external RADIUS server. The MAC authentication is not validated against the local database. This functionality is applicable to Releases 8.5, 8.7, 8.8, and later releases via the fix for CSCvh85830.

Previously, if MAC filtering was configured, the controller tried to authenticate the wireless clients using the local MAC filter. RADIUS servers were attempted only if the wireless clients were not found in the local MAC filter.

Protected Management Frames (802.11w)

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients. They therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and an AP.

The 802.11w protocol applies only to a set of robust management frames protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

This section contains the following subsections:

Restrictions for Protected Management Frames (802.11w)

- With PMF settings set to Optional or Enabled, a wireless client may intermittently fail temporarily to reassociate to an access point. This impact will be mitigated by enabling **Fast Transition Over the Air**, and by setting the **PMF Comeback Timer** value to 1 second.
- The 802.11w standard is not supported .
- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.

- PMF is not supported in Cisco Aironet 1810, 1815, 1832, 1852, 1542, and 1800 series APs in FlexConnect mode prior to Release 8.9.

Configuring Protected Management Frames (802.11w) (GUI)

Procedure

Step 1 Choose **WLANs** > WLAN ID to open the WLANs > Edit page.

Step 2 In the **Security** tab, choose the **Layer 2** security tab.

Step 3 From the Layer 2 Security drop-down list, choose **WPA+WPA2**.

The 802.11w IGTK Key is derived using the 4-way handshake, which means that it can only be used on WLANs that are configured for WPA2 security at Layer 2.

Note
WPA2 is mandatory and encryption type must be AES. TKIP is not valid.

Step 4 Choose the PMF state from the drop-down list

The following options are available:

- **Disabled**—Disables 802.11w MFP protection on a WLAN
- **Optional**—To be used if the client supports 802.11w.
- **Required**—Ensures that the clients that do not support 802.11w cannot associate with the WLAN.

Step 5 If you choose the PMF state as either **Optional** or **Required**, do the following:

a) In the Comeback Timer box, enter the association comeback interval in milliseconds. It is the time within which the access point reassociates with the client after a valid security association.

b) In the SA Query Timeout box, enter the maximum time before an Security Association (SA) query times out.

Step 6 In the Authentication Key Management section, follow these steps:

a) Select or unselect the **PMF 802.1X** check box to configure the 802.1X authentication for the protection of management frames.

b) Select or unselect the **PMF PSK** check box to configure the preshared keys for PMF. Choose the PSK format as either ASCII or Hexadecimal and enter the PSK.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Related Topics

Configuring Infrastructure MFP (GUI)

Configuring Protected Management Frames (802.11w) 802.11w (CLI)

Procedure

- Configure the 802.1X authentication for PMF by entering this command:

config wlan security wpa akm pmf 802.1x {**enable** | **disable**} *wlan-id*

- Configure the preshared key support for PMF by entering this command:

  config wlan security wpa akm pmf psk {**enable** | **disable**} *wlan-id*

- If not done, configure a preshared key for a WLAN by entering this command:

  config wlan security wpa akm psk set-key {*ascii* | *hex*} *psk wlan-id*

- Configure protected management frames by entering this command:

  config wlan security pmf {**disable** | **optional** | **required**} *wlan-id*

- Configure the association comeback time settings by entering this command:

  config wlan security pmf association-comeback *timeout-in-seconds wlan-id*

- Configure the SA query retry timeout settings by entering this command:

  config wlan security pmf saquery-retrytimeout *timeout-in-milliseconds wlan-id*

- See the 802.11w configuration status for a WLAN by entering this command:

  show wlan *wlan-id*

- Configure the debugging of PMF by entering this command:

  debug pmf events {**enable** | **disable**}

Related Topics

Configuring Infrastructure MFP (CLI)

Fast Secure Roaming

802.11r Fast Transition

802.11r, which is the IEEE standard and generally recommended in order to speed roaming when using EAP, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

From Release 8.0, you can create an 802.11r WLAN that is also an WPAv2 WLAN. In earlier releases, you had to create separate WLANs for 802.11r and for normal security. Non-802.11r clients can now join 802.11r-enabled WLANs as the 802.11r WLANs can accept non-802.11r associations. If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANS. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode.

How a Client Roams

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

Note Over-the-Air is the preferred and recommended method compared to the Over-the-DS method.

Figure 1: Message Exchanges when Over the Air client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

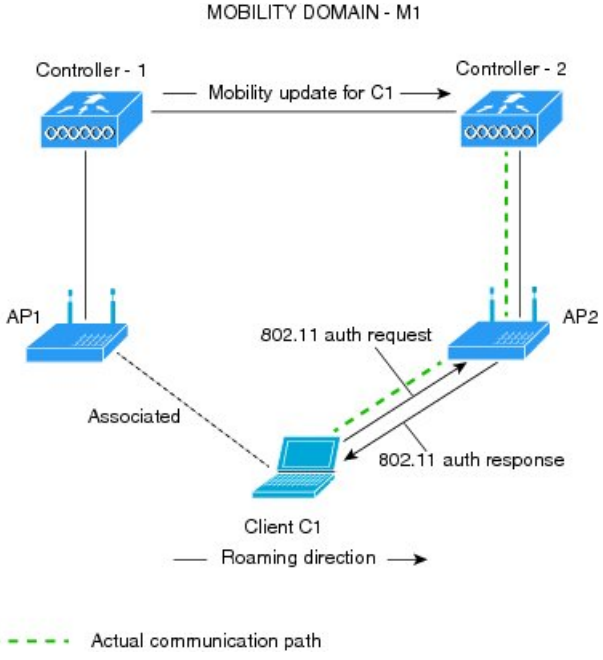
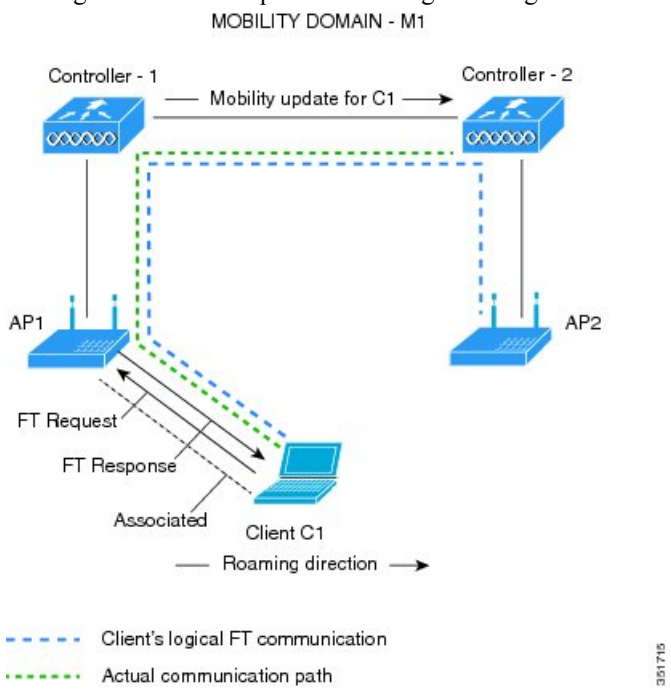


Figure 2: Message Exchanges when Over the DS client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.



This section contains the following subsections:

Restrictions for 802.11r Fast Transition

- This feature is not supported on mesh access points.
- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.
- For APs in FlexConnect mode:
  - 802.11r Fast Transition is supported in central and locally switched WLANs.
  - This feature is not supported for the WLANs enabled for local authentication.
  - 802.11r client association is not supported on access points in standalone mode.
  - 802.11r fast roaming is not supported on access points in standalone mode.
  - 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
  - 802.11r fast roaming works only if the APs are in the same FlexConnect group.
- 802.11r fast roaming is not supported if the client uses Over-the-DS preauthentication in standalone mode.
- EAP LEAP method is not supported. WAN link latency prevents association time to a maximum of 2 seconds.
- The service from standalone AP to client is only supported until the session timer expires.

- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The controller handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- This feature is supported on open and WPA2 configured WLANs.
- It is not possible to enable WPA1 encryption along with Fast Transition on a WLAN using the controller GUI. The workaround is to configure it using the controller CLI. For more information, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp05137.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  802.11i Opportunistic Key Caching (Proactive Key Caching) is supported only by Microsoft Windows clients. It is always enabled and cannot be disabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three Fast Transition handshakes with different APs.
- Disable the fast transition padding option for keys setting in the client to prevent the client from getting de-authenticated from an SSID with 802.11r Fast Transition enabled.
- Non-802.11r capable devices will not be able to associate with FT-enabled WLAN.
- 802.11r FT + PMF is not recommended.
- 802.11r FT Over-the-Air roaming is recommended for FlexConnect deployments.
- In a default FlexGroup scenario, fast roaming is not supported.

Configuring 802.11r Fast Transition (GUI)

Procedure

Step 1 Choose **WLANs** to open the **WLANs** window.

Step 2 Click a WLAN ID to open the **WLANs > Edit** window.

Step 3 Choose **Security** > **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.

The Authentication Key Management parameters for Fast Transition are displayed.

Step 5 From the **Fast Transition** drop-down list, choose Fast Transition on the WLAN.

Step 6 Uncheck the **Over the DS** check box to enable Fast Transition Over the Air.

Fast Transition Over the Air is the recommended configuration for this feature.

This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

Step 7 In the **Reassociation Timeout** field, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.

Note
This option is available only if you enable Fast Transition.

Step 8 Under Authentication Key Management, choose **FT 802.1X** or **FT PSK**. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the **FT PSK** check box, from the PSK Format drop-down list, choose **ASCII** or **Hex** and enter the key value.

Note
When Fast Transition adaptive is enabled, you can use only **802.1X** and **PSK AKM.**.

Step 9 From the **WPA gtk-randomize State** drop-down list, choose **Enable** or **Disable** to configure the Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state.

Step 10 Click **Apply** to save your settings.

Configuring 802.11r Fast Transition (CLI)

802.11r-enabled WLAN provides faster roaming for wireless client devices. However, if 802.11r is enabled on a WLAN and advertises fast transition (FT) and non-FT AKMs in Beacon and Probe RSN IE, some of the devices with bad implementation may not recognize FT/WPA2 authentication key-management (AKM) in RSN IE and fails to join. As a result, customers cannot enable 802.11r on the SSID.

To overcome this, Cisco Wireless infrastructure introduces adaptive 802.11r feature. When FT mode is set to adaptive, WLAN advertises 802.11r Mobility Domain ID on an 802.11i-enabled WLAN. Apple iOS10 client devices identifies the presence of MDIE on a 80211i/WPA2 WLAN and does a proprietary handshake to establish 802.11r association. Once the client completes successful 802.11r association, it will be able to do FT roaming as in a normal 802.11r enabled WLAN.

The FT adaptive is applicable only to selected Apple iOS10 devices. All other clients will continue to have 802.11i association on the WLAN.

Procedure

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**adaptive** | **enable** | **disable**} *wlan-id* command.

Fast Transition adaptive option is enabled by default when you create a new WLAN, from the controller, Release 8.3, onwards. However, the existing WLANs will retain its current configuration when the controller upgrades to Release 8.3 from an earlier release.

Enable Fast SSID feature for allowing client devices a smother switching smoother switching from one WLAN to another..

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

The Client devices normally prefer fast transition over-the-ds if the capability is advertised in the WLAN. To force a client to perform fast transition over-the-air, disable fast transition over-the-ds.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft psk** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable authentication key management for adaptive using PSK, use the **config wlan security wpa akm psk** {**enable** | **disable**} *wlan-id* command.

Step 5 To enable or disable authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.

By default, authentication key management using 802.1X is enabled.

Step 6 To enable or disable authentication key management for adaptive using 802.1x, use the **config wlan security wpa akm 802.1x** {**enable** | **disable**} *wlan-id* command.

Note
When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM.

Step 7 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.

The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To view the fast transition configuration on a client, use the **show client detail** *client-mac* command.

Note
This command is relevant only for a connected or connecting client station (STA).

Step 10 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

What to do next

- The tech support command output and xml config will not display fast transition information when it is disabled.
- The tech support command output and xml config will display Adaptive 802.11r information when it is enabled.
- To display a comprehensive view of the current controller configuration, use the **show run-config all** command.
- The fast transition adaptive mode is not supported on Releases prior to Release 8.3, the fast transition adaptive WLANs default to fast transition disable when the controller is downgraded from Release 8.3 to a previous release, and the fast transition adaptive configuration is invalidated.

Troubleshooting 802.11r BSS Fast Transition

Symptom	Resolution
Non-802.11r legacy clients are no longer connecting.	Check if the WLAN has FT enabled. If so, non-FT WLAN will need to be created.
When configuring WLAN, the FT setup options are not shown.	Check if WPA2 is being used (802.1x / PSK). FT is supported only on WPA2 and OPEN SSIDs.
802.11r clients appear to reauthenticate when they do a Layer 2 roam to a new controller.	Check if the reassociation timeout has been lowered from the default of 20 by navigating to **WLANs** > *WLAN Name* > **Security** > **Layer 2** on the controller GUI.

802.11i Sticky Key Caching

The controller supports sticky key caching (SKC). With sticky key caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC, the client stores each Pairwise Master Key ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

SKC is useful only in cases where you have a small number of clients, which roam among a small number of APs.

This section contains the following subsections:

Restrictions for Sticky Key Caching

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC works only on WPA2-enabled WLANs.
- SKC does not work across controllers in a mobility group.
- SKC works only on local mode APs.

Configuring Sticky Key Caching (CLI)

Procedure

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Enable sticky key caching by entering this command:

config wlan security wpa wpa2 cache sticky enable *wlan_id*

By default, SKC is disabled and opportunistic key caching (OKC) is enabled.

Note
SKC works only on WPA2 enabled WLANs.

You can check if SKC is enabled by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 2
Profile Name..................................... new
Network Name (SSID).............................. new
Status........................................... Disabled
MAC Filtering.................................... Disabled
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE)............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      Auth Key Management
         802.1x.................................. Disabled
         PSK..................................... Enabled
         CCKM.................................... Disabled
         FT(802.11r)............................. Disabled
         FT-PSK(802.11r)......................... Disabled
     SKC Cache Support.......................... Enabled
      FT Reassociation Timeout................... 20
      FT Over-The-Air mode....................... Enabled
      FT Over-The-Ds mode........................ Enabled
CCKM tsf Tolerance............................... 1000
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
```

Step 3 Enable the WLAN by entering this command:

config wlan enable *wlan_id*

Step 4 Save your settings by entering this command:

save config

Cisco Centralized Key Management (CCKM)

Cisco Centralized Key Management (CCKM) is an older proprietary method of fast secure roaming that was supported with dynamic WEP, WPA1 & WPA2 EAP security. With WPA2, CCKM is supported only by Cisco wireless phones and Cisco WGBs. It has been superseded by the 802.11r FT standard.

CCKM uses a fast rekeying technique that enables clients to roam from one AP to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the

client to mutually authenticate with the new AP and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

If you enable CCKM, the functionality of APs differs from the controller's for fast roaming in the following ways:

- If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
- If an association request sent by a client has CCKM enabled in RSN IE but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then AP does a full authentication. The access point does not use PMKID sent with the association request when CCKM is enabled in RSN IE.

For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc24.

Wi-Fi Protected Areas (WPA)

WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

Note WPA1 is deprecated. It may not be configured by itself, but only enabled if WPA2/CCMP128 (AES) is also enabled. WPA2 is the default. WPA3 is the emerging standard.

These standards provide for an authentication method and a cipher management method. The authentication methods supported are: 802.1X (a.k.a WPA Enterprise) and PSK.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default. However, these options are also available:

- 802.1X—The standard for wireless LAN security, as defined by IEEE, is called 802.1X for 802.11, or simply 802.1X. An access point that supports 802.1X acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network. If 802.1X is selected, only 802.1X clients are supported.

  In the 802.1X(Enterprise) authentication method, the clients use EAP (extensible authentication protocol) to authenticate with an authentication server. The authentication server can be an external RADIUS or LDAP server, or a local auth server running within the controller.

  To speed up roaming, a fast secure roaming method may optionally be deployed to bypass the authentication and key exchange phases.

- PSK—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.
- CCKM—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

  When CCKM is enabled, the behavior of access points differs from the controller's for fast roaming in the following ways:

  - If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
  - If an association request sent by a client has CCKM enabled in RSN IE but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then AP does a full authentication. The access point does not use PMKID sent with the association request when CCKM is enabled in RSN IE.

- 802.1X+CCKM—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/ 802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

This section contains the following subsections:

Configuring WPA1+WPA2 (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Security** and **Layer 2** tabs to open the **WLANs > Edit (Security > Layer 2)** page.

Step 4 Choose **WPA+WPA2** from the **Layer 2 Security** drop-down list.

Step 5 Under WPA+WPA2 Parameters, select the **WPA Policy** check box to enable WPA1, select the **WPA2 Policy** check box to enable WPA2, or select both check boxes to enable both WPA1 and WPA2.

Note
By default, WPA2 with CCMP128 is enabled. Optionally, WPA1 with CCMP128 and/or TKIP may be enabled, but WPA1 may not be configured with WPA2 disabled.

Note
Configure CCMP128(AES) for compatibility with greatest range of clients. Optionally, more secure ciphers (CCMP256, GCMP128, GCMP256) may be selected for greater security with recently released clients.

If using 802.1X (Enterprise) authentication, select 802.1X-SHA1 for compatibility with greatest range of clients. Or optionally, select 802.1X-SHA2 for use with recently released clients.

Step 6 Select the **WPA2 Policy-AES** check box to enable AES data encryption .

Note
Based on guidance from the Wi-Fi alliance (WFA), WPA/TKIP can only be configured on a secondary interface (CLI). Any previously saved TKIP configurations are retained upon upgrade and can be viewed on the CLI. This allows customers with Wi-Fi clients that only support WPA/TKIP to have a planned migration to devices that support AES.

Step 7 Choose one of the following key management methods from the Auth Key Mgmt drop-down list: **802.1X**, **CCKM**, **PSK**, or **802.1X+CCKM**.

Step 8 If you chose PSK, choose **ASCII** or **HEX** from the PSK Format drop-down list and then enter a preshared key in the blank text box. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Note
The PSK parameter is a set-only parameter. The value set for the PSK key is not visible to the user for security reasons. For example, if you selected HEX as the key format when setting the PSK key, and later when you view the parameters of this WLAN, the value shown is the default value. The default is ASCII.

Step 9 Save the configuration.

Configuring WPA1+WPA2 (CLI)

Procedure

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Enable or disable WPA for the WLAN by entering this command:

config wlan security wpa {**enable** | **disable**} *wlan_id*

Step 3 Enable or disable WPA1 for the WLAN by entering this command:

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

Step 4 Enable or disable WPA2 for the WLAN by entering this command:

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

Step 5 Enable or disable AES or TKIP data encryption for WPA1 or WPA2 by entering one of these commands:

- **config wlan security wpa wpa1 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*
- **config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

The default values are TKIP for WPA1 and AES for WPA2.

Note
From Release 8.0, you cannot configure TKIP as a standalone encryption method. TKIP can be used only with the AES encryption method.

Note
You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI.

When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need configure the encryption cipher mode globally on the multicast interface by entering the following command: **encryption mode ciphers tkip**.

Step 6 Enable or disable 802.1X, PSK, or CCKM authenticated key management by entering this command:

config wlan security wpa akm {**802.1X** | **psk** | **cckm**} {**enable** | **disable**} *wlan_id*

The default value is 802.1X.

Step 7 If you enabled PSK in *Step 6*, enter this command to specify a preshared key:

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 8 Enable or disable authentication key management suite for fast transition by entering this command:

config wlan security wpa akm ft {**802.1X** | **psk**} {**enable** | **disable**} *wlan_id*

Note
You can now choose between the PSK and the fast transition PSK as the AKM suite.

Step 9 Enable or disable randomization of group temporal keys (GTK) between AP and clients by entering this command:

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Step 10 If you enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting. To see the amount of time remaining before the timer expires, enter this command:

show pmk-cache all

If you enabled WPA2 with 802.1X authenticated key management, the controller supports both opportunistic PMKID caching and sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching (SKC), the client stores multiple PMKIDs, a different PMKID for every AP it associates with. Opportunistic PMKID caching (OKC) stores only one PMKID per client. By default, the controller supports OKC.

Step 11 Enable the WLAN by entering this command:

config wlan enable wlan_id

Step 12 Save your settings by entering this command:

save config

Wireless Encryption Protocol (WEP)

WLAN for Static WEP

You can configure up to four WLANs to support static WEP keys. Follow these guidelines when configuring a WLAN for static WEP:

- When you configure static WEP as the Layer 2 security policy, no other security policies can be specified. That is, you cannot configure web authentication. However, when you configure static WEP as the Layer 2 security policy, you can configure web authentication.

Restrictions for Configuring Static WEP

- The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit client functionality. Clients must support CCXv4 or v5 in order to use CCKM. For more information about CCX, see the Configuring Cisco Client Extensions section.
- In a unified architecture where multiple VLAN clients are supported for a WGB, you also need to configure encryption cipher suite and WEP keys globally, when the WEP encryption is enabled on the WGB. Otherwise, multicast traffic for wired VLAN clients fail.

Configuring Dynamic WEP (CLI)

Controllers can control 802.1X dynamic WEP keys using Extensible Authentication Protocol (EAP) across access points and support 802.1X dynamic key settings for WLANs.

Note WEP is deprecated and is only supported in Cisco Wave 1 (IOS-based) APs; not supported on Cisco Wave 2 or 802.11ax (Wi-Fi 6) APs.

Note To use LEAP with lightweight access points and wireless clients, make sure to choose **Cisco-Aironet** as the RADIUS server type when configuring the CiscoSecure Access Control Server (ACS).

- Check the security settings of each WLAN by entering this command:

  show wlan *wlan_id*

  The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.

- Disable or enable the 802.1X authentication by entering this command:

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

After you enable 802.1X authentication, the controller sends EAP authentication packets between the wireless client and the authentication server. This command allows all EAP-type packets to be sent to and from the controller.

Note The controller performs both web authentication and 802.1X authentication in the same WLAN. The clients are initially authenticated with 802.1X. After a successful authentication, the client must provide the web authentication credentials. After a successful web authentication, the client is moved to the run state.

- Change the 802.1X encryption level for a WLAN by entering this command:

  config wlan security 802.1X encryption *wlan_id* **[0 | 40 | 104]**

  - Use the **0** option to specify no 802.1X encryption.
  - Use the **40** option to specify 40/64-bit encryption.
  - Use the **104** option to specify 104/128-bit encryption. (This is the default encryption setting.)

MAC Authentication Failover to 802.1X Authentication

You can configure the controller to start 802.1X authentication when MAC authentication for the client fails. If the RADIUS server rejects an access request from a client instead of deauthenticating the client, the controller can force the client to undergo an 802.1X authentication. If the client fails the 802.1X authentication too, then the client is deauthenticated.

If MAC authentication is successful and the client requests for an 802.1X authentication, the client has to pass the 802.1X authentication to be allowed to send data traffic. If the client does not choose an 802.1X authentication, the client is declared to be authenticated if the client passes the MAC authentication.

Note WLAN with **WPA2 + 802.1X + WebAuth with WebAuth** on MAC failure is not supported.

This section contains the following subsections:

Configuring MAC Authentication Failover to 802.1x Authentication (GUI)

Procedure

Step 1 Choose **WLANs** > **WLAN ID** to open the WLANs > Edit page.

Step 2 In the **Security** tab, click the **Layer 2** tab.

Step 3 Select the **MAC Filtering** check box.

Step 4 Select the **Mac Auth or Dot1x** check box.

Configuring MAC Authentication Failover to 802.1X Authentication (CLI)

Procedure

To configure MAC authentication failover to 802.1X authentication, enter this command:

config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

Identity PSK

This feature is designed to provide a simple and secured way for the growing number of devices to connect to the network. Some devices such as Internet of Things (IoT) clients may not support the 802.1x security protocol. These devices can connect to the network using the PSK authentication mechanism.

If all the clients are using the same key and if the key is shared with unauthorized users, then it leads to security breach.

The IPSK feature enables the administrator to configure WPA-PSK protocol-based unique pre-shared keys in the same SSID. This pre-shared key can be issued to an individual or group of users for their devices to connect to the network easily and safely. This also helps in identifying and managing a set of devices without affecting the other pre-shared key devices connected to the network. These keys can be configured with rules to authenticate and provide the appropriate level of access in the network.

Here, the AAA RADIUS server key is used to authenticate the client.

For documentation on Cisco ISE configuration, see the relevant administration guide at https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html.

This section contains the following subsections:

Prerequisites for Identity PSK

The RADIUS server must be configured to return the following Cisco AV pairs in its response to the MAC-filtering authentication request:

- psk-mode=ascii
- psk=cisco123

Key length must be between 8 and 63 characters for ASCII and 64 characters for HEX. If the key configured on the RADIUS server does not meet the length requirement, the client can be authenticated with PSK configured on the WLAN.

Configuring Identity PSK (GUI)

Procedure

Step 1 Choose **WLAN** to open the WLAN page.

Step 2 Create a new WLAN or click an existing WLAN.

Step 3 Check the **Status Enabled** check box.

Step 4 Choose **Security** > **Layer 2** tab.

Step 5 Choose **WPA+WPA2** or **WPA2+WPA3** from the **Layer 2 Security** drop-down list.

Step 6 In the **Security Type** drop-down list, select **Personal**.

Step 7 (Optional) Check the **MAC Filtering** check box.

Step 8 Check the **AutoConfig iPSK** check box.

Step 9 Choose **Security** > **AAA Servers** tab.

Step 10 Check the **Authentication Servers Enabled** check box.

Step 11 Select the **Server IP address and port number** from the drop-down list.

If the RADIUS server is not configured, the RADIUS server is selected from the global list.

Step 12 Choose **Advanced** tab.

Step 13 Check the **Allow AAA Override Enabled** check box to enable AAA override. The default value is disabled.

Step 14 Click **Apply**.

Configuring Identity PSK (CLI)

Procedure

- Enable MAC filtering by entering this command:
  config wlan mac-filtering enable *wlan-id*
- Enable AAA-override on a WLAN by entering this command:
  config wlan aaa-override enable *wlan-id*
- Enable RADIUS authentication on a WLAN by entering this command:
  config wlan radius_server auth enable *wlan-id*
- Enable PSK support on a WLAN by entering this command:
  config wlan security wpa akm psk enable *wlan-id*
- Configure the PSK pre-share key by entering this command:
  config wlan security wpa akm psk set-key *ascii/hex psk-key wlan-id*

Layer 3 Security

Layer 3 security takes effect only after Layer 2 is operational and also the wireless client has a working IP address. Layer 3 security is triggered by the client opening a web session (HTTP or HTTPS).



Note Layer 2 security should not be considered as a truly effective security method unless used in conjunction with a strong Layer 2 security method. This is because without Layer 2 security, the client's data can be captured in clear text over the air.

This section contains the following subsections:

With Layer 3 security, the client will issue a DNS query for a web server; the controller spoofs the DNS response, providing its own Virtual IP address. The client then opens a web connection (HTTP port 80 or HTTPS port 443) to that address. The controller redirects (to itself [Local Web Authentication] or to an external server [Central Web Authentication]), and then that dialog is used to authorize the client to connect to the network.

- Hijacking an initial HTTPS connection is an inherently problematic operation, as HTTPS is designed to prevent hijacking. In general, you can expect client browsers to prevent, or at least warn, the user against connecting.
- If the Layer 3 redirect goes to HTTPS rather than HTTP, the client browser is also likely to be warnted against connecting, unless the HTTPS server provides a valid certificate chain that is trusted by the client.

Types of Layer 3 Security

- Web Passthrough: This is a variation of the internal web authentication. It displays a page with a warning or an alert statement, but does not prompt for credentials. The user should click **ok**. You can enable email input, and the user can enter their email address, which becomes their username. When the user is connected, check your active clients list; that user is listed with the email address they entered as the username. For more information, see the Wireless LAN Controller 5760/3850 Web Passthrough Configuration Example.
- Local Web Authentication: Validates credentials against local database or RADIUS server. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html.
- Redirect to External Web Authentication: With external web authentication, the login page used for web authentication is stored on an external web server. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html.
- Central Webauth with Cisco ISE: In the case of Central Web Authentication (CWA), web authentication occurs on the Cisco ISE server. The web portal in the Cisco ISE server provides a login page to a client. After the credentials are verified on the Cisco ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a change of authorization (CoA) is reached. The credentials and ACLs are received from the Cisco ISE server. For more information, see Central Web Authentication, on page 40.

This section contains the following subsections:

Information About Web Authentication

For more information about web authentication, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html.

Prerequisites for Configuring Web Authentication on a WLAN

- To initiate HTTP/HTTPS web authentication redirection, use HTTP URL or HTTPS URL.
- If the CPU ACLs are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.
- Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.

- When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. We recommend that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.
- If the web authentication is enabled on the WLAN and you also have the CPU ACL rules, the client-based web authentication rules take higher precedence as long as the client is unauthenticated (in the webAuth_Reqd state). Once the client goes to the RUN state, the CPU ACL rules get applied. Therefore, if the CPU ACL rules are enabled in the controller, an allow rule for the virtual interface IP is required (in any direction) with the following conditions:
  - When the CPU ACL does not have an allow ACL rule for both directions.
  - When an allow ALL rule exists, but also a DENY rule for port 443 or 80 of higher precedence.
- The allow rule for the virtual IP should be for TCP protocol and port 80 (if secureweb is disabled) or port 443 (if secureweb is enabled). This process is required to allow client's access to the virtual interface IP address, post successful authentication when the CPU ACL rules are in place.

Restrictions for Configuring Web Authentication on a WLAN

- Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK.
- Special charecters are not supported in the username field for web-authentication.
- When clients connect to a WebAuth SSID and a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

  You can select the following identity stores to authenticate web-auth user, under **WLANs > Security > AAA servers > Authentication priority** order for web-auth user section:
  - Local
  - RADIUS
  - LDAP

  If multiple identity stores are selected, then the controller checks each identity store in the list, in the order specified, from top to bottom, until authentication for the user succeeds. The authentication fails, if the controller reaches the end of the list and user remains un-authenticated in any of the identity stores.

Default Web Authentication Login Page

If you are using a custom web-auth bundle that is served by the internal controller web server, the page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller 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 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 do not want users to connect to a web page using a browser that is configured with SSLv2 only, you can disable SSLv2 for web authentication by entering the **config network secureweb cipher-option sslv2**

disable command. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is disabled.



Note Cisco TAC is not responsible for creating a custom webauth bundle.

If you have a complex custom web authentication module, it is recommended that you use an external web-auth config on the controller, where the full login page is hosted at an external web server.

This section contains the following subsections:

Choosing the Default Web Authentication Login Page (GUI)

Procedure

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **Internal (Default)**.

Step 3 If you want to use the default web authentication login page as is, go to Step 8. If you want to modify the default login page, go to Step 4.

Step 4 If you want to hide the Cisco logo that appears in the top right corner of the default page, choose the Cisco Logo **Hide** option. Otherwise, click the **Show** option.

Step 5 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter the desired URL in the Redirect URL After Login text box. You can enter up to 254 characters.

Step 6 If you want to create your own headline on the login page, enter the desired text in the Headline text box. You can enter up to 127 characters. The default headline is "Welcome to the Cisco wireless network."

Step 7 If you want to create your own message on the login page, enter the desired text in the Message text box. You can enter up to 2047 characters. The default message is "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work."

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Preview** to view the web authentication login page.

Step 10 If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes. Otherwise, repeat any of the previous steps as necessary to achieve your desired results.

Choosing the Default Web Authentication Login Page (CLI)

Procedure

Step 1 Specify the default web authentication type by entering this command:

config custom-web webauth_type internal

Step 2 If you want to use the default web authentication login page as is, go to Step 7. If you want to modify the default login page, go to Step 3.

Step 3 To show or hide the Cisco logo that appears in the top right corner of the default login page, enter this command:

config custom-web weblogo {**enable** | **disable**}

Step 4 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter this command:

config custom-web redirecturl *url*

You can enter up to 130 characters for the URL. To change the redirect back to the default setting, enter the **clear redirecturl** command.

Step 5 If you want to create your own headline on the login page, enter this command:

config custom-web webtitle *title*

You can enter up to 130 characters. The default headline is "Welcome to the Cisco wireless network." To reset the headline to the default setting, enter the **clear webtitle** command.

Step 6 If you want to create your own message on the login page, enter this command:

config custom-web webmessage *message*

You can enter up to 130 characters. The default message is "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work." To reset the message to the default setting, enter the **clear webmessage** command.

Step 7 To enable or disable the web authentication logout popup window, enter this command:

config custom-web logout-popup {**enable** | **disable**}

Step 8 Enter the **save config** command to save your settings.

Step 9 Import your own logo into the web authentication login page as follows:

a. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

b. Ensure that the controller can contact the TFTP server by entering this command:

ping ip-address

c. Copy the logo file (in .jpg, .gif, or .png format) to the default directory on your TFTP server. The maximum file size is 30 kilobits. For an optimal fit, the logo should be approximately 180 pixels wide and 360 pixels high.

d. Specify the download mode by entering this command:

transfer download mode tftp

e. Specify the type of file to be downloaded by entering this command:

transfer download datatype image

f. Specify the IP address of the TFTP server by entering this command:

transfer download serverip *tftp-server-ip-address*

Note
Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

g. Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

h. Specify the file to be downloaded by entering this command:

transfer download filename {*filename.jpg* | *filename.gif* | *filename.png*}

i. View your updated settings and answer *y* to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

j. Save your settings by entering this command:

save config

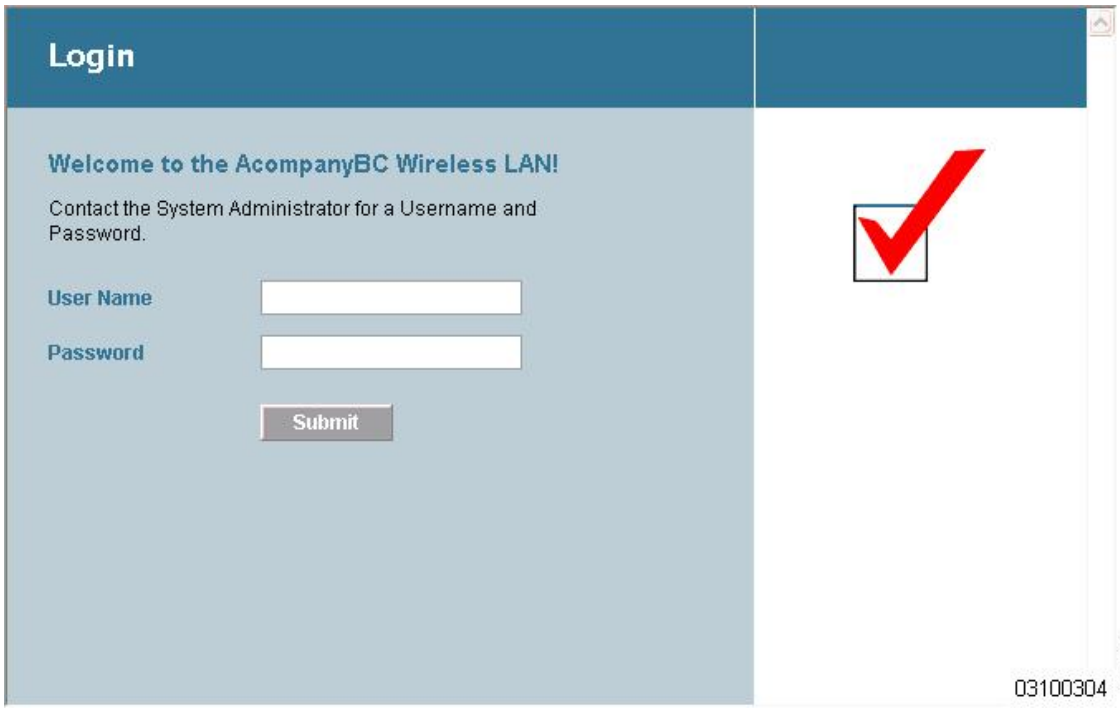
Note
If you ever want to remove this logo from the web authentication login page, enter the **clear webimage** command.

Step 10 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 34 section to verify your settings.

Example: Modified Default Web Authentication Login Page Example

Figure 3: Modified Default Web Authentication Login Page Example

This figure shows an example of a modified default web authentication login page.



These CLI commands were used to create this login page:

- **config custom-web weblogo** *disable*
- **config custom-web webtitle** *Welcome to the AcompanyBC Wireless LAN!*
- **config custom-web webmessage** *Contact the System Administrator for a Username and Password.*
- **transfer download** *start*
- **config custom-web redirecturl** *url*

Using a Customized Web Authentication Login Page from an External Web Server

Information About Customized Web Authentication Login Page

You can customize the web authentication login page to redirect to an external web server. When you enable this feature, the user is directed to your customized login page on the external web server.

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 **Layer 3 Security > Web Policy** on the **WLANs > Edit** page.

Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)

Procedure

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the **Web Authentication Type** drop-down list, choose **External (Redirect to external server)**.

Step 3 In the **Redirect URL after Login** field, enter the 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. of the customized web authentication login page on your web server. You can enter up to 252 characters.

Step 4 In the **External Webauth URL** field, enter the URL that is to be used for external web authentication.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)

Procedure

Step 1 Specify the web authentication type by entering this command:

config custom-web webauth_type external

Step 2 Specify the URL of the customized web authentication login page on your web server by entering this command:

config custom-web ext-webauth-url *url*

You can enter up to 252 characters for the URL.

Step 3 Specify the IP address of your web server by entering this command:

config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

Step 4 Enter the **save config** command to save your settings.

Step 5 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 34 section to verify your settings.

Example: Creating a Customized Web Authentication Login Page

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page:

Note We recommend that you follow the Cisco guidelines to create a customized web authentication login page. If you have upgraded to the latest versions of Google Chrome or Mozilla Firefox browsers, ensure that your webauth bundle has the following line in the *login.html* file:

```
<body onload="loadAction();">
```

For more information about this issue, see CSCvj17640.

```
<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 (document.forms[0].action == "") {
  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);
  }
   document.forms[0].action = args.switch_url;
  }

      if(equalIndex >= 0) {
  equalIndex += searchString.length;
  redirectUrl = "";
  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 Switch URL to post user credentials is " + args.switch_url);
      document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
      }
```

```
      else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further action
 is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username is
 already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<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>
```

These parameters are added to the URL when the user's Internet browser is redirected to the customized login page:

- **ap_mac**—The MAC address of the access point to which the wireless user is associated.

- **switch_url**—The URL of the controller to which the user credentials should be posted.
- **redirect**—The URL to which the user is redirected after authentication is successful.
- **statusCode**—The status code returned from the controller's web authentication server.
- **wlan**—The WLAN SSID to which the wireless user is associated.

The available status codes are as follows:

- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username is already logged into the system?"
- Status Code 4: "You have been excluded."
- Status Code 5: "The User Name and Password combination you have entered is invalid. Please try again."



Note For additional information, see the *External Web Authentication with Wireless LAN Controllers Configuration Example* at http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html.

Downloading a Customized Web Authentication Login Page

You can compress the page and image files used for displaying a web authentication login page into a.tar file for download to a controller. These files are known as the webauth bundle. The maximum allowed size of the files in their uncompressed state is 1 MB. When the .tar file is downloaded from a local TFTP server, it enters the controller's file system as an untarred file.

You can download a login page example from Cisco Prime Infrastructure and use it as a starting point for your customized login page. For more information, see the Cisco Prime Infrastructure documentation.



Note If you load a webauth bundle with a .tar compression application that is not GNU compliant, the controller cannot extract the files in the bundle and the following error messages appear: "Extracting error" and "TFTP transfer failed." Therefore, we recommend that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file for the webauth bundle.



Note Configuration backups do not include extra files or components, such as the webauth bundle or external licenses, that you download and store on your controller, so you should manually save external backup copies of those files or components.

Note If the customized webauth bundle has more than 3 separated elements, we advise you to use an external server to prevent page load issues that may be caused because of TCP rate-limiting policy on the controller.

Prerequisites for Downloading a Customized Web Authentication Login Page

- Name the login page `login.html`. The controller prepares the web authentication URL based on this name. If the server does not find this file after the webauth bundle has been untarred, the bundle is discarded, and an error message appears.
- Include input text boxes for both a username and password.
- Retain the redirect URL as a hidden input item after extracting from the original URL.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- Ensure that all paths used in the main page (to refer to images, for example).
- Ensure that no filenames within the bundle are greater than 30 characters.

Downloading a Customized Web Authentication Login Page (GUI)

Procedure

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the **File Type** drop-down list, choose **Webauth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 5 In the **IP Address** field, enter the IP address of the server.

Step 6 If you are using a TFTP server, enter the maximum number of times the controller should attempt to download the .tar file in the Maximum Retries field.

The range is 1 to 254.

The default is 10.

Step 7 If you are using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the *.tar file in the Timeout field.

The range is 1 to 254 seconds.

The default is 6 seconds.

Step 8 In the **File Path** field, enter the path of the .tar file to be downloaded. The default value is "/."

Step 9 In the **File Name** field, enter the name of the .tar file to be downloaded.

Step 10 If you are using an FTP server, follow these steps:

a. In the **Server Login Username** field, enter the username to log into the FTP server.

b. In the **Server Login Password** field, enter the password to log into the FTP server.

c. In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the .tar file to the controller.

Step 12 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 13 From the **Web Authentication Type** drop-down list, choose **Customized (Downloaded)**.

Step 14 Click **Apply**.

Step 15 Click **Preview** to view your customized web authentication login page.

Step 16 If you are satisfied with the content and appearance of the login page, click **Save Configuration**.

Downloading a Customized Web Authentication Login Page (CLI)

Procedure

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Specify the download mode by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of file to be downloaded by entering this command:

transfer download datatype webauthbundle

Step 4 Specify the IP address of the TFTP server by entering this command:

transfer download serverip *tftp-server-ip-address.*

Note
Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 5 Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

Step 6 Specify the file to be downloaded by entering this command:

transfer download filename *filename.tar*

Step 7 View your updated settings and answer **y** to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

Step 8 Specify the web authentication type by entering this command:

config custom-web webauth_type *customized*

Step 9 Enter the **save config** command to save your settings.

Example: Customized Web Authentication Login Page

Figure 4: Customized Web Authentication Login Page Example

This figure shows an example of a customized web authentication login page.



Verifying the Web Authentication Login Page Settings (CLI)

Verify your changes to the web authentication login page by entering this command:

show custom-web

Assigning Login, Login Failure, and Logout Pages per WLAN

You can display different web authentication login, login failure, and logout pages to users per WLAN. This feature enables user-specific web authentication pages to be displayed for a variety of network users, such as guest users or employees within different departments of an organization.

Different login pages are available for all web authentication types (internal, external, and customized). However, different login failure and logout pages can be specified only when you choose customized as the web authentication type.

This section contains the following subsections:

Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to which you want to assign a web login, login failure, or logout page.

Step 3 Choose **Security** > **Layer 3**.

Step 4 Make sure that **Web Policy** and **Authentication** are selected.

Step 5 To override the global authentication configuration web authentication pages, select the **Override Global Config** check box.

Step 6 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wireless guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note
  These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 7 If you chose External as the web authentication type in Step 6, choose **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note
The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 8 Establish the priority in which the servers are contacted to perform web authentication as follows:

Note
The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click **Up** and **Down** until the desired server type is at the top of the box.

c. Click the < arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)

Procedure

Step 1 Determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page by entering this command:

show wlan summary

Step 2 If you want wireless guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the WLAN for which it should display:

- **config wlan custom-web login-page** *page_name wlan_id—Defines a customized login page for a* given WLAN.
- **config wlan custom-web loginfailure-page** *page_name wlan_id—Defines a customized login* failure page for a given WLAN.

  Note
  To use the controller's default login failure page, enter the **config wlan custom-web loginfailure-page none** *wlan_id* command.

- **config wlan custom-web logout-page** *page_name wlan_id—Defines a customized logout page for* a given WLAN.

  Note
  To use the controller's default logout page, enter the **config wlan custom-web logout-page none** *wlan_id* command.

Step 3 Redirect wireless guess users to an external server before accessing the web login page by entering this command to specify the URL of the external server:

config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

Note
For the external web authentication URL, the CLI does not accept the *?* character. For example, if the URL is *https://example.com?text*, the CLI saves the URL as *https://example.comtext*. For more information, see CSCvu53350.

Step 4 Define the order in which web authentication servers are contacted by entering this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS and LDAP.

Note
All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

Step 5 Define which web authentication page displays for a wireless guest user by entering this command:

config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web login page that was configured in *Step 2*.

  Note
  You do not need to define the web authentication type in *Step 5* for the login failure and logout pages as they are always customized.

- **external** redirects users to the URL that was configured in *Step 3*.

Step 6 Use a WLAN-specific custom web configuration rather than a global custom web configuration by entering this command:

config wlan custom-web global disable *wlan_id*

Note
If you enter the **config wlan custom-web global enable** *wlan_id* command, the custom web authentication configuration at the global level is used.

Step 7 Save your changes by entering this command:

save config

Captive Network Assistant Bypass

Many clients will attempt to determine whether their wireless network connection is being intercepted by Layer 3 security, in order to improve the user interaction experience. For example: Windows 10, Apple iOS, Firefox. Such a software interface is known as a Captive Network Assistant (CNA). In rare cases, the functionality of a CNA can cause problems with Layer 3 security; in such a situation, you can enable Captive Network Assistant Bypass (CNAB). With CNAB, the congtroller tries to trick the CNA into thinking that it is fully connected to the Internet, thus requiring the client to Layer-3 authenticate using a full browser session.



Note Enabling CNAB does not guarantee that all CNAs will fail to detect the Captive Portal because CNA implementations are continually refining their Captive Portal detection heuristics.

Configuring Captive Bypassing (CLI)

Use these commands to configure captive bypassing:

- **config network web-auth captive-bypass** {**enable** | **disable**}—Enables or disables the controller to support bypass of captive portals at the network level.
- **show network summary**—Displays the status for the WISPr protocol detection feature.

Configuring Captive Network Assistant Bypass per WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the WLAN ID.

Step 3 Click the **Security** tab and then click the **Layer 3** tab.

Step 4 From the **Captive Network Assistant Bypass** drop-down list, choose:

- **None**: Global Captive Network Assistant Bypass setting is applied
- **Enable**: Captive Network Assistant Bypass is enabled for this particular WLAN
- **Disable**: Captive Network Assistant Bypass is disabled for this particular WLAN

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Captive Network Assistant Bypass per WLAN (CLI)

Procedure

- Enable, disable or activate global Captive Network Assistant Bypass per WLAN by entering this command:

  config wlan security web-auth captive-bypass {**none** | **enable** | **disable**} *wlan-id*

  By default, Captive Network Assistant Bypass per WLAN is in disabled state.

Fallback Policy with MAC Filtering and Web Authentication

You can configure a fallback policy mechanism that combines Layer 2 and Layer 3 security. In a scenario where you have both MAC filtering and web authentication implemented, when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, you can configure the authentication to fall back to web authentication. When a client passes the MAC filter authentication, the web authentication is skipped and the client is connected to the WLAN. With this feature, you can avoid disassociations based on only a MAC filter authentication failure.

Restrictions

- MAC filtering does not support passthrough web-authentication. It supports only username and password for web-authentication.

Mobility is not supported for SSIDs with security type configured for Webauth on MAC filter failure.

This section contains the following subsections:

Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI)



Note Before configuring a fallback policy, you must have MAC filtering enabled.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the fallback policy for web authentication. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 From the Layer 3 Security drop-down list, choose **None.**

Step 5 Select the **Web Policy** check box.

Note
The controller forwards DNS traffic to and from wireless clients prior to authentication.

The following options are displayed:

- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

Step 6 Click **On MAC Filter Failure**.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your settings.

Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI)



Note Before configuring a fallback policy, you must have MAC filtering enabled.

Procedure

Step 1 Enable or disable web authentication on a particular WLAN by entering this command:

config wlan security web-auth on-macfilter-failure *wlan-id*

Step 2 See the web authentication status by entering this command:

show wlan *wlan_id*

```
FT Over-The-Ds mode.............................. Enabled
CKIP ..................................... Disabled
   IP Security.................................. Disabled
   IP Security Passthru......................... Disabled
   Web Based Authentication..................... Enabled-On-MACFilter-Failure
        ACL..................................... Unconfigured
        Web Authentication server precedence:
        1....................................... local
        2....................................... radius
        3....................................... ldap
```

Central Web Authentication

In the case of Central Web Authentication (CWA), web authentication occurs on the Cisco ISE server. The web portal in the Cisco ISE server provides a login page to a client. After the credentials are verified on the Cisco ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a change of authorization (CoA) is reached. The credentials and ACLs are received from Cisco ISE server.

Note

- In a CWA and MAC filtering configuration scenario, if a change in VLAN occurs during pre-authentication and post-authentication, dissociation request is sent to clients and the clients are forced to go through DHCP again.
- Inter-controller roaming with non-802.1X L2 security, with MAC filtering and CWA, is not supported prior to 8.9.

For new clients, the RADIUS access accept message carries redirected URL for port 80 and pre-auth ACLs or quarantine VLAN. Definition of ACL is defined in the controller (IP addresses and ports).

Clients will be redirected to the URL provided in the access accept message and put into a new state until posture validation is done. Clients in this state validate themselves against ISE server and the policies configured on the ISE NAC server.

The NAC agent on the clients initiates posture validation (traffic to port 80): The agent sends HTTP discovery request to port 80, which the controller redirects to the URL provided in the access accept message. Cisco ISE knows that the client is trying to reach and responds directly to the client. This way, the client learns about the Cisco ISE IP address and from now on, the client talks directly with the Cisco ISE.

The controller allows this traffic because the ACL is configured to allow this traffic. In case of VLAN override, the traffic is bridged so that it reaches the Cisco ISE.

ISE NAC

After the client completes the assessment, a RADIUS CoA-Req with reauth service is sent to the controller. This initiates reauthentication of the client (by sending EAP-START). Once reauthentication succeeds, the Cisco ISE sends an access accept message with a new ACL (if any) and no URL redirect, or access VLAN.

The controller has support for CoA-Req and Disconnect-Req as per RFC 3576. The controller needs to support CoA-Req for re-auth service, as per RFC 5176.

Instead of downloadable ACLs, pre-configured ACLs are used on the controller. Cisco ISE sends the ACL name, which is already configured in the controller.

This design should work for both VLAN and ACL cases. In case of VLAN override, the port 80 is redirected and allows (bridge) rest of the traffic on the quarantine VLAN. For the ACL, the pre-auth ACL received in the access accept message is applied.

Here is the workflow:

1. The guest user associates with the controller.
2. The controller sends a MAB Request to ISE.
3. ISE matches the first authorization rules, and sends the redirect parameters (ACL and URL).
4. The controller redirects the GUEST to ISE.
5. After the guest is authenticated, ISE makes a second authorization, which is called RADIUS Change of Authorization (CoA). In this second authorization, a profile must be returned so that the guest is permitted access to the network. We can use usecase: guestflow to easily match this second authorization.



Note Guest clients connecting to a web-auth WLAN in a CWA setup may also reach the internal virtual interface web-auth login page using port 80 or by using port 443 when the web authentication secure web is enabled in the Cisco AireOS controllers. This behavior is in line with how Cisco AireOS controllers handle all web authentication redirect scenarios and have no potential risk or vulnerability.

Authentication of Sleeping Clients

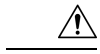
Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is lesser than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

The order of precedence is session timeout, sleeping client timeout, and user idle timeout. If the user idle timeout expires, then the sleeping client comes into play. If the sleeping client wakes up and if the sleeping client timeout has not expired, but if the session timeout has expired, the client must reauthenticate.



Note The sleeping timer expires every 5 minutes.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.



Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

Supported Mobility Scenarios

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controllers in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller.
- Suppose there are three controllers in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

This section contains the following subsections:

Restrictions for Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security. Web passthrough is supported on Release 8.0 and later.
- You can configure the sleeping clients only on a per-WLAN basis.
- With Release 8.8.111.0, sleeping clients are supported in a scenario where both Layer 2 security and Layer 3 security are configured on a WLAN.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.
- The number of sleeping clients that are supported depends on the controller platform:
  - Cisco 5520 Wireless Controller—25000
  - Cisco 8540 Wireless Controller—64000
  - Cisco Virtual Wireless LAN Controller—500

• Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)—500

Configuring Authentication for Sleeping Clients (GUI)

Procedure

Step 1 Choose **WLANs**.

Step 2 Click the corresponding WLAN ID.

The **WLANs > Edit** page is displayed.

Step 3 Click the **Security** tab and then click the **Layer 3** tab.

Step 4 Select the **Sleeping Client** check box to enable authentication for sleeping clients.

Step 5 Enter the **Sleeping Client Timeout**, which is the duration for which the sleeping clients are to be remembered before reauthentication becomes necessary.

The default timeout is 12 hours.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

- Enable or disable authentication for sleeping clients on a WLAN by entering this command:
  config wlan custom-web sleep-client {**enable** | **disable**} *wlan-id*
- Configure the sleeping client timeout on a WLAN by entering this command:
  config wlan custom-web sleep-client timeout *wlan-id duration*
- View the sleeping client configuration on a WLAN by entering this command:
  show wlan *wlan-id*
- Delete any unwanted sleeping client entries by entering this command:
  config custom-web sleep-client delete *client-mac-addr*
- View a summary of all the sleeping client entries by entering this command:
  show custom-web sleep-client summary
- View the details of a sleeping client entry based on the MAC address of the client by entering this command:
  show custom-web sleep-client detail *client-mac-addr*

Authenticating Sleeping Clients on L2+L3 Enabled WLANs

With this feature enhancement, the sleeping client functionality works even if L2 and L3 credentials are different.

This feature also supports a configuration which allows sleeping clients to be authenticated automatically when they wake up without the need for the user to try web access.

Although the security parameters have not changed, the feature functions with only 802.1X + web authentication setups.

Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (GUI)

Procedure

Step 1 Choose **WLANs** > **WLANs** to open the WLAN page.

Step 2 Click the WLAN-ID number of the WLAN to which you want to configure the feature.

Step 3 Choose the **Security** > **Layer 3** > tab from the **WLANs** > **Edit** page.

Step 4 Check the **Sleeping Client** check box to enable authentication for sleeping clients

Step 5 Enter the value for **Sleeping Client Timeout**,

This is the duration for which the sleeping clients are to be remembered before reauthentication is required. The default timeout is 12 hours.

Step 6 Check the **Sleeping Client Auto Authenticate** check box to enable auto authentication of the sleeping clients when they wake up .

Step 7 Save the configuration.

Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (CLI)

Procedure

- Enable or disable the auto authentication of the sleeping client on wake up without the need for web access by entering this command:

  config wlan custom-web sleep-client authenticate-without-trigger {**enable | disable**} *wlan-id*

  The default value is **Enabled**.

- View the status of the sleeping client authentication by entering this command:

  show wlan *wlan-id*

Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

This section contains the following subsections:

Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under

which the redirect occurs on your RADIUS server. Conditions might include the user's password reaching expiration or the user needing to pay his or her bill for continued usage.

If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair "url-redirect-acl," the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a "url-redirect," the client is considered fully authorized and allowed to pass traffic.

Note The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.

Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server and the corresponding ACL to allow access to this server in "url-redirect-acl". If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a "url-redirect."

Note The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

Suppose there are backend applications running on the wireless clients and they use HTTP or HTTPS port for their communication. If the applications start communicating before the actual web page is opened, the redirect functionality does not work with web passthrough.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Configuring the RADIUS Server (GUI)

Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Procedure

Step 1 From the CiscoSecure ACS main menu, choose **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down list, choose **RADIUS (Cisco IOS/PIX 6.0)**.

Step 4 Select the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://url

url-redirect-acl=acl_name

Configuring Web Redirect

Configuring Web Redirect (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 4 From the Layer 2 Security drop-down list, choose **802.1X** or **WPA+WPA2**.

Step 5 Set any additional parameters for 802.1X or WPA+WPA2.

Step 6 Choose the **Layer 3** tab to open the WLANs > Edit (Security > Layer 3) page.

Step 7 From the Layer 3 Security drop-down list, choose **None**.

Step 8 Check the **Web Policy** check box.

Step 9 Choose one of the following options to enable conditional or splash page web redirect: **Conditional Web Redirect** or **Splash Page Web Redirect**. The default value is disabled for both parameters.

Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring Web Redirect (CLI)

Procedure

Step 1 Enable or disable conditional web redirect by entering this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 Enable or disable splash page web redirect by entering this command:

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 Save your settings by entering this command:

save config

Step 4 See the status of the web redirect features for a particular WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
...
```

Web Authentication Proxy

This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the user's browser is configured with manual proxy settings with a configured port number as 8080 or 3128 and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet proxy settings to automatically detect the proxy settings so that the browser's manual proxy settings information does not get lost. After enabling this settings, the user can get access to the network through the web authentication policy. This functionality is given for port 8080 and 3128 because these are the most commonly used ports for the web proxy server.



Note The web authentication proxy redirect ports are not blocked through CPU ACL. If a CPU ACL is configured to block the port 8080, 3128, and one random port as part of web authentication proxy configuration, those ports are not blocked because the webauth rules take higher precedence than the CPU ACL rules unless the client is in the webauth_req state.

A web browser has the following three types of Internet settings that you can configure:

- Auto detect

- System Proxy
- Manual

In a manual proxy server configuration, the browser uses the IP address of a proxy server and a port. If this configuration is enabled on the browser, the wireless client communicates with the IP address of the destination proxy server on the configured port. In a web authentication scenario, the controller does not listen to such proxy ports and the client is not able to establish a TCP connection with the controller. The user is unable to get any login page to authentication and get access to the network.

When a wireless client enters a web-authenticated WLAN, the client tries to access a URL. If a manual proxy configuration is configured on the client's browser, all the web traffic going out from the client will be destined to the proxy IP and port configured on the browser.

- A TCP connection is established between the client and the proxy server IP address that the controller proxies for.
- The client processes the DHCP response and obtains a JavaScript file from the controller. The script disables all proxy configurations on the client for that session.

Note For external clients, the controller sends the login page as is (with or without JavaScipt).

- Any requests that bypass the proxy configuration. The controller can then perform web-redirection, login, and authentication.
- When the client goes out of the network, and then back into its own network, a DHCP refresh occurs and the client continues to use the old proxy configuration configured on the browser.
- If the external DHCP server is used with webauth proxy, then DHCP option 252 must be configured on the DHCP server for that scope. The value of option 252 will have the format http://<virtual ip>/proxy.js. No extra configuration is needed for internal DHCP servers.

Note When you configure FIPS mode with secure web authentication, we recommend that you use Mozilla Firefox as your browser.

- If web authentication redirect to HTTPS is enabled, then both the client HTTPS and client HTTP requests are redirected to HTTPS web authentication.

Note This enhancement was introduced in Release 8.0.

This section contains the following subsections:

Configuring Web Authentication Proxy (GUI)

Procedure

Step 1 Choose **Controller** > **General**

Step 2 From the **WebAuth Proxy Redirection Mode** drop-down list, choose **Enabled** or **Disabled**.

Step 3 In the **WebAuth Proxy Redirection Port** text box, enter the port number of the web auth proxy.

This text box consists of the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.

Step 4 Click **Apply**.

Configuring Web Authentication Proxy (CLI)

Procedure

- Enable web authentication proxy redirection by entering this command:
  config network web-auth proxy-redirect {**enable** | **disable**}
- Configure the secure web (HTTPS) authentication for clients by entering this command:
  config network web-auth secureweb {**enable** | **disable**}

  The default secure web (HTTPS) authentication for clients is enabled.

Note If you configure to disallow secure web (HTTPS) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the controller to implement the change.

- Set the web authentication port number by entering this command:
  config network web-auth port *port-number*

  This parameter specifies the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.
- Configure secure redirection (HTTPS) for web authentication clients by entering this command:
  config network web-auth https-redirect {**enable** | **disable**}
- See the current status of the web authentication proxy configuration by entering one of the following commands:
  - **show network summary**
  - **show running-config**

Supporting IPv6 Client Guest Access

The client is in WebAuth Required state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once authenticated, the user's MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

In order to support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com which returns a DNSv6 (AAAA) record.

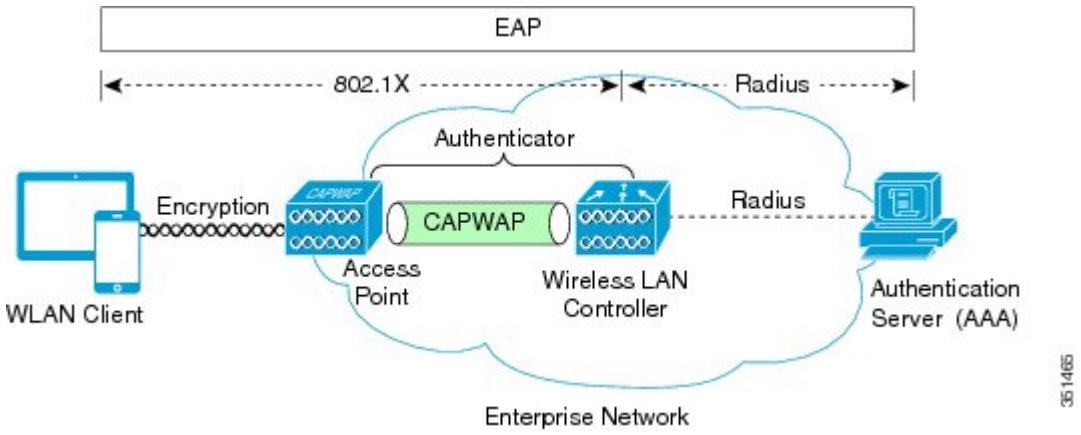
EAP and AAA Servers

This section contains the following subsections:

802.1X and Extensible Authentication Protocol

In order to provide enterprise-level WLAN security, 802.1X and Extensible Authentication Protocol (EAP) authentication mechanisms were implemented to provide mutual authentication of WLANs and WLAN client devices. The following figure shows the basic 802.1X and EAP authentication secure topology.

Figure 5: 802.1X and EAP Wireless LAN Security Topology



802.1X is an IEEE standard for port-based network access control and was adopted by the 802.11i security standard workgroup. The 802.1X standard provides authenticated access to 802.11 wireless LAN networks using the following logic:

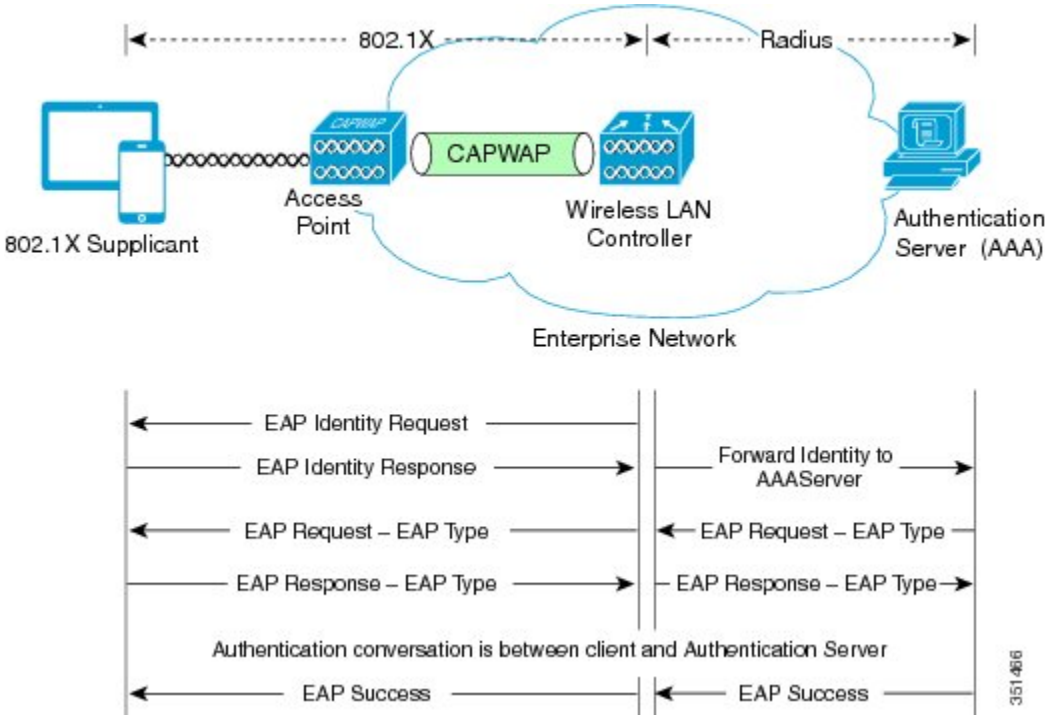
- A virtual port is created at the AP during the 802.11 association process for each WLAN client device.
- The AP then blocks all data frames on this virtual port except for 802.1X-based traffic.
- EAP authentication packets are carried in 802.1X traffic frames and are passed by the AP and Wireless LAN Controller to the AAA authentication server.
- Assuming EAP authentication is successful, the authentication server sends an EAP success message back to the Wireless LAN Controller and AP, which in turn pass the message on to the WLAN client device.

- The AP then allows data traffic (including voice and video) from the WLAN client device to flow through the virtual port.
- Before the virtual port opens to allow data traffic, data link encryption is established between the client device and the AP.

During the authentication process, a unique per-user per-session shared key is derived, and a portion of this key is used as a per-session encryption key.

The EAP authentication process supports a number of protocols, and which protocol is used ultimately depends on the capabilities of the WLAN client device supplicant and the WLAN infrastructure. Regardless of the EAP type that is used, all protocols generally behave as shown in the example EAP flow in the following figure:

Figure 6: EAP Protocol Flow



EAP as defined by RFC 3748 supports four packet types as part of the EAP authentication process:

- **EAP request**: The request packet that is sent by the authenticator (in the preceding figure, it is the Wireless LAN Controller and AP in combination) to the 802.1X supplicant (in the preceding figure, it is the WLAN client device). Each EAP request has a specific type that indicates what is being requested. In the example in the preceding figure, the first EAP request is for the WLAN client device identity, while the second EAP request is for the EAP type to be used for the authentication. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- **EAP response**: The response packet is sent by the WLAN client device to the AP and in turn to the controller, and uses a sequence number to match the initiating EAP request. In the case of an identity or type response, the response is forwarded by the controller to the authentication server.

- **EAP success**: Assuming that the WLAN client device or user has provided appropriate credentials during the authentication conversation, as shown in the preceding figure, the AAA server sends an EAP success packet to the controller, which in turn relays it through the AP to the WLAN client device.
- **EAP failure**: If the appropriate credentials are not provided at the WLAN client device or some other failure occurs, the AAA server sends an EAP failure packet to the controller, which relays it through the AP to the WLAN client device, resulting in failure of the authentication.

For more information, see https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd/CCVP_BK_R7805F20_00_rtowlan-srnd_chapter_0100.html#CCVP_RF_8B1E3C6A_00.

LDAP

An LDAP backend database allows the controller 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 backend database to retrieve user credentials.

Note From Release 8.0, IPv6 can also be used to configure the LDAP server on the controller.

Fallback LDAP Servers

The LDAP servers are configured on a WLAN for authentication. You require at least two LDAP servers to configure them for fallback behavior. A maximum of three LDAP servers can be configured for the fallback behavior per WLAN. The servers are listed in the priority order for authentication. If the first LDAP server becomes irresponsive, then the controller switches to the next LDAP server. If the second LDAP server becomes irresponsive, then the controller switches again to the third LDAP server.

The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, EAP-FAST/EAP-GTC and PEAPv0/MSCHAPv2 are also supported, but only if the LDAP server is set up to return a clear-text password.

Controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory.

This section contains the following subsections:

Configuring LDAP (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **LDAP** to open the LDAP Servers page.

- If you want to delete an existing LDAP server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 2 Perform one of the following:

- To edit an existing LDAP server, click the index number for that server. The **LDAP Servers > Edit** page is displayed.
- To add an LDAP server, click **New**. The **LDAP Servers > New** page is displayed. If you are adding a new server, choose a number from the Server Index (Priority) drop-down list 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 controller cannot reach the first server, it tries the second one in the list and so on.

Step 3 If you are adding a new server, enter the IP address of the LDAP server in the **Server IP Address** field. Both IPv4 and IPv6 addresses are supported.

Step 4 If you are adding a new server, enter the LDAP server's TCP port number in the **Port Number** field. The valid range is 1 to 65535, and the default value is 389.

Note
Only LDAP port 389 is supported on the controller. No other ports are supported for LDAP.

Step 5 From the **Server Mode (via TLS)** drop-down list, choose **Disabled** to establish LDAP connection (without secure tunnel) between LDAP server and the controller using TCP or **Enabled** to establish a secure LDAP connection using TLS.

Step 6 Check the **Enable Server Status** check box to enable this LDAP server or unselect it to disable it. The default value is disabled.

Step 7 From the **Simple Bind** drop-down list, choose **Anonymous** or **Authenticated** to specify the local authentication bind method for the LDAP server. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access. The default value is Anonymous.

Step 8 If you chose **Authenticated** in the previous step, follow these steps:

a) In the **Bind Username** field, enter a 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 controller 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.

b) In the **Bind Username** field, enter a username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

Step 9 In the **User Base DN** field, enter the 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 containing users is the base DN, type.

o=*corporation*.com

or

dc=*corporation*, **dc=com**

Step 10 In the **User Attribute** field, enter the name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.

Step 11 In the **User Object Type** field, enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.

Step 12 In the **Server Timeout** field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 13 Click **Apply** to commit your changes.

Step 14 Click **Save Configuration** to save your changes.

Step 15 Specify LDAP as the priority backend database server for local EAP authentication as follows:

a) Choose **Security** > **Local EAP** > **Authentication Priority** to open the **Priority Order > Local-Auth** page.

b) Highlight **LOCAL** and click **<** to move it to the left **User Credentials** field.

c) Highlight **LDAP** and click **>** to move it to the right **User Credentials** field. The database that is displayed at the top of the right **User Credentials** field is used when retrieving user credentials.

Note
If both LDAP and LOCAL appear in the right **User Credentials** field with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend 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 backend database.

d) Click **Apply** to commit your changes.

e) Click **Save Configuration** to save your changes.

Step 16 (Optional) Assign specific LDAP servers to a WLAN as follows:

a) Choose **WLANs** to open the WLANs page.

b) Click the ID number of the desired WLAN.

c) When the **WLANs > Edit** page is displayed, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.

d) From the **LDAP Servers** drop-down lists, choose the LDAP server(s) that you want to use with this WLAN. You can choose up to three LDAP servers, which are tried in priority order.

Note
These LDAP servers apply only to WLANs with web authentication enabled. They are not used by local EAP.

e) Click **Apply** to commit your changes.

f) Click **Save Configuration** to save your changes.

Step 17 Specify the LDAP server fallback behavior, as follows:

a) Choose **WLAN** > **AAA Server** to open the **Fallback Parameters** page.

b) From the **LDAP Servers** drop-down list, choose the LDAP server in the order of priority when the controller attempts to authenticate management users. The order of authentication is from server.

c) Choose **Security** > **AAA** > **LDAP** to view the list of global LDAP servers configured for the controller.

Configuring LDAP (CLI)

Procedure

- Configure an LDAP server by entering these commands:

- **config ldap add** *index server_ip_address port# user_base user_attr user_type* **secure**— Adds an LDAP server for secure LDAP.
- **config ldap delete** *index*—Deletes a previously added LDAP server.
- **config ldap** {**enable** | **disable**} *index*—Enables or disables an LDAP server.
- **config ldap security-mode enable** *index*—Enables the LDAP server using index with existing commands.
- **config ldap simple-bind** {**anonymous** *index* | **authenticated** *index* **username** *username* **password** *password*}—Specifies the local authentication bind method for the LDAP server. The anonymous method allows anonymous access to the LDAP server whereas the authenticated method requires that a username and password be entered to secure access. The default value is anonymous. The username can contain up to 80 characters.

  If the username starts with "cn=" (in lowercase letters), the controller 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.
- **config ldap retransmit-timeout** *index timeout*—Configures the number of seconds between retransmissions for an LDAP server.

• Specify LDAP as the priority backend database server by entering this command:

config local-auth user-credentials ldap

If you enter the **config local-auth user-credentials ldap local command**, local EAP attempts to authenticate clients using the LDAP backend 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 you enter the **config local-auth user-credentials local ldap command**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

• (Optional) Assign specific LDAP servers to a WLAN by entering these commands:

- **config wlan ldap add** *wlan_id server_index*—Links a configured LDAP server to a WLAN.

  The LDAP servers specified in this command apply only to WLANs with web authentication enabled. They are not used by local EAP.
- **config wlan ldap delete** *wlan_id* {*all* | *index*}—Deletes a specific or all configured LDAP server(s) from a WLAN.

• View information pertaining to configured LDAP servers by entering these commands:

- **show ldap summary**—Shows a summary of the configured LDAP servers.

```
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4           389    No
2    10.10.20.22       389    Yes


Idx      Server Address      Port     Enabled  Secure
---      --------------      -----    ------  -------
1         2.3.1.4            389       No       No
2         2.3.1.5            389       Yes      No
```

- **show ldap** *index*—Shows detailed LDAP server information. Information like the following appears:

```
Server Index..................................... 2
Address.......................................... 10.10.20.22
Port............................................. 389
Enabled.......................................... Yes
User DN.......................................... ou=active,ou=employees,ou=people,

    o=cisco.com
User Attribute................................... uid
User Type........................................ Person
Retransmit Timeout............................... 2 seconds
Bind Method ..................................... Authenticated
Bind Username.................................... user1
```

```
(Cisco Controller)> show ldap 1
Server Index..................................... 1
Address.......................................... 9.1.0.100
Port............................................. 389
Server State..................................... Disabled
User DN.......................................... user1
User Attribute................................... user
User Type........................................ user
Retransmit Timeout............................... 2 seconds
Secure (via TLS)................................. Disabled
Bind Method ..................................... Anonymous
```

- **show ldap statistics**—Shows LDAP server statistics.

```
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed.......................... 0
  Server not found............................... 0
  No received attributes......................... 0
  No passed username............................. 0
  Not connected to server........................ 0
  Internal error................................. 0
  Retries........................................ 0

Server Index..................................... 2
..
```

- **show wlan** *wlan_id*—Shows the LDAP servers that are applied to a WLAN.

- Make sure the controller can reach the LDAP server by entering this command:
  ping *server_ip_address*
- Save your changes by entering this command:
  save config
- Enable or disable debugging for LDAP by entering this command:
  debug aaa ldap {**enable | disable}**

Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

This section contains the following subsections:

Related Topics

Downloading Device Certificates

Restrictions for Local EAP

- Timer restrictions for local and central authentication using EAP: The EAP timeout cannot be configured on Wave 2 APs. Even though you can configure the EAP timeout on the controller, for Wave 2 APs, the EAP timeout is hardcoded to 30 seconds. This is due to the following reasons:
  - Clients get stuck in 8021X state indefinitely if AP moves from connected to standalone mode while EAP is in process.
  - Controller does not send EAP frames due to some issue, resulting in clients getting stuck indefinitely at AP.

  This has impact on clients, such as Windows clients, that wait for EAP identity request to pop up and are prompted for username and password. This issue is not seen on clients such as Apple, Samsung, Zebra, or WPA supplicants because they take the username and password beforehand.
- For mesh APs, you cannot configure EAP parameters. The mesh APs have the following static EAP configuration: EAP request timeout set to 60 seconds and the maximum number of EAP identity request retries set to 2.
- Legacy clients that require RC4 or 3DES encryption type are not supported in Local EAP authentication.

Configuring Local EAP (GUI)

Before you begin

Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

Procedure

Step 1 If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.

Step 2 If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.

Step 3 If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.

Step 4 Specify the order in which user credentials are retrieved from the backend database servers as follows:

a) Choose **Security** > **Local EAP** > **Authentication Priority** to open the **Priority Order > Local-Auth** page.

b) Determine the priority order in which user credentials are to be retrieved from the local and/or LDAP databases. For example, you may want the LDAP database to be given priority over the local user database, or you may not want the LDAP database to be considered at all.

c) When you have decided on a priority order, highlight the desired database. Then 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 backend 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 backend database.

d) Click **Apply** to commit your changes.

Step 5 Specify values for the local EAP timers as follows:

a) Choose **Security** > **Local EAP** > **General** to open the General page.

b) In the **Local Auth Active Timeout** field, enter the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 300 seconds.

Step 6 Specify values for the **Advanced EAP** parameters as follows:

a) Choose **Security**> **Advanced EAP**.

b) In the **Identity Request Timeout** field, enter the amount of time (in seconds) in which the controller 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 30 seconds.

c) In the **Identity Request Max Retries** field, enter the maximum number of times that the controller 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 2 retries.

d) In the **Dynamic WEP Key Index** field, enter the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

This feature is no longer supported.

e) In the **Request Timeout** field, enter the amount of time (in seconds) in which the controller 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 30 seconds.

f) In the **Request Max Retries** field, enter the maximum number of times that the controller 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 2 retries.

g) From the **Max-Login Ignore Identity Response** drop-down list, enable the feature if you want to ignore the EAP identity responses when enforcing the net user login limit.

h) In the **EAPOL-Key Timeout** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.

i) In the **EAPOL-Key Max Retries** field, enter the maximum number of times that the controller 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.

j) In the **EAP-Broadcast Key Interval** field, enter the interval between the Group Temporal Key (GTK) key rotation for all the stations on a BSSID that is using WPA protocol. The default interval is 3600 seconds.

k) Click **Apply** to commit your changes.

Step 7 Create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients as follows:

a) Choose **Security** > **Local EAP** > **Profiles** to open the Local EAP Profiles page.

This page lists any local EAP profiles that have already been configured and specifies their EAP types. You can create up to 16 local EAP profiles.

Note
If you want to delete an existing profile, hover your cursor over the blue drop-down arrow for that profile and choose **Remove**.

b) Click **New** to open the **Local EAP Profiles > New** page.

c) In the **Profile Name** field, enter a name for your new profile and then click **Apply**.

Note
You can enter up to 63 alphanumeric characters for the profile name. Make sure not to include spaces.

d) When the **Local EAP Profiles** page is displayed again, click the name of your new profile. The **Local EAP Profiles > Edit** page is displayed.

e) Check the **LEAP**, **EAP-FAST**, **EAP-TLS,** and/or **PEAP** check boxes to specify the EAP type that can be used for local authentication.

Note
You can specify more than one EAP type per profile. However, if you choose multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all the EAP types must use the same certificate (from either Cisco or another vendor).

Note
If you check the **PEAP** check box, both PEAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

f) If you chose EAP-FAST and want the device certificate on the controller to be used for authentication, check the **Local Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note

This option applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

g) If you chose EAP-FAST and want the wireless clients to send their device certificates to the controller in order to authenticate, check the **Client Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unchecked, which is the default setting.

Note
This option applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

h) If you chose EAP-FAST with certificates, EAP-TLS, or PEAP, choose which certificates will be sent to the client, the ones from **Cisco** or the ones from another **Vendor**, from the **Certificate Issuer** drop-down list. The default setting is Cisco.

i) If you chose EAP-FAST with certificates or EAP-TLS and want the incoming certificate from the client to be validated against the CA certificates on the controller, check the **Check against CA certificates** check box. The default setting is enabled.

j) If you chose EAP-FAST with certificates or EAP-TLS and want the common name (CN) in the incoming certificate to be validated against the Local Net Users configured on the controller, check the **Verify Certificate CN Identity** check box. The default setting is disabled.

k) If you chose EAP-FAST with certificates or EAP-TLS and want the controller to verify that the incoming device certificate is still valid and has not expired, check the **Check Certificate Date Validity** check box. The default setting is enabled.

Note
Certificate date validity is checked against the current UTC (GMT) time that is configured on the controller. Timezone offset will be ignored.

l) Click **Apply** to commit your changes.

Step 8 If you created an EAP-FAST profile, follow these steps to configure the EAP-FAST parameters:

a) Choose **Security** > **Local EAP** > **EAP-FAST Parameters** to open the EAP-FAST Method Parameters page.

b) In the **Server Key** and **Confirm Server Key** fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

c) In the **Time to Live for the PAC** field, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

d) In the **Authority ID** field, enter the 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.

e) In the **Authority ID Information** field, enter the authority identifier of the local EAP-FAST server in text format.

f) If you want to enable anonymous provisioning, check the **Anonymous Provision** check box. 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. The default setting is enabled.

Note
If the local and/or client certificates are required and you want to force all EAP-FAST clients to use certificates, uncheck the **Anonymous Provision** check box.

g) Click **Apply** to commit your changes.

Step 9 Enable local EAP on a WLAN as follows:

a) Choose **WLANs** to open the WLANs page.

b) Click the ID number of the desired WLAN.

c) When the **WLANs > Edit** page is displayed, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.
d) Uncheck the **Enabled** check boxes for RADIUS Authentication Servers and Accounting Server to disable RADIUS accounting and authentication for this WLAN.
e) Check the **Local EAP Authentication** check box to enable local EAP for this WLAN.
f) From the **EAP Profile Name** drop-down list, choose the EAP profile that you want to use for this WLAN.
g) If desired, choose the LDAP server that you want to use with local EAP on this WLAN from the **LDAP Servers** drop-down lists.
h) Click **Apply** to commit your changes.

Step 10 Enable EAP parameters on a WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the desired WLAN.
c) When the **WLANs > Edit** page is displayed, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.
d) Check the **Enable** check box to configure EAP parameters for this WLAN.
e) In the **EAPOL Key Timeout (200 to 5000 millisec)** field, enter the amount of time (in milliseconds) in which the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds and the default value is 1000 milliseconds.
f) In the **EAPOL Key Retries (0 to 4)** field, enter the maximum number of times that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 0 to 4 retries and the default setting is 2 retries.
g) In the **Identity Request Timeout (1 to 120 sec)** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds and the default value is 30 seconds.
h) In the **Identity Request Retries (1 to 20 sec)** field, enter the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
i) In the **Request Timeout (1 to 120 sec)** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
j) In the **Request Retries (1 to 20 sec)** field, enter the maximum number of times that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
k) Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Configuring Local EAP (CLI)

Before you begin

Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACbs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

Procedure

Step 1 If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.

Step 2 If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.

Step 3 If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.

Step 4 Specify the order in which user credentials are retrieved from the local and/or LDAP databases by entering this command:

config local-auth user-credentials {*local* | *ldap*}

Note
If you enter the **config local-auth user-credentials ldap local** command, local EAP attempts to authenticate clients using the LDAP backend 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 you enter the **config local-auth user-credentials local ldap command**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

Step 5 Specify values for the local EAP timers by entering these commands:

- **config advanced eap identity-request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller 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 30 seconds.
- **config advanced eap bcast-key-interval** *seconds*—Configures EAP-broadcast key renew interval time in seconds. The valid range is 120 to 86400 seconds.
- **config advanced eap identity-request-retries** *retries*—Specifies the maximum number of times that the controller 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.
- **config advanced eap key-index** *index*—Specifies the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).
- **config advanced eap request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller 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 30 seconds.
- **config advanced eap request-retries** *retries*—Specifies the maximum number of times that the controller 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.
- **config advanced eap eapol-key-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.

  Note
  If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

- **config advanced eap eapol-key-retries** *retries*—Specifies the maximum number of times that the controller 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.
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}—

  Enable the feature if you want to ignore the EAP identity responses when enforcing the net user login limit. See the User Login Policies section for details.

Step 6 Specify values for the local EAP timers on a WLAN by entering these commands:

- **config wlan security eap-params {enable | disable}** *wlan_id*—Specifies to enable or disable SSID specific EAP timeouts or retries. The default value is disabled.
- **config wlan security eap-params eapol-key-timeout** *timeout wlan_id*—Specifies the amount of time (in milliseconds) in which the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.
- **config wlan security eap-params eapol-key-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
- **config wlan security eap-params identity-request-timeout** *timeout wlan_id*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config wlan security eap-params identity-request-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
- **config wlan security eap-params request-timeout** *timeout wlan_id*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config wlan security eap-params request-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.

Step 7 Create a local EAP profile by entering this command:

config local-auth eap-profile add *profile_name*

Note
Do not include spaces within the profile name.

Note
To delete a local EAP profile, enter the **config local-auth eap-profile delete** *profile_name* command.

Step 8 Add an EAP method to a local EAP profile by entering this command:

config local-auth eap-profile method add *method profile_name*

The supported methods are leap, fast, tls, and peap.

Note
If you choose peap, both P EAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

Note
You can specify more than one EAP type per profile. However, if you create a profile with multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all of the EAP types must use the same certificate (from either Cisco or another vendor).

Note

To delete an EAP method from a local EAP profile, enter the **config local-auth eap-profile method delete** *method profile_name* command.

Step 9 Configure EAP-FAST parameters if you created an EAP-FAST profile by entering this command:

config local-auth method fast *?*

where *?* is one of the following:

- **anon-prov** {**enable** | **disable**}—Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during PAC provisioning.
- **authority-id** *auth_id*—Specifies the authority identifier of the local EAP-FAST server.
- **pac-ttl** *days*—Specifies the number of days for the PAC to remain viable.
- **server-key** *key*—Specifies the server key used to encrypt and decrypt PACs.

Step 10 Configure certificate parameters per profile by entering these commands:

- **config local-auth eap-profile method fast local-cert** {**enable** | **disable**} *profile_name*— Specifies whether the device certificate on the controller is required for authentication.

  Note
  This command applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

- **config local-auth eap-profile method fast client-cert** {**enable** | **disable**} *profile_name*— Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.

  Note
  This command applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

- **config local-auth eap-profile cert-issuer** {**cisco** | **vendor**} *profile_name*—If you specified EAP-FAST with certificates, EAP-TLS, or PEAP, specifies whether the certificates that will be sent to the client are from Cisco or another vendor.
- **config local-auth eap-profile cert-verify ca-issuer** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the incoming certificate from the client is to be validated against the CA certificates on the controller.
- **config local-auth eap-profile cert-verify cn-verify** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
- **config local-auth eap-profile cert-verify date-valid** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Step 11 Enable local EAP and attach an EAP profile to a WLAN by entering this command:

config wlan local-auth enable *profile_name wlan_id*

Note
To disable local EAP for a WLAN, enter the **config wlan local-auth disable** *wlan_id command.*

Step 12 Save your changes by entering this command:

save config

Step 13 View information pertaining to local EAP by entering these commands:

- **show local-auth config—**Shows the local EAP configuration on the controller.

```
User credentials database search order:
   Primary ..................................... Local DB

Timer:
    Active timeout ............................. 300

Configured EAP profiles:
   Name ........................................ fast-cert
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. Yes
       Client certificate required ............. Yes
     Enabled methods ........................... fast
     Configured on WLANs ....................... 1

   Name ........................................ tls
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. No
       Client certificate required ............. No
     Enabled methods ........................... tls
     Configured on WLANs ....................... 2

EAP Method configuration:
   Low-Cipher Support(TLSv1.0 for local EAP)..... Enabled
   EAP-FAST:
     Server key ................................ <hidden>
     TTL for the PAC ........................... 10
     Anonymous provision allowed ............... Yes
     Accept client on auth prov ................ No
     Authority ID ...... 436973636f00000000000000000000000
     Authority Information ..................... Cisco A-ID
```

- **show local-auth statistics**—Shows the local EAP statistics.
- **show local-auth certificates**—Shows the certificates available for local EAP.
- **show local-auth user-credentials**—Shows the priority order that the controller uses when retrieving user credentials from the local and/or LDAP databases.
- **show advanced eap**—Shows the timer values for local EAP.

```
EAP-Identity-Request Timeout (seconds)........... 1
EAP-Identity-Request Max Retries................. 20
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response........... enable
EAP-Request Timeout (seconds).................... 20
EAP-Request Max Retries.......................... 20
EAPOL-Key Timeout (seconds)...................... 1
```

```
EAPOL-Key Max Retries..................... 2
```

- **show ap stats wlan** *Cisco_AP*—Shows the EAP timeout and failure counters for a specific access point for each WLAN.
- **show client detail** *client_mac*—Shows the EAP timeout and failure counters for a specific associated client. These statistics are useful in troubleshooting client association issues.

```
...
Client Statistics:
      Number of Bytes Received.................. 10
      Number of Bytes Sent...................... 10
      Number of Packets Received................ 2
      Number of Packets Sent.................... 2
      Number of EAP Id Request Msg Timeouts..... 0
      Number of EAP Id Request Msg Failures..... 0
      Number of EAP Request Msg Timeouts........ 2
      Number of EAP Request Msg Failures........ 1
      Number of EAP Key Msg Timeouts............ 0
      Number of EAP Key Msg Failures............ 0
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... Unavailable
      Signal to Noise Ratio..................... Unavailable
```

- **show wlan** *wlan_id*—Shows the status of local EAP on a particular WLAN.

Step 14 (Optional) Troubleshoot local EAP sessions by entering these commands:

- **debug aaa local-auth eap method** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}— Enables or disables debugging of local EAP methods.
- **debug aaa local-auth eap framework** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}— Enables or disables debugging of the local EAP framework.

  Note
  In these two debug commands, **sm** is the state machine.

- **clear stats local-auth**—Clears the local EAP counters.
- **clear stats ap wlan** *Cisco_AP*—Clears the EAP timeout and failure counters for a specific access point for each WLAN.

```
WLAN      1
   EAP Id Request Msg Timeouts.................. 0
   EAP Id Request Msg Timeouts Failures......... 0
   EAP Request Msg Timeouts..................... 2
   EAP Request Msg Timeouts Failures............ 1
   EAP Key Msg Timeouts......................... 0
   EAP Key Msg Timeouts Failures................ 0
WLAN      2
   EAP Id Request Msg Timeouts.................. 1
   EAP Id Request Msg Timeouts Failures......... 0
   EAP Request Msg Timeouts..................... 0
   EAP Request Msg Timeouts Failures............ 0
   EAP Key Msg Timeouts......................... 3
EAP Key Msg Timeouts Failures.............. 1
```

Local Network Users on Controller

You can add local network users to the local user database on the controller. The local user database stores the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. Local network user entries can be used to authenticate clients through web authentication or local EAP.

This section contains the following subsections:

Configuring Local Network Users for the Controller (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **Local Net Users** to open the Local Net Users page.

Note
If you want to delete an existing user, hover your cursor over the blue drop-down arrow for that user and choose **Remove**.

When admin modifies the credentials of a local network user, the user gets disassociated from the WLAN. Here, credentials refer to the change in password or wlan profile for that user.

Step 2 Perform one of the following:

- To edit an existing local network user, click the username for that user. The **Local Net Users > Edit** page appears.
- To add a local network user, click **New**. The **Local Net Users > New** page appears.

Step 3 If you are adding a new user, enter a username for the local user in the **User Name** text box. You can enter up to 49 alphanumeric characters.

Note
Local network usernames must be unique because they are all stored in the same database.

Step 4 In the **Password** and **Confirm Password** text boxes, enter a password for the local user. You can enter up to 49 alphanumeric characters.

Step 5 If you are adding a new user, select the **Guest User** check box if you want to limit the amount of time that the user has access to the local network. The default setting is unselected.

Step 6 If you are adding a new user and 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 2,592,000 seconds (30 days) inclusive, and the default setting is 86,400 seconds.

Step 7 If you are adding a new user, you selected the **Guest User** check box, and you want to assign a QoS role to this guest user, select the **Guest User Role** check box. The default setting is unselected.

Note
If you do not assign a QoS role to a guest user, the bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Step 8 If you are adding a new user and you selected the **Guest User Role** check box, choose the QoS role that you want to assign to this guest user from the Role drop-down list.

Step 9 From the WLAN Profile drop-down list, choose the name of the WLAN that is to be accessed by the local user. If you choose **Any WLAN**, which is the default setting, the user can access any of the configured WLANs.

Note
If you are deleting a WLAN associated with network users, then the system prompts you to delete all network users associated with the WLAN before deleting the WLAN itself.

Step 10 In the **Description** text box, enter a descriptive title for the local user (such as "User 1").

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring Local Network Users for the Controller (CLI)

Procedure

- Configure a local network user by entering these commands:
  - **config netuser add** *username password* **wlan** *wlan_id userType* **permanent description** *description*—Adds a permanent user to the local user database on the controller.
  - **config netuser add** *username password* {**wlan | guestlan} {***wlan_id* | *guest_lan_id}* **userType guestlifetime** *seconds* **description** *description*—Adds a guest user on a WLAN or wired guest LAN to the local user database on the controller.

Note Instead of adding a permanent user or a guest user to the local user database from the controller, you can choose to create an entry on the RADIUS server for the user and enable RADIUS authentication for the WLAN on which web authentication is performed.

  - **config netuser delete** {**username** *username* | **wlan-id** *wlan-id*}
    - *username*—Deletes a user from the local user database on the controller.

Note Local network usernames must be unique because they are all stored in the same database.

    - *wlan-id*—Delete all the network users associated with the WLAN ID.

Note When a WLAN associated with network users is deleted, the system prompts to delete all network users associated with the WLAN first. After deleting the network users, you can delete the WLAN.

- See information related to the local network users configured on the controller by entering these commands:

- **show netuser detail** *username*—Shows the configuration of a particular user in the local user database.
- **show netuser summary**—Lists all the users in the local user database.

- Save your changes by entering this command:

  save config

Uploading PACs for EAP-FAST

Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication with a local EAP authentication server during EAP-FAST authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller.

Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the PAC upload. Follow these guidelines when setting up a TFTP or FTP server:

- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

PAC Provisioning and Device Enrolment

Controller device enrollment is initiated by controller as part of Protected Access Credential (PAC) provisioning with the Cisco ISE server. Controller initiates EAP-FAST and gets a PAC. This is accomplished by using the infrastructure of LOCAL-EAP EAP-FAST PAC provisioning. The PAC that is obtained uniquely maps to the device ID. If the device ID changes, the PAC data associated with the previous device ID is removed from the PAC store. PAC provisioning is triggered when a RADIUS server instance is enabled to provision the PAC.

Note Ensure that the Cisco ISE and the controller time are synchronized for PAC to be downloaded on controller appropriately.

In a High Availability (HA) setup, PACs are not shared over redundancy channel; instead, PAC download is reinitiated on a new active controller immediately after switchover.

This section contains the following subsections:

Uploading PACs (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **PAC (Protected Access Credential)**.

Step 3 In the **User** field, enter the name of the user who will use the PAC.

Step 4 In the **Validity** field, enter the number of days for the PAC to remain valid. The default setting is zero (0).

Step 5 In the **Password** and **Confirm Password** text boxes, enter a password to protect the PAC.

Step 6 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 7 In the **IP Address (IPv4/IPv6)** field, enter the IPv4/IPv6 address of the server.

Step 8 In the **File Path** field, enter the directory path of the PAC.

Step 9 In the **File Name** field, enter the name of the PAC file. PAC files have a .pac extension.

Step 10 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 11 Click **Upload** to upload the PAC from the controller. A message appears indicating the status of the upload.

Step 12 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Uploading PACs (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to upload the config file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 3 Upload a Protected Access Credential (PAC) by entering this command:

transfer upload datatype pac

Step 4 Specify the identification of the user by entering this command:

transfer upload pac *username validity password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Note
The server supports both, IPv4 and IPv6.

Step 6 Specify the directory path of the config file by entering this command:

transfer upload path *server-path-to-file*

Step 7 Specify the name of the config file to be uploaded by entering this command:

transfer upload filename *manual*.pac.

Step 8 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note
The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

Step 10 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Advanced WLAN Security

This section contains the following subsections:

AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Most of the configuration to allow AAA override is done at the RADIUS server, where you should configure the Access Control Server (ACS) with the override properties you would like it to return to the controller (for example, Interface-Name, QoS-Level, and VLAN-Tag).

On the controller, enable the **Allow AAA Override** configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.

This section contains the following subsections:

Restrictions for AAA Override

- If a client moves to a new interface due to the AAA override and then you apply an ACL to that interface, the ACL does not take effect until the client reauthenticates. To work around this issue, apply the ACL and then enable the WLAN so that all clients connect to the ACL that is already configured on the interface, or disable and then reenable the WLAN after you apply the interface so that the clients can reauthenticate.
- If the ACL returned from the AAA server does not exist on the controller or if the ACL is configured with an incorrect name, then the clients are not allowed to be authenticated.
- With FlexConnect local switching, Multicast is forwarded only for the VLAN that the SSID is mapped to and not to any overridden VLANs. Therefore, IPv6 does not work as expected because Multicast

traffic is forwarded from the incorrect VLAN. Use the following command to have multicast traffic forwarded for the overridden VLAN:

config flexconnect group *group-name* **multicast overridden-interface enable**

- Most of the configuration for allowing AAA override is done at the RADIUS server, where you should configure the Access Control Server (ACS) with the override properties you would like it to return to the controller (for example, Interface-Name, QoS-Level, and VLAN-Tag).
- On the controller, enable the Allow AAA Override configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.
- During Layer2 authentication if AAA override is enabled, local policies are not applied and the override takes precedence.
- Cisco TrustSec security group tag is not applied until you enable AAA override on a WLAN.

Updating the RADIUS Server Dictionary File for Proper QoS Values

If you are using a Steel-Belted RADIUS (SBR), FreeRadius, or similar RADIUS server, clients may not obtain the correct QoS values after the AAA override feature is enabled. For these servers, which allow you to edit the dictionary file, you need to update the file to reflect the proper QoS values: Silver is 0, Gold is 1, Platinum is 2, and Bronze is 3. To update the RADIUS server dictionary file, follow these steps:



Note This issue does not apply to the Cisco Secure Access Control Server (ACS).

To update the RADIUS server dictionary file, follow these steps:

1. Stop the SBR service (or other RADIUS service).
2. Save the following text to the `Radius_Install_Directory\Service` folder as `ciscowlan.dct`:

```
##################################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
##################################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level          Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze     3
VALUE Aire-QoS-Level Silver     0
```

```
VALUE Aire-QoS-Level Gold       1
VALUE Aire-QoS-Level Platinum   2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

###############################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
###############################################################################
```

3. Open the `dictiona.dcm` file (in the same directory) and add the line "@ciscowlan.dct."
4. Save and close the `dictiona.dcm` file.
5. Open the `vendor.ini` file (in the same directory) and add the following text:

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id              =
```

6. Save and close the `vendor.ini` file.
7. Start the SBR service (or other RADIUS service).
8. Launch the SBR Administrator (or other RADIUS Administrator).
9. Add a RADIUS client (if not already added). Choose **Cisco WLAN Controller** from the Make/Model drop-down list.

Configuring AAA Override (GUI)

Procedure

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the ID number of the WLAN that you want to configure. The **WLANs > Edit** page appears.

Step 3 Choose the **Advanced** tab.

Step 4 Select the **Allow AAA Override** check box to enable AAA override or unselect it to disable this feature. The default value is disabled.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring AAA Override (CLI)

Procedure

- Configure override of user policy through AAA on a WLAN by entering this command:
  config wlan aaa-override {**enable** | **disable**} *wlan-id*

  For *wlan-id*, enter a value between 1 and 16.
- Configure debugging of 802.1X AAA interactions by entering this command:
  debug dot1x aaa {**enable** | **disable**}
- Configure debugging of AAA QoS override by entering this command:
  debug ap aaaqos-dump {**enable** | **disable**}

ISE NAC Support

The Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of the Cisco Network Admission Control (NAC) in one integrated platform.

Cisco ISE was introduced in Cisco Wireless Release 7.0.116.0. Cisco ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your controller. When a client associates with a controller on a ISE NAC–enabled WLAN with OPEN/Layer 2 + MAC Filtering, the controller forwards the request to the Cisco ISE server without verifying in the local database.

Note ISE NAC was previously known as RADIUS NAC.

This section contains the following subsections:

Device Registration

Device registration enables you to authenticate and provision new devices on the WLAN with RADIUS NAC enabled. When a device is registered on the WLAN, it can use the network based on the configured ACL.

Central Web Authentication

In the case of Central Web Authentication (CWA), web authentication occurs on the Cisco ISE server. The web portal in the Cisco ISE server provides a login page to a client. After the credentials are verified on the Cisco ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a change of authorization (CoA) is reached. The credentials and ACLs are received from Cisco ISE server.

Note

- In a CWA and MAC filtering configuration scenario, if a change in VLAN occurs during pre-authentication and post-authentication, dissociation request is sent to clients and the clients are forced to go through DHCP again.
- Inter-controller roaming with non-802.1X L2 security, with MAC filtering and CWA, is not supported prior to 8.9.

For new clients, the RADIUS access accept message carries redirected URL for port 80 and pre-auth ACLs or quarantine VLAN. Definition of ACL is defined in the controller (IP addresses and ports).

Clients will be redirected to the URL provided in the access accept message and put into a new state until posture validation is done. Clients in this state validate themselves against ISE server and the policies configured on the ISE NAC server.

The NAC agent on the clients initiates posture validation (traffic to port 80): The agent sends HTTP discovery request to port 80, which the controller redirects to the URL provided in the access accept message. Cisco ISE knows that the client is trying to reach and responds directly to the client. This way, the client learns about the Cisco ISE IP address and from now on, the client talks directly with the Cisco ISE.

The controller allows this traffic because the ACL is configured to allow this traffic. In case of VLAN override, the traffic is bridged so that it reaches the Cisco ISE.

ISE NAC

After the client completes the assessment, a RADIUS CoA-Req with reauth service is sent to the controller. This initiates reauthentication of the client (by sending EAP-START). Once reauthentication succeeds, the Cisco ISE sends an access accept message with a new ACL (if any) and no URL redirect, or access VLAN.

The controller has support for CoA-Req and Disconnect-Req as per RFC 3576. The controller needs to support CoA-Req for re-auth service, as per RFC 5176.

Instead of downloadable ACLs, pre-configured ACLs are used on the controller. Cisco ISE sends the ACL name, which is already configured in the controller.

This design should work for both VLAN and ACL cases. In case of VLAN override, the port 80 is redirected and allows (bridge) rest of the traffic on the quarantine VLAN. For the ACL, the pre-auth ACL received in the access accept message is applied.

Here is the workflow:

1. The guest user associates with the controller.
2. The controller sends a MAB Request to ISE.
3. ISE matches the first authorization rules, and sends the redirect parameters (ACL and URL).
4. The controller redirects the GUEST to ISE.
5. After the guest is authenticated, ISE makes a second authorization, which is called RADIUS Change of Authorization (CoA). In this second authorization, a profile must be returned so that the guest is permitted access to the network. We can use usecase: guestflow to easily match this second authorization.



Note Guest clients connecting to a web-auth WLAN in a CWA setup may also reach the internal virtual interface web-auth login page using port 80 or by using port 443 when the web authentication secure web is enabled in the Cisco AireOS controllers. This behavior is in line with how Cisco AireOS controllers handle all web authentication redirect scenarios and have no potential risk or vulnerability.

Local Web Authentication

Local web authentication is not supported for RADIUS NAC.

Table 1: ISE Network Authentication Flow

WLAN Configuration	CWA	LWA	Device Registration
RADIUS NAC Enabled	Yes	No	Yes
L2 PSK	802.1X	PSK	No
L3 None	N/A	Internal/External	N/A
MAC Filtering Enabled	Yes	No	Yes

Guidelines and Restrictions on ISE NAC Support

Guidelines

- When either an authentication or accounting RADIUS server fails, the corresponding server in the authentication or accounting server list will be made inactive. This ensures that client authentication and accounting occurs on the same IP authentication and accounting servers. However, the authentication and accounting servers should be added in the same order while configuring the RADIUS servers if they have to work together.
- When a client moves from one WLAN to another, the controller retains the client's audit session ID if it returns to the WLAN before the idle timeout occurs. As a result, when the client associates with the controller before the idle timeout session expires, it is immediately moved to Run state. The client is validated if it reassociates with the controller after the session timeout.
- If you have two WLANs, and WLAN 1 is configured on a controller (WLC1) and WLAN2 is configured on another controller (WLC2) and both are ISE NAC enabled, the client first connects to WLC1 and moves to the RUN state after posture validation. Assume that the client now moves to WLC2. If the client connects back to WLC1 before the PMK expires for this client in WLC1, the posture validation is skipped for the client. The client directly moves to Run state by passing posture validation because the controller retains the old audit session ID for the client that is already known to Cisco ISE.
- When deploying ISE NAC in your wireless network, do not configure a primary and secondary Cisco ISE server. Instead, we recommend that you configure High Availability (HA) between the two Cisco ISE servers. Having a primary and secondary ISE setup will require posture validation to occur before the clients move to the Run state. If HA is configured, the client is automatically moved to the Run state in the fallback Cisco ISE server.
- Do not swap AAA server indexes in a live network because clients might get disconnected and have to reconnect to the RADIUS server, which might result in log messages to be appended to the ISE server logs.
- Enable AAA override on the WLAN to use ISE NAC.
- ISE NAC is supported with open authentication/Layer 2 (PSK/802.1x) + MAC Filtering security types.
- During slow roaming, clients go through posture validation.
- If the AAA url-redirect-acl and url-redirect attributes are expected from the AAA server, the AAA override feature must be enabled on the controller.

Restrictions

- For ISE NAC WLANs, the MAC authentication request is always sent to the external RADIUS server. The MAC authentication is not validated against the local database. This functionality is applicable to Releases 8.5, 8.7, 8.8, and later releases via the fix for CSCvh85830.
- The ISE NAC functionality does not work if the configured accounting server is different from the authentication (Cisco ISE) server. You should configure the same server as the authentication and accounting server if Cisco ISE functionalities are used. If Cisco ISE is used only for Cisco ACS functionality, the accounting server can be flexible.
- The controller software configured with ISE NAC does not support a CoA on the service port.
- Guest tunneling mobility is supported only for ISE NAC–enabled WLANs.
- VLAN select is not supported.
- Workgroup bridges are not supported.
- The AP Group over NAC is not supported in ISE NAC.
- When ISE NAC is enabled, the RADIUS server overwrite interface is not supported.
- Remote LANs (RLANs) are not supported.
- Audit session ID is not supported across mobility domains if the controller belongs to a different mobility domain.

Configuring ISE NAC Support (GUI)

Procedure

Step 1 Choose **WLANs**.

Step 2 Click the WLAN ID.

The **WLANs > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 From the **NAC State** drop-down list, choose from the following options:

- **None**
- **SNMP NAC**—Uses SNMP NAC for the WLAN.
- **ISE NAC**—Uses ISE NAC for the WLAN.

Note
AAA override is automatically enabled when you use ISE NAC on a WLAN.

Step 5 Save the configuration.

Configuring ISE NAC Support (CLI)

Enter the following command:

config wlan nac radius {**enable** | **disable**} *wlan_id*

Enabling ISE NAC on a WPA/WPA2-PSK WLAN

Information About Enabling ISE NAC on a WPA and WPA2-PSK WLAN

It is possible to enable both ISE NAC and WPA and WPA2-PSK on a WLAN.

This enhancement is introduced in Release 8.3. Prior to Release 8.3, it was not possible to enable both these configurations on the same WLAN.

A use case is Web redirect with PSK on controllers for the purpose of device onboarding. For example, on-board devices using an SSID with a PSK send the MAC address to Cisco ISE using central web authentication (CWA), and determine if it is registered.

Workflow

To support PSK along with ISE NAC, you must enable MAC filtering to facilitate a communication link to the AAA server to get redirect URL and preauthentication ACLs. The WLAN configuration that is supported is WPA and WPA-2 PSK + MAC filtering + ISE NAC.

1. A client joins the WLAN with Layer 2 authentication method, that is, PSK with the credentials created at the time of creating the WLAN.
2. Controller looks up the AAA server to check if MAC filtering is enabled. If yes, the AAA server provides the redirect URL and preauthentication ACLs. The client moves to central web authentication (CWA) state.
3. The client should log on via the redirect URL and authenticate using the available credentials. The CoA is then sent from the AAA server to controller.
4. As part of the CoA, controller triggers DISSOC to the client with the reason as UNSPECIFIED by starting a rejoin timer with 30 seconds.
5. The final authentication is a MAC authentication to which the final authorization results, such as the final VLAN and ACL, are returned.
6. Expecting the client to rejoin performing Layer 2 authentication generating PMK and GTK, thus the wireless encrypted link, the controller sends ACCESS REQ to the AAA server and related ACCESS RESP in which the controller provides the VLAN change or other enforcement attributes in the AAA server. With this attribute enforcement, the client moves to the Run state.

Additional References

- Web Authentication on WLAN Controller—http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc17
- Central Web Authentication on the controller and ISE Configuration Example—http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Enabling ISE NAC on WPA/WPA2-PSK WLAN (GUI)

Procedure

Step 1 Configure controller:

a) Add Cisco ISE as RADIUS server in controller with change of authorization (CoA) in Enabled state.

b) Configure a WLAN with Layer 2 security type set to **WPA+WPA2**, MAC filtering in Enabled state, Authentication Key Management set to **PSK**, and NAC state set to **ISE NAC**:

1. Choose **WLANs** and click the WLAN ID.
2. On the **WLANs > Edit** page, choose **Security** > **Layer 2** tab.
3. Set Layer 2 Security to **WPA+WPA2**.
4. Enable **MAC Filtering**.
5. Under **Authentication Key Management**, enable **PSK** and set the PSK format.
6. In the **Advanced** tab, set the **NAC State** to **ISE NAC**.

c) Create a preauthentication ACL to communicate with only the Cisco ISE server. For instructions on how to create an ACL, see (Link to be provided to the Configuring Access Control Lists chapter).

Note

- In addition to ISE traffic, allow other necessary traffic such as DNS, DHCP to be specified to permit DNS and DHCP traffic on the redirect ACL.
- If the APs are in FlexConnect mode, a preauth ACL is irrelevant. FlexConnect ACLs can be used to allow access for clients that have not been authenticated.

Step 2 Configure Cisco ISE:

a) Ensure that controller is in Cisco ISE.

b) Add an authentication profile.

c) Add an authorization profile.

d) Add postauthentication policies.

e) Add authorization policy.

Note

1. The first instance is when a user associates with the SSID and when the central web authentication profile is returned (unknown MAC address; therefore, you must set the user for redirection).
2. The second instance is when a user authenticated on the web portal, such that it matches the default rule (internal users) in this configuration (it can be configured to meet your requirements). It is important that the authorization part does not match the central web authentication profile again. Otherwise, there will be a redirection loop.

For instructions on Cisco ISE configuration, see http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html#anc6.

Client Exclusion Policies

Client exclusion policies allow wireless networks to block clients from associating based on various types of client misbehavior. You can configure the period of time during which clients are excluded or clients might be excluded indefinitely.

The controller maintains an exclusion list of MAC addresses, which blocks clients from associating with the controller. Clients can be automatically added to the exclusion list due to their misbehavior or can be manually added by MAC address. The automatically added clients can be automatically removed from the exclusion list based upon the WLAN's exclusion list timeout, or can be manually removed.

The criteria by which clients are excluded is configured globally on the controller. On each WLAN, exclusion may be enabled or disabled; if exclusion is enabled, the exclusion list timeout is configurable.

Additional Reference

For information about 802.1X client exclusion, see https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/214466-802-1x-client-exclusion-on-an-aireos-wlc.html.

This section contains the following subsections:

Configuring Client Exclusion Policies (GUI)

Procedure

Step 1 Choose **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** to open the Client Exclusion Policies page.

Step 2 Select any of these check boxes if you want the controller to exclude clients for the condition specified. The default value for each exclusion policy is enabled.

- **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 802.1X Authentication Failures**: Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.

  Note
  In some configurations, 802.1X exclusion may not occur. For more information, see https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/214466-802-1x-client-exclusion-on-an-aireos-wlc.html.

- **Maximum 802.1x-AAA Failure Attempts**: Clients are excluded after a maximum number of 802.1X-AAA failure attempts with the RADIUS server. Valid range of maximum number of 802.1X-AAA failure attempts that you can configure is 1 to 10 with the default value being 3.
- **IP Theft or IP 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.

Step 3 Save your configuration.

Configuring Client Exclusion Policies (CLI)

Procedure

Step 1 Enable or disable the controller to exclude clients on the sixth 802.11 association attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-assoc {**enable** | **disable**}

Step 2 Enable or disable the controller to exclude clients on the sixth 802.11 authentication attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-auth {**enable** | **disable**}

Step 3 Enable or disable the controller to exclude clients on the fourth 802.1X authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion 802.1x-auth {**enable** | **disable**}

Step 4 Configure the controller to exclude clients after a maximum number of 802.1X-AAA failure attempts with the RADIUS server by entering this command:

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts *num-of-attempts*

Valid range for the maximum number of 802.1X-AAA failure attempts with the RADIUS is 1 to 10 with the default value being 3.

Step 5 Enable or disable the controller to exclude clients if the IP address is already assigned to another device by entering this command:

config wps client-exclusion ip-theft {**enable** | **disable**}

Step 6 Enable or disable the controller to exclude clients on the fourth web authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion web-auth {**enable** | **disable**}

Step 7 Enable or disable the controller to exclude clients for all of the above reasons by entering this command:

config wps client-exclusion all {**enable** | **disable**}

Step 8 Use the following command to add or delete client exclusion entries.

config exclusionlist {**add** *mac-addr description* | **delete** *mac-addr* | **description** *mac-addr description*}

- **add**: Creates a local exclusion-list entry.
- **delete**: Deletes a local exclusion-list entry.
- **description**: Sets the description for an exclusion-list entry.

Step 9 Save your changes by entering this command:

save config

Step 10 See a list of clients that have been dynamically excluded, by entering this command:

show exclusionlist

Information similar to the following appears:

```
Dynamically Disabled Clients
----------------------------
  MAC Address      Exclusion Reason     Time Remaining (in secs)
  -----------      ----------------     ------------------------

00:40:96:b4:82:55    802.1X Failure            51
```

Step 11 See a list of FlexConnect clients that have been excluded in an AP locally by entering this command:

show flexconnect client exclusion-list

Information similar to the following appears:

```
cisco-ap#show flexconnect client exclusion-list
Client Exclusion List:
     Excluded Mac life    Type
8E:BB:02:65:55:AA    0  static
A0:B4:35:B1:AG:55    0  static
E8:02:FH:C4:6A:11   35 dynamic
```

Step 12 See the client exclusion policy configuration settings by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
 Auto-Immune.............................. Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
  Maximum 802.1x-AAA failure attempts............ 3

Signature Policy
  Signature Processing....................... Enabled
```

Configuring Client Exclusion Policies for a WLAN (GUI)

The 802.1X client exclusion feature prevents clients from sending authentication attempts for a period of time after excessive 802.1X authentication failures. You can configure client exclusion policies applicable to all clients by navigating to **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** . This section provides instructions on how to configure client exclusion on a per-WLAN basis.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN.

Step 3 On the **WLANs > Edit (Advanced)** page, click the **Advanced** tab.

Step 4 Locate the **Client Exclusion** label, check the check box adjacent to it to enable client exclusion policies, and enter the timeout value, in seconds. The timeout value represents the time period for which the excluded clients are prevented from sending 802.1X authentication attempts.

Step 5 Save the configuration.

Configuring Client Exclusion Policies for a WLAN (CLI)

The 802.1X client exclusion feature prevents clients from sending authentication attempts for a period of time after excessive 802.1X authentication failures. You can configure client exclusion policies applicable to all clients by entering the **config wps client-exclusion 802.1x-auth** {**enable** | **disable**} command. This section provides instructions on how to configure client exclusion policies on a per-WLAN basis.

Procedure

Step 1 Configure client exclusion policies for a WLAN by entering this command:

config wlan exclusionlist *wlan-id* {**enable** | **disable**}

Step 2 Configure the client exclusion list timeout period by entering this command:

config wlan exclusionlist *wlan-id timeout-in-seconds*

The timeout value represents the time period for which the excluded clients are prevented from sending 802.1X authentication attempts.

Step 3 Save the configuration by entering this command:

save config

Wi-Fi Direct Client Policy

Some clients support Wi-Fi Direct, which enables direct peer-to-peer connections; for example, from a PC to a printer. Wi-Fi Direct allows such a peer-to-peer connection simultaneously with an AP association.

Wi-Fi Direct Client Policy enables the network administrator to block associations from clients that have Wi-Fi Direct enabled.

This section contains the following subsections:

Restrictions for the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.
- Cisco APs in FlexConnect mode (even in central authentication and central switching) is not supported.
- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.

Configuring the Wi-Fi Direct Client Policy (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID of the WLAN for which you want to configure the Wi-Fi Direct Client Policy. The **WLANs > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 From the **Wi-Fi Direct Clients Policy** drop-down list, choose one of the following options:

- **Disabled**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
- **Allow**—Allows Wi-Fi Direct clients to associate with the WLAN
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN
- **Xconnect-Not-Allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection

Step 5 Save the configuration.

Configuring the Wi-Fi Direct Client Policy (CLI)

Procedure

Step 1 Configure the Wi-Fi Direct Client Policy on WLANs by entering this command:

config wlan wifidirect {**allow** | **disable** | **not-allow**} *wlan-id*

The syntax of the command is as follows:

- **allow**—Allows Wi-Fi Direct clients to associate with the WLAN
- **disable**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
- **not-allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN
- **xconnect-not-allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection
- *wlan-id*—WLAN identifier

Step 2 Save your configuration by entering this command:

save config

Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI)

Procedure

- Monitor and troubleshoot the Wi-Fi Direct Client Policy by entering theses commands:
  - **show wlan wifidirect** *wlan-id*—Displays status of the Wi-Fi Direct Client Policy on the WLAN.
  - **show client wifiDirect-stats**—Displays the total number of clients associated and the number of clients rejected if the Wi-Fi Direct Client Policy is enabled.

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the controller, dropped by the controller, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.



Note Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP.Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs. P2P blocking is supported for both locally switched and centrally switched WLANs.

Restrictions on Peer-to-Peer Blocking

- The Cisco controllers and APs supporting the IPSK-tag based P2P blocking feature are:
  - Cisco controllers—3504, 5520, 8540 Series controllers
  - Cisco APs—Cisco Wave 2 and 802.11ax APs.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, solution peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Cisco controller with central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as peer-to-peer drop and client packets are dropped.
- Cisco controller with central switching clients supports peer-to-peer blocking for clients associated with different APs. However, with FlexConnect local switching, only clients connected to the same AP are blocked. FlexConnect ACLs can be used as a workaround for this limitation.
- For Flex+ local switching feature to function, ensure that the APs are not a part of the default flex-group.
- P2P forward-upstream action is not supported for anchored clients.

Configuring Peer-to-Peer Blocking (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 Choose one of the following options from the P2P Blocking drop-down list:

- **Disabled**—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.

  Note
  Traffic is never bridged across VLANs in the controller.

- **Drop**—Causes the controller to discard the packets.
- **Forward-UpStream**—Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.

  Note
  To enable peer-to-peer blocking on a WLAN configured for FlexConnect local switching, select **Drop** from the P2P Blocking drop-down list and select the **FlexConnect Local Switching** check box.

- **Allow-Private-Group**—Applicable to PSK clients only. The traffic forwarding decision is taken based on the associated IPSK tags for the source and destination client devices.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Peer-to-Peer Blocking (CLI)

Procedure

Step 1 Configure a WLAN for peer-to-peer blocking by entering this command:

config wlan peer-blocking {**disable** | **drop** | **forward-upstream** | **allow-private-group**} *wlan_id*

Note
Allow-private-group is applicable to PSK clients only.

Step 2 Save your changes by entering this command:

save config

Step 3 See the status of peer-to-peer blocking for a WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.............................. 1
Profile Name................................. test
Network Name (SSID).......................... test
Status....................................... Enabled
...
...
...
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy................................. All
Local EAP Authentication..................... Disabled
```

Step 4 See the ipsk-tag associated with the client by entering this command:

show client summary ipsk-tag

Peer-to-Peer Blocking Using IPSK Tags

P2P blocking is not applied as traffic does not get bridged across VLANs. IPSK-based peer-blocking is an exception, where the inter-VLAN client traffic is forwarded to upstream switch if the IPSK-tag matches and dropped otherwise.

The enhancement is supported on IPv4 and IPv6 protocols on central switching and Flex + local switching with the **Allow Private Group** enabled on the controller.

Table 2: IPSK Tag Traffic Flow

WLAN P2P configuration	IPSK Source device tag	IPSK Destination device tag	Traffic bridging decision	Result
Drop	Any	Any	Block	With this configuration, all the p2p traffic gets dropped.
Disable	Any	Any	Allow	With this configuration, all the p2p traffic gets bridged.
Up Stream	Any	Any	Forward up	With this configuration, all the p2p traffic gets forwarded to the next hop switch.

WLAN P2P configuration	IPSK Source device tag	IPSK Destination device tag	Traffic bridging decision	Result
Allow Private Group	T1	T2	Block	With this configuration, the p2p traffic with different tag values T1 and T2 gets dropped even if the clients are in different VLANs.
Allow Private Group	T	T	Allow	With this configuration, the p2p traffic with the same tag value T gets bridged. If the clients are in different vlans, the traffic gets forwarded to the upstream switch.

Local Policies

Controller can do profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the clients. You can configure the device-based policies and enforce per-user or per-device policy on the network. The controller also displays statistics that are based on per-user or per-device end points and policies that are applicable per device. The maximum number of policies that you can configure is 64.



Note The policy enforcement behavior in the Cisco AireOS Wireless Controller differs from that in the Cisco Embedded Wireless Controller.

The policies are defined based on the following attributes:

- User group or user role
- Device type such as Windows clients, smartphones, tablets, and so on
- Service Set Identifier (SSID)
- Location, based on the access point group that the end point is connected to
- Time of the day
- Extensible Authentication Protocol (EAP) type, to check what EAP method that the client is getting connected to

When these policy attributes match, you can define the following actions:

- Virtual local area network (VLAN)

- Access control list (ACL)
- Quality of Service (QoS) level
- Session timeout value
- Sleeping client timeout value
- Select either AVC profile or role, or both based on local policy attributes defined in the AAA server.

  The following are the different ways by which local policies are applied based on a combination of AVC profile and role defined in the AAA server:

  - Both AVC profile and role are derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile is prioritized and is applied.
    - If AAA override is disabled, then role matching is applied.
  - Only role is derived from the AAA server and role matching takes place, the following options are available:
    - If profile is defined in the policy, then role policy is applied.
    - If profile is not defined in the policy, then AVC profile defined in WLAN is applied.
  - Only AVC profile is derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile received from the AAA server is applied.
    - If AAA override is disabled, then AVC profile defined on the WLAN is applied.

This section contains the following subsections:

Guidelines and Restrictions for Local Policy Classification

- If you enable AAA override and there are AAA attributes other than the role type from the AAA server, the configured policy action is not applied. The AAA override attributes have higher precedence.
- On a WLAN, when local profiling is enabled, RADIUS profiling is not allowed.
- Client profiling uses existing profiles on the controller.
- You cannot create custom profiles.
- Wired clients behind the workgroup bridge (WGB) are not profiled and the policy action is not taken.
- Only the first policy rule which matches with the policy profile is given precedence. Each policy profile has an associated policy rule, which is used to match the policies.
- You can configure up to 64 policies, out of which you can configure up to 16 policies per WLAN.
- Policy action is taken after Layer 2 authentication is complete, or after Layer 3 authentication is complete, or when the device sends HTTP traffic and gets the device profiled. Therefore, profiling and policy actions occur more than once per client.
- Only VLAN, ACL, Session Timeout, and QoS are supported as policy action attributes.

- If you want a local policy session timeout to be applied and overridden for a WLAN, you must enable the session timeout at the WLAN with a value greater than 0.
- Profiling is performed only on IPv4 clients.
- For all the controllers in a mobility group, it is mandatory that the local policy configurations have the same match criteria attributes and action attributes. Otherwise, the local policy configuration becomes invalid when roaming occurs across the controllers.
- When local policy is configured for device type policy match and configured on a WLAN with guest anchor enabled, the AVC profile name from local policy is not applied at anchor.
- Local policies are enforced after profiling using OUI irrespective of DHCP or HTTP profiling. For more information, see CSCvp70783.

Table 3: Differences Between Cisco Identity Services Engine (ISE) and Controller Profiling Support

ISE	Controller
Supports profiling using RADIUS probes, DHCP probes, HTTP, and other protocols used to identify the client type.	Supports MAC OUI, DHCP, and HTTP-based profiling.
Supports multiple different attributes for the policy action and has an interface to pick and select each of the attributes.	Supports VLAN, ACL, Session Timeout, and QoS as policy action attributes.
Supports customization of profiling rules with user-defined attributes.	Supports only default profiling rules.

Local Policy—Best Practices

Create and apply effective local policies for the clients on a WLAN, and the some of the recommended practices are listed below.

- We recommend you to have multiple policies on priority orders for different selection criteria on WLAN. The recommended priority order is:

  1. P1 policy with device type
  2. P2 policy with eap-type
  3. P3 policy with active hours

  For example a WLAN can have device-type policy as priority one, eap-type policy as priority 2 and so on and active hour policy should be the least priority always. If you want different policies matching with client better to create different WLAN as its always on priority base, the higher priority configured on WLAN will match and get applied to the client.

- We do not recommend having multiple policies of the same type on a single WLAN, nor recommend multiple active hour policies on a single WLAN. You should configure different WLANs with different active hour range to allow the client to join
- For the active hour policy, you should configure only the allowed range in the active hour because, other than active hours, the device does not allow the client to join. So, there is no need for a deny policy with active hours.

- We do not recommend having multiple active hour configurations on the same day

Use Case: Configure client behavior where the clients are allowed to join between 00:00-07:00 and 20:00-23:59 time on all days of the week and blocked during 07:01-19:59 time on all days.

Solution: You need to configure two WLANs:

- WLAN_1, with the policy as All days active hours 00:00-07:00 and allow IPv4 address
- WLAN_2 with the policy as All days active hours 20:00-23:59 and allow IPv4 address

Result: The clients can join WLAN_1 between 00:00 and 07:00. The clients can join WLAN_2 between 20:00 and 23:59. Other than these two-time slots, the client cannot join either WLAN_1 or WLAN_2.

Configuring Local Policies (GUI)

Procedure

Step 1 Choose **Security** > **Local Policies**.

Step 2 Click **New** to create a new policy.

Step 3 Enter the policy name and click **Apply**.

Step 4 On the **Policy List** page, click the policy name to be configured.

Step 5 On the **Policy > Edit** page, follow these steps:

a) In the **Match Criteria** area, enter a value for **Match Role String**. This is the user type or user group of the user, for example, student, teacher, and so on.

b) From the **Match EAP Type** drop-down list, choose the EAP authentication method used by the client.

c) From the **Device Type** drop-down list, choose the device type.

d) Click **Add** to add the device type to the policy device list.

The device type you choose is listed in the **Device List**.

e) In the **Action** area, specify the policies that are to be enforced. From the **IPv4 ACL** drop-down list, choose an IPv4 ACL for the policy.

f) Enter the **VLAN ID** that should be associated with the policy.

g) From the **QoS Policy** drop-down list, choose a QoS policy to be applied.

h) Enter a value for **Session Timeout**. This is the maximum amount of time, in seconds, after which a client is forced to reauthenticate.

i) Enter a value for **Sleeping Client Timeout**, which is the timeout for sleeping clients.

Sleeping clients are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page.

This sleeping client timeout configuration overrides the WLAN-specific sleeping client timeout configuration.

j) From the **AVC Profile** drop-down list, choose an AVC profile to be applied based on the role defined in AAA.

k) In the **Active Hours** area, from the **Day** drop-down list, choose the days on which the policy has to be active.
l) Enter the **Start Time** and **End Time** of the policy.
m) Click **Add**.

The day and start time and end time that you specify is listed.

n) Click **Apply**.

What to do next

Apply a local policy that you have created to a WLAN by following these steps:

1. Choose **WLANs**.
2. Click the corresponding WLAN ID.

   The **WLANs > Edit** page is displayed.
3. Click the **Policy-Mapping** tab.
4. Enter the **Priority Index** for a policy.
5. From the **Local Policy** drop-down list, choose the policy that has to be applied for the WLAN.
6. Click **Add**.

   The priority index and the policy that you choose is listed. You can apply up to 16 policies for a WLAN.

Configuring Local Policies (CLI)

Procedure

- Create or delete a local policy by entering this command:

  config policy *policy-name* {**create** | **delete**}

- Configure a match type to a policy by entering these commands:
  - **config policy** *policy-name* **match device-type** {**add** | **delete**} *device-type*
  - **config policy** *policy-name* **match eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**}
  - **config policy** *policy-name* **match role** {*role-name* | *none*}
- Configure an action that has to be enforced as part of a policy by entering these commands:
  - ACL action to a policy—**config policy** *policy-name* **action acl** {**enable** | **disable**} *acl-name*
  - QoS average data rate—**config policy** *policy-name* **action average-data-rate** {**enable** | **disable**} *rate*
  - QoS average real-time data rate—**config policy** *policy-name* **action average-realtime-rate** {**enable** | **disable**} *rate*
  - QoS burst data rate—**config policy** *policy-name* **action burst-data-rate** {**enable** | **disable**} *rate*
  - QoS burst real-time data rate—**config policy** *policy-name* **action burst-realtime-rate** {**enable** | **disable**} *rate*
  - QoS action—**config policy** *policy-name* **action qos** {**enable** | **disable**} {**bronze** | **gold** | **platinum** | **silver**}

- Session timeout action—**config policy** *policy-name* **action session-timeout** {**enable** | **disable**} *timeout-in-seconds*
- Sleeping client timeout action—**config policy** *policy-name* **action sleeping-client-timeout** {**enable** | **disable**} *timeout-in-hours*
- Enable AVC profile—**config policy** *policy-name* **action avc-profile-name enable** *avc-profile-name*
- Disable AVC profile—**config policy** *policy-name* **action avc-profile-name disable**
- VLAN action—**config policy** *policy-name* **action vlan** {**enable** | **disable**} *vlan-id*



Note Ensure that you configure the Average Data Rate before you configure the Burst Data Rate.

- Configure the active time for a policy by entering this command:

  config policy *policy-name* **active** {**add** | **delete**} **hours start-time end-time days** {*mon* | *tue* | *wed* | *thu* | *fri* | *sat* | *sun* | *daily* | *weekdays*}

- Apply a local policy to a WLAN by entering this command:

  config wlan policy {**add** | **delete**} *priority-index policy-name wlan-id*

- Enable or disable client profiling in local mode for a WLAN, based on HTTP, DHCP, or both by entering this command:

  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- Apply a local policy to an AP group of a WLAN by entering this command:

  config wlan apgroup policy {**add** | **delete**} *priority-index policy-name ap-group-name wlan-id*

- View information about a policy by entering this command:

  show policy {**summary** | *policy-name*} **statistics**

- View local device classification profile summary by entering this command:

  show profiling policy summary

- View all the clients with a type of device by entering this command:

  show client wlan *wlan-id* **device-type** *device-type*

- View a client profiling status that includes profiling done by the RADIUS server and the controller by entering this command:

  show wlan *wlan-id*

- View the policy details for AP groups by entering this command:

  show wlan apgroups

- Configure the task of debugging of policies by entering this command:

  debug policy {**error** | **event**} {**enable** | **disable**}

Updating Organizationally Unique Identifier List

Updating Organizationally Unique Identifier List (GUI)

Procedure

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **OUI Update**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.

The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the controller by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Organizationally Unique Identifier List (CLI)

Procedure

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Specify the server type by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:

transfer download datatype oui-update

Step 4 Begin the download of the file by entering this command:

transfer download start

Note
Follow the on-screen instructions to complete the download process.

Step 5 Reboot the controller by entering this command:

reset system

Step 6 See the updated OUI list by entering this command:

show profiling oui-string summary

Note

HA support for OUI update: HA link must be up while downloading the OUI file to the Active controller, so that the OUI update gets applied to the Standby controller as well.

Updating Device Profile List

Updating Device Profile List (GUI)

Procedure

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **Device Profile**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.

The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the controller by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Device Profile List (CLI)

Procedure

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Specify the server type by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:

transfer download datatype device-profile

Step 4 Specify the file name by entering this command:

transfer download filename *device_profile-xml-file*

Step 5 Begin the download of the file by entering this command:

transfer download start

Note
Follow the on-screen instructions to complete the download process.

Step 6 Reboot the controller by entering this command:

reset system

Step 7 See the updated OUI list by entering this command:

show profiling policy summary

Wired Guest Access

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract.

You can create a basic peer to peer WLAN ACL and apply it to the wired guest WLAN. This will not block peer to peer traffic and the guest users can still communicate with each other.

This section contains the following subsections:

Prerequisites for Configuring Wired Guest Access

To configure wired guest access on a wireless network, you must perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

Restrictions for Configuring Wired Guest Access

- Wired guest access interfaces must be tagged.
- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.
- The controller does not use the callStationIDType parameter configured for the Radius server while authenticating wired clients, instead the controller uses the system MAC address configured for the callStationIDType parameter.

Configuring Wired Guest Access (GUI)

Procedure

Step 1 To create a dynamic interface for wired guest user access, choose **Controller** > **Interfaces**. The Interfaces page appears.

Step 2 Click **New** to open the **Interfaces > New** page.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Click **Apply** to commit your changes.

Step 5 In the **Port Number** text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

Step 6 Select the **Guest LAN** check box.

Step 7 Click **Apply** to commit your changes.

Step 8 To create a wired LAN for guest user access, choose **WLANs**.

Step 9 On the WLANs page, choose **Create New** from the drop-down list and click **Go**. The **WLANs** > **New page** appears.

Step 10 From the Type drop-down list, choose **Guest LAN**.

Step 11 In the **Profile Name** text box, enter a name that identifies the guest LAN. Do not use any spaces.

Step 12 From the WLAN ID drop-down list, choose the ID number for this guest LAN.

Note
You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).

Step 13 Click **Apply** to commit your changes.

Step 14 Select the **Enabled** check box for the Status parameter.

Step 15 Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing *Step 16* and *Step 17*.

Step 16 From the Ingress Interface drop-down list, choose the VLAN that you created in *Step 3*. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 17 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18 If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security** > **Layer 3**. The **WLANs > Edit (Security > Layer 3)** page appears.

Step 19 From the Layer 3 Security drop-down list, choose one of the following:

- **None**—Layer 3 security is disabled.
- **Web Authentication**—Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
- **Web Passthrough**—Allows users to access the network without entering a username and password.

  Note
  There should not be a Layer 3 gateway on the guest wired VLAN, as this would bypass the web authentication done through the controller.

Step 20 If you choose the Web Passthrough option, an **Email Input** check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21 To override the global authentication configuration set on the Web Login page, select the **Override Global Config** check box.

Step 22 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wired guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note
  These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 23 If you chose External as the web authentication type in *Step 22*, choose **Security > AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note
You can configure the Authentication and LDAP Server using both IPv4 and IPv6 addresses.

Note
The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 24 To establish the priority in which the servers are contacted to perform web authentication as follows:

Note
The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click **Up** and **Down** until the desired server type is at the top of the box.

c. Click the < arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 25 Click **Apply**.

Step 26 Click **Save Configuration**.

Step 27 Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Procedure

Step 1 Create a dynamic interface (VLAN) for wired guest user access by entering this command:

config interface create *interface_name vlan_id*

Step 2 If link aggregation trunk is not configured, enter this command to map a physical port to the interface:

config interface port *interface_name primary_port* {*secondary_port*}

Step 3 Enable or disable the guest LAN VLAN by entering this command:

config interface guest-lan *interface_name* {**enable | disable}**

This VLAN is later associated with the ingress interface created in *Step 5*.

Step 4 Create a wired LAN for wired client traffic and associate it to an interface by entering this command:

config guest-lan create *guest_lan_id interface_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).

Note
To delete a wired guest LAN, enter the **config guest-lan delete** *guest_lan_id command.*

Step 5 Configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch by entering this command:

config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 Configure an egress interface to transmit wired guest traffic out of the controller by entering this command:

config guest-lan interface *guest_lan_id interface_name*

Note

If the wired guest traffic is terminating on another controller, repeat *Step 4* and *Step 6* for the terminating (anchor) controller and *Step 1* through *Step 5* for the originating (foreign) controller. Additionally, configure the **config mobility group anchor add** {**guest-lan** *guest_lan_id* | **wlan** *wlan_id} IP_address* command for both controllers.

Step 7 Configure the security policy for the wired guest LAN by entering this command:

config guest-lan security {**web-auth enable guest_lan_id** | **web-passthrough enable** *guest_lan_id*}

Note
Web authentication is the default setting.

Step 8 Enable or disable a wired guest LAN by entering this command:

config guest-lan {enable | disable} *guest_lan_id*

Step 9 If you want wired guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the guest LAN for which it should display:

- **config guest-lan custom-web login-page** *page_name guest_lan_id—Defines a web login page.*
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id—Defines a web login failure* page.

  Note
  To use the controller's default login failure page, enter the **config guest-lan custom-web loginfailure-page none** *guest_lan_id* command.

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*—Defines a web logout page.

  Note
  To use the controller's default logout page, enter the **config guest-lan custom-web logout-page none** *guest_lan_id* command.

Step 10 If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Step 11 If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note
All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 Define the web login page for wired guest users by entering this command:

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web pages (login, login failure, or logout) that were configured in *Step 9*.
- **external** redirects users to the URL that was configured in *Step 10*.

Step 13 Use a guest-LAN specific custom web configuration rather than a global custom web configuration by entering this command:

config guest-lan custom-web global disable *guest_lan_id*

Note
If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

Step 14 Save your changes by entering this command:

save config

Note
Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

Step 15 Display the customized web authentication settings for a specific guest LAN by entering this command:

show custom-web {all | guest-lan guest_lan_id}

Note
If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Step 16 Display a summary of the local interfaces by entering this command:

show interface summary

Note
The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

Display detailed interface information by entering this command:

show interface detailed *interface_name*

Step 17 Display the configuration of a specific wired guest LAN by entering this command:

show guest-lan *guest_lan_id*

Note
Enter the **show guest-lan summary** command to see all wired guest LANs configured on the controller.

Step 18 Display the active wired guest LAN clients by entering this command:

show client summary guest-lan

Step 19 Display detailed information for a specific client by entering this command:

show client detail *client_mac*