



# CHAPTER 12

## Configuring Hybrid REAP

---

This chapter describes hybrid REAP and explains how to configure this feature on controllers and access points. It contains these sections:

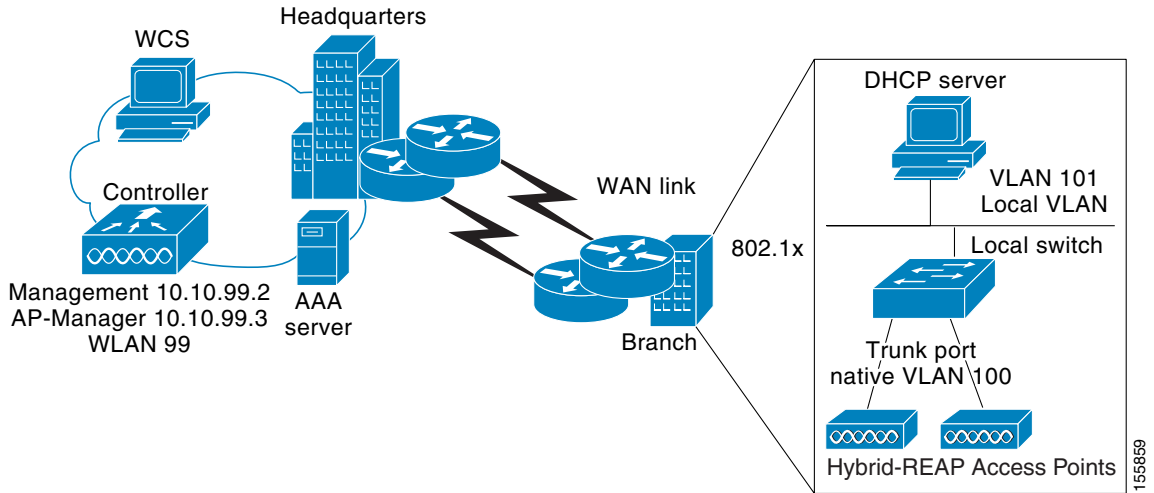
- [Overview of Hybrid REAP, page 12-2](#)
- [Configuring Hybrid REAP, page 12-4](#)

# Overview of Hybrid REAP

Hybrid REAP is a solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of hybrid-REAP access points per location. The hybrid-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

Hybrid REAP is supported only on the 1130AG and 1240AG access points and on the 2000 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Controller Network Module for Integrated Services Routers, and the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch. Figure 12-1 illustrates a typical hybrid-REAP deployment.

Figure 12-1 Hybrid REAP Deployment



## Hybrid-REAP Authentication Process

When a hybrid-REAP access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A hybrid-REAP access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular LWAPP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43.]



Note

OTAP does not work on the first boot out of the box.

- If the access point has been assigned a static IP address, it can discover a controller through any of the LWAPP discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast or OTAP, Cisco recommends DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

When a hybrid-REAP access point can reach the controller (referred to as *connected mode*), the controller assists in client authentication. When a hybrid-REAP access point cannot access the controller, the access point enters standalone mode and authenticates clients by itself.


**Note**

The LEDs on the access point change as the device enters different hybrid-REAP modes. Refer to the Hardware Installation Guide for your access point for information on LED patterns.

When a client associates to a hybrid-REAP access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **central authentication, central switching**—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.
- **central authentication, local switching**—In this state, the controller handles client authentication, and the hybrid-REAP access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the hybrid-REAP access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- **local authentication, local switching**—In this state, the hybrid-REAP access point handles client authentication and switches client data packets locally. This state is valid only in standalone mode.
- **authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.
- **authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a hybrid-REAP access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured to central switching) or the “authentication down, local switching” state (if the WLAN was configured to local-switch).

When a hybrid-REAP access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For 802.1x or web-authentication WLANs, existing clients are not disassociated, but the hybrid-REAP access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to 802.1x or web-authentication WLANs. Controller-dependent activities such as 802.1x authentication, NAC, and web authentication (guest access) are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller. Furthermore, most radio resource management (RRM) features

(such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a hybrid-REAP access point supports dynamic frequency selection in standalone modes.

**Note**

If your controller is configured for network access control (NAC), clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. Once a client is assigned to a quarantined VLAN, all of its data packets are centrally switched.

The hybrid-REAP access point maintains client connectivity even after entering standalone mode. However, once the access point re-establishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

## Hybrid REAP Guidelines

Keep these guidelines in mind when using hybrid REAP:

- A hybrid-REAP access point can be deployed with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- Hybrid REAP supports a 500-byte maximum transmission unit (MTU) WAN link at minimum.
- Roundtrip latency must not exceed 100 milliseconds (ms) between the access point and the controller, and LWAPP control packets must be prioritized over all other traffic.
- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In hybrid-REAP mode, the access point can receive multicast packets only in unicast form.
- Hybrid REAP supports CCKM full authentication but not CCKM fast roaming.
- Hybrid REAP supports a 1-1 network address translation (NAT) configuration. It also supports port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPSec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic, provided that these security types are accessible locally at the access point.

## Configuring Hybrid REAP

To configure hybrid REAP, you must follow the instructions in these sections in the order provided:

- [Configuring the Switch at the Remote Site, page 12-4](#)
- [Configuring the Controller for Hybrid REAP, page 12-6](#)
- [Configuring an Access Point for Hybrid REAP, page 12-9](#)
- [Connecting Client Devices to the WLANs, page 12-12](#)

## Configuring the Switch at the Remote Site

Follow these steps to prepare the switch at the remote site.

**Step 1** Attach the access point that will be enabled for hybrid REAP to a trunk or access port on the switch.



**Note** The sample configuration below shows the hybrid-REAP access point connected to a trunk port on the switch.

**Step 2** Refer to the sample configuration below to configure the switch to support the hybrid-REAP access point.

In this sample configuration, the hybrid-REAP access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) will be used by the hybrid-REAP access point, and the second DHCP pool (LOCAL-SWITCH) will be used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration illustrates these settings.



**Note** The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

#### Sample local switch configuration:

```
ip dhcp pool NATIVE
  network 10.10.100.0 255.255.255.0
  default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
  network 10.10.101.0 255.255.255.0
  default-router 10.10.101.1
!
interface FastEthernet1/0/1
  description Uplink port
  no switchport
  ip address 10.10.98.2 255.255.255.0
  spanning-tree portfast
!
interface FastEthernet1/0/2
description the Access Point port
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
spanning-tree portfast
!
interface Vlan100
  ip address 10.10.100.1 255.255.255.0
  ip helper-address 10.10.100.1
!
interface Vlan101
  ip address 10.10.101.1 255.255.255.0
  ip helper-address 10.10.101.1
end
```

## Configuring the Controller for Hybrid REAP

This section provides instructions for configuring the controller for hybrid REAP. The controller configuration for hybrid REAP consists of creating centrally switched and locally switched WLANs. This procedure uses these three WLANs as examples:

WLAN	Security	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	101 (local switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)

- Step 1** Follow these steps to create a centrally switched WLAN. In our example, this is the first WLAN (employee).
- Choose **Configure > Controllers**.
  - Click in the IP Address column for a particular controller.
  - Click **WLANs > WLANs** to access the WLANs page.
  - Choose **Add WLAN** from the Select a command drop-down menu and click **GO** (see [Figure 12-2](#)).



**Note** Cisco access points can support up to 16 WLANs per controller. However, some Cisco access points do not support WLANs that have a WLAN ID greater than 8. In such cases, when you attempt to create a WLAN, you get a message that says “Not all types of AP support WLAN ID greater than 8, do you wish to continue?”. Clicking OK creates a WLAN with the next available WLAN ID. However, if you delete a WLAN that has a WLAN ID less than 8, then the WLAN ID of the deleted WLAN is applied to the next created WLAN.

Figure 12-2 WLANs &gt; New Page

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area is titled "172.19.7.85 > WLAN > Add From Template". It features a navigation menu on the left with categories like "Controllers", "Properties", "System", "WLANs", and "Security". The "WLANs" section is expanded, showing "WLANs" and "AP Groups: VLANs". The "Alarm Summary" table is visible, showing various metrics like Rogue AP, Coverage Hole, Security, etc.

Category	Count	Percentage
Rogue AP	0	138
Coverage Hole	0	137
Security	9	2
Controllers	1	0
Access Points	768	42
Mesh Links	0	0
Location	1	14

The configuration form for the "Amber" template includes the following fields:

- Profile Name: Amber
- SSID: Amber
- WLAN Status:  Enabled
- Security Policies: **None** (Modifications done under security tab will appear after save operation.)
- Radio Policy: All
- Interface: management
- BroadCast SSID:  Enabled

Foot Notes:

- 1 When enabled, a excluded timeout value of zero means infinity (will require administrative override to reset excluded clients.)
- 2 Layer 3 security must be set to 'none' for IPv6 to be enabled.
- 3 Web Authentication cannot be used in combination with IPsec and L2TP.
- 4 CKIP is not supported on 10xx APs.
- 5 H-REAP Local Switching is not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications. It is not applicable to WLAN IDs 9-16.
- 6 Client MFP is not active unless WPA2 is configured.

- e. If you want to apply a template to this controller, choose a template name from the drop-down menu. The parameters will populate according to how the template is set. If you want to create a new WLAN template, use the *click here* link to be redirected to the template creation page (see the “Configuring WLAN Templates” section on page 10-9).
- f. Modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box.
- g. Be sure to enable this WLAN by checking the **Admin Status** check box under General Policies.



**Note** If NAC is enabled and you created a quarantined VLAN and want to use it for this WLAN, make sure to select it from the Interface drop-down box under General Policies. Also, check the **Allow AAA Override** check box to ensure that the controller checks for a quarantine VLAN assignment.

- h. Click **Apply** to commit your changes.

**Step 2** Follow these steps to create a locally switched WLAN. In our example, this is the second WLAN (employee-local).

- a. Follow the substeps in **Step 1** to create a new WLAN. In our example, this WLAN is named “employee-local.”
- b. Click a WLAN ID from the original WLAN window to move to a WLANs edit page. Modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box. Make sure to choose PSK authentication key management and enter a pre-shared key.




---

**Note** Make sure to enable this WLAN by checking the **Admin Status** check box under General Policies. Also, make sure to enable local switching by checking the **H-REAP Local Switching** check box. When you enable local switching, any hybrid-REAP access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

---




---

**Note** For hybrid-REAP access points, the interface mapping at the controller for WLANs configured for H-REAP Local Switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID, per hybrid-REAP access point. Non-hybrid-REAP access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each WLAN's interface mapping.

---

- c. Click **Apply** to commit your changes.

**Step 3** Follow these steps if you also want to create a centrally switched WLAN that is used for guest access. In our example, this is the third WLAN (guest-central). You might want to tunnel guest traffic to the controller so you can exercise your corporate data policies for unprotected guest traffic from a central site.

- a. Follow the substeps in [Step 1](#) to create a new WLAN. In our example, this WLAN is named “guest-central.”
- b. In the WLANs Edit page, modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **None** from both the Layer 2 Security and Layer 3 Security drop-down boxes, check the **Web Policy** check box, and make sure **Authentication** is selected.




---

**Note** If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL.

---

- c. Make sure to enable this WLAN by checking the **Admin Status** check box under General Policies.
- d. Click **Apply** to commit your changes.
- e. If you want to customize the content and appearance of the login page that guest users will see the first time they access this WLAN, follow the instructions in the [“Configuring a Web Authentication Template”](#) section on page 10-42.
- f. To add a local user to this WLAN, click **Security** and then click **Local Net Users**.
- g. When the Local Net Users page appears, choose **Add Local Net User** from the Select a command drop-down menu.
- h. In the User Name and Password fields, enter a username and password for the local user. Click the **Generate Password** check box if you want a password automatically generated. The Password and Confirm Password parameters will be automatically populated. If automatic generation is not enabled, you must supply a password twice.
- i. From the SSID drop-down list, choose which SSID this guest user applies to. Only those WLANs for which web security is enabled are listed. The SSID must be a WLAN that has Layer 3 web authentication policy configured.
- j. Enter a description of the guest user account.

- k. From the Lifetime drop-down list, choose the number of days, hours, or minutes for this user account to remain active.
  - l. Click **Save**.
- Step 4** Go to the [“Configuring an Access Point for Hybrid REAP”](#) section on page 12-9 to configure two or three access points for hybrid REAP.
- 

## Configuring an Access Point for Hybrid REAP

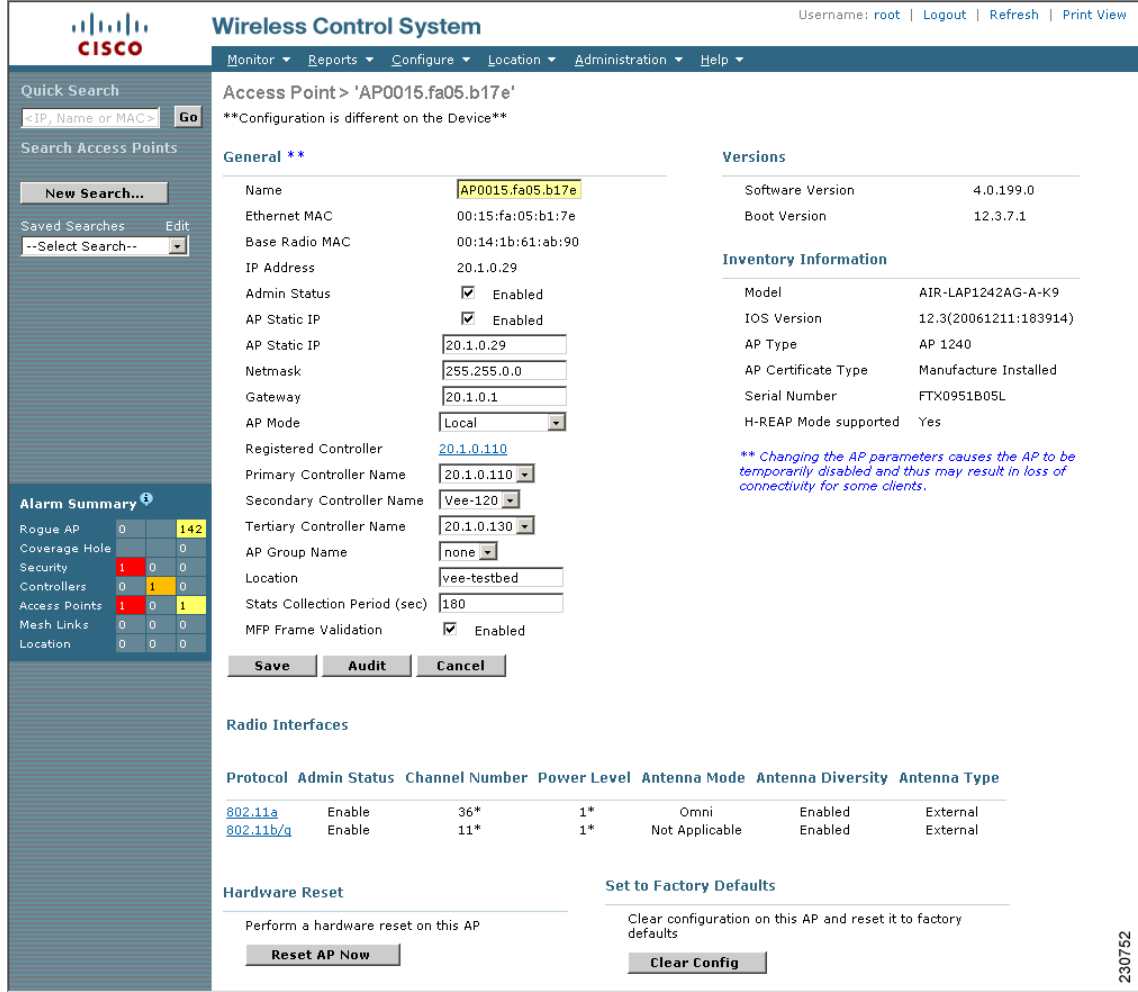
This section provides instructions for configuring an access point for hybrid REAP.

Follow these steps to configure an access point for hybrid REAP.

---

- Step 1** Make sure that the access point has been physically added to your network.
- Step 2** Choose **Configure > Access Points**.
- Step 3** Choose which access point you want to configure for hybrid REAP by clicking one from the AP Name list. The detailed access point window appears (see [Figure 12-3](#)).

Figure 12-3 Detailed Access Point Window



The last parameter under Inventory Information indicates whether this access point can be configured for hybrid REAP. Only the 1130AG and 1240AG access points support hybrid REAP.

- Step 4** Verify that the H-REAP Mode Supported parameter displays Yes. If it does not, continue to Step 5. If H-REAP is showing as supported, skip to Step 7.
- Step 5** Choose **Configure > Access Point Templates**.
- Step 6** Choose which access point you want to configure for hybrid REAP by clicking one from the AP Name list. The AP/Radio Templates window appears (see Figure 12-4).

230752

Figure 12-4 AP/Radio Template Window

The screenshot shows the 'AP/Radio Templates' configuration window in the Cisco Wireless Control System. The window is titled 'AP/Radio Templates > test'. It has several tabs: 'AP Parameters', '802.11a/n Parameters', '802.11b/g/n Parameters', 'Select APs', and 'Apply'. The 'AP Parameters' tab is active, showing a list of configuration options. The 'Native VLAN ID' field is highlighted in yellow, indicating the step to configure it. The 'Native VLAN ID' field is currently set to 0. The 'H-REAP Configuration' section has a 'VLAN Support' checkbox that is unchecked, and a 'Native VLAN ID' field that is currently set to 0.

Category	Field	Value
Location	Location	
Admin Status	Admin Status	<input type="checkbox"/> Enabled
AP Mode	AP Mode	Local
Mirror Mode	Mirror Mode	<input type="checkbox"/> Enabled
Country Code	Country Code	AR - Argentina
Stats Collection Interval	Stats Collection Interval	0
Bridging(Mesh APs only)	Bridging(Mesh APs only)	<input type="checkbox"/> Enabled
Role	Role	MAP
Bridge Group Name	Bridge Group Name	
Data Rate	Data Rate	
Ethernet Bridging	Ethernet Bridging	Disabled
Cisco Discovery Protocol	Cisco Discovery Protocol	<input type="checkbox"/> Enabled
Reboot AP	Reboot AP (Selecting this will reboot AP after making other selected updates, if any)	<input type="checkbox"/> Enabled
Controllers	Primary Controller Name	
Controllers	Secondary Controller Name	
Controllers	Tertiary Controller Name	
Group VLAN name	Group VLAN name	
H-REAP Configuration	VLAN Support	<input type="checkbox"/> Enabled
H-REAP Configuration	Native VLAN ID	0

**Alarm Summary**

Rogue AP	0	146
Coverage Hole	0	0
Security	2	0
Controllers	0	1
Access Points	1	0
Mesh Links	0	0
Location	0	0

230753

- Step 7** Check the **Enable VLAN** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN Identifier** field.



**Note** By default, a VLAN is not enabled on the hybrid-REAP access point. Once hybrid REAP is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per hybrid-REAP access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

- Step 8** Click **Save** to save your changes.
- Step 9** The Locally Switched VLANs section allows you to view which WLANs are locally switched and their VLAN identifier. You can edit the number of VLANs from which the clients will get an IP address by clicking the **Edit** link. You are then redirected to a page where you can save the VLAN identifier changes.
- Step 10** Click **Save** to save your changes.
- Step 11** Repeat this procedure for any additional access points that need to be configured for hybrid REAP at the remote site.

## Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the [“Configuring the Controller for Hybrid REAP”](#) section on page 12-6.

In our example, you would create three profiles on the client:

1. To connect to the “employee” WLAN, you would create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it should get an IP address from the management VLAN of the controller.
2. To connect to the “local-employee” WLAN, you would create a client profile that uses WPA/WPA2-PSK authentication. When the client becomes authenticated, it should get an IP address from VLAN 101 on the local switch.
3. To connect to the “guest-central” WLAN, you would create a profile that uses open authentication. Once the client becomes authenticated, it should get an IP address from VLAN 101 on the network local to the access point. Once the client connects, the local user can type any http address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters his or her username and password.

To see if a client’s data traffic is being locally or centrally switched, click **Monitor > Devices > Clients**.

---