



CHAPTER 13

Configuring Hybrid REAP

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

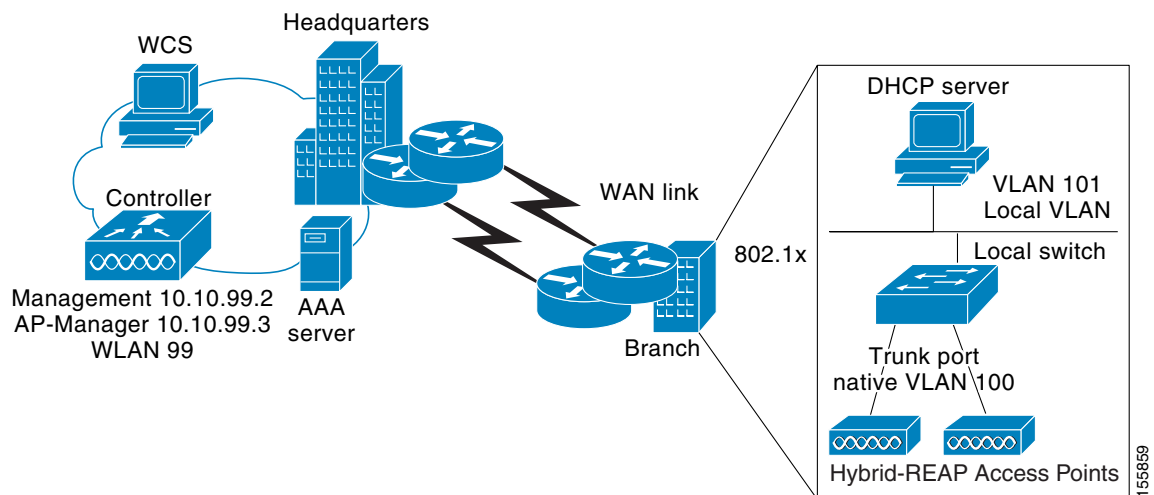
- [Overview of Hybrid REAP, page 13-2](#)
- [Configuring Hybrid REAP, page 13-5](#)
- [Configuring Hybrid-REAP Groups, page 13-15](#)

Overview of Hybrid REAP

Hybrid REAP is a wireless 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. 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, 1140, 1240AG, 1250, and AP801 access points and on the 2100 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Controller Network Module for Integrated Services Routers. [Figure 13-1](#) illustrates a typical hybrid-REAP deployment.

Figure 13-1 Hybrid REAP Deployment



There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restriction remains 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

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 and configuration from the controller, 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 CAPWAP or 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. Refer to [“The Controller Discovery Process”](#) section on page 7-2 for more information.

- If the access point has been assigned a static IP address, it can discover a controller through any of the 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 CAPWAP or 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.

**Note**

Refer to [Chapter 7](#) or the controller deployment guide at this URL for more information on how access points find controllers:

<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>

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 is tunneled 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. In controller software release 4.2 or later, this is also true for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or CCKM, but these authentication types require that an external RADIUS server be configured. Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

When hybrid-REAP access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the **config radius auth add** CLI command (unless the server order is overridden for a particular WLAN). However, in order to support 802.1X EAP authentication, hybrid-REAP access points in standalone mode need to have their own backup RADIUS server to authenticate clients. This backup RADIUS server may or may not be the one used by the controller. You can configure a backup RADIUS server for individual hybrid-REAP access points in standalone mode by using the controller CLI or for groups of hybrid-REAP access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a hybrid-REAP group.

When a hybrid-REAP access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For 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 web-authentication WLANs. Controller-dependent activities such as network access control (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 mode.


Note

If your controller is configured for 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. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the “[Configuring Dynamic Interfaces](#)” section on page 3-16 for information on creating quarantined VLANs and the “[Configuring NAC Out-of-Band Integration](#)” section on page 6-59 for information on configuring NAC out-of-band support.

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 up to four fragmented packets or a minimum 500-byte maximum transmission unit (MTU) WAN link.
- Roundtrip latency must not exceed 100 milliseconds (ms) between the access point and the controller, and CAPWAP 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.
- To use CCKM fast roaming with hybrid-REAP access points, you need to configure hybrid-REAP groups. See the “[Configuring Hybrid-REAP Groups](#)” section on page 13-15 for more information.

- Hybrid-REAP access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. Hybrid-REAP access points also support a many-to-one NAT/PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.



Note Although NAT and PAT are supported for hybrid-REAP access points, they are not supported on the corresponding controller. Cisco does not support configurations in which the controller is behind a NAT/PAT boundary.

- VPN and PPTP are supported for locally switched traffic, provided that these security types are accessible locally at the access point.
- Hybrid-REAP access points support multiple SSIDs. Refer to the [“Using the CLI to Create WLANs” section on page 6-6](#) for more information.
- NAC out-of-band integration is supported only on WLANs configured for hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching. Refer to the [“Configuring NAC Out-of-Band Integration” section on page 6-59](#) for more information.
- The primary and secondary controllers for a hybrid-REAP access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features (such as WLAN override, AP group VLANs, static channel number, and so on) might not operate correctly. In addition, make sure to duplicate the SSID of the hybrid-REAP access point and its index number on both controllers.

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 13-5](#)
- [Configuring the Controller for Hybrid REAP, page 13-6](#)
- [Configuring an Access Point for Hybrid REAP, page 13-11](#)
- [Connecting Client Devices to the WLANs, page 13-15](#)

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 using either the GUI or the CLI.

Using the GUI to Configure the Controller for Hybrid REAP

The controller configuration for hybrid REAP consists of creating centrally switched and locally switched WLANs. Follow the steps in this section to use the GUI to configure the controller for these 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 (locally switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)



Note

See the “[Using the CLI to Configure the Controller for Hybrid REAP](#)” section on page 13-11 if you would prefer to configure the controller for hybrid REAP using the CLI.

Step 1

Follow these steps to create a centrally switched WLAN. In our example, this is the first WLAN (employee).

- a. Click **WLANs** to open the WLANs page.
- b. Choose **Create New** from the drop-down box and click **Go** to open the WLANs > New page (see [Figure 13-2](#)).

Figure 13-2 WLANs > New Page

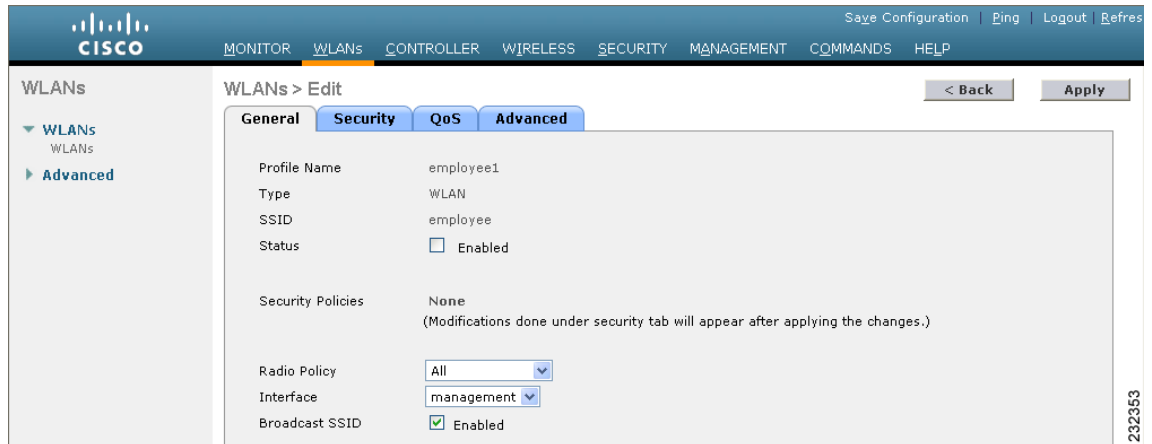
The screenshot shows the Cisco WLANs > New page. The page has a navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The main content area is titled 'WLANs > New' and contains a form with the following fields:

- Type: WLAN (dropdown menu)
- Profile Name: (text input field)
- WLAN SSID: (text input field)
- WLAN ID: 5 (dropdown menu)

At the bottom right of the form, there are two buttons: '< Back' and 'Apply'.

- c. From the Type drop-down box, choose **WLAN**.
- d. Enter a unique profile name for the WLAN in the Profile Name field.
- e. Enter a name for the WLAN in the WLAN SSID field.
- f. From the WLAN ID drop-down box, choose the ID number for this WLAN.
- g. Click **Apply** to commit your changes. The WLANs > Edit page appears (see [Figure 13-3](#)).

Figure 13-3 WLANs > Edit Page



- h. Modify the configuration parameters for this WLAN using the various WLANs > Edit tabs. In our employee WLAN example, you would need to choose **WPA+WPA2** for Layer 2 Security from the Security > Layer 2 tabs and then set the WPA+WPA2 parameters.



Note Be sure to enable this WLAN by checking the **Status** check box on the General tab.



Note If NAC is enabled and you created a quarantined VLAN and want to use it for this WLAN, be sure to select it from the Interface drop-down box on the General tab.

- i. Click **Apply** to commit your changes.
- j. Click **Save Configuration** to save 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. When the WLANs > Edit page appears, modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA+WPA2** for Layer 2 Security from the Security > Layer 2 tabs and then set the WPA+WPA2 parameters.



Note Be sure to enable this WLAN by checking the **Status** check box on the General tab. Also, be sure to enable local switching by checking the **H-REAP Local Switching** check box on the Advanced tab. 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**

When you enable hybrid-REAP local switching, the **Learn Client IP Address** check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

**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.
- d. Click **Save Configuration** to save 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.

**Note**

[Chapter 10](#) provides additional information on creating guest user accounts.

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

**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 on the Layer 3 tab. See [Chapter 5](#) for more information on ACLs.

**Note**

Make sure to enable this WLAN by checking the **Status** check box on the General tab.

- c. Click **Apply** to commit your changes.
- d. Click **Save Configuration** to save 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 [Chapter 5](#).
- f. To add a local user to this WLAN, click **Security > AAA > Local Net Users**.
- g. When the Local Net Users page appears, click **New**. The Local Net Users > New page appears (see [Figure 13-4](#)).

Figure 13-4 Local Net Users > New Page

The screenshot shows the Cisco configuration interface for creating a new local user. The left sidebar lists navigation options under 'Security', including AAA, Local EAP, and Access Control Lists. The main content area is titled 'Local Net Users > New' and contains the following fields:

- User Name: cisco123
- Password: [masked]
- Confirm Password: [masked]
- Guest User:
- Lifetime (seconds): 86400
- Guest User Role:
- WLAN Profile: Any WLAN (dropdown menu)
- Description: Guest user

Buttons for '< Back' and 'Apply' are located at the top right of the form area. The Cisco logo and navigation tabs (MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP) are visible at the top.

- h. In the User Name and Password fields, enter a username and password for the local user.
- i. In the Confirm Password field, re-enter the password.
- j. Check the **Guest User** check box to enable this local user account.
- k. In the Lifetime field, enter the amount of time (in seconds) for this user account to remain active.
- l. If you are adding a new user, you checked the Guest User check box, and you want to assign a QoS role to this guest user, check the **Guest User Role** check box. The default setting is unchecked.



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.

- m. If you are adding a new user and you checked the Guest User Role check box, choose the QoS role that you want to assign to this guest user from the Role drop-down box. If you want to create a new QoS role, see the [“Configuring Quality of Service Roles”](#) section on page 4-48 for instructions.
- n. From the WLAN Profile drop-down box, 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.
- o. In the Description field, enter a descriptive title for the local user (such as “Guest user”).
- p. Click **Apply** to commit your changes.
- q. Click **Save Configuration** to save your changes.

Step 4 Go to the [“Configuring an Access Point for Hybrid REAP”](#) section on page 13-11 to configure up to six access points for hybrid REAP.

Using the CLI to Configure the Controller for Hybrid REAP

Use these commands to configure the controller for hybrid REAP:

- **config wlan h-reap local-switching *wlan_id* enable**—Configures the WLAN for local switching.



Note

When you enable hybrid-REAP local switching, the controller waits to learn the client IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Use this command to disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client IP address: **config wlan h-reap learn-ipaddr *wlan_id* disable**. The ability to disable this feature is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching. If you later want to re-enable this feature, enter this command: **config wlan h-reap learn-ipaddr *wlan_id* enable**.

- **config wlan h-reap local-switching *wlan_id* disable**—Configures the WLAN for central switching. This is the default value.



Note

Go to the [“Configuring an Access Point for Hybrid REAP” section on page 13-11](#) to configure up to six access points for hybrid REAP.

Use these commands to obtain hybrid-REAP information:

- **show ap config general *Cisco_AP***—Shows VLAN configurations.
- **show wlan *wlan_id***—Shows whether the WLAN is locally or centrally switched.
- **show client detail *client_mac***—Shows whether the client is locally or centrally switched.

Use these commands to obtain debug information:

- **debug hreap aaa {event | error} {enable | disable}**—Enables or disables debugging of hybrid-REAP backup RADIUS server events or errors.
- **debug hreap cckm {enable | disable}**—Enables or disables debugging of hybrid-REAP CCKM.
- **debug hreap group {enable | disable}**—Enables or disables debugging of hybrid-REAP groups.
- **debug pem state {enable | disable}**—Enables or disables debugging of the policy manager state machine.
- **debug pem events {enable | disable}**—Enables or disables debugging of policy manager events.

Configuring an Access Point for Hybrid REAP

This section provides instructions for configuring an access point for hybrid REAP using either the controller GUI or CLI.

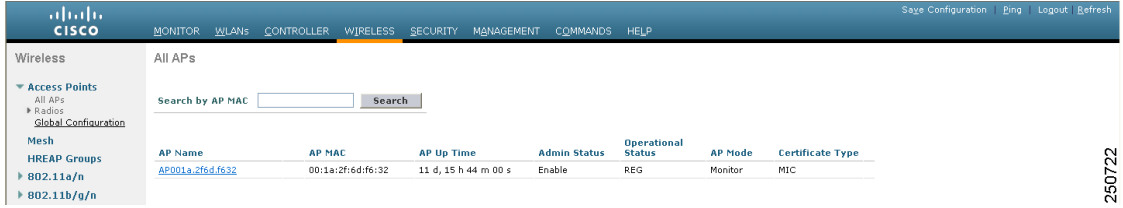
Using the GUI to Configure an Access Point for Hybrid REAP

Follow these steps to configure an access point for hybrid REAP using the controller GUI.

-
- Step 1** Make sure that the access point has been physically added to your network.

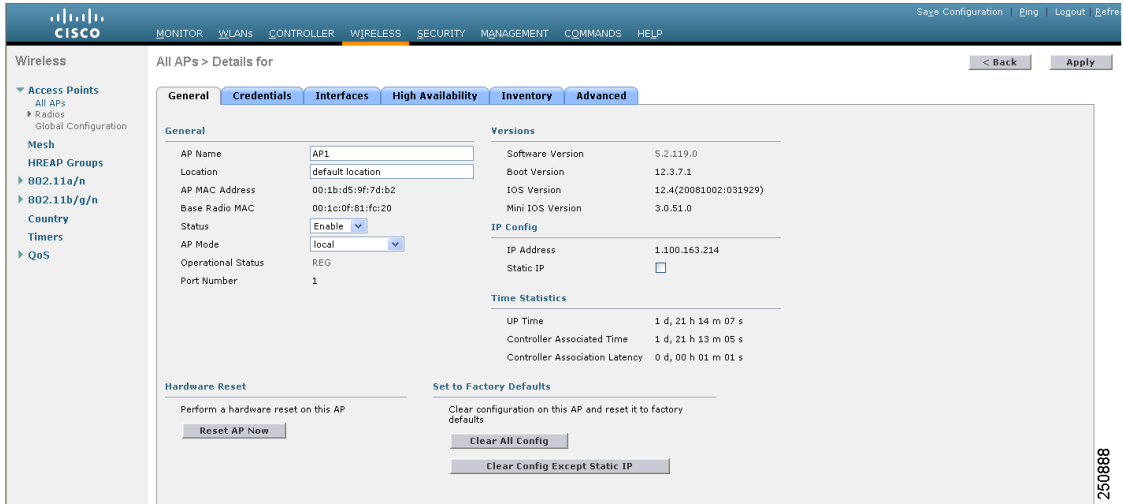
Step 2 Click **Wireless** to open the All APs page (see [Figure 13-5](#)).

Figure 13-5 All APs Page



Step 3 Click the name of the desired access point. The All APs > Details (General) page appears (see [Figure 13-6](#)).

Figure 13-6 All APs > Details for (General) Page



Step 4 Choose **H-REAP** from the AP Mode drop-down box to enable hybrid REAP for this access point.

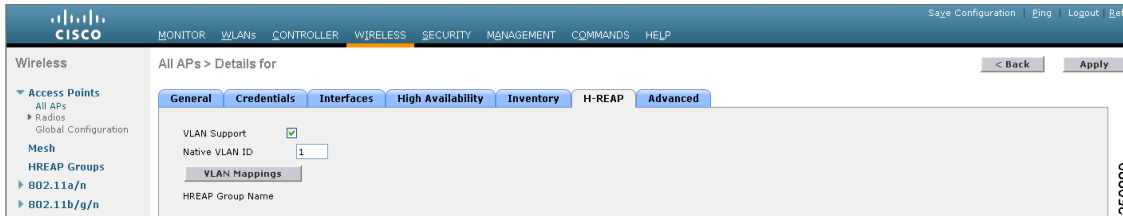


Note The last parameter on the Inventory tab indicates whether this access point can be configured for hybrid REAP. Only the 1130AG, 1240AG, and 1250 access points support hybrid REAP.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Step 6 Click the **H-REAP** tab to open the All APs > Details for (H-REAP) page (see [Figure 13-7](#)).

Figure 13-7 All APs > Details for (H-REAP) Page



If the access point belongs to a hybrid-REAP group, the name of the group appears in the HREAP Group Name field.

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

- Step 8** Click **Apply** to commit your changes. The access point temporarily loses its connection to the controller while its Ethernet port is reset.
- Step 9** Click the name of the same access point and then click the **H-REAP** tab.
- Step 10** Click **VLAN Mappings** to open the All APs > Access Point Name > VLAN Mappings page (see Figure 13-8).

Figure 13-8 All APs > Access Point Name > VLAN Mappings Page

The screenshot shows the Cisco Wireless LAN Controller configuration page for VLAN Mappings. The page title is "All APs > 1240-SHD-33558c > VLAN Mappings". The page includes a navigation menu with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The WIRELESS tab is selected. The page content is divided into two main sections: "Wireless" and "Centrally switched Wlans".

The "Wireless" section shows a table with columns for WLAN Id, SSID, and VLAN ID. The table contains one row with WLAN Id 2, SSID employee-local, and VLAN ID 101.

WLAN Id	SSID	VLAN ID
2	employee-local	101

The "Centrally switched Wlans" section shows a table with columns for WLAN Id, SSID, and VLAN ID. The table contains two rows with WLAN Ids 1 and 3, SSIDs employee and guest-access, and VLAN IDs N/A.

WLAN Id	SSID	VLAN ID
1	employee	N/A
3	guest-access	N/A

- Step 11** Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the VLAN ID field.
- Step 12** Click **Apply** to commit your changes.
- Step 13** Click **Save Configuration** to save your changes.
- Step 14** Repeat this procedure for any additional access points that need to be configured for hybrid REAP at the remote site.

Using the CLI to Configure an Access Point for Hybrid REAP

Use these commands on the controller to configure an access point for hybrid REAP:

- **config ap mode h-reap** *Cisco_AP*—Enables hybrid REAP for this access point.
- **config ap h-reap radius auth set** {primary | secondary} *ip_address auth_port secret Cisco_AP*—Configures a primary or secondary RADIUS server for a specific hybrid-REAP access point.



Note Only the Session Timeout RADIUS attribute is supported in standalone mode. All other attributes as well as RADIUS accounting are not supported.



Note To delete a RADIUS server that is configured for a hybrid-REAP access point, enter this command: **config ap h-reap radius auth delete** {primary | secondary} *Cisco_AP*

- **config ap h-reap vlan wlan** *wlan_id vlan-id Cisco_AP*—Enables you to assign a VLAN ID to this hybrid-REAP access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap h-reap vlan** {enable | disable} *Cisco_AP*—Enables or disables VLAN tagging for this hybrid-REAP access point. By default, VLAN tagging is not enabled. Once VLAN tagging is enabled on the hybrid-REAP access point, WLANs enabled for local switching inherit the VLAN assigned at the controller.
- **config ap h-reap vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this hybrid-REAP access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per hybrid-REAP access point (when VLAN tagging is enabled). Make sure the switchport to which the access point is connected has a corresponding native VLAN configured as well. If the hybrid-REAP access point's native VLAN setting and the upstream switchport native VLAN do not match, the access point cannot transmit packets to and from the controller.

Use these commands on the hybrid-REAP access point to obtain status information:

- **show capwap reap status**—Shows the status of the hybrid-REAP access point (connected or standalone).
- **show capwap reap association**—Shows the list of clients associated to this access point and their SSIDs.

Use these commands on the hybrid-REAP access point to obtain debug information:

- **debug capwap reap**—Shows general hybrid-REAP activities.
- **debug capwap reap mgmt**—Shows client authentication and association messages.
- **debug capwap reap load**—Shows payload activities, which is useful when the hybrid-REAP access point boots up in standalone mode.
- **debug dot11 mgmt interface**—Shows 802.11 management interface events.
- **debug dot11 mgmt msg**—Shows 802.11 management messages.
- **debug dot11 mgmt ssid**—Shows SSID management events.
- **debug dot11 mgmt state-machine**—Shows the 802.11 state machine.
- **debug dot11 mgmt station**—Shows client events.

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 13-6](#).

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. Once 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 authentication. Once 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 client 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.

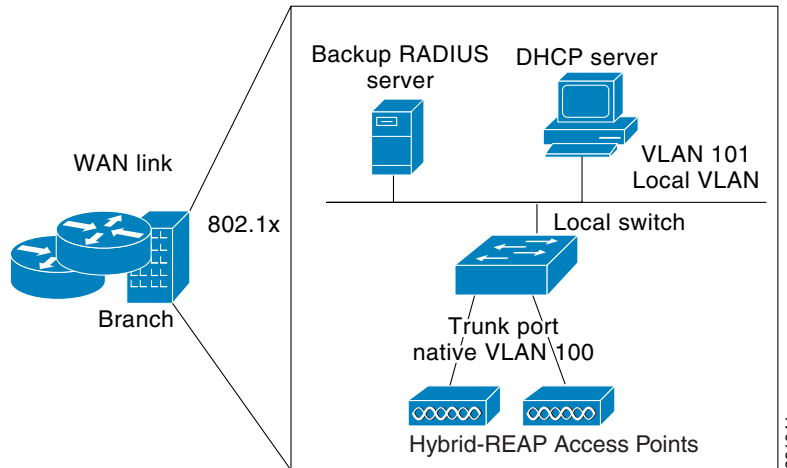
To see if a client’s data traffic is being locally or centrally switched, click **Monitor** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the Data Switching parameter under AP Properties.

Configuring Hybrid-REAP Groups

In order to better organize and manage your hybrid-REAP access points, you can create hybrid-REAP groups and assign specific access points to them. Per controller, you can configure up to 20 hybrid-REAP groups with up to 25 access points per group.

All of the hybrid-REAP access points in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple hybrid-REAP access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a hybrid-REAP group rather than having to configure the same server on each access point. [Figure 13-9](#) illustrates a typical hybrid-REAP group deployment with a backup RADIUS server in the branch office.

Figure 13-9 Hybrid-REAP Group Deployment



Hybrid-REAP Groups and Backup RADIUS Servers

You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. You can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers are used only when the hybrid-REAP access point is not connected to the controller.

Hybrid-REAP Groups and CCKM

Hybrid-REAP groups are required for CCKM fast roaming to work with hybrid-REAP access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The hybrid-REAP access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a hybrid-REAP group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.



Note

CCKM fast roaming among hybrid-REAP and non-hybrid-REAP access points is not supported. Refer to the [“WPA1 and WPA2”](#) section on page 6-23 for information on configuring CCKM.

Hybrid-REAP Groups and Local Authentication

You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the static list of usernames and passwords to each hybrid-REAP access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight hybrid-REAP access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.



Note

This feature can be used in conjunction with the hybrid-REAP backup RADIUS server feature. If a hybrid-REAP group is configured with both a backup RADIUS server and local authentication, the hybrid-REAP access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the hybrid-REAP access point itself (if the primary and secondary are not reachable).

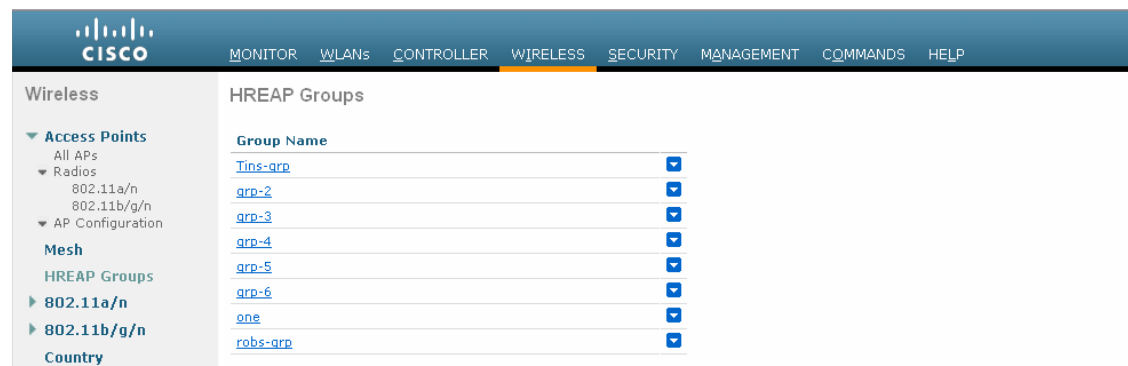
Follow the instructions in this section to configure hybrid-REAP groups using the controller GUI or CLI.

Using the GUI to Configure Hybrid-REAP Groups

Follow these steps to configure hybrid-REAP groups using the controller GUI.

- Step 1** Click **Wireless > HREAP Groups** to open the HREAP Groups page (see [Figure 13-10](#)).

Figure 13-10 HREAP Groups Page



203156

This page lists any hybrid-REAP groups that have already been created.



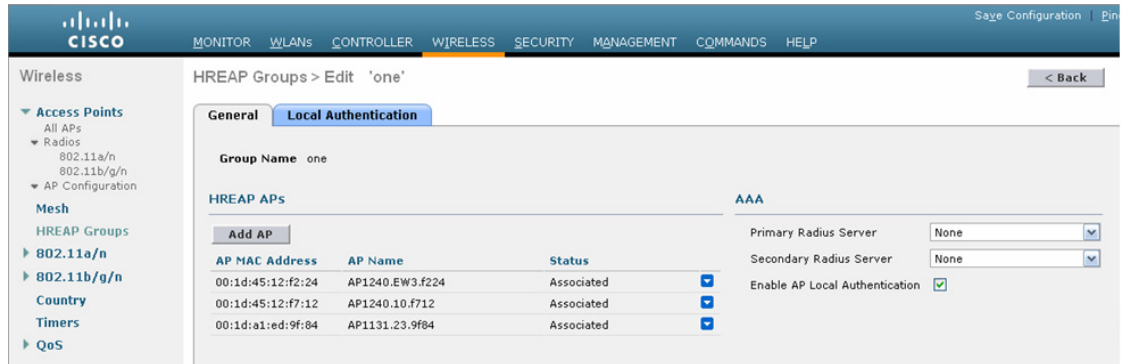
Note

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

- Step 2** To create a new hybrid-REAP group, click **New**.
- Step 3** When the HREAP Groups > New page appears, enter the name of the new group in the Group Name field. You can enter up to 32 alphanumeric characters.

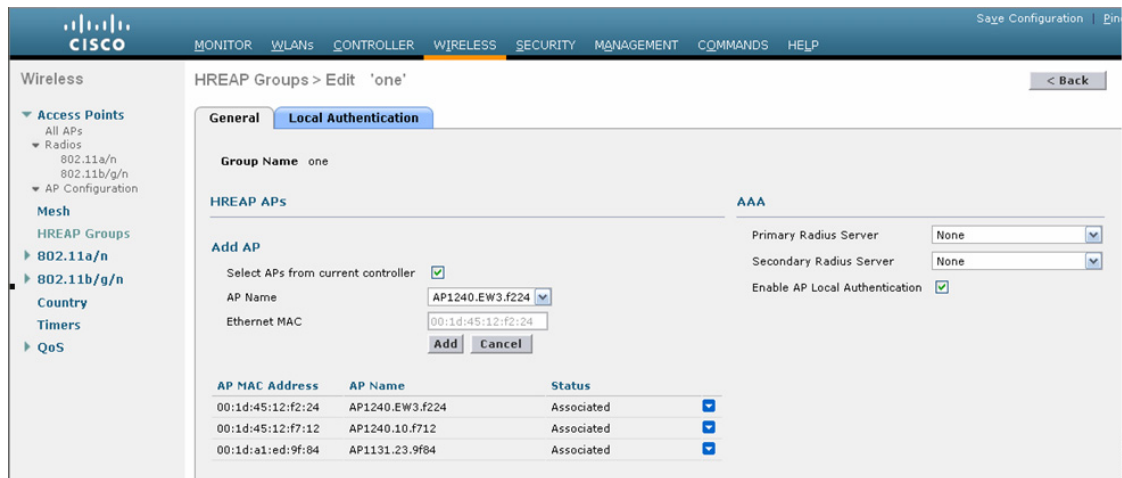
- Step 4** Click **Apply** to commit your changes. The new group appears on the HREAP Groups page.
- Step 5** To edit the properties of a group, click the name of the desired group. The HREAP Groups > Edit (General) page appears (see [Figure 13-11](#)).

Figure 13-11 HREAP Groups > Edit (General) Page



- Step 6** If you want to configure a primary RADIUS server for this group (for example, the access points are using 802.1X authentication), choose the desired server from the Primary RADIUS Server drop-down list. Otherwise, leave the field set to the default value of None.
- Step 7** If you want to configure a secondary RADIUS server for this group, choose the server from the Secondary RADIUS Server drop-down list. Otherwise, leave the field set to the default value of None.
- Step 8** To add an access point to the group, click **Add AP**. Additional fields appear on the page under “Add AP” (see [Figure 13-12](#)).

Figure 13-12 HREAP Groups > Edit (General) Page



Step 9 Perform one of the following:

- To choose an access point that is connected to this controller, check the **Select APs from Current Controller** check box and choose the name of the access point from the AP Name drop-down box.



Note If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC field to prevent any mismatches from occurring.

- To choose an access point that is connected to a different controller, leave the **Select APs from Current Controller** check box unchecked and enter its MAC address in the Ethernet MAC field.



Note If the hybrid-REAP access points within a group are connected to different controllers, all of the controllers must belong to the same mobility group.

Step 10 Click **Add** to add the access point to this hybrid-REAP group. The access point's MAC address, name, and status appear at the bottom of the page.



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

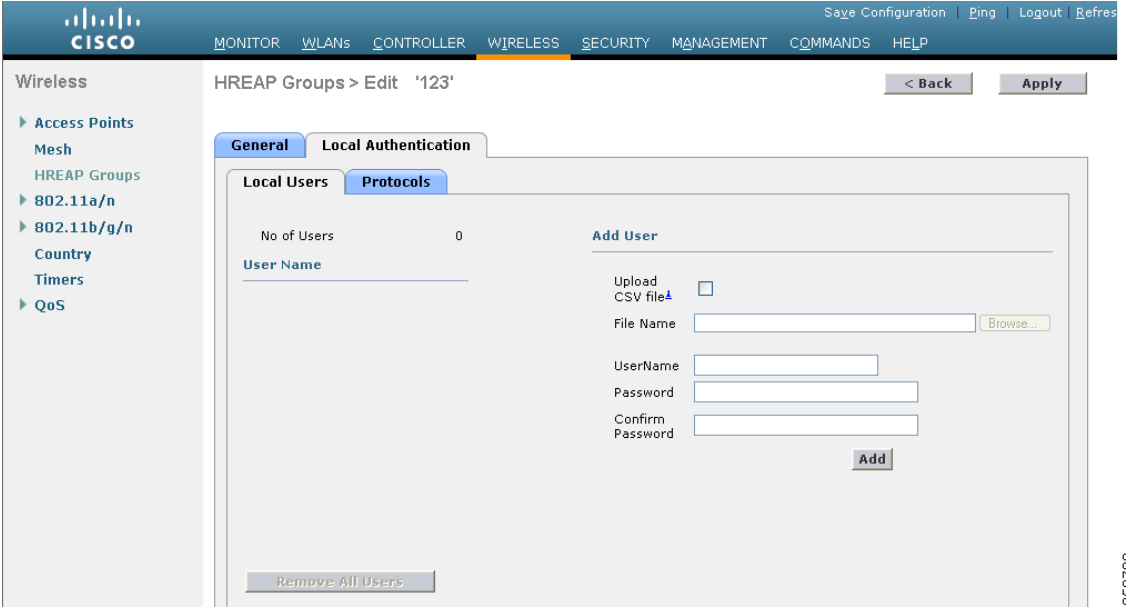
Step 11 Click **Apply** to commit your changes.

Step 12 Repeat [Step 9](#) through [Step 11](#) if you want to add more access points to this hybrid-REAP group.

Step 13 If you want to enable local authentication for a hybrid-REAP group, follow these steps:

- a. Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None**.
- b. Check the **Enable AP Local Authentication** check box to enable local authentication for this hybrid-REAP group. The default value is unchecked.
- c. Click **Apply** to commit your changes.
- d. Click the **Local Authentication** tab to open the HREAP Groups > Edit (Local Authentication > Local Users) page (see [Figure 13-13](#)).

Figure 13-13 HREAP Groups > Edit (Local Authentication > Local Users) Page



e. To add clients that you want to be able to authenticate using LEAP or EAP-FAST, perform one of the following:

- Upload a comma-separated values (CSV) file by checking the **Upload CSV File** check box, clicking the **Browse** button to browse to a CSV file that contains usernames and passwords (each line of the file needs to be in the following format: username, password), and clicking **Add** to upload the CSV file. The clients' names appear on the left side of the page under the "User Name" heading.
- Add clients individually by entering the client's username in the User Name field and a password for the client in the Password and Confirm Password fields, and clicking **Add** to add this client to the list of supported local users. The client name appears on the left side of the page under the "User Name" heading.



Note You can add up to 100 clients.

- f. Click **Apply** to commit your changes.
- g. Click the **Protocols** tab to open the HREAP Groups > Edit (Local Authentication > Protocols) page (see Figure 13-14).

Figure 13-14 HREAP Groups > Edit (Local Authentication > Protocols) Page

- h. To allow a hybrid-REAP access point to authenticate clients using LEAP, check the **Enable LEAP Authentication** check box; then go to [Step n](#).
- i. To allow a hybrid-REAP access point to authenticate clients using EAP-FAST, check the **Enable EAP-FAST Authentication** check box; then go to the next step. The default value is unchecked.
- j. Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:
 - To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key fields. The key must be 32 hexadecimal characters.
 - To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, check the **Enable Auto Key Generation** check box.
- k. In the Authority ID field, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
- l. In the Authority Info field, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
- m. To specify a PAC timeout value, check the **PAC Timeout** check box and enter the number of seconds for the PAC to remain viable in the edit box. The default value is unchecked, and the valid range is 2 to 4095 seconds when enabled.
- n. Click **Apply** to commit your changes.

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

Step 15 Repeat this procedure if you want to add more hybrid-REAP groups.




Note To see if an individual access point belongs to a hybrid-REAP group, you can click **Wireless > Access Points > All APs > the name of the desired access point > the H-REAP** tab. If the access point belongs to a hybrid-REAP group, the name of the group appears in the HREAP Group Name field.

Using the CLI to Configure Hybrid-REAP Groups

Follow these steps to configure hybrid-REAP groups using the controller CLI.

-
- Step 1** To add or delete a hybrid-REAP group, enter this command:
- ```
config hreap group group_name {add | delete}
```
- Step 2** To configure a primary or secondary RADIUS server for the hybrid-REAP group, enter this command:
- ```
config hreap group group_name radius server {add | delete} {primary | secondary} server_index
```
- Step 3** To add an access point to the hybrid-REAP group, enter this command:
- ```
config hreap group group_name ap {add | delete} ap_mac
```
- Step 4** To configure local authentication for a hybrid-REAP group, follow these steps:
- Make sure that a primary and secondary RADIUS server are not configured for the hybrid-REAP group.
  - To enable or disable local authentication for this hybrid-REAP group, enter this command:

```
config hreap group group_name radius ap {enable | disable}
```
  - To enter the username and password of a client that you want to be able to authenticate using LEAP or EAP-FAST, enter this command:

```
config hreap group group_name radius ap user add username password password
```
- 
-  **Note** You can add up to 100 clients.
- 
- To allow a hybrid-REAP access point to authenticate clients using LEAP or to disable this behavior, enter this command:

```
config hreap group group_name radius ap leap {enable | disable}
```
  - To allow a hybrid-REAP access point to authenticate clients using EAP-FAST or to disable this behavior, enter this command:

```
config hreap group group_name radius ap eap-fast {enable | disable}
```
  - Enter one of the following commands, depending on how you want PACs to be provisioned:
    - config hreap group** *group\_name* **radius ap server-key** *key*—Specifies the server key used to encrypt and decrypt PACs. The key must be 32 hexadecimal characters.
    - config hreap group** *group\_name* **radius ap server-key auto**—Allows PACs to be sent automatically to clients that do not have one during PAC provisioning.
  - To specify the authority identifier of the EAP-FAST server, enter this command:

```
config hreap group group_name radius ap authority id id
```

where *id* is 32 hexadecimal characters.
  - To specify the authority identifier of the EAP-FAST server in text format, enter this command:

```
config hreap group group_name radius ap authority info info
```

where *info* is up to 32 hexadecimal characters.

- i. To specify the number of seconds for the PAC to remain viable, enter this command:

```
config hreap group group_name radius ap pac-timeout timeout
```

where *timeout* is a value between 2 and 4095 seconds (inclusive) or 0. A value of 0, which the default value, disables the PAC timeout.

- Step 5** To save your changes, enter this command:

```
save config
```

- Step 6** To see the current list of hybrid-REAP groups, enter this command:

```
show hreap group summary
```

Information similar to the following appears:

```
HREAP Group Summary: Count 2
```

```
Group Name # Aps
Group 1 1
Group 2 1
```

- Step 7** To see the details for a specific hybrid-REAP group, enter this command:

```
show hreap group detail group_name
```

Information similar to the following appears:

```
Number of Ap's in Group: 3
```

```
00:1d:45:12:f2:24 AP1240.EW3.f224 Joined
00:1d:45:12:f7:12 AP1240.10.f712 Joined
00:1d:a1:ed:9f:84 AP1131.23.9f84 Joined
```

```
Group Radius Servers Settings:
```

```
Primary Server Index..... Disabled
Secondary Server Index..... Disabled
```

```
Group Radius AP Settings:
```

```
AP RADIUS server..... Enabled
EAP-FAST Auth..... Enabled
LEAP Auth..... Enabled
Server Key Auto Generated... No
Server Key..... <hidden>
Authority ID..... 436973636f0000000000000000000000
Authority Info..... Cisco A_ID
PAC Timeout..... 0
Number of User's in Group: 20
```

```
1cisco 2cisco
3cisco 4cisco
 cisco test1
test10 test11
test12 test13
test14 test15
 test2 test3
 test4 test5
 test6 test7
test8 test9
```

