Configuring OfficeExtend Access Points

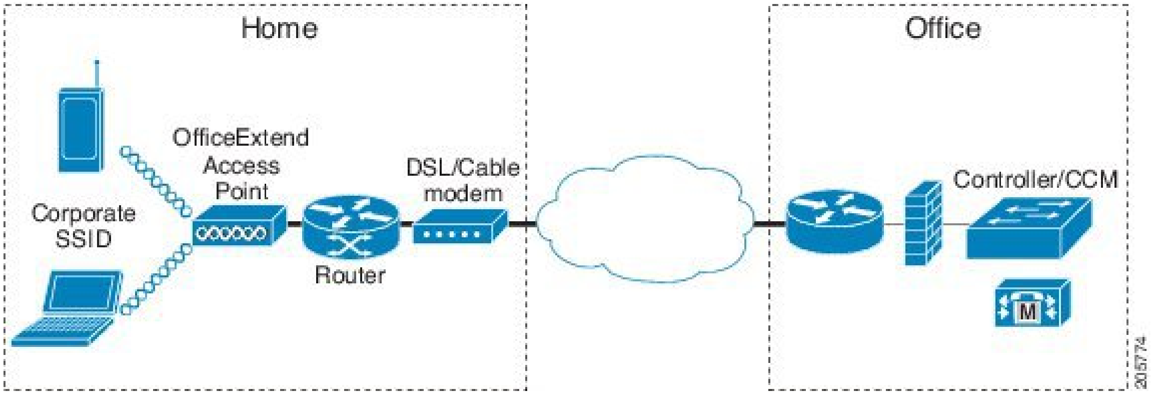
Information About OfficeExtend Access Points

A Cisco OfficeExtend access point (Cisco OEAP) provides secure communications from a Cisco WLC to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Note DTLS is permanently enabled on the Cisco OEAP. You cannot disable DTLS on this access point.

The following figure shows a typical OfficeExtend access point setup.

Figure 1: Typical OfficeExtend Access Point Setup



Note Cisco OEAPs are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device.

All the supported indoor AP models with integrated antenna can be configured as OEAP except the AP-700I, AP-700W, and AP802 series access points.

Note See the Release Notes for information about supported Cisco OEAPs.

OEAP 600 Series Access Points

This section details the requirements for configuring a Cisco wireless LAN controller for use with the Cisco 600 Series OfficeExtend Access Point. The 600 Series OfficeExtend Access Point supports split mode operation, and it requires configuration through the WLAN controller in local mode. This section describes the configurations necessary for proper connection and supported feature sets.

Note IPv6 is not supported on Cisco 600 Series OfficeExtend Access Points.

Note The CAPWAP UDP 5246 and 5247 ports must be open on the firewall between the WLAN controller and the 600 Series OfficeExtend Access Point.

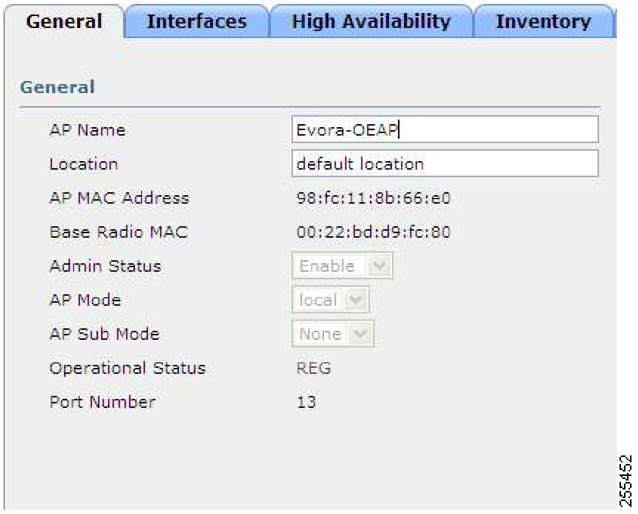
Note Multicast is not supported on Cisco 600 Series OfficeExtend Access Points.

OEAP in Local Mode

The Cisco OEAP connects to the Cisco WLC in local mode. You cannot alter these settings.

Note Monitor mode, FlexConnect mode, Sniffer mode, Rogue Detector, Bridge, and SE-Connect are not supported on the Cisco OEAP and are not configurable.

Figure 2: OEAP Mode



General

AP Name	Evora-OEAP
Location	default location
AP MAC Address	98:fc:11:8b:66:e0
Base Radio MAC	00:22:bd:d9:fc:80
Admin Status	Enable
AP Mode	local
AP Sub Mode	None
Operational Status	REG
Port Number	13

Supported WLAN Settings for 600 Series OfficeExtend Access Point

The 600 Series OfficeExtend Access Point supports a maximum of three WLANs and one remote LAN. If your network deployment has more than three WLANs, you must place the 600 Series OfficeExtend Access Point in an AP group. If the 600 Series OfficeExtend Access Points are added to an AP group, the same limit of three WLANs and one remote LAN still applies for the configuration of the AP group.

If the 600 Series OfficeExtend Access Point is in the default group, which means that it is not in a defined AP group, the WLAN/remote LAN IDs must be set lower than ID 8.

If additional WLANs or remote LANs are created with the intent of changing the WLANs or remote LAN being used by the 600 Series OfficeExtend Access Point, you must disable the current WLANs or remote LAN that you are removing before enabling the new WLANs or remote LAN on the 600 Series OfficeExtend Access Point. If there are more than one remote LANs enabled for an AP group, disable all remote LANs and then enable only one of them.

If more than three WLANs are enabled for an AP group, disable all WLANs and then enable only three of them.

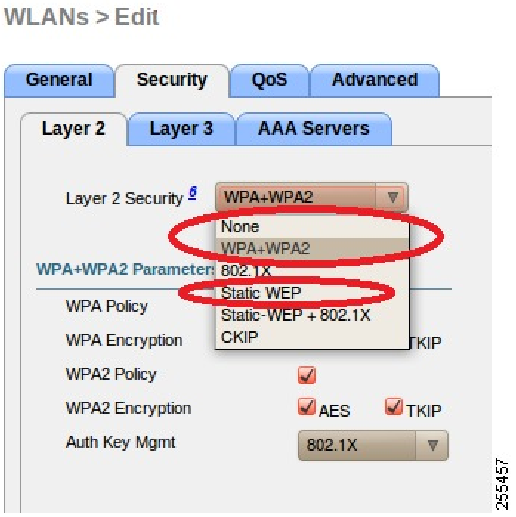
WLAN Security Settings for the 600 Series OfficeExtend Access Point

When configuring the security settings in the WLAN (see the following figure), note that there are specific elements that are not supported on the 600 Series OfficeExtend Access Point. CCX is not supported on the 600 Series OfficeExtend Access Point, and elements related to CCX are not supported.

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

- None
- WPA+WPA2
- Static WEP
- 802.1X (only for remote LANs)

Figure 3: WLAN Layer 2 Security Settings



WLANs > Edit

Layer 2 Security[6] WPA+WPA2

WPA+WPA2 Parameters

WPA Policy

WPA Encryption TKIP

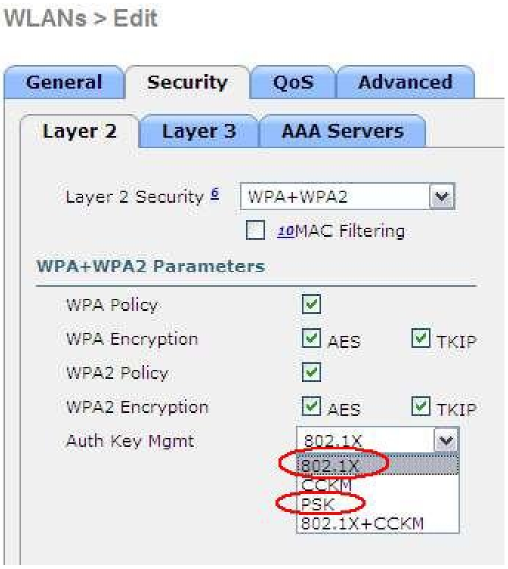
WPA2 Policy ☑

WPA2 Encryption ☑ AES ☑ TKIP

Auth Key Mgmt 802.1X

In the Security tab (see the following figure), do not select CCKM in WPA+WPA2 settings. Select only 802.1X or PSK.

Figure 4: WLAN Security Settings - Auth Key Management



WLANs > Edit

Layer 2 Security [6] WPA+WPA2

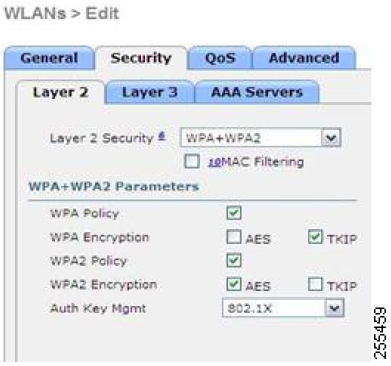
□ [10]MAC Filtering

WPA+WPA2 Parameters

WPA Policy	☑	
WPA Encryption	☑ AES	☑ TKIP
WPA2 Policy	☑	
WPA2 Encryption	☑ AES	☑ TKIP
Auth Key Mgmt	802.1X	

Security encryption settings must be identical for WPA and WPA2 for TKIP and AES. The following are examples of incompatible settings for TKIP and AES.

Figure 5: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series



Layer 2 Security: WPA+WPA2

□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☑

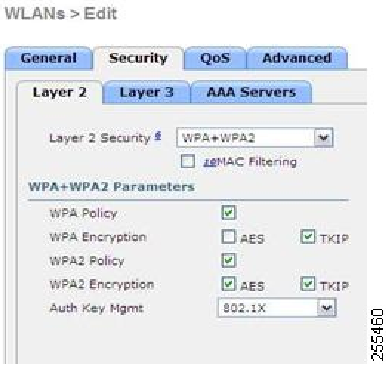
WPA Encryption □ AES ☑ TKIP

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Auth Key Mgmt: 802.1X

Figure 6: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series



Layer 2 Security: WPA+WPA2

□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☑

WPA Encryption □ AES ☑ TKIP

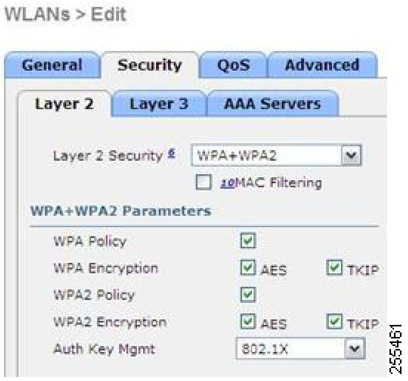
WPA2 Policy ☑

WPA2 Encryption ☑ AES ☑ TKIP

Auth Key Mgmt: 802.1X

The following are examples of compatible settings:

Figure 7: Compatible Security Settings for OEAP Series



Layer 2 Security WPA+WPA2

□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☑

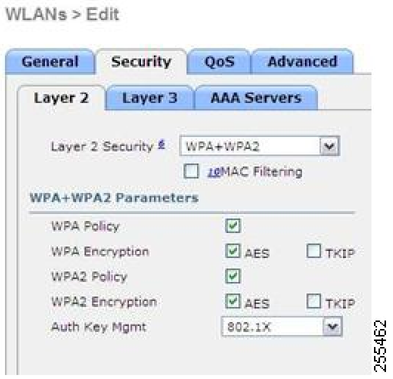
WPA Encryption ☑ AES ☑ TKIP

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☑ TKIP

Auth Key Mgmt 802.1X

Figure 8: Compatible Security Settings for OEAP Series



Layer 2 Security WPA+WPA2

□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☑

WPA Encryption ☑ AES □ TKIP

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

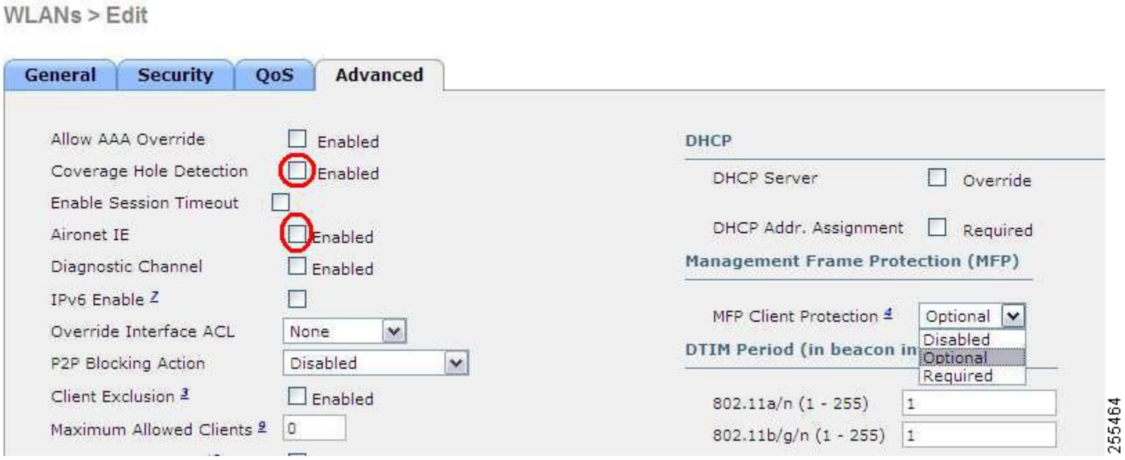
Auth Key Mgmt 802.1X

QoS settings are supported (see the following figure), but CAC is not supported and should not be enabled.

Note Do not enable Coverage Hole Detection.

Note Aironet IE should not be enabled. This option is not supported.

Figure 9: QoS Settings for OEAP 600



WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection □ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable 7 □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 3 □ Enabled
Maximum Allowed Clients 9 0

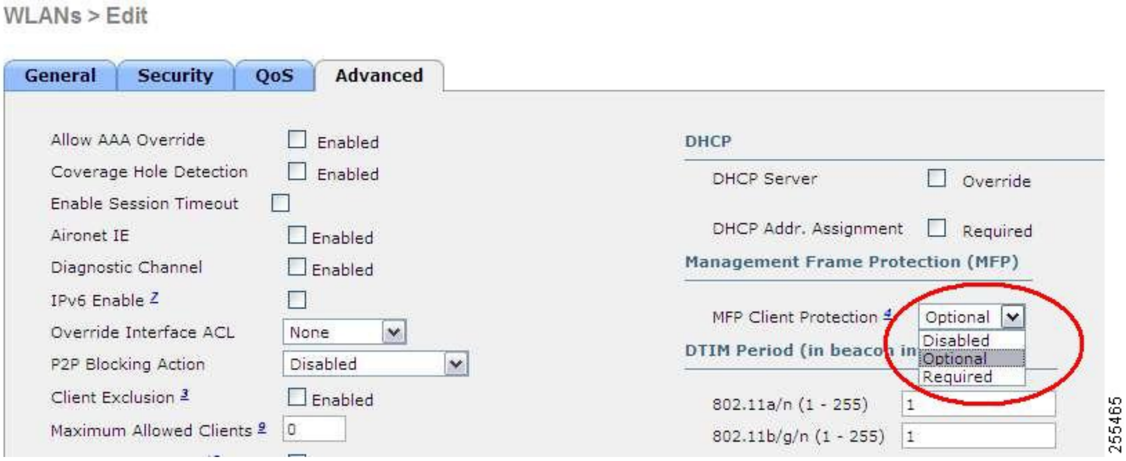
DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon in
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

MFP is also not supported and should be disabled or set to optional.

Figure 10: MFP Settings for OEAP Series Access Points



WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection □ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable 7 □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 3 □ Enabled
Maximum Allowed Clients 9 0

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beaco in
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

Client Load Balancing and Client Band Select are not supported.

Authentication Settings

For authentication on the 600 Series OfficeExtend Access Point, LEAP is not supported. This configuration must be addressed on the clients and RADIUS servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.

If Local EAP is being utilized on the controller, the settings would also have to be modified not to use LEAP.

Supported User Count on 600 Series OfficeExtend Access Point

Only 15 users are allowed to connect on the WLANs provided on the Cisco 600 Series OEAP at any one time, a sixteenth user cannot authenticate until one of the first clients is deauthenticated or timeout on the controller occurs. This number is cumulative across the controller WLANs on the 600 Series OfficeExtend Access Point.

For example, if two controller WLANs are configured and there are 15 users on one of the WLANs, no other users can join the other WLAN on the 600 Series OfficeExtend Access Point at that time.

This limit does not apply to the local private WLANs that the end user configures on the 600 Series OfficeExtend Access Point for personal use. Clients connected on these private WLANs or on the wired ports do not affect these limits.

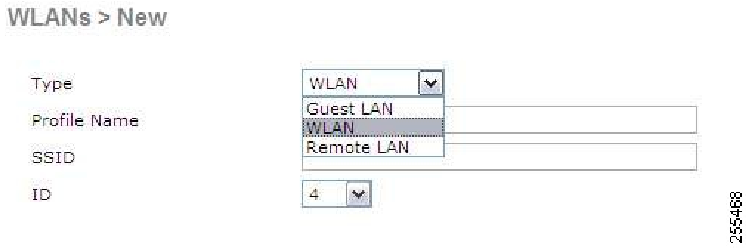
Note This limit does not apply to other AP models that operate in the OfficeExtend mode.

Remote LAN Settings

Only four clients can connect through a remote LAN port on the 600 Series OfficeExtend Access Point. This number does not affect the fifteen user limit imposed for the Controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

Remote LAN is configured in the same way that a WLAN or Guest LAN is configured on the controller:

Figure 11: Remote LAN Settings for OEAP 600 Series AP



WLANs > New

Type: WLAN

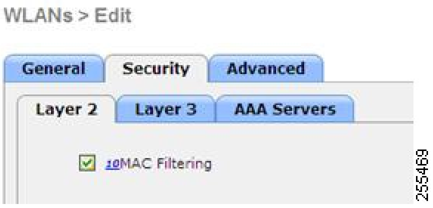
Profile Name

SSID

ID: 4

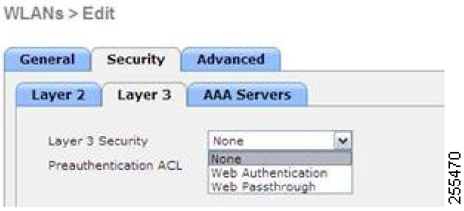
Security settings can be left open, set for MAC filtering, or set for Web Authentication. The default is to use MAC filtering. Additionally, you can specify 802.1X Layer 2 security settings.

Figure 12: Layer 2 Security Settings for OEAP 600 Series APs in Remote LANs



☑ 10MAC Filtering

Figure 13: Layer 3 Security Settings for OEAP 600 Series APs in Remote LANs



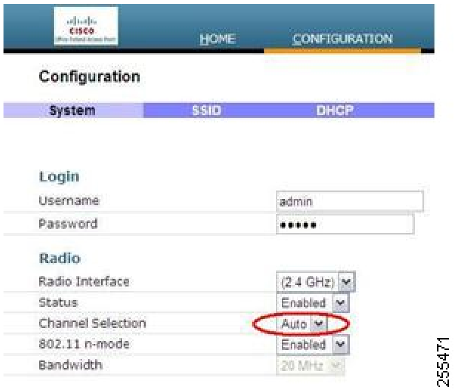
Layer 3 Security: None
Preauthentication ACL

Channel Management and Settings

The radios for the 600 Series OfficeExtend Access Point are controlled through the Local GUI on the access point and not through the Wireless LAN Controller. The Tx power and channel settings can be set manually through the controller interface. RRM is not supported on the 600 Series OfficeExtend Access Point.

The 600 series scans and chooses channels for 2.4-GHz and 5-GHz during startup as long as the default settings on the local GUI are left as default in both spectrums.

Figure 14: Channel Selection for OEAP 600 Series APs

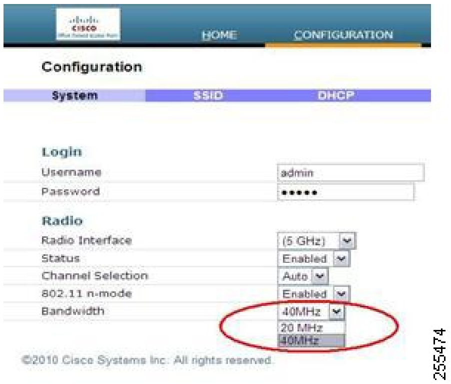


Login
Username: admin
Password: •••••

Radio
Radio Interface: (2.4 GHz)
Status: Enabled
Channel Selection: Auto
802.11 n-mode: Enabled
Bandwidth: 20 MHz

The channel bandwidth for 5.0 GHz is also configured on the 600 Series OfficeExtend Access Point Local GUI, for 20-MHz or 40-MHz wide channels. Setting the channel width to 40 MHz for 2.4 GHz is not supported and fixed at 20 MHz.

Figure 15: Channel Width for OEAP 600 APs



Configuration

Login

Username	admin
Password	•••••

Radio

Radio Interface	(5 GHz)
Status	Enabled
Channel Selection	Auto
802.11 n-mode	Enabled
Bandwidth	40MHz 20 MHz 40MHz

©2010 Cisco Systems Inc. All rights reserved.

Firewall Settings

Firewall can be enabled on Cisco 600 Series OfficeExtend Access Point and filtering and forwarding rules can be applied. These ten pre-configured applications can be enabled or disabled:

- FTP
- Telnet
- SMTP
- DNS
- TFTP
- HTTP
- POP3
- NNTP
- SNMP
- HTTPS

These applications can be unblocked by providing the protocol (TCP/UDP), LAN client IP range and destination port range.

Note The firewall is applicable only to the personal traffic on the OEAP 600 APs The data traffic between the controller and OEAP 600 APs is addressed by a firewall in the corporate network.

600 Series OfficeExtend Access Point supports a maximum of ten port forwarding rules. Every rule takes protocol (TCP/UDP), WAN port range, Local LAN client IP (where traffic will be forwarded), LAN port range, and enable or disable as a parameter.

The DMZ feature allows one network computer connected to local LAN or WLAN to be exposed to the Internet for use of a special-purpose service like Internet gaming. DMZ forwards all the ports terminating on WAN IP at the same time to one PC. The Port Range Forwarding feature opens only the required ports to be opened, while DMZ opens all the ports of one computer, exposing the computer to the Internet or WAN. This will forward all the incoming WAN packets to any port which has the port forwarding rule configured on it. CAPWAP control and data connection ports will not be forwarded to DMZ IP.

Additional Caveats

- The Cisco 600 Series OfficeExtend Access Points (OEAPs) are designed for single AP deployments, therefore client roaming between Cisco 600 Series OEAPs is not supported.

  Disabling the 802.11a/n/ac or 802.11b/g/n on the controller may not disable these spectrums on the Cisco 600 Series OEAP because local SSID may be still working.

- Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

- Cisco Aironet APs other than 600 Series OEAPs that are converted to OEAP mode and mapped to locally switched WLAN forward the DHCP request to the local subnet on the AP connected switch. To avoid this condition, you must disable local switching and local authentication.

- For Cisco 600 Series OEAP to associate with Cisco Virtual Wireless LAN Controller, follow these steps:

  1. Configure the OEAP to associate with a physical controller that is using 7.5 or a later release and download the corresponding AP image.
  2. Configure the OEAP so that the OEAP does not associate with the physical controller again; for example, you can implement an ACL in the network to block CAPWAP between the OEAP and the physical controller.
  3. Configure the OEAP to associate with the Cisco Virtual Wireless LAN Controller.

Implementing Security

Note The LSC configuration is optional. The Cisco OEAPs points do not support LSC.

1. Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in Authorizing Access Points Using LSCs.

2. Implement AAA server validation using the access point’s MAC address, name, or both as the username in authorization requests, by entering this command:

   config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

   Using the access point name for validation can ensure that only the OfficeExtend access points of valid employees can associate with the controller. To implement this security policy, ensure that you name each OfficeExtend access point with an employee ID or employee number. When an employee is terminated, run a script to remove this user from the AAA server database, which prevents that employee’s OfficeExtend access point from joining the network.

3 Save your changes by entering this command:

```
save config
```

Note CCX is not supported on the 600 OEAP. Elements related to CCX are not supported. Also, only 802.1X or PSK is supported. TKIP and AES security encryption settings must be identical for WPA and WPA2.

Licensing for an OfficeExtend Access Point

To use Cisco OEAPs, a base license must be installed and in use on the Cisco WLC. After the license is installed, you can enable the OfficeExtend mode on the supported Cisco Aironet AP models that support OfficeExtend mode.

Configuring OfficeExtend Access Points

After Cisco Aironet access point has associated with the controller, you can configure it as an OfficeExtend access point.

Configuring OfficeExtend Access Points (GUI)

Step 1 Choose **Wireless** to open the **All APs** page.

Step 2 Click the name of the desired access point to open the **All APs > Details** page.

Step 3 Enable FlexConnect on the access point as follows:

a) In the **General** tab, choose **FlexConnect** from the **AP Mode** drop-down list to enable FlexConnect for this access point.

Step 4 Configure one or more controllers for the access point as follows:

a) Click the **High Availability** tab.

b) Enter the name and IP address of the primary controller for this access point in the **Primary Controller Name** and **Management IP Address** text boxes.

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

c) If desired, enter the name and IP address of a secondary or tertiary controller (or both) in the corresponding **Controller Name** and **Management IP Address** text boxes.

d) Click **Apply**. The access point reboots and then rejoins the controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 5 Enable OfficeExtend access point settings as follows:

a) Click the **FlexConnect** tab.

b) Select the **Enable OfficeExtend AP** check box to enable the OfficeExtend mode for this access point. The default value is selected.

Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter **clear ap config** *Cisco_AP* on the controller CLI. If you want to clear only the access point's personal SSID, click **Reset Personal SSID**.

Note The OfficeExtend AP support is enabled for all the supported Cisco Aironet integrated antenna access points.

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the **Data Encryption** check box on the **All APs > Details for (Advanced)** page.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the **Telnet** or **SSH** check box on the **All APs > Details for (Advanced)** page.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the **Enable Link Latency** check box on the All APs > Details for (Advanced) page.

c) Check the **Enable Least Latency Controller Join** check box if you want the access point to choose the controller with the least latency when joining. Otherwise, leave this check box unchecked, which is the default value. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco WLC that responds first.

d) Click **Apply**.
The **OfficeExtend AP** text box on the All APs page shows which access points are configured as OfficeExtend access points.

Step 6 Configure a specific username and password for the OfficeExtend access point so that the user at home can log into the GUI of the OfficeExtend access point:

a) Click the **Credentials** tab.

b) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

c) In the **Username**, **Password**, and **Enable Password** text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

d) Click **Apply**.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Step 7 Configure access to local GUI, LAN ports, and local SSID of the OfficeExtend access points:

a) Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

b) Under OEAP Config Parameters, select or unselect the **Disable Local Access** check box to enable or disable local access of the OfficeExtend access points.

Note By default, the **Disable Local Access** check box is unselected and therefore the Ethernet ports and personal SSIDs are enabled. This configuration does not affect remote LAN. The port is enabled only when you configure a remote LAN.

Step 8 Configure split tunneling for the OfficeExtend access points as follows:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.

b) In the OEAP Config Parameters area, select or unselect the **Disable Split Tunnel** check box.
Disabling split tunneling here disables split tunneling for all the WLANs and remote LANs. You can also disable split tunneling on a specific WLAN or remote LAN.

c) Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 If your controller supports only OfficeExtend access points, see the Configuring RRM section for instructions on setting the recommended values for the DCA interval, channel scan duration, and neighbor packet frequency.

Configuring OfficeExtend Access Points (CLI)

- Enable FlexConnect on the access point by entering this command:
  config ap mode flexconnect *Cisco_AP*

- Configure one or more controllers for the access point by entering one or all of these commands:
  config ap primary-base *controller_name Cisco_AP controller_ip_address*

  config ap secondary-base *controller_name Cisco_AP controller_ip_address*

  config ap tertiary-base *controller_name Cisco_AP controller_ip_address*

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

- Enable the OfficeExtend mode for this access point by entering this command:
  config flexconnect office-extend {**enable** | **disable**} *Cisco_AP*

  The default value is enabled. The **disable** parameter disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter this command:

  clear ap config *cisco-ap*

  If you want to clear only the access point's personal SSID, enter this command:

  config flexconnect office-extend clear-personalssid-config *Cisco_AP*

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point or for all access points using the **config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all**} command. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using the **config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using the **config ap** {**telnet** | **ssh**} {**enable** | **disable**} *Cisco_AP* command.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using the **config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

- Enable the access point to choose the controller with the least latency when joining by entering this command:
  config flexconnect join min-latency {**enable** | **disable**} *Cisco_AP*

  The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco WLC that responds first.

- Configure a specific username and password that users at home can enter to log into the GUI of the OfficeExtend access point by entering this command:
  config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

  The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

- To configure access to the local network for the Cisco OfficeExtend access points, enter the following command:
  config network oeap local-network {**enable** | **disable**}

When disabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote LAN configuration if configured on the access points.

- Configure the Dual R-LAN Ports feature, which allows the Ethernet port 3 of Cisco OfficeExtend access points to operate as a remote LAN by entering this command:
  config network oeap dual-rlan-ports {**enable** | **disable**}

  This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

  The remote LAN mapping is different depending on whether the default group or AP Groups is used:

  - Default Group—If you are using the default group, a single remote LAN with an even numbered remote LAN ID is mapped to port 4. For example, a remote LAN with remote LAN ID 2 is mapped to port 4. The remote LAN with an odd numbered remote LAN ID is mapped to port 3. For example, a remote LAN with remote LAN ID 1 is mapped to port 3.
  - AP Groups—If you are using an AP group, the mapping to the OEAP ports is determined by the order of the AP groups. To use an AP group, you must first delete all remote LANs and WLANs from the AP group leaving it empty. Then, add the two remote LANs to the AP group adding the port 3 AP remote LAN first, and the port 4 remote group second, followed by any WLANs.

- Enable or disable split tunneling by entering this command:
  config network oeap split-tunnel {**enable** | **disable**}
  Disabling split tunneling here disables split tunneling for all the WLANs and remote LANs. You can also disable split tunneling on a specific WLAN or remote LAN.
- Enable split tunneling without gateway override by entering this command:
  config wlan split-tunnel *wlan-id* **enabled apply-acl** *acl name*
- Enable split tunneling with gateway override by entering this command:
  config wlan split-tunnel *wlan-id* **enabled override gateway** *gateway ip* **mask** *subnet mask* **apply-acl** *acl name*
- Save your changes by entering this command:
  save config

Note If your controller supports only OfficeExtend access points, see the Configuring Radio Resource Management section for instructions on setting the recommended value for the DCA interval.

Configuring Split Tunneling for a WLAN or a Remote LAN

Configuring Split Tunneling for a WLAN or a Remote LAN (GUI)

Step 1 Choose **WLANs** and click the WLAN ID to open the WLANs > Edit page.
The WLAN that you choose can be a WLAN or a remote LAN depending on its configuration.

Step 2 Click the **Advanced** tab.

Step 3 In the OEAP area, select or unselect the **Split Tunnel** check box.

Step 4 Select the **Gateway Override** check box to configure the **Gateway IP** and **Subnet Mask**. The interface mapped to the WLAN or RLAN will be used if the checkbox is unchecked.

Step 5 From the drop-down list select the **Associated ACL**. If you choose None, an error message appears indicating that you must choose an ACL.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring Split Tunneling for a WLAN or a Remote LAN (CLI)

- Enable or disable split tunneling for a WLAN by entering this command:
  config wlan split-tunnel *wlan-id* {**enable** | **disable**}
- See the split tunneling status for a WLAN by entering this command:
  show wlan *wlan-id*
- Enable or disable split tunneling for a remote LAN by entering this command:
  config remote-lan split-tunnel *rlan-id* {**enable** | **disable**}
- See the split tunneling status for a remote LAN by entering this command:
  show remote-lan *rlan-id*

Note When a remote LAN or wireless client on a corporate SSID communicate among themselves, all the traffic on the corporate SSID and remote LAN is tunneled back to the controller.

Configuring OEAP ACLs

Configuring OEAP ACLs (GUI)

Step 1 Choose **Wireless** > **OEAP ACLs** .
The **OEAP ACL** page is displayed.

This page lists all the OEAP ACLs configured on the controller. To remove an ACL, hover your mouse over the blue drop-down arrow adjacent to the corresponding ACL name and choose **Remove**.

Step 2 Add a new ACL by clicking **New**.
The **Access Control Lists** > **New** page is displayed.

Step 3 In the **Access Control List Name** text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

Step 5 When the Access Control Lists page reappears, click the name of the new ACL.
When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists** > **Rules** > **New** page is displayed.

Step 6 Configure a rule for this ACL as follows:

a) The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the **Sequence** text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- **Any—**Any source (This is the default value.)
- **IP Address—**A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding text boxes.

c) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any—**Any destination (This is the default value.)
- **IP Address—**A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.
- **Network List—**A specific network list. If you choose this option, enter the corporate subnets configured in the network list.

d) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- **Any—**Any protocol (This is the default value.)
- **TCP**
- **UDP**
- **Other—**Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose Other, enter the number of the desired protocol in the **Protocol** text box. You can find the list of available protocols in the INAI website.

e) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, **Permit** to cause this ACL to allow packets, or **Nat-route** to route all packets matching the rule to the local network or NAT the packets matching the rule to the internet.The default value is **Deny**.

f) Click **Apply**.
The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

g) Repeat this procedure to add additional rules, if any, for this ACL.

Step 7 Click **Save Configuration**.

Configuring OEAP ACLs (CLI)

Step 1 Create or delete an ACL by entering this command:
config oeap-acl create|delete

Step 2 Create an ACL rule by entering this command:
config oeap-acl rule

Step 3 Specify the action of an ACL rule by entering this command:
config oeap-acl rule action

Step 4 Specify the destination for an ACL rule by entering this command:
config oeap-acl rule destination mode address|local|network-list

Step 5 Specify the destination port for an ACL rule by entering this command:
config oeap-acl rule destination port

Step 6 Specify the source address for an ACL rule by entering this command:
config oeap-acl rule source address

Step 7 Specify the source port for an ACL rule by entering this command:
config oeap-acl rule source port

Step 8 Specify the protocol for an ACL rule by entering this command:
config oeap-acl rule protocol *protocol*

where *protocol*parameter is a value between 0 and 255 or any.

Step 9 Swap the indices or precedence of two ACL rules by entering this command:
config oeap-acl rule swap index

Step 10 Change the indices or precedence of an ACL rule by entering this command:
config oeap-acl rule change index

Step 11 Delete an ACL rule by entering this command:
config oeap-acl rule delete

Step 12 List all the ACLs by entering this command:
show oeap-acl summary

Step 13 Display the details of a particular ACL by entering this command:
show oeap-acl detailed*ACL_name*

Configuring a Personal SSID on an OfficeExtend Access Point Other than 600 Series OEAP

The Cisco 600 Series OEAPs are not supported from Cisco Wireless Release 8.4.

Step 1 Find the IP address of your OfficeExtend access point by doing one of the following:

- Log on to your home router and look for the IP address of your OfficeExtend access point.
- Ask your company's IT professional for the IP address of your OfficeExtend access point.
- Use an application such as Network Magic to detect devices on your network and their IP addresses.

Step 2 With the OfficeExtend access point connected to your home router, enter the IP address of the OfficeExtend access point in the Address text box of your Internet browser and click **Go**.

Note Make sure that you are not connected to your company's network using a virtual private network (VPN) connection.

Step 3 When prompted, enter the username and password to log into the access point.

Step 4 On the OfficeExtend Access Point Welcome page, click **Enter**. The OfficeExtend Access Point Home page appears.

Step 5 Choose **Configuration** to open the Configuration page.

Step 6 In the SSID text box, enter the personal SSID that you want to assign to this access point. This SSID is locally switched.

Note A controller with an OfficeExtend access point publishes only up to 15 WLANs to each connected access point because it reserves one WLAN for the personal SSID.

Step 7 From the Security drop-down list, choose **Open**, **WPA2/PSK (AES)**, or **104 bit WEP** to set the security type to be used by this access point.

Note If you choose WPA2/PSK (AES), make sure that the client is configured for WPA2/PSK and AES encryption.

Step 8 If you chose WPA2/PSK (AES) in *Step 8*, enter an 8- to 38-character WPA2 passphrase in the Secret text box. If you chose 104 bit WEP, enter a 13-character ASCII key in the Key text box.

Step 9 Click **Apply**.

Note If you want to use the OfficeExtend access point for another application, you can clear this configuration and return the access point to the factory-default settings by clicking **Clear Config**. You can also clear the access point's configuration from the controller CLI by entering the **clear ap config** *Cisco_AP* command.

These steps can be used for configuring a personal SSID on OfficeExtend access points only. See the *Aironet 600 Series OfficeExtend Access Point Configuration Guide* for information on configuring a personal SSID on OEAP 600 APs.

Viewing OfficeExtend Access Point Statistics

Use these commands to view information about the OfficeExtend access points on your network:

- See a list of all OfficeExtend access points by entering this command:

  show flexconnect office-extend summary

- See the link delay for OfficeExtend access points by entering this command:

show flexconnect office-extend latency

- See the encryption state of all access points or a specific access point by entering this command:

  show ap link-encryption {**all** | *Cisco_AP*}

  This command also shows authentication errors, which track the number of integrity check failures, and replay errors, which track the number of times that the access point receives the same packet. See the data plane status for all access points or a specific access point by entering this command:

  show ap data-plane {**all** | *Cisco_AP*}

Viewing Voice Metrics on OfficeExtend Access Points

Use this command to view information about voice metrics on the OfficeExtend access points in your network:

show ap stats 802.11{a | b} *Cisco_AP*
Information similar to the following appears:

```
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Background:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Video:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Voice:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
```

View the voice metrics on the OfficeExtend access points in your network using the WLC GUI as follows:

- Choose**Wireless** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n**. The 802.11a/n/ac Radios or 802.11b/g/n Radios page appears.
- Hover your cursor over the blue drop-down arrow for the desired access point and click the **Detail** link for the desired client to open the Radio > Statistics page.

  This page shows the **OEAP WMM counters** for this access point.

Running Network Diagnostics

Information About Running Network Diagnostics

Network Diagnostics determines the non-DTLS throughput of the system by running a speed test on demand. Network Diagnostics allows troubleshooting of root causes leading to failures. It also determines the link latency and jitter by running a test on demand or periodically.

Running Network Diagnostics (GUI)

Step 1 Choose **WAN** > **Network Diagnostics**.
The Network Diagnostics page is displayed.

Step 2 Click **Start Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics on the Controller

Step 1 Choose **Wireless** > **All APs** > **Details**.

Step 2 Choose the **Network Diagnostics** tab.
The Network Diagnostics page is displayed.

Step 3 Click **Start Network Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics (CLI)

- To run network diagnostics, enter this command on the Cisco WLC:
show ap network-diagnostics *Ap_Name*

Remote LANs

Information About Remote LANs

This section describes how to configure remote LANs.

Prerequisites

- You must remove all remote LANs from a controller's configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later.
- Remote LAN can be applied on a dedicated LAN port on a Cisco Aironet 600 Series OEAP.

Restrictions

- Only four clients can connect to a Cisco Aironet 600 Series OEAP through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.
- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

Configuring a Remote LAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.
This page lists all of the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs/Remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/Remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a Remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the row, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point’s radio.

Step 2 Create a new Remote-LAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.

Step 3 From the Type drop-down list, choose **Remote LAN** to create a remote LAN.

Step 4 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

Step 5 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 6 Click **Apply** to commit your changes. The **WLANs > Edit** page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 7 Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

Step 8 On the General tab, select the **Status** check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.

Note You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

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

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

Configuring a Remote LAN (CLI)

- See the current configuration of the remote LAN by entering this command:

  show remote-lan *remote-lan-id*

- Enable or disable remote LAN by entering this command:

  config remote-lan {**enable** | **disable**} *remote-lan-id*

- Enable or disable 802.1X authentication for remote LAN by entering this command:

  config remote-lan security 802.1X {**enable** | **disable**} *remote-lan-id*

  Note The encryption on a remote LAN is always “none.”

- Enable or disable local EAP with the controller as an authentication server, by entering this command:

  config remote-lan local-auth enable *profile-name remote-lan-id*

- If you are using an external AAA authentication server, use the following command:

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id server id*

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id*